Introduction to Semigroup Theory

ทฤษฎีกึ่งกรุปเบื้องต้น

$$
\begin{tikzcd}
 & \mathcal{J} \arrow[d, dash] & \\
 & \mathcal{D} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathcal{L} \arrow[dr, dash] & & \mathcal{R} \arrow[dl, dash] \\
 & \mathcal{H} &
\end{tikzcd}
$$

ผศ.ดร. อนันต์ยา อนันตยเศรษฐี

คำนำ

ตำราสอนเล่มนี้แต่งขึ้นโดยมีจุดมุ่งหมายเพื่อใช้เป็นตำราเรียนในรายวิชา กึ่งกรุปเบื้องต้น (Introduction to Semigroup Theory) ในหลักสูตรคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยมหาสารคาม ตำรากึ่งกรุปส่วนใหญ่จะเป็นภาษาอังกฤษ และมีจำนวนน้อย นิสิตมีความยากลำบากต่อการทำความเข้าใจ ผู้เขียนจึงได้พยายามเรียบเรียงตำราเล่มนี้ขึ้นมา สำหรับให้ผู้เรียนได้ศึกษาเนื้อหาวิชา อย่างกว้างๆและมีตัวอย่างประกอบเพื่อให้เกิดความเข้าใจมากยิ่งขึ้น ตำราฉบับนี้ปรับปรุงมาจากเอกสารประกอบการสอนที่ใช้สอนมาตั้งแต่ปีการศึกษา 2557 โดยเพิ่มเนื้อหาและรายละเอียดในแต่ละบทให้มากขึ้น

บทแรก เป็นการทบทวนความรู้พื้นฐานที่จำเป็นต้องใช้ในการศึกษา และกล่าวถึง นิยาม ความรู้เบื้องต้นเกี่ยวกับกึ่งกรุป ตลอดจนกึ่งกรุปชนิดต่างๆ

บทที่ 2 กล่าวถึงไอดีล ไอดีลมุขสำคัญ ไอดีลแท้ กึ่งกรุปเชิงเดียว กึ่งกรุปศูนย์เชิงเดียว

บทที่ 3 กล่าวถึงสาทิสสัณฐาน สมสัณฐาน สมภาค และกึ่งกรุปผลหาร

บทที่ 4 เป็นการศึกษาความสัมพันธ์ของกรีนชนิดต่างๆ

บทที่ 5 ศึกษาเกี่ยวกับกึ่งกรุปผกผัน

ผู้เขียนขอขอบคุณ ผศ.ดร. ประกิต จำปาชนม์ ผู้สอนวิชากึ่งกรุปให้ผู้เขียนเป็นคนแรก ขอขอบคุณ ผศ.ดร.ดรุณี บุญชารี ผู้ช่วยช่วยเหลือแนะนำการใช้โปรแกรมลาเท็กซ์ในการจัดพิมพ์ต้นฉบับ ขอบคุณนิสิตภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ มหาวิทยาลัยมหาสารคาม ที่ช่วย ให้ตำราเล่มนี้สำเร็จด้วยดี ผู้เขียนตระหนักดีว่าคงมีความผิดพลาดบ้างในการเรียบเรียงตำราเล่มนี้ จึงขออภัยมาล่วงหน้า

อนันต์ยา อนันตยเศรษฐี
ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์
มหาวิทยาลัยมหาสารคาม
ธันวาคม 2560

สารบัญ

เรื่อง **หน้า**

รายละเอียดเอกสารประกอบการสอน

1) **ชื่อวิชา** กึ่งกลุ่ม (Semigroups)
รหัสวิชา 0201 510 วิชาระดับปริญญาตรี
จำนวนหน่วยกิต 3(3-0-6)

2) **คำอธิบายรายวิชา**
ความรู้พื้นฐาน ไอดีล กึ่งกรุปแถบ เซมิแลตทิซ กึ่งกรุปศูนย์ กึ่งกรุปเชิงเดียว
ทางซ้ายและกึ่งกรุปเชิงเดียวทางขวา กึ่งกรุปปรกติ กึ่งกรุปผกผัน กึ่งกรุปผลหาร ความสัมพันธ์ของกรีน
Basic concepts, ideals, bands, semilattices, zero semigroups left and right simple semigroups, normal semigroups, inverse semigroups, quotient semigroups, Green's relations.

3) **วัตถุประสงค์**
กึ่งกรุปเป็นโครงสร้างทางคณิตศาสตร์แบบหนึ่งที่มีผู้ศึกษาและทำวิจัยอย่าง กว้างขวาง โครงสร้างของกึ่งกรุปมีลักษณะไม่ซับซ้อนมากนักเมื่อเทียบกับโครงสร้าง ทางคณิตศาสตร์แบบอื่นๆทำให้ง่ายต่อการทำความเข้าใจ นอกจากนี้ยังมีการนำความรู้ทางด้านนี้ไปประยุกต์ใช้กับสาขาอื่น เช่น นำไปประยุกต์ใช้ทางวิทยาศาสตร์คอมพิวเตอร์ จุดมุ่งหมายของรายวิชานี้ จึงเพื่อให้ผู้เรียนศึกษาและเข้าใจแนวคิดพื้นฐาน รูปแบบของ โครงสร้างของกึ่งกรุป ชนิดของกึ่งกรุปในแบบต่างๆ ตลอดจนเพื่อเป็นพื้นฐานความรู้ในการศึกษา ในขั้นสูงต่อไป

4) **ระยะเวลาในการสอน**

1. จำนวน 15 สัปดาห์ รวมทั้งสิ้น 45 ชั่วโมง
2. จำนวนชั่วโมงบรรยายต่อสัปดาห์ บรรยาย 3 ชั่วโมง

5) **กิจกรรมการเรียนการสอน**

1. บรรยาย - ซักถาม

2. ศึกษาเพิ่มเติมจากตัวอย่าง
3. ฝึกทักษะการแก้ปัญหาจากแบบฝึกหัด
4. ทดสอบย่อย

6) **วัสดุและอุปกรณ์การสอน**

1. เอกสารประกอบการสอน
2. กระดาษ

7) **หนังสืออ่านประกอบ**

1. R. Butkote, **Universal-algebraic and Semigroup-theoretical Properties of Boolean Operations** : Dissertation Universitat Potsdam, 2009.
2. T. Harju. **Lecture Note on Semigroups**. Department of Mathematics, Turku University, Finland, 1996.
3. J. Howie. **Fundamentals of Semigroups Theory**. USA: Oxford University Press Inc. 1995.
4. J. Howie and N. Ruskuc. **Semigroups and Applications**. USA: World Scientific Publishing Co. Pte. Ltd, 1998.

8) **การประเมินผล**

1. การบ้านและงานที่ได้รับมอบหมาย 10 %
2. ทดสอบครั้งที่ 1 บทที่ 1 - บทที่ 2 30 %
3. ทดสอบครั้งที่ 2 บทที่ 3 - บทที่ 4 30 %
4. ทดสอบครั้งที่ 3 บทที่ 5 30 %

9) **เกณฑ์การประเมิน**

1. คะแนน 30 - 100 คะแนน ตัดเกรดโดยอิงเกณฑ์ เกรด A - D
2. คะแนน 0 - 29 คะแนน ตัดเกรดโดยอิงเกณฑ์ เกรด F

รายละเอียดแผนการสอน

รายวิชา 0201 510 กึ่งกลุ่ม

จำนวน 3 หน่วยกิต

สัปดาห์ที่	จำนวนชั่วโมง	บทที่ / เนื้อหา	กิจกรรมการเรียนการสอน	สื่อการสอน
1	3	บทที่ 1 1.ความรู้พื้นฐาน 2. นิยามและสมบัติเบื้องต้นของกึ่งกรุป 3. กึ่งกรุปของการดำเนินการบูลีน n ภาค	1. บรรยาย-ซักถาม 2.ศึกษาเพิ่มเติมจากตัวอย่าง 3.ฝึกทักษะจากแบบฝึกหัด	เอกสารประกอบการสอน
2	3	4. สมาชิกพิเศษ 5. กึ่งกรุปย่อย 6. กึ่งกรุปแถบ, แถบมุมฉาก	1. บรรยาย-ซักถาม 2.ศึกษาเพิ่มเติมจากตัวอย่าง 3.ฝึกทักษะจากแบบฝึกหัด	เอกสารประกอบการสอน
3	3	7. กึ่งกรุปนอร์มัล กึ่งกรุปว่าง 8. กึ่งกรุปศูนย์, เซมิแลตทิซ 9. กึ่งกรุปปรกติ	1. บรรยาย-ซักถาม 2.ศึกษาเพิ่มเติมจากตัวอย่าง 3.ฝึกทักษะจากแบบฝึกหัด	เอกสารประกอบการสอน
4	3	บทที่ 2 1. ไอดีล, ไอดีลแท้ 2. ไอดีลที่ก่อกำเนิดโดยเซตย่อย	1. บรรยาย-ซักถาม 2.ศึกษาเพิ่มเติมจากตัวอย่าง 3.ฝึกทักษะจากแบบฝึกหัด	เอกสารประกอบการสอน
5-6	3	3.กึ่งกรุปเชิงเดียว, 0-เชิงเดียว	1.บรรยาย-ซักถาม 2.ศึกษาเพิ่มเติมจากตัวอย่าง 3.ฝึกทักษะจากแบบฝึกหัด	เอกสารประกอบการสอน
		สอบครั้งที่ 1 30 %		

สัปดาห์ที่	จำนวนชั่วโมง	บทที่ / เนื้อหา	กิจกรรมการเรียนการสอน	สื่อการสอน
7	3	<u>บทที่ 3</u> 1. สาทิสสัณฐาน 2. สมภาค	1.บรรยาย-ซักถาม 2.ศึกษาเพิ่มเติมจากตัวอย่าง 3.ฝึกทักษะจากแบบฝึกหัด	เอกสารประกอบการสอน
8	3	3. กึ่งกรุปผลหาร 4. สาทิสสัณฐานธรรมชาติ	1.บรรยาย-ซักถาม 2.ศึกษาเพิ่มเติมจากตัวอย่าง 3.ฝึกทักษะจากแบบฝึกหัด	เอกสารประกอบการสอน
9	3	<u>บทที่ 4</u> 1. ความสัมพันธ์ของกรีนแบบ L, R	1.บรรยาย-ซักถาม 2.ศึกษาเพิ่มเติมจากตัวอย่าง 3.ฝึกทักษะจากแบบฝึกหัด	เอกสารประกอบการสอน
10	3	2. ความสัมพันธ์ของกรีนแบบ H, D	1.บรรยาย-ซักถาม 2.ศึกษาเพิ่มเติมจากตัวอย่าง 3.ฝึกทักษะจากแบบฝึกหัด	เอกสารประกอบการสอน
		สอบครั้งที่ 2 30 %		
11	3	<u>บทที่ 5</u> 1. สมาชิกผกผันในกึ่งกรุป	1.บรรยาย-ซักถาม 2.ศึกษาเพิ่มเติมจากตัวอย่าง 3.ฝึกทักษะจากแบบฝึกหัด	เอกสารประกอบการสอน
12	3	2.กึ่งกรุปผกผัน	1.บรรยาย-ซักถาม 2.ศึกษาเพิ่มเติมจากตัวอย่าง 3.ฝึกทักษะจากแบบฝึกหัด	เอกสารประกอบการสอน
13	3	3. สมาชิกนิจพลกับกึ่งกรุปผกผัน	1.บรรยาย-ซักถาม 2.ศึกษาเพิ่มเติมจากตัวอย่าง 3.ฝึกทักษะจากแบบฝึกหัด	เอกสารประกอบการสอน

สัปดาห์ที่	จำนวนชั่วโมง	บทที่ / เนื้อหา	กิจกรรมการเรียนการสอน	สื่อการสอน
14	3	4.สมาชิกเรกูลาร์กับกึ่งกรุปผกผัน	1.บรรยาย-ซักถาม 2.ศึกษาเพิ่มเติมจากตัวอย่าง 3.ฝึกทักษะจากแบบฝึกหัด	เอกสารประกอบการสอน
15	3	5.กึ่งกรุปผกผันและความสัมพันธ์ของกรีน	1.บรรยาย-ซักถาม 2.ศึกษาเพิ่มเติมจากตัวอย่าง 3.ฝึกทักษะจากแบบฝึกหัด	เอกสารประกอบการสอน
		สอบครั้งที่ 3 30 %		

บทที่ 1

ความรู้เบื้องต้น (Basic Concepts)

การศึกษากึ่งกรุปอย่างเป็นทางการเริ่มขึ้นราวๆศตวรรษที่ 20 แนวคิดของกึ่งกรุป นับว่า มีความสำคัญต่อการศึกษาคณิตศาสตร์ในหลากหลายด้าน ในทางคณิตศาสตร์ประยุกต์ ได้ใช้กึ่งกรุปเป็นตัวแบบพื้นฐาน (fundamental model) สำหรับการศึกษาระบบเชิงเส้นที่ไม่ แปรเปลี่ยนตามเวลา (linear time-invariant system) นับตั้งแต่ปี ค.ศ. 1950 เป็นต้นมา กึ่งกรุปมีบทบาทสำคัญในการ ศึกษาทฤษฎีวิทยาการคอมพิวเตอร์ ทั้งนี้เพราะโครงสร้างของกึ่งกรุปจำกัดมีความเชื่อมโยงกับออโตมาตาจำกัด (finite automata) การที่ออโตมาตาจะทำงานได้นั้นต้องอาศัยภาษา (langauges) ในการสร้างภาษา เราต้องศึกษาทฤษฎีของไวยากรณ์ (grammar) ภาษาเรกูลาร์ (regular langauges) ภาษาทางการ (formal langauges) ซึ่งอาศัยโครงสร้างของกึ่งกรุปเพราะลักษณะของการสร้างประโยคของภาษานั้นอาศัย สมบัติของการปิดและการเปลี่ยนกลุ่ม ซึ่งเป็นเงื่อนไขของระบบทางคณิตศาสตร์ที่เป็นกึ่งกรุป นอกจากนี้แล้วโครงสร้างของกึ่งกรุป มีความซับซ้อนน้อยกว่าโครงสร้างทางพีชคณิตนามธรรมอื่นๆ

ในบทนี้จะกล่าวถึงนิยามและผลลัพธ์เบื้องต้นที่จะนำไปใช้ในการศึกษาในบทต่อๆไป

1.1 ทบทวนความรู้พื้นฐาน (Preliminaries)

บทนิยาม 1.1 ผลคูณคาร์ทีเซียน (cartesian product) ของเซตไม่ว่าง A และ B เขียนแทนด้วย $A \times B$ ซึ่งกำหนดโดย

$$A \times B = \{(a, b) | a \in A, b \in B\}$$

บทนิยาม 1.2 ความสัมพันธ์ (relation) R จากเซต A ไปเซต B คือสับเซตของ $A \times B$

ถ้า R เป็นความสัมพันธ์จากA ไป A เราจะกล่าวว่า R เป็นความสัมพันธ์ใน A หรือความสัมพันธ์บน A

ถ้า $(a, b) \in R$ เราจะกล่าวว่า a มีความสัมพันธ์ R ต่อ b เขียนแทนด้วย aRb

ตัวอย่าง 1.1 กำหนด $A = \{a, b, c, d\}$ และ $B = \{x, y, z\}$ จะได้ว่า

$R_1 = \{(a, x), (a, y), (c, z), (d, x)\}$ เป็นความสัมพันธ์จาก A ไป B

$R_2 = \{(a,a),(a,b),(c,d),(c,c),(d,a)\}$ เป็นความสัมพันธ์จาก A ไป A หรือเป็นความสัมพันธ์บน A

$R_3 = A \times B$ เป็นความสัมพันธ์จาก A ไป B

$R_4 = \{(a,x),(b,y),(c,z),(d,a)\}$ ไม่เป็นความสัมพันธ์จาก A ไป B เพราะ $(d,a) \notin A \times B$

$R_5 = \{(a,x),(b,y),(c,z)\}$ เป็นความสัมพันธ์จาก A ไป B

$R_6 = \{(a,x),(b,x),(c,z),(d,y)\}$ เป็นความสัมพันธ์จาก A ไป B

บทนิยาม 1.3 กำหนด R เป็นความสัมพันธ์บนเซต A

1) R มี **สมบัติสะท้อน** (reflexive property) ก็ต่อเมื่อ $\forall x \in A\big((x,x) \in R\big)$

2) R มี **สมบัติสมมาตร** (symmetric property) ก็ต่อเมื่อ $\forall x,y \in A\big((x,y) \in R \rightarrow (y,x) \in R\big)$

3) R มี**สมบัติการถ่ายทอด** (transitive property) ก็ต่อเมื่อ $\forall x,y \in A\big((x,y) \in R \wedge (y,z) \in R \rightarrow (x,z) \in R\big)$

บทนิยาม 1.4 กำหนด R เป็นความสัมพันธ์ในเซต A R เป็น**ความสัมพันธ์สมมูล** (equivalence relation) ก็ต่อเมื่อ R มีสมบัติสะท้อน สมมาตรและถ่ายทอด

บทนิยาม 1.5 ให้ $\sim$ เป็นความสัมพันธ์สมมูลในเซต A และ $a \in A$ **ชั้นสมมูล** (equivalence class) ของ a เขียนแทนด้วย $[a]_\sim$ หมายถึง เซตของสมาชิกทั้งหมดของ A ที่มีความสัมพันธ์ $\sim$ กับ a นั่นคือ

$$[a]_\sim = \{x \in A | x \sim a\} = \{x \in A | (x,a) \in \sim\}$$

ตัวอย่าง 1.2 กำหนด $A = \{a,b,c\}$ และกำหนด R_1, R_2 และ R_3 ดังนี้

$$R_1 = \{(a,a),(a,b),(b,c)\}$$
$$R_2 = \{(a,a),(a,b),(b,a),(b,b),(c,c)\}$$
$$R_3 = \{(a,a),(a,b),(a,c),(b,a),(b,b),(c,c)\}$$

จะได้ว่า R_1 ไม่มีสมบัติ สะท้อน สมมาตร และถ่ายทอด

R_2 มีสมบัติ สะท้อน สมมาตร และถ่ายทอด

R_3 มีสมบัติ สะท้อน แต่ไม่มีสมบัติสมมาตร และถ่ายทอด

ดังนั้น R_2 เป็นความสัมพันธ์สมมูล แต่ R_1 และ R_3 ไม่เป็นความสัมพันธ์สมมูล

ตัวอย่าง 1.3 กำหนด S เป็นเซตจำกัดที่ไม่ว่าง และ $P(S)$ เป็นเซตกำลัง(power set) ของ S จะได้ว่า ความสัมพันธ์ " เป็นสับเซตของ " บน $P(S)$ ไม่เป็นความสัมพันธ์สมมูล ทั้งนี้เพราะขาดสมบัติการสมมาตร

ทฤษฎีบท 1.1 ให้ $\sim$ เป็นความสัมพันธ์สมมูลบนเซต A และ $a, b \in A$ จะได้ว่า

1) $a \sim b$ ก็ต่อเมื่อ $[a]_\sim = [b]_\sim$

2) ถ้า $a \in [b]_\sim$ แล้ว $[a]_\sim = [b]_\sim$

3) $\{[x]_\sim \mid x \in A\}$ เป็นพาร์ทิชัน (partition) ของ A

บทนิยาม 1.6 ให้ f เป็นความสัมพันธ์จาก A ไป B จะกล่าวว่า f เป็นฟังก์ชัน (function) ก็ต่อเมื่อ ถ้า $(x, y) \in f$ และ $(x, z) \in f$ แล้ว $y = z$

ตัวอย่าง 1.4 จาก **ตัวอย่าง** 1.1 จะได้ว่า R_1, R_3, R_4 ไม่เป็นฟังก์ชันจาก A ไป B แต่ R_5, R_6 เป็นฟังก์ชันจาก A ไป B

บทนิยาม 1.7 ให้ S เป็นเซตไม่ว่าง **การดำเนินการทวิภาค** (binary operation) บนเซต S คือ ฟังก์ชันจาก $S \times S$ ไปยัง S

สำหรับการดำเนินการทวิภาค $*$ บน S เราให้ $a * b$ เป็นสมาชิกใน Sที่ถูกจับคู่โดย $(a, b) \in S \times S$ ภายใต้ $*$ นั่นคือ

$$(a, b) \mapsto a * b$$

หมายเหตุ 1.1 สำหรับ $a * b$ เพื่อความสะดวกเราอาจเขียนละเครื่องหมายการดำเนินการทวิภาคได้ นั่นคือเขียนแทน $a * b$ ด้วย ab

ตัวอย่าง 1.5 ให้ $S = \{1, 2, 3\}$ นิยามการกระทำทวิภาค $*$ บน S โดย $a * b = b$ จะได้ว่า $1 * 2 = 2$, $2 * 3 = 3$ และ $3 * 1 = 1$ เป็นต้น

ตัวอย่าง 1.6 นิยามการกระทำทวิภาค $\bullet$ บน Z^+ โดยสำหรับ $a, b \in Z^+$, $a \bullet b = a + 1$ จะได้ว่า $2 \bullet 3 = 2 + 1 = 3$, $5 \bullet 5 = 5 + 1 = 6$ และ $10 \bullet 15 = 10 + 1 = 11$ เป็นต้น

ในการนิยามการดำเนินการทวิภาคบนเซต S ที่กำหนด สิ่งที่เราต้องตรวจสอบเพื่อให้แน่ใจว่าการนิยามเช่นนั้นเป็นการดำเนินการทวิภาคหรือไม่ ก็คือ แต่ละคู่ลำดับของสมาชิกของ S ถูกจับคู่กับสมาชิกของ S เพียงตัวเดียวเท่านั้นโดยการกระทำนี้หรือไม่ สำหรับเงื่อนไขที่ว่า แต่ละคู่ลำดับ ของสมาชิกของ S ถูกจับคู่กับสมาชิกของ S

โดยการกระทำ $*$ เราจะกล่าวว่า S **ปิด** (closed) ภายใต้การดำเนินการ $*$ นั่นคือ S ปิดภายใต้การดำเนินการ $*$ ถ้า $a, b \in S$ แล้ว $a * b \in S$

จาก **ตัวอย่าง** 1.5 เนื่องจาก $*$ เป็นการดำเนินการทวิภาคดังนั้นจึงอนุญาตให้กระทำได้ ทีละสองสมาชิก สมมติว่าเราต้องการพิจารณา $a * b * c$ ซึ่งมีสามสมาชิกจะทำได้อย่างไร การที่จะหาผลลัพธ์ของ $a * b * c$ นั้น เราอาจหา $(a * b) * c$ หรือ $a * (b * c)$ เช่น ถ้า $a = 1, b = 2, c = 3$ จะได้ว่า $(1 * 2) * 3 = 2 * 3 = 3$ และ $1 * (2 * 3) = 1 * 3 = 3$ ดังนั้น $(1 * 2) * 3 = 1 * (2 * 3)$ ยิ่งไปกว่านั้นเราได้ว่า $(a * b) * c = b * c = c = a * c = a * (b * c)$ สำหรับ $a, b, c \in S$ แต่สำหรับ **ตัวอย่าง** 1.6 เราพบว่า $(1 \bullet 2) \bullet 3 = (1 + 1) \bullet 3 = 2 \bullet 3 = 2 + 1 = 3$ แต่ $1 \bullet (2 \bullet 3) = 1 \bullet (2 + 1) = 1 \bullet 3 = 1 + 1 = 2$ ดังนั้น $(a \bullet b) \bullet c \neq a \bullet (b \bullet c)$

การดำเนินการทวิภาคบนเซตจำกัดสามารถแสดงแทนด้วยตาราง นั่นคือ สำหรับเซตจำกัด S นิยามการดำเนินการทวิภาค $*$ บน S โดยใช้กฏ

สมาชิกในตำแหน่งที่ i ทางซ้าย $*$ สมาชิกในตำแหน่งที่ j ทางด้านบน = สมาชิกในตำแหน่งแถวที่ i หลักที่ j ในตัวตาราง

ตัวอย่าง 1.7 ตารางที่กำหนดต่อไปนี้นิยามการดำเนินการทวิภาค $*$ บนเซต $S = \{1, 2, 3\}$

*	1	2	3
1	1	2	2
2	3	3	3
3	2	3	1

จากตารางเราพบว่า $1 * 2 = 2$, $3 * 1 = 2$ เป็นต้น

บทนิยาม 1.8 การดำเนินการทวิภาค $*$ บน S จะกล่าวว่า มีสมบัติ **การเปลี่ยนกลุ่ม** (associative) ก็ต่อเมื่อ $a * (b * c) = (a * b) * c$ สำหรับทุก $a, b, c \in S$ และจะกล่าวว่า $*$ มี **สมบัติการสลับที่** (commutative) ก็ต่อเมื่อ $a * b = b * a$ สำหรับทุก $a, b \in S$

ตัวอย่าง 1.8

1) จาก **ตัวอย่าง** 1.7 จะพบว่า $*$ ไม่มีสมบัติการเปลี่ยนกลุ่ม ทั้งนี้เพราะว่า $(1 * 2) * 1 = 3 \neq 2 = 1 * (2 * 1)$

2) การบวกปกติ (usual addition) $+$ บนเซตของจำนวนเต็มมีสมบัติการเปลี่ยนกลุ่ม

3) การคูณปกติ (usual multiplication) $\times$ บนเซตของจำนวนจริง มีสมบัติการเปลี่ยนกลุ่ม

หมายเหตุ 1.2 ถ้าการดำเนินการทวิภาค $*$ มีสมบัติการเปลี่ยนกลุ่ม แล้วตำแหน่งของเครื่องหมายวงเล็บ ไม่มีผลต่อผลลัพธ์ ดังนั้นเราอาจเขียน

$$a_1a_2a_3\ldots a_n = a_1(a_2(a_3(\ldots(a_{n-1}a_n))\ldots)$$

1.2 นิยามและสมบัติเบื้องต้นของกึ่งกรุป (Semigroups)

บทนิยาม 1.9 กรุปพอยด์ (groupoid) คือระบบ $(S\,;*)$ ซึ่งประกอบไปด้วยเซตไม่ว่าง S และ การดำเนินการทวิภาค $*$ ที่นิยามบน S

ตัวอย่าง 1.9 1) $(\mathbb{Z}^+;+)$ เป็นกรุปพอยด์ เมื่อ $\mathbb{Z}^+$ แทนเซตของจำนวนเต็มบวก

2) $(\mathbb{Z}^+;-)$ ไม่เป็นกรุปพอยด์ เพราะ $1-3=-2\notin\mathbb{Z}^+$

3) $(\mathbb{R};-)$ เป็นกรุปพอยด์ เมื่อ $\mathbb{R}$ แทนเซตของจำนวนจริง

4) $(\mathbb{R};\times)$ เป็นกรุปพอยด์

5) $(P(A);\cap)$ เป็นกรุปพอยด์ โดยที่ $A=\{a,b,c\}$ และ $P(A)$ เป็นเซตกำลัง(power set)ของ A

6) $(P(A);\cup)$ เป็นกรุปพอยด์ โดยที่ $A=\{a,b,c\}$ และ $P(A)$ เป็นเซตกำลัง(power set)ของ A

บทนิยาม 1.10 กึ่งกรุป (semigroup) คือ กรุปพอยด์ $(S\,;*)$ ซึ่ง $*$ มีสมบัติการเปลี่ยนกลุ่ม (associative)

หรือกล่าวอีกนัยหนึ่งว่า กึ่งกรุป คือ ระบบ $(S\,;*)$ โดยที่ $*$ เป็นการดำเนินการทวิภาค บน S และมีสมบัติการเปลี่ยนกลุ่ม

ตัวอย่าง 1.10 จาก **ตัวอย่าง** 1.9 $(\mathbb{Z}^+\,;+)$, $(\mathbb{R};\times)$, $(P(A);\cap)$ และ $(P(A);\cup)$ เป็นกึ่งกรุป แต่ $(\mathbb{R};-)$ ไม่เป็นกึ่งกรุป

ตัวอย่าง 1.11 ให้ $*:\mathbb{Z}\times\mathbb{Z}\longrightarrow\mathbb{Z}$ กำหนดโดย $a*b=a+b+ab$ สำหรับ $a,b\in\mathbb{Z}$ และ $+$ เป็นการบวกปกติ (usual addition) จงพิจารณาว่า ($S\,;*$) เป็นกึ่งกรุป หรือไม่

วิธีทำ. ให้ $a, b, c \in \mathbb{Z}$ เนื่องจาก $a + b + ab \in \mathbb{Z}$ จะได้ว่า $a * b \in \mathbb{Z}$
เนื่องจาก

$$\begin{aligned}(a * b) * c &= (a + b + ab)\\ &= (a + b + ab) + c + (a + b + ab)c\\ &= a + b + ab + c + ac + bc + abc\end{aligned}$$

และ

$$\begin{aligned}a * (b * c) &= a * (b + c + bc)\\ &= a + (b + c + bc) + a(b + c + bc)\\ &= a + b + c + +bc + ab + ac + abc\\ &= a + b + ab + c + ac + bc + abc\end{aligned}$$

จะได้ว่า $(a * b) * c) = a * (b * c)$ ดังนั้น $*$ มีสมบัติการเปลี่ยนกลุ่ม นั่นคือ $(S; *)$ เป็นกึ่งกรุป □

ตัวอย่าง 1.12 กำหนด $A = \{1, 2, 3\}$ และกำหนดการกระทำ $*$ ดังตาราง

*	1	2	3
1	1	2	3
2	3	3	3
3	2	3	1

จงแสดงว่า $(A; *)$ เป็นกึ่งกรุปหรือไม่

วิธีทำ. เนื่องจาก $(2 * 3) * 3 = 3 * 3 = 1$ และ $2 * (3 * 3) = 2 * 1 = 3$ จะได้ว่า $(2 * 3) * 3 \neq 2 * (3 * 3)$ นั่นคือ $*$ ไม่มีสมบัติการเปลี่ยนกลุ่ม แสดงว่า $(A; *)$ ไม่เป็นกึ่งกรุป □

สำหรับ $k \in \mathbb{N} = \{0, 1, 2, 3, \ldots\}$ กำหนดสัญลักษณ์ $N_k = \{0, 1, 2, 3, \ldots k\}$

ตัวอย่าง 1.13 บน N_k นิยามการกระทำ min โดย $a\ min\ b = min\{a, b\} := minimum\{a, b\}$ เพื่อความสะดวก เราจะเขียนแทน $minimum\{a, b\}$ ด้วย $min\{a, b\}$ จงพิจารณาว่า $(N_k; min)$ เป็นกึ่งกรุปหรือไม่

วิธีทำ. เห็นได้ชัดว่า min เป็นการกระทำทวิภาคบน N_k ต่อไปจะแสดงว่า min มีสมบัติการเปลี่ยนกลุ่ม ให้ $a, b, c \in N_k$ จะได้ว่า

$$\begin{aligned}(a\ min\ b)\ min\ c &= (min\ \{a, b\})\ min\ c \\ &= min\ \{min\ \{a, b\}, c\} \\ &= min\ \{a, b, c\} \\ &= min\ \{a,\ min\ \{b, c\}\} \\ &= a\ min\ (min\ \{b, c\}) \\ &= a\ min\ (b\ min\ c)\end{aligned}$$

ดังนั้น $(N_k; min)$ เป็นกึ่งกรุป □

ตัวอย่าง 1.14 จงแสดงว่า $(N_k; max)$ เป็นกึ่งกรุปหรือไม่ เมื่อการกระทำ max นิยามโดย $a\ max\ b = max\{a, b\} := maximum\{a, b\}$ สำหรับ $a, b \in N_k$

วิธีทำ. ให้ทำเป็นแบบฝึกหัด □

ตัวอย่าง 1.15 ให้ T_X เป็นเซตของฟังก์ชันทั้งหมดจาก X ไป X จะได้ว่า $(T_X; \circ)$ เป็นกึ่งกรุป โดยที่ $\circ$ เป็นคอมโพสิชัน (composition) ของฟังก์ชัน

ให้ S เป็นกึ่งกรุป และ A, B เป็นเซตย่อยของ S เรานิยาม AB ดังนี้

$$AB = \{ab \mid a \in A, b \in B\}$$

ถ้า $A = \emptyset$ หรือ $B = \emptyset$ เรากำหนดให้ $AB = \emptyset$

โดยนิยามเห็นได้ชัดว่า $(AB)C = A(BC)$ สำหรับทุก $A, B, C \in P(S)$ เมื่อ $P(S)$ คือเซตกำลัง (power set) ของ S ดังนั้นการ ดำเนินการทวิภาคนี้มีสมบัติการเปลี่ยนกลุ่ม นั่นคือ เราได้ว่า $P(S)$ เป็นกึ่งกรุป เรียกว่า **กึ่งกรุปโกลบอล** หรือ **กึ่งกรุปกำลัง** (global semigroup or power semigroup of S) ของ S (อ้างอิงจาก [8])

ประพจน์ 1.1 ให้ S เป็นกึ่งกรุป และ$A, B, C \subseteq S$ ถ้า $A \subseteq B$ แล้ว $AC \subseteq BC$ และ $CA \subseteq CB$

พิสูจน์. ให้ $x \in AC$ จะได้ว่า มี $a \in A, c \in C$ ซึ่งทำให้ $x = ac$ เนื่องจาก $a \in A \subseteq B$ จะได้ว่า $x = ac \in BC$ ดังนั้น $AC \subseteq BC$

สำหรับการพิสูจน์ว่า $CA \subseteq CB$ สามารถแสดงได้ในทำนองเดียวกัน □

เมื่อ $(S;*)$ เป็นกึ่งกรุป และ $a \in S$ สำหรับ $n \in Z^+$ เรานิยาม a^n โดยวิธีการอุปนัย ดังนี้

(i) $a^1 = a$

(ii) $a^{n+1} = a * a^n$ สำหรับ $n \geq 1$

สำหรับ $A \subseteq S$ เรานิยาม A^n ได้ในทำนองเดียวกัน นั่นคือ

(i) $A^1 = A$

(ii) $A^{n+1} = AA^n$ สำหรับ $n \geq 1$

ดังนั้นเราได้ว่า

$$A^n = \{a_1a_2a_3\ldots a_n \mid a_i \in A, i \in \{1,2,\ldots,n\}\}$$

1.3 กึ่งกรุปของการดำเนินการบูลีน n ภาค (Semigroup of n-ary Boolean Operations)

ให้ $A = \{0,1\}$ และ

$$A^n = \underbrace{A \times A \times \ldots \times A}_{n \text{ ตัว}} \qquad ; n \in \{1,2,\ldots\}$$

จะเรียกฟังก์ชัน $f : A^n \longrightarrow A$ ว่า **การดำเนินการบูลีน n ภาค** บนเซต A (n-ary Boolean operation defined on A)

ให้ $O^n(A) :=$ เซตของการกระทำบูลีนอันดับที่ n ทั้งหมดบน A

= $\{f \mid f : A^n \longrightarrow A\}$

ตัวอย่าง 1.16 กำหนด $A = \{0,1\}$ พิจารณาฟังก์ชัน $f : A^2 \longrightarrow A$ ซึ่งมีทั้งหมด 16 ฟังก์ชัน ดังตาราง

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
(0,0)	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
(0,1)	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
(1,0)	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
(1,1)	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1

ให้

$$\begin{aligned} K_0 &:= \{f \in O^2(A) | f(0,0) = 0 \wedge f(1,1) = 0\} \\ K_1 &:= \{f \in O^2(A) | f(0,0) = 1 \wedge f(1,1) = 1\} \\ C_4 &:= \{f \in O^2(A) | f(0,0) = 0 \wedge f(1,1) = 1\} \\ \neg C_4 &:= \{f \in O^2(A) | f(0,0) = 1 \wedge f(1,1) = 0\} \end{aligned}$$

ดังนั้น

$$\begin{aligned} K_0 &= \{f_1, f_2, f_3, f_4\} \\ K_1 &= \{f_{13}, f_{14}, f_{15}, f_{16}\} \\ C_4 &= \{f_5, f_6, f_7, f_8\} \\ \text{และ} \quad \neg C_4 &= \{f_9, f_{10}, f_{11}, f_{12}\} \end{aligned}$$

เราพบว่า $O^2(A) = K_0 \cup K_1 \cup C_4 \cup \neg C_4$ และ $\{K_0, K_1, C_4, C_4\}$ เป็นผลแบ่งกั้น (partition) ของ $O^2(A)$

สำหรับ f_1 และ f_{16} จะเป็นฟังก์ชันคงที่ (costant mapping) ที่ส่งไปยังค่าคงที่ $0 \in A$ และ $1 \in A$ ตามลำดับ เพื่อความสะดวกและง่ายต่อการจดจำเราจะแทน f_1 ด้วย c_0 และแทน f_{16} ด้วย c_1

รุ่งลาวัลย์ บุตรโคตร (R. Butkote) และ เค เดเนคเก (K. Denecke) [3] ได้นิยามการกระทำ $+$ บน $O^2(A)$ ดังนี้

สำหรับ $f, g \in O^2(A)$

$$f + g := f(g, g)$$

นั่นคือ สำหรับ $a_1, a_2 \in A$

$$(f + g)(a_1, a_2) = f(g(a_1, a_2), g(a_1, a_2))$$

จากนิยาม เห็นได้ชัดว่า $f + g \in O^2(A)$ นั่นคือ $+$ เป็นการกระทำทวิภาคบน $O^2(A)$ ต่อไปเราจะพิจารณาสมบัติการเปลี่ยนกลุ่มของ การกระทำ $+$

ให้ $f, g, h \in O^2(A)$ และ $\underline{a} \in A^2$

$$\begin{aligned} ((f + g) + h)(\underline{a}) &= (f + g)(h(\underline{a}), h(\underline{a})) \\ &= f(g(h(\underline{a}), h(\underline{a})), g(h(\underline{a}), h(\underline{a}))) \\ &= f((g + h)(\underline{a}), (g + h)(\underline{a})) \\ &= (f + (g + h))(\underline{a}) \end{aligned}$$

ดังนั้น $(f+g)+h = f+(g+h)$

เราพบว่า $+$ มีสมบัติการเปลี่ยนกลุ่ม นั่นคือ $(O^2(A);+)$ เป็นกึ่งกรุป เราเรียกกึ่งกรุปนี้ว่า **กึ่งกรุปของการดำเนินการบูลีน n ภาค** (semigroup of n-ary Boolean operations) ต่อไปเราจะพิจารณาสมบัติเบื้องต้นของการกระทำทวิภาค $+$ บน $O^2(A)$

ประพจน์ 1.2 [3] ถ้า $f \in C_4$ แล้ว $f+g=g$ สำหรับทุก $g \in O^2(A)$

พิสูจน์. ให้ $f \in C_4$ จะได้ว่า $f(0,0)=0$ และ $f(1,1)=1$ ให้ $g \in O^2(A)$ และ $\underline{a} \in A^2$ จะได้ว่า $(f+g)(\underline{a}) = f(g(\underline{a}), g(\underline{a}))$

ถ้า $g(\underline{a})=0$ จะได้ $(f+g)(\underline{a}) = f(0,0) = 0 = g(\underline{a})$

ถ้า $g(\underline{a})=1$ จะได้ $(f+g)(\underline{a}) = f(1,1) = 1 = g(\underline{a})$

ดังนั้น $f+g=g$ □

ประพจน์ 1.3 [3] ถ้า $f \in K_0$ และ $g \in O^2(A)$ แล้ว $f+g=c_0$

พิสูจน์. ให้ $f \in K_0$ และ $g \in O^2(A)$ จะได้ว่า $f(0,0) = f(1,1) = 0$ และให้ $\underline{a} \in A^2$ จะได้ว่า $(f+g)(\underline{a}) = f(g(\underline{a}), g(\underline{a}))$

ถ้า $g(\underline{a})=0$ จะได้ $(f+g)(\underline{a}) = f(0,0) = 0 = c_0(\underline{a})$

ถ้า $g(\underline{a})=1$ จะได้ $(f+g)(\underline{a}) = f(1,1) = 0 = c_0(\underline{a})$

ดังนั้น $f+g=c_0$ □

เราสามารถพิจารณาการบวกใน K_1 ได้ในทำนองเดียวกันและจะได้ว่า

ประพจน์ 1.4 [3] ถ้า $f \in K_1$ และ $g \in O^2(A)$ แล้ว $f+g=c_1$

พิสูจน์. สามารถพิสูจน์ได้ในทำนองเดียวกันกับทฤษฎีบทที่ผ่านมา □

1.4 สมาชิกพิเศษ (Special Elements)

บทนิยาม 1.11 สมาชิก e ของ กึ่งกรุป S จะเรียกว่า **เอกลักษณ์ทางซ้าย** (left identity) ของ S ถ้า $ea=a$ สำหรับทุก ๆ $a \in S$ และจะเรียก e ว่า **เอกลักษณ์ทางขวา** (right identity) ของ S ถ้า $ae=a$ สำหรับทุก $a \in S$

ถ้า e เป็นเอกลักษณ์ทางซ้ายและเอกลักษณ์ทางขวา แล้วจะเรียก e ว่าเป็น **เอกลักษณ์** (identity) ของ S

ตัวอย่าง 1.17 1) พิจารณากึ่งกรุป $(\mathbb{N};+)$ โดยที่ $\mathbb{N} = \{0,1,2,\ldots\}$

จะได้ว่า 0 เป็นเอกลักษณ์ ทั้งนี้เพราะว่า $0+n=n=n+0$ สำหรับทุก $n \in \mathbb{N}$

2) พิจารณากึ่งกรุป $(\mathbb{Z};\cdot)$ เมื่อ $\cdot$ เป็นการคูณปกติ (usual multiplication) จะได้ว่า 1 เป็นเอกลักษณ์ เพราะว่า $1\cdot z = z = z\cdot 1$ สำหรับทุก $z \in \mathbb{Z}$

3) ในกึ่งกรุป $(O^2(A);+)$ จะได้ว่า ทุกๆ $f \in C_4$ เป็นเอกลักษณ์ทางซ้าย ทั้งนี้ โดย **ประพจน์** 1.2 เราได้ว่า $f+g=g$ สำหรับทุก $g \in O^2(A)$

4) ในกึ่งกรุป $(K_0;+)$ ไม่มีเอกลักษณ์

ในกึ่งกรุปใดๆนั้นอาจมีเอกลักษณ์หรือไม่มีก็ได้ และอาจเป็นไปได้ว่ามีบางกึ่งกรุปที่มีเอกลักษณ์ทางซ้ายหรือทางขวามากกว่าหนึ่งสมาชิก แต่ถ้ากึ่งกรุปนั้นบรรจุเอกลักษณ์ทั้งทางซ้ายและทางขวาแล้ว เอกลักษณ์เหล่านั้นต้องเป็นตัวเดียวกัน ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 1.2 ถ้า e เป็นเอกลักษณ์ทางซ้ายของ S และ e' เป็นเอกลักษณ์ทางขวาของ S แล้ว $e=e'$

พิสูจน์. เนื่องจาก e เป็นเอกลักษณ์ทางซ้าย จะได้ว่า $ee'=e'$ และเนื่องจาก e' เป็นเอกลักษณ์ทางขวา จะได้ว่า $ee'=e$ ดังนั้น $e=ee'=e'$ □

ทฤษฎีบท 1.3 ทุก ๆ กึ่งกรุป จะบรรจุเอกลักษณ์อย่างมาก 1 สมาชิก

พิสูจน์. ให้ e และ e' เป็น เอกลักษณ์ของกึ่งกรุป S เนื่องจาก e เป็น เอกลักษณ์ จะได้ว่า $ee'=e$ ในทำนองเดียวกัน เนื่องจาก e' เป็น เอกลักษณ์ จะได้ว่า $ee'=e$ ดังนั้น$e'=ee'=e$ □

โดยทั่วไปเราจะแทนเอกลักษณ์ของกึ่งกรุปด้วยสัญลักษณ์ 1

บทนิยาม 1.12 เราเรียกกึ่งกรุปที่มีเอกลักษณ์ ว่า **โมนอยด์** (monoid)

ตัวอย่าง 1.18 1) $(\mathbb{Z};\cdot)$ เป็นโมนอยด์ ที่มี 1 เป็นสมาชิกเอกลักษณ์

2) $(\mathbb{Z};+)$ เป็นโมนอยด์ ที่มี 0 เป็นสมาชิกเอกลักษณ์

3) $(\mathbb{Z}_4;+)$ เป็นโมนอยด์ที่มี $\overline{0}$ เป็นสมาชิกเอกลักษณ์

4) $(N_3;min)$ เป็นโมนอยด์ที่มี 3 เป็นสมาชิกเอกลักษณ์

บทนิยาม 1.13 โมนอยด์ G ที่มี 1 เป็นเอกลักษณ์ จะเรียกว่าเป็น **กรุป** (group) ถ้าทุกสมาชิก $x \in G,$ มีตัวผกผัน (inverse) $x^{-1} \in G$ โดยที่ $xx^{-1}=1=x^{-1}x$

ตัวอย่าง 1.19 1) $(\mathbf{Z};+)$ เป็นกรุป ที่มีเอกลักษณ์เป็น 0 ทั้งนี้เพราะว่าแต่ละ $x \in \mathbb{Z}$ จะมี $x^{-1} = -x \in \mathbb{Z}$ ซึ่งทำให้ $x + (-x) = 0 = -x + x$

2) ให้ $\mathbb{M}^{2\times 2} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ จะได้ว่า $\left(\mathbb{M}^{2\times 2}; +\right)$ เป็นกรุปที่มี $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ เป็นเอกลักษณ์ ทั้งนี้เพราะว่า แต่ละ $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{M}^{2\times 2}$ จะมี $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} \in \mathbb{M}^{2\times 2}$ ซึ่งทำให้ $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

ให้ $(S;*)$ เป็นกึ่งกรุปซึ่งไม่มีเอกลักษณ์ เราสามารถสร้างกึ่งกรุปที่มีเอกลักษณ์จากกึ่งกรุป S นี้ได้โดยการเพิ่มสมาชิกพิเศษ 1 เข้าไปใน S เพื่อทำหน้าที่เป็นสมาชิกเอกลักษณ์ การสร้างโมนอยด์จากกึ่งกรุป S มีวิธีการ ดังนี้

ให้ $1 \notin S$ ขยายการดำเนินการทวิภาค $*$บนS ไปยัง $S \cup \{1\}$ โดยนิยาม

$$1 * 1 = 1 \text{ และ } 1 * x = x = x * 1 \text{ สำหรับทุก } x \in S$$

ดังนั้น จะได้ $(S \cup \{1\}\,;*)$ เป็นโมนอยด์ที่มีเอกลักษณ์เป็น 1

ตัวอย่าง 1.20 กำหนด $S = \{a, b, c, d\}$ และนิยามการดำเนินการ $*$ ดังตาราง

$*$	a	b	c	d
a	a	a	a	a
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

จะได้ว่า $(S;*)$ เป็นกึ่งกรุป และ S ไม่มีเอกลักษณ์ เราจะสร้างกึ่งกรุป $S \cup \{1\}$ ให้บรรจุเอกลักษณ์ นิยามการกระทำทวิภาค $*$บน$S \cup \{1\}$ ดังนี้ ให้

$x * y$ นิยามตามกึ่งกรุป S ถ้า $x, y \in S$ และ $x * 1 = 1 * x = x,\ 1 * 1 = 1$

ดังนั้นจะได้โมนอยด์ $S \cup \{1\}$ ดังตาราง

$*$	a	b	c	d	1
a	a	a	a	a	a
b	b	b	b	b	b
c	c	c	c	c	c
d	d	d	d	d	d
1	a	b	c	d	1

ให้ S เป็นกึ่งกรุป เรานิยาม S^1 ดังนี้

$$S^1 = \begin{cases} S & \text{ถ้า } S \text{ มีเอกลักษณ์} \\ S \cup \{1\} & \text{ถ้า } S \text{ ไม่มีเอกลักษณ์} \end{cases}$$

นั่นคือ S^1 เป็นโมนอยด์ที่ได้จากกึ่งกรุป S โดยการเพิ่มเอกลักษณ์เข้าไปใน S ถ้า S ไม่บรรจุเอกลักษณ์

บทนิยาม 1.14 สมาชิก a ในกึ่งกรุป S จะเรียกว่า**สมาชิกนิจพล** (idempotent element) ถ้า $aa = a^2 = a$ และจะเรียก a ว่าเป็น**สมาชิกปกติ** (regular element) ถ้า มี $b \in S$ ที่ทำให้ $aba = a$

ตัวอย่าง 1.21 1) ในกึ่งกรุป $(\mathbb{Z}; +)$ จะได้ว่า 0 เป็นสมาชิกนิจพลและเป็นสมาชิกปกติ

2) พิจารณากึ่งกรุป $(O^2(A); +)$ โดย **ประพจน์** 1.2 จะได้ว่าสำหรับทุก $f \in C_4$, $f + f = f$ ดังนั้นf เป็นสมาชิกนิจพลสำหรับทุก $f \in C_4$ ยิ่งไปกว่านั้นเราได้ว่า $f + f + f = f + (f + f) = f + f = f$ นั่นคือ f เป็นสมาชิกปกติสำหรับทุก $f \in C_4$

3) พิจารณากึ่งกรุป $(N_k; min)$ จะได้ว่าสำหรับแต่ละ $x \in N_k$, $x\ min\ x = min\{x, x\} = x$ และ $x\ min\ x\ min\ x = min\{x, x, x\} = x$ ดังนั้นทุกสมาชิกใน N_k เป็นสมาชิกนิจพลและเป็นสมาชิกปกติ

4) พิจารณากึ่งกรุป $(P(X); \cap)$ เมื่อ X เป็นเซตจำกัดที่ไม่เป็นเซตว่าง ให้ $Y \in P(X)$ จะได้ว่า $Y \cap Y = Y$ และ $Y \cap Y \cap Y$ ดังนั้นทุกสมาชิกใน $P(X)$ เป็นสมาชิกนิจพลและเป็นสมาชิกปกติ

หมายเหตุ 1.3 ถ้า a เป็นสมาชิกนิจพล แล้ว a เป็นสมาชิกปกติ ทั้งนี้เพราะว่า $a^3 = aa^2 = aa = a$ แต่บทกลับไม่จริง ดังตัวอย่างต่อไปนี้

ตัวอย่าง 1.22 ให้ $\mathbb{M}^{2\times 2} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ พิจารณากึ่งกรุป $(\mathbb{M}^{2\times 2}; +)$ โดยที่ $+$ เป็นการบวกของเมตริกซ์

เนื่องจาก $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ จะได้ว่า $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ เป็น

สมาชิกปกติ แต่เนื่องจาก $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}+\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}=\begin{bmatrix}2 & 0\\0 & 2\end{bmatrix}\neq\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$ จะได้ว่า $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$ ไม่เป็นสมาชิกนิจพล

สำหรับ กึ่งกรุป S กำหนดสัญลักษณ์

$E(S)$ แทน เซตของสมาชิกสมาชิกนิจพล ทั้งหมดใน S

$R(S)$ แทน เซตของสมาชิกปกติทั้งหมดใน S

นั่นคือ

$E(S)=\{a\in S \mid a*a=a\}$ และ

$R(S)=\{a\in S \mid \exists b\in S;(a*b*a=a)\}$

เราได้ว่า $E(S)\subseteq R(S)$

ตัวอย่าง 1.23 จงหา $E(\mathbb{N})$ และ $R(\mathbb{N})$ ของกึ่งกรุป $(\mathbb{N};+)$

วิธีทำ เนื่องจาก $0\in\mathbb{N}$ และ $0+0=0$ จะได้ว่า $0\in E(\mathbb{N})$
ให้ $0\neq a\in\mathbb{N}$ จะได้ว่า $a+a=2a\neq a$ ดังนั้น $a\notin E(\mathbb{N})$ นั่นคือ $E(\mathbb{N})=\{0\}$ ให้ $0\neq x\in\mathbb{N}$ จะได้ว่าแต่ละ $b\in\mathbb{N}, x+b+x=2x+b\neq x$ ดังนั้น $R(\mathbb{N})=E(\mathbb{N})=\{0\}$

ทฤษฎีบท 1.4 ถ้า G เป็นกรุปแล้ว $E(G)=\{1\}$

พิสูจน์. พิสูจน์เป็นแบบฝึกหัด □

บทนิยาม 1.15 สมาชิก z ของกึ่งกรุป S จะเรียกว่าเป็น**สมาชิกศูนย์ทางซ้าย** (left zero element) ของ S ถ้า $zx=z$ สำหรับทุก $x\in S$ และจะเรียก z ว่าเป็น **สมาชิกศูนย์ทางขวา** (right zero element) ของ S ถ้า $xz=z$ สำหรับทุก $x\in S$

ถ้า z เป็นทั้งสมาชิกศูนย์ทางซ้าย และ ศูนย์ทางขวา แล้ว จะเรียก z ว่า **สมาชิกศูนย์** (zero element) ของ S

ตัวอย่าง 1.24 1) ในกึ่งกรุป $(\mathbb{Z};\cdot)$ มีสมาชิก 0 เป็นสมาชิกศูนย์ทางซ้ายและศูนย์
ทางขวา

2) ให้ X เป็นเซตจำกัดที่ไม่ว่าง ในกึ่งกรุป $(P(X);\cap)$ มีสมาชิก $\emptyset$ เป็นสมาชิกศูนย์ทางซ้าย และศูนย์ทางขวา

3) ให้ X เป็นเซตจำกัดที่ไม่ว่าง ในกึ่งกรุป $(P(X);\cup)$ มีสมาชิก X เป็นสมาชิกศูนย์ทางซ้าย และศูนย์ทางขวา

4) ในกึ่งกรุป $(O^2(A);+)$ มีสมาชิก c_0 และ c_1 เป็นสมาชิกศูนย์ทางซ้าย

5) ในกึ่งกรุป $(N_5;max)$ มีสมาชิก 5 เป็นสมาชิกศูนย์ทางซ้าย และศูนย์ทางขวา

ตัวอย่าง 1.25 กำหนด $S=\{a,b,c,d\}$ และนิยามการกระทำทวิภาค $*$ บน S ดังตาราง

$*$	a	b	c	d
a	a	a	a	a
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

จงพิจารณาว่า สมาชิกใดเป็นสมาชิกศูนย์ทางซ้ายหรือศูนย์ทางขวา ของ S

วิธีทำ เนื่องจาก $a*x=a$ สำหรับทุก $x\in S$ จะได้ว่า a เป็นสมาชิกศูนย์ทางซ้ายของ S ในทำนองเดียวกันเราสามารถแสดงได้ว่า b,c และ d เป็นสมาชิกศูนย์ทางซ้ายของ S ด้วยเหมือนกัน ต่อไปจะพิจารณาว่ามีสมาชิกศูนย์ทางขวาของ a หรือไม่ สำหรับแต่ละ $x\in S$ จะได้ว่า $w*x=w$ สำหรับทุก $w\in S$ ดังนั้น ไม่มีสมาชิกศูนย์ทางขวาในกึ่งกรุป S

ประพจน์ 1.5 ถ้ากึ่งกรุป S บรรจุสมาชิกศูนย์ทางซ้าย และสมาชิกศูนย์ทางขวา แล้ว S จะบรรจุสมาชิกศูนย์

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

ประพจน์ 1.6 ในกึ่งกรุป ใดๆจะบรรจุสมาชิกศูนย์อย่างมาก 1 สมาชิก

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

ให้ $(S;*)$ เป็นกึ่งกรุปซึ่งไม่มีสมาชิกศูนย์ เราสามารถสร้างกึ่งกรุปที่มีสมาชิกศูนย์จากกึ่งกรุป S ได้ โดยการเพิ่มสมาชิกพิเศษ 0 เข้าไปใน S มีวิธีการ ดังนี้

ให้ $0\notin S$ ขยายการดำเนินการทวิภาค $*$บนS ไปยัง $S\cup\{0\}$ โดยนิยาม

$$0*x=x*0=0\ \ \forall x\in S$$

จะได้ $(S\cup\{0\};*)$ เป็นกึ่งกรุปที่บรรจุสมาชิกศูยน์

สำหรับกึ่งกรุป S เรานิยาม S^0 ดังนี้

$$S^0=\begin{cases} S & \text{ถ้า } S \text{ มีสมาชิกศูนย์} \\ S\cup\{0\} & \text{ถ้า } S \text{ ไม่มีสมาชิกศูนย์} \end{cases}$$

1.5 กึ่งกรุปย่อย (Subsemigroups)

บทนิยาม 1.16 ให้ $(S;*)$ เป็นกึ่งกรุป และ $\emptyset \neq T \subseteq S$ จะกล่าวว่า T เป็น **กึ่งกรุปย่อย** (subsemigroup) ของ S ถ้า $(T;*)$ เป็นกึ่งกรุป เขียนแทนด้วยสัญลักษณ์ $T \leq S$

กล่าวอีกนัยหนึ่งว่า $T \leq S$ ถ้า T ปิดภายใต้การกระทำทวิภาคเดียวกันกับกึ่งกรุป S นั่นคือ สำหรับ $x, y \in T$, $xy \in T$ หรือ

$$T \leq S \iff T^2 \subseteq T$$

ตัวอย่าง 1.26 1) พิจารณากึ่งกรุป $(\mathbb{Z}_4;+)$ จะได้ว่า $\{\bar{0}, \bar{2}\}$ เป็นกึ่งกรุปย่อยของ $\mathbb{Z}_4$

2) สำหรับ $k \in \mathbb{N}$ พิจารณากึ่งกรุป $(N_k; min)$ จะได้ว่า $\{0, 1, 2, \ldots, n\}$ โดยที่ $n \leq k$ เป็นกึ่งกรุปย่อยของ N_k

3) พิจารณากึ่งกรุป $(\mathbb{R};+)$ จะได้ว่า $\mathbb{Z}^+$ เป็นกึ่งกรุปย่อยของ $\mathbb{R}$

4) ให้ X เป็นเซตจำกัดที่ไม่ว่าง พิจารณากึ่งกรุป $(P(X);\cup)$ จะได้ว่า $\{\emptyset, X\}$ เป็นกึ่งกรุปย่อยของ $P(X)$

ตัวอย่าง 1.27 C_4 , K_0 และ K_1 เป็นกึ่งกรุปย่อยของ $(O^2(A);+)$

วิธีทำ. อันดับแรกเราจะแสดงว่า C_4 เป็นกึ่งกรุปย่อยของ $O^2(A)$ ให้ $f, g \in C_4$ โดย **ประพจน์** 1.2 จะได้ว่า $f + g = g \in C_4$ ดังนั้น C_4 ปิดภายใต้การกระทำทวิภาค $+$ นั่นคือ C_4 เป็นกึ่งกรุปย่อยของ $O^2(A)$

สำหรับการแสดงว่า $K_0 \leq O^2(A)$ และ $K_1 \leq O^2(A)$ ให้ทำเป็นแบบฝึกหัด $\square$

บทนิยาม 1.17 [9] ให้ c เป็นสมาชิกของกึ่งกรุป S เรากล่าวว่า c เป็น **เซนทรัล** (central) ถ้า $cx = xc$ สำหรับทุกๆ $x \in S$ เซตของสมาชิกเซนทรัลทั้งหมดของ S เรียกว่า **เซนเตอร์** (centre) ของ S เขียนแทนด้วยสัญสักษณ์ $Z(S)$

ตัวอย่าง 1.28 1) พิจารณากึ่งกรุป $(N_5; min)$ จะได้ว่า 0 เป็นเซนทรัล ยิ่งไปกว่านั้น $Z(N_5) = \{0\}$

2) พิจารณากึ่งกรุป $(K_0;+)$ จะได้ว่า $Z(K_0) = K_0$

3) พิจารณากึ่งกรุป $(C_4;+)$ จะได้ว่า $Z(C_4) = \emptyset$

ประพจน์ 1.7 ถ้า $Z(S) \neq \emptyset$ แล้ว $Z(S)$ เป็นกึ่งกรุปย่อยของ S

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด $\square$

ทฤษฎีบทต่อไปนี้แสดงว่าสำหรับกึ่งกรุป S ใดๆ การอินเตอร์เซกชันแบบจำกัดที่ไม่เป็นเซตว่างของกึ่งกรุปย่อยของ S จะเป็นกึ่งกรุปย่อยของ S

ทฤษฎีบท 1.5 ให้ $T_i \leq S$ เป็นกึ่งกรุปย่อยของ S สำหรับทุก $i \in I$ เมื่อ I เป็นเซตดัชนี ถ้า $\bigcap_{i \in I} T_i \neq \emptyset$ แล้ว $\bigcap_{i \in I} T_i \leq S$

พิสูจน์. ให้ $x, y \in \bigcap_{i \in I} T_i$ จะได้ $x, y \in T_i$ สำหรับทุก $i \in I$ เนื่องจากแต่ละ $i \in I,$ T_i เป็นกึ่งกรุป จะได้ว่า $xy \in T_i$ สำหรับทุก $i \in I$ ดังนั้น $xy \in \bigcap_{i \in I} T_i$ นั่นคือ $\bigcap_{i \in I} T_i \leq S$ $\square$

ถ้า T และ U เป็นกึ่งกรุปย่อยของ S แล้ว $T \cup U$ ไม่จำเป็นต้องเป็นกึ่งกรุปย่อยของ S ดังตัวอย่างต่อไปนี้

ตัวอย่าง 1.29 ให้ $X = \{a, b\}$ พิจารณากึ่งกรุป $(P(X); \cup)$ จะได้ว่า $T = \{\emptyset, \{a\}\}$ และ $U = \{\emptyset, \{b\}\}$ เป็นกึ่งกรุปย่อยของ $P(X)$ แต่ $T \cup U = \{\emptyset, \{a\}, \{b\}\}$ ไม่เป็นกึ่งกรุปย่อยของ $P(X)$ ทั้งนี้เพราะว่า $\{a\} \cup \{b\} = \{a, b\} \notin T \cup U$

สำหรับเซตย่อยที่ไม่ว่าง X ของกึ่งกรุป S เราให้

$$\langle X \rangle := \bigcap \{A \mid X \subseteq A \text{ และ } A \leq S\}$$

เนื่องจาก $X \subseteq \langle X \rangle$ ดังนั้นโดย **ทฤษฎีบทที่** 1.5 จะได้ว่า $\langle X \rangle$ เป็นกึ่งกรุปย่อยของ S เรียกกึ่งกรุปย่อยนี้ว่า **กึ่งกรุปย่อยที่ก่อกำเนิดโดย** X (subsemigroup of S generated by X) เราได้ว่า $\langle X \rangle$ สอดคล้องกับสมบัติสองข้อต่อไปนี้

(i) $X \subseteq \langle X \rangle$

(ii) ถ้า T เป็นกึ่งกรุปย่อยของ S และ $X \subseteq T$ แล้ว $\langle X \rangle \subseteq T$

ถ้า $X = \{x_1, x_2, \ldots, x_n\}$ เพื่อความสะดวกเราเขียนแทน $\langle X \rangle$ ด้วย $\langle x_1, x_2, \ldots, x_n \rangle$

ข้อสังเกต 1.1 ให้ S เป็นกึ่งกรุป และ A , B เป็นเซตย่อยของ S

1) ถ้า $A \subseteq B$ แล้ว $\langle A\rangle \le \langle B\rangle$

2) ถ้า $A \le S$ แล้ว $\langle A\rangle = A$

ทฤษฎีบท 1.6 [8] ให้ X เป็นเซตย่อยที่ไม่ว่างของกึ่งกรุป S แล้วจะได้ว่า

$$\langle X\rangle = \bigcup_{n=1}^{\infty} X^n = \{x_1x_2\dots x_n \mid n \ge 1, x_i \in X\}$$

พิสูจน์. เนื่องจาก $X \subseteq \langle X\rangle$ และ $\langle X\rangle$เป็นกึ่งกรุป จะได้ว่า $X^n \subseteq \langle X\rangle$ สำหรับทุก $n \ge 1$ ดังนั้น $\bigcup_{n=1}^{\infty} X^n \subseteq \langle X\rangle$

เนื่องจาก $\bigcup_{n=1}^{\infty} X^n \le S$ และ $X \subseteq \bigcup_{n=1}^{\infty} X^n$ จะได้ว่า $\langle X\rangle \subseteq \langle \bigcup_{n=1}^{\infty} X^n\rangle = \bigcup_{n=1}^{\infty} X^n$ นั่นคือเราได้ว่า $\langle X\rangle = \bigcup_{n=1}^{\infty} X^n$ $\square$

จาก **ทฤษฎีบท** 1.6 ถ้า $X = \{a\}$ จะได้ว่า $\langle X\rangle = \langle a\rangle = \{a, a^2, a^3, \dots\}$ เรียก $\langle a\rangle$ ว่า**กึ่งกรุปวัฏจักร** (cyclic semigroup) ที่ก่อกำเนิดโดย a

ตัวอย่าง 1.30 1) พิจารณากึ่งกรุป $(P(X);\cap)$ โดยที่ $X = \{a, b\}$ จะได้ว่า $\langle\{a\}\rangle = \{\{a\}\}$ และ $\langle\{a\},\{b\}\rangle = \{\emptyset,\{a\},\{b\}\}$

2) สำหรับกึ่งกรุป $(\mathbb{Z}_4;+)$ จะได้ว่า $\langle\overline{0}\rangle = \{\overline{0}\}$, $\langle\overline{1}\rangle = \{\overline{0},\overline{1},\overline{2},\overline{3}\}$ และ $\langle\overline{0},\overline{2}\rangle = \{\overline{0},\overline{2}\}$

3) พิจารณากึ่งกรุป $(N_5; max)$ เราได้ว่า $\langle 0, 3\rangle = \{0, 3\}$ และ $\langle 1, 2, 3\rangle = \{1, 2, 3\}$

4) พิจารณากึ่งกรุป $(\mathbb{I}^+;+)$ เราได้ว่า $\langle 1\rangle = \{1, 2, 3, \dots\}$ และ $\langle 2\rangle = \{2, 4, 6, \dots\}$

บทนิยาม 1.18 ให้ X เป็นเซตย่อยที่ไม่ว่างของกึ่งกรุป S ถ้า $\langle X\rangle = S$ แล้วเรากล่าวว่า X เป็น **เซตของตัวก่อกำเนิด** (set of generators) หรือ **เซตก่อกำเนิด** (generating set) ของ S

ตัวอย่าง 1.31 จาก**ตัวอย่าง** 1.30 จะได้ว่า $\{\overline{1}\}$ เป็นเซตก่อกำเนิดของกึ่งกรุป $\mathbb{Z}_4$ และ $\{1\}$ เป็นเซตก่อกำเนิดของกึ่งกรุป $\mathbb{I}^+$

บทนิยาม 1.19 ให้ a เป็นสมาชิกของกึ่งกรุป S **อันดับ** (order) ของ a เขียนแทนด้วย $|a|$ หรือ $ord(a)$ นิยามโดย $|a| = |\langle a\rangle|$

ตัวอย่าง 1.32 1) ในกึ่งกรุป $(\mathbb{Z}_4; +)$ จะได้ว่า $|\overline{0}| = 0$, $|\overline{1}| = 4$, $|\overline{2}| = 2$ และ $|\overline{3}| = 4$

2) พิจารณากึ่งกรุป $(P(X); \cap)$ โดยที่ $X = \{a, b\}$ จะได้ว่า $|x| = 1$ สำหรับทุก $x \in P(X)$ และ $\langle \{a\}, \{b\} \rangle = \big\{\emptyset, \{a\}, \{b\}\big\}$

3) พิจารณากึ่งกรุป $(O^2(A); +)$ เมื่อ $A = \{0, 1\}$ จะได้ว่า

$$|f| = \begin{cases} 1 & \text{ถ้า } f \in C_4 \cup \{c_0, c_1\} \\ 2 & \text{ถ้า } f \in \neg C_4 \cup K_0 \cup K_1 \setminus \{c_0, c_1\} \end{cases}$$

บทนิยาม 1.20 จะเรียกกึ่งกรุป S ว่าเป็น **กึ่งกรุปโมโนจีนิค** (monogenic semigroup) ถ้ามี $a \in S$ ซึ่งทำให้ $\langle a \rangle = S$

ตัวอย่าง 1.33 1) กึ่งกรุป $(\mathbb{I}^+; +)$ เป็นโมโนจีนิค เพราะ $\langle 1 \rangle = \mathbb{I}^+$

2) กึ่งกรุป $(\mathbb{Z}_4; +)$ เป็นโมโนจีนิค เพราะ $\langle \overline{1} \rangle = \mathbb{Z}_4$

ให้ a เป็นสมาชิกของกึ่งกรุป S พิจารณากึ่งกรุปย่อยโมโนจีนิคที่ก่อกำเนิดโดยสมาชิก a

$$\langle a \rangle = \big\{a, a^2, a^3, \ldots\big\}$$

ถ้าในเซต $\big\{a, a^2, a^3, \ldots\big\}$ มีสมาชิกไม่ซ้ำกัน จะได้ว่า $\langle a \rangle$ เป็นเซตอนันต์ ถ้ามีบางสมาชิกซ้ำกัน จะได้ว่า

$$\{x \in \mathbb{I}^+ \mid \exists y \in \mathbb{I}^+(a^x = a^y, x \neq y)\}$$

ไม่เป็นเซตว่าง ดังนั้นจะมีสมาชิกน้อยที่สุด (least element) ให้แทนด้วย m ซึ่งเราเรียกว่าเป็น **ดัชนี** (index) ของ a นั่นคือ เซต

$$\{x \in \mathbb{I}^+ \mid a^{m+x} = a^m\}$$

ไม่เป็นเซตว่าง ดังนั้นเซตนี้จะมีสมาชิกน้อยที่สุด ให้เป็น r ซึ่งเราเรียกว่าเป็น **คาบ** (period) ของ a

ให้สมาชิก a มีดัชนีเป็น m และ คาบเป็น r เราได้ว่า $a^m = a^{m+r}$
ดังนั้น

$$a^m = a^{m+r} = a^m a^r = a^{m+r} a^r = a^{m+2r} = \ldots = a^{m+qr} = \ldots$$

สำหรับ $q \in \mathbb{I}^+$

โดยสมบัติของสมาชิกน้อยที่สุด m และ r จะได้ว่า

$$a, a^2, a^3, \ldots, a^m, a^{m+1}, \ldots, a^{m+r-1}$$

แตกต่างกันทั้งหมด

สำหรับ $t \geq m$ โดยขั้นตอนวิธีการหาร (division algorithm) เราเขียน $t = m + qr + s$ โดยที่ $q \geq 0$, $0 \leq s \leq r - 1$ จะได้ว่า

$$a^t = a^{m+qr+s} = a^{m+qr} a^s = a^m a^s = a^{m+s}$$

ดังนั้น

$$\langle a \rangle = \left\{a, a^2, a^3, \ldots, a^m, a^{m+1}, \ldots, a^{m+r-1}\right\}$$

และ $|\langle a \rangle| = m + r - 1$ นั่นคือ a มีอันดับจำกัด (finite order) และ

อันดับของ a = (ดัชนีของ a) + (คาบของ a) - 1

นอกจากนี้เราได้ว่าเซตย่อย $\left\{a^m, a^{m+1}, \ldots, a^{m+r-1}\right\}$ เป็นกึ่งกรุปย่อยของ $\langle a \rangle$ เราสามารถเขียนความสัมพันธ์ของสมาชิกใน $\langle a \rangle$ ได้ดังแผนผังต่อไปนี้

$$\begin{tikzcd}
 & & & a^{n+1} \arrow[r] & a^{n+2} \arrow[dr] & \\
a \arrow[r] & a^2 \arrow[r] & \ldots a^n \arrow[ur] & & & a^{n+3} \arrow[dl] \\
 & & & a^{n+r-1} \arrow[ul] & \ldots \arrow[l] &
\end{tikzcd}$$

ตัวอย่าง 1.34 ในกึ่งกรุป $(\mathbb{Z}_6; +)$ พิจารณาสมาชิก $\overline{2}$ จะได้ว่า

$$\begin{aligned}
(\overline{2})^1 &= \overline{2}, & (\overline{2})^2 &= \overline{2} + \overline{2} = \overline{4} \\
(\overline{2})^3 = (\overline{2})^2 + \overline{2} &= \overline{6} = \overline{0}, & (\overline{2})^4 &= (\overline{2})^3 + \overline{2} = \overline{2} \\
(\overline{2})^5 = (\overline{2})^4 + \overline{2} &= \overline{4}, & (\overline{2})^6 &= (\overline{2})^5 + \overline{2} = \overline{6} = \overline{0}
\end{aligned}$$

จะได้ว่า $\overline{2}$ มีดัชนีเป็น 1 และ มีคาบเป็น 3 ดังนั้น

$$\langle \overline{2} \rangle = \left\{(\overline{2})^1, \ldots, (\overline{2})^{m+r-1=1+3-1=3}\right\} = \left\{\overline{2}, \overline{4}, \overline{0}\right\}$$

เราได้ว่า

$$\begin{tikzcd} & \overline{2}^2 = \overline{4} \arrow[dr] & \\ \overline{2} \arrow[ur] & & \overline{2}^3 = \overline{0} \arrow[ll] \end{tikzcd}$$

บทตั้ง 1.1 (The Idempotent Power Lemma) [17]
ให้ a เป็นสมาชิกของกึ่งกรุป S ถ้า $\langle a \rangle$ เป็นเซตจำกัดแล้ว $\langle a \rangle$ จะบรรจุสมาชิกนิจพล

พิสูจน์. ให้ m และ r เป็นดัชนีและคาบของ a ตามลำดับ เลือก $s \in \{0, 1, 2, \ldots,\}$ โดยที่ $s \equiv -m(mod\, r)$ จะได้ว่า $s + m \equiv 0(mod\, r)$ ดังนั้น $s + m = kr$ สำหรับบาง $k \in \{1, 2, \ldots,\}$ ดังนั้น

$$\begin{aligned}(a^{m+s})^2 &= a^{m+m+s+s} \\ &= a^{m+kr+s} \\ &= a^{m+kr}a^s \\ &= a^m a^s \\ &= a^{m+s}\end{aligned}$$

นั่นคือ $a^{m+s} \in E(S)$ □

บทแทรก 1.1 [17] ทุกๆกึ่งกรุปจำกัดจะบรรจุสมาชิกนิจพล

พิสูจน์. ให้ทำเป็นแบบฝึกหัด □

ประพจน์ 1.8 [8] ให้ m และ r เป็นดัชนีและคาบของสมาชิก a ในกึ่งกรุป S จะได้ว่า

$$K_a = \left\{a^m, a^{m+1}, \ldots, a^{m+r-1}\right\}$$

เป็นกึ่งกรุปย่อยของ S ยิ่งไปกว่านั้น K_a เป็นกรุป

พิสูจน์. ให้ทำเป็นแบบฝึกหัด □

1.6 กึ่งกรุปชนิดต่างๆ (Various Kinds of Semigroups)

บทนิยาม 1.21 กึ่งกรุป S จะเรียกว่า **กึ่งกรุปแถบ** (band) ถ้า ทุก ๆ สมาชิก ใน S เป็นสมาชิกสมาชิกนิจพล นั่นคือ $x^2 = x$ สำหรับทุก $x \in S$

ตัวอย่าง 1.35 1) $(C_4; +)$ เป็นกึ่งกรุปแถบ

2) $(\mathbb{N}; min)$ เป็นกึ่งกรุปแถบ

3) $(\mathbb{N}; max)$ เป็นกึ่งกรุปแถบ

4) ถ้า $|S| = 1$ แล้ว กึ่งกรุป S เป็นกึ่งกรุปแถบ

บทนิยาม 1.22 จะเรียกกึ่งกรุป S ว่า **กึ่งกรุปปรกติ** (regular semigroup) ถ้าทุกสมาชิกของ S เป็นสมาชิกปรกติ (regular element)

ตัวอย่าง 1.36 1) กึ่งกรุป $(C_4; +)$, $(\mathbb{N}; min)$ และ $(\mathbb{N}; max)$ เป็นกึ่งกรุปปรกติ

2) ให้ $\mathbb{M}^{2\times2} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ พิจารณากึ่งกรุป $(\mathbb{M}^{2\times2}; +)$

ให้ $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{M}^{2\times2}$ จะได้ว่า $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ ดังนั้นทุกๆสมาชิก $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{M}^{2\times2}$ เป็นสมาชิกปรกติ นั่นคือ $\mathbb{M}^{2\times2}$ เป็นกึ่งกรุปปรกติ

หมายเหตุ 1.4 ทุกๆกึ่งกรุปแถบจะเป็นกึ่งกรุปปรกติ แต่บทกลับไม่จริง ตัวอย่างเช่น $(\mathbb{M}^{2\times2}; +)$ เป็นกึ่งกรุปปรกติแต่ไม่เป็นกึ่งกรุปแถบ

ประพจน์ 1.9 ถ้า S เป็นกึ่งกรุปปรกติ แล้ว eSe เป็นกึ่งกรุปย่อยปรกติ (regular subsemigroup) ของ S สำหรับทุก $e \in E(S)$

พิสูจน์. เนื่องจาก $eee = e^2e = ee = e$ จะได้ว่า $e \in eSe$ ดังนั้น $eSe \neq \emptyset$ ให้ $x, y \in eSe$ จะได้ว่า มี a และ b ใน S ซึ่งทำให้ $x = eae$ และ $y = ebe$ ดังนั้นเราได้ว่า $xy = (eae)(ebe) = e(aeeb)e = e \in eSe$ นั่นคือ $eSe \leq S$ นอกจากนี้เราได้ว่า $xe = (eae)e = ea(ee) = eae = x$ และ $ex = e(eae) = (ee)ae = eae = x$

เนื่องจาก S เป็นกึ่งกรุปปกติ จะได้ว่า มีสมาชิก $w \in S$ ซึ่งทำให้ $x = xwx$ ดังนั้น $x = xwx = (xe)w(ex) = x(ewe)x$ นั่นคือ x เป็นสมาชิกปกติในกึ่งกรุป eSe □

บทนิยาม 1.23 กึ่งกรุป S จะเรียกว่า **กึ่งกรุปแถบมุมฉาก** (rectangular band) ถ้า $xyx = x$ สำหรับทุก $x, y \in S$

ตัวอย่าง 1.37

1) $(C_4; +)$ เป็นกึ่งกรุปแถบมุมฉาก

2) $(\{c_1, c_0; +\})$ เป็นกึ่งกรุปแถบมุมฉาก

3) $(\mathbb{N}; min)$ ไม่เป็นกึ่งกรุปแถบมุมฉาก ทั้งนี้เพราะ $2\ min\ 0\ min 2 = 0 \neq 2$

ทฤษฎีบท 1.7 [9] ให้ S เป็นกึ่งกรุป จะได้ว่า ข้อความต่อไปนี้สมมูลกัน

(i) S เป็นกึ่งกรุปแถบมุมฉาก

(ii) ทุกสมาชิกของ S เป็นสมาชิกนิจพล และ $abc = ac$ สำหรับทุก $a, b, c \in S$

พิสูจน์. (i) $\Rightarrow$(ii)

ให้ $x \in S$ โดยสมมุติฐานการพิสูจน์ (i) จะได้ว่า $x^3 = xxx = x$ และ $x^4 = xx^2x = x$ ดังนั้น $x = x^4 = xx^3 = xx = x^2$ นั่นคือ x เป็นสมาชิกนิจพลสำหรับทุก $x \in S$

ให้ $a, b, c \in S$ โดยสมมุติฐานการพิสูจน์ (i) จะได้ว่า $aba = a$ และ $cbc = c$ ดังนั้น $ac = (aba)(cbc) = a(b(ac)b)c = abc$

(ii)$\Rightarrow$ (i)

ให้เงื่อนไข (ii) เป็นจริง และ ให้ $x, y \in S$ จะได้ว่า $xyx = xx = x$ ดังนั้น S เป็นกึ่งกรุปแถบมุมฉาก □

บทนิยาม 1.24 กึ่งกรุป S จะเรียกว่า **กึ่งกรุปว่าง** (null semigroup or zero semigroup) ถ้ามี $a \in S$ ซึ่ง $xy = a$ สำหรับทุก $x, y \in S$

จาก **บทนิยาม** 1.24 เราพบว่าสมาชิก a เป็น สมาชิกศูนย์ (zero element) ของ S

ตัวอย่าง 1.38 $(K_0; +)$ และ $(K_1; +)$ เป็นกึ่งกรุปว่าง

หมายเหตุ 1.5 ถ้า S เป็นกึ่งกรุปว่างแล้ว S จะบรรจุสมาชิกศูนย์ แต่บทกลับไม่จริง นั่นคือ ถ้ากึ่งกรุป S บรรจุสมาชิกศูนย์ แล้ว S ไม่จำเป็นต้องเป็นกึ่งกรุปว่าง ตัวอย่างเช่น $(N_3; min)$ มี 0 ทำหน้าที่เป็นสมาชิกศูนย์ แต่ $(N_3; min)$ ไม่เป็นกึ่งกรุปว่าง

บทนิยาม 1.25 กึ่งกรุป S จะเรียกว่า **กึ่งกรุปศูนย์ทางซ้าย** (left zero semigroup) ถ้า ทุกๆ สมาชิก ของ S เป็นตัวศูนย์ทางซ้าย นั่นคือ $zx = z$ สำหรับทุก $x, z \in S$

จะเรียก S ว่า **กึ่งกรุปศูนย์ทางขวา** (right zero semigroup) ถ้า ทุกๆ สมาชิก ของ S เป็นตัวศูนย์ทางขวา นั่นคือ $xz = z$ สำหรับทุก $x, z \in S$

ตัวอย่าง 1.39 กำหนด $S = \{a, b, c, d\}$ และกำหนดการดำเนินการทวิภาค $*$ ดังตาราง

$*$	a	b	c	d
a	a	a	a	a
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

เนื่องจากแต่ละสมาชิกของ $x \in S$, $xy = x$ สำหรับทุก $y \in S$ จะได้ว่าทุกสมาชิก ใน S เป็นตัวศูนย์ทางซ้าย ดังนั้น S เป็นกึ่งกรุปศูนย์ทางซ้าย

ตัวอย่าง 1.40 $(C_4; +)$ เป็นกึ่งกรุปศูนย์ทางขวา

ทฤษฎีบท 1.8 ให้ S เป็นกึ่งกรุปแถบมุมฉาก และ $x \in S$ แล้วจะได้ว่า Sx เป็นกึ่งกรุปย่อยศูนย์ทางซ้าย และ xS เป็นกึ่งกรุปย่อยศูนย์ทางขวาของ S

พิสูจน์. ให้ $a, b \in Sx$ จะได้ว่ามี $s, s' \in S$ ซึ่งทำให้ $a = sx$ และ $b = s'x$ ดังนั้น $ab = (sx)(s'x) = (sxs')x \in Sx$ ยิ่งไปกว่านั้น $ab = (sx)(s'x) = s(xs')x = sx = a$ โดย **ทฤษฎีบท** 1.7 นั่นคือ Sx เป็นกึ่งกรุปย่อยศูนย์ทางซ้ายของ S
การพิสูจน์ xS เป็นกึ่งกรุปย่อยศูนย์ทางขวาของ S ให้ทำเป็นแบบฝึกหัด □

บทนิยาม 1.26 จะเรียกกึ่งกรุป S ว่า **เซมิแลตทิซ** (semilattice) ถ้า $x^2 = x$ และ $xy = yx$ สำหรับทุก $x, y \in S$

ตัวอย่าง 1.41 1) $(N_5; max)$ เป็นเซมิแลททิซ

2) $(P(X); \cup)$ โดยที่ X เป็นเซตจำกัด เป็นเซมิแลททิซ

3) $(C_4; +)$ ไม่เป็นเซมิแลททิซ ทั้งนี้เพราะว่า $f_5 + f_6 = f_6 \neq f_5 = f_6 + f_5$

4) $(K_0; +)$ ไม่เป็นเซมิแลททิซ ทั้งนี้เพราะว่า $f_3 + f_3 = c_0 \neq f_3$

บทนิยาม 1.27 (S. Schwarz [16]) กึ่งกรุป S จะเรียกว่าเป็น **กึ่งกรุปนอร์มัล** (normal semigroup) ถ้า $Sx = xS$ สำหรับทุก $x \in S$

ตัวอย่าง 1.42 $(N_3; min)$ เป็นกึ่งกรุปนอร์มัล ทั้งนี้เพราะว่า สำหรับแต่ละ $n \in N_3$

$$\begin{aligned} nN_3 &= \{n\ min\ x \mid x \in N_3\} \\ &= \{min\{n,x\} \mid x \in N_3\} \\ &= \{min\{x,n\} \mid x \in N_3\} \\ &= \{x\ min\ n \mid x \in N_3\} \\ &= N_3 n \end{aligned}$$

ตัวอย่าง 1.43 $(K_0; +)$ เป็นกึ่งกรุปนอร์มัล ทั้งนี้เพราะว่า สำหรับแต่ละ $f \in K_0$

$$\begin{aligned} fK_0 &= \{f + g \mid g \in K_0\} \\ &= \{c_0\} \\ &= \{g + f \mid g \in K_0\} \\ &= K_0 f \end{aligned}$$

ตัวอย่าง 1.44 $(C_4; +)$ ไม่เป็นกึ่งกรุปนอร์มัล ทั้งนี้เพราะ $fC_4 = C_4 \neq f = C_4 f$ สำหรับ $f \in C_4$

ตัวอย่าง 1.45 พิจารณากึ่งกรุป S กำหนดดังตาราง

$*$	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

จะได้ว่า S ไม่เป็นกึ่งกรุปนอร์มัล เพราะว่า

$$\begin{aligned} aS &= \{ax \mid x \in S\} \\ &= \{a\} \\ &\neq S \\ &= \{xa \mid x \in S\} \\ &= Sa \end{aligned}$$

ประพจน์ 1.10 [16] ถ้า S เป็นกึ่งกรุปนอร์มัล และ $\emptyset \neq X \subseteq S$ แล้ว $SX = XS$

พิสูจน์. ให้ $X = \{x_1, x_2, \ldots, x_k\}$ สำหรับ $k \in I^+$ เนื่องจาก S เป็นกึ่งกรุปนอร์มัล จะได้ว่า $Sx_i = x_iS$ สำหรับทุก $i \in \{1, 2, \ldots, k\}$ ดังนั้น $Sx_1 \cup Sx_2 \cup \ldots \cup Sx_k = x_1S \cup x_2S \cup \ldots \cup x_kS$ นั่นคือ $SX = XS$ □

ประพจน์ 1.11 [16] ถ้า S เป็นกึ่งกรุปนอร์มัล แล้ว สมาชิกนิจพลเป็นเซนทรัล, i.e. $E(S) \subseteq Z(S)$

พิสูจน์. ให้ $x \in S$ และ e เป็นสมาชิกนิจพล เนื่องจาก S เป็นกึ่งกรุปนอร์มัล จะได้ว่า $eS = Se$ ดังนั้น จะมีสมาชิก $u, v \in S$ ซึ่งทำให้ $ex = ue$ และ $ev = xe$

นั่นคือ เราได้

$$\begin{aligned} exe &= (ex)e \\ &= (ue)e \\ &= u(ee) \\ &= ue && ;\ \text{e เป็นสมาชิกนิจพล} \\ &= ex \end{aligned}$$

และ

$$\begin{aligned} exe &= e(xe) \\ &= e(ev) \\ &= (ee)v \\ &= ev && ;\ \text{e เป็นสมาชิกนิจพล} \\ &= xe \end{aligned}$$

แสดงว่า $ex = xe$ นั่นคือ e เป็นเซนทรัล □

หมายเหตุ 1.6 บทกลับของ **ประพจน์** 1.11 ไม่จริง นั่นคือ ถ้าทุกๆสมาชิกนิจพลเป็นเซนทรัล แล้ว กึ่งกรุป S ไม่จำเป็นต้องเป็นนอร์มัล ดังตัวอย่างต่อไปนี้

ตัวอย่าง 1.46 พิจารณากึ่งกรุป S กำหนดดังตาราง

$*$	0	a	b	c
0	0	0	0	0
a	0	0	0	0
b	0	0	0	0
c	0	0	a	a

เราพบว่า $E(S) = \{0\}$ ดังนั้นทุกสมาชิกนิจพลของ S เป็นเซนทรัล แต่ S ไม่เป็นนอร์มัล ทั้งนี้เพราะว่า $Sb \neq bS$

1.7 แบบฝึกหัด (Exercise)

1) ให้ $T = \{x \mid x = 2k+1 \;\; \exists k \in \mathbb{N}\}$ จงแสดงว่า $(T;+)$ เป็นกึ่งกรุปหรือไม่ เมื่อ $+$ เป็นการบวกปกติ (usaul addition)

2) ให้ $F = \{x \mid x = 2k \;\; \exists k \in \mathbb{N}\}$ จงแสดงว่า $(T;\cdot) \leq (\mathbb{N};\cdot)$ หรือไม่ เมื่อ $\cdot$ เป็นการคูณปกติ (usaul multiplication)

3) ให้
$$\mathbb{Z}^{2\times 2} = \Big\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in \mathbb{Z} \Big\}$$
และ
$$\mathbb{M}^{2\times 2} = \Big\{ \begin{bmatrix} 0 & 2x \\ 2y & 0 \end{bmatrix} \mid x,y \in \mathbb{Z} \Big\}$$
จงแสดงว่า $(\mathbb{M}^{2\times 2};+) \leq (\mathbb{Z}^{2\times 2};+)$ หรือไม่

4) กึ่งกรุป S จะเรียกว่าเป็น **กึ่งกรุปสลับที่** (commutative semigroup) ถ้า $xy = yx$ สำหรับทุก $x,y \in S$
จงพิจารณาว่า $(\mathbb{Z};*)$ เป็นกึ่งกรุปสลับที่หรือไม่ เมื่อกำหนดการดำเนินการทวิภาค $*$ โดย สำหรับ $a,b \in \mathbb{Z}$ ให้ $a*b = (2a+b)b + a^2$

5) บน N_4 นิยามการกระทำ min โดย $a \; min \; b = min\{a,b\}$ จงพิจารณาว่า $(N_4; min)$ เป็นกึ่งกรุปหรือไม่

6) จงแสดงว่า $(N_k; max)$ เป็นกึ่งกรุปหรือไม่ เมื่อการกระทำ max นิยามโดย $a \; max \; b = max\{a,b\}$ สำหรับ $a,b \in N_k$

7) พิจารณากึ่งกรุป $(\mathbb{N};+)$ จงหา $E(\mathbb{N}), R(\mathbb{N})$ และสมาชิกศูนย์ของ $\mathbb{N}$

8) จงยกตัวอย่างกึ่งกรุปที่มีเอกลักษณ์ทางซ้ายมากกว่าสองสมาชิก

9) จงยกตัวอย่างกึ่งกรุปที่มีสมาชิกศูนย์ทางขวามากกว่าสองสมาชิก

จงพิสูจน์ข้อความต่อไปนี้

10) ให้ S เป็นกึ่งกรุป และ$A, B, C \subseteq S$ ถ้า $A \subseteq B$ แล้ว $CA \subseteq CB$

11) ถ้า G เป็นกรุป แล้ว $E(G) = \{1\}$ โดยที่ 1 เป็นสมาชิกเอกลักษณ์

12) ถ้ากึ่งกรุป S บรรจุสมาชิกศูนย์ทางซ้ายและสมาชิกศูนย์ทางขวา แล้ว S บรรจุสมาชิกศูนย์

13) ให้ S เป็นกึ่งกรุป และ e เป็นสมาชิกนิจพลของ S แล้วจะได้ว่า

$$S_e = \{x \in S \mid xe = ex = x\}$$

เป็นกึ่งกรุปย่อยของ S

14) ทุกๆกึ่งกรุปจำกัดจะบรรจุสมาชิกนิจพล

15) ให้ m และ r เป็นดัชนีและคาบของสมาชิก a ในกึ่งกรุป S จะได้ว่า

$$K_a = \left\{a^m, a^{m+1}, \ldots, a^{m+r-1}\right\}$$

เป็นกึ่งกรุปย่อยของ S

16) S เป็นกึ่งกรุปแถบปกติ ก็ต่อเมื่อ ถ้า $ab = ba$ แล้ว $a = b$ สำหรับทุก $a, b \in S$

17) ถ้า S เป็นกึ่งกรุปศูนย์ทางซ้าย แล้ว S เป็นกึ่งกรุปแถบมุมฉาก

18) ถ้า S เป็นกึ่งกรุปปรกติแล้ว โกลบอลกึ่งกรุป $P(S)$ เป็นนอร์มัล

19) ถ้า $Z(S) \neq \emptyset$ แล้ว $Z(S)$ เป็นกึ่งกรุปย่อยของ S

จงพิจารณาว่าข้อความต่อไปนี้เป็นจริงหรือเป็นเท็จ ถ้าเป็นจริงจงแสดงการพิสูจน์ ถ้าเป็นเท็จจงยกตัวอย่างค้าน

20) ถ้า S เป็นกึ่งกรุปศูนย์ทางขวา แล้ว S เป็นกึ่งกรุปแถบปกติ

21) ถ้า A และ B เป็นกึ่งกรุปย่อยของ S แล้ว $A \cup B$ เป็นกึ่งกรุปย่อยของ S

22) ถ้า S เป็นกึ่งกรุปศูนย์ทางซ้าย แล้ว S บรรจุสมาชิกศูนย์

23) ถ้า S เป็นกึ่งกรุปนอร์มัล และ $A \leq S$ แล้ว A เป็นกึ่งกรุปนอร์มัล

24) ให้ S เป็นกึ่งกรุป $n \in \mathbb{N}$ กำหนด

$$S^n := \{a_1 a_2 a_3 \dots a_n\}$$

ถ้า S เป็นโมนอยด์ แล้ว $S^n = S$

บทที่ 2

ไอดีล (Ideals)

2.1 ไอดีล (Ideals)

บทนิยาม 2.1 ให้ S เป็นกึ่งกรุป และ $\phi \neq A \subseteq S$ จะเรียก A ว่าเป็น **ไอดีลทางซ้าย** (left ideal) ของ S ถ้า $SA \subseteq A$

จะเรียก A ว่าเป็น **ไอดีลทางขวา** (right ideal) ของ S ถ้า $AS \subseteq A$

ถ้า A เป็นไอดีลทางซ้ายและไอดีลทางขวาแล้ว จะเรียก A ว่าเป็น **ไอดีล 2 ข้าง** หรือ **ไอดีล** (two - side ideal or ideal) ของ S นั่นคือ $SA \subseteq A$ และ $AS \subseteq A$

จาก**บทนิยาม** 2.1 จะได้ว่าเซตย่อยที่ไม่ว่าง A ของกึ่งกรุป S เป็น :

(i) ไอดีลทางซ้ายของ S ถ้า ทุก $a \in A$ และ $s \in S$, $sa \in A$

(ii) ไอดีลทางขวาของ S ถ้า ทุก $a \in A$ และ $s \in S$, $as \in A$

(iii) ไอดีลของ S ถ้า ทุก $a \in A$ และ $s \in S$, $sa, as \in A$

ตัวอย่าง 2.1 ในกึ่งกรุป $(\mathbb{Z}_4; +)$ จงพิจารณาว่าเซต A ที่กำหนดในแต่ละข้อต่อไปนี้ เป็นไอดีลทางซ้ายหรือทางขวาของ $\mathbb{Z}_4$ หรือไม่

(ก) $A = \{\overline{0}\}$

(ข) $A = \{\overline{0}, \overline{2}\}$

(ค) $A = \mathbb{Z}_4$

(ง) $A = \{\overline{0}, \overline{3}\}$

(จ) $A = \{\overline{1}, \overline{2}\}$

วิธีทำ. (ก) เนื่องจาก

$$\begin{aligned}\mathbb{Z}_4A &= \{z+a \mid z \in \mathbb{Z}_4, a \in A\}\\ &= \left\{z+a \mid z \in \mathbb{Z}_4, a \in \{\overline{0}\}\right\}\\ &= \left\{z+\overline{0} \mid z \in \mathbb{Z}_4\right\}\\ &= \left\{\overline{0}+\overline{0}, \overline{1}+\overline{0}, \overline{2}+\overline{0}, \overline{3}+\overline{0}\right\}\\ &= \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\right\}\\ &= \mathbb{Z}_4 \nsubseteq A\end{aligned}$$

ดังนั้น A ไม่เป็นไอดีลทางซ้าย ของ $\mathbb{Z}_4$

ในทำนองเดียวกัน

$$\begin{aligned}A\mathbb{Z}_4 &= \{a+z \mid a \in A, z \in \mathbb{Z}_4\}\\ &= \left\{\overline{0}+z \mid z \in \mathbb{Z}_4\right\}\\ &= \left\{\overline{0}+\overline{0}, \overline{0}+\overline{1}, \overline{0}+\overline{2}, \overline{0}+\overline{3}\right\}\\ &= \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\right\}\\ &= \mathbb{Z}_4 \nsubseteq A\end{aligned}$$

ดังนั้น A ไม่เป็นไอดีลทางขวา $\mathbb{Z}_4$

(ข) พิจารณา

$$\begin{aligned}\mathbb{Z}_4A &= \{z+a \mid z \in \mathbb{Z}_4, a \in A\}\\ &= \left\{\overline{0}+\overline{0}, \overline{1}+\overline{1}, \overline{2}+\overline{0}, \overline{1}+\overline{3}, \overline{0}+\overline{2}, \overline{1}+\overline{2}, \overline{2}+\overline{2}, \overline{3}+\overline{2}\right\}\\ &= \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\right\}\\ &= \mathbb{Z}_4 \nsubseteq A\end{aligned}$$

ดังนั้น A ไม่เป็นไอดีลทางซ้าย ของ $\mathbb{Z}_4$ ในทำนองเดียวกันเราสามารถแสดงได้ว่า A ไม่เป็นไอดีลทางขวาของ $\mathbb{Z}_4$

(ค) - (จ) ให้ทำเป็นแบบฝึกหัด □

ตัวอย่าง 2.2 ในกึ่งกรุป $(K_0;+)$ จงแสดงว่า $A = \{c_0, f_2\}$ เป็นไอดีล K_0 หรือไม่

วิธีทำ. เนื่องจาก

$$\begin{aligned}K_0A &= \{f+g \mid f \in K_0, g \in A\}\\ &= \{c_0\} \subseteq \{c_0, f_2\} = A\end{aligned}$$

จะได้ว่า A เป็นไอดีลทางซ้ายของ K_0 เนื่องจาก $AK_0 = K_0A = \{c_0\} \subseteq A$ จะได้ว่า A เป็นไอดีลทางขวาของ K_0 นั่นคือ A เป็นไอดีลของK_0 □

ตัวอย่าง 2.3 พิจารณากึ่งกรุป $(P(X); \cup)$ เมื่อ $X = \{a, b\}$ จงแสดงว่าเซตที่กำหนดในแต่ละข้อต่อไปนี้เป็นไอดีลทางซ้ายของ $P(X)$ หรือไม่

(ก) $A_1 = \{\emptyset\}$

(ข) $A_2 = \{\{a, b\}\}$

(ค) $A_3 = \{\{a\}, \{a, b\}\}$

วิธีทำ. (ก) เนื่องจาก $P(X)A_1 = P(X)\{\emptyset\} = \{B \cup \emptyset \mid B \in P(X)\} = P(X) \nsubseteq \{\emptyset\} = A_1$ จะได้ว่า A_1 ไม่เป็นไอดีลทางซ้าย

(ข) เนื่องจาก $P(X)A_2 = P(X)\{\{a, b\}\} = \{B \cup \{a, b\} \mid B \in P(X)\} = \{\{a, b\}\} \subseteq A_2$ จะได้ว่า A_2 เป็นไอดีลทางซ้าย

(ค) เนื่องจาก $P(X)A_3 = P(X)\{\{a\}, \{a, b\}\} = \{B \cup \{a\},\ B \cup \{a, b\} \mid B \in P(X)\} = \{\{a\}, \{a, b\}\} \subseteq A_3$ จะได้ว่า A_3 เป็นไอดีลทางซ้าย □

นิยามของไอดีลมีลักษณะคล้ายกับนิยามของกึ่งกรุปย่อย เราพบว่า ทุกๆไอดีล ไอดีลทางซ้าย ไอดีลทางขวา เป็นกึ่งกรุปย่อย ดังประพจน์ต่อไปนี้

ประพจน์ 2.1 ให้ S เป็นกึ่งกรุป จะได้ว่า

(i) ถ้า A เป็นไอดีลทางซ้ายของ S แล้ว A เป็นกึ่งกรุปย่อยของ S

(ii) ถ้า A เป็นไอดีลทางขวาของ S แล้ว A เป็นกึ่งกรุปย่อยของ S

(iii) ถ้า A เป็นไอดีลของ S แล้ว A เป็นกึ่งกรุปย่อยของ S

พิสูจน์. (i) ให้ A เป็นไอดีลทางซ้ายของ S จะได้ว่า $SA \subseteq A$

ให้ $a, b \in A$ เนื่องจาก $a \in A \subseteq S$ จะได้ว่า $a * b \in SA$ แต่ $SA \subseteq A$ ดังนั้น จะได้ $a * b \in A$ นั่นคือ $A \leq S$

ข้อ (ii) และ (iii) ให้ทำเป็นแบบฝึกหัด □

ถ้า A เป็นกึ่งกรุปย่อยของ กึ่งกรุป S แล้ว A ไม่จำเป็นต้องเป็นไอดีลทางซ้าย ไอดีลทางขวาหรือไอดีล นั่นคือบทกลับของ **ประพจน์** 2.1 ไม่จริง ดังใน**ตัวอย่าง** 2.1 ข้อ (ข) เราพบว่า $\{\overline{0}, \overline{2}\}$ เป็นกึ่งกรุปย่อยของ Z_4 แต่ ไม่เป็นไอดีล

ในการพิจารณาว่าเซตย่อยไม่ว่าง A ใดๆ ของกึ่งกรุป S เป็นไอดีลทางซ้าย ไอดีลทางขวา หรือ ไอดีล ของ S หรือไม่ นั้น นอกจากตรวจสอบโดยใช้นิยามโดยตรงแล้ว เรายังสามารถ ตรวจสอบโดยการพิจารณารูปแบบเซตย่อยบางรูปแบบที่สมบัติเป็นไอดีลทางซ้าย ไอดีลทางขวา หรือ ไอดีล ซึ่งเซตที่มีคุณสมบัติดังกล่าวคือเซตย่อยที่อยู่ในรูป SA, AS และ SA ดังประพจน์ต่อไปนี้

ทฤษฎีบท 2.1 ให้ S เป็นกึ่งกรุป และ $\emptyset \neq A \subseteq S$ จะได้ว่า SA เป็นไอดีลทางซ้ายของ S

พิสูจน์. ให้ $x \in S\,(SA)$ จะได้ว่า $x = sw$ สำหรับบาง $s \in S, w \in SA$ เนื่องจาก $w \in SA$ จะได้ $w = s'a$ สำหรับบาง $s' \in S, a \in A$ ดังนั้น $x = sw = s(s'a) = (ss')\,a \in SA$ นั่นคือ $S\,(SA) \subseteq SA$ เพราะฉะนั้น SA เป็นไอดีลทางซ้ายของ S $\square$

ประพจน์ 2.2 ให้ S เป็นกึ่งกรุป และ $\emptyset \neq A \subseteq S$ จะได้ว่า AS เป็นไอดีลทางขวาของ S

พิสูจน์. เนื่องจาก $SS \subseteq S$ โดย **ประพจน์** 1.1 จะได้ว่า $(AS)S = A(SS) \subseteq AS$ ดังนั้น AS เป็นไอดีลทางขวาของ S $\square$

ประพจน์ 2.3 ให้ S เป็นกึ่งกรุป และ $\emptyset \neq A \subseteq S$ จะได้ว่า SAS เป็นไอดีลของ S

พิสูจน์. เนื่องจาก $SS \subseteq S$ โดย**ประพจน์** 1.1 จะได้ว่า $S(SAS) = (SS)(AS) \subseteq S(AS)$ และ $(SAS)S = (SA)(SS) \subseteq (SA)S$ นั่นคือ SAS เป็นไอดีลของ S $\square$

ถ้า $A = \{a\}$ จะได้ว่า Sa, aS และ SaS เป็นไอดีลทางซ้าย ไอดีลทางขวา และไอดีลของ S ตามลำดับ

ตัวอย่าง 2.4 กำหนด $(\mathbb{N}; min)$ จงแสดงว่า
(ก) $A = \{0\}$ เป็นไอดีลทางซ้ายของ $\mathbb{N}$ หรือไม่
(ข) $B = \{0, 1\}$ เป็นไอดีลทางขวาของ $\mathbb{N}$ หรือไม่
(ค) $C = \{0, 1, 2, 3, 4, 5\}$ เป็นไอดีลของ $\mathbb{N}$ หรือไม่

วิธีทำ (ก) เนื่องจาก

$$\begin{aligned}\mathbb{N}0 &= \{n\ min\ 0 \mid n \in \mathbb{N}\} \\ &= \{min\{n, 0\} \mid n \in \mathbb{N}\} \\ &= \{0\} = A\end{aligned}$$

ดังนั้นโดย**ประพจน์** 2.1 จะได้ว่า A เป็นไอดีลทางซ้ายของ $\mathbb{N}$

(ข) เนื่องจาก

$$\begin{aligned} 1\mathbb{N} &= \{1 \ min \ n \mid n \in \mathbb{N}\} \\ &= \{min\{n, 1\} \mid n \in \mathbb{N}\} \\ &= \{0, 1\} = B \end{aligned}$$

ดังนั้นโดย**ประพจน์** 2.2 จะได้ว่า B เป็นไอดีลทางขวาของ $\mathbb{N}$

(ค) เนื่องจาก

$$\begin{aligned} \mathbb{N}5\mathbb{N} &= \{n \ min \ 5 \ min \ m| \ n, m \in \mathbb{N}\} \\ &= \{min\,(n, 5, m) \ \mid n, m \in \mathbb{N}\} \\ &= \{0, 1, 2, 3, 4, 5\} = C \end{aligned}$$

ดังนั้นโดย**ประพจน์** 2.3 จะได้ว่า A เป็นไอดีลของ $\mathbb{N}$

ต่อไปเราจะพิจารณากลุ่มของไอดีลทางซ้าย (ทางขวา, ไอดีล) ของกึ่งกรุป เราพบว่า ผลคูณของไอดีล(ไอดีลทางซ้าย, ไอดีลทางขวา)ใดๆ จะเป็นไอดีล(ไอดีลทางซ้าย, ไอดีลทางขวา) เสมอ ดังประพจน์ต่อไปนี้

ประพจน์ 2.4 ให้ S เป็นกึ่งกรุป

(i) ถ้า A และ B เป็นไอดีลทางซ้ายของ S แล้ว AB เป็นไอดีลทางซ้ายของ S

(ii) ถ้า A และ B เป็นไอดีลทางขวาของ S แล้ว AB เป็นไอดีลทางขวาของ S

(iii) ถ้า A และ B เป็นไอดีลของ S แล้ว AB เป็นไอดีลของ S

พิสูจน์. (i) ให้ A และ B เป็นไอดีลทางซ้ายของ S จะได้ว่า $SA \subseteq A$ และ $SB \subseteq B$ ดังนั้น $S(AB) \subseteq (SA)B \subseteq AB$ นั่นคือ AB เป็นไอดีลทางซ้ายของ S

ข้อ (ii) และ (iii) สามารถพิสูจน์ได้ในทำนองเดียวกัน □

สำหรับกึ่งกรุป S ให้

$$\Gamma := \{A \mid A \text{ เป็นไอดีลทางขวาของ} S\}$$
$$\Omega := \{A \mid A \text{ เป็นไอดีลทางซ้ายของ} S\}$$

บทแทรก 2.1 ให้ S เป็นกึ่งกรุป จะได้ว่า

(i) Ω เป็นกึ่งกรุปย่อยของกึ่งกรุปกำลังของ S

(ii) Γ เป็นกึ่งกรุปย่อยของกึ่งกรุปกำลังของ S

(iii) เซตของไอดีลทั้งหมดของ S เป็นกึ่งกรุปย่อยของกึ่งกรุปกำลังของ S

พิสูจน์. เป็นผลโดยตรงจาก **ประพจน์** 2.4 $\square$

ตัวอย่าง 2.5 จาก **ตัวอย่าง** 2.3 เราได้ว่า A_2 และ A_3 เป็นไอดีลทางซ้ายของ $P(X)$ ดังนั้นโดย **ประพจน์** 2.4 จะได้ว่า $A_2A_3 = \{\{a, b\}\}$ เป็นไอดีลทางซ้ายของ $P(X)$

ประพจน์ 2.5 ให้ S เป็นกึ่งกรุป จะได้ว่า

(i) ถ้า A เป็นไอดีลทางซ้ายของ S แล้ว AM เป็นไอดีลทางซ้ายของ S สำหรับทุกๆ $\emptyset \neq M \subseteq S$

(ii) ถ้า A เป็นไอดีลทางขวาของ S แล้ว MA เป็นไอดีลทางขวาของ S สำหรับทุกๆ $\emptyset \neq M \subseteq S$

(iis) ถ้า A เป็นไอดีลของ S แล้ว AMA เป็นไอดีลของ S สำหรับทุกๆ $\emptyset \neq M \subseteq S$

พิสูจน์. (i) เนื่องจาก A เป็นไอดีลทางซ้าย จะได้ว่า $S(AM) = (SA)M \subseteq AM$ ดังนั้น AM เป็นไอดีลทางซ้ายของ S

(ii) พิสูจน์ในทำนองเดียวกันกับ (i)

(iii) เนื่องจาก A เป็นไอดีล จะได้ว่า $S(AMA) = (SA)MA \subseteq AMA$ และ $(AMA)S = AM(AS) \subseteq AMA$ ดังนั้น AMA เป็นไอดีลของ S $\square$

ประพจน์ 2.6 Γ เป็นไอดีลทางซ้ายของกึ่งกรุปกำลังของ S

พิสูจน์. ให้ $W \in P(S)\Gamma$ จะได้ว่ามี $M \in P(S)$ และ $A \in \Gamma$ ซึ่งทำให้ $W = MA$ เนื่องจาก A เป็นไอดีลทางขวาของ S โดย **ประพจน์** 2.5(ii) จะได้ว่า MA เป็นไอดีลทางขวาของ S ดังนั้น $W = MA \in \Gamma$ นั่นคือ $P(S)\Gamma \subseteq \Gamma$ แสดงว่า Γ เป็นไอดีลทางซ้ายของ $P(S)$ $\square$

ประพจน์ 2.7 Ω เป็นไอดีลทางขวาของกึ่งกรุปกำลังของ S

พิสูจน์. พิสูจน์ในทำนองเดียวกันกับ **ประพจน์** 2.6 $\square$

ต่อไปเราจะพิจารณาว่า การยูเนียนแบบจำกัดและการอินเตอร์เซกชันแบบจำกัดของกลุ่มของไอดีลทางซ้าย ไอดีลทางขวา หรือไอดีล ในกึ่งกรุปยังคงเป็นไอดีลทางซ้าย ไอดีลทางขวา หรือไอดีลหรือไม่ ดังตัวอย่างต่อไปนี้

ตัวอย่าง 2.6 พิจารณากึ่งกรุป $(N_4; max)$ จงแสดงว่า เซต ที่กำหนดในแต่ละข้อต่อไปนี้
เป็นไอดีลทางซ้ายของ N_4 หรือไม่

(ก) $A_1 = \{4\}$

(ข) $A_2 = \{2, 3, 4\}$

(ค) $A_3 = A_1 \cap A_2$

(ง) $A_4 = A_1 \cup A_2$

วิธีทำ. (ก) เนื่องจาก $N_4A_1 = \{s\ max\ 4 \mid s \in N_4\} = \{4\} \subseteq A_1$ จะได้ว่า $A_1 = \{4\}$ เป็นไอดีลทางซ้ายของ N_4

(ข) เนื่องจาก $N_4A_2 = \big\{s\ max\ a \mid s \in N_4, a \in \{2, 3, 4\}\big\} = \{2, 3, 4\} \subseteq A_1$ จะได้ว่า $A_2 = \{2, 3, 4\}$ เป็นไอดีลทางซ้ายของ N_4

(ค) -(ง) เนื่องจาก $A_3 = A_1 \cap A_2 = A_1$ และ $A_4 = A_1 \cup A_2 = A_2$ จะได้ว่า A_3 และ A_4 เป็นไอดีลทางซ้ายของ N_4

□

จากตัวอย่างที่ผ่านมา เมื่อพิจารณาผลยูเนียน และผลอินเตอร์เซกชันของไอดีลทางซ้าย ของกึ่งกรุป S จากตัวอย่างเราพบว่าผลอินเตอร์เซกชันไม่เป็นเซตว่าง และเราพบว่า ผลยังคงเป็นไอดีลทางซ้าย นอกจากนี้เมื่อเราพิจารณาไอดีลทางขวา ก็จะให้ผลในทำนองเดียวกัน ดังนั้น ถ้าเราขยายเป็นการยูเนียนแบบจำกัด (finite union) หรืออินเตอร์เซกชัน
แบบจำกัด (finite intersection) โดยที่ผลอินเตอร์เซกชันไม่เป็นเซตว่าง จะได้ผลดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.2 ให้ S เป็นกึ่งกรุป และให้ $\{A_i | i \in I\}$ เป็นแฟมิลีของไอดีลทางซ้าย (ไอดีลทางขวา) ของ S จะได้ว่า

(i) $\bigcap\limits_{i\in I} A_i$ เป็นไอดีลทางซ้าย (ไอดีลทางขวา) ของ S ถ้า $\bigcap\limits_{i\in I} A_i \neq \emptyset$

(ii) $\bigcup\limits_{i\in I} A_i$ เป็นไอดีลทางซ้าย (ไอดีลทางขวา)ของ S

พิสูจน์. (i) ให้ $x \in S\big(\bigcap\limits_{i\in I} A_i\big)$ จะได้ว่า $x = sw$ สำหรับบาง $s \in S, w \in \bigcap\limits_{i\in I} A_i$ เนื่องจาก $w \in \bigcap\limits_{i\in I} A_i$ จะได้ว่าแต่ละ $i \in I,\ w \in A_i$ ดังนั้น $x = sw \in SA_i$ สำหรับทุกๆ $i \in I$ เนื่องจากแต่ละ $i \in I,$ A_i เป็นไอดีลทางซ้ายของ S จะได้ว่า $SA_i \subseteq A_i$ ดังนั้น $x = sw \in SA_i \subseteq A_i$ สำหรับทุก $i \in I$ นั่นคือ $x \in \bigcap\limits_{i\in I} A_i$ แสดงว่า $S\big(\bigcap\limits_{i\in I} A_i\big) \subseteq \bigcap\limits_{i\in I} A_i$ ดังนั้น $\bigcap\limits_{i\in I} A_i$ เป็นไอดีลทางซ้ายของ S

(ii) ให้ $x \in S(\bigcup\limits_{i\in I} A_i)$ จะได้ว่า $x = sw$ สำหรับบาง $s \in S, w \in \bigcup\limits_{i\in I} A_i$ เนื่องจาก $w \in \bigcup\limits_{i\in I} A_i$ จะได้ว่า $w \in A_i$ สำหรับบาง $i \in I$ ดังนั้น $x = sw \in SA_i$ สำหรับบาง $i \in I$ เนื่องจาก แต่ละ $i \in I$ เรามี A_i เป็นไอดีลทางซ้าย ของ S จะได้ว่า $SA_i \subseteq A_i$ ดังนั้น $x = sw \in SA_i \subseteq A_i$ สำหรับบาง $i \in I$ นั่นคือ $x \in \bigcup\limits_{i\in I} A_i$ แสดงว่า $\bigcup\limits_{i\in I} A_i$ เป็นไอดีลทางซ้ายของ S $\square$

สำหรับการยูเนียนแบบจำกัดและอินเตอร์เซกชันแบบจำกัดของไอดีลในกึ่งกรุปใดๆ จะเป็นไอดีลเสมอ ก่อนอื่นเราจะแสดงว่า อินเตอร์เซกชันแบบจำกัดของไอดีลไม่เป็นเซตว่าง ดังบทตั้งต่อไปนี้

บทตั้ง 2.1 ให้ $A_1, A_2, \ldots, A_n$ เป็นไอดีลของกึ่งกรุป S สำหรับ $n \in \mathbb{I}^+$ จะได้ว่า $A_1A_2A_3\ldots A_n \subseteq \bigcap\limits_{i=1}^{n} A_i$

พิสูจน์. เนื่องจาก แต่ละ $i \in \mathbb{I}^+$, A_i เป็นไอดีลของกึ่งกรุป S จะได้ว่า $A_iS \subseteq A_i$ และ $SA_i \subseteq A_i$ สำหรับทุก $i \in \mathbb{I}^+$
ดังนั้น แต่ละ $i \in \mathbb{I}^+$ เราได้ว่า

$$\begin{aligned}
A_1A_2\ldots A_n &= A_1A_2\ldots A_{i-1}A_iA_{i+1}\ldots A_n \\
&= (A_1A_2\ldots A_{i-1})A_i(A_{i+1}\ldots A_n) \\
&\subseteq (A_1A_2\ldots A_{i-1})A_iS \\
&= (A_1A_2\ldots A_{i-1})(A_iS) \\
&\subseteq (A_1A_2\ldots A_{i-1})A_i \\
&\subseteq SA_i \subseteq A_i
\end{aligned}$$

นั่นคือ $A_1A_2A_3\ldots A_n \subseteq \bigcap\limits_{i=1}^{n} A_i$ $\square$

ทฤษฎีบท 2.3 ให้ S เป็นกึ่งกรุป และให้ $\{A_i|i \in I\}$ เป็นแฟมิลีของไอดีลทางของ S จะได้ว่า

(i) $\bigcap_{i\in I} A_i$ เป็นไอดีลของ S

(ii) $\bigcup_{i\in I} A_i$ เป็นไอดีลของ S

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

ต่อไปเราจะศึกษากลุ่มของเซตย่อยของกึ่งกรุป S อีกชนิดหนึ่ง ซึ่งเรียกว่า ไบ-ไอดีล (bi-ideal) ของ S ผู้ที่ให้นิยามนี้คือ R. A. Good และ D. R. Hughes [7]

บทนิยาม 2.2 [13] ให้ S เป็นกึ่งกรุป และ $\emptyset \neq A \subseteq S$ จะเรียก A ว่าเป็น **ไบ-ไอดีล** (bi-ideal) ของ S ถ้าสอดคล้องกับเงื่อนไข 2 ข้อต่อไปนี้

(i) A เป็นกึ่งกรุปย่อยของ S

(ii) $ASA \subseteq A$

ตัวอย่าง 2.7 กำหนด $X = \{a, b, c\}$ จงแสดงว่าเซตที่กำหนดให้ในแต่ละข้อต่อไปนี้เป็นไบ-ไอดีลของ $(P(X); \cap)$ หรือไม่

(ก) $A = \{\{a\}, \{a, b\}\}$

(ข) $B = \{\emptyset, \{a, b\}, \{a, c\}\}$

(ค) $C = \{\emptyset, \{a, b\}, \{a, c\}, \{a\}\}$

(ง) $D = \{\emptyset, \{a, b\}, \{a\}, \{b\}\}$

(จ) $F = P(X)$

วิธีทำ. (ก) เนื่องจาก $AP(X)A = \{\emptyset, \{a\}, \{a, b\}\} \nsubseteq A$ ดังนั้น A ไม่เป็นไบ-ไอดีลของ $P(X)$

(ข) เนื่องจาก B ไม่เป็นกึ่งกรุปย่อยของ ดังนั้น B ไม่เป็นไบ-ไอดีลของ $P(X)$

(ค) เนื่องจาก $CP(X)C = \{\emptyset, \{a, b\}, \{a, c\}, \{a\}, \{b\}, \{c\}\} \nsubseteq C$ ดังนั้น C ไม่เป็นไบ-ไอดีลของ $P(X)$

(ง) เนื่องจาก $DP(X)D = \{\emptyset, \{a, b\}, \{a\}, \{b\}\} \subseteq D$ และ D เป็นกึ่งกรุปย่อยของ $P(X)$ ดังนั้น D เป็นไบ-ไอดีลของ $P(X)$

(จ) เห็นได้ชัดว่า $F = P(X)$ เป็นไบ-ไอดีลของ $P(X)$ □

ประพจน์ 2.8 ให้ S เป็นกึ่งกรุป จะได้ว่า

(i) ทุกๆไอดีลทางซ้ายของ S เป็น ไบ-ไอดีล

(ii) ทุกๆไอดีลทางขวาของ S เป็น ไบ-ไอดีล

(iii) ทุกๆไอดีลของ S เป็น ไบ-ไอดีล

พิสูจน์. (i) ให้ A เป็นไอดีลทางซ้ายของ S จะได้ว่า $ASA = A(SA) \subseteq AA \subseteq SA \subseteq A$ นอกจากนี้ โดย **ประพจน์** 2.1(i) จะได้ว่า A เป็นกึ่งกรุปย่อยของ S ดังนั้น A เป็น ไบ-ไอดีลของ S

(ii)-(iii) พิสูจน์ได้ในทำนองเดียวกันกับ (i) □

ประพจน์ 2.9 ให้ $A_1, A_2, \ldots, A_n$ เป็นไบ-ไอดีลของกึ่งกรุป S แล้วจะได้ว่า $A_1A_2 \ldots A_n$ เป็นไบ-ไอดีลของ S

พิสูจน์. ให้ $a_1, a_1' \in A_i$ สำหรับ $i = 1, 2, \ldots, n$ จะได้ว่า $(a_1a_2 \ldots a_n)(a_1'a_2' \ldots a_n') = (a_1(a_2 \ldots a_n)a_1')a_2' \ldots a_n' \in A_1A_2 \ldots A_n$ ทั้งนี้เพราะว่า $a_1(a_2 \ldots a_n)a_1' \in A_1SA_1 \subseteq A_1$ แสดงว่า $A_1A_2 \ldots A_n$ เป็นกึ่งกรุปย่อยของ S
เนื่องจาก $A_1(A_2A_3 \ldots A_nS)A_1 \subseteq A_1SA_1 \subseteq A_1$ จะได้ว่า

$$\begin{aligned}(A_1A_2A_3 \ldots A_n)S(A_1A_2A_3 \ldots A_n) &= (A_1(A_2A_3 \ldots A_nS)A_1)A_2A_3 \ldots A_n) \\ &\subseteq A_1A_2A_3 \ldots A_n\end{aligned}$$

นั่นคือ $A_1A_2A_3 \ldots A_n$ เป็นไบ-ไอดีลของ S □

ประพจน์ 2.10 เซตของไบ-ไอดีลทั้งหมดของกึ่งกรุป S เป็นกึ่งกรุปย่อยของกึ่งกรุปกำลังของ S

พิสูจน์. เป็นผลโดยตรงจาก **ประพจน์** 2.6 □

ประพจน์ 2.11 ให้ S เป็นกึ่งกรุป และ $\emptyset \neq A \subseteq S$ แล้วจะได้ว่า ASA เป็นไบ-ไอดีลของ S

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

ประพจน์ 2.12 ให้ I เป็นเซตดัชนีและ $\{B_i \mid i \in I\}$ เป็นแฟมิลี่ของไบ-ไอดีลของกึ่งกรุป S แล้วจะได้ว่า

ถ้า $\bigcap_{i \in I} B_i \neq \emptyset$ แล้ว $\bigcap_{i \in I} B_i$ เป็นไบ-ไอดีลของ S

พิสูจน์. สำหรับการพิสูจน์ว่า $\bigcap\limits_{i\in I} B_i \leq S$ ให้พิสูจน์เป็นแบบฝึกหัด
ต่อไปเราจะแสดงว่า $(\bigcap\limits_{i\in I} B_i)S(\bigcap\limits_{i\in I} B_i) \subseteq \bigcap\limits_{i\in I} B_i$ ให้ $b, b' \in \bigcap\limits_{i\in I} B_i$ และ $s \in S$ จะได้ว่า $b, b' \in B_i$ สำหรับทุก $i \in I$ ดังนั้น $bsb' \in B_iSB_i$ สำหรับทุก $i \in I$ เนื่องจากแต่ละ B_i เป็นไบ-ไอดีล จะได้ว่า $bsb' \in B_iSB_i \subseteq B_i$ สำหรับทุก $i \in I$ นั่นคือ $bsb' \in \bigcap\limits_{i\in I} B_i$ □

ประพจน์ 2.13 [13] ให้ A เป็นไบ-ไอดีล และ B เป็นเซตย่อยที่ไม่ว่างของกึ่งกรุป S แล้วจะได้ว่า AB และ BA เป็นไบ-ไอดีลของ S

พิสูจน์. ให้ $a, a' \in A$ และ $b, b' \in B$ จะได้ว่า $(ab)(a'b') = (aba')b' \in AB$ ทั้งนี้เพราะ $aba' \in ABA \subseteq ASA \subseteq A$ และ $b' \in B$ ดังนั้น $AB \leq S$ นอกจากนี้ สำหรับ $s \in S$ เราได้ว่า $(ab)s(a'b') = (a(bs)a')b' \in AB$ ทั้งนี้เพราะ $a(bs)a' \in ASA \subseteq A$ นั่นคือ $(AB)S(AB) \subseteq AB$
สำหรับการพิสูจน์ BA เป็นไบ-ไอดีล ให้ทำเป็นแบบฝึกหัด □

บทแทรก 2.2 ถ้า A และ B เป็นไบ-ไอดีล ของกึ่งกรุป S แล้วจะได้ว่า AB เป็นไบ-ไอดีลของ S

พิสูจน์. เป็นผลโดยตรงจาก **ประพจน์** 2.13 □

ประพจน์ 2.14 [12] ให้ A เป็นไอดีลของกึ่งกรุป S จะได้ว่า ข้อความต่อไปนี้สมมูลกัน

(i) A เป็นกึ่งกรุปนอร์มัล

(ii) $XA = AX$ สำหรับทุก $\emptyset \neq X \subseteq S$

(iii) $(xS^1)A = A(S^1x)$ สำหรับทุก $x \in S$

(iv) $(xS^1)A = Ax$ สำหรับทุก $x \in S$

(v) $xA = A(S^1x)$ สำหรับทุก $x \in S$

พิสูจน์. $(i) \Rightarrow (ii)$ ให้ A เป็นกึ่งกรุปนอร์มัล และ $\emptyset \neq X \subseteq S$ ให้ $w \in XA$ จะได้ว่า $w = xa$ สำหรับบาง $x \in X, a \in A$ เนื่องจาก A เป็นกึ่งกรุปนอร์มัล จะได้ว่า $xa \in xA = Ax \subseteq AX$ ดังนั้น $XA \subseteq AX$ ในทำนองเดียวกันเราสามารถแสดงได้ว่า $AX \subseteq XA$ นั่นคือ $XA = AX$
การพิสูจน์ $(ii) \Rightarrow (iii)$, $(iii) \Rightarrow (iv)$, $(iv) \Rightarrow (v)$ และ $(v) \Rightarrow (i)$ ให้ทำเป็นแบบฝึกหัด □

ประพจน์ 2.15 [12] ถ้า A และ B เป็นนอร์มัลไอดีลของกึ่งกรุป S แล้ว AB, BA เป็นนอร์มัลไอดีลของ S และ $AB = BA$

พิสูจน์. โดย **ประพจน์** 2.14 จะได้ว่า $AB = BA$ และโดย **ประพจน์** 2.4 จะได้ว่า AB เป็นไอดีล ให้ $x \in S$ เราได้ว่า $x(AB) = (xA)B = (Ax)B = A(xB) = A(Bx) = (AB)x$ แสดงว่า AB เป็นกึ่งกรุปนอร์มัล □

ในกึ่งกรุป S ใดๆ จะมีไอดีลเสมอ ทั้งนี้เพราะว่า $SS \subseteq S$ นั่นคือ S เป็นไอดีลของตัวมันเองเสมอ ถ้า กึ่งกรุป S บรรจุสมาชิกศูนย์ 0 จะได้ว่า S และ $\{0\}$ เป็นไอดีลของกึ่งกรุปนี้

บทนิยาม 2.3 จะเรียกไอดีล I ว่า **ไอดีลแท้(ไอดีลทางซ้ายแท้, ไอดีลทางขวาแท้)** (proper ideal, proper left ideal, proper right ideal) ถ้า $I \neq \{0\}$ และ $I \neq S$

ตัวอย่าง 2.8 1) พิจารณากึ่งกรุป $(N_3; min)$ จะได้ว่า $\{0, 1, 2\}$ เป็น ไอดีลแท้ ไอดีลทางซ้ายแท้และ ไอดีลทางขวาแท้

2) ให้ $X = \{a, b\}$ พิจารณากึ่งกรุป $(P(X); \cap)$ จะได้ว่า $\{\emptyset, \{a\}\}$, $\{\emptyset, \{a\}, \{b\}\}$ เป็น ไอดีลแท้ ไอดีลทางซ้ายแท้และ ไอดีลทางขวาแท้

3) ในกึ่งกรุป $(\mathbb{Z}_4; +)$ ไม่มี ไอดีลแท้ ไอดีลทางซ้ายแท้และ ไอดีลทางขวาแท้

ข้อสังเกต 2.1 ให้ S เป็นกึ่งกรุป

1) ถ้า S ไม่มีไอดีลทางซ้ายแท้ แล้ว S ไม่มีไอดีลแท้

2) ถ้า S ไม่มีไอดีลทางขวาแท้ แล้ว S ไม่มีไอดีลแท้

บทกลับของข้อสังเกตข้างต้น ไม่จริง นั่นคือ ข้อความต่อไปนี้ไม่จริง
ถ้า S ไม่มีไอดีลแท้ แล้ว S ไม่มีไอดีลทางซ้ายแท้ และ
ถ้า S ไม่มีไอดีลแท้ แล้ว S ไม่มีไอดีลทางขวาแท้
ดังตัวอย่างต่อไปนี้

ตัวอย่าง 2.9 กำหนด $S = \{a, b, c, d\}$ และกำหนดการดำเนินการทวิภาค $*$ ดังตาราง

$*$	a	b	c	d
a	a	b	c	d
b	a	b	c	d
c	a	b	c	d
d	a	b	c	d

จะได้ว่า กึ่งกรุป S ไม่มีไอดีลแท้ ทั้งนี้เพราะว่า ถ้า S มีไอดีลแท้ ให้เป็น ไอดีล I จะได้ว่า $SI \cup IS \subseteq I$ เนื่องจาก $IS = \{yx|y \in I,\ x \in S\} = \{x|x \in S\} = S$ จะได้ว่า $S \subseteq I$ ดังนั้น $S = I$ ซึ่งขัดแย้ง

ให้ $A = \{a, b\}$ จะได้ว่า

$$\begin{aligned} SA &= \{xy \mid x \in S, y \in A\} \\ &= \{xa,\ xb \mid x \in S\} \\ &= \{a, b\} \subseteq A \end{aligned}$$

นั่นคือ A เป็นไอดีลทางซ้ายของ S เนื่องจาก $A \neq S$ จะได้ว่า A เป็นไอดีลทางซ้ายแท้ของ S

ตัวอย่าง 2.10 กำหนด $S = \{a, b, c, d\}$ และกำหนดการดำเนินการทวิภาค $*$ ดังตาราง

$*$	a	b	c	d
a	a	a	a	a
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

จะได้ว่า กึ่งกรุป S ไม่มีไอดีลแท้ ให้ $A = \{a, b\}$ จะได้ว่า

$$\begin{aligned} AS &= \{xy \mid x \in A, y \in S\} \\ &= \{ay,\ by \mid x \in S\} \\ &= \{a, b\} \subseteq A \end{aligned}$$

นั่นคือ A เป็นไอดีลทางขวาของ S เนื่องจาก $A \neq S$ จะได้ว่า A เป็นไอดีลทางขวา
แท้ของ S

2.2 ไอดีลที่ก่อกำเนิดโดยเซตย่อย (Ideal Generated by Subsets)

ในกึ่งกรุป S ใดๆ เราสามารถสร้างไอดีลทางซ้าย ไอดีลทางขวา และ ไอดีล ได้เสมอ โดยสร้างจาก SA, AS และ SAS เมื่อ $\emptyset \neq A \subseteq S$ แต่เซตทั้งสามรูปแบบนี้

ไม่จำเป็นต้องบรรจุ A นั่นคือไม่จำเป็นที่ A จะเป็นเซตย่อยของเซตทั้งสามรูปแบบนี้ ดังตัวอย่าง

ตัวอย่าง 2.11 พิจารณากึ่งกรุป $(K_0;+)$ ให้ $A=\{f_2\}$ จะได้ว่า

$K_0A=\{c_0\}$ เป็นไอดีลทางซ้ายของ S

$AK_0=\{c_0\}$ เป็นไอดีลทางขวาของ S

$K_0AK_0=\{c_0\}$ เป็นไอดีลของ S

แต่ $A\not\subseteq K_0A$, $A\not\subseteq AK_0$ และ $A\not\subseteq K_0AK_0$

ในการสร้างไอดีลที่บรรจุ A นั้น เราอาศัย S^1 เป็นตัวสร้าง ดังนี้
พิจารณา

$$\begin{aligned}
S^1A &= \{sa \mid s\in S^1,\ \ a\in A\}\\
&= \{sa \mid s\in S\cup\{1\},\ \ a\in A\}\\
&= \{sa \mid s\in S,\ a\in A\}\cup\{sa\mid s\in\{1\},a\in A\}\\
&= \{sa \mid s\in S,a\in A\}\cup\{1a|a\in A\}\\
&= SA\cup A
\end{aligned}$$

$$\therefore S^1A = SA\cup A$$

$$\begin{aligned}
AS^1 &= \{as\mid a\in A\wedge s\in S^1\}\\
&= \{as\mid a\in A\wedge(s\in S\cup\{1\})\}\\
&= \{as\mid a\in A,s\in S\}\cup\{as\mid a\in A,s\in\{1\}\}\\
&= \{as\mid a\in A,s\in S\}\cup\{a1\mid a\in A\}\\
&= AS\cup A
\end{aligned}$$

$$\therefore AS^1 = AS\cup A$$

$$\begin{aligned}
S^1AS^1 &= \{sas'\mid s\in S^1,a\in A,s'\in S^1\}\\
&= \{sas'\mid s\in S^1,a\in A,s'\in S\cup\{1\}\}\\
&= \{sas'\mid s\in S,a\in A,s'\in S\}\cup\{sas'|s\in\{1\},a\in A,s'\in S\}\cup\\
&\quad \{sas'|s\in S,a\in A,s'\in\{1\}\}\cup\{sas'\mid s\in\{1\},a\in A,s'\in\{1\}\}\\
&= SAS\cup AS\cup SA\cup A
\end{aligned}$$

ดังนั้นเราได้ว่า $A\subseteq S^1A$, $A\subseteq AS^1$, และ $A\subseteq S^1AS^1$ ยิ่งไปกว่านั้น S^1A, AS^1 และ S^1AS^1 เป็นไอดีลทางซ้าย ไอดีลทางขวา และไอดีลของ S ตามลำดับ ดังการพิสูจน์ต่อไปนี้

ทฤษฎีบท 2.4 ให้ S เป็นกึ่งกรุป และ $\phi \neq A \subseteq S$ แล้ว จะได้ว่า S^1A เป็นไอดีลทางซ้ายของ S ที่เล็กที่สุดที่บรรจุ A (smallest left ideal of S containig A)

พิสูจน์. เนื่องจาก $S \subseteq S^1$ และ S^1 เป็นกึ่งกรุป จะได้ว่า $SS^1 \subseteq S^1$ ดังนั้น $S(S^1A) = (SS^1)A \subseteq S^1A$ นั่นคือ S^1A เป็นไอดีลทางซ้ายของ S
ต่อไปจะแสดงว่า S^1A เป็นไอดีลทางซ้ายที่เล็กที่สุดที่บรรจุ A ให้ I เป็นไอดีลทางซ้ายใดๆ ของ S ที่บรรจุ A จะได้ว่า $A \subseteq I$ และ $SI \subseteq I$ ดังนั้น $SA \subseteq SI \subseteq I$ นั่นคือ $S^1A = SA \cup A \subseteq I$ แสดงว่า S^1A เป็นทางซ้ายของ S ที่เล็กที่สุดที่บรรจุ A □

ในทำนองเดียวกัน เราจะได้ว่า :

ทฤษฎีบท 2.5 ให้ S เป็นกึ่งกรุป และ $\phi \neq A \subseteq S$ แล้ว

1) AS^1 เป็นไอดีลทางขวาที่เล็กที่สุดที่บรรจุ A

2) S^1AS^1 เป็นไอดีลที่เล็กที่สุดที่บรรจุ A

พิสูจน์. พิสูจน์ในทำนองเดียวกันกับ **ทฤษฎีบท** 2.4 □

เนื่องจาก S^1A เป็นไอดีลทางซ้ายที่เล็กที่สุดที่บรรจุ A ดังนั้นเราได้ว่า

$S^1A =$ อินเตอร์เซกชันของไอดีลทางซ้ายทั้งหมดของ S ที่บรรจุ A
$= \bigcap\{I \mid A \subseteq I\text{และ}I\text{ไอดีลทางซ้ายของ}S\}$
$=$ ไอดีลทางซ้ายของ Sที่ก่อกำเนิดโดย $A(left\ ideal\ of\ S\ generated\ by\ A)$
$= SA \cup A$

ในทำนองเดียวกัน เราได้ว่า

$AS^1 =$ อินเตอร์เซกชันของไอดีลทางขวาทั้งหมดของ S ที่บรรจุ A
$= \bigcap\{I \mid A \subseteq I\text{และ}I\text{ไอดีลทางขวาของ}S\}$
$=$ ไอดีลทางขวาของ Sที่ก่อกำเนิดโดย $A(right\ ideal\ of\ S\ generated\ by\ A)$
$= AS \cup A$

และ

$$\begin{aligned} S^1AS^1 &= \text{อินเตอร์เซกชันของไอดีลทั้งหมดของ S ที่บรรจุ A} \\ &= \bigcap\{I \mid A \subseteq I \text{และ} I \text{ไอดีลของ} S\} \\ &= \text{ไอดีลของ } S \text{ที่ก่อกำเนิดโดย } A(\ ideal\ of\ S\ generated\ by\ A) \\ &= SA \cup AS \cup SAS \cup A \end{aligned}$$

บทนิยาม 2.4 ให้ a เป็นสมาชิกของกึ่งกรุป S

จะเรียก S^1a ว่า **ไอดีลมุขสำคัญทางซ้าย ที่ก่อกำเนิดโดย** a (principal left ideal generated by a)

จะเรียก aS^1 ว่า **ไอดีลมุขสำคัญทางขวา ที่ก่อกำเนิดโดย** a (principal right ideal generated by a) และ

จะเรียก S^1aS^1 ว่า **ไอดีลมุขสำคัญที่ก่อกำเนิดโดย** a (principal ideal generated by a)

ทฤษฎีบท 2.6 ถ้า $a = axa$ แล้ว $S^1a = Sa$, $aS^1 = aS$ และ $S^1aS^1 = SaS$

พิสูจน์. เนื่องจาก $a = axa = (ax)a \in Sa$ จะได้ว่า $S^1a = Sa \cup \{a\} = Sa$ ในทำนองเดียวกันจะได้ว่า $aS^1 = aS$ และ $S^1aS^1 = SaS$ □

ในประพจน์ถัดไป จะกล่าวถึงความสัมพันธ์ของไอดีลมุขสำคัญทางซ้ายที่ก่อกำเนิดจากสมาชิกที่ต่างกัน เราพบว่า ถ้าเราสร้างไอดีลมุขสำคัญทางซ้ายจากตัวก่อกำเนิดที่มาจากไอดีลมุขสำคัญทางซ้ายหนึ่ง จะได้ว่า ไอดีลมุขสำคัญทางซ้ายที่สร้างได้นี้จะเป็นเซตย่อยของไอดีลมุขสำคัญทางซ้ายนั้น และในทางตรงกันข้าม

ประพจน์ 2.16 ให้ S เป็นกึ่งกรุป และ $a, b \in S$ แล้วจะได้ว่า $S^1a \subseteq S^1b$ ก็ต่อเมื่อ $a \in S^1b$

พิสูจน์. $(\Rightarrow)$ ให้ $S^1a \subseteq S^1b$ จะได้ว่า $a \in Sa \cup \{a\} = S^1a \subseteq S^1b$

$(\Leftarrow)$ ให้ $a \in S^1b$ เนื่องจาก S^1a เป็นไอดีลทางซ้ายที่เล็กที่สุดที่บรรจุ a และS^1b เป็นไอดีลทางซ้ายของ S ที่บรรจุ a จะได้ว่า $S^1a \subseteq S^1b$ □

ประพจน์ 2.17 ให้ S เป็นกึ่งกรุป และ $a, b \in S$ แล้วจะได้ว่า $aS^1 \subseteq bS^1$ ก็ต่อเมื่อ $a \in bS^1$

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

2.3 กึ่งกรุปเชิงเดียว (Simple Semigroup)

บทนิยาม 2.5 ให้ S เป็นกึ่งกรุปที่ไม่บรรจุสมาชิกศูนย์ จะเรียก S ว่าเป็น **กึ่งกรุปเชิงเดียวทางซ้าย** (left simple semigroup) ถ้า S ไม่มีไอดีลทางซ้ายแท้ จะเรียก S ว่าเป็น **กึ่งกรุปเชิงเดียวทางขวา** (right simple semigroup) ถ้า S ไม่มีไอดีลทางขวาแท้ และ จะเรียก S ว่าเป็น **กึ่งกรุปเชิงเดียว** (simple semigroup) ถ้า S ไม่มีไอดีลแท้

โดย **นิยาม** 2.5 เรากล่าวอีกนัยหนึ่งว่า S เป็นกึ่งกรุปเชิงเดียว (กึ่งกรุปเชิงเดียวทางซ้าย, กึ่งกรุปเชิงเดียวทางขวา) ถ้า S มีไอดีล (ไอดีลทางซ้าย, ไอดีลทางขวา) เพียงตัวเดียวเท่านั้นคือ S

ตัวอย่าง 2.12 กำหนดกึ่งกรุป S ดังนี้

$*$	a	b	c	d
a	a	a	a	a
b	b	b	b	b
c	c	c	c	c
d	d	d	d	d

จงพิจารณาว่า S เป็นกึ่งกรุปเชิงเดียวทางซ้าย, กึ่งกรุปเชิงเดียวทางขวา หรือกึ่งกรุปเชิงเดียวหรือไม่

วิธีทำ. ก่อนอื่นเราจะพิจารณาว่า S เป็นกึ่งกรุปเชิงเดียวทางซ้ายหรือไม่

ให้ I เป็นไอดีลทางซ้ายใดๆของ S จะได้ว่า $I \subseteq S$ และ $SI \subseteq I$ เนื่องจาก $SI = \{si \mid s \in S, \ \ i \in I\} = \{s \mid s \in S\} = S$ จะได้ว่า $S = SI \subseteq I$ ดังนั้น S ไม่มีไอดีลทางซ้ายแท้ นั่นคือ S เป็นกึ่งกรุปเชิงเดียวทางซ้าย

ต่อไปเราจะพิจารณาว่า S เป็นกึ่งกรุปเชิงเดียวทางขวาหรือไม่

ให้ $I = \{a\}$ จะได้ว่า $IS = \{as \mid s \in S\} = \{a\} \subseteq I$ ดังนั้น I เป็นไอดีลทางขวาของ S และเป็นไอดีลทางขวาแท้ นั่นคือ S ไม่เป็นกึ่งกรุปเชิงเดียวทางขวา

ต่อไปเราจะพิจารณาว่า S เป็นกึ่งกรุปเชิงเดียวหรือไม่

ให้ I เป็นไอดีลใดๆ จะได้ว่า $SI \subseteq I, \ IS \subseteq I$ ดังนั้น $S = SI \subseteq I$ นั่นคือ $S = I$ แสดงว่า S ไม่มีไอดีลแท้ ดังนั้นเราได้ว่า S เป็นกึ่งกรุปเชิงเดียว □

ตัวอย่าง 2.13 1) $(Z_4;+)$ เป็นกึ่งกรุปเชิงเดียวทางซ้าย กึ่งกรุปเชิงเดียวทางขวา และกึ่งกรุปเชิงเดียว

2) $(C_4;+)$ เป็นกึ่งกรุปเชิงเดียวทางขวา กึ่งกรุปเชิงเชิงเดียว แต่ไม่เป็นกึ่งกรุปเชิงเดียวทางซ้าย

3) $(N_5;min)$ ไม่เป็นกึ่งกรุปเชิงเดียวทางซ้าย กึ่งกรุปเชิงเดียวทางขวา และกึ่งกรุปเชิงเดียว

ข้อสังเกต 2.2 1) ทุกๆกึ่งกรุปเชิงเดียวทางซ้ายเป็นกึ่งกรุปเชิงเดียว

2) ทุกๆกึ่งกรุปเชิงเดียวทางขวาเป็นกึ่งกรุปเชิงเดียว

3) ถ้า S เป็นกึ่งกรุปเชิงเดียวแล้ว ไม่จำเป็นที่ S จะเป็นกึ่งกรุปเชิงเดียวทางซ้ายและกึ่งกรุปเชิงเดียวทางขวา

ในกึ่งกรุปเชิงเดียวทางซ้าย เราพบว่าทุกๆไอดีลมุขสำคัญทางซ้ายจะเป็นเซตเดียวกัน และเป็นเซตเดียวกันกับกึ่งกรุปนั้น ยิ่งไปกว่านั้น เราได้ว่า $a \in Sa$ สำหรับทุกๆสมาชิก $a \in S$

ทฤษฎีบท 2.7 ให้ S เป็นกึ่งกรุปที่ไม่บรรจุสมาชิกศูนย์ แล้วจะได้ว่า

(i) S เป็นกึ่งกรุปเชิงเดียวทางซ้าย ก็ต่อเมื่อ $Sa = S$ สำหรับทุก $a \in S$

(ii) S เป็นกึ่งกรุปเชิงเดียวทางซ้าย ก็ต่อเมื่อ $S^1a = S$ สำหรับทุก $a \in S$

พิสูจน์. (i) $(\Rightarrow)$ ให้ S เป็นกึ่งกรุปเชิงเดียวทางซ้าย จะได้ว่า S มีไอดีลทางซ้ายเพียงตัวเดียวเท่านั้นคือ S สำหรับ $a \in S$ โดย**ประพจน์** 2.1 จะได้ว่า Sa เป็นไอดีล
ทางซ้ายของ S ดังนั้น $Sa = S$ สำหรับทุก $a \in S$

$(\Leftarrow)$ ให้ $Sa = S$ สำหรับทุก $a \in S$ ให้ I เป็นไอดีลทางซ้ายใดๆของ S จะได้ว่า $\phi \neq I \subseteq S$ และ $SI \subseteq I$ ให้ $x \in I$ โดยสมมุติฐานของการพิสูจน์จะได้ว่า $Sx = S$ ดังนั้น $S = Sx \subseteq SI \subseteq I$ นั่นคือ $S = I$ แสดงว่าไอดีลทางซ้ายของ S มีเพียงตัวเดียวเท่านั้น คือ S นั่นคือ S เป็นกึ่งกรุปเชิงเดียวทางซ้าย

(ii) $(\Rightarrow)$ พิสูจน์ในทำนองเดียวกันกับ (i)

$(\Leftarrow)$ ให้ I เป็นไอดีลทางซ้ายใดๆของ S จะได้ว่า $I \subseteq S$ และ $SI \subseteq I$ ให้ $a \in I$ จะได้ว่า $\{a\} \subseteq I$ ดังนั้น $Sa \subseteq SI \subseteq I$ นั่นคือ $S^1a = Sa \cup \{a\} \subseteq I$

ดังนั้นเราได้ว่า $S = I$ แสดงว่าไอดีลทางซ้ายของ S มีเพียงตัวเดียวเท่านั้น คือ S นั่นคือ S เป็นกึ่งกรุปเชิงเดียวทางซ้าย $\square$

เราได้ผลลัพธ์ในทำนองเดียวกันเมื่อพิจารณากึ่งกรุปเชิงเดียวทางขวา และกึ่งกรุปเชิงเดียว ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.8 ให้ S เป็นกึ่งกรุปที่ไม่มีสมาชิกศูนย์ จะได้ว่า

(i) S เป็นกึ่งกรุปเชิงเดียวทางขวา ก็ต่อเมื่อ $aS = S$ สำหรับทุก $a \in S$

(ii) S เป็นกึ่งกรุปเชิงเดียวทางขวา ก็ต่อเมื่อ $aS^1 = S$ สำหรับทุก $a \in S$

(iii) S เป็นกึ่งกรุปเชิงเดียว ก็ต่อเมื่อ $SaS = S$ สำหรับทุก $a \in S$

(iv) S เป็นกึ่งกรุปเชิงเดียว ก็ต่อเมื่อ $S^1aS^1 = S$ สำหรับทุก $a \in S$

พิสูจน์. พิสูจน์เป็นแบบฝึกหัด $\square$

ต่อไปเราจะพิจารณากึ่งกรุปที่บรรจุสมาชิกศูนย์

บทนิยาม 2.6 ให้ S เป็นกึ่งกรุปที่บรรจุสมาชิกศูนย์ จะเรียก S ว่า 0 -**เชิงเดียว** (0 - simple) ถ้า สอดคล้องกับเงื่อนไขดังต่อไปนี้

(i) มี $\{0\}$ และ S เท่านั้นที่เป็นไอดีล

(ii) $S^2 \neq \{0\}$

ตัวอย่าง 2.14 กึ่งกรุป S ที่กำหนดดังตาราง เป็น 0 - เชิงเดียว

*	a	b	c	z
a	a	a	a	z
b	b	b	b	z
c	c	c	c	z
z	z	z	z	z

จากตารางเราได้ว่า z เป็นสมาชิกศูนย์ของ S ทั้งนี้เพราะว่า $zx = z = xz$ สำหรับทุก $x \in S$ ให้ I เป็นไอดีลใดๆของ S โดยที่ $I \neq \{z\}$ จะได้ว่ามี $z \neq x \in I$ ดังนั้น $IS = \{is \mid i \in I,\ s \in S\} = \{xs, is \mid i \in I - \{x\}, s \in S\} = \{s \mid s \in S\} = S$ แต่ $S = IS \subseteq I$ นั่นคือ $I = S$ แสดงว่า S มีไอดีลคือ $\{z\}$ และ S เท่านั้น นั่นคือ S เป็น 0 - เชิงเดียว

ทฤษฎีบท 2.9 [9] กึ่งกรุป S เป็น 0- เชิงเดียว ก็ต่อเมื่อ $SaS = S$ สำหรับทุกๆ $0 \neq a \in S$

พิสูจน์. ($\Rightarrow$) เนื่องจาก S เป็น 0 - เชิงเดียว จะได้ว่า $SS = S^2 \neq \{0\}$ แต่ S^2 เป็นไอดีลของ S ดังนั้น $S^2 = S$ นั่นคือเราได้ว่า $S^3 = S^2S = SS = S$ ให้ $0 \neq a \in S$ โดย **ประพจน์** 2.3 จะได้ว่า SaS เป็นไอดีลของ S ดังนั้น $SaS = S$ หรือ $SaS = \{0\}$ สมมติ $SaS = \{0\}$ จะได้ว่า $a \in I = \{x \mid SxS = \{0\}\}$ ให้ $w \in SI$ จะได้ว่า $w = si$ สำหรับบาง $s \in S,\ i \in I$ ดังนั้น $SwS = S(si)S = (Ss)iS \subseteq SiS = \{0\}$ นั่นคือ $SwS = \{0\}$ ดังนั้นเราได้ว่า $w \in I$ แสดงว่า $SI \subseteq I$ นั่นคือ I เป็นไอดีลทางซ้ายของ S ในทำนองเดียวกันเราสามารถพิสูจน์ได้ว่า I เป็นไอดีลทางขวาของ S ดังนั้น I เป็นไอดีลของ S นั่นคือเราได้ว่า $I = S$ และ $SaS = \{0\}$ สำหรับทุก $a \in S$ แสดงว่า $S^3 = SSS = \{0\}$ ขัดแย้ง ดังนั้น $SaS = S$

($\Leftarrow$) ให้ $SaS = S$ สำหรับทุก $a \in S$ จะได้ว่า $S = SaS = (Sa)S \subseteq SS = S^2$ ดังนั้น $S^2 \neq \{0\}$ ให้ I เป็นไอดีลใดๆของ S โดยที่ $I \neq \{0\}$ จะได้ว่ามี $0 \neq x \in I$ ดังนั้น $S = SxS \subseteq SIS = (SI)S \subseteq IS \subseteq I$ นั่นคือ $I = S$ แสดงว่า S เป็นกึ่งกรุป 0 - เชิงเดียว □

2.4 แบบฝึกหัด (Exercise)

1) จงพิจารณากึ่งกรุป S ดังต่อไปนี้

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

จงพิจารณาว่า เซตต่อไปนี้ เป็นไอดีลของ S หรือไม่

(ก) $\{a, b\}$

(ข) $\{a, c\}$

(ค) $\{b, c, d\}$

2) ให้ $S = \{$ก, ข, ค, ง, จ, ฉ, ช$\}$ และกำหนดการกระทำทวิภาค $*$ บน S ดังนี้

$$x * y = \text{ก} \quad \text{สำหรับทุก } x, y \in S$$

จงหา (ข้อละ 1 เซต)

(ก) ไอดีลทางซ้ายของ S ที่แตกต่างจาก S

(ข) ไอดีลมุขสำคัญทางซ้ายของ S

(ค) ไอดีลมุขสำคัญทางขวาของ S

3) กำหนดกึ่งกรุป $\left(Z_6; +\right)$ จงหา

(ก) ไอดีลของ Z_6 ที่บรรจุ $\{\overline{2}, \overline{4}\}$

(ข) พิจารณาว่า Z_6 เป็นกึ่งกรุปเชิงเดียวหรือไม่

4) จากกึ่งกรุป $(\mathbb{I}^+; +)$ จงพิจารณาว่า $I = \{2x \mid x \in \mathbb{I}^+\}$ เป็นไอดีลของ $\mathbb{I}^+$ หรือไม่

5) จงแสดงว่า $(\mathbb{N}; +)$ เป็นกึ่งกรุปเชิงเดียวหรือไม่

6) จงแสดงว่า $(K_0; +)$ เป็นเซิกรุปเชิงเดียวทางซ้ายหรือไม่

7) จงแสดงว่า ทุกๆไอดีล I ของกึ่งกรุป $(N_k; min)$ จะอยู่ในรูป $I = \{0, 1, 2, ..., m\}$ เมื่อ $m \leq k$

8) จงแสดงว่า ทุกๆไอดีล I ของกึ่งกรุป $(\mathbb{N}; max)$ จะอยู่ในรูป $I = \{m, m+1, m+2, ...\}$ เมื่อ $m \in \mathbb{N}$

จงพิสูจน์ข้อความต่อไปนี้

9) ให้ S เป็นกึ่งกรุป จะได้ว่า

   (i) เซตของไอดีลทางซ้ายทั้งหมดของ S เป็นกึ่งกรุปย่อยของกึ่งกรุปกำลังของ S

   (ii) เซตของไอดีลทางขวาทั้งหมดของ S เป็นกึ่งกรุปย่อยของกึ่งกรุปกำลังของ S

   (iii) เซตของไอดีลทางทั้งหมดของ S เป็นกึ่งกรุปย่อยของกึ่งกรุปกำลังของ S

10) ให้ S เป็นกึ่งกรุป แล้วจะได้ว่า เซตของไอดีลทั้งหมดของ S เป็นไอดีลของกึ่งกรุปกำลังของ S

11) ถ้า S เป็นกึ่งกรุปเชิงเดียวทางซ้ายแล้ว S เป็นกึ่งกรุปเชิงเดียว

12) ถ้า S เป็นกึ่งกรุปเชิงเดียวทางขวาแล้ว S เป็นกึ่งกรุปเชิงเดียว

13) ให้ S เป็นกึ่งกรุปว่าง (zero semigroup) โดยมี z เป็นสมาชิกศูนย์ ถ้า $\emptyset \neq A \subseteq S$ และ $z \in A$ แล้ว A เป็นไอดีลของ S สำหรับ

จงพิสูจน์หรือยกตัวอย่างค้านข้อความต่อไปนี้

14) ถ้า S เป็นกึ่งกรุปว่าง (zero semigroup) และ A เป็นกึ่งกรุปย่อยของ S แล้ว A เป็นไอดีลของ S

15) ถ้า S เป็นกึ่งกรุป และ a เป็นสมาชิกนิจพล (idempotent) แล้ว Sa เป็นไอดีลมุขสำคัญทางซ้ายที่ก่อกำเนิดโดย a

16) ให้ S เป็นกึ่งกรุป และ $\emptyset \neq A \subseteq S$
ถ้า A เป็นไอดีลทางขวาของ S แล้ว AS เป็นไอดีลทางขวาของ S

17) ให้ S เป็นกึ่งกรุป และ $\emptyset \neq A \subseteq S$
ถ้า A เป็นไอดีลของ S แล้ว SAS เป็นไอดีลของ S

18) ให้ $n \in \mathbb{N}$ และ S เป็นกึ่งกรุป แล้ว

$$S^n := \{a_1 a_2 a_3 \ldots a_n \mid a_i \in S$$

เป็นไอดีลของ S

บทที่ 3

สาทิสสัณฐาน (Homomorphisms)

ในกลุ่มของกึ่งกรุปทั้งหลาย โครงสร้างของแต่ละกึ่งกรุปอาจเหมือนหรือแตกต่างกัน บางกลุ่มอาจมีลักษณะโครงสร้างที่เหมือนกัน นั่นคือ ลักษณะของการกระทำทวิภาคที่นิยาม ในกึ่งกรุปเหล่านั้นเป็นแบบเดียวกัน ถ้าเราสามารถจัดกลุ่มของกึ่งกรุปที่มีลักษณะโครงสร้างคล้ายกันไว้ด้วยกันได้จะเป็นการง่ายต่อการศึกษาสมบัติต่างๆของกึ่งกรุปเพราะถ้าโครงสร้างเหมือนกันกึ่งกรุปเหล่านั้นก็จะมีสมบัติแบบเดียวกัน

3.1 สาทิสสัณฐาน (Homomorphisms)

บทนิยาม 3.1 ให้ $(S;*)$ และ $(T;\cdot)$ เป็นกึ่งกรุป จะเรียกฟังก์ชัน $\phi : S \to T$ ว่าเป็น **สาทิสสัณฐาน**(homomorphism) จาก S ไปยัง T ถ้าทุกๆ $a,b \in S$, $\phi(a*b) = \phi(a)\cdot\phi(b)$ หรือเขียนสั้นๆเป็น $\phi(ab) = \phi(a)\phi(b)$

ตัวอย่าง 3.1 กำหนดกึ่งกรุป $(S;*)$ และกึ่งกรุป $(T;\cdot)$ ดังตาราง

$*$	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

,

$\cdot$	ก	ข	ค	ง
ก	ก	ก	ก	ก
ข	ก	ก	ก	ก
ค	ก	ก	ก	ก
ง	ก	ก	ก	ก

ให้ฟังก์ชัน $\phi : S \to T$ กำหนดโดย $\phi(s) =$ ก สำหรับทุก $s \in S$
จงพิจารณาว่า ϕ เป็นสาทิสสัณฐานหรือไม่

วิธีทำ. ให้ $s, w \in S$ เนื่องจาก

$$\begin{aligned}\phi(s*w) &= \text{ก}\\ &= \text{ก}\cdot\text{ก}\\ &= \phi(s)\cdot\phi(w)\end{aligned}$$

จะได้ว่า ϕ เป็นสาทิสสัณฐาน □

ตัวอย่าง 3.2 พิจารณากึ่งกรุป $(\mathbb{N};+)$ และ $(\mathbb{N};\cdot)$ เมื่อ $+,\ \cdot$ เป็นการบวกและการคูณปกติ นิยาม $\phi:\mathbb{N}\rightarrow\mathbb{N}$ โดย $\phi\left(n\right)=2^{n}$ สำหรับทุก $n\in\mathbb{N}$ จงพิจารณา ว่า ϕ เป็นสาทิสสัณฐานหรือไม่

วิธีทำ. ให้ $x,y\in\mathbb{N}$

เนื่องจาก

$$\begin{aligned}\phi\left(x+y\right)&=2^{x+y}\\&=2^{x}2^{y}\\&=\phi\left(x\right)\phi\left(y\right)\end{aligned}$$

เพราะฉะนั้น ϕ เป็นสาทิสสัณฐาน □

ตัวอย่าง 3.3 พิจารณากึ่งกรุป $(\mathbb{Z}_3;+)$ และ $(N_2;min)$ ให้ $\phi:\mathbb{Z}_3\longrightarrow N_2$ กำหนดโดย $\phi(\overline{x})=x$ จะได้ว่า ϕ ไม่เป็นสาทิสสัณฐาน ทั้งนี้เพราะว่า $\phi(\overline{1}+\overline{1})=\phi(\overline{2})=2\neq\phi(\overline{1})\ min\ \phi(\overline{1})=1\ min\ 1=1$

ตัวอย่าง 3.4 พิจารณากึ่งกรุป $S=(\mathbb{Z};\cdot)$ และ $T=(\mathbb{Z};+)$ โดยที่ $\cdot$ และ $+$ เป็นการคูณและการบวกปกติ ตามลำดับ นิยาม $\phi:S\rightarrow T$ โดย $\phi(x)=x$ สำหรับทุก $x\in\mathbb{Z}$ จะได้ว่า ϕ ไม่เป็นสาทิสสัณฐาน ทั้งนี้เพราะว่า

$$\begin{aligned}\phi(3\cdot5)&=\phi(15)\\&=15\\&\neq8=3+5\\&=\phi(3)+\phi(5)\end{aligned}$$

ตัวอย่าง 3.5 1) ให้ $\phi:K_0\longrightarrow K_1$ กำหนดโดย $\phi(f)=c_1$ สำหรับทุก $f\in K_0$ จะได้ว่า ϕ เป็น สาทิสสัณฐาน

2) ให้ S เป็นกึ่งกรุป และให้ $1_S:S\longrightarrow S$ กำหนดโดย $1_S(x)=x$ สำหรับทุก $x\in S$ จะได้ว่า 1_S เป็น สาทิสสัณฐาน

บทนิยาม 3.2 ให้ $\phi:S\rightarrow T$ เป็นสาทิสสัณฐานของกึ่งกรุป

จะเรียก ϕ ว่าเป็น **อิพิมอร์ฟิสซึม** (epimorphism) เขียนแทนด้วย $\phi:S\twoheadrightarrow T$ ถ้า ϕ เป็นฟังก์ชันทั่วถึง (onto) นั่นคือ สำหรับทุก $y\in P$ จะมี $x\in S$ ซึ่ง $\phi(x)=y$

จะเรียก ϕ ว่าเป็น **เอมเบดดิ้ง** (embedding) หรือ **โมโนมอร์ฟิสซึม** (monomorphism)

เขียนแทนด้วย $\phi : S \hookrightarrow T$ ถ้า ϕ เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่ง นั่นคือ ถ้า $\phi(x) = \phi(y)$ แล้ว $x = y$

จะเรียก ϕ ว่าเป็น **สมสัณฐาน** (isomorphisms) เขียนแทนด้วย $\phi : S \rightarrowtail T$ ถ้า ϕ เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่งและทั่วถึง ($1-1$, onto) และจะกล่าวว่า S และ T สมสัณฐานต่อกัน เขียนแทนด้วยสัญลักษณ์ $S \cong T$

จากนิยาม เราได้ว่า $S \cong T$ ก็ต่อเมื่อ มีสมสัณฐานจาก S ไป T

ตัวอย่าง 3.6 1) สำหรับกึ่งกรุป S ใดๆ จะได้ว่า $S \cong S$

2) $K_0 \cong K_1$

3) $C_4 \cong S$ เมื่อ S เป็นกึ่งกรุปศูนย์ทางขวาที่มี $|S| = 4$

ตัวอย่าง 3.7 จาก **ตัวอย่าง** 3.2 จะได้ว่า ϕ ไม่เป็นสมสัณฐาน ทั้งนี้เพราะ มี $0 \in \mathbb{N}$ แต่ไม่มี $x \in \mathbb{N}$ ซึ่งทำให้ $\phi(x) = 2^x = 0$ ดังนั้น ϕ ไม่เป็นฟังก์ชันชนิดทั่วถึง

ประพจน์ 3.1 ให้ $\psi : S \to T$ และ $\phi : T \to U$ เป็นสาทิสสัณฐานของกึ่งกรุป แล้วจะได้ว่า $\phi \circ \psi : S \to U$ เป็น สาทิสสัณฐานของกึ่งกรุป

พิสูจน์. ให้ $(S; *)$, $(T; \cdot)$ และ $(U; \heartsuit)$ เป็นกึ่งกรุป และให้ $a, b \in S$ จะได้ว่า

$$\begin{aligned}
(\phi \circ \psi)(a * b) &= \phi\big(\psi(a * b)\big) \\
&= \phi\big(\psi(a) \cdot \psi(b)\big) && ;\psi \text{ เป็นสาทิสสัณฐาน} \\
&= \phi\big(\psi(a)\big) \heartsuit \phi\big(\psi(b)\big) && ;\phi \text{ เป็นสาทิสสัณฐาน} \\
&= (\phi \circ \psi)(a) \heartsuit (\phi \circ \psi)(b)
\end{aligned}$$

ดังนั้น $\phi \circ \psi$ เป็นสาทิสสัณฐาน □

ประพจน์ 3.2 ถ้า $\phi : S \to T$ เป็นสาทิสสัณฐานของกึ่งกรุป และ แล้ว $\phi^{-1} : T \to S$ เป็นสมสัณฐาน

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

ประพจน์ 3.3 ให้ $\phi : S \to T$ เป็นสาทิสสัณฐานของกึ่งกรุป จะได้ว่า $\phi\big(a_1 a_2 \dots a_n\big) = \phi(a_1)\phi(a_2)\dots\phi(a_n)$ สำหรับทุก $a_1, a_2, \dots, a_n \in S$

พิสูจน์.

$$\begin{aligned}\phi\left(a_1a_2\ldots a_n\right) &= \phi\left(a_1\left(a_2a_3\ldots a_n\right)\right)\\ &= \phi\left(a_1\right)\phi\left(a_2a_3\ldots a_n\right)\\ &= \phi\left(a_1\right)\phi\left(a_2\left(a_3\ldots a_n\right)\right)\\ &= \phi\left(a_1\right)\phi\left(a_2\right)\phi\left(a_3\ldots a_n\right)\\ &\vdots\\ &= \phi\left(a_1\right)\phi\left(a_2\right)\phi\left(a_3\right)\ldots\phi\left(a_n\right)\end{aligned}$$

□

บทแทรก 3.1 ให้ $\phi : S \to T$ เป็นสาทิสสัณฐานของกึ่งกรุป จะได้ว่า $\phi(a^n) = \left(\phi(a)\right)^n$ สำหรับทุก $a \in S$ และ $n \geq 1$

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

ในการจับคู่ของสมาชิกในกึ่งกรุปที่มีเอกลักษณ์สองกึ่งกรุป โดยสาทิสสัณฐาน จะพบ ว่า เอกลักษณ์ของกึ่งกรุปทั้งสองต้องจับคู่กันเสมอ ทำให้เราได้ว่า ถ้า ในกึ่งกรุปทั้งสองนั้นมีเอกลักษณ์แค่กึ่งกรุปเดียว จะทำให้ กึ่งกรุปทั้งสองนั้นไม่สมสัณฐานต่อกัน

ประพจน์ 3.4 ให้ S และ T เป็นกึ่งกรุปที่มีเอกลักษณ์ ถ้า $\phi : S \to T$ เป็นกึ่งกรุปสาทิสสัณฐาน แล้ว $\phi(e) = e'$ โดยที่ e เป็นเอกลักษณ์ของ S และ e' เป็นเอกลักษณ์ ของ T

พิสูจน์. ให้ $a \in S$ เนื่องจาก $\phi\left(a\right) = \phi(ae) = \phi(a)\phi(e)$ และ $\phi\left(a\right) = \phi(ea) = \phi(e)\phi(a)$ จะได้ว่า $\phi(e)$ เป็นเอกลักษณ์ในกึ่งกรุป T เพราะฉะนั้น $\phi\left(e\right) = e'$ □

ให้ $\phi : S \to T$ เป็นสาทิสสัณฐานของกึ่งกรุป เขียนแทนเรนจ์ (range) ของ ϕ ด้วย $\phi(S)$ และเรียก $\phi(S)$ ว่า **ภาพสาทิสสัณฐานของ S ภายใต้** ϕ (homomorphic image of S under ϕ) ดังนั้นเราได้ว่า

$$\phi\left(S\right) = \{\phi\left(x\right) \mid x \in S\}$$

นอกจากนี้ สำหรับเซตย่อย A ที่ไม่ว่างใดๆของกึ่งกรุป S จะได้ว่า

$$\phi\left(A\right) = \{\phi\left(x\right) \mid x \in A\}$$

ถ้าเราพิจารณาภาพสาทิสสัณฐานของเซตย่อย A ในกึ่งกรุป S จะพบว่าเซตนี้จะเป็นกึ่งกรุปย่อยของ S เสมอ

ประพจน์ 3.5 ถ้า $\phi : S \to T$ เป็นสาทิสสัณฐานของกึ่งกรุป และ $A \leq S$ แล้ว $\phi(A) \leq T$

พิสูจน์. เป็นการเพียงพอที่จะแสดงเฉพาะสมบัติปิด ให้ $x, y \in \phi(A)$ จะได้ว่ามีสมาชิก x', y' ใน A ซึ่ง $\phi(x') = x, \phi(y') = y$ ดังนั้นโดยสมบัติสาทิสสัณฐานของ ϕ และสมบัติปิดของ A เราได้ $xy = \phi(x')\phi(y') = \phi(x'y') \in \phi(A)$ □

บทแทรก 3.2 ถ้า $\phi : S \to T$ เป็นสาทิสสัณฐานของกึ่งกรุป แล้ว $\phi(S) \leq T$

พิสูจน์. พิสูจน์เป็นแบบฝึกหัด □

ประพจน์ 3.6 ถ้า $\alpha : S \to P$ เป็นสาทิสสัณฐานของกึ่งกรุป (semigroup homomorphism) และ S เป็นกึ่งกรุปปรกติ(regular semigroup) แล้ว $\alpha(S)$ เป็นกึ่งกรุปปกติ

พิสูจน์. ให้ $x \in \alpha(S)$ จะได้ว่า มี $x' \in S$ ซึ่งทำให้ $x = \alpha(x')$ เนื่องจาก S เป็นกึ่งกรุปปกติ จะได้ว่า มี $y \in S$ ซึ่งทำให้ $x' = x'yx'$

ดังนั้น

$$\begin{aligned} x &= \alpha(x') \\ &= \alpha(x'yx') \\ &= \alpha(x')\alpha(y)\alpha(x') \end{aligned}$$

นั่นคือ x เป็นสมาชิกปกติ ดังนั้น $\alpha(S)$ เป็นกึ่งกรุปปกติ □

บทแทรก 3.3 ถ้า $\alpha : S \to P$ เป็นสมสัณฐานของกึ่งกรุป (semigroup isomorphism) และ S เป็นกึ่งกรุปปรกติ(regular semigroup) แล้ว P เป็นกึ่งกรุปปกติ

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

สำหรับกึ่งกรุปย่อยที่ก่อกำเนิดโดยเซตย่อย ของกึ่งกรุปใดๆ เมื่อเราพิจารณาเซตของ ภาพสาทิสสัณฐานของกึ่งกรุปย่อยนี้ จะพบว่า เป็นเซตเดียวกันกับกึ่งกรุปย่อยที่ก่อกำเนิดโดยภาพสาทิสสัณฐานของเซตย่อยนั้น

ประพจน์ 3.7 [8] ให้ $\phi : S \to T$ เป็นสาทิสสัณฐานของกึ่งกรุป ถ้า $\emptyset \neq X \subseteq S$ แล้ว $\phi\big(\langle X \rangle\big) = \langle \phi(X) \rangle$

พิสูจน์. ให้ $x \in \phi\big(\langle X\rangle\big)$ จะได้ว่ามี $w \in \langle X\rangle$ ซึ่งทำให้ $\phi(w) = x$ เนื่องจาก $w \in \langle X\rangle$ โดย **ทฤษฎีบท** 1.6 จะได้ว่า $x = a_1a_2\ldots a_n$ โดยที่ $a_i \in X$, $n \geq 1$ เนื่องจาก ϕ เป็นสาทิสสัณฐาน จะได้ว่า $\phi(x) = \phi\big(a_1a_2\ldots a_n\big) = \phi(a_1)\phi(a_2)\ldots\phi(a_n) \in \langle\phi(X)\rangle$ ดังนั้น $\phi\big(\langle X\rangle\big) \subseteq \langle\phi(X)\rangle$

ให้ $t \in \langle\phi(X)\rangle$ โดย **ทฤษฎีบท** 1.6 จะได้ว่า $t = \phi(b_1)\phi(b_2)\ldots\phi(b_n)$ โดยที่ $\phi(b_i) \in \phi(X)$, $n \geq 1$ และ $b_i \in X$ จากสมบัติของสาทิสสัณฐาน ϕ จะได้ว่า $t = \phi(b_1)\phi(b_2)\ldots\phi(b_n) = \phi\big(b_1b_2\ldots b_n\big) \in \phi(X)$ □

ทฤษฎีบท 3.1 [9] ถ้า S เป็นกึ่งกรุปแถบมุมฉาก แล้วจะมีกึ่งกรุปย่อยศูนย์ทางซ้าย L และกึ่งกรุปย่อยศูนย์ทางขวา R ของ S ซึ่ง $S \cong L \times R$

พิสูจน์. ให้ $c \in S$ ให้ $L = Sc$ และ $R = cS$ โดย **ทฤษฎีบท** 1.8 จะได้ว่า Sc เป็นกึ่งกรุปย่อยทางซ้าย และ cS เป็นกึ่งกรุปย่อยทางขวาของ S

ให้ $\phi : S \to L \times R$ นิยามโดย $\phi(x) = (xc, cx)$ สำหรับทุก $x \in S$ เห็นได้ชัดว่า ϕ เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่ง ต่อไปจะแสดงว่า ϕ เป็นฟังก์ชันชนิดทั่วถึง ให้ $(ac, cb) \in L \times R$ จะได้ว่า โดย**ทฤษฎีบท** 1.7 $(ac, cb) = (abc, cab) = ((ab)c, c(ab)) = \phi(ab)$ นั่นคือ เราได้ว่าสำหรับแต่ละ $(ac, cb) \in L \times R$ จะมี $ab \in S$ ซึ่ง $\phi(ab) = (ac, cb)$ ดังนั้น ϕ เป็นฟังก์ชันชนิดทั่วถึง

ต่อไปเราจะแสดงว่า ϕ เป็นสมสัณฐาน ให้ $a, b \in S$ จะได้ว่า

$$\begin{aligned}
\phi(ab) &= ((ab)c, c(ab)) \\
&= (abc, cab) \\
&= (ac, cb) \\
&= (a(cb)c, c(ac)b) \\
&= ((ac)(bc), (ca)(cb)) \\
&= (ac, ca)(bc, cb) \\
&= \phi(a)\phi(b)
\end{aligned}$$

□

3.2 สมภาค (Congruences)

บทนิยาม 3.3 ให้ ρ เป็นความสัมพันธ์สมมูลบนกึ่งกรุป S จะเรียก ρ ว่าเป็น **สมภาคทางซ้าย** (left congruence) ถ้า

$$\big(\forall x, y, z \in S\big) \;:\; x \,\rho\, y \Rightarrow (zx) \,\rho\, (zy)$$

จะเรียก ρ ว่าเป็น **สมภาคทางขวา** (right congruence) ถ้า

$$\big(\forall x, y, z \in S\big) \;:\; x \,\rho\, y \Rightarrow (xz) \,\rho\, (yz)$$

จะเรียก ρ ว่าเป็น **สมภาค** (congruence) ถ้า ρ เป็นสมภาคทางซ้ายและทางขวา และจะเรียก ชั้นสมมูล (equivalence class) ของสมภาค ว่า **ชั้นสมภาค** (congruence class)

สำหรับกึ่งกรุป S ใดๆ กำหนดให้

$\Delta_S = \{(a, a) \mid a \in S\}$ และ

$\nabla_S = \{(a, b) \mid a, b \in S\} = S \times S$

ตัวอย่าง 3.8 พิจารณากึ่งกรุป $\big(N_3; min\big)$ จงพิจารณาว่า ความสัมพันธ์ที่กำหนดในแต่ละข้อต่อไปนี้ เป็นสมภาคหรือไม่

(ก) $\rho = \Delta_{N_3} \cup \{(1, 2), (2, 1)\}$

(ข) $\phi = \Delta_{N_3} \cup \{(2, 3), (3, 2)\}$

วิธีทำ. (ก) เห็นได้ชัดว่า ρ เป็นความสัมพันธ์สมมูลบน N_3 ต่อไปจะพิจารณาว่า ρ เป็นสมภาคทางซ้ายหรือไม่ ให้ $(x, y) \in \rho$ และ $z \in N_3$

ถ้า $x = y$ โดยสมบัติการสะท้อนของ ρ จะได้ว่า $(zx, zy) = (zx, zx) \in \rho$

ถ้า $x \neq y$ จะได้ว่า $(x, y) = (1, 2)$ หรือ $(x, y) = (2, 1)$ ถ้า $(x, y) = (1, 2)$ จะได้ว่า $(zx, zy) = (z\ min\ 1, z\ min\ 2) \in \{(0, 0), (1, 1), (1, 2)\} \subseteq \rho$ ถ้า $(x, y) = (2, 1)$ จะได้ว่า $(zx, zy) = (z\ min\ 2, z\ min\ 1) \in \{(0, 0), (1, 1), (2, 1)\} \subseteq \rho$ แสดงว่า สำหรับทุก $z \in N_3$ และทุก $(x, y) \in \rho$ เราได้ว่า $(zx, zy) \in \rho$ นั่นคือ ρ เป็นสมภาคทางซ้าย

ต่อไปจะแสดงว่า ρ เป็นสมภาคทางขวาหรือไม่ เนื่องจาก $zx = z\ min\ x = min\{z, x\} = min\{x, z\} = xz$ สำหรับทุก $z, x \in N_3$ จะได้ว่า $(zx, zy) = (xz, yz)$ ดังนั้น $(zx, zy) \in \rho$ สำหรับทุก $z \in N_3$ และทุก $(x, y) \in \rho$

นั่นคือ ρ เป็นสมภาค

(ข) ให้ทำเป็นแบบฝึกหัด □

ตัวอย่าง 3.9 พิจารณากึ่งกรุป $\big(N_3; min\big)$ จงพิจารณาว่า $\rho = \Delta_{N_3} \cup \{(1, 3), (3, 1)\}$ เป็นสมภาคหรือไม่

วิธีทำ. เนื่องจาก $2 \in N_3$ และ $(1, 3) \in \rho$ แต่ $(2\ min\ 1, 2\ min\ 3) = (1, 2) \notin N_3$ จะได้ว่า ρ ไม่เป็นสมภาคทางซ้าย ดังนั้น ρ ไม่เป็นสมภาค □

ตัวอย่าง 3.10 ในกึ่งกรุป $(N_3; max)$ จงพิจารณาว่า ความสัมพันธ์ที่กำหนดให้ในแต่ ละข้อต่อไปนี้เป็นสมภาคหรือไม่

(ก) $\rho_1 = \Delta_{N_3} \cup \{(1,2),(2,1)\}$

(ข) $\rho_2 = \Delta_{N_3} \cup \{(0,3),(3,0)\}$

วิธีทำ. ให้ทำเป็นแบบฝึกหัด □

ตัวอย่าง 3.11 ให้ S เป็นกึ่งกรุป จะได้ว่า

1) Δ_S เป็นสมภาค และเป็นสมภาคที่เล็กที่สุดของ S

2) ∇_S เป็นสมภาค และเป็นสมภาคที่ใหญ่ที่สุดของ S

วิธีทำ. ให้ทำเป็นแบบฝึกหัด □

เราพบว่า ผลคุณของสองคู่อันดับใดๆในสมภาค จะยังคงเป็นสมาชิกใน สมภาคนั้นเสมอ หรือกล่าวอีกนัยหนึ่งคือ ผลคุณที่เกิดขึ้นอยู่ในชั้นสมภาค (congruence class) เดียวกัน

ทฤษฎีบท 3.2 ให้ ρ เป็นความสัมพันธ์สมมูลบนกึ่งกรุป S แล้วจะได้ว่า
ρ เป็นสมภาค ก็ต่อเมื่อ สำหรับทุก $x_1, x_2, y_1, y_2 \in S$ $\big(x_1 \ \rho \ y_1 \ \wedge \ x_2 \ \rho \ y_2 \Rightarrow x_1x_2 \ \rho \ y_1y_2\big)$

x_1 y_1		x_1x_2 y_1y_2
	x_2 y_2	

พิสูจน์. $(\Rightarrow)$ ให้ $(x_1, y_1) \in \rho$ และ $(x_2, y_2) \in \rho$ เนื่องจาก ρ เป็นสมภาค จะได้ว่า $(x_1x_2, y_1x_2) \in \rho$ และ $(y_1x_2, y_1y_2) \in \rho$ ดังนั้น โดยสมบัติการถ่ายทอดของ ρ จะได้ว่า $(x_1x_2, y_1y_2) \in \rho$

$(\Leftarrow)$ ให้ $(x, y) \in \rho$ และ $z \in S$ เนื่องจาก ρ มีสมบัติการสะท้อนบน S จะได้ว่า $(z, z) \in \rho$ ดังนั้นโดยสมมติฐานของการพิสูจน์จะได้ว่า $(zx, zy) \in \rho$ และ $(xz, yz) \in \rho$ นั่นคือ ρ เป็นสมภาค □

สำหรับกึ่งกรุป S ใดๆ กำหนดสัญลักษณ์ $Con(S)$ ดังนี้

$$Con(S) = \{\ \rho \mid \rho \text{ เป็นสมภาคบน } S\}$$

เราพบว่าเซตของสมภาคปิดภายใต้การอินเตอร์เซกชันแบบจำกัด (finite intersection) ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.3 ให้ I เป็นเซตดัชนี ถ้า $\rho_i \in Con(S)$ สำหรับ $i \in I$ แล้วจะได้ว่า $\bigcap\limits_{i \in I} \rho_i \in Con(S)$

พิสูจน์. เนื่องจากแต่ละ ρ_i สำหรับ $i \in I$ เป็นความสัมพันธ์สมมูลจะได้ว่า $\bigcap\limits_{i \in I} \rho_i$ เป็นความสัมพันธ์สมมูลบน S ให้ $(x, y) \in \bigcap\limits_{i \in I} \rho_i$ จะได้ว่า $(x, y) \in \rho_i$ สำหรับทุก $i \in I$ ดังนั้น สำหรับทุก $z \in S$ และ $i \in I$ จะได้ว่า $(zx, zy),\ (xz, yz) \in \rho_i$ นั่นคือ $(zx, zy),\ (xz, yz) \in \bigcap\limits_{i \in I} \rho_i$ แสดงว่า $\bigcap\limits_{i \in I} \rho_i$ เป็นสมภาค $\square$

เซตของสมภาคไม่ปิดภายใต้การยูเนียนแบบจำกัด (finite union) ดังตัวอย่างต่อไปนี้

ตัวอย่าง 3.12 จาก **ตัวอย่าง** 3.8 เราพบว่า ρ และ ϕ เป็นสมภาค พิจารณา

$$\rho \cup \phi = \Delta_{N_3} \cup \{(1, 2), (2, 1), (2, 3), (3, 2)\}$$

จะพบว่า $\rho \cup \phi$ ไม่เป็นความสัมพันธ์สมมูล ทั้งนี้เพราะ $(1, 2), (2, 3) \in \rho \cup \phi$ แต่ $(1, 3) \notin \rho \cup \phi$ ดังนั้น $\rho \cup \phi$ ไม่เป็นสมภาค

ประพจน์ 3.8 ให้ I เป็นเซตดัชนี และ $\rho_i \in Con(S)$ สำหรับ $i \in I$ แล้วจะได้ว่า
ถ้า $\bigcup\limits_{i \in I} \rho_i$ เป็นความสัมพันธ์สมมูล แล้ว $\bigcup\limits_{i \in I} \rho_i \in Con(S)$

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด $\square$

3.3 กึ่งกรุปผลหาร (Quotient Semigroups)

ถ้าเรามีกึ่งกรุป และสมภาคบนกึ่งกรุปนั้น เราสามารถสร้างกึ่งกรุปใหม่จาก กึ่งกรุป และสมภาคนั้นได้เสมอ

ให้ $(S; *)$ เป็นกึ่งกรุป และ $\rho \in Con(S)$ กำหนดเซต S/ρ ดังนี้

$$S/\rho \ = \ \{\ [x]_\rho \mid x \in S\ \}$$

นิยามการดำเนินการทวิภาคบน S/ρ โดย สำหรับ $[x]_\rho,\ [y]_\rho \in S/\rho$ เราให้

$$[x]_\rho[y]_\rho = [x * y]_\rho$$

สามารถตรวจสอบได้โดยง่ายว่าการดำเนินการทวิภาคที่นิยามนี้มีสมบัติการเปลี่ยนกลุ่ม ดังนั้น S/ρ เป็นกึ่งกรุป เรียกว่า **กึ่งกรุปผลหารของ S มอดูโล** ρ (quotient semigroup of S modulo ρ) หรือเรียกสั้นๆว่า **กึ่งกรุปผลหาร**

ข้อสังเกต 3.1 สำหรับกึ่งกรุป S ใดๆ

1) $|S/\Delta_S| = |S|$

2) $|S/\nabla_S| = 1$

ตัวอย่าง 3.13 จาก **ตัวอย่าง** 3.8 จะได้ $N_3/\rho = \{\ [0]_\rho, [1]_\rho = [2]_\rho, [3]_\rho\ \}$ และตารางการคูณของกึ่งกรุปผลหาร N_3/ρ ปรากฏดังตาราง

	$[0]_\rho$	$[1]_\rho$	$[3]_\rho$
$[0]_\rho$	$[0]_\rho$	$[0]_\rho$	$[0]_\rho$
$[1]_\rho$	$[0]_\rho$	$[1]_\rho$	$[1]_\rho$
$[3]_\rho$	$[0]_\rho$	$[1]_\rho$	$[3]_\rho$

3.4 สาทิสสัณฐานธรรมชาติ (Natural Homomorphisms)

ในกึ่งกรุปใดๆ เราสามารถสร้างกึ่งกรุปผลหารของมันได้เสมอ นอกจากนี้เรายังสามารถสร้าง สาทิสสัณฐานระหว่างกึ่งกรุปและกึ่งกรุปผลหารของมันได้เสมอ ซึ่งมีวิธีการสร้างดังนี้

ให้ $\rho \in Con(S)$ นิยาม $\rho^{nat} : S \to S/\rho$ โดย

สำหรับทุก $x \in S$

$$\rho^{nat}(x) \ = \ [x]_\rho$$

ดังนั้น สำหรับ $x, y \in S$ เราได้ว่า

$$\begin{aligned}\rho^{nat}(xy) &= \big[xy\big]_\rho \\ &= [x]_\rho[y]_\rho \\ &= \rho^{nat}(x)\rho^{nat}(y)\end{aligned}$$

ดังนั้น ρ^{nat} เป็นสาทิสสัณฐาน เรียกว่า **สาทิสสัณฐานธรรมชาติ** (natural homomorphism)

ตัวอย่าง 3.14 จาก **ตัวอย่าง** 3.13 จะได้สาทิสสัณฐานธรรมชาติ $\rho^{nat} : N_3 \to N_3/\rho$ โดยที่ $\rho^{nat}(0) = [0]_\rho$, $\rho^{nat}(1) = [1]_\rho$, $\rho^{nat}(2) = [1]_\rho$ และ $\rho^{nat}(3) = [3]_\rho$

ทฤษฎีบท 3.4 ถ้า $\rho \in Con(S)$ แล้ว ρ^{nat} เป็นอิพิมอร์ฟิสซึม

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

ให้ $\phi : S \to T$ เป็นสาทิสสัณฐานของกึ่งกรุป นิยาม **เคอร์เนล** (kernel) ของ ϕ ดังนี้

$$ker(\phi) \ := \ \{(x, y) \mid \phi(x) = \phi(y)\}$$

เป็นการง่ายที่จะแสดงว่า $ker(\phi)$ เป็นความสัมพันธ์สมมูล

ตัวอย่าง 3.15 จาก **ตัวอย่าง** 3.14 จะได้ $ker(\rho^{nat}) = \{(0,0), (1,1), (1,2), (2,1), (3,3)\}$

ตัวอย่าง 3.16 1) ในกึ่งกรุป S ใดๆ เราได้ว่า $ker(1_S) = \Delta_S$

2) ถ้า $\phi : S \to T$ เป็นสมสัณฐานของกึ่งกรุป แล้ว $ker(\phi) = \Delta_S$

เราสามารถสร้างสมภาคจากสาทิสสัณฐานระหว่างกึ่งกรุปได้ เสมอ ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.5 ถ้า $\phi : S \to T$ เป็นสาทิสสัณฐานของกึ่งกรุป แล้ว $ker(\phi)$ เป็นสมภาคของ S

พิสูจน์. ให้ $(x, y) \in ker(\phi)$ จะได้ว่า $\phi(x) = \phi(y)$ สำหรับ ทุก $z \in S$ เราได้ว่า

$$\begin{aligned} \phi(zx) &= \phi(z)\phi(x) \\ &= \phi(z)\phi(y) \\ &= \phi(zy) \end{aligned}$$

และ

$$\begin{aligned} \phi(xz) &= \phi(x)\phi(z) \\ &= \phi(y)\phi(z) \\ &= \phi(yz) \end{aligned}$$

ดังนั้น $(zx, zy) \in ker(\phi)$ และ $(xz, yz) \in ker(phi)$ นั่นคือ $\mathrm{ker}(\phi)$ เป็นสมภาค □

เราพบว่า ทุกๆสมภาคเป็นเคอร์เนลของบางสาทิสสัณฐาน ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 3.6 ถ้า $\rho \in Con(S)$ แล้วจะได้ว่า $\rho = ker(\rho^{nat})$

พิสูจน์. ให้ $(x, y) \in \rho$ จะได้ว่า $x \ \rho \ y$ ดังนั้น $x \in [y]_\rho$ นั่นคือ $[x]_\rho = [y]_\rho$ แสดงว่า $\rho^{nat}(x) = \rho^{nat}(y)$ ดังนั้น $(x, y) \in ker(\rho^{nat})$ นั่นคือ $\rho \subseteq ker(\rho^{nat})$

ให้ $(x, y) \in ker(\rho^{nat})$ จะได้ว่า $\rho^{nat}(x) = \rho^{nat}(y)$ ดังนั้น $[x]_\rho = [y]_\rho$ แสดงว่า $x\rho y$ นั่นคือ $(x, y) \in \rho$ □

บทแทรก 3.4 ทุกๆสมภาคเป็นเคอร์เนลของบางสาทิสสัณฐาน

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

ตัวอย่าง 3.17 จาก **ตัวอย่าง** 3.8 และ ตัวอย่าง 3.14 จะได้ว่า $\rho = \Delta_{N_3} \cup \{(1, 2), (2, 1)\} = ker(\rho^{nat})$

ทฤษฎีบท 3.7 (Homomorphism Theorem)
ถ้า $\alpha : S \to P$ เป็นสาทิสสัณฐานของกึ่งกรุป แล้วจะได้ว่ามีเอมเบดดิ้ง $\beta : S/ker(\alpha) \hookrightarrow P$ เพียงหนึ่งเดียว ซึ่งทำให้ไดอะแกรมต่อไปนี้สลับ(diagram commutes) นั่นคือ $\alpha = \beta \circ \big(ker(\alpha)\big)^{nat}$

$$\begin{tikzcd}
S \arrow[rr, "\alpha"] \arrow[dr, "ker(\alpha)^{nat}"'] & & P \\
& S/ker(\alpha) \arrow[ur, "\beta"'] &
\end{tikzcd}$$

พิสูจน์. ให้ $\rho = ker(\alpha)$ จะได้ว่า $\rho^{nat} : S \to S/\rho$ นิยาม $\beta : S/\rho \to P$ โดย $\beta\big([x]_\rho\big) = \alpha(x)$ สำหรับ ทุก $x \in S$ ต่อไปจะแสดงว่า β เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่ง ให้ $\beta([x]_\rho) = \beta([y]_\rho)$ จะได้ว่า $\alpha(x) = \alpha(y)$ ดังนั้น $(x, y) \in ker(\alpha)$ แต่ $ker(\alpha) = \rho$ ดังนั้น $(x, y) \in \rho$ นั่นคือ $[x]_\rho = [y]_\rho$

นอกจากนี้เราได้ว่า β เป็น สาทิสสัณฐาน ทั้งนี้เพราะว่า

$$\begin{aligned}
\beta\big([x]_\rho[y]_\rho\big) &= \beta\big([xy]_\rho\big) \\
&= \alpha(xy) \\
&= \alpha(x)\alpha(y) \\
&= \beta\big([x]_\rho\big)\beta\big([y]_\rho\big)
\end{aligned}$$

นั่นคือ β เป็นเอมเบดดิ้ง
ให้ $x \in S$ จะได้ว่า

$$\begin{aligned}\beta \circ \rho^{nat}(x) &= \beta(rho^{nat}(x)) \\ &= \beta\big([x]_\rho\big) \\ &= \alpha(x)\end{aligned}$$

แสดงว่า $\beta \circ \rho^{nat} = \alpha$ นั่นคือ $ker(\alpha) \circ \rho^{nat} = \alpha$

สมมุติมีเอมเบดดิ้ง $\gamma : S/\rho \to P$ ซึ่งมีคุณสมบัติเหมือนกับ β นั่นคือ $\alpha = \gamma \circ \rho^{nat}$ ดังนั้น สำหรับ $x \in S$ เราได้ว่า $\gamma\big([x]_\rho\big) = \alpha(x)$ แสดงว่า $\gamma = \beta$ □

ทฤษฎีบท 3.8 (Isomorphism Theorem)
ให้ $\alpha : S \to P$ เป็นสาทิสสัณฐานของกึ่งกรุป จะได้ว่า $\alpha(S) \cong S/ker(\alpha)$

พิสูจน์. พิสูจน์เป็นแบบฝึกหัด □

3.5 แบบฝึกหัด (Exercise)

1) ให้ $S = (Z; \cdot)$ และ $T = (Z; +)$ โดยที่ $\cdot$ คือการคูณปกติ และให้ $\phi : S \to T$ กำหนดโดย $\phi(x) = x$ สำหรับทุก $x \in Z$ จงแสดงว่า ϕ เป็นสาทิสสัณฐานหรือไม่

2) กำหนด a เป็นสมาชิกใดๆในกึ่งกรุป S และให้ $\phi : S \to Sa$ นิยามโดย $\phi(x) = xa$ สำหรับทุก $x \in S$
(ก) จงแสดงว่า ϕ เป็นสาทิสสัณฐานหรือไม่
(ข) จงหา $ker\phi$

3) สำหรับกึ่งกรุป $(N_3; min)$ จงพิจารณาว่า $\phi = \Delta_{N_3} \cup \{(2,3),(3,2)\}$ เป็นสมภาค หรือไม่

4) พิจารณากึ่งกรุป $(N_3; max)$ จงแสดงว่าความสัมพันธ์ที่กำหนดต่อไปนี้เป็นสมภาค หรือไม่
(ก) $\rho_1 = \Delta_{N_3} \cup \{(1,2),(2,1)\}$
(ข) $\rho_2 = \Delta_{N_3} \cup \{(0,3),(3,0)\}$

จงพิจารณาว่าข้อความต่อไปนี้เป็นจริงหรือเท็จ ถ้าเป็นจริงจงพิสูจน์ ถ้าเป็นเท็จจงยกตัวอย่างค้าน

5) ให้ S เป็นกึ่งกรุป แล้วจะได้ว่า $(\mathbb{Z}_4; +) \cong \langle a \rangle$ เมื่อ $a \in S$ และ $|a| = 4$

6) ถ้า $\phi : S \to T$ เป็นสาทิสสัณฐานของกึ่งกรุป และ A เป็นกึ่งกรุปย่อยของ T แล้ว $\phi^{-1}(A)$ เป็นเซตว่างหรือ $\phi^{-1}(A)$ เป็นกึ่งกรุปย่อยของ S อย่างใดอย่างหนึ่ง

จงพิสูจน์ข้อความต่อไปนี้

7) ถ้า $\phi : S \to T$ เป็นสาทิสสัณฐานของกึ่งกรุป แล้ว ϕ^{-1} เป็น สาทิสสัณฐานของกึ่งกรุป

8) ให้ S เป็นกึ่งกรุป จะได้ว่า Δ_S^{nat} เป็นสมสัณฐาน

9) Δ_S เป็นสมภาคที่เล็กที่สุดของกึ่งกรุป S

10) ∇_S เป็นสมภาคที่ใหญ่ที่สุดของกึ่งกรุป S

11) ถ้า $\rho \in Con(S)$ แล้ว ρ^{nat} เป็นอีพิมอร์ฟิสซึม

12) ถ้า $\alpha : S \to T$ เป็นสาทิสสัณฐานของกึ่งกรุป แล้วจะได้ว่า $\alpha(S) \cong S/ker(\alpha)$

บทที่ 4

ความสัมพันธ์ของกรีน (Green ’s Relations)

ในปี ค.ศ. 1951 เจมส์ อเล็กซานเดอร์ กรีน (Jams Alexxander Green) ได้นิยามความสัมพันธ์ บนกึ่งกรุป ซึ่งต่อมาถูกเรียกกันโดยทั่วไปว่า **ความสัมพันธ์ของกรีน** (Green’s relations) ความสัมพันธ์เหล่านี้ถูกใช้ ในจำแนกสมาชิกในกึ่งกรุปโดยอาศัยแนวคิดของไอดีลมุขสำคัญ (principal ideal) ที่สมาชิกเหล่านั้นก่อกำเนิดขึ้น นอกจากนี้ความสัมพันธ์ของกรีนยังเป็นเครื่องมือ สำคัญในการศึกษา เกี่ยวกับการหาร (divisibility) หลายชนิดในกึ่งกรุป

4.1 ความสัมพันธ์ของกรีน แบบ $\mathcal{L}, \mathcal{R}$ และ $\mathcal{J}$ (Green’s Relations $\mathcal{L}, \mathcal{R}$,$\mathcal{J}$)

ก่อนอื่นเราจะกล่าวถึงความสัมพันธ์ของกรีนสามแบบแรกที่เป็นที่นิยมศึกษากันโดยทั่วไป คือ ความสัมพันธ์ $\mathcal{L}, \mathcal{R}$ และ $\mathcal{J}$ ความสัมพันธ์ทั้งสามแบบนี้อาศัยไอดีลมุขสำคัญ ไอดีลมุขสำคัญทางซ้าย ไอดีลมุขสำคัญทางขวา ในการนิยาม

บทนิยาม 4.1 ให้ S เป็นกึ่งกรุป นิยามความสัมพันธ์ $\mathcal{L}, \mathcal{R}$ และ $\mathcal{J}$ ดังนี้
สำหรับ $a, b \in S$

$$
\begin{aligned}
a\mathcal{L}b &\iff S^1a = S^1b \\
a\mathcal{R}b &\iff aS^1 = bS^1 \\
a\mathcal{J}b &\iff S^1aS^1 = S^1bS^1
\end{aligned}
$$

ข้อสังเกต 4.1 1) $\mathcal{L}, \mathcal{R}$ และ $\mathcal{J}$ เป็นความสัมพันธ์สมมูล

2) $\mathcal{L} \subseteq \mathcal{J}$ และ $\mathcal{R} \subseteq \mathcal{J}$

ตัวอย่าง 4.1 พิจารณากึ่งกรุป S กำหนดดังตาราง

$*$	a	b	c
a	a	a	a
b	b	b	b
c	b	c	c

จงหาความสัมพันธ์ $\mathcal{L}, \mathcal{R}$ และ $\mathcal{J}$

วิธีทำ. อันดับแรก หาความสัมพันธ์ $\mathcal{L}$
สำหรับ $x \in S$ จะได้ว่า

$$\begin{aligned} S^1x &= Sx \cup \{x\} \\ &= \{sx | s \in S\} \cup \{x\} \\ &= \{s | s \in S\} \cup \{x\} \\ &= S \end{aligned}$$

ดังนั้น $S^1a = S^1b = S^1c = S$
นั่นคือ $\mathcal{L} = \big\{(a,a),(a,b),(a,c),(b,a),(b,b),(b,c),(c,a),(c,b),(c,c)\big\} = S \times S$

ต่อไปจะพิจารณาความสัมพันธ์ $\mathcal{R}$
สำหรับ $x \in S$ จะได้ว่า

$$\begin{aligned} xS^1 &= xS \cup \{x\} \\ &= \{xs | s \in S\} \cup \{x\} \\ &= \{x\} \cup \{x\} \\ &= \{x\} \end{aligned}$$

แสดงว่า สำหรับ $x, y \in S$, $xS^1 = yS^1$ ก็ต่อเมื่อ $x = y$ นั่นคือ $\mathcal{R} = \big\{(a,a),(b,b),(c,c)\big\}$

ต่อไปจะพิจารณาความสัมพันธ์ $\mathcal{J}$ สำหรับ แต่ละ $x \in S$ จะได้ว่า $S = Sx \subseteq S^1xS^1$
ดังนั้น $S^1xS^1 = S$ สำหรับทุก $x \in S$

นั่นคือ $\mathcal{J} = \big\{(a,a),(a,b),(a,c),(b,a),(b,b),(b,c),(c,a),(c,b),(c,c)\big\} = S \times S$ □

ตัวอย่าง 4.2 กำหนดกึ่งกรุป $(N_5; min)$ จงหา $\mathcal{L}, \mathcal{R}$ และ $\mathcal{J}$

วิธีทำ. ให้ $x, y \in N_5$ จะได้ว่า $(N_3)^1x = \{x \; min \; m \mid n \in N_5\} = \{0, 1, 2, \ldots, x\}$
ดังนั้น $(N_5)^1x = (N_5)^1y$ ก็ต่อเมื่อ $x = y$ นั่นคือ $\mathcal{L} = \Delta_{N_5}$

เนื่องจาก $(N_5)^1x = x(N_5)^1$ จะได้ว่า $x(N_5)^1 = y(N_5)^1$ ก็ต่อเมื่อ $x = y$ ดังนั้น $\mathcal{R} = \Delta_{N_5}$ นอกจากนี้ยังได้ว่า $\mathcal{J} = \Delta_{N_5}$ □

ตัวอย่าง 4.3 กำหนดกึ่งกรุป $(Z_4;+)$ จงหาความสัมพันธ์ $\mathcal{L},\mathcal{R}$ และ $\mathcal{J}$

วิธีทำ. ให้ทำเป็นแบบฝึกหัด □

ประพจน์ 4.1 ให้ S เป็นกึ่งกรุป และ $a,b\in S$ จะได้ว่า

(i) $a\mathcal{L}b$ ก็ต่อเมื่อ $a=xb$ และ $b=ya$ สำหรับบาง $x,y\in S^1$

(ii) $a\mathcal{R}b$ ก็ต่อเมื่อ $a=bx$ และ $b=ay$ สำหรับบาง $x,y\in S^1$

พิสูจน์. (i) $(\Rightarrow)$ ให้ $a\mathcal{L}b$ จะได้ว่า $S^1a=S^1b$ เนื่องจาก $a\in Sa\cup\{a\}=S^1a=S^1b$ จะได้ว่า $a=xb$ สำหรับบาง $x\in S^1$ ในทำนองเดียวกัน $b\in Sb\cup\{b\}=S^1b=S^1a$ จะได้ว่า $b=ya$ สำหรับบาง $y\in S^1$

$(\Leftarrow)$ ให้ $a=xb$ และ $b=ya$ สำหรับบาง $x,y\in S^1$ จะแสดงว่า $a\mathcal{L}b$ นั่นคือต้องแสดงว่า $S^1a=S^1b$

ให้ $w\in S^1a$ จะได้ว่า $w=sa$ สำหรับบาง $s\in S^1$ ดังนั้น $w=sa=s(xb)=(sx)b\in S^1b$ นั่นคือ $S^1a\subseteq S^1b$ ในทำนองเดียวกันสามารถแสดงได้ว่า $S^1b\subseteq S^1a$ นั่นคือ $S^1a=S^1b$

(ii) สามารถพิสูจน์ได้ในทำนองเดียวกันกับ (i) □

ประพจน์ 4.2 ให้ S เป็นกึ่งกรุป และ $a,b\in S$ จะได้ว่า

$a\mathcal{J}b$ ก็ต่อเมื่อ $a=xbu$ และ $b=yav$ สำหรับบาง $x,y,u,v\in S^1$

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

ประพจน์ 4.3 ความสัมพันธ์ $\mathcal{L}$ เป็นสมภาคทางขวา และ ความสัมพันธ์ $\mathcal{R}$ เป็นสมภาคทางซ้าย

พิสูจน์. ให้ $(x,y)\in\mathcal{L}$ จะได้ว่า $S^1x=S^1y$ ดังนั้น สำหรับแต่ละ $z\in S$, $(S^1x)z=(S^1y)z$ นั่นคือ $S^1(xz)=S^1(yz)$ แสดงว่า $(xz,yz)\in\mathcal{L}$ ดังนั้น $\mathcal{L}$ เป็นสมภาคทางขวา

สำหรับการแสดงว่าความสัมพันธ์ $\mathcal{R}$ เป็นสมภาคทางซ้าย สามารถแสดงได้ในทำนองเดียวกัน □

กำหนดกึ่งกรุป S และ $x\in S$ เราให้ L_x และ R_x แทน **ชั้นสมมูลที่บรรจุ** x (equivalence class containing x) ดังนั้น

$$L_x=\{a\in S\mid x\mathcal{L}a\}\ ,\quad R_x=\{a\in S\mid x\mathcal{R}a\}$$

ตัวอย่าง 4.4 จาก **ตัวอย่าง** 4.1 จะได้ว่า $L_a=\{a,b,c\}$, $L_b=\{a,b,c\}$, $L_c=\{a,b,c\}$, $R_a=\{a\}$, $R_b=\{a\}$ และ $R_c=\{c\}$,

ประพจน์ 4.4 ถ้า e เป็นสมาชิกนิจพลในกึ่งกรุป S แล้ว e เป็นเอกลักษณ์ทางซ้ายสำหรับ R_e และ เป็นเอกลักษณ์ทางขวาสำหรับ L_e

พิสูจน์. ให้ $x \in R_e$ จะได้ว่า $x\mathcal{R}e$ ดังนั้น $xS^1 = eS^1$ นั่นคือจะมี $w \in S^1$ ซึ่งทำให้ $x = ew$ เนื่องจาก $ex = e(ew) = (ee)w = ew = x$ จะได้ว่า e เป็นเอกลักษณ์ทางซ้ายของ x

สำหรับการแสดงว่า e เป็นเอกลักษณ์ทางขวาสำหรับ L_e สามารถแสดงได้ในทำนองเดียวกัน □

บทแทรก 4.1 ให้ S เป็นกึ่งกรุป และ $a \in S$

(i) ถ้า a เป็นสมาชิกสมาชิกนิจพล แล้ว $sa = s$ สำหรับทุก $s \in L_a$

(ii) ถ้า a เป็นสมาชิกสมาชิกนิจพล แล้ว $as = s$ สำหรับทุก $s \in R_a$

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

ประพจน์ 4.5 [17] (Principle Ideal for Idempotents) ให้ $a \in S$ และ $e \in E(S)$ แล้วจะได้ว่า

(i) $S^1a \subseteq S^1e \Leftrightarrow ae = a$

(ii) $aS^1 \subseteq eS^1 \Leftrightarrow ea = a$

พิสูจน์. (i) ($\Rightarrow$) ให้ $S^1a \subseteq S^1e$ จะได้ว่า $a = te$ สำหรับบาง $t \in S^1$ ดังนั้น $ae = (te)e = t(ee) = te = a$

($\Leftarrow$) ให้ $ae = a$ จะได้ว่า $a \in S^1e$, i.e. $\{a\} \subseteq S^1e$ ดังนั้น $S^1a = S^1\{a\} \subseteq S^1(S^1e) \subseteq S^1e$

การพิสูจน์ (ii) ให้ทำเป็นแบบฝึกหัด □

บทแทรก 4.2 [17] ให้ $e \in E(S)$ จะได้ว่า

(i) ถ้า $a\mathcal{R}e$ แล้ว $ea = a$

(ii) ถ้า $a\mathcal{L}e$ แล้ว $ae = a$

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

ประพจน์ 4.6 [8] ให้ $e, f \in E(S)$ จะได้ว่า ถ้า $x \in R_e \cap L_f$ แล้วจะมี $y \in R_f \cap L_e$ โดยที่ $xy = e$ และ $yx = f$

พิสูจน์. ให้ $x \in R_e \cap L_f$ โดยบทแทรก 4.2 จะได้ว่า $x = ex = xf$ เนื่องจาก $x\mathcal{R}e$ และ $x\mathcal{L}f$ จะได้ว่า $x = eu$ และ $f = vx$ สำหรับบาง $u, v \in S^1$ ตามลำดับ ดังนั้นเราได้

$$\begin{aligned} f &= vx \\ &= v(ex) \\ &= v(xu)x \\ &= (vx)ux \\ &= fux \\ &= (fu)x \end{aligned}$$

และ

$$\begin{aligned} e &= xu \\ &= (xf)u \\ &= x(fu) \end{aligned}$$

ให้ $y = fu$ ดังนั้น $f = yx$ และ $e = xy$
เนื่องจาก $f = yx$ และ $y = fu$ จะได้ว่า $yS^1 = (fu)S^1 = f(uS^1) \subseteq fS^1$ และ $fS^1 = (yx)S^1 = y(xS^1) \subseteq yS^1$ ตามลำดับ ดังนั้น $yS^1 = fS^1$ นั่นคือ $y\mathcal{R}f$ ทำให้ได้ว่า $y \in R_f$ ในทำนองเดียวกัน เนื่องจาก $e = xy$ และ $y = fu = (vx)u = ve$ จะได้ว่า $y\mathcal{L}e$ ดังนั้น $y \in L_e$ นั่นคือเราได้ว่า $y \in R_f \cap L_e$ □

ประพจน์ 4.7 ให้ S เป็นกึ่งกรุป และ a, b เป็นสมาชิกเรกูลาร์ (regular element) ของ S จะได้ว่า

(i) $a\mathcal{L}b$ ก็ต่อเมื่อ $Sa = Sb$

(ii) $a\mathcal{R}b$ ก็ต่อเมื่อ $aS = bS$

(iii) $a\mathcal{J}b$ ก็ต่อเมื่อ $SaS = SbS$

พิสูจน์. ให้ a และ b เป็นสมาชิกเรกูลาร์ จะได้ว่า $a = axa$ และ $b = byb$ สำหรับบาง $a, b \in S$

(i) ($\Rightarrow$) ให้ $a\mathcal{L}b$ จะได้ว่า $S^1a = S^1b$ ดังนั้น $a = axa = (ax)a \in S^1a$ นั่นคือ $S^1a = Sa \cup \{a\} = Sa$ ในทำนองเดียวกันจะได้ว่า $S^1b = Sb$ แสดงว่า $Sa = Sb$

($\Leftarrow$) ให้ $Sa = Sb$ เนื่องจาก $a = axa = (ax)a \in Sa$ และ $b = byb = (by)b \in Sb$ จะได้ว่า $S^1a = Sa \cup \{a\} = Sa = Sb = Sb \cup \{b\} = S^1b$

(ii) และ (iii) สามารถพิสูจน์ได้ในทำนองเดียวกัน □

บทแทรก 4.3 ให้ S เป็นกึ่งกรุป และ a, b เป็นสมาชิกเรกูลาร์ (regular) ของ S จะได้ว่า

(i) $a\mathcal{L}b$ ก็ต่อเมื่อ $a = xb$ และ $b = ya$ สำหรับบาง $x, y \in S$

(ii) $a\mathcal{R}b$ ก็ต่อเมื่อ $a = bx$ และ $b = ay$ สำหรับบาง $x, y \in S$

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

ประพจน์ 4.8 ให้ S เป็นกึ่งกรุป จะได้ว่า

(i) S เป็นกึ่งกรุปเชิงเดียวทางซ้าย (left simple) ก็ต่อเมื่อ $a\mathcal{L}b$ สำหรับทุก $a, b \in S$

(ii) S เป็นกึ่งกรุปเชิงเดียวทางซ้าย (left simple) ก็ต่อเมื่อ $\mathcal{L} = S \times S$

(iii) S เป็นกึ่งกรุปเชิงเดียวทางซ้าย (left simple) ก็ต่อเมื่อ $\mathcal{L}_a = S$ สำหรับทุก $a \in S$

พิสูจน์. (i) $(\Rightarrow)$ ให้ S เป็นกึ่งกรุปเชิงเดียวทางซ้าย จะได้ว่า S มีไอดีลทางซ้ายเพียงตัวเดียวเท่านั้นคือ S ให้ $a, b \in S$ เนื่องจาก S^1a และ S^1b เป็นไอดีลทางซ้ายของ S ดังนั้น $S^1a = S = S^1b$ นั่นคือ $(a, b) \in \mathcal{L}$

$(\Leftarrow)$ ให้ $a\mathcal{L}b$ สำหรับทุก $a, b \in S$ จะได้ว่า $S^1a = S^1b$ ให้ I เป็นไอดีลทางซ้ายใดๆของ S จะได้ว่า $I \subseteq S$ และ $SI \subseteq I$ ให้ $x \in S$ เนื่องจาก $x \in S^1x$ และ $S^1x = S^1i$ สำหรับ $i \in I$ จะได้ว่า $x \in S^1i \subseteq S^1I = SI \cup I = I$ ดังนั้น $S \subseteq I$ นั่นคือ $S = I$ แสดงว่า S มีไอดีลทางซ้ายเพียงตัวเดียวเท่านั้นคือ S ดังนั้น S เป็นกึ่งกรุปเชิงเดียวทางซ้าย

(ii) และ (iii) เป็นผลโดยตรงจาก (i) □

ประพจน์ 4.9 ให้ S เป็นกึ่งกรุป จะได้ว่า

(i) S เป็นกึ่งกรุปเชิงเดียวทางขวา (right simple) ก็ต่อเมื่อ $a\mathcal{R}b$ สำหรับทุก $a, b \in S$

(ii) S เป็นกึ่งกรุปเชิงเดียวทางขวา (right simple) ก็ต่อเมื่อ $\mathcal{R} = S \times S$

(iii) S เป็นกึ่งกรุปเชิงเดียวทางขวา (right simple) ก็ต่อเมื่อ $\mathcal{R}_a = S$ สำหรับทุก $a \in S$

พิสูจน์. พิสูจน์ได้ในทำนองเดียวกันกับ ประพจน์ที่แล้ว □

4.2 ความสัมพันธ์ของกรีน แบบ $\mathcal{D}$ และ $\mathcal{H}$ (Green's Relations $\mathcal{D}$, $\mathcal{H}$)

ในหัวข้อนี้เราจะศึกษาความสัมพันธ์ของกรีนอีกสองชนิด ซึ่งสร้างมาจากความสัมพันธ์สมมูล $\mathcal{L}$ และ $\mathcal{R}$
นิยาม $\mathcal{L} \circ \mathcal{R}$ และ $\mathcal{R} \circ \mathcal{L}$ ดังนี้

$$\mathcal{L} \circ \mathcal{R} = \big\{(x, y) \in S \times S \mid \exists z \in S \, \big(x\mathcal{L}z \wedge z\mathcal{R}y\big)\big\}$$
$$\mathcal{R} \circ \mathcal{L} = \big\{(x, y) \in S \times S \mid \exists z \in S \, \big(x\mathcal{R}z \wedge z\mathcal{L}y\big)\big\}$$

เราพบว่า ความสัมพันธ์ $\mathcal{L}$ และ $\mathcal{R}$ สลับที่ได้ ดังประพจน์ต่อไปนี้

ประพจน์ 4.10 ความสัมพันธ์ $\mathcal{L}$ และ $\mathcal{R}$ สลับที่ได้ : $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$

พิสูจน์. ให้ $(x, y) \in \mathcal{L} \circ \mathcal{R}$ จะได้ว่ามี $z \in S$ ซึ่งทำให้ $x\mathcal{L}z$ และ $z\mathcal{R}y$ ดังนั้น โดย **ประพจน์** 4.1 จะได้ว่า มี $a, b, c, d \in S^1$ ซึ่งทำให้ $x = az$, $z = bx$ และ $z = yc$, $y = zd$ ดังนั้น $x = az = a(yc) = a(zd)c = (azd)c$ และ $azd = (az)d = xd$ เราให้ $w = azd$ จะได้ว่า $x = wc$ และ $w = xd$ ดังนั้น $x\mathcal{R}w$ เนื่องจาก $w = azd = a(zd) = ay$ และ $y = zd = (bx)d = b(az)d = b(azd) = bw$ จะได้ว่า $w\mathcal{L}y$ แสดงว่าตอนนี้เรามี $w \in S^1$ ซึ่งทำให้ $x\mathcal{R}w$ และ $w\mathcal{L}y$ ดังนั้น $(x, y) \in \mathcal{R} \circ \mathcal{L}$ นั่นคือ $\mathcal{L} \circ \mathcal{R} \subseteq \mathcal{R} \circ \mathcal{L}$ สำหรับ $\mathcal{R} \circ \mathcal{L} \subseteq \mathcal{L} \circ \mathcal{R}$ สามารถพิสูจน์ได้ในทำนองเดียวกัน $\square$

เราให้

$$\begin{aligned} \mathcal{D} &= \mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L} \\ \mathcal{H} &= \mathcal{L} \cap \mathcal{R} \end{aligned}$$

สำหรับ $(x, y) \in \mathcal{L}$ จะได้ว่า $(x, y) \in \mathcal{D}$ ทั้งนี้เพราะว่า $(x, y) \in \mathcal{L}$ และ $(y, y) \in \mathcal{R}$ นั่นคือ $\mathcal{L} \subseteq \mathcal{D}$ ในทำนองเดียวกัน สำหรับ $(x, y) \in \mathcal{R}$ จะได้ว่า $(x, y) \in \mathcal{D}$ ทั้งนี้เพราะว่า $(x, x) \in \mathcal{L}$ และ $(x, y) \in \mathcal{R}$ นั่นคือ $\mathcal{R} \subseteq \mathcal{D}$ แสดงว่า ความสัมพันธ์ $\mathcal{D}$ บรรจุ (contains) $\mathcal{L}$ และ $\mathcal{R}$ นอกจากนี้เราได้ว่า $\mathcal{D}$ เป็นความสัมพันธ์สมมูลที่เล็กที่สุดที่มี $\mathcal{L}$ และ $\mathcal{R}$ เป็นเซตย่อย ส่วน $\mathcal{H}$ เป็นความสัมพันธ์สมมูลที่ใหญ่ที่สุดบรรจุ (contained) อยู่ใน $\mathcal{L}$ และ $\mathcal{R}$

ประพจน์ 4.11 $\mathcal{D}$ เป็นความสัมพันธ์สมมูลที่เล็กที่สุดที่บรรจุ $\mathcal{L}$ และ $\mathcal{R}$

พิสูจน์. เป็นการง่ายในการพิสูจน์สมบัติการสะท้อนและสมบัติการสมมาตรของ $\mathcal{D}$ ต่อไปเราจะแสดงสมบัติการถ่ายทอด ให้ $(x, y) \in \mathcal{D}$ และ $(y, z) \in \mathcal{D}$ จะได้ว่า มี $t_1, t_2 \in S$ ซึ่งทำให้ $x\mathcal{L}t_1, t_1\mathcal{R}y$ และ $y\mathcal{L}t_2, t_2\mathcal{R}z$ เนื่องจาก $t_1\mathcal{R}y$ และ $y\mathcal{L}t_2$ จะได้ว่า $(t_1, t_2) \in \mathcal{R} \circ \mathcal{L} = D = \mathcal{L} \circ \mathcal{R}$ ดังนั้น จะมี $t_3 \in S$ ซึ่งทำให้ $t_1\mathcal{L}t_3$ และ $t_3\mathcal{R}t_2$ แสดงว่า ตอนนี้เรามี $x\mathcal{L}t_1$, $t_1\mathcal{L}t_3$ และ $t_3\mathcal{R}t_2$, $t_2\mathcal{R}z$ ดังนั้นเราได้ว่า $x\mathcal{L}t_3$ และ $t_3\mathcal{R}z$ นั่นคือ $(x, z) \in D$

สำหรับการแสดงว่า $\mathcal{D}$ เป็นความสัมพันธ์สมมูลที่เล็กที่สุดที่บรรจุ $\mathcal{L}$ และ $\mathcal{R}$ ให้ทำเป็นแบบฝึกหัด □

เราสามารถเขียนนิยามของ $\mathcal{D}$ และ $\mathcal{H}$ ได้ดังนี้

บทนิยาม 4.2 ให้ S เป็นกึ่งกรุป สำหรับ $a, b \in S$

$$
\begin{aligned}
a\mathcal{H}b &\iff a\mathcal{L}b \;\wedge\; a\mathcal{R}b \\
a\mathcal{D}b &\iff \exists z \in S \;\big(a\mathcal{L}z \;\wedge\; z\mathcal{R}b\big) \\
a\mathcal{D}b &\iff \exists z \in S \;\big(a\mathcal{R}z \;\wedge\; z\mathcal{L}b\big) \\
a\mathcal{D}b &\iff \exists z \in S \;\big(a\mathcal{L}z \;\wedge\; z\mathcal{R}b\big)
\end{aligned}
$$

ตัวอย่าง 4.5 พิจารณากึ่งกรุป S กำหนดดังตาราง

$*$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

จงหาความสัมพันธ์ $\mathcal{H}$ และ $\mathcal{D}$

วิธีทำ. จาก **ตัวอย่าง** 4.1 เรามี

$\mathcal{L} = \big\{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\big\} = S \times S$ $\mathcal{R} = \big\{(a, a), (b, b), (c, c)\big\}$

จะได้ว่า $\mathcal{H} = \mathcal{L} \cap \mathcal{R} = \big\{(a, a), (b, b), (c, c)\big\}$

$\mathcal{D} = \mathcal{L} \circ \mathcal{R} = S \times S$ □

เนื่องจาก $\mathcal{J}$ เป็นความสัมพันธ์สมมูล และ $\mathcal{L} \cup \mathcal{R} \subseteq \mathcal{J}$ ดังนั้นเราได้ว่า $\mathcal{D} \subseteq \mathcal{J}$ ความสัมพันธ์ของ $\mathcal{L}, \mathcal{R}, \mathcal{H}$ และ $\mathcal{D}$ แสดงดังใน Hasse Diagram ต่อไปนี้

$$
\begin{tikzcd}
 & \mathcal{J} \arrow[d, no head] & \\
 & \mathcal{D} \arrow[dl, no head] \arrow[dr, no head] & \\
\mathcal{L} \arrow[dr, no head] & & \mathcal{R} \arrow[dl, no head] \\
 & \mathcal{H} &
\end{tikzcd}
$$

สำหรับ $x \in S$ เราให้สัญลักษณ์ D_x และ H_x แทน **ชั้นสมมูลที่บรรจุ** x (equivalence class containing x) ภายใต้ความสัมพันธ์สมมูล $\mathcal{D}$ และ $\mathcal{H}$ ตามลำดับ

ประพจน์ 4.12 ให้ e เป็นสมาชิกนิจพลของกึ่งกรุป S ถ้า $a\mathcal{H}e$ แล้ว $ea = a = ae$

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

ประพจน์ 4.13 [17] ถ้า $e \in E(S)$ แล้ว $H_e \leq S$

พิสูจน์. ให้ $a, b \in H_e$ จะได้ว่า $a\mathcal{H}e$ และ $b\mathcal{H}e$ ดังนั้น $a\mathcal{L}e$, $a\mathcal{R}e$ และ $b\mathcal{L}e$, $b\mathcal{R}e$ เนื่องจาก $a\mathcal{L}e$ โดย **บทแทรก** 4.2 (ii) จะได้ว่า $ae = a$ เนื่องจาก $b\mathcal{R}e$ และ $\mathcal{R}$ เป็นสมภาคทางซ้าย จะได้ว่า $ab\mathcal{R}ae$ ดังนั้น $ab\mathcal{R}a$ แต่ $a\mathcal{R}e$ นั่นคือ $ab\mathcal{R}e$
ต่อไปจะแสดงว่า $ab\mathcal{L}a$ เนื่องจาก $a\mathcal{L}e$ และ $\mathcal{L}$ เป็นสมภาคทางขวา จะได้ว่า $ab\mathcal{L}eb$ เนื่องจาก $b\mathcal{R}e$ โดย **บทแทรก** 4.2 (i) จะได้ว่า $eb = b$ ดังนั้น $ab\mathcal{L}b$ แต่$b\mathcal{R}e$ นั่นคือ $ab\mathcal{R}e$ ดังนั้น ตอนนี้เรามี $ab\mathcal{R}e$ และ $ab\mathcal{R}e$, i.e. $ab \in H_e$ □

ข้อสังเกต 4.2 ให้ a เป็นสมาชิกของกึ่งกรุป S จะได้ว่า

(i) $\mathcal{D} \subseteq \mathcal{J}$

(ii) 2. $R_a \cap L_a = H_a$ สำหรับ $a \in S$

ในกึ่งกรุปใดๆ เราพบว่า L-คลาสและ R-คลาส ของแต่ละสมาชิก จะบรรจุอยู่ใน D-คลาส ของสมาชิกนั้นเสมอ ดังประพจน์ต่อไปนี้

ประพจน์ 4.14 ให้ a เป็นสมาชิกของกึ่งกรุป S แล้วจะได้ว่า

(i) $L_a \subseteq D_a$

(ii) $R_a \subseteq D_a$

พิสูจน์. (i) ให้ $x \in L_a$ จะได้ว่า $x\mathcal{L}a$ เนื่องจาก $\mathcal{R}$ มีสมบัติการสะท้อน จะได้ว่า $a\mathcal{R}a$ แสดงว่าเรามี $x\mathcal{L}a$ และ $a\mathcal{R}a$ ดังนั้น $x\mathcal{D}a$ นั่นคือ $x \in D_a$

(ii) ให้ $x \in R_a$ จะได้ว่า $x\mathcal{R}a$ เนื่องจาก $\mathcal{L}$ มีสมบัติการสะท้อน จะได้ว่า $x\mathcal{L}x$ แสดงว่าเรามี $x\mathcal{L}x$ และ $x\mathcal{R}a$ ดังนั้น $x\mathcal{D}a$ นั่นคือ $x \in D_a$ □

ประพจน์ถัดไปจะแสดงถึงเงื่อนไขที่จำเป็นและพอเพียงของสมาชิกคู่ใดๆ ที่จะมีความสัมพันธ์แบบ D ต่อกัน

ประพจน์ 4.15 [8] ให้ a และ b เป็นสมาชิกของกึ่งกรุป S แล้วจะได้ว่า

(i) $a\mathcal{D}b$ ก็ต่อเมื่อ $L_a \cap R_b \neq \emptyset$

(ii) $a\mathcal{D}b$ ก็ต่อเมื่อ $R_a \cap L_b \neq \emptyset$

พิสูจน์. (i) ($\Rightarrow$) ให้ $a\mathcal{D}b$ จะได้ว่า มี $x \in S$ ซึ่งทำให้ $a\mathcal{L}x$ และ $x\mathcal{R}b$ ดังนั้น $x \in L_a$ และ $x \in R_b$ นั่นคือ $L_a \cap R_b \neq \emptyset$

($\Leftarrow$) ให้ $t \in L_a \cap R_b$ จะได้ว่า $t \in L_a$ และ $t \in R_b$ ดังนั้น $L_t = L_a$ และ $R_t = R_b$ จาก **ประพจน์** 4.14 เรามี $L_t \subseteq D_t$ และ $R_t \subseteq D_t$ ทำให้ได้ว่า $a \in L_a = L_t \subseteq D_t$ และ $b \in R_b = R_t \subseteq D_t$ ดังนั้น $a, b \in D_t$ แสดงว่า $a\mathcal{D}b$

(ii) สามารถพิสูจน์ได้ในทำนองเดียวกันกับ (i) □

ประพจน์ 4.16 [8] ถ้า $u \in L_a \cap R_b$ แล้ว $L_a \cap R_b = H_u$

พิสูจน์. ให้ $u \in L_a \cap R_b$ จะได้ว่า $L_u = L_a$ และ $R_u = R_b$ จากข้อสังเกต 4.2 (ii) จะได้ว่า $H_u = R_u \cap L_u = R_b \cap L_a$ □

ประพจน์ 4.17 สำหรับสมาชิก x ใดๆ ของกึ่งกรุป S จะได้ว่า $D_x = \bigcup\limits_{y \in D_x} L_y = \bigcup\limits_{y \in D_x} R_y$

พิสูจน์. ให้ $w \in D_x$ เนื่องจาก $w \in L_w$ จะได้ว่า $w \in \bigcup\limits_{y \in D_x} L_y$ ดังนั้น $D_x \subseteq \bigcup\limits_{y \in D_x} L_y$

ให้ $a \in \bigcup\limits_{y \in D_x} L_y$ จะได้ว่า $a \in L_y$ สำหรับบาง $y \in D_x$ เนื่องจาก $y \in D_x$ จะได้ว่า $y\mathcal{D}x$ ดังนั้น จะมี $t \in S$ ซึ่งทำให้ $y\mathcal{L}t$ และ $t\mathcal{R}x$ แสดงว่า เรามี $a \in L_y$ และ $y\mathcal{L}t$ ดังนั้นโดยสมบัติการถ่ายทอดจะได้ว่า $a\mathcal{L}t$ ตอนนี้เรามี $a\mathcal{L}t$ และ $t\mathcal{R}x$ ดังนั้น $a\mathcal{D}x$ นั่น

คือ $a \in D_x$ แสดงว่า $\bigcup\limits_{y \in D_x} L_y \subseteq D_x$

ต่อไปจะแสดงว่า $D_x = \bigcup\limits_{y \in D_x} R_y$ ให้ $w \in D_x$ เนื่องจาก $w \in R_w$ จะได้ว่า $w \in \bigcup\limits_{y \in D_x} R_y$ ดังนั้น $D_x \subseteq \bigcup\limits_{y \in D_x} R_y$

ให้ $a \in \bigcup\limits_{y \in D_x} R_y$ จะได้ว่า $a \in R_y$ สำหรับบาง $y \in D_x$ ดังนั้น $a\mathcal{R}y$ และ $x \in D_y$ ทำให้ได้ว่า $y\mathcal{R}a$ และมี $m \in S$ ซึ่งทำให้ $x\mathcal{L}m$ และ $m\mathcal{R}y$ เนื่องจาก $m\mathcal{R}y$ และ $y\mathcal{R}a$ จะได้ว่า $m\mathcal{R}a$ แสดงว่าตอนนี้เรามี $x\mathcal{L}m$ และ $m\mathcal{R}a$ ดังนั้น $x\mathcal{D}a$ นั่นคือ $a \in D_x$ □

บทนิยาม 4.3 กึ่งกรุป S จะเรียกว่าเป็น **พีริโอดิก**(periodic) ถ้าทุกๆสมาชิกของ S มีอันดับ(order) จำกัด

ในกึ่งกรุปโดยทั่วไป $\mathcal{D} \subseteq \mathcal{J}$ แต่ในกึ่งกรุปพีริโอดิก เราพบว่าความสัมพันธ์ทั้งสองแบบนี้เป็นเซตเดียวกัน ดังทฤษฎีบทต่อไปนี้

ประพจน์ 4.18 [9] ถ้ากึ่งกรุป S เป็นพีริโอดิก แล้ว $\mathcal{D} = \mathcal{J}$

พิสูจน์. เห็นได้ชัดว่า $\mathcal{D} \subseteq \mathcal{J}$ ต่อไปจะแสดงว่า $\mathcal{J} \subseteq \mathcal{D}$
ให้ $(a, b) \in \mathcal{J}$ จะได้ว่ามี $x, y, u, v \in S^1$ ซึ่งทำให้ $xay = b$ และ $ubv = a$ ดังนั้นเราได้ว่า

$$\begin{aligned}
a &= ubv \\
&= u(xay)v \\
&= (ux)a(yv) \\
&= (ux)^2 a(yv)^2 \\
&= (ux)^3 a(yv)^3 = \dots
\end{aligned}$$

และ

$$\begin{aligned} b &= xay \\ &= x(ubv)y \\ &= (xu)b(vy) \\ &= (xu)^2b(vy)^2 \\ &= (xu)^3b(vy)^3 = \dots \end{aligned}$$

เนื่องจาก S เป็นพีริโอดิก โดย **บทตั้ง** 1.1 จะได้ว่าจะมี $m \in \mathbb{N}$ ซึ่งทำให้ $(ux)^m$ เป็นสมาชิกนิจพล ดังนั้น เราให้ $c = xa$ จะได้ว่า

$$\begin{aligned} a &= (ux)^m a(yv)^m \\ &= (ux)^m(ux)^m a(yv)^m \\ &= (ux)^m a \\ &= (ux)^{m-1}uc \end{aligned}$$

นั่นคือ $a\mathcal{L}c$

ในทำนองเดียวกัน จะมี $n \in \mathbb{N}$ ซึ่งทำให้ $(vy)^n$ เป็นสมาชิกนิจพล ดังนั้น

$$\begin{aligned} c &= xa = x(ux)^{n+1}a(yv)^{n+1} \\ &= (xu)^{n+1}xay(vy)^n v = (xu)^{n+1}b(vy)^{2n}v \\ &= (xu)^{n+1}b(vy)^{n+1}(vy)^{n-1}v \\ &= b(vy)^{n-1}v \end{aligned}$$

นั่นคือ $c\mathcal{R}b$ □

ประพจน์ 4.19 [9] ถ้า a เป็นสมาชิกปกติ(regular) ของกึ่งกรุป S แล้ว ทุกๆสมาชิกของ D_a เป็นสมาชิกปกติ

พิสูจน์. พิสูจน์เป็นแบบฝึกหัด □

ประพจน์ 4.20 [8] แต่ละ H-คลาส บรรจุสมาชิกนิจพล(idempotent) อย่างมากหนึ่งสมาชิก

พิสูจน์. ให้ e และ e' เป็นสมาชิกนิจพลที่บรรจุใน H_a จะได้ว่า $e\mathcal{H}a$ และ $e'\mathcal{H}a$ ดังนั้น $e\mathcal{L}a, e\mathcal{R}a$ และ $e'\mathcal{L}a, e'\mathcal{R}a$ นั่นคือ $e\mathcal{L}e'$ และ $e\mathcal{R}e'$ โดย **บทแทรก** 4.1 จะได้ว่า $ee' = e$ และ $ee' = e'$ ดังนั้น $e = e'$ $\square$

บทนิยาม 4.4 ให้ S เป็นกึ่งกรุป และ $s \in S$ นิยาม $\rho_s : S^1 \to S^1$ ดังนี้

$$\text{สำหรับ } x \in S, \quad \rho_s(x) = sx$$

เรียก ρ_s ว่าเป็น **การเลื่อนขนานทางซ้าย** (left translation)

บทตั้ง 4.1 [8], [9] (Green's Lemma)
ให้ x , y เป็นสมาชิกของกึ่งกรุป S และ $x\mathcal{L}y$ โดยที่ $sx = y$ และ $s'y = x$ สำหรับบาง $s, s' \in S^1$ และให้ $\rho_s = \phi$, $\rho_{s'} = \chi$ แล้วจะได้ว่า

(i) $\rho_{s|_{R_x}} : R_x \to R_y$ และ $\rho_{s'|_{R_y}} : R_y \to R_x$ เป็นชนิดหนึ่งต่อหนึ่งและทั่วถึง

(ii) $\rho_{s'|_{R_y}} = (\rho_{s|_{R_x}})^{-1}$ เป็นฟังก์ชันอินเวอร์สของ ρ จำกัดบน R_x

(iii) $\rho_{s|_{R_x}}$ ตรึง (fixes) L- คราส นั่นคือ $z\mathcal{L}\rho_{s|_{R_x}}(z)$ สำหรับทุก $z \in R_x$

(iv) $\rho_{s|_{R_x}}$ รักษาการคงสภาพ (preserves) ของ H-คราส นั่นคือ สำหรับแต่ละ $u, v \in R_x$, $u\mathcal{H}v \Longleftrightarrow \rho_{s|_{R_x}}(u)\mathcal{H}\rho_{s|_{R_x}}(v)$

พิสูจน์. (i) อันดับแรกจะแสดงว่า $\rho_{s|_{R_x}} : R_x \to R_y$
ให้ $z \in R_x$ จะได้ว่า $z\mathcal{R}x$ นั่นคือ $zS^1 = xS^1$ ดังนั้นเราได้ $szS^1 = sxS^1 = yS^1$ แสดงว่า $sz\mathcal{R}y$ นั่นคือ $\rho_{s|_{Rx}}(z) = sz \in R_y$

ต่อไปจะแสดงว่า $\rho_{s|_{R_x}}$ เป็น 1-1

<u>Claim</u>: $z = s'sz$ สำหรับทุก $z \in R_x$

พิจารณา

$$\begin{aligned} z &= xu \\ &= (s'y)u \\ &= s'(sx)u \\ &= s's(xu) \\ &= s'sz \end{aligned}$$

ให้ $z_1, z_2 \in R_x$ โดยที่ $\rho_{s|_{Rx}}(z_1) = \rho_{s|_{Rx}}(z_2)$ จะได้ว่า $sz_1 = sz_2$ ดังนั้น $z_1 = s'sz_1 = sz_2 = z_2$ นั่นคือ $\rho_{s|_{Rx}}$ เป็นฟังก์ชันชนิด 1-1

ให้ $w \in R_y$ จะได้ว่า $wS^1 = yS^1$ ดังนั้น จะมี $t \in S^1$ ซึ่งทำให้ $w = yt$ ดังนั้น $w = (sx)t = s(xt) = \rho_{s|_{R_x}}(xt)$ นั่นคือ $\rho_{s|_{Rx}}$ เป็นฟังก์ชันชนิดทั่วถึง
สำหรับการแสดงว่า $\rho_{s'|_{R_y}} : R_y \to R_x$ เป็นชนิดหนึ่งต่อหนึ่งและทั่วถึง สามารถพิสูจน์ได้ในทำนองเดียวกัน

(ii) ให้ $z \in R_x$ เนื่องจาก $(\rho_{s|_{R_y}} \circ \rho_{s|_{R_x}})(z) = s'sz = z$ และ $(\rho_{s|_{R_x}} \circ \rho_{s'|_{R_y}})(z) = ss'z = z$ จะได้ว่า $\rho_{s|_{R_y}} \circ \rho_{s|_{R_x}}$ และ $\rho_{s|_{R_x}} \circ \rho_{s'|_{R_y}}$ เป็นฟังก์ชันเอกลักษณ์บน R_x และ R_y ตามลำดับ

(iii) ให้ $z \in R_x$ โดย <u>Claim</u> จะได้ว่า $s'sz = z$ ดังนั้น $z \in S^1sz$ ทำให้ได้ว่า $S^1z \subseteq S^1(S^1sz) = (S^1S^1)sz \subseteq S^1sz$ เห็นได้ชัดว่า $S^1sz \subseteq S^1z$ ดังนั้น $S^1z = S^1sz$ นั่นคือ $z\mathcal{L}sz$ ดังนั้น $z\mathcal{L}\rho_{s|_{R_x}}(z)$

(iv) ให้ $u, v \in R_x$ และ $u\mathcal{H}v$ จะได้ว่า $u\mathcal{L}v$ และ $u\mathcal{R}v$ เนื่องจาก $u, v \in R_x$ และ $u\mathcal{L}v$ โดย (iii) จะได้ว่า $u\mathcal{L}\rho_{s|_{R_x}}(u)$ และ $v\mathcal{L}\rho_{s|_{R_x}}(v)$ นั่นคือ $u\mathcal{L}su$ และ $v\mathcal{L}sv$ ดังนั้นโดยสมบัติการถ่ายทอดของ $\mathcal{L}$ จะได้ว่า $su\mathcal{L}sv$ ....(*)
เนื่องจาก $u\mathcal{R}v$ และ $\mathcal{R}$ เป็นสมภาคทางซ้าย จะได้ว่า $su\mathcal{R}sv$.....(**)
จาก (*) และ (**) จะได้ว่า $su\mathcal{H}sv$ นั่นคือ $\rho_{s|_{R_x}}(u)\mathcal{H}\rho_{s|_{R_x}}(v)$ □

ในปี ค.ศ. 1956 Miller และ Clifford ได้สร้างทฤษฎีบทที่เรียกว่า **Location Theorem** ดังต่อไปนี้

ทฤษฎีบท 4.1 [8] (Location Theorem)
ให้ x และ y เป็นสมาชิกของกึ่งกรุป S จะได้ว่า

$xy \in R_x \cap L_y \iff R_y \cap L_x$ บรรจุสมาชิกนิจพลเพียงหนึ่งตัวเท่านั้น

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

4.3 แบบฝึกหัด(Exercise)

1) พิจารณากึ่งกรุป S ต่อไปนี้

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

จงหา
ก. $\mathcal{L}, \mathcal{R}, \mathcal{J}, \mathcal{H}$ และ $\mathcal{D}$
ข. L_x, R_x, J_x, H_x และ D_x สำหรับ $x \in S$

2) กำหนด $B = \{1, 2, 3, 4\}$ พิจารณากึ่งกรุป $(P(B); \cup)$ จงหา
ก. $\mathcal{L}, \mathcal{R}, \mathcal{J}, \mathcal{H}$ และ $\mathcal{D}$
ข. L_x, R_x, J_x, H_x และ D_x สำหรับ $x \in S$

3) พิจารณากึ่งกรุป $(\mathbf{R}; +)$ จงหา
ก. $\mathcal{L}, \mathcal{R}, \mathcal{J}, \mathcal{H}$ และ $\mathcal{D}$
ข. L_x, R_x, J_x, H_x และ D_x สำหรับ $x \in S$

จงพิสูจน์หรือยกตัวอย่างค้านข้อความต่อไปนี้

4) $\mathcal{L} \subseteq \mathcal{J}$ และ $\mathcal{R} \subseteq \mathcal{J}$

5) ให้ a และ b เป็นสมาชิกของกึ่งกรุป จะได้ว่า $a\mathcal{R}b$ ก็ต่อเมื่อ $a = bx$ และ $b = ay$ สำหรับบาง $x, y \in S^1$

6) $a\mathcal{D}b$ ก็ต่อเมื่อ $R_a \cap L_b \neq \emptyset$

7) ความสัมพันธ์ R เป็น สมภาคทางซ้าย (left congruence)

8) ถ้า $a\mathcal{L}b$ และ a, b เป็นสมาชิกนิจพล (idempotent) แล้ว $Sa = Sb$

9) ถ้า S เป็นกึ่งกรุปศูนย์ทางขวา (right zero semigroup) แล้ว $\mathcal{R} = S \times S$

10) ถ้า $\mathcal{L} = S \times S$ แล้ว S เป็นกึ่งกรุปเชิงเดียว (simple semigroup)

11) ถ้า S เป็นกึ่งกรุปเชิงเดียวทางขวา (right simple semigroup) แล้ว $\mathcal{R} = S \times S$

บทที่ 5

กึ่งกรุปผกผัน (Inverse Semigroups)

ในปีช่วง ปี พ.ศ. 2495 วี วากเนอร์ (V. Wagner) จาก สหภาพโซเวียต ได้นำเสนอแนวคิดเกี่ยวกับ กึ่งกรุปผกผันเป็นคนแรก และในปี พ.ศ.2497 จี เพรสตัน (G. Preston) จากประเทศอังกฤษได้นำเสนอแนวคิดเกี่ยวกับกึ่งกรุปเช่นเดียวกันโดยไม่ได้อิงอาศัย แนวคิดของ วากเนอร์ ในช่วงแรกนั้น วากเนอร์ได้เรียกกึ่งกรุปเหล่านี้ว่า **กรุปวางนัยทั่วไป** (generalized groups) แนวคิดของกึ่งกรุปผกผันนี้เป็นผลมาจากการศึกษากึ่งกรุปของการแปลงย่อยชนิดหนึ่งต่อหนึ่ง (partial one-one tranformation) ของเซต

5.1 กึ่งกรุปปกติ(Regular Semigroups)

ก่อนอื่นเราจะกล่าวถึงกึ่งกรุปปกติ (regular semigroup) และสมบัติบางประการของกึ่งกรุปชนิดนี้ ทั้งนี้เพราะว่าการศึกษาเรื่องกึ่งกรุปผกผันมีความเกี่ยวข้องสัมพันธ์กับกึ่งกรุปกติอยู่ค่อนข้างมาก เราได้กล่าวถึงกึ่งกรุปปกติ มาบ้างแล้วในบทที่ 1 กึ่งกรุปปกติคือกึ่งกรุปที่ทุกๆสมาชิกเป็นสมาชิกปกติ(regular element), i.e. สำหรับสมาชิก x ใดๆ จะมีสมาชิก y ซึ่งทำให้ $x = xyx$

ประพจน์ 5.1 ให้ a, x เป็นสมาชิกของกึ่งกรุป S ถ้า $a = axa$ จะได้ว่า ax, xa เป็นสมาชิกนิจพล (idempotent)

พิสูจน์. เนื่องจาก $(ax)(ax) = (axa)x = ax$ และ $(xa)(xa) = x(axa) = xa$ ดังนั้น ax, xa เป็นสมาชิกนิจพล □

ประพจน์ 5.2 [8] ให้ x เป็นสมาชิกของกึ่งกรุป S จะได้ว่าข้อความต่อไปนี้สมมูลกัน

(i) x เป็นสมาชิกปกติ

(ii) $x\mathcal{R}e$ สำหรับบาง $e \in E(S)$

(iii) $x\mathcal{L}f$ สำหรับบาง $f \in E(S)$

พิสูจน์. (i) $\Rightarrow$ (ii) : ให้ x เป็นสมาชิกปกติ จะได้ว่า $x = xyx$ สำหรับบาง $x \in S$ ดังนั้น โดยประพจน์ 5.1 จะได้ว่า $e = xy$ และ $f = yx$ เป็นสมาชิกนิจพล

นอกจากนี้เราได้ว่า

$$xS^1 = (xyx)S^1 = xy(xS^1) \subseteq xyS^1 \text{ และ } xyS^1 = x(yS^1) \subseteq xS^1$$

นั่นคือ $xS^1 = xyS^1$ แสดงว่า $x\mathcal{R}xy$

(i) $\Rightarrow$ (iii) : ในทำนองเดียวกันเราสามารถแสดงได้ว่า $x\mathcal{L}yx$

(ii) $\Rightarrow$ (i) : เนื่องจาก $x\mathcal{R}xy$ และ xy เป็นนิจพล โดยบทแทรก 4.2 จะได้ว่า $x = (xy)x = xyx$ ดังนั้น x เป็นสมาชิกปกติ

(iii) $\Rightarrow$ (i) : สามารถพิสูจน์ได้ในทำนองเดียวกัน □

บทแทรก 5.1 ให้ x เป็นสมาชิกของกึ่งกรุป S ถ้า $x = xyx$ สำหรับบาง $y \in S$ แล้ว $x\mathcal{R}xy$ และ $x\mathcal{L}yx$

พิสูจน์. เป็นผลโดยตรงจากประพจน์ 5.2 □

สำหรับ $e, f \in E(S)$ โดยประพจน์ 4.6 จะได้ว่าสำหรับ $x \in R_e \cap L_f$ จะมี $y \in R_f \cap L_e$ โดยที่ $xy = e$ และ $yx = f$

	$L_x = L_f$		L_e	
$R_x = R_e$	x		$e = xy$	
R_f	$f = yx$		y	

บทนิยาม 5.1 ให้ S เป็นกึ่งกรุป คลาส D_x จะกล่าวว่าเป็นปกติ(regular) ถ้าทุกๆสมาชิกของคลาสนี้เป็นสมาชิกปกติของ S

บทตั้ง 5.1 [8] ถ้า x เป็นสมาชิกปกติของกึ่งกรุป S แล้ว D_x เป็นปกติ

พิสูจน์. ให้ x เป็นสมาชิกปกติของกึ่งกรุป S โดยประพจน์ 5.2 จะได้ว่ามี $e, f \in E(S)$ โดยที่ $x\mathcal{R}e$ และ $x\mathcal{L}f$

เนื่องจาก $x\mathcal{L}x$ และ $x\mathcal{R}e$ จะได้ว่า $x \in L_x \cap R_e$ นั่นคือ $L_x \cap R_e \neq \emptyset$ โดยประพจน์ 4.15 จะได้ว่า $x\mathcal{D}e$ ทำให้ได้ว่า $D_x = D_e$

ให้ $z \in D_x = D_e$ จะได้ว่า $z\mathcal{D}x$ ดังนั้นจะมี $u \in S$ ซึ่งทำให้ $z\mathcal{L}u$ และ $u\mathcal{R}x$ เนื่องจาก $u\mathcal{L}u$ และ $u\mathcal{R}x$ จะได้ $u\mathcal{D}x$ ดังนั้น $u \in D_x = D_e$

เนื่องจาก $e\mathcal{R}x$ และ $x\mathcal{R}u$ โดยสมบัติการถ่ายทอดของ $\mathcal{R}$ จะได้ $e\mathcal{R}u$ ดังนั้นเรามี $u \in D_x$ โดยที่ $e\mathcal{R}u$ และ $u\mathcal{L}z$ ดังนั้นจะได้ว่ามี $r, s, s' \in S$ ซึ่งทำให้

$$e = ur,\ u = sz \text{ และ } z = s'u$$

เนื่องจาก $e \in E(S)$ และ $u\mathcal{R}e$ โดยบทแทรก 4.1 จะได้ว่า $x = eu$

ดังนั้นเราได้ว่า

$$\begin{aligned} z = s'u = s'(eu) &= s'e(sz) \\ &= s'(ur)sz \\ &= (s'u)rsz \\ &= z(rs)z \end{aligned}$$

นั่นคือ z เป็นสมาชิกปกติ □

บทตั้ง 5.2 [8] ถ้า D-คลาส D เป็นปกติ แล้วแต่ละ $L_x \subseteq D$ และแต่ละ $R_x \subseteq D$ บรรจุสมาชิกนิจพล

พิสูจน์. ให้ $x \in D$ โดย บทตั้ง 5.1 จะได้ว่า x เป็นสมาชิกปกติของ S ดังนั้นจะมี $y \in S$ ซึ่ง $x = xyx$ ทำให้ได้ว่า $x\mathcal{L}yx$ และ $x\mathcal{R}xy$ โดยที่ xy, yx เป็นสมาชิกนิจพล นั่นคือ $xy \in R_x$ และ $yx \in L_x$ □

ทฤษฎีบท 5.1 [8] D-คลาส D เป็นปกติ ก็ต่อเมื่อ D บรรจุสมาชิกนิจพล

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

5.2 ตัวผกผันของสมาชิกในกึ่งกรุป (Inverse of Element)

บทนิยาม 5.2 ให้ S เป็นกึ่งกรุป และ $a, x \in S$ เราจะกล่าวว่า x เป็น **ตัวผกผัน** (inverse element) ของ a ถ้า

$$a = axa \quad \text{และ} \quad x = xax$$

ตัวอย่าง 5.1 พิจารณากึ่งกรุป S ต่อไปนี้

$*$	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

จงหาตัวผกผันของ a, b และ c

วิธีทำ. พิจารณาตัวผกผันของ a
เนื่องจาก $a = aaa$ จะได้ว่า a เป็นตัวผกผันของ a

เนื่องจาก $a = a(ba) = aba$ และ $b = b(ab) = bab$ จะได้ว่า b เป็นตัวผกผันของ a เนื่องจาก $a = a(ca) = aca$ และ $c = c(ac) = cac$ จะได้ว่า c เป็นตัวผกผันของ a

ในทำนองเดียวกัน จะได้ว่า a, b, c เป็นตัวผกผันของ b และ a, b, c เป็นตัวผกผันของ c $\square$

ตัวอย่าง 5.2 พิจารณากึ่งกรุป $(\mathbb{Z}_2; +)$ จงหาตัวผกผันของ $\overline{0}, \overline{1}$ ถ้ามี

วิธีทำ. พิจารณาหาตัวผกผันของ $\overline{0}$

เนื่องจาก $\overline{0} = \overline{0} + \overline{0} + \overline{0}$ เพราะฉะนั้น $\overline{0}$ เป็นตัวผกผันของ $\overline{0}$

$\overline{1}$ ไม่เป็นตัวผกผันของ $\overline{0}$ ทั้งนี้เพราะว่า $\overline{0} \neq \overline{0} + \overline{1} + \overline{0} = \overline{1}$

ต่อไปพิจารณาหาตัวผกผันของ $\overline{1}$

เนื่องจาก $\overline{1} = \overline{1} + \overline{1} + \overline{1}$ เพราะฉะนั้น $\overline{1}$ เป็นตัวผกผันของ $\overline{1}$

เนื่องจาก $\overline{1} \neq \overline{1} + \overline{0} + \overline{1} = \overline{0}$ จะได้ว่า $\overline{0}$ ไม่เป็นตัวผกผันของ $\overline{1}$ $\square$

ตัวอย่าง 5.3 พิจารณากึ่งกรุป $(K_0; +)$ จงหาตัวผกผันของแต่ละสมาชิกใน K_0

วิธีทำ. เนื่องจาก $c_0 = c_0 + c_0 + c_0$ จะได้ว่า c_0 เป็นอิเวอร์สของ c_0

ให้ $f \in K_0 \setminus \{c_0\}$ จะได้ว่า สำหรับทุก $g \in K_0$

$$f + g + f = c_0 \neq f$$

ดังนั้น f ไม่มีตัวผกผัน $\square$

สำหรับสมาชิก a ของกึ่งกรุป S ให้สัญลักษณ์ $V(a)$ แทนเซตของตัวผกผันทั้งหมดของ a นั่นคือ

$$V(a) = \{x \in S \mid a = axa \wedge x = xax\}$$

ข้อสังเกต 5.1 (i) ถ้า a เป็นสมาชิกนิจพล (idempotent) แล้ว a เป็นตัวผกผันของตัวมันเอง

(ii) ถ้า a เป็นสมาชิกนิจพล (idempotent) แล้ว $|V(a)| \geq 1$

(iii) ถ้า x เป็นตัวผกผันของ a แล้ว a เป็นตัวผกผันของ x

(iv) ถ้า a มีตัวผกผัน แล้ว a เป็นสมาชิกปกติ (regular)

เราพบว่าบทกลับของข้อสังเกต (iv) ข้างต้นเป็นจริง ดังประพจน์ต่อไปนี้

ประพจน์ 5.3 ถ้า x เป็นสมาชิกเรกูลาร์ (regular) แล้ว x มีตัวผกผัน

วิธีทำ. ให้ x เป็นสมาชิกเรกูลาร์ จะได้ว่า มี $y \in S$ ซึ่งทำให้ $x = xyx$
ดังนั้น จะได้

$$\begin{aligned} x &= xyx \\ &= (xyx)yx \\ &= x(yxy)x \end{aligned}$$

และ

$$\begin{aligned} (yxy)x(yxy) &= y(xyx)yxy \\ &= y(x)yxy \\ &= y(xyx)y \\ &= yxy \end{aligned}$$

ดังนั้น yxy เป็นตัวผกผันของ x □

ข้อสังเกต 5.2 (i) ถ้า S เป็นกึ่งกรุปปรกติ (regular semigroup) จะได้ว่าทุกสมาชิกของ S มีตัวผกผัน

(ii) ถ้า S เป็นกึ่งกรุปปรกติ (regular semigroup) จะได้ว่า $E(S) \neq \emptyset$

ประพจน์ 5.4 [8] ให้ P เป็นกึ่งกรุป, S เป็นกึ่งกรุปปรกติ(regular semigroup) และ $\alpha : S \to P$ เป็นอีพิมอร์ฟิสซึม แล้วจะได้ว่า
ถ้า $e \in E(P)$ แล้ว $\alpha^{-1}(e) \cap E(S) \neq \emptyset$, i.e. จะมีสมาชิกนิจพล $f \in E(S)$ โดยที่ $\alpha(f) = e$

พิสูจน์. เนื่องจาก α เป็นฟังก์ชันทั่วถึงบน P จะได้ว่ามี $x \in S$ โดยที่ $\alpha(x) = e$ ให้ y เป็นตัวผกผันของ $x^2 \in S$ จะได้ว่า $x^2 = x^2yx^2$ และ $y = yx^2y$

ให้ $f = xyx$ จะได้ว่า

$$\begin{aligned} f^2 &= (xyx)(xyx) \\ &= x(yx^2y)x \\ &= xyx \end{aligned}$$

ดังนั้น $f \in E(S)$

นอกจากนี้เราได้ว่า

$$\begin{aligned} \alpha(f) = \alpha(xyx) &= \alpha(x)\alpha(y)\alpha(x) \\ &= (\alpha(x)\alpha(x))\alpha(y)(\alpha(x)\alpha(x)) \\ &= \alpha(x^2)\alpha(y)\alpha(x^2) \\ &= \alpha(x^2yx^2) \\ &= \alpha(x^2) = \alpha(x)\alpha(x) \\ &= \alpha(x) = e \end{aligned}$$

□

ทฤษฎีบท 5.2 ให้ ρ เป็นสมภาคของกึ่งกรุปปรกติ S โดยที่ S เป็นเซตจำกัด แล้วจะได้ว่า

$$[x]_\rho \in E(S/\rho) \Longrightarrow \exists e \in E(S) : [x]_\rho = [e]_\rho$$

พิสูจน์. ให้ $[x]_\rho \in E(S/\rho)$ จะได้ว่า $[x]_\rho = [x]_\rho[x]_\rho = [xx]_\rho = [x^2]_\rho$ ดังนั้น $x^2 \in [x]_\rho$ นั่นคือ $x^2 \rho\, x$ เนื่องจาก ρ เป็นสมภาค จะได้ว่า $x^3 \rho\, x^2$ ดังนั้น $x^3 \in [x]_\rho$ ในทำนองเดียวกันสามารถแสดงได้ว่า $x^n \in [x]_\rho$ สำหรับ $n \geq 1$ นั่นคือ $\langle x \rangle = \{x^n | n \geq 1\} \subseteq [x]_\rho$ โดยบทตั้ง 1.1 จะได้ว่า $\langle x \rangle$ บรรจุสมาชิกนิจพล ให้เป็น e ดังนั้น $e \in \langle x \rangle \subseteq [x]_\rho$ นั่นคือ $[e]_\rho = [x]_\rho$ □

ทฤษฎีบท 5.3 ถ้า $\alpha : S \to P$ เป็นสาทิสสัณฐานของกึ่งกรุป โดยที่ S เป็นกึ่งกรุปปรกติ แล้วจะได้ว่า $\alpha(S)$ เป็นกึ่งกรุปปรกติ

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

5.3 กึ่งกรุปผกผัน (Inverse Semigroups)

บทนิยาม 5.3 จะเรียกกึ่งกรุป S ว่า **กึ่งกรุปผกผัน** (inverse Semigroup) ถ้าแต่ละสมาชิกของ S มีตัวผกผัน เพียงตัวเดียวเท่านั้น

สำหรับสมาชิก x ในกึ่งกรุปผกผัน S เราใช้สัญลักษณ์ x^{-1} แทน ตัวผกผันของ x

ตัวอย่าง 5.4 จาก **ตัวอย่าง** 5.1, 5.2 และ 5.3 จะได้ว่า $(S;*)$ และ $(K_0;+)$ ไม่เป็นกึ่งกรุปผกผัน แต่ $(Z_2;+)$ เป็นกึ่งกรุปผกผัน

ตัวอย่าง 5.5 จงพิจารณาว่า $(N_3;min)$ เป็นกึ่งกรุปผกผันหรือไม่

วิธีทำ. ให้ $a \in N_3$ พิจารณาหาตัวผกผันของ a

$$
\begin{aligned}
V(a) &= \{x \in N_3 \mid a = axa \text{ และ } x = xax\} \\
&= \{x \in N_3 \mid a = a\ min\ x\ min\ a \text{ และ } x = x\ min\ a\ min\ x\} \\
&= \{x \in N_3 \mid a = min\ \{x, a\} \text{ และ } x = min\ \{a, x\}\} \\
&= \{x \in N_3 \mid x \geq a \text{ และ } x \leq a\} \\
&= \{x \in N_3 \mid x = a\} \\
&= \{a\}
\end{aligned}
$$

แสดงว่าแต่ละสมาชิกใน N_3 มีตัวผกผัน และมีเพียงตัวเดียวเท่านั้น นั่นคือ $(N_3;min)$ เป็นกึ่งกรุปผกผัน □

ตัวอย่าง 5.6 ให้ $X = \{a, b\}$ จงพิจารณาว่า $\big(P(X);\cup\big)$ เป็นกึ่งกรุปผกผันหรือไม่

วิธีทำ. ให้ทำเป็นแบบฝึกหัด □

ข้อสังเกต 5.3 ถ้า S เป็นกึ่งกรุปผกผัน แล้ว S เป็นกึ่งกรุปปกติ
แต่บทกลับของข้อความนี้ไม่จริง ดังตัวอย่างต่อไปนี้

ตัวอย่าง 5.7 กำหนดกึ่งกรุป S ดังตาราง

$*$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

เราได้ว่า S เป็นกึ่งกรุปปกติ และมี $V(a) = V(b) = V(c) = \{a, b, c\}$ ดังนั้น S ไม่เป็นกึ่งกรุปผกผัน

ประพจน์ 5.5 ให้ S เป็นกึ่งกรุป และ $a \in S$ ถ้า $S^1a = S^1w$ สำหรับบาง $w \in E(S)$ แล้ว $aw = a$

พิสูจน์. ให้ $S^1a = S^1w$ สำหรับบาง $w \in E(S)$ เนื่องจาก $a \in \{a\} \cup Sa = S^1a = S^1w$ จะได้ว่า $a = sw$ สำหรับบาง $s \in S^1$ ดังนั้นจะได้ว่า $aw = (sw)w = s(ww) = sw = a$ □

ประพจน์ 5.6 ถ้า S เป็นเซมิแลททิซ แล้ว S เป็นกึ่งกรุปผกผัน

พิสูจน์. ให้ $x \in S$ จะได้ว่า $x^2 = x$ ดังนั้น x เป็นสมาชิกนิจพล แสดงว่า x เป็นตัวผกผันของตัวมันเอง ให้ $x' \in S$ เป็นตัวผกผันของ x จะได้ว่า $xx'x = x$ และ $x'xx' = x'$

ดังนั้นเราได้

$$
\begin{aligned}
x = xx'x = x(x'x) & \\
&= x(xx') && \text{; สมาชิกของแลททิซสลับที่ได้} \\
&= (xx)x' \\
&= xx' && \text{; x เป็นสมาชิกนิจพล} \\
&= x(x'x') \\
&= (xx')x' \\
&= x'xx' = x'
\end{aligned}
$$

แสดงว่าแต่ละสมาชิกในกึ่งกรุป S มีตัวผกผัน และมีเพียงตัวเดียวเท่านั้น นั่นคือ S เป็นกึ่งกรุปผกผัน □

สำหรับประพจน์ถัดไปจะกล่าวถึงความเกี่ยวข้องของสมาชิกเรกูลาร์ (regular element) กับสมาชิกสมาชิกนิจพล (idempotent) โดยอาศัยแนวคิดของไอดีลมุขสำคัญ (principal ideal)

ประพจน์ 5.7 ให้ S เป็นกึ่งกรุป และ $a \in S$ จะได้ว่า a เป็นสมาชิกปกติ (regular element) ก็ต่อเมื่อ $S^1a = S^1w$ สำหรับบาง $w \in E(S)$

พิสูจน์. ($\Rightarrow$) ให้ a เป็นเรกูลาร์ จะได้ว่า $a = axa$ สำหรับบาง $x \in S$ โดย **ประพจน์** 5.1 จะได้ว่า $xa \in E(S)$ ให้ $w = ax$ ต่อไปจะแสดงว่า $S^1a = S^1w$

เนื่องจาก $S^1x \subseteq S^1$ จะได้ว่า $S^1w = S^1(xa) = (S^1x)a \subseteq S^1a$
ในทำนองเดียวกัน เนื่องจาก $S^1a \subseteq S^1$ จะได้ว่า $S^1a = S^1(axa) = (S^1a)(xa) \subseteq S^1(xa) = S^1w$ ดังนั้น $S^1a = S^1w$

($\Leftarrow$) ให้ $S^1a = S^1w$ สำหรับบาง $w \in E(S)$ โดย **ประพจน์** 5.5 จะได้ว่า $a = aw$ เนื่องจาก $w \in S^1w = S^1a$ จะได้ว่า $w = sa$ สำหรับบาง $s \in S^1 = S \cup \{1\}$

ถ้า $s \in \{1\}$ จะได้ว่า $s = 1$ ดังนั้น $a = aw = a(sa) = a(1a) = aa$ แสดงว่า a เป็นไอเด็มโพเทนท์ นั่นคือ a เป็นสมาชิกเรกูลาร์

ถ้า $s \in S$ จะได้ว่า $a = aw = asa$ ดังนั้น a เป็นสมาชิกเรกูลาร์ □

ในทำนองเดียวกันกับประพจน์ที่ผ่านมา เราสามารถพิสูจน์ได้ว่า :

ประพจน์ 5.8 ให้ S เป็นกึ่งกรุป และ $a \in S$ จะได้ว่า a เป็นสมาชิกปกติ (regular) ก็ต่อเมื่อ $aS^1 = wS^1$ สำหรับบาง $w \in E(S)$

พิสูจน์. ให้ทำเป็นแบบฝึกหัด □

ยิ่งไปกว่านั้น เราได้ว่า

ประพจน์ 5.9 ให้ S เป็นกึ่งกรุป และ $a \in S$ จะได้ว่า ถ้า a เป็นสมาชิกปกติ (regular) แล้ว $S^1aS^1 = S^1wS^1$ สำหรับบาง $w \in E(S)$

พิสูจน์. เป็นผลโดยตรงจาก **ประพจน์** 5.7 หรือ **ประพจน์** 5.8 □

ประพจน์ 5.10 ให้ S เป็นกึ่งกรุป และ $e, f \in E(S)$ ถ้า $ef, fe \in E(S)$ แล้ว ef และ fe เป็นตัวผกผันซึ่งกันและกัน

พิสูจน์. ให้ ef และ fe เป็นสมาชิกนิจพล จะได้ว่า

$$\begin{aligned} ef &= (ef)(ef) \\ &= (e(ff))((ee)f) \\ &= ef(fe)ef \\ \text{และ} \qquad fe &= (fe)(fe) \\ &= f(ee)(ff)e \\ &= (fe)(ef)fe \end{aligned}$$

ดังนั้น ef เป็นตัวผกผันของ fe และ fe เป็นตัวผกผันของ ef □

ประพจน์ 5.11 ให้ S เป็นกึ่งกรุปผกผัน และ $x \in S$ จะได้ว่า xx^{-1} และ $x^{-1}x$ เป็นสมาชิกนิจพล (idempotent)

พิสูจน์. พิสูจน์เป็นแบบฝึกหัด □

ประพจน์ 5.12 ให้ S เป็นกึ่งกรุปผกผัน ถ้า e และ f เป็นสมาชิกนิจพล แล้ว $f(ef)^{-1}e$ เป็นสมาชิกนิจพลและเป็นตัวผกผันของ ef

พิสูจน์. เนื่องจาก

$$\begin{aligned}\big(f(ef)^{-1}e\big)\big(f(ef)^{-1}e\big) &= f\big((ef)^{-1}ef(ef)^{-1}\big)e \\ &= f(ef)^{-1}e\end{aligned}$$

จะได้ว่า $f(ef)^{-1}e$ เป็นสมาชิกนิจพล
ต่อไปจะแสดงว่า $f(ef)^{-1}e$ เป็นตัวผกผันของ ef
เนื่องจาก

$$\begin{aligned}ef\big(f(ef)^{-1}e\big)ef &= e(ff)(ef)^{-1}(ee)f \\ &= ef(ef)^{-1}ef \\ &= ef\end{aligned}$$

และ

$$\begin{aligned}\big(f(ef)^{-1}e\big)ef\big(f(ef)^{-1}e\big) &= f(ef)^{-1}(ee)(ff)(ef)^{-1}e \\ &= f(ef)^{-1}ef(ef)^{-1}e \\ &= f\big((ef)^{-1}ef(ef)^{-1}\big)e \\ &= f(ef)^{-1}e\end{aligned}$$

จะได้ว่า $f(ef)^{-1}e$ เป็นตัวผกผันของ ef □

ประพจน์ 5.13 ให้ S เป็นกึ่งกรุปผกผัน ถ้า e และ f เป็นสมาชิกนิจพล แล้ว ef เป็นสมาชิกนิจพล

พิสูจน์. ให้ e และ f เป็นสมาชิกนิจพล โดย **ประพจน์** 5.12 จะได้ว่า $f(ef)^{-1}e$ เป็นสมาชิกนิจพลและเป็นตัวผกผันของ ef ดังนั้น $(ef)^{-1} = f(ef)^{-1}e$ นั่นคือ $(ef)^{-1}$ เป็นสมาชิกนิจพล ทำให้ได้ว่า $(ef)^{-1}$ เป็นตัวผกผันของ $(ef)^{-1}$ แต่เนื่องจาก ef เป็นตัวผกผันของ $(ef)^{-1}$ และแต่ละสมาชิกมีตัวผกผันเพียงตัวเดียวเท่านั้น ทำให้ได้ว่า $ef = (ef)^{-1}$ ดังนั้น ef เป็นสมาชิกนิจพล □

จากทฤษฎีบทข้างบนทำให้ได้ว่า ในกึ่งกรุปผกผันใดๆ เซตของสมาชิกนิจพล(idempotent)ทั้งหมด จะเป็นกึ่งกรุปย่อยของอินเวอร์กึ่งกรุปนั้น ดังประพจน์ต่อไปนี้

ประพจน์ 5.14 ถ้า S เป็นกึ่งกรุปผกผัน แล้ว $E(S) \leq S$

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

เซตของสมาชิกนิจพลในกึ่งกรุปผกผันนอกจากจะมีคุณสมบัติปิด แล้วยังมีสมบัติการสลับที่ด้วย ดังทฤษฎีบทต่อไปนี้

ประพจน์ 5.15 ถ้า S เป็นกึ่งกรุปผกผัน แล้ว สมาชิกนิจพล (idempotent) ของ S สลับที่ได้

พิสูจน์. ให้ e และ f เป็นสมาชิกนิจพล โดย **ประพจน์** 5.12 จะได้ว่า ef และ fe เป็นสมาชิกนิจพล และ โดย **ประพจน์** 5.10 จะได้ว่า ef และ fe เป็นตัวผกผันซึ่งกันและกัน ดังนั้น $(ef)^{-1} = fe$ เนื่องจาก ef เป็นสมาชิกนิจพล ดังนั้น ef เป็นตัวผกผันของตัวมันเอง แสดงว่า $ef = (ef)^{-1} = fe$ □

ประพจน์ 5.16 ให้ S เป็นกึ่งกรุปผกผัน แล้วจะได้ว่า $E(S)$ เป็นเซมิแลททิซ

พิสูจน์. เป็นผลโดยตรงจากประพจน์ 5.14 และประพจน์ 5.15 □

ตัวผกผันในกึ่งกรุปจะมีพฤติกรรมคล้ายกับตัวผกผันในกรุป นั่นคือ :

ทฤษฎีบท 5.4 ให้ S เป็นกึ่งกรุปผกผัน จะได้ว่า $(a^{-1})^{-1} = a$ และ $(ab)^{-1} = b^{-1}a^{-1}$ สำหรับทุก $a, b \in S$

พิสูจน์. เนื่องจาก a^{-1} เป็นตัวผกผันของ a จะได้ว่า a เป็นตัวผกผันของ a^{-1} ด้วย ดังนั้น $\left(a^{-1}\right)^{-1} = a$
ต่อไปจะแสดงว่า $(ab)^{-1} = b^{-1}a^{-1}$
พิจารณา

$$\begin{aligned}
ab(b^{-1}a^{-1})ab &= a(bb^{-1})(a^{-1}a)b \\
&= a(a^{-1}a)(bb^{-1})b \qquad \text{; สมาชิกนิจพลสลับที่ได้} \\
&= (aa^{-1}a)(bb^{-1}b) \\
&= ab \\
\text{และ} \quad b^{-1}a^{-1}(ab)b^{-1}a^{-1} &= b(a^{-1}a)(bb^{-1})a^{-1} \\
&= b^{-1}(bb^{-1})(a^{-1}a)a^{-1} \\
&= (b^{-1}bb^{-1})(a^{-1}aa^{-1}) \\
&= b^{-1}a^{-1}
\end{aligned}$$

ดังนั้น $b^{-1}a^{-1}$ เป็นตัวผกผันของ ab นั่นคือ $(ab)^{-1} = b^{-1}a^{-1}$ □

บทแทรก 5.2 ให้ $a_1, a_2, \ldots, a_n$ เป็นสมาชิกของกึ่งกรุปผกผัน S แล้วจะได้ว่า

$$\left(a_1 a_2 \ldots a_n\right)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1}$$

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

ประพจน์ 5.17 ถ้า S เป็นกึ่งกรุปผกผัน และ a เป็นสมาชิกนิจพล จะได้ว่า $a = aa^{-1} = a^{-1}a$

พิสูจน์. ให้ a เป็น ไอเด็มโพเทนท์ จะได้ว่า a เป็นตัวผกผันของตัวมันเอง นั่นคือ $a^{-1} = a$ ดังนั้นเราได้ว่า $aa^{-1} = aa = a$ และ $a^{-1}a = aa = a$ □

ประพจน์ 5.18 ถ้า S เป็นกึ่งกรุปผกผัน และ e เป็นสมาชิกนิจพล แล้ว xex^{-1} และ $x^{-1}ex$ เป็นสมาชิกนิจพล สำหรับทุก $x \in S$

พิสูจน์. เนื่องจาก

$$\begin{aligned}
(xex^{-1})(xex^{-1}) &= xe(x^{-1}x)ex^{-1} \\
&= x(x^{-1}x)eex^{-1} && \text{; สมาชิกนิจพลสลับที่ได้} \\
&= (xx^{-1}x)(ee)x^{-1} \\
&= xex^{-1}
\end{aligned}$$

จะได้ว่า xex^{-1} เป็นสมาชิกนิจพล

สำหรับการพิสูจน์ว่า $x^{-1}ex$ เป็นสมาชิกนิจพล สามารถแสดงได้ในทำนองเดียวกัน □

บทแทรก 5.3 ให้ S เป็นกึ่งกรุปผกผัน แล้วจะได้ว่า $x^{-1}E(S)x \subseteq E(S)$ สำหรับทุก $x \in S$

พิสูจน์. เป็นผลโดยตรงจากประพจน์ 5.18 □

ทฤษฎีบท 5.5 [9] ให้ S เป็นกึ่งกรุปผกผัน และ $a, b \in S$ จะได้ว่าข้อความต่อไปนี้สมมูลกัน

(i) $aa^{-1} = ab^{-1}$

(ii) $aa^{-1} = ba^{-1}$

(iii) $a^{-1}a = a^{-1}b$

(iv) $a^{-1}a = b^{-1}a$

(v) $ab^{-1}a = a$

(vi) $a^{-1}ba^{-1} = a^{-1}$

พิสูจน์. (i) $\Rightarrow$ (ii)

ให้ $aa^{-1} = ab^{-1}$ จะได้ว่า $\left(aa^{-1}\right)^{-1} = \left(ab^{-1}\right)^{-1}$ ดังนั้นโดย **ทฤษฎีบท** 5.4 จะได้ $(a^{-1})^{-1}a^{-1} = (b^{-1})^{-1}a^{-1}$ นั่นคือ $aa^{-1} = ba^{-1}$

(ii) $\Rightarrow$ (i)

ให้ $aa^{-1} = ba^{-1}$ จะได้ว่า $\left(aa^{-1}\right)^{-1} = \left(ba^{-1}\right)^{-1}$ ดังนั้นโดย **ทฤษฎีบท** 5.4 จะได้ $(a^{-1})^{-1}a = (a^{-1})^{-1}b^{-1}$ นั่นคือ $aa^{-1} = ab^{-1}$

(iii) $\Rightarrow$ (iv)

ให้ $a^{-1}a = a^{-1}b$ จะได้ว่า $(a^{-1}a)^{-1} = (a^{-1}b)^{-1}$ ดังนั้น $a^{-1}(a^{-1})^{-1} = b^{-1}(a^{-1})^{-1}$ แสดงว่า $a^{-1}a = b^{-1}a$

(iv) $\Rightarrow$ (iii)

ให้ $a^{-1}a = b^{-1}a$ จะได้ว่า $(a^{-1}a)^{-1} = (b^{-1}a)^{-1}$ โดย **ทฤษฎีบท** 5.4 จะได้ว่า $a^{-1}(a^{-1})^{-1} = a^{-1}(b^{-1})^{-1}$ นั่นคือ $a^{-1}a = a^{-1}b$

(v) $\Rightarrow$ (vi)

ให้ $ab^{-1}a = a$ จะได้ว่า

$$\begin{aligned} a^{-1} &= (a(b^{-1}a))^{-1} \\ &= (b^{-1}a)^{-1}a^{-1} \\ &= (a^{-1}(b^{-1})^{-1})a^{-1} \\ &= a^{-1}ba^{-1} \end{aligned}$$

(vi) $\Rightarrow$ (v)

ให้ $a^{-1}ba^{-1} = a^{-1}$ จะได้ว่า

$$\begin{aligned} a &= (a^{-1})^{-1} \\ &= (a^{-1}ba^{-1})^{-1} \\ &= (a^{-1}(ba^{-1}))^{-1} \\ &= (ba^{-1})^{-1}(a^{-1})^{-1} \\ &= ((a^{-1})^{-1}b^{-1})a \\ &= ab^{-1}a \end{aligned}$$

(ii) $\Rightarrow$ (iii)

ให้ $aa^{-1} = ba^{-1}$ เนื่องจาก S เป็นกึ่งกรุปผกผัน โดย **ประพจน์** 2.1 จะได้ว่า $a^{-1}a$

เป็นสมาชิกนิจพล ยิ่งไปกว่านั้น เราได้ว่า $a^{-1}b$ เป็นสมาชิกนิจพลทั้งนี้เพราะว่า $(a^{-1}b)(a^{-1}b) = a^{-1}(ba^{-1})b = a^{-1}(aa^{-1})b = (a^{-1}aa^{-1})b = a^{-1}b$

ดังนั้น

$$\begin{aligned} a^{-1}b &= (a^{-1}aa^{-1})b \\ &= (a^{-1}a)(a^{-1}b) \\ &= (a^{-1}b)(a^{-1}a) && \text{; สมาชิกนิจพลสลับที่ได้} \\ &= a^{-1}(ba^{-1})a \\ &= a^{-1}(aa^{-1})a \\ &= (a^{-1}aa^{-1})a \\ &= a^{-1}a \end{aligned}$$

(iv) $\Rightarrow$ (v)

ให้ $a^{-1}a = b^{-1}a$ จะได้ว่า

$$\begin{aligned} ab^{-1}a &= a(b^{-1}a) \\ &= a(a^{-1}a) \\ &= aa^{-1}a = a \end{aligned}$$

(v) $\Rightarrow$ (i)

ให้ $ab^{-1}a = a$ เนื่องจาก S เป็นกึ่งกรุปผกผัน โดย **ประพจน์** 2.1 จะได้ว่า aa^{-1} เป็นสมาชิกนิจพล ยิ่งไปกว่านั้น เราได้ว่า ab^{-1} เป็นสมาชิกนิจพลทั้งนี้เพราะว่า $(ab^{-1})(ab^{-1}) = (ab^{-1}a)b^{-1} = ab^{-1}$

ดังนั้น

$$\begin{aligned} ab^{-1} &= (aa^{-1}a)b^{-1} \\ &= (aa^{-1})(ab^{-1}) \\ &= (ab^{-1})(aa^{-1}) && \text{; โดย\textbf{ประพจน์} 5.15 สมาชิกนิจพลสลับที่ได้} \\ &= (ab^{-1}a)a^{-1} \\ &= aa^{-1} \end{aligned}$$

□

ในกึ่งกรุปผกผันนั้น ชั้นสมมูลใดๆของความสัมพันธ์ของกรีนแบบ $\mathcal{L}$ จะบรรจุสมาชิกนิจพลเสมอ

ทฤษฎีบท 5.6 ให้ S เป็นกึ่งกรุปผกผัน และ $x \in S$ จะได้ว่า L_x บรรจุสมาชิกนิจพล (idempotent) เพียงตัวเดียวเท่านั้น และอยู่ในรูป $x^{-1}x$

พิสูจน์. ให้ $x \in S$ โดย **ประพจน์** 5.11 จะได้ว่า $x^{-1}x$ เป็นสมาชิกนิจพล ต่อไปจะแสดงว่า $x^{-1}x \in L_x$ นั่นคือต้องแสดงว่า $S^1(x^{-1}x) = S^1x$

เนื่องจาก $S^1x^{-1} \subseteq S^1$ จะได้ว่า $S^1(x^{-1}x) = (S^1x^{-1})x \subseteq S^1x$
นอกจากนี้จะได้ว่า $S^1x = S^1(xx^{-1}x) = (S^1x)(x^{-1}x) \subseteq S^1(x^{-1}x$ ทั้งนี้เพราะว่า $S^1x \subseteq S^1$ ดังนั้น $S^1(x^{-1}x) = S^1x$ ต่อไปจะแสดงว่า L_x บรรจุสมาชิกนิจพล
เพียงตัวเดียวเท่านั้น ให้ $e, f \in L_x$ และ e, f เป็นสมาชิกนิจพล โดย **ประพจน์** 5.15 จะได้ว่าไอเด็มโพเทนท์สลับที่ได้ นั่นคือ $ef = fe$ เนื่องจาก $S^1e = S^1f$ โดย **ประพจน์** 5.5 จะได้ว่า $ef = e$ และ $fe = f$ ดังนั้น $e = f$ □

ในทำนองเดียวกัน ชั้นสมมูล R_x ของความสัมพันธ์กรีนแบบ $\mathcal{R}$ จะบรรจุสมาชิก
นิจพลเสมอ และอยู่ในรูป xx^{-1}

ทฤษฎีบท 5.7 ให้ S เป็นกึ่งกรุปผกผัน และ $x \in S$ จะได้ว่า R_x บรรจุสมาชิกนิจพล ในรูปของ xx^{-1}

พิสูจน์. พิสูจน์เป็นแบบฝึกหัด □

ทฤษฎีบทถัดไปจะกล่าวถึงเงื่อนไขพอเพียงของกึ่งกรุปใดๆที่จะเป็นกึ่งกรุปผกผัน เงื่อนไข
ดังกล่าวก็คือ ทุกๆสมาชิกของกึ่งกรุปนั้นต้องเป็นสมาชิกเรกูลาร์ และสมาชิก
นิจพลต้องมีสมบัติสลับที่

ทฤษฎีบท 5.8 ให้ S เป็นกึ่งกรุปปกติ ถ้าสมาชิกนิจพลใน S สลับที่ได้ แล้ว S เป็นกึ่งกรุปผกผัน

พิสูจน์. ให้สมาชิกนิจพลใน S สลับที่ได้ และให้ $x \in S$ เนื่องจาก S เป็นเรกูลาร์กึ่งกรุป และโดย **ประพจน์** 5.3 จะได้ว่า x มีตัวผกผัน สมมติให้ u, v เป็นตัวผกผันของ x จะได้ว่า $x = xux, u = uxu$ และ $x = xvx, v = vxv$

พิจารณา

$$\begin{aligned}
u &= uxu \\
&= u(xvx)u \\
&= (ux)(vx)u \\
&= (vx)(ux)u\ ; \qquad vx, ux \text{ เป็นไอเด็มโพเทนท์} \\
&= vxu(x)u \\
&= vxu(xvx)u) \\
&= v(xux)vxu \\
&= vxvxu \\
&= v(xv)(xu) \\
&= v(xu)(xv)\ ; \qquad vx, ux \text{ เป็นไอเด็มโพเทนท์} \\
&= v(xux)v \\
&= vxv \\
&= v
\end{aligned}$$

ดังนั้น $u = v$ นั่นคือ x มีตัวผกผันตัวเดียวเท่านั้น แสดงว่า S เป็นกึ่งกรุปผกผัน □

ทฤษฎีบทต่อไปนี้จะให้ลักษณะของกึ่งกรุปผกผัน

ทฤษฎีบท 5.9 [8] ให้ S เป็นกึ่งกรุป จะได้ว่าข้อความต่อไปนี้สมมูลกัน

(i) S เป็นกึ่งกรุปผกผัน

(ii) S เป็นกึ่งกรุปปกติและสมาชิกนิจพลสลับที่ได้

(iii) แต่ละ L-คลาส และ R-คลาสบรรจุสมาชิกนิจพลหนึ่งสมาชิก

พิสูจน์. (i) $\rightarrow$ (ii) : ให้ S เป็นกึ่งกรุปผกผัน จะได้ว่า S เป็นกึ่งกรุปปกติ และโดยประพจน์ 5.15 จะได้ว่าสมาชิกนิจพลของ S สลับที่ได้

(ii) $\rightarrow$ (iii) : เนื่องจาก S เป็นกึ่งกรุปปกติ ดังนั้นโดย บทตั้ง 5.1 จะได้ว่าทุกๆ D-คลาสเป็นปกติ และโดยบทตั้ง 5.2 จะได้ว่าแต่ละ L-คลาส และ R-คลาสบรรจุสมาชิกนิจพล ต่อไปจะแสดงว่า แต่ละ L-คลาสบรรจุสมาชิกนิจพลเพียงตัวเดียวเท่านั้น ให้

$f \in L_e$ โดยที่ $f, e \in E(S)$ จะได้ว่ามี $x, y \in S^1$ ซึ่งทำให้ $e = xf$ และ $f = ye$
นั่นคือ

$$\begin{aligned} e = xf &= x(ff) \\ &= (xf)f \\ &= ef \\ &= fe && \text{; สมาชิกนิจพลสลับที่ได้} \\ &= (ye)e \\ &= y(ee) \\ &= ye = f \end{aligned}$$

(iii) $\rightarrow$ (i) : โดยประพจน์ 4.14 $L_x \subseteq D_x$ และ $R_x \subseteq D_x$ สำหรับทุก $x \in S$ ดังนั้น แต่ละ D-คลาส บรรจุสมาชิกนิจพล โดยทฤษฎีบท 5.1 จะได้ว่า แต่ละ D-คลาส เป็นปกติ ทำให้เราได้ว่าแต่ละสมาชิกใน D-คลาส เป็นสมาชิกปกติ นั่นคือแต่ละสมาชิก $x \in S$ จะมีตัวผกผัน (โดยประพจน์ 5.3) สมมุติ x มีตัวผกผัน 2 ตัว ให้เป็น y และ z โดยประพจน์ 5.1 จะได้ว่า $yx, zx \in E(S)$ และโดยประพจน์ 5.2 จะได้ว่า $yx\mathcal{L}x$ และ $zx\mathcal{L}x$ แสดงว่า $yx, zx \in L_x \cap E(S)$ โดยสมมุติฐานของการพิสูจน์จะได้ว่า $yx = zx$

โดยการพิสูจน์ในทำนองเดียวกันโดยใช้ความสัมพันธ์ $\mathcal{R}$ จะได้ $xy = xz$
ดังนั้น

$$\begin{aligned} y &= yxy \\ &= y(xy) \\ &= y(xz) \\ &= (yx)z \\ &= (zx)z = z \end{aligned}$$

□

ทฤษฎีบทถัดไปจะกล่าวถึงความสัมพันธ์ของสมาชิกในกึ่งกรุปผกผันที่มีความสัมพันธ์แบบกรีนชนิด $\mathcal{L}$ และ $\mathcal{R}$ ต่อกัน

ทฤษฎีบท 5.10 ให้ S เป็นกึ่งกรุปผกผัน $x, y \in S$ และ $e, f \in E(S)$ แล้วจะได้ว่า

(i) $x \, \mathcal{L} \, y$ ก็ต่อเมื่อ $x^{-1}x = y^{-1}y$

(ii) $x \mathcal{R} y$ ก็ต่อเมื่อ $xx^{-1} = yy^{-1}$

พิสูจน์. (i)

($\Rightarrow$) ให้ $x \mathcal{L} y$ จะได้ว่า $x \in L_y$ โดย **ทฤษฎีบท** 5.6 จะได้ว่า $x^{-1}x \in L_x$ และ $y^{-1}y \in L_y$ ดังนั้นเราได้ว่า $x\mathcal{L}y^{-1}y$ โดยสมบัติการถ่ายทอดจะได้ว่า $x^{-1}x \mathcal{L} y^{-1}y$ แสดงว่า $x^{-1}x$ และ $y^{-1}y$ อยู่ใน L-คลาส เดียวกัน โดย **ทฤษฎีบท** 5.6 จะได้ว่า $x^{-1}x = y^{-1}y$

($\Leftarrow$) เห็นได้ชัด

(ii) สามารถพิสูจน์ได้ในทำนองเดียวกันกับ (i) □

ประพจน์ 5.19 ให้ S เป็นกึ่งกรุปผกผัน และ $e, f \in E(S)$ แล้วจะได้ว่า

$e \mathcal{D} f$ ก็ต่อเมื่อ $e = zz^{-1}$, $f = z^{-1}z$ สำหรับบาง $z \in S$

พิสูจน์. ($\Rightarrow$) ให้ $e \mathcal{D} f$ จะได้ว่า มี $z \in S$ ซึ่งทำให้ $e\mathcal{R}z$ และ $z\mathcal{L}f$ โดย **ทฤษฎีบท** 5.10 จะได้ว่า $ee^{-1} = zz^{-1}$ และ $z^{-1}z = f^{-1}f$ ดังนั้น $e = zz^{-1}$ และ $f = z^{-1}z$

($\Leftarrow$) ให้ $e = zz^{-1}$, $f = z^{-1}z$ สำหรับบาง $z \in S$ เนื่องจาก $e = e^{-1}$ และ $f = f^{-1}$ จะได้ว่า $ee^{-1} = e = zz^{-1}$ และ $z^{-1}z = f = f^{-1}f$ ดังนั้น โดย **ทฤษฎีบท** 5.10 จะได้ว่า $e\mathcal{R}z$ และ $z\mathcal{L}f$ นั่นคือ $e\mathcal{D}f$ □

ทฤษฎีบท 5.11 ทุก ๆ กรุป จะเป็นกึ่งกรุปผกผัน

พิสูจน์. ให้ G เป็นกรุป (จะแสดงว่า G เป็นกึ่งกรุปผกผัน)

ให้ $a \in G$ เนื่องจาก G เป็นกรุปจะได้ว่ามี $a^{-1} \in G$ ซึ่ง $a^{-1}a = e = aa^{-1}$ โดยที่ e เป็นเอกลักษณ์ใน G

พิจารณา

$$\begin{aligned} a^{-1}a &= e \\ a(a^{-1}a) &= ae \\ aa^{-1}a &= a \end{aligned}$$

และ

$$\begin{aligned} aa^{-1} &= e \\ a^{-1}(aa^{-1}) &= a^{-1}e \\ a^{-1}aa^{-1} &= a^{-1} \end{aligned}$$

แสดงว่า เรามี $a = aa^{-1}a$ และ $a^{-1} = a^{-1}aa^{-1}$ นั่นคือ a^{-1} เป็นตัวผกผัน(ในกึ่งกรุป)ของ a

ต่อไปจะแสดงว่า a มีตัวผกผันเพียงตัวเดียวเท่านั้น สมมติ ให้ a' เป็นตัวผกผันของ a ในกึ่งกรุป G จะได้ว่า $a = aa'a$ และ $a' = a'aa'$
พิจารณา

$$\begin{aligned} aa'a &= aa^{-1}a \\ a^{-1}(aa'a) &= a^{-1}(aa^{-1}a) \\ (a^{-1}a)a'a &= (a^{-1}a)a^{-1}a \\ (e)a'a &= (e)a^{-1}a \\ a'a &= a^{-1}a && ;e \text{ เป็นเอกลักษณ์} \\ (a'a)a^{-1} &= (a^{-1}a)a^{-1} \\ a'(aa^{-1}) &= a^{-1}aa^{-1} \\ a'e &= a^{-1} && ;e \text{ เป็นเอกลักษณ์} \\ a' &= a^{-1} \end{aligned}$$

ดังนั้น G เป็นกึ่งกรุปผกผัน □

ทฤษฎีบท 5.12 ให้ S เป็นกึ่งกรุปผกผัน จะได้ว่า
S เป็นกรุป ก็ต่อเมื่อ S บรรจุสมาชิกนิจพล (idempotent) เพียงตัวเดียวเท่านั้น

พิสูจน์. ($\Rightarrow$) ให้ S เป็นกรุป จะได้ว่า S จะบรรจุเอกลักษณ์ให้เป็น e ดังนั้น $ee = e$ นั่นคือ e เป็นสมาชิกนิจพล

ต่อไปจะแสดงว่า S บรรจุสมาชิกนิจพลเพียงตัวเดียวเท่านั้น สมมติให้ a เป็นสมาชิกนิจพลของ S จะได้ว่า $aa = a$
พิจารณา

$$\begin{aligned} ea &= e(aa) \\ &= aa && ;e \text{ เป็นเอกลักษณ์} \end{aligned}$$

จะได้ว่า

$$\begin{aligned} (ea)a^{-1} &= (aa)a^{-1} \\ e(aa^{-1}) &= a(aa^{-1}) \\ ee &= ae && ;a \text{ และ } a^{-1} \text{ เป็นตัวผกผันซึ่งกันและกันในกรุป } S \\ e &= a && ;e \text{ เป็นเอกลักษณ์} \end{aligned}$$

นั่นคือ S บรรจุสมาชิกนิจพลเพียงตัวเดียวเท่านั้น

($\Leftarrow$) ให้กึ่งกรุปผกผัน S บรรจุสมาชิกนิจพลเพียงตัวเดียวเท่านั้น ให้เป็น e เนื่องจาก

S เป็นกึ่งกรุป จะได้ว่า S มีสมบัติปิดและเปลี่ยนกลุ่ม ต่อไปจะแสดงว่า S มีเอกลักษณ์

ให้ $x \in S$ และ x^{-1} เป็นตัวผกผันของ x ในกึ่งกรุป S โดย **ประพจน์** 5.11 จะได้ว่า xx^{-1} และ $x^{-1}x$ เป็นสมาชิกนิจพล เนื่องจากกึ่งกรุป S มีไอเด็มโพเทนท์เพียงตัวเดียวคือ e ดังนั้นจะได้ว่า $xx^{-1} = e = x^{-1}x$ เนื่องจาก $ex = (xx^{-1})x = xx^{-1}x = x$ และ $xe = x(x^{-1}x) = xx^{-1}x = x$ จะได้ว่า e เป็นสมาชิกเอกลักษณ์ใน S ยิ่งไปกว่านั้นเราได้ว่า x^{-1} เป็นตัวผกผัน(ในกรุป)ของ x ทั้งนี้เพราะว่า $xx^{-1} = e = x^{-1}x$ ต่อไปจะแสดงว่า x มีตัวผกผันเพียงตัวเดียวเท่านั้น สมมติให้ x' เป็นตัวผกผันของ x จะได้ว่า

$$\begin{aligned} x'x &= e = xx' \\ x^{-1}(x'x) &= x^{-1}(xx') \\ x^{-1}e &= (x^{-1}x)x' \\ x^{-1} &= ex' = x' \end{aligned}$$

ดังนั้น S เป็นกรุป □

ทฤษฎีบท 5.13 ให้ $\phi : S \to T$ เป็นสาทิสสัณฐานของกึ่งกรุป และ S, T เป็นกึ่งกรุปผกผัน จะได้ว่า

(i) $\phi(a^{-1}) = (\phi(a))^{-1}$ สำหรับ ทุก $a \in S$

(ii) ถ้า $e \in E(S)$ แล้ว $\phi(e) \in E(T)$

(iii) $\phi(S)$ เป็นกึ่งกรุปย่อยของ T และ เป็นกึ่งกรุปผกผัน

พิสูจน์. (i) ให้ $a \in S$ จะได้ว่า a มีตัวผกผัน ให้เป็น a^{-1} ดังนั้น $a = aa^{-1}a$ และ $a^{-1} = a^{-1}aa^{-1}$ เราได้ว่า

$$\begin{aligned} \phi(a) &= \phi(aa^{-1}a) \\ &= \phi(a)\phi(a^{-1})\phi(a) \end{aligned}$$

และ

$$\begin{aligned} \phi(a^{-1}) &= \phi(a^{-1}aa^{-1}) \\ &= \phi(a^{-1})\phi(a)\phi(a^{-1}) \end{aligned}$$

ดังนั้น $\phi(a^{-1})$ เป็นตัวผกผันของ $\phi(a)$ เนื่องจาก T เป็นกึ่งกรุปผกผัน แสดงว่า $\phi(a)$ มีตัวผกผันเพียงตัวเดียวเท่านั้น ดังนั้น $(\phi(a))^{-1} = \phi(a^{-1})$

(ii) ให้ $e \in E(S)$ จะได้ว่า $\phi(e) = \phi(ee) = \phi(e)\phi(e)$ นั่นคือ $\phi(e) \in E(T)$

(iii) ก่อนอื่นจะแสดงว่า $\phi(S)$ เป็นกึ่งกรุปย่อยของ T เนื่องจาก $\phi(S) = \{\phi(s)|s \in S\}$ จะได้ว่า $\emptyset \neq \phi(S) \subseteq T$ ให้ $a, b \in \phi(S)$ จะได้ว่า มี $x, y \in S$ ซึ่ง $\phi(x) = a$ และ $\phi(y) = b$ ดังนั้น $ab = \phi(x)\phi(y) = \phi(xy)$ โดยสมบัติปิดของกึ่งกรุป S จะได้ว่า $xy \in S$ ดังนั้น $ab = \phi(xy) \in \phi(S)$ นั่นคือ $\phi(S)$ เป็นกึ่งกรุปย่อยของ T

ต่อไปจะแสดงว่า $\phi(S)$ เป็นอินเวอรส์กึ่งกรุป ให้ $a \in \phi(S)$ จะได้ว่า มี $x \in S$ ซึ่ง $\phi(x) = a$ เนื่องจาก $x \in S$ และ S เป็นกึ่งกรุปผกผัน จะได้ว่ามี $x^{-1} \in S$ โดยที่ $x = xx^{-1}x$ และ $x^{-1} = x^{-1}xx^{-1}$

ดังนั้น เราได้ว่า

$$\begin{aligned} a &= \phi(x) \\ &= \phi(xx^{-1}x) \\ &= \phi(x)\phi(x^{-1})\phi(x) \\ &= \phi(x)(\phi(x))^{-1}\phi(x) \\ &= aa^{-1}a \end{aligned}$$

และ

$$\begin{aligned} a^{-1} &= (\phi(x))^{-1} \\ &= \phi(x^{-1}) \\ &= \phi(x^{-1}xx^{-1}) \\ &= \phi(x^{-1})\phi(x)\phi(x^{-1}) \\ &= (\phi(x))^{-1}\phi(x)(\phi(x))^{-1} \\ &= a^{-1}aa^{-1} \end{aligned}$$

เนื่องจาก $x^{-1} \in S$ และ $a^{-1} = \phi(x^{-1})$ จะได้ว่า $a^{-1} \in \phi(S)$ ดังนั้น a^{-1} เป็นตัวผกผันของ a ใน $\phi(S)$ $\square$

ประพจน์ 5.20 ให้ S เป็นกึ่งกรุปผกผัน ถ้า ρ เป็นสมภาคของ S แล้ว จะได้ว่า S/ρ เป็นกึ่งกรุปผกผัน

พิสูจน์. เป็นการเพียงพอที่จะแสดงว่า แต่ละสมาชิกใน S/ρ มีตัวผกผันเพียงตัวเดียวเท่านั้น ให้ $[x]_\rho \in S/\rho$ จะได้ว่า $[x^{-1}]_\rho \in S/\rho$ นอกจากนี้เราได้ว่า

$$\begin{aligned} [x]_\rho[x^{-1}]_\rho[x]_\rho &= [xx^{-1}x]_\rho \\ &= [x]_\rho \end{aligned}$$

และ

$$\begin{aligned} [x^{-1}]_\rho[x]_\rho[x^{-1}]_\rho &= [x^{-1}xx^{-1}]_\rho \\ &= [x^{-1}]_\rho \end{aligned}$$

แสดงว่า $[x^{-1}]_\rho$ เป็นตัวผกผันของ $[x]_\rho$ □

ประพจน์ 5.21 ให้ S เป็นกึ่งกรุปผกผัน และ ρ เป็นสมภาคของ S แล้ว จะได้ว่า สำหรับ $x, y \in S$

$$x \;\rho\; y \quad \text{ก็ต่อเมื่อ} \quad x^{-1} \;\rho\; y^{-1}$$

พิสูจน์. ให้พิสูจน์เป็นแบบฝึกหัด □

5.4 แบบฝึกหัด (Exercise)

1) ให้ $S = \{$ก, ข, ค, ง, จ$\}$ กำหนดการกระทำทวิภาค $*$ บน S ดังนี้

$$x * y = \text{ก} \qquad \text{สำหรับทุก } x, y \in S$$

จงแสดงว่า $(S; *)$ เป็นกึ่งกรุปผกผันหรือไม่

2) พิจารณากึ่งกรุป S ต่อไปนี้

$*$	a	b	c	d
a	a	b	c	d
b	b	c	a	d
c	c	a	b	d
d	d	d	d	d

จงหา $V(x)$ เมื่อ $x \in S$

3) กำหนดกึ่งกรุป $(N; +)$ เมื่อ $N = \{0, 1, 2, 3, \ldots\}$ และ $+$ เป็นการบวกปกติ (usual addition) จงหา (แสดงวิธีหาด้วย)
ก. ตัวผกผันทั้งหมดของ 0
ข. ตัวผกผันทั้งหมดของ 5

4) กำหนดกึ่งกรุป $(N_5; +)$ เมื่อ $N_5 = \{0, 1, 2, \ldots, 5\}$ จงหา (แสดงวิธีหาด้วย)
ก. ตัวผกผันทั้งหมดของ 0
ข. ตัวผกผันทั้งหมดของ 5

5) กำหนดกึ่งกรุป $(N_4; min)$ จงหา
ก. $\left(((2^{-1})^{-1})^{-1}\right)^{-1}$
ข. $\left((2^{-1})^{-1}(3^{-1})\right)^{-1}$

6) ให้ $A = \{a, b\}$ จงพิจารณาว่ากึ่งกรุป $(P(A); \cup)$ เป็นกึ่งกรุปผกผันหรือไม่

7) จงแสดงว่ากึ่งกรุป $(I; +)$ เป็นกึ่งกรุปผกผันหรือไม่ เมื่อ $I = \{0, 1, 2, \ldots\}$

จงพิสูจน์ข้อความต่อไปนี้

8) ให้ S เป็นกึ่งกรุป และ $a \in S$ ถ้า $a = axa$ สำหรับบาง $x \in S$ แล้ว xa มีตัวผกผัน

9) ถ้า S เป็นกึ่งกรุปผกผัน แล้ว $E(S) \leq S$

10) ให้ $a_1, a_2, \ldots, a_n$ เป็นสมาชิกของกึ่งกรุปผกผัน S แล้วจะได้ว่า

$$\left(a_1 a_2 \ldots a_n\right)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1}$$

11) ให้ a เป็นสมาชิกของกึ่งกรุป S จะได้ว่า ถ้า $aS' = wS'$ สำหรับบาง $w \in E(S)$ แล้ว a เป็นสมาชิกเรกูลาร์(regular element)

จงพิสูจน์หรือยกตัวอย่างค้าน

12) ให้ a และ b เป็นสมาชิกของกึ่งกรุป S จะได้ว่า ถ้า a และ b เป็นสมาชิกเรกูลาร์ แล้ว $SaS = SbS$

13) ให้ a และ b เป็นสมาชิกของกึ่งกรุป S จะได้ว่า
ถ้า $a\mathcal{R}b$ แล้ว $a = bx$ และ $b = ay$ สำหรับบาง $x, y \in S^1$

14) ให้ a เป็นสมาชิกของกึ่งกรุป S จะได้ว่า
ถ้า S เป็นกึ่งกรุปผกผัน แล้ว R_a บรรจุสมาชิกสมาชิกนิจพลในรูปของ aa^{-1}

15) ถ้า S เป็นเรกูลาร์กึ่งกรุป แล้ว S เป็นกึ่งกรุปผกผัน

ภาคผนวก

การพิสูจน์แบบต่างๆ (Methods of Proof)

1. การพิสูจน์ทางตรง (Directed Proof)

โดยส่วนมากทฤษฎีบททางคณิตศาสตร์จะกำหนดอยู่ในรูปประโยคอิมพลิเคชัน $P \Rightarrow Q$ ดังนั้นเทคนิคของการพิสูจน์ที่ใช้โดยทั่วไปคือการพิสูจน์โดยตรง นั่นคือโดยการยอมรับว่าประโยค P เป็นจริง แล้วพิสูจน์ แสดงเหตุผลให้ได้ว่าประโยค Q เป็นจริง การพิสูจน์แบบนี้เราเรียกว่า **การพิสูจน์ทางตรง** (directed proof) ดังตัวอย่างต่อไปนี้

ตัวอย่าง 1.1 ถ้า n เป็นจำนวนเต็มคู่ แล้ว $5n+3$ เป็นจำนวนเต็มคี่

พิสูจน์ ให้ n เป็นจำนวนเต็มคู่ จะได้ว่า $n = 2k$ สำหรับบางจำนวนเต็ม k
ดังนั้น $5n+3 = 5(2k)+3 = 10k+3 = 10k+2+1 = 2(5k+1)+1$
เนื่องจาก $2k+1$ เป็นจำนวนเต็ม ดังนั้น $5n+3$ เป็นจำนวนคี่

ตัวอย่าง 1.2 ให้ a เป็นสมาชิกของกึ่งกรุป S ถ้า a มีตัวผกผันแล้ว a เป็นสมาชิกปกติ (regular element) ของ S

พิสูจน์ ให้ a มีตัวผกผัน จะได้ว่า มี $x \in S$ ซึ่งทำให้ $a = axa$ และ $x = xax$ ดังนั้น a เป็นสมาชิกปกติ

ตัวอย่าง 1.3 ถ้า x เป็นสมาชิกเรกูลาร์ (regular) ของกึ่งกรุป S แล้ว x มีตัวผกผัน

พิสูจน์ ให้ x เป็นสมาชิกเรกูลาร์ จะได้ว่า มี $y \in S$ ซึ่งทำให้ $x = xyx$
ดังนั้น จะได้

$$\begin{aligned} x &= xyx \\ &= (xyx)yx \\ &= x(yxy)x \end{aligned}$$

และ

$$\begin{aligned}(yxy)x(yxy) &= y(xyx)yxy \\ &= y(x)yxy \\ &= y(xyx)y \\ &= yxy\end{aligned}$$

ดังนั้น yxy เป็นตัวผกผันของ x

2. การยกตัวอย่างค้าน (Counterexamples)

ประโยคทางคณิตศาสตร์ที่สามารถแสดงในรูปแบบของอิมพลิเคชัน $P \Rightarrow Q$ สามารถแสดงได้ว่าเป็นเท็จโดยการยกตัวอย่างค้าน ให้ประโยค P และ Q เกี่ยวข้องกับสมาชิกของบางเซต S ถ้าสามารถหาได้ว่ามี สมาชิก $x \in S$ ซึ่งทำให้ประโยค P เป็นจริง แต่ทำให้ประโยค Q เป็นเท็จ แสดงว่า x เป็นตัวอย่างค้านของประโยค $P \Rightarrow Q$

ตัวอย่าง 2.1 ถ้า n เป็นจำนวนเต็ม แล้ว $3n + 1$ เป็นจำนวนเฉพาะ

พิสูจน์ เนื่องจาก 3 เป็นจำนวนเต็ม แต่ $3(3) + 1 = 9 + 1 = 10$ ซึ่ง 10 ไม่เป็นจำนวนเฉพาะ ดังนั้นประโยค " ถ้า n เป็นจำนวนเต็ม แล้ว $3n + 1$ เป็นจำนวนเฉพาะ" เป็นเท็จ

ตัวอย่าง 2.2 ถ้า a และ b เป็นจำนวนอตรรกยะ แล้ว ab เป็นจำนวนอตรรกยะ

พิสูจน์ เนื่องจาก $\sqrt{2}$ และ $3\sqrt{2}$ เป็นจำนวนอตรรกยะ แต่ $(\sqrt{2})(3\sqrt{2}) = 6$ ซึ่ง 6 ไม่เป็นจำนวนอตรรกยะ ดังนั้นประโยค " ถ้า a และ b เป็นจำนวนอตรรกยะ แล้ว ab เป็นจำนวนอตรรกยะ " เป็นเท็จ

3. การพิสูจน์โดยการแย้งสลับที่ (Proof by Contrapositive)

ประโยคแย้งสลับที่ (contrapositive) ของประโยคอิมพลิเคชัน $P \Rightarrow Q$ คือประโยคอิมพลิเคชัน $(\sim Q) \Rightarrow (\sim P)$ เนื่องจากว่าประโยคอิมพลิเคชันทั้งสองนี้สมมูลต่อกันนั่นคือมีค่าความจริงเหมือนกัน ดังนั้นการพิสูจน์ประโยค $P \Rightarrow Q$ สามารถพิสูจน์ประโยค $(\sim Q) \Rightarrow (\sim P)$ แทนได้

ในการพิสูจน์ประโยค $P \Rightarrow Q$ โดยใช้การพิสูจน์ประโยคแย้งสลับที่นั้น ทำได้ดังนี้คือ

เรากำหนดว่า ประโยค Q เป็นเท็จ แล้วพิสูจน์แสดงเหตุผลให้ได้ว่าประโยค P เป็นเท็จ ดังตัวอย่างต่อไปนี้

ตัวอย่าง 3.1 ให้ n เป็นจำนวนเต็ม ถ้า $11n - 5$ เป็นจำนวนคี่ แล้ว n เป็นจำนวนคู่

พิสูจน์ ให้ n ไม่เป็นจำนวนคู่ จะได้ว่า n เป็นจำนววนคี่ ดังนั้นจะมีบางจำนวนเต็ม k ซึ่งทำให้ $n = 2k + 1$ ทำให้ได้ว่า

$$11n - 5 = 11(2k + 1) - 5 = 22k + 11 - 5 = 22k + 6 = 2(11k + 3)$$

แสดงว่า $11n - 5$ เป็นจำนวนคู่

ตัวอย่าง 3.2 ให้ $a,$ และ b เป็นจำนวนเต็ม ถ้า $a+b$ เป็นจำนวนคี่ แล้ว a เป็นจำนวนคู่ หรือ b เป็นจำนวนคู่

พิสูจน์ ให้ a เป็นจำนวนคี่ และ b เป็นจำนวนคี่ จะได้ว่า $a = 2k+1$ และ $b = 2t+1$ สำหรับบางจำนวนเต็ม k, t

ดังนั้น

$$a + b = (2k + 1) + (2t + 1) = 2k + 2t + 2 = 2(k + t + 1)$$

เนื่องจาก $k + t + 1$ เป็นจำนวนเต็ม ดังนั้น $a + b$ เป็นจำนวนคู่

4. การพิสูจน์โดยการหาข้อขัดแย้ง (Proof by Contradiction)

ในการพิสูจน์โดยการหาข้อขัดแย้งของประโยคทางคณิตศาสตร์ S นั้น เราจะสมมุติให้ประโยค S เป็นเท็จแล้วแสดงว่าจากการสมมุตินี้นำไปสู่ข้อขัดแย้ง ถ้า S เป็นประโยคอิมพลิเคชัน $P \Rightarrow Q$ ในการพิสูจน์โดยการหาข้อขัดแย้งของอิมพลิเคชันนี้ เรากำหนดให้ประโยค $P \Rightarrow Q$ เป็นเท็จ นั่นคือกำหนดประโยค P เป็นจริงและประโยค Q เป็นเท็จ แล้วพิสูจน์ให้ได้ข้อขัดแย้ง ดังตัวอย่างต่อไปนี้

ตัวอย่าง 4.1 ให้ n เป็นจำนวนเต็มบวก ถ้า $n^3 + 1$ เป็นจำนวนเฉพาะ แล้ว $n = 1$

พิสูจน์ ให้ $n^3 + 1$ เป็นจำนวนเฉพาะ สมมุติว่า $n \neq 1$ จะได้ว่า $n \geq 2$ ดังนั้น $n + 1 \geq 3$ และ $n^2 - n + 1 = n(n - 1) + 1 \geq 3$

เนื่องจาก $n^3 + 1 = (n + 1)(n^2 - n + 1)$ แสดงว่า $n + 1$ และ $n^2 - n + 1$ เป็นตัวประกอบของ $n^3 - 1$ ดังนั้น $n^3 - 1$ ไม่เป็นจำนวนเฉพาะ : ขัดแย้ง

ดังนั้นการกำหนด $n \neq 1$ จึงเป็นไปไม่ได้ แสดงว่า ถ้า $n^3 + 1$ เป็นจำนวนเฉพาะ แล้ว $n = 1$

ตัวอย่าง 4.2 จงพิสูจน์ว่า $\sqrt{3}$ เป็นจำนวนอตรรกยะ

พิสูจน์ สมมุติว่า $\sqrt{3}$ ไม่ เป็นจำนวนอตรรกยะ จะได้ว่า $\sqrt{3}$ เป็นจำนวนตรรกยะ ดังนั้น สามารถเขียน $\sqrt{3}$ ให้อยู่ในรูปของเศษส่วนอย่างต่ำได้ ให้ $\sqrt{3} = \frac{a}{b}$ เป็นเศษส่วนดังกล่าว โดยที่ a และ $0 \neq b$ เป็นจำนวนเต็ม

ดังนั้นเราได้ $2b^2 = a^2$ นั่นคือ a^2 เป็นจำนวนคู่ ทำให้ได้ว่า a เป็นจำนวนคู่ ให้ $a = 2k$ สำหรับบางจำนวนเต็ม k จะได้ว่า $2b^2 = (2k)^2 = 4k^2$ ดังนั้น $b^2 = 2k^2$ แสดงว่า b^2 เป็นจำนวนคู่ ดังนั้น $\frac{a}{b}$ ไม่เป็นเศษส่วนอย่างต่ำ : ขัดแย้ง

แสดงว่า $\sqrt{3}$ เป็นจำนวนอตรรกยะ

5. การพิสูจน์ว่ามี (Existence Proofs)

มีประโยคทางคณิตศาสตร์จำนวนมากที่สร้างขึ้นโดยใช้การมีอยู่ของตัวบ่งปริมาณ (existenial quantifier, e.g., there exists, there is for some, there is at least one) การตรวจสอบประโยคทางคณิตศาสตร์ในลักษณะนี้วิธีการหนึ่งคือโดยหาตัวอย่างที่เหมาะสมสอดคล้องกับประโยคดังกล่าว ตัวอย่างเช่น

ตัวอย่าง 5.1 จงพิจารณาว่าข้อความต่อไปนี้เป็นจริงหรือเท็จ ” มีจำนวนเต็ม a, b และ c ที่มากกว่าหรือเท่ากับ 1 ซึ่งทำให้ $a^2 + b^3 + c^4$ เป็นจำนวนเฉพาะ”

พิสูจน์ ให้ $a = 7$, $b = c = 2$ จะได้ว่า

$$\begin{aligned} a^2 + b^3 + c^4 &= 7^2 + 2^3 + 2^4 \\ &= 49 + 8 + 16 \\ &= 73 \end{aligned}$$

ซึ่ง 73 เป็นจำนวนเฉพาะ ดังนั้นประโยค ” มีจำนวนเต็ม a, b และ c ที่มากกว่าหรือเท่ากับ 1 ซึ่งทำให้ $a^2 + b^3 + c^4$ เป็นจำนวนเฉพาะ ” เป็นจริง

ตัวอย่าง 5.2 ถ้า ϵ เป็นจำนวนจริงบวก แล้วจะมีจำนวนจริงบวก δ ซึ่งทำให้ ถ้า $|x-2| < \delta$ แล้ว $|(2x+3)-7| < \epsilon$

พิสูจน์ ให้ ϵ เป็นจำนวนจริงบวกใดๆ และให้ $\delta = \frac{\epsilon}{2}$
ให้ $|x-2| < \delta$ จะได้ว่า

$$\begin{aligned}|(2x+3)-7| &= |2x-4| \\ &= |2(x-2)| \\ &= 2|x-2| < 2(\frac{\epsilon}{2}) = \epsilon\end{aligned}$$

6. การพิสูจน์โดยการอุปนัยทางคณิตศาสตร์ (Mathematical Induction)

ให้ $P(n)$ เป็นประโยคเปิดที่เกี่ยวข้องกับจำนวนเต็มบวก n ถ้าต้องการแสดงว่า $P(1)$, $P(2), \ldots, P(n), \ldots$ เป็นจริงโดยใช้การอุปนัยทางคณิตศาสตร์ เราต้องแสดงว่า

(1) $P(1)$ เป็นจริง (Basis Step)

(2) ถ้า $P(k)$ แล้ว $P(k+1)$ เป็นจริง สำหรับทุกจำนวนเต็มบวก k (Induction Step)

ตัวอย่าง 6.1 ทุกๆจำนวนเต็มบวก n, $2^{n+2} \geq 7n+1$

พิสูจน์ ให้ $P(n) : 2^{n+2} \geq 7n+1$
พิจารณา $P(1)$:
เมื่อ $n = 1$ จะได้ว่า $2^{1+2} = 2^3 = 8 = 7(1)+1$ นั่นคือ $P(1)$ เป็นจริง
ให้ $P(k)$ เป็นจริง สำหรับ $k \in I^+$ จะได้ว่า $2^{k+2} \geq 7k+1$ ต้องการแสดงว่า $P(k+1)$ เป็นจริง นั่นคือต้องแสดงว่า $2^{(k+1)+2} \geq 7(k+1)+1$
เนื่องจาก

$$\begin{aligned}2^{(k+1)+2} &= 2 \cdot 2^{k+2} \\ &\geq 2(7k+1) && \text{เพราะว่า } 2^{k+2} \geq 7k+1 \\ &= 2(7k)+2 \\ &= 7k+7k+2 \\ &\geq 7k+7+2 && \text{เพราะว่า } 7k \geq 7 \\ &\geq 7k+8\end{aligned}$$

จะได้ว่า $P(k+1)$ เป็นจริง

ตัวอย่าง 6.2 $2^n < n!$ เมื่อ n เป็นจำนวนเต็มบวก และ $n \geq 4$

พิสูจน์ ให้ $P(n) : 2^n < n!$ เมื่อ n เป็นจำนวนเต็มบวก และ $n \geq 4$

พิจารณา $P(4)$:

เมื่อ $n = 4$ จะได้ว่า $2^4 = 16 < 24 = 4!$ ดังนั้น $P(4)$ เป็นจริง

ให้ $P(k)$ เป็นจริง สำหรับ $k \geq 4$ นั่นคือ $2^k < k!$ เป็นจริง ต้องการแสดงว่า $P(k+1)$ เป็นจริง นั่นคือต้องแสดงว่า $2^{k+1} < (k+1)!$

เนื่องจาก

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k \\ &< (k+1)k! \qquad \text{เพราะว่า}, \ \ 2 < k+1 \text{ และ } 2^k < k! \\ &= (k+1)! \end{aligned}$$

จะได้ว่า $P(k+1)$ เป็นจริง

เฉลยแบบฝึกหัด

แบบฝึกหัด 1.7

1) $(T;+)$ เป็นกึ่งกรุป เพราะ $+$ ไม่มีสมบัติการปิด

3) $(\mathbb{M}^{2\times 2};+)$ เป็นกึ่งกรุปย่อยของ $(\mathbb{Z}^{2\times 2};+)$ ทั้งนี้เพราะว่า

$$\begin{bmatrix} 0 & 2x \\ 2y & 0 \end{bmatrix} + \begin{bmatrix} 0 & 2t \\ 2w & 0 \end{bmatrix} = \begin{bmatrix} 0 & 2x+2t \\ 2y+2w & 0 \end{bmatrix} = \begin{bmatrix} 0 & 2(x+t) \\ 2(y+w) & 0 \end{bmatrix}$$

และ $x+t, y+w \in \mathbb{Z}$ สำหรับทุก $x, y, t, w \in \mathbb{Z}$

5) $(N_4; min)$ เป็นกึ่งกรุป เพราะการกระทำ min เป็นการกระทำทวิภาคบน N_4 และมีสมบัติการเปลี่ยนกลุ่ม

7) $E(\mathbb{N}) = \{0\}$ และ $R(\mathbb{N}) = \{0\}$

9) ให้ $S = \{a, b, c, d\}$ และกำหนดการกระทำ $*$ ดังตาราง

$*$	a	b	c	d
a	a	b	c	d
b	a	b	c	d
c	a	b	c	d
d	a	b	c	d

11) เป็นจริง
พิสูจน์ : ให้ $e \in E(S)$ จะได้ว่า e เป็นสมาชิกนิจพล นั่นคือ $ee = e$
ดังนั้น $ee = e = e1$ ทำให้ได้ว่า

$$\begin{aligned} e^{-1}(ee) &= e^{-1}(e1) \\ (e^{-1}e)e &= (e^{-1}e)1 \\ (1)e &= (1)1 \\ e &= 1 \end{aligned}$$

13) เป็นจริง

พิสูจน์ : ให้ $x, y \in S_e$ จะได้ว่า $xe = ex = x$ และ $ye = ey = y$
ดังนั้น

$$\begin{aligned} xy &= (xe)(ye) \\ &= x(ey)e \\ &= x(ye)e \\ &= xy(ee) \\ &= (xy)e \end{aligned}$$

สำหรับการแสดง $xy = e(xy)$ ทำได้ในทำนองเดียวกัน ดังนั้น $xy \in S_e$

15) $(\Rightarrow)$

$$\begin{aligned} a = aba &= (ab)a \\ &= (ba)a \\ &= b(aa) \\ &= ba \\ &= (bb)a \\ &= b(ba) \\ &= b(ab) = b \end{aligned}$$

แบบฝึกหัด 2.4

1) (ก) ให้ $A = \{a, b\}$ เนื่องจาก

$$\begin{aligned} SA &= \{xy \mid x \in S, y \in A\} \\ &= \{xa, xb \mid x \in S\} \\ &= \{x \mid x \in S\} \\ &= S \nsubseteq A \end{aligned}$$

จะได้ว่า A ไม่เป็นไอดีลทางซ้ายของ S แสดงว่า A ไม่เป็นไอดีลของ S
ข้อ (ข) - (ค) พิจารณาในทำนองเดียวกัน

3) (ก) เนื่องจาก S^1AS^1 เป็นไอดีลของกึ่งกรุป S สำหรับ $\emptyset \neq A \subseteq S$ ดังนั้น เราได้ว่า $(Z_6)^1A(Z_6)^1$ เป็นไอดีลของ Z_6 ที่บรรจุ $A = \{\overline{2}, \overline{4}\}$ โดยที่

$$\begin{aligned}(Z_6)^1A(Z_6)^1 &= Z_6AZ_6 \cup Z_6A \cup AZ_6 \cup A\\ &= Z_6\end{aligned}$$

(ข) Z_6 เป็นกึ่งกรุปเชิงเดียว
พิสูจน์ : ให้ I เป็นไอดีลของ Z_6 จะได้ว่า $Z_6I \subseteq I$ และ $IZ_6 \subseteq I$
เนื่องจาก

$$\begin{aligned}Z_6I &= \{x + i \mid x \in Z_6, i \in I\}\\ &= \{\overline{0} + i, \overline{1} + i, \ldots, \overline{5} + i \mid i \in I\}\\ &= \{\overline{0}, \overline{1}, \ldots, \overline{5}\}\\ &= Z_6\end{aligned}$$

จะได้ว่า $Z_6 = Z_6I \subseteq I$ ดังนั้น $I = Z_6$ นั่นคือ Z_6 ไม่มีไอดีลแท้

5) $(\mathbb{N}; +)$ ไม่เป็นกึ่งกรุปเชิงเดียว เพราะมีไอดีล $I = \{1, 2, 3, \ldots, \}$ ซึ่งเป็นไอดีลแท้ของ $\mathbb{N}$

7) ให้ I เป็นไอดีลใดๆของ $N + k$ จะได้ว่า $N_kI \subseteq I$
ดังนั้น

$$\begin{aligned}N_kI &= \{x \; min \; a \mid x \in N_k, a \in I\}\\ &= \{0 \; min \; a, 1 \; min \; a, \ldots, k \; min \; a \mid a \in I\}\\ &= \{0, 1, \ldots, m \mid m = \text{max of } I\}\end{aligned}$$

9) (i) ให้ S เป็นกึ่งกรุป

พิสูจน์. ให้ T เป็นเซตของไอดีลทางซ้ายทั้งหมดของ S และให้ $A, B \in T$ จะได้ว่า A และ B เป็นไอดีลทางซ้ายของ S ดังนั้น $SA \subseteq A$ และ $SB \subseteq B$
ต้องการแสดงว่า $AB \in T$, i. e. ต้องแสดงว่า $S(AB) \subseteq AB$
เนื่องจาก $SA \subseteq A$ จะได้ว่า $S(AB) = (SA)B \subseteq AB$
ข้อ (ii) - ข้อ (iii) พิสูจน์ได้ในทำนองเดียวกัน □

11) ***พิสูจน์.*** ให้ S เป็นกึ่งกรุปเชิงเดียวทางซ้าย และให้ I เป็นไอดีลใดๆของ S จะได้ว่า I เป็นไอดีลทางซ้ายของ S เนื่องจาก S เป็นกึ่งกรุปเชิงเดียวทางซ้าย ดังนั้น $I = S$ □

13) ***พิสูจน์.*** ให้ $z \in A$ จะได้ว่า

$$\begin{aligned} SA &= \{sa \mid s \in S, a \in A\} \\ &= \{z\} \subseteq A \end{aligned}$$

และ

$$\begin{aligned} AS &= \{as \mid s \in S, a \in A\} \\ &= \{z\} \subseteq A \end{aligned}$$

ดังนั้น A เป็นไอดีลของ S □

15) เป็นจริง

พิสูจน์. เนื่องจาก $a = aa \in Sa$ จะได้ว่า $S^1a = \{a\} \cup Sa = Sa$ ดังนั้น Sa เป็นไอดีลมุขสำคัญที่ก่อกำเนิดโดย a □

17) เป็นจริง

พิสูจน์. ให้ A เป็นไอดีลของกึ่งกรุป S จะได้ว่า $AS \subseteq A$ และ $SA \subseteq A$ ดังนั้น $S(SAS) = (SA)AS \subseteq S(AS)$ และ $(SAS)S = SA(SS) \subseteq SAS$ นั่นคือ SAS เป็นไอดีลของ S □

แบบฝึกหัด 3.5

1) ϕ ไม่เป็นสาทิสสัณฐาน ทั้งนี้เพราะว่า มี $2, 3 \in \mathbb{Z}$ ซึ่ง $\phi(2 \cdot 3) = \phi(6) = 6$ แต่ $\phi(2) + \phi(3) = 2 + 3 = 5$ ทำให้ $\phi(2 \cdot 3) \neq \phi(2) + \phi(3)$

3) เห็นได้ชัดว่า ϕ เป็นความสัมพันธ์สมมูล ต่อไปเราจะตรวจสอบว่า ϕ เป็นสมภาคทางซ้ายหรือไม่
ให้ $(x, y) \in \phi$ และ $z \in \mathbb{N}_3$
ถ้า $x = y$ โดยสมบัติการสะท้อนของ ϕ จะได้ว่า $(zx, zy) = (zx, zx) \in \phi$
ถ้า $x \neq y$ จะได้ว่า $(x, y) = (2, 3)$ หรือ $(x, y) = (3, 2)$
ถ้า $(x, y) = (2, 3)$ จะได้ว่า

$$(z2, z3) = (zmin2, zmin3) \in \{(0,0), (1,1), (2,2), (2,3)\} \subseteq \phi$$

ถ้า $(x, y) = (3, 2)$ จะได้ว่า

$$(z2, z3) = (zmin2, zmin3) \in \{(0,0), (1,1), (2,2), (3,2)\} \subseteq \phi$$

ดังนั้น ϕ เป็นสมภาคทางซ้าย
เนื่องจาก

$$\begin{aligned}(zx, zy) &= (zminx, zminy)\\ &= (xminz, yminz)\\ &= (xz, yz)\end{aligned}$$

ดังนั้น ϕ เป็นสมภาคทางขวา

7) เป็นเท็จ เช่น ให้ S, T เป็นกึ่งกรุปที่บรรจุเอกลักษณ์ โดยที่ $|S| \geq 2$, $|T| \geq 2$ นิยาม ϕ โดย

$$\phi : S \to T \text{ กำหนดโดย } \quad \phi(x) = 1_T \text{ สำหรับทุก } x \in S$$

เห็นได้ชัดว่า ϕ เป็นสาทิสสัณฐาน แต่ $\phi^{-1} : \{1_T\} \to S$ ไม่เป็นสาทิสสัณฐาน เพราะไม่เป็นฟังก์ชัน

9) ***พิสูจน์.*** เห็นได้ชัดว่า $\Delta_S = \{(a, a) \mid a \in S$ เป็นความสัมพันธ์สมมูล นอกจากนี้ สำหรับ $z \in S$ เราได้ว่า $(za, za), (az, az) \in \Delta_S$ ดังนั้น Δ_S เป็นสมภาค □

แบบฝึกหัด 4.3

1)

$$\begin{aligned}S^1a &= SA \cup \{a\}\\ &= \{sa | s \in S\} \cup \{a\}\\ &= S\end{aligned}$$

ในทำนองเดียวกันเราได้ว่า $S^1b = S^1c = S^1d = S$ ดังนั้น $\mathcal{L} = S \times S$

3) (ก) ให้ $x, y \in \mathbb{R}$ เราได้ว่า

$$\begin{aligned}\mathbb{R}^1 x &= \mathbb{R}x \cup \{x\} \\ &= \{r + x \mid r \in \mathbb{R}\} \cup \{x\}\end{aligned}$$

และ

$$\begin{aligned}\mathbb{R}^1 y &= \mathbb{R}y \cup \{y\} \\ &= \{r + y \mid r \in \mathbb{R}\} \cup \{y\}\end{aligned}$$

ดังนั้น $\mathbb{R}^1 x = \mathbb{R}^1 y$ ก็ต่อเมื่อ $x = y$
นั่นคือ $\mathcal{L} = \{(x, x) \mid x \in \mathbb{R}\}$

5) ($\Rightarrow$) ให้ $a\mathcal{R}b$ จะได้ว่า $aS^1 = bS^1$ เนื่องจาก $a \in \{a\} \cup aS = aS^1 = bS^1$ จะได้ว่า $a = bx$ สำหรับบาง $x \in S^1$ ในทำนองเดียวกัน $b \in \{b\} \cup bS = bS^1 = aS^1$ ดังนั้น $b = ay$ สำหรับบาง $y \in S^1$
($\Leftarrow$) ให้ $a = bx$ และ $b = ay$ สำหรับบาง $x, y \in S^1$ เราได้ว่า

$$\begin{aligned}aS &= (bx)S = b(xS) \subseteq bS \subseteq bS^1 \\ bS &= (ay)S = a(yS) \subseteq aS \subseteq aS^1\end{aligned}$$

นอกจากนี้เรามี

$$\begin{aligned}a &= bx \in bS \subseteq bS^1 \\ b &= ay \in aS \subseteq aS^1\end{aligned}$$

ดังนั้น

$$\begin{aligned}aS^1 &= \{a\} \cup aS \subseteq bS^1 \\ bS^1 &= \{b\} \cup bS \subseteq aS^1\end{aligned}$$

บรรณานุกรม

[1] ราชบัณฑิตยสถาน (2553) พจนานุกรมศัพท์คณิตศาสตร์ ฉบับราชบัณฑิตยสถาน พิมพ์ครั้งที่ 10 นานมีบุ๊คส์พับลิเคชั่นส์ กรุงเทพฯ

[2] Butkote, Runglawan. (2009). Universal-algebraic and Semigroup-theoretical Properties of Boolean Operations. Dissertation Universitat Potsdam, Germany.

[3] Butkote, Runglawan and Denecke, Klaus. (2008). Semigroup Properties of Boolean Operations : Asian-Eur. J. Math. Vol.1(2). pp 157-175.

[4] Butkote, Runglawan. Denecke , Klaus and Ratanaprasert, Chaweewan. (2008). Semigroup Properties of n-ary Operations on Finite Sets : Asian-Eur. J. Math. Vol.1(1). pp 27-44.

[5] Carman, K. S. (1949). Semigroups Ideals. University of Tennessee, Knoxville. USA. http://trace.tennessee.edu/cgi/viewcontent.cgi?article=2398context=utk-gradthes

[6] Denecke, Klaus and Wismath, S.L. (2002). Universal algebra and Application in Theoretical Computer Science. Washington D.C : Chapman-Hall/CRC.

[7] Good, R. A. and Hughes, D. R. Associated Groups for a Semigroup. Bull. amer. Math. Soc., 58, 624-625 (1954).

[8] Harju, Tero. (1996). Lecture notes on Semigroups. Department of Mathematics, Turku University. Finland.

[9] Howie, J. (1995). Fundamentals of Semigroup Theory. USA : Oxford University Press Inc.

[10] Howie, J. and Ruskuc, N. (1998). Semigroups and Applications. USA : World Scientific Publishing Co. Pte. Ltd.

[11] Kolman, B. Busby, R. and Ross, S. (2004). Discrete Mathematical Structures. Upper Saddle River, N.J. : Pearson/Pentice Hall.

[12] Kuroki, N. (1977). On Normal Semigroups. Czechoslovak Math. J. Vol 27(1), pp 43-53.

[13] Lajos, S. On the Bi-ideals in Semigroups. Proc. Japan Acad. Vol(45), pp 710-712.

[14] Lawson, M. (1998). Inverse semigroups: the Theory of Partial Symmetries. New Jersey : World Scientific.

[15] Pin, J.E. Syntactic Semigroup. University Paris VI, Paris, France: https:// www.irif.fr/ jep/PDF/HandBook.pdf

[16] Schwarz, S. (1960). A Theorem on Normal Semigroups. Czechoslovak Math. J. Vol 10(2), pp 197-200.

[17] Vicky, G. Lecture Note on Semigroup Theory. http:// math.arizona.edu/ jaytaylor/files/york/SemigroupTheory.pdf

ดรรชนี