พีชคณิตนามธรรม
Abstract Algebra

สาขาวิชาคณิตศาสตร์ คณะครุศาสตร์

มหาวิทยาลัยราชภัฏสวนสุนันทา

2567

MAC3310

พีชคณิตนามธรรม

Abstract Algebra

ผู้ช่วยศาสตราจารย์ ดร.ธนัชยศ จำปาหวาย
สาขาวิชาคณิตศาสตร์ คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา
เอกสารประกอบการสอนวิชาพีชคณิตนามธรรม ปีการศึกษา 1/2567

สารบัญ

บทที่ 1

ความรู้พื้นฐาน

เมื่อแรกเริ่มคณิตศาสตร์เกิดขึ้นมาเพื่อแก้ปัญหาต่าง ๆ ของมนุษย์เช่น จำนวนนับเกิดจากการแก้ปัญหาของคนเลี้ยงแกะเพื่อตรวจสอบว่าจำนวนแกะก่อนและหลังพาไปกินหญ้ามีจำนวนเท่าเดิมหรือไม่ ดังนั้นคณิตศาสตร์ในเบื้องต้นมักอธิบายให้เห็นเป็นรูปธรรมได้อย่างเด่นชัดและเป็นกฎเกณฑ์ที่สอดคล้องกับธรรมชาติอย่างลงตัว แต่ด้วยจินตนาการของนักคณิตศาสตร์พยายามจะขยายกฎเกณฑ์ต่าง ๆ ที่ได้มาให้อยู่ในรูปแบบทั่วไปมากยิ่งขึ้น เป็นผลให้นิยามสิ่งใหม่ ๆ และเกิดกฎเกณฑ์ตามมาในรูปแบบที่เป็นนามธรรม พีชคณิตนามธรรมก็ถูกพัฒนามาจากแนวคิดนี้ดังจะกล่าวใน 1.1 จากนั้นกล่าวถึงความรู้พื้นฐานที่จะนำไปใช้ในการทำความเข้าใจเกี่ยวกับพีชคณิตนามธรรม

1.1 วิวัฒนาการของวิชาพีชคณิตนามธรรม

คำว่า **พีชคณิต** ตรงกับคำในภาษาอังกฤษ **algebra** ซึ่งมาจากภาษาอาหรับ al jebr ใช้ครั้งแรกราวศตวรรษที่ 9 โดยนักคณิตศาสตร์ชาวอาหรับนามว่า มูฮัมหมัดแห่งคาริซม์ (Mohammed of Kharizm) ช่วงเริ่มต้นคำว่าพีชคณิตใช้แทนวิธีการต่าง ๆ ในการหาคำตอบของสมการ (Charles C. Pinter. 2016. หน้า3) และใช้ครั้งแรกในยุโรปโดยนักคณิตศาสตร์ชื่อว่า โอมาร์ เคย์แยม (Omar Khayyam) หมายถึงวิทยาการการหาคำตอบของสมการ (the science of sloving equations)

การหาคำตอบในรูปทั่วไปของสมการเชิงเส้น (linear equation) $ax + b = 0$ และสมการกำลังสอง (quadratic equation) $ax^2 + bx + c = 0$ มีผู้หาคำตอบได้ก่อนสมัยกรีก-โรมันโบราณ แต่ในตอนนั้นยังไม่มีผู้ใดหาคำตอบในรูปทั่วไปของสมการกำลังสาม (cubic equation) ในรูป

$$x^3 + ax^2 + bx = c$$

และสมการกำลังสี่ (quartic equation) ในรูป

$$x^4 + ax^3 + bx^2 + cx = d$$

ในช่วงศตรรษที่ 16 นักคณิตศาสตร์ชาวอิตาลีชื่อ กิโรลาโม คาร์ดาน (Girolamo Cardan) มีความสนใจคณิตศาสตร์ในรูปนามธรรมและความสำเร็จอย่างหนึ่งคือการตีพิมพ์หนังสือชื่อ Ars Magna (The Great Art) ซึ่งเขียนเกี่ยวกับความรู้ทางพีชคณิตอย่างเป็นระบบ ตัวอย่างเช่นการหา

คำตอบของสมการ $x^3 + ax + b = 0$ โดยการเปลี่ยนตัวแปร $x = u + v$ จะได้ว่า

$$x^3 = (u+v)^3 = u^3 + v^3 + 3uv(u+v) = u^3 + v^3 + 3uvx$$

ดังนั้น

$$x^3 - 3uvx - (u^3 + v^3) = 0$$

โดยเทียบสัมประสิทธิ์กับสมการ $x^3 + ax + b = 0$ จะได้ว่า

$$-3uv = a \quad \text{และ} \quad u^3 + v^3 = -b \text{ นั่นคือ } u^3 = -b - v^3$$

กำหนดให้ $t = v^3$ จากสมการ $-3uv = a$ จะได้ว่า

$$27bt + 27t^2 - a^3 = 0 \tag{1.1}$$

จะเห็นได้ว่าสมการ (1.1) เป็นสมการกำลังสองซึ่งหาคำตอบของ t ได้เสมอจึงทำให้หาค่าของ v และ u จนสุดท้ายได้คำตอบคือ $x = u + v$ ของสมการ $x^3 + ax + b = 0$ เรียกวิธีการนี้ว่า **วิธีของคาร์ดาน** (Cardan's method)

ตัวอย่าง 1.1.1 จงหาคำตอบของสมการ $x^3 - 27x - 54 = 0$ โดยวิธีของคาร์ดาน

แต่การค้นพบของคาร์ดานก็มิใช่คำตอบของรูปแบบทั่วไปของสมการกำลังสาม ผู้คนพบคือตาร์แทกเลีย (Tartaglia) ซึ่งคาร์ดานได้ใช้ความพยายามเป็นอย่างมากเพื่อให้ตาร์แทกเลียยอมให้ตีพิมพ์ผลงานดังกล่าว จนในที่สุดตาร์แทกเลียก็ยอมตีพิมพ์ในหนังสือเล่มนี้โดยคาร์ดานได้เขียนไว้ในหนังสือว่าเป็นของตาร์แทกเลีย

ต่อมา ลูโดวิโค เฟอร์ราริ (Ludovico Ferrari) ซึ่งเป็นคนรับใช้ส่วนตัวของคาร์ดาน ได้ค้นพบคำตอบในรูปทั่วไปของสมการ

$$x^4 + ax^3 + bx^2 + cx = d$$

200 ปีต่อมานักคณิตศาสตร์หลาย ๆ คนพยายามหาคำตอบในรูปทั่วไปของสมการที่กำลังมากกว่าสี่แต่ไม่สำเร็จจนในปี 1824 นีลส์ อาเบล (Niels Abel) ได้พิสูจน์ให้เห็นว่าไม่สามารถหาคำตอบในรูปทั่วไปของสมการกำลังที่มากกว่าสี่

การค้นพบของอาเบลเป็นเหตุทำให้นักคณิตศาสตร์หลายท่านหันมาสนใจและทำงานด้านนี้มากยิ่งขึ้น มีการทำงานกันอย่างอิสระทำให้เกิดงานที่หลากหลายในยุโรปในช่วงนั้น งานวิจัยของพวกเขาทำให้เกิดสาขาคณิตศาสตร์ที่แตกต่างกันจนนำไปสู่การหาที่มาของคำว่าพีชคณิต ในกรณีที่ไม่มีวิธีการหาคำตอบในรูปทั่วไปของสมการ ทำให้นักคณิตศาสตร์ขยายแนวคิดให้กว้างมากยิ่งขึ้นว่าอะไรกันแน่ที่เกี่ยวข้องกับพีชคณิต ต่อมามีการพัฒนาพีชคณิตแบบใหม่ให้สูงขึ้นอย่างเป็นธรรมชาติและสมบูรณ์แบบ และเชื่อมโยงไปใช้ในการแก้ปัญหาด้านต่าง ๆ ได้

ปัจจุบันพีชคณิตคือการศึกษาภายใต้ระบบสัจพจน์นั่นคือการศึกษาในรูปนามธรรม (abstract) นักคณิตศาสตร์จะศึกษาโครงสร้างพีชคณิตในรูปทั่วไป และมีการเปรียบเทียบกับโครงสร้างอื่น ๆ และหาความสัมพันธ์ระหว่างโครงสร้างเหล่านั้น ผลที่ได้จากพีชคณิตนามธรรมอาจจะเป็นวิธีการใหม่ หรือคำตอบที่ต่างกันกันออกไปในแต่ละโครงสร้างที่เราไม่เคยค้นพบมาก่อน เป็นการเติมเต็มคำตอบชนิดใหม่

ความรู้เบื้องต้นในการศึกษาพีชคณิตนามธรรมคือเซตซึ่ง **เซต (Set)** เป็นคำอนิยาม หมายถึงคำที่ต้องยอมรับกันในเบื้องต้นว่าไม่สามารถให้ความหมายที่รัดกุมได้ คำว่าเซตจึงหมายถึงกลุ่มของสิ่งของต่าง ๆ เมื่อกล่าวถึงกลุ่มใดแล้วจะสามารถบอกได้แน่นอนว่าสิ่งใดอยู่ในกลุ่ม และสิ่งใดอยู่นอกกลุ่ม เรียกสิ่งต่าง ๆ ที่อยู่ในเซตว่า **สมาชิก (element)** (P. Glendinning. 2012. หน้า 48) ถ้า a เป็นสมาชิกของเซต A เขียนแทนด้วย $a \in A$ และถ้า a ไม่เป็นสมาชิกของเซต A เขียนแทนด้วย $a \notin A$ เช่น $A = \{1, 2, 3\}$ จะได้ว่า $1 \in A$ แต่ $4 \notin A$ เป็นต้น

การเขียนเซตประกอบด้วย 2 วิธีคือ วิธีแจกแจงสมาชิก และวิธีบอกเงื่อนไขของสมาชิก

1. **วิธีแจกแจงสมาชิก** (Tabular form) การเขียนเซตแบบแจกแจงสมาชิก คือการเขียนเซตโดยเขียนสมาชิกลงในเครื่องหมายวงเล็บปีกกา $\{\}$ และใช้เครื่องหมายจุลภาค $(,)$ คั่นระหว่างสมาชิกแต่ละตัว ตัวอย่างเช่น $\{1, 2, 3\}, \{4, 5, 6\}$ และ $\{a, b, c\}$ เป็นต้น

2. **วิธีบอกเงื่อนไขของสมาชิก** (Set builder form) การเขียนเซตแบบบอกเงื่อนไขประกอบด้วย 2 ส่วน ส่วนแรกหมายถึงสมาชิก และส่วนที่สองคือเงื่อนไขของสมาชิก โดยมีเครื่องหมายทวิภาค (:) คั่นระหว่างสองส่วนนั้น อ่านว่า "โดยที่"

   $$A = \{ \text{สมาชิก} : \text{เงื่อนไขของสมาชิก} \}$$

   ตัวอย่างเช่น $A = \{x : x$ เป็นจำนวนเต็มบวกที่น้อยกว่า $5\}$ หมายถึง $A = \{1, 2, 3, 4\}$

สำหรับเซต A ที่มีสมาชิกทุกตัวอยู่ในเซต B จะกล่าวว่า A เป็น **เซตย่อย** (subset) ของ B เขียนแทนด้วย $A \subseteq B$ และเรียกเซตของเซตย่อยของ A ว่า **เซตกำลัง** (power set) ของ A เขียนแทนด้วย นั่นคือ

$$\mathcal{P}(A) = \{X : X \subseteq A\}$$

สำหรับเซตที่ไม่มีสมาชิกเขียนแทนด้วย $\varnothing$ เรียกว่า **เซตว่าง** (empty set) และ **เอกภพสัมพัทธ์** (universe) คือเซตที่ถูกกำหนดขึ้นโดยมีข้อตกลงว่า จะกล่าวถึงสิ่งที่เป็นสมาชิกของเซตนี้เท่านั้น และนิยมใช้ $\mathcal{U}$ แทนเอกภพสัมพัทธ์ เมื่อให้ A และ B เป็นเซตในเอกภพสัมพัทธ์ $\mathcal{U}$ นิยามการดำเนินการบนเซตดังต่อไปนี้

ยูเนียน (union) $\quad A \cup B = \{x \in \mathcal{U} : x \in A \text{ หรือ } x \in B\}$

อินเตอร์เซกชัน (intersection) $\quad A \cap B = \{x \in \mathcal{U} : x \in A \text{ และ } x \in B\}$

ผลต่าง (difference) $\quad A - B = \{x \in \mathcal{U} : x \in A \text{ และ } x \notin B\}$

ส่วนเติมเต็ม (complement) $\quad A^c = \{x \in \mathcal{U} : x \notin A\}$

ในกรณีที่ทราบจำนวนสมาชิกของเซต A เรียกว่า **เซตจำกัด** (finite set) เขียน $|A|$ แทนจำนวนสมาชิกของ A และเซตที่ไม่มช่เซตจำกัดเรียกว่า **เซตอนันต์** (infinite set)

ในเบื้องต้นเพื่อให้ง่ายต่อการนำไปใช้ กำหนดสัญลักษณ์ดังนี้

$\mathbb{C}$	แทนเซตของจำนวนเชิงซ้อน	$\mathbb{Q}^c$	แทนเซตของจำนวนอตรรกยะ
$\mathbb{R}$	แทนเซตของจำนวนจริง	$\mathbb{Z}$	แทนเซตของจำนวนเต็ม
$\mathbb{Q}$	แทนเซตของจำนวนตรรกยะ	$\mathbb{N}$	แทนเซตของจำนวนนับ

สำหรับ $\mathbb{R}^+$, $\mathbb{Q}^+$ และ $\mathbb{Z}^+$ หมายถึงเซตของจำนวนจริงบวก เซตของจำนวนตรรกยะบวก และเซตของจำนวนเต็มบวกตามลำดับ $\mathbb{R}^-$, $\mathbb{Q}^-$ และ $\mathbb{Z}^-$ หมายถึงเซตของจำนวนจริงลบ เซตของจำนวนตรรกยะลบ และเซตของจำนวนเต็มลบตามลำดับ $\mathbb{C}^*$, $\mathbb{R}^*$, $\mathbb{Q}^*$ และ $\mathbb{Z}^*$ หมายถึง เซตของจำนวนเชิงซ้อนที่ไม่ใช่ศูนย์ เซตของจำนวนจริงที่ไม่ใช่ศูนย์ เซตของจำนวนตรรกยะที่ไม่ใช่ศูนย์ และเซตของจำนวนเต็มที่ไม่ใช่ศูนย์ตามลำดับ และใช้ $\mathbb{N}_0$ แทนเซต $\mathbb{N} \cup \{0\}$

สำหรับเซตย่อยของจำนวนจริง ถ้า $a, b \in \mathbb{R}$ เมื่อ $a < b$ **ช่วง** (interval) ของจำนวนจริงต่าง ๆ คือ

$\{x \in \mathbb{R} : a < x < b\}$	เขียนแทนด้วย	(a, b)
$\{x \in \mathbb{R} : a \leq x \leq b\}$	เขียนแทนด้วย	$[a, b]$
$\{x \in \mathbb{R} : a \leq x < b\}$	เขียนแทนด้วย	$[a, b)$
$\{x \in \mathbb{R} : a < x \leq b\}$	เขียนแทนด้วย	$(a, b]$
$\{x \in \mathbb{R} : x > a\}$	เขียนแทนด้วย	(a, ∞)
$\{x \in \mathbb{R} : x \geq a\}$	เขียนแทนด้วย	$[a, \infty)$
$\{x \in \mathbb{R} : x < b\}$	เขียนแทนด้วย	$(-\infty, b)$
$\{x \in \mathbb{R} : x \leq b\}$	เขียนแทนด้วย	$(-\infty, b]$

แบบฝึกหัด 1.1

1. เพราะเหตุใดนักคณิตศาสตร์จึงหันมาสนใจพีชคณิตมากยิ่งขึ้นในศตวรรษที่ 19

2. จงหาคำตอบในรูปทั่วไปของสมการ $x^2 + ax + b = 0$

3. จงใช้วิธีของคาร์ดานหาคำตอบของสมการต่อไปนี้ โดยการกำหนด $x = u + v$ และ $t = u^3$

   3.1 $x^3 - 27x + 54 = 0$
   3.2 $x^3 - 18x + 35 = 0$
   3.3 $x^3 - 12x - 16 = 0$
   3.4 $x^3 + 15x - 72 = 0$
   3.5 $x^3 + 20x - 225 = 0$
   3.6 $x^3 - 14x - 245 = 0$

4. จงหาคำตอบในรูปทั่วไปของสมการ $x^3 + ax + b = 0$ โดยใช้วิธีของคาร์ดาน

5. จงยกตัวอย่างลักษณะกลุ่มที่ไม่เป็นเซตมาอย่างน้อย 2 ตัวอย่าง พร้อมให้เหตุผลประกอบ

6. ให้เอกภพสัมพัทธ์ $\mathcal{U} = \mathbb{N}$ และกำหนดให้ $A_n = \{1, 2, 3, ..., n\}$ เมื่อ $n \in \mathbb{N}$ จงหา

   6.1 $A_2 \cup A_4$
   6.2 $A_3 \cap A_5$
   6.3 $A_1^c - A_2^c$
   6.4 $A_{2562} \cap A_{2019}$

1.2 อุปนัยเชิงคณิตศาสตร์

ในหัวข้อนี้จะกล่าวถึงเครื่องมือที่ใช้ในการพิสูจน์ข้อความเกี่ยวกับจำนวนเต็ม โดยเริ่มต้นจากสัจพจน์เกี่ยวกับสมบัติของจำนวนเต็มที่เรียกว่า **หลักการจัดอันดับดี** (Well Ordering Principle) กล่าวคือ

ให้ $S \subseteq \mathbb{N}$ และ $S \neq \varnothing$ จะได้ว่า S มีสมาชิกตัวเล็กสุด หรือ มี $m \in S$ ซึ่ง $m \leq s$ ทุก ๆ $s \in S$

ทฤษฎีบท 1.2.1 **หลักการของอาร์คีมีดีส** (Archimedean Principle)
สำหรับจำนวนเต็มบวก a และ b ใด ๆ จะมีจำนวนเต็มบวก n ซึ่ง $na \geq b$

ทฤษฎีบท 1.2.2 ถ้า $S \subseteq \mathbb{N}$ สอดคล้อง 2 เงื่อนไขต่อไปนี้

1. $1 \in S$
2. ถ้า $k \in S$ แล้ว $k+1 \in S$

แล้วจะได้ว่า $S = \mathbb{N}$

โดยทฤษฎีบท 1.2.2 สามารถนำไปใช้ในการพิสูจน์ข้อความต่าง ๆ ทางคณิตศาสตร์ในรูป

$P(n)$ แทนข้อความที่เกี่ยวข้องกับ n เมื่อ $n \in \mathbb{N}$

การพิสูจน์ทำได้ 2 ขั้นตอนดังนี้

1. **ขั้นฐาน** (Basic step) : $P(1)$ เป็นจริง
2. **ขั้นอุปนัย** (Inductive step) : สำหรับจำนวนนับ k ถ้า $P(k)$ เป็นจริง แล้ว $P(k+1)$ เป็นจริง

แล้วสรุปได้ว่า $P(n)$ เป็นจริงสำหรับทุก ๆ จำนวนนับ n
เรียกการพิสูจน์นี้ว่า **การพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์** (proof by mathematical induction)

ตัวอย่าง 1.2.3 จงพิสูจน์ข้อความต่อไปนี้โดยหลักอุปนัยเชิงคณิตศาสตร์

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3} \quad \text{สำหรับทุกจำนวนนับ} \quad n$$

ต่อไปกล่าวถึงการพิสูจน์อุปนัยเชิงคณิตศาสตร์ที่ขั้นฐานเริ่มต้นที่ $n_0 \in \mathbb{Z}$ เมื่อ $P(n)$ แทนข้อ-ความที่เกี่ยวข้องกับจำนวนเต็ม ที่สอดคล้อง 2 เงื่อนไขต่อไปนี้

1. **ขั้นฐาน** : $P(n_0)$ เป็นจริง
2. **ขั้นอุปนัย** : สำหรับจำนวนเต็ม k ซึ่ง $k \geq n_0$ ถ้า $P(k)$ เป็นจริง แล้ว $P(k+1)$ เป็นจริง

สรุปได้ว่า $P(n)$ เป็นจริงสำหรับทุก ๆ จำนวนเต็ม $n \geq n_0$

ตัวอย่าง 1.2.4 จงหาจำนวนนับ n_0 เริ่มต้นที่ทำให้ $2^n \geq n^2$ ทุก ๆ จำนวนนับ $n \geq n_0$ พร้อมทั้งพิสูจน์ข้อความข้างต้น

ในกรณีข้อความเกี่ยวกับจำนวนนับไม่สามารถพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์ที่กล่าวมาข้างต้น อาจจะใช้รูปแบบการพิสูจน์ได้ดังต่อไปนี้ ให้ $P(n)$ แทนข้อความเกี่ยวกับจำนวนนับ ถ้า

1. **ขั้นฐาน** : $P(1)$ เป็นจริง
2. **ขั้นอุปนัย** : ถ้า $P(k)$ เป็นจริงสำหรับทุกจำนวนนับ k ที่ $k < m$ แล้ว $P(m)$ เป็นจริง

สรุปได้ว่า $P(n)$ เป็นจริงสำหรับทุกจำนวนนับ n

ตัวอย่าง 1.2.5 ลำดับลูคัส (Lucus sequence) นิยามโดย $a_1 = 1,\ a_2 = 3$ และ

$$a_n = a_{n-1} + a_{n-2} \qquad \text{สำหรับ } n = 3, 4, 5, ...$$

จงพิสูจน์ว่า $a_n < \left(\frac{7}{4}\right)^n$ เป็นจริงสำหรับทุกจำนวนนับ n

แบบฝึกหัด 1.2

1. จงพิสูจน์ข้อความต่อไปนี้เป็นจริงทุกจำนวนนับ n โดยใช้หลักอุปนัยเชิงคณิตศาสตร์

   1.1 $1^2+2^2+3^2+\cdots+n^2=\frac{1}{3}n^3+\frac{1}{2}n^2+\frac{1}{6}n$

   1.2 $1^3+2^3+3^3+\cdots+n^3=\frac{1}{4}n^4+\frac{1}{2}n^3+\frac{1}{4}n^2$

   1.3 $1^4+2^4+3^4+\cdots+n^4=\frac{1}{5}n^5+\frac{1}{2}n^4+\frac{1}{3}n^3-\frac{1}{30}n$

   1.4 $1+3+5+\cdots+(2n-1)=n^2$

   1.5 $2+4+6+\cdots+(2n)=n(n+1)$

   1.6 $2+2^2+2^3+\cdots+2^n=2^{n+1}-2$

   1.7 $1\cdot 2+2\cdot 2^2+3\cdot 2^3+\cdots+n\cdot 2^n=(n-1)2^{n+1}+2$

   1.8 $1(1!)+2(2!)+3(3!)+\cdots+n(n!)=(n+1)!-1$

   1.9 $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}+\dfrac{1}{3\cdot 4}+\cdots+\dfrac{1}{n(n+1)}=\dfrac{n}{n+1}$

   1.10 $2^n\le 2^{n+1}-2^{n-1}-1$

   1.11 $2^n>n$

2. จงหาจำนวนนับ n_0 เริ่มต้นที่ทำให้ $2^n\ge n^2$ ทุก ๆ จำนวนนับ $n\ge n_0$ พร้อมทั้งพิสูจน์

   2.1 $2^{n-1}\le n!$

   2.2 $4^n>n^4$

   2.3 $(2n)!<2^{2n}(n!)^2$

   2.4 $n^2<\left(\dfrac{3}{2}\right)^n$

3. ให้ a เป็นจำนวนจริง จงพิสูจน์ว่า

$$a^n-1=(a-1)(a^{n-1}+a^{n-2}+\cdots+a+1)\quad \text{สำหรับทุกจำนวนนับ}\quad n$$

4. ให้ x เป็นจำนวนจริงซึ่ง $x\ge -1$ จงพิสูจน์ว่า

$$(1+x)^n\ge 1+nx\quad \text{สำหรับทุกจำนวนนับ}\quad n$$

1.3 ทฤษฎีจำนวนเบื้องต้น

บทนิยาม 1.3.1 ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ จะกล่าวว่า a **หาร** b **ลงตัว** แทนด้วยสัญลักษณ์ $a \mid b$ นิยามโดย

$$a \mid b \quad \text{ก็ต่อเมื่อ} \quad \text{มีจำนวนเต็ม} \quad c \quad \text{ที่ทำให้} \quad b = ac$$

เรียก a ว่า**ตัวหาร** (divisor) ของ b ถ้า a **หาร** b **ไม่ลงตัว** เขียนแทนด้วย $a \nmid b$

ข้อสังเกต 1.3.2 สำหรับจำนวนเต็ม a ใด ๆ

1. $1 \mid a$
2. $a \mid 0$ เมื่อ $a \neq 0$
3. $a \mid a$ เมื่อ $a \neq 0$

ทฤษฎีบท 1.3.3 ให้ a, b และ c เป็นจำนวนเต็ม แล้ว

1. ถ้า $a \mid b$ และ $b \neq 0$ แล้ว $|a| \leq |b|$
2. ถ้า $a \mid b$ และ $b \mid a$ แล้ว $a = \pm b$

ทฤษฎีบท 1.3.4 ให้ a, b และ c เป็นจำนวนเต็ม

1. ถ้า $a \mid b$ และ $b \mid c$ แล้ว $a \mid c$
2. ถ้า $a \mid b$ แล้ว $(ac) \mid (bc)$ เมื่อ $c \neq 0$
3. ถ้า $a \mid b$ และ $c \mid d$ แล้ว $ac \mid bd$

ทฤษฎีบท 1.3.5 ให้ a, b และ c เป็นจำนวนเต็ม แล้ว

1. ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a \mid (b+c)$
2. ถ้า $a \mid b$ แล้ว $a \mid (bx)$ ทุก ๆ จำนวนเต็ม x
3. ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a \mid (bx+cy)$ ทุก ๆ จำนวนเต็ม x และ y

ทฤษฎีบท 1.3.6 ให้ a, b และ c เป็นจำนวนเต็ม

$$\text{ถ้า} \quad a \mid (b+c) \quad \text{และ} \quad a \mid b \quad \text{แล้ว} \quad a \mid c$$

ตัวอย่าง 1.3.7 จงหาจำนวนเต็มบวก n ที่สอดคล้อง $n \mid (n+8)^2$

ทฤษฎีบท 1.3.8 **ขั้นตอนวิธีการหาร** (The Division Algorithm)
ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ แล้วมีจำนวนเต็ม q และ r เพียงคู่เดียวที่ทำให้

$$b = aq + r \qquad \text{โดยที่} \qquad 0 \leq r < |a| \tag{1.2}$$

เรียก q ว่า**ผลหาร** (quotient) และ r ว่า**เศษเหลือ** (remainder)

ตัวอย่าง 1.3.9 สำหรับจำนวนเต็ม n จงพิสูจน์ว่า $3 \mid (n^3 - n)$

บทนิยาม 1.3.10 ให้ a และ b เป็นจำนวนเต็มที่ไม่ใช่ศูนย์พร้อมกัน จำนวนเต็ม d เป็น**ตัวหารร่วมมาก** (greatest common divisior) ของ a และ b เขียนแทนด้วย $\gcd(a, b)$ ก็ต่อเมื่อ

(ก) $d \mid a$ และ $d \mid b$

(ข) ทุกจำนวนเต็ม c ถ้า $c \mid a$ และ $c \mid b$ แล้ว $c \leq d$

ในกรณี $\gcd(a, b) = 1$ จะเรียก a และ b เป็น**จำนวนเฉพาะสัมพัทธ์** (relatively prime)

ทฤษฎีบท 1.3.11 ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ และ $d = \gcd(a, b)$ แล้ว

$$\text{จะมี } x, y \in \mathbb{Z} \text{ ที่ทำให้} \qquad d = ax + by$$

ทฤษฎีบท 1.3.12 ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ แล้ว

$$\gcd(a, b) = 1 \qquad \text{ก็ต่อเมื่อ} \qquad \text{มี} \quad x, y \in \mathbb{Z} \quad \text{ที่ทำให้} \quad 1 = ax + by$$

ทฤษฎีบท 1.3.13 ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ หรือ $b \neq 0$ และ $d = \gcd(a, b)$ แล้ว

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

บทนิยาม 1.3.14 ให้ $a_1, a_2, ..., a_n$ เป็นจำนวนเต็มที่ไม่ใช่ศูนย์พร้อมกัน แล้ว

จำนวนเต็มบวก d จะเป็น**ตัวหารร่วม**ของ $a_1, a_2, ..., a_n$ ก็ต่อเมื่อ $d \mid a_1, d \mid a_2, ..., d \mid a_n$ และ d จะเป็น**ตัวหารร่วมมาก**ของ $a_1, a_2, ..., a_n$ เขียนแทนด้วย gcd$(a_1, a_2, ..., a_n)$ ก็ต่อเมื่อ

(1) d เป็นตัวหารร่วมของ $a_1, a_2, ..., a_n$ และ

(2) สำหรับจำนวนเต็มบวก c ถ้า c เป็นตัวหารร่วมของ $a_1, a_2, ..., a_n$ แล้ว $d \leq c$

บทแทรก 1.3.15 ให้ $a_1, a_2, ..., a_n \in \mathbb{Z}$ โดยที่ a_i ไม่ใช่ศูนย์บาง $i \in \{1, 2, ..., n\}$
และ $d =$ gcd$(a_1, a_2, ..., a_n) = d$ แล้ว

$$\text{gcd}\left(\frac{a_1}{d}, \frac{a_2}{d}, ..., \frac{a_n}{d}\right) = 1$$

ทฤษฎีบท 1.3.16 ให้ a, b, c, m เป็นจำนวนเต็ม จะได้ว่า

1. ถ้า $a \mid bc$ และ gcd$(a, b) = 1$ แล้ว $a \mid c$
2. ถ้า $a \mid c$ และ $b \mid c$ โดยที่ gcd$(a, b) = 1$ แล้ว $(ab) \mid c$

บทนิยาม 1.3.17 ให้ a และ b เป็นจำนวนเต็มที่ไม่ใช่ศูนย์ จำนวนเต็มบวก m จะเป็น**ตัวคูณร่วมน้อย** (least common multiple) ของ a และ b เขียนแทนด้วย $\ell\text{cm}(a, b)$ ก็ต่อเมื่อ

(ก) $a \mid m$ และ $b \mid m$

(ข) ทุกจำนวนเต็มบวก c ถ้า $a \mid c$ และ $b \mid c$ แล้ว $m \leq c$

ทฤษฎีบท 1.3.18 ให้ a, b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ และ $b \neq 0$ จะได้ว่า

$$\text{gcd}(a, b) \cdot \ell\text{cm}(a, b) = |ab|$$

ตัวอย่าง 1.3.19 จงหาตัวคูณร่วมน้อยของ 131 และ 100

บทนิยาม 1.3.20 จำนวนเต็ม $p \in \mathbb{Z}$ ซึ่ง $|p| > 1$ เรียกว่า **จำนวนเฉพาะ** (prime) ก็ต่อเมื่อ

$$p \text{ มีตัวหารคือ } \pm 1 \text{ และ } \pm p \text{ เท่านั้น}$$

จำนวนเต็มที่มากกว่า 1 หรือน้อยกว่า -1 ที่ไม่ใช่จำนวนเฉพาะเรียกว่า **จำนวนประกอบ** (composite number)

จากบทนิยามจะเห็นว่าถ้า p เป็นจำนวนเฉพาะ แล้ว $-p$ เป็นจำนวนเฉพาะด้วย เพื่อให้ง่ายต่อการศึกษาทฤษฎีบทต่าง ๆ เราจะศึกษาในกรณีที่ $p > 1$ เท่านั้น ซึ่งผลที่ได้สามารถครอบคลุมถึง $p < -1$ ด้วยเช่นกัน (ในหนังสือบางเล่มอาจนิยามจำนวนเฉพาะ $p > 1$)

ข้อสังเกต 1.3.21 จากนิยามจะได้ว่า

1. 2 เป็นจำนวนเฉพาะที่เป็นจำนวนคู่เพียงตัวเดียวเท่านั้น
2. p เป็นจำนวนเฉพาะ ก็ต่อเมื่อ $d \nmid p$ ทุก ๆ จำนวนเต็ม d ซึ่ง $1 < d < p$
3. ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ ถ้า $a \mid p$ แล้ว $a = \pm 1$ หรือ $a = \pm p$
4. ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ จะได้ว่า $p \mid a$ ก็ต่อเมื่อ $\gcd(a, p) = p$
5. ให้ p เป็นจำนวนเฉพาะ และ $a \in \mathbb{Z}$ จะได้ว่า $p \nmid a$ ก็ต่อเมื่อ $\gcd(a, p) = 1$
6. ให้ p และ q เป็นจำนวนเฉพาะ ถ้า $p \mid q$ แล้ว $p = q$
7. a เป็นจำนวนประกอบ ก็ต่อเมื่อ มีจำนวนเต็ม d ซึ่ง $1 < d < a$ ที่ทำให้ $d \mid a$
8. a เป็นจำนวนประกอบ ก็ต่อเมื่อ มีจำนวนเต็ม b, c ซึ่ง $1 < b \leq c < a$ ที่ทำให้ $a = bc$

ต่อไปเป็นจำนวนเฉพาะทั้งหมดที่น้อยกว่า 1,000

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	419	421	431	433	439
443	449	457	461	463	467	479	487	491	499	503	509
521	523	541	547	557	563	569	571	577	587	593	599
601	607	613	617	619	631	641	643	647	653	659	661
673	677	683	691	701	709	719	727	733	739	743	751
757	761	769	773	787	797	809	811	821	823	827	829
839	853	859	863	877	881	883	887	907	911	919	929
937	941	947	953	967	971	977	983	911	997		

ทฤษฎีบท 1.3.22 ทุกจำนวนเต็ม a ที่มากกว่า 1 จะมีจำนวนเฉพาะ p ที่ $p \mid a$

ทฤษฎีบท 1.3.23 ให้ p เป็นจำนวนเฉพาะ และ $a, b \in \mathbb{Z}$ จะได้ว่า

ถ้า $p \mid ab$ แล้ว $p \mid a$ หรือ $p \mid b$

ทฤษฎีบท 1.3.24 ให้ p เป็นจำนวนเฉพาะ และ $a, b, a_1, a_2, ..., a_n \in \mathbb{Z}$ เมื่อ $n \in \mathbb{N}$ จะได้ว่า

ถ้า $p \mid (a_1 a_2 ... a_n)$ แล้ว $p \mid a_i$ สำหรับบางจำนวน $i \in \{1, 2, ..., n\}$

ทฤษฎีบท 1.3.25 **ทฤษฎีบทหลักมูลเลขคณิต** (The Fundamental Theorem of Arithmematic) จำนวนเต็มที่มากกว่า 1 ใด ๆ สามารถเขียนในรูปผลคูณของจำนวนเฉพาะได้ และถ้าไม่คิดลำดับเป็นสำคัญแล้วการเขียนนี้ทำได้เพียงวิธีเดียวเท่านั้น
หรือกล่าวได้ว่า จำนวนเต็ม $n > 1$ สามารถเขียนในรูป

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_k^{a_k}$$

โดยที่ $p_1, p_2, p_3, ..., p_k$ เป็นจำนวนเฉพาะซึ่ง $p_1 < p_2 < p_3 < ... < p_k$ และ $a_i \in \mathbb{N}$ สำหรับทุก $i = 1, 2, 3, ..., k$ และเขียน n ในรูปดังกล่าวได้เพียงแบบเดียวเท่านั้น เรียกการเขียน n รูปแบบนี้ว่า **รูปแบบบัญญัติ** (canonical form) ของ n

ตัวอย่าง 1.3.26 จงเขียนรูปแบบบัญญัติของจำนวนต่อไปนี้

1. 3600
2. $20!$

ตัวอย่าง 1.3.27 จงหาตัวประกอบทั้งหมดของ 144

ต่อไปจะกล่าวถึงฟังก์ชันฟีซึ่งเป็นฟังก์ชันที่สำคัญในวิชาพีชคณิตนามธรรม

บทนิยาม 1.3.28 ให้ $n \in \mathbb{N}$ นิยาม

$$\phi(n) = \text{จำนวนของจำนวนเต็มบวก } k \leq n \text{ และ } \gcd(k, n) = 1$$

เรียกว่า **ฟังก์ชันฟีออยเลอร์** (Euler phi function) หรือ **ฟังก์ชันฟี** (phi function)

ข้อสังเกต 1.3.29 $\phi(1) = 1$ และ $\phi(p) = p - 1$ เมื่อ p เป็นจำนวนเฉพาะ

ในกรณีที่จำนวนประกอบ n มีรูปเป็นรูปแบบบัญเป็น $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_k^{a_k}$ จะได้ว่า

$$\phi(n) = (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots (p_k^{a_k} - p_k^{a_k-1})$$

โดยเฉพาะอย่างยิ่ง $\phi(p^k) = p^k - p^{k-1}$ เมื่อ p เป็นจำนวนเฉพาะ และ $k \in \mathbb{N}$

ตัวอย่าง 1.3.30 จงหาค่าของ

1. $\phi(100)$
2. $\phi(120)$
3. $\phi(300)$
4. $\phi(1500)$

แบบฝึกหัด 1.3

1. ให้ a, b และ c เป็นจำนวนเต็ม จงพิสูจน์

   1.1 ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a \mid (bc)$

   1.2 ถ้า $a \mid b$ แล้ว $a^2 \mid b^2$

2. จงพิสูจน์ข้อความต่อไปนี้ โดยใช้หลักอุปนัยเชิงคณิตศาสตร์

   2.1 $5 \mid (n^5 - n)$ สำหรับจำนวนนับ n

   2.2 $7 \mid (3^{2n+1} + 2^{n+2})$ สำหรับจำนวนนับ n

   2.3 $8 \mid (7 \cdot 3^{2n} - 7)$ สำหรับจำนวนนับ n

3. กำหนดให้ a, b, c, d เป็นจำนวนเต็ม จงพิจารณาข้อความต่อไปนี้ ถ้าเป็นจริงจงพิสูจน์ ถ้าเป็นเท็จจงยกตัวอย่างค้าน

   3.1 ถ้า $a \mid b^2$ แล้ว $a \mid b$

   3.2 ถ้า $a \mid b$ และ $a \mid c$ แล้ว $a^2 \mid bc$

   3.3 $\ell\text{cm}(a^2, b^2) = (\ell\text{cm}(a, b))^2$

   3.4 ถ้า $a \mid c$ และ $b \mid c$ และ $\ell\text{cm}(a, b) = |ab|$ แล้ว $ab \mid c$

   3.5 $\ell\text{cm}(ca, b) = c \cdot \ell\text{cm}(a, b)$

4. จงแสดงว่า ถ้า $\text{gcd}(a, 4) = 2$ และ $\text{gcd}(b, 4) = 2$ แล้ว $\text{gcd}(a + b, 4) = 2$ เมื่อ $a, b \in \mathbb{Z}$

5. ให้ $a, b \in \mathbb{Z}$ โดยที่ $a \neq 0$ และ $b \neq 0$ จงพิสูจน์ว่าถ้า $\text{gcd}(a, b^n) = 1$ cแล้ว $\text{gcd}(a, b) = 1$ สำหรับจำนวนนับ n ใด ๆ

6. ให้ $a, b, c \in \mathbb{Z}$ จงแสดงว่า $\ell\text{cm}(a, b) \mid c$ ก็ต่อเมื่อ $a \mid c$ และ $b \mid c$

7. จงเขียนจำนวนต่อไปนี้ในรูปแบบบัญญัติ

7.1 1000	7.3 25025	7.5 $100!$
7.2 1500	7.4 65304	7.6 88442

8. จงแสดงว่า ถ้า p เป็นจำนวนเฉพาะ แล้ว $p \mid (2^p - 2)$

9. ถ้า p และ q เป็นจำนวนเฉพาะซึ่ง $p \geq q > 4$ จงแสดงว่า $24 \mid (p^2 - q^2)$

10. จงหาค่าต่อไปนี้

10.1 $\phi(72)$	10.3 $\phi(450)$	10.5 $\phi(4900)$
10.2 $\phi(150)$	10.4 $\phi(1000)$	10.6 $\phi(8100)$

1.4 ความสัมพันธ์และฟังก์ชัน

บทนิยาม 1.4.1 ให้ A และ B เป็นเซตใด ๆ **ผลคูณคาร์ทีเซียน** (cartesian product) นิยามโดย

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

สำหรับ $A \times A$ จะเขียนแทนด้วย A^2 ทำนองเดียวกัน $\underbrace{A \times A \times \cdots \times A}_{n \text{ ตัว}}$ เขียนแทนด้วย A^n

ตัวอย่าง 1.4.2 ให้ $A = \{1, 2\}$ และ $B = \{3, 4, 5\}$ จงหาผลคูณคาร์ทีเซียน $A \times B$ และ $B \times A$

ทฤษฎีบท 1.4.3 ให้ A และ B เป็นเซตจำกัด แล้ว $|A \times B| = |A| \cdot |B|$

บทนิยาม 1.4.4 **ความสัมพันธ์** (relation) จากเซต A ไป B คือเซตย่อยของ $A \times B$

ถ้า R เป็นความสัมพันธ์จาก A ไป B และ $(a, b) \in R$ เขียนแทนด้วย $a\,R\,b$

ในกรณีที่ R เป็นความสัมพันธ์จาก A ไป A จะเรียก R ว่าความสัมพันธ์บน A

บทนิยาม 1.4.5 ให้ R เป็นความสัมพันธ์ใน A โดยที่ A เป็นเซตที่ไม่ใช่เซตว่าง แล้วจะเรียก R ว่า **ความสัมพันธ์สมมูล** (equivalence relation) ก็ต่อเมื่อมีสมบัติ 3 ข้อดังต่อไปนี้

1. **สะท้อน** (Reflexive) ก็ต่อเมื่อ $a\,R\,a$ ทุก ๆ $a \in A$
2. **สมมาตร** (Symmetric) ก็ต่อเมื่อ ถ้า $a\,R\,b$ แล้ว $b\,R\,a$ ทุก ๆ $a, b \in A$
3. **ถ่ายทอด** (Transitive) ก็ต่อเมื่อ ถ้า $a\,R\,b$ และ $b\,R\,c$ แล้ว $a\,R\,c$ ทุก ๆ $a, b, c \in A$

ถ้า R เป็นความสัมพันธ์สมมูล และ $a \in A$ **ชั้นสมมูลของ** a **มอดุโล** R (equivalence class of a modulo R)

$$[a] = \{x \in A \,:\, x\,R\,a\}$$

และเซตของชั้นสมมูลเรียกว่า A **มอดุโล** R (A mudulo R) เขียนแทนด้วย A/R ดังนั้น

$$A/R = \{[a] \,:\, a \in A\}$$

ตัวอย่าง 1.4.6 ให้ $x, y \in \mathbb{Z}$ กำหนดให้

$$x\,R\,y \quad \text{ก็ต่อเมื่อ} \quad 3 \mid (y - x)$$

จงพิสูจน์ว่า R เป็นความสัมพันธ์สมมูลบน $\mathbb{Z}$ พร้อมหา $\mathbb{Z}/R$

ทฤษฎีบท 1.4.7 ให้ R เป็นความสัมพันธ์สมมูลบนเซต $A \neq \varnothing$ แล้ว

1. $\forall a \in A,\ [a] \neq \varnothing$
2. $\forall a, b \in A,\ [a] \cap [b] \neq \varnothing \leftrightarrow a\,R\,b$
3. $\forall a, b \in A,\ [a] = [b] \leftrightarrow a\,R\,b$
4. $\forall a, b \in A,\ [a] \neq [b] \leftrightarrow [a] \cap [b] = \varnothing$

บทนิยาม 1.4.8 ให้ A เป็นเซตที่ไม่ใช่เซตว่าง และ Λ เป็นเซตดรรชนี จะกล่าวว่า

$$\Pi = \{A_\alpha : \varnothing \neq A_\alpha \subseteq A \text{ และ } \alpha \in \Lambda\}$$

เป็น**ผลแบ่งกัน** (partition) ของ A ถ้า

(1) $\displaystyle\bigcup_{\alpha \in \Lambda} A_\alpha = A$

(2) $\forall \alpha, \beta \in \Lambda,\ A_\alpha = A_\beta$ หรือ $A_\alpha \cap A_\beta = \varnothing$

เมื่อ $\displaystyle\bigcup_{\alpha \in \Lambda} A_\alpha = \{x : x \in A_\alpha \text{ สำหรับบาง } \alpha \in \Lambda\}$

ทฤษฎีบท 1.4.9 ให้ A เป็นเซตไม่ใช่เซตว่าง และ R เป็นความสัมพันธ์สมมูลบน A แล้ว

$$A/R \text{ เป็นผลแบ่งกั้นหนึ่งของ } A$$

จากตัวอย่าง 1.4.6 จะได้ว่า $\{[0], [1], [2]\}$ เป็นผลแบ่งกันของ $\mathbb{Z}$ ต่อไปจะพิจารณากรณีทั่วไปของความสัมพันธ์ในตัวอย่างดังกล่าวคือ

$$a \sim b \qquad \text{ก็ต่อเมื่อ} \qquad n \mid (b-a)$$

เมื่อ n เป็นจำนวนเต็มบวก พิสูจน์คล้ายกับตัวอย่าง 1.4.6 จะได้ว่า $\sim$ เป็นความสัมพันธ์สมมูลบน $\mathbb{Z}$ ชั้นสมมูลของ $a \in \mathbb{Z}$ เขียนแทนด้วย $\bar{a}$ นั่นคือ

$$\bar{a} = \{a + kn \,:\, k \in \mathbb{Z}\}$$

ข้อสังเกต 1.4.10 ในกรณี $\bar{a} = \bar{b}$ โดยทฤษฎีบท 1.4.7 ข้อ 3 จะได้ว่า $a \sim b$ นั่นคือ $n \mid (b-a)$ ดังนั้นมีจำนวนเต็ม k ซึ่ง $b = a + kn$ หรือกล่าวได้ว่า

$$\bar{a} = \bar{b} \qquad \text{ก็ต่อเมื่อ} \qquad b = a + kn \quad \text{สำหรับบางจำนวนเต็ม } k$$

หรือกล่าวอีกนัยหนึ่งได้ว่า

$$\bar{a} = \bar{b} \qquad \text{ก็ต่อเมื่อ} \qquad \text{เมื่อนำ } n \text{ ไปหาร } a \text{ และ } b \text{ แล้วมีเศษเหลือเท่ากัน}$$

ชั้นสมมูลที่แตกต่างกันมีทั้งหมด n เซตดังนี้

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

เรียกเซตของชั้นสมมูลว่า **เซตของจำนวนเต็มมอดุโล** ***n*** (the set of integer molulo *n*) เขียนแทนด้วย $\mathbb{Z}_n$ ดังนั้น

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

ต่อไปคือตัวอย่างของเซตของจำนวนเต็มมอดุโล *n*

เซตของจำนวนเต็มมอดุโล *n*	แจกแจงสมาชิก
$\mathbb{Z}_1$	$\{\bar{0}\}$
$\mathbb{Z}_2$	$\{\bar{0}, \bar{1}\}$
$\mathbb{Z}_3$	
$\mathbb{Z}_4$	
$\mathbb{Z}_5$	
$\mathbb{Z}_6$	
$\mathbb{Z}_7$	
$\mathbb{Z}_{11}$	

บทนิยาม 1.4.11 จะกล่าวว่าความสัมพันธ์ $f \subseteq A \times B$ เป็น**ฟังก์ชัน** (function) ก็ต่อเมื่อ

แต่ละ (x_1, y_1) และ (x_2, y_2) ใน f ถ้า $x_1 = x_2$ แล้ว $y_1 = y_2$

ถ้า f เป็นฟังก์ชัน และ $(x, y) \in f$ เขียนแทนด้วย $y = f(x)$ หรือ $x \mapsto f(x)$

บทนิยาม 1.4.12 f เป็น**ฟังก์ชันจาก** A **ไป** B (function from A into B) เขียนแทนด้วย $f : A \to B$ ก็ต่อเมื่อ

1. f เป็นฟังก์ชัน
2. $\text{Dom}(f) = A$
3. $\text{Ran}(f) \subseteq B$

เมื่อ $\text{Dom}(f) = \{x \in A : \exists y \in B,\ (x, y) \in f\}$ เรียกว่า **โดเมน** (domain) ของ f
และ $\text{Ran}(f) = \{y \in B : \exists x \in A,\ (x, y) \in f\}$ เรียกว่า **เรนจ์** (range) ของ f

บทนิยาม 1.4.13 กำหนดให้ $f : A \to B$ จะกล่าวว่า

1. f เป็น**ฟังก์ชันหนึ่งต่อหนึ่ง** (one-to-one **หรือ** injection) หรือ ฟังก์ชัน 1-1 ก็ต่อเมื่อ

$$\forall x_1, x_2 \in A,\ f(x_1) = f(x_2) \to x_1 = x_2$$

2. f เป็น**ฟังก์ชันทั่วถึง** (onto function **หรือ** surjection) ก็ต่อเมื่อ $\text{Ran}(f) = B$
3. f เป็น**ฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึง** (bijection) ก็ต่อเมื่อ f เป็นฟังก์ชันหนึ่งต่อหนึ่งและเป็นฟังก์ชันทั่วถึง

ข้อสังเกต 1.4.14 ให้ $f : A \to B$ โดยที่ A และ B เป็นเซตจำกัด

1. ถ้า f เป็นฟังก์ชันหนึ่งต่อหนึ่ง แล้ว $|A| \leq |B|$
2. ถ้า f เป็นฟังก์ชันทั่วถึง แล้ว $|A| \geq |B|$
3. ถ้า f เป็นฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึง แล้ว $|A| = |B|$

ในกรณี $A = \{a_1, a_2, a_3, ..., a_n\}$ และ f ฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึง จาก A ไป B เขียนแทนด้วยแผนภาพต่อไปนี้

$$\begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ f(a_1) & f(a_2) & f(a_3) & \cdots & f(a_n) \end{pmatrix}$$

ตัวอย่าง 1.4.15 จงเขียนแผนภาพแทนฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึงจาก A ไป A เมื่อ $A = \{1, 2, 3\}$

บทนิยาม 1.4.16 ให้ $f : A \to B$ และ $g : B \to C$ แล้ว $g \circ f : A \to C$ เรียกว่า**ฟังก์ชันประกอบ** (composite function) ของ f และ g นิยามโดย

$$(g \circ f)(x) = g(f(x))$$

ฟังก์ชันเอกลักษณ์ (indentity function) คือ $i_A : A \to A$ นิยามโดย $i_A(x) = x$

ตัวอย่าง 1.4.17 ให้ $A = \{1, 2, 3, 4\}$ และ f, g เป็นฟังก์ชันจาก A ไป A โดยที่

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \text{และ} \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

จงหาฟังก์ชันต่อไปนี้

1. i_A

2. $f \circ g$

3. $g \circ f$

4. $f \circ f$

บทนิยาม 1.4.18 ให้ $f : A \to B$ จะกล่าวว่า f เป็น**ฟังก์ชันผกผันได้** (invertible function)

ก็ต่อเมื่อ

$$f^{-1} = \{(y, x) \,:\, (x, y) \in f\} \text{ เป็นฟังก์ชัน}$$

และเรียก f^{-1} ว่า**ฟังก์ชันผกผัน** (inverse function) ของ f

ทฤษฎีบท 1.4.19 ให้ $f : A \to B$ แล้วจะได้ว่า

$$f \text{ เป็นฟังก์ชันผกผันได้ ก็ต่อเมื่อ } f \text{ เป็นฟังก์ชัน 1-1}$$

ทฤษฎีบท 1.4.20 $f : A \to B$ เป็นฟังก์ชัน 1-1 แบบทั่วถึง ก็ต่อเมื่อ $f^{-1} : B \to A$ เป็นฟังก์ชัน 1-1 แบบทั่วถึง

ตัวอย่าง 1.4.21 ให้ $A = \{1, 2, 3, 4\}$ และ f, g เป็นฟังก์ชันจาก A ไป A โดยที่

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \qquad \text{และ} \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

จงหาฟังก์ชันต่อไปนี้

1. f^{-1}

2. g^{-1}

3. $f^{-1} \circ g^{-1}$

4. $(f \circ g)^{-1}$

ทฤษฎีบท 1.4.22 ให้ $f : A \to B$ แล้ว

1. $f \circ i_A = f$
2. $i_B \circ f = f$

ทฤษฎีบท 1.4.23 ให้ $f : A \to B$ เป็นฟังก์ชัน 1-1 แบบทั่วถึง จะได้ว่า

1. $f \circ f^{-1} = i_B$
2. $f^{-1} \circ f = i_A$

แบบฝึกหัด 1.4

1. ให้ $n \in \mathbb{N}$ จงแสดงว่า $\sim$ เป็นความสัมพันธ์สมมูลบน $\mathbb{Z}$ โดยที่

$$a \sim b \qquad \text{ก็ต่อเมื่อ} \qquad n \mid (b-a)$$

2. ความสัมพันธ์ R บน $\mathbb{Z}$ นิยามโดย $\quad a\,R\,b \quad$ ก็ต่อเมื่อ $\quad 2 \mid (a+b)$
จงแสดงว่า R เป็นความสัมพันธ์สมมูล และหา $\mathbb{Z}/R$

3. จงแจกแจงสมาชิกของเซตต่อไปนี้ $\mathbb{Z}_8$, $\mathbb{Z}_{13}$ และ $\mathbb{Z}_{18}$

4. ให้ $f : A \to B$ เป็นฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึง จงพิสูจน์ว่าความสัมพันธ์ที่นิยามโดย

$$a \sim b \qquad \text{ก็ต่อเมื่อ} \qquad f(a) = f(b)$$

เป็นความสัมพันธ์สมมูล และหาชั้นของสมมูล

5. ถ้า f, g, h เป็นฟังก์ชันจาก A ไป A จงแสดงว่า $f \circ (g \circ h) = (f \circ g) \circ h$

6. จงตรวจสอบว่า $f : \mathbb{Q} \to \mathbb{Q}$ นิยามโดย $f(a/b) = a$ เป็นฟังก์ชันหรือไม่

7. ให้ $f(x) = \dfrac{x-1}{x+1}$ เมื่อ $x \neq -1$ จงหาสูตรของ $f^{-1}(x)$

8. ให้ $A = \{1, 2, 3, 4, 5\}$ และ f, g เป็นฟังก์ชันจาก A ไป A โดยที่

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \qquad \text{and} \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

จงหาฟังก์ชันต่อไปนี้

8.1 $f \circ g$ 8.3 $g \circ g$ 8.5 $f^{-1} \circ g$ 8.7 $(f \circ g)^{-1}$

8.2 $g \circ f$ 8.4 $f \circ f$ 8.6 $g \circ f^{-1}$ 8.8 $(g \circ f)^{-1}$

1.5 การดำเนินการทวิภาค

หลายคนคงคุ้นเคยกับการดำเนินการต่าง ๆ โดยเฉพาะทางเลขคณิต เช่น การบวก ลบ คูณ หาร $(+, -, \cdot, \div)$ มาบ้างแล้ว ในหัวข้อนี้จะนำเสนอนิยามของการเนินการให้อยู่ในรูปทั่วไปมากขึ้น ซึ่งเรียกว่า**การดำเนินการทวิภาค** (binary operation) ซึ่งเป็นฟังก์ชันหนึ่งโดยนิยามดังต่อไปนี้

บทนิยาม 1.5.1 ให้ G เป็นเซตที่ไม่ใช่เซตว่าง แล้ว $*$ เป็น **การดำเนินการทวิภาค** บนเซต G ก็ต่อเมื่อ

$$* : G \times G \to G$$

นิยมเขียน $a * b = c$ แทน $*(a, b) = c$

ข้อสังเกต 1.5.2 ถ้า $*$ เป็นการดำเนินการทวิภาคบน G แล้ว

$$a * b \in G \qquad \text{ทุก ๆ } a, b \in G$$

และกล่าวว่า G มี **สมบัติปิด** (closed) ภายใต้ $*$

ตัวอย่าง 1.5.3 ต่อไปนี้เป็นตัวอย่างการดำเนินการทวิภาคที่คุ้นเคย เช่น

1. $+$ เป็นการดำเนินการทวิภาคบน $\mathbb{Z}$ เขียน $a + b$ แทน $+((a, b))$
2. $\times$ เป็นการดำเนินการทวิภาคบน $\mathbb{Z}$ เขียน $a \times b$ แทน $\times((a, b))$
3. $\cup$ เป็นการดำเนินการทวิภาคบนเอกภพสัมพัทธ์ เขียน $A \cap B$ แทน $\cap((A, B))$

ตัวอย่าง 1.5.4 จงตรวจสอบว่า $*$ เป็นการดำเนินการทวิภาคหรือไม่

1. $a * b = a + b + 1$ บน $\mathbb{Z}$
2. $a * b = \dfrac{a + b}{2}$ บน $\mathbb{Z}$

ตัวอย่าง 1.5.5 ให้ $*$ เป็นการดำเนินการทวิภาคบนเซตของจำนวนนับ โดย

$$a * b = \frac{1}{2}(a + b)(a + b - 1)$$

จงหาค่าของ $3 * 2$ และ $1 * (2 * 3)$

ต่อไปจะกล่าวถึงการสร้าง **ตารางเคย์เลย์** (Cayley table) หรือ **ตารางกรุป** (group table) สำหรับการดำเนินการบนเซตจำกัดเพื่อให้แสดงถึงค่าต่าง ๆ ที่เกิดจากการดำเนินการที่กำหนดให้ โดยมีหลักว่าตัวดำเนินการตัวหน้ากำหนดไว้เป็นหลักแรกและตัวดำเนินการตัวหลังกำหนดไว้แถวบนสุด และผลการดำเนินการคือส่วนตารางที่เกิดการจากตัวหน้าและตัวหลัง ดังตัวอย่าง $*$ เป็นการดำเนินการทวิภาคบนเซต $\{a, b, c\}$

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

สำหรับการบวกและการคูณบนเซต $\{1, 2, 3\}$ เขียนตารางเคย์เลย์ได้ดังนี้

$+$	1	2	3
1	2	3	4
2	3	4	5
3	4	5	6

$\times$	1	2	3
1	1	2	3
2	2	4	6
3	3	6	9

ตัวอย่าง 1.5.6 จงสร้างตารางเคย์เลย์สำหรับดำเนินการทวิภาค $*$ ดังต่อไปนี้

1. $a * b = ab$ บน $\{0, 1\}$

2. $a * b = a^b$ บน $\{-1, 1\}$

3. $a * b = \dfrac{(-1)^a + (-1)^b}{2}$ บน $\{-1, 0, 1\}$

4. $\bar{a} * \bar{b} = \overline{a+b}$ บน $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

ตัวอย่าง 1.5.7 ตารางเคย์เลย์ของการดำเนินการทวิภาค $*$ บนเซต $G = \{1, 2, 3, 4\}$ คือ

$*$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

จงหาค่าต่อไปนี้

1. $(1 * 2) * (3 * 2)$
2. $(4 * 4) * (3 * 3)$
3. $1 * (2 * (3 * 4))$

บทนิยาม 1.5.8 ให้ $*$ เป็นการดำเนินการทวิภาคบนเซต G และให้ $A \subseteq G$ ถ้า

$$a * b \in A \qquad \text{ทุก ๆ } a, b \in A$$

แล้วจะกล่าวว่า เซต A มี**สมบัติปิด** (closed) ภายใต้ $*$ หรือ $*$ มีสมบัติปิดบนเซต A

เห็นได้ว่าการบวกและการคูณมีสมบัติปิดบนเซตจำนวนจริง จำนวนเต็ม และจำนวนตรรกยะ

ตัวอย่าง 1.5.9 ให้ $\mathbb{E} = \{0, \pm 2, \pm 4, \pm 6, ...\}$ และ $\mathbb{O} = \{\pm 1, \pm 3, \pm 5, ...\}$ จงตรวจสอบว่า $\mathbb{E}$ และ $\mathbb{O}$ มีสมบัติปิดภายใต้การบวกและการคูณหรือไม่

ตัวอย่าง 1.5.10 พิจารณาการดำเนินการต่อไปนี้ว่ามีสมบัติปิดบนเซต $\mathbb{N}$ หรือไม่

1. $a * b = a + b + 1$
2. $a * b = a + b - 2$

สามารถตรวจสอบสมบัติปิดโดยใช้ตารางเคย์เลย์ได้ดังนี้ตัวอย่างต่อไปนี้

ตัวอย่าง 1.5.11 จงใช้ตารางเคย์เลย์ตรวจสอบสมบัติปิดของตัวดำเนินการทวิภาคต่อไปนี้

1. $a * b = \sqrt[3]{ab}$ บน $A = \{-1, 0, 1\}$

2. $B = \{1,\ \sqrt{2}+1, \sqrt{2}-1\}$ กับการคูณ

บทนิยาม 1.5.12 ให้ $*$ เป็นการดำเนินการทวิภาคบนเซต G ถ้า

$$a * b = b * a \qquad \text{ทุก ๆ } a, b \in G$$

จะกล่าวว่าเซต G มี**สมบัติการสลับที่** (commutative law) ภายใต้ $*$ หรือ $*$ มีสมบัติการสลับที่บนเซต G

เห็นได้ว่าการบวกและการคูณมีสมบัติการสับที่บนเซตจำนวนจริง จำนวนเต็ม และจำนวนตรรกยะ

ตัวอย่าง 1.5.13 พิจารณาการดำเนินทวิภาคต่อไปนี้มีสมบัติการสลับที่หรือไม่

1. กำหนดให้ $a * b = a + b + 5$ เมื่อ $a, b \in \mathbb{N}$

2. กำหนดให้ $a * b = a^2 + ab$ เมื่อ $a, b \in \mathbb{Z}$

การตรวจสอบสมบัติการสลับที่จากตารางเคย์เลย์ ทำได้โดยลากเส้นผ่านแนวทแยงจากซ้ายบนไปยังขวาล่างถ้าค่าแต่ละค่าในตารางสมมาตรกันผ่านเส้นทแยงจะได้สรุปได้ว่าการดำเนินการนั้นมีสมบัติปิด

ตัวอย่าง 1.5.14 กำหนดตารางเคย์เลย์ของการดำเนินทวิภาค $*$

1. นิยาม $*$ บน $G_1 = \{0, 1, 2\}$ ดังนี้

$*$	0	1	2
0	2	0	0
1	0	1	2
2	1	2	2

2. นิยาม $\star$ บน $G_2 = \{1, 2, 3\}$ ดังนี้

$\star$	1	2	3
1	1	3	2
2	3	2	1
3	2	1	3

บทนิยาม 1.5.15 ให้ $*$ เป็นการดำเนินการทวิภาคบนเซต G ถ้า

$$a * (b * c) = (a * b) * c \qquad \text{ทุก ๆ } a, b, c \in G$$

แล้วจะกล่าวว่า เซต G มี**สมบัติการเปลี่ยนกลุ่ม** (associative law) ที่ภายใต้ $*$ หรือ $*$ มีสมบัติการเปลี่ยนกลุ่มที่บนเซต G

เห็นได้ว่าการบวกและการคูณมีสมบัติการเปลี่ยนกลุ่มบนเซตจำนวนจริง จำนวนเต็ม และจำนวนตรรกยะ

ตัวอย่าง 1.5.16 จงตรวจสอบสมบัติการเปลี่ยนกลุ่มของการดำเนินทวิภาคต่อไปนี้

1. กำหนดให้ $a * b = a + b + 1$ เมื่อ $a, b \in \mathbb{N}$

2. กำหนดให้ $a * b = a + 2b$ เมื่อ $a, b \in \mathbb{Z}$

บทนิยาม 1.5.17 ให้ $*$ เป็นการดำเนินการทวิภาคบนเซต G ถ้ามี $e \in G$ ซึ่งสอดคล้อง

$$a * e = a = e * a \qquad \text{ทุก ๆ } a \in G$$

แล้วจะกล่าวว่าเซต G มี e เป็น **เอกลักษณ์** (identity) ภายใต้ $*$

สำหรับเซตจำนวนจริงการบวกมี 0 เป็นเอกลักษณ์ และการคูณมี 1 เป็นเอกลักษณ์

ตัวอย่าง 1.5.18 จากตารางเคย์เลย์

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

จงหาเอกลักษณ์ของ $\{1, 2, 3\}$ ภายใต้ $*$

ตัวอย่าง 1.5.19 จงหาเอกลักษณ์ (ถ้ามี) ของการดำเนินบนเซตในแต่ละข้อต่อไปนี้

1. ให้ $a * b = a + b - 7$ เมื่อ $a, b \in \mathbb{Z}$

2. ให้ $a * b = 7ab$ เมื่อ $a, b \in \mathbb{Z}$

3. ให้ $a * b = a - 2b$ เมื่อ $a, b \in \mathbb{Q}$

ทฤษฎีบท 1.5.20 ถ้า G มีเอกลักษณ์ภายใต้การดำเนินการ $*$ จะมีได้เพียงตัวเดียวเท่านั้น

บทนิยาม 1.5.21 ให้ $*$ เป็นการดำเนินการทวิภาคบนเซต G ที่มี e เป็นเอกลักษณ์ ถ้า $a \in G$ และ

$$\text{มี } b \in G \text{ ซึ่ง} \qquad a * b = e = b * a$$

จะกล่าวว่า b ว่า**ตัวผกผัน (inverse)** ของ a ภายใต้ $*$ หรือเรียกสั้น ๆ ว่า b เป็นตัวผกผันของ a เขียนสัญลักษณ์ด้วย a^{-1}

ข้อสังเกต 1.5.22 ถ้า b เป็นตัวผกผันของ a ภายใต้ $*$ แล้ว a เป็นตัวผกผันของ b ภายใต้ $*$ เช่นกัน

ตัวอย่าง 1.5.23 จงหาตัวผกผัน (ถ้ามี) ของสมาชิกทุกตัวจากตารางเคย์เลย์

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

ตัวอย่าง 1.5.24 ให้ $G = \{-1, 1, -i, i\}$ เมื่อ $i = \sqrt{-1}$ กับการคูณ แสดงตารางเคย์เลย์ได้ดังนี้

$\times$	-1	1	$-i$	i
-1				
1				
$-i$				
i				

จงหาตัวผกผันของสมาชิแต่ละตัว

ตัวอย่าง 1.5.25 กำหนดให้ $a * b = a + b - 7$ สำหรับ $a, b \in \mathbb{Z}$ จงหาตัวผกผันของ

1. 2
3. 19
2. 14
4. $x \in \mathbb{Z}$

ทฤษฎีบท 1.5.26 ให้ $n \in \mathbb{N}$ สำหรับ $\bar{a}, \bar{b} \in \mathbb{Z}_n$ โดยที่

$$\bar{a} + \bar{b} = \overline{a + b} \qquad \text{และ} \qquad \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

เป็นการดำเนินการทวิภาคบน $\mathbb{Z}_n$ และเรียกว่าการบวกและการคูณบน $\mathbb{Z}_n$ ตามลำดับ

จากทฤษฎีบท 1.5.26 พิสูจน์ได้โดยง่ายว่าการบวกและการคูณบน $\mathbb{Z}_n$ มีสมบัติการสลับที่และเปลี่ยนกลุ่ม โดยมี $\bar{0}$ เป็นเอกลักษณ์การบวก $\bar{1}$ เป็นเอกลักษณ์การคูณ

ตัวอย่าง 1.5.27 จงหาตัวผกผันสำหรับการบวกและการคูณของแต่ละสมาชิกใน $\mathbb{Z}_5$

สมาชิก	ตัวผกผัน การบวก	เหตุผล
$\bar{0}$		
$\bar{1}$		
$\bar{2}$		
$\bar{3}$		
$\bar{4}$		

สมาชิก	ตัวผกผันการคูณ การคูณ	เหตุผล
$\bar{0}$		
$\bar{1}$		
$\bar{2}$		
$\bar{3}$		
$\bar{4}$		

แบบฝึกหัด 1.5

1. จงตรวจสอบสมบัติปิดของการดำเนินการทวิภาค $*$ บนเซต A ต่อไปนี้

   1.1 นิยาม $a*b=\dfrac{a^2-ab-2b^2}{a+b}$ บน $A=\mathbb{N}$

   1.2 นิยาม $a*b=\dfrac{(a+b)^2-(a+b)}{2}$ บน $A=\mathbb{N}$

   1.3 นิยาม $a*b=$ เศษที่เหลือจากการหาร $a+b$ ด้วย 7 บน $A=\{0,1,2,3,4,5,6\}$

   1.4 นิยาม $a*b=(2^a)(2^b)$ บน $A=\{0,2,4,6,8,...\}$

   1.5 นิยาม $a*b=\dfrac{a+b}{a+b+1}$ บน $A=[0,1]$

2. จงตรวจสอบสมบัติสลับที่และเปลี่ยนกลุ่ม พร้อมหาเอกลักษณ์และตัวผกผัน ของการดำเนินการทวิภาค $*$ บนเซต G ต่อไปนี้

   2.1 $G=\mathbb{Z}$ นิยาม $a*b=a^2b+ab^2$

   2.2 $G=\mathbb{R}$ นิยาม $a*b=a(-1)^b+b(-1)^a$

   2.3 $G=\mathbb{Q}^+$ นิยาม $a*b=a\sqrt{b}+b\sqrt{a}$

   2.4 $G=\mathbb{R}^+$ นิยาม $a*b=\dfrac{a^2+ab}{a+b+ab}$

   2.5 $G=\mathbb{Q}$ นิยาม $a*b=8ab$

   2.6 $G=\mathbb{Z}$ นิยาม $a*b=2a+2b$

   2.7 $G=\mathbb{R}^+$ นิยาม $a*b=\dfrac{1}{a}+\dfrac{1}{b}$

   2.8 $G=\mathbb{Z}$ นิยาม $a*b=1-a-b$

   2.9 $G=\mathbb{Z}$ นิยาม $a*b=a+b-\pi$

   2.10 $G=\mathbb{Q}$ นิยาม $a*b=5ab$

   2.11 $G=\mathbb{R}$ นิยาม $a*b=ab+1$

   2.12 $G=\mathbb{R}$ นิยาม $a*b=a+2b$

   2.13 $G=\mathbb{Q}^c$ นิยาม $a*b=a+b\sqrt{2}$

   2.14 $G=\mathbb{R}$ นิยาม $a*b=a+b+ab$

   2.15 $G=\mathbb{R}^+$ นิยาม $a*b=\sqrt{a}+\sqrt{b}$

   2.16 $G=\mathbb{R}^+$ นิยาม $a*b=\dfrac{a+b}{\sqrt{a}+\sqrt{b}}$

3. จงหาตัวผกผันของ $-\frac{2}{3}, -2, 0, 1, \frac{1}{2}$ และจำนวนตรรกยะทุกตัวมีตัวผกผันหรือไม่ ของการดำเนินการ

$$\text{นิยาม } a*b=-ab \quad \text{สำหรับ } a,b\in\mathbb{Q}$$

4. กำหนดให้ $x\circledcirc(x-y)=x^2+y^2$ เมื่อ $x,y\in\mathbb{R}$ จงหาค่าของ $20\circledcirc(5\circledcirc 3)$

5. กำหนดให้ $a\odot b=2a+3b$ เมื่อ $a,b\in\mathbb{Q}$ ถ้ามี $x,y,z\in\mathbb{Q}$ ซึ่ง $x\odot(y\odot z)=(x\odot y)\odot z$ และ $x\odot z=3$ จงหาค่าของ $z\odot(y\odot x)-(z\odot y)\odot x$

6. กำหนดให้ $a\otimes b=a(a+b)$ เมื่อ $a,b\in\mathbb{Z}^+$ ถ้า $a\otimes b=55$ แล้วค่ามากสุดของ $b\otimes a$ มีค่าเท่าใด

7. กำหนดให้ $a\oplus b=a+b+2$ เมื่อ $a,b\in\mathbb{Z}$ จงหาตัวผกผันของ 4 ภายใต้ $\oplus$

8. กำหนดให้ $a,b,c\in\mathbb{R}$ ถ้ามี a เป็นอินเวอร์สการบวกของ b จงหา c ที่ทำให้

$$4a+4b-2c+12=0$$

9. จงหาตัวผกผันภายใต้การคูณของ $\sqrt{a+1}-\sqrt{a}$ เมื่อ $a>0$

บทที่ 2

กรุป

พื้นฐานที่สำคัญทางพีชคณิตนามธรรมคือการศึกษาโครงสร้างพีชคณิตที่เรียกว่า **กรุป** (group) โดยการพิจารณาสมบัติของการดำเนินทวิภาคบนเซตที่สนใจ ดังจะกล่าวในหัวข้อเริ่มต้น และยกตัวอย่างต่าง ๆ ที่หลากหลายของกรุป ศึกษาสมบัติเบื้องต้นเกี่ยวกับกรุป และศึกษากรุปสมมาตรซึ่งเป็นตัวอย่างของกรุปสลับที่ไม่ได้แบบจำกัด

2.1 นิยามและตัวอย่างของกรุป

บทนิยาม 2.1.1 กรุป (Group) หมายถึงเซต G กับการดำเนินการทวิภาค $*$ เขียนแทนด้วยคู่อันดับ $(G, *)$ ที่มีสมบัติ 3 ข้อต่อไปนี้

1. **สมบัติการเปลี่ยนกลุ่ม** กล่าวคือ

$$a * (b * c) = (a * b) * c \qquad \text{สำหรับทุก ๆ } a, b, c \in G$$

2. **การมีเอกลักษณ์** กล่าวคือ มี $e \in G$ ซึ่ง

$$a * e = a = e * a \qquad \text{สำหรับทุก ๆ } a \in G$$

   เรียก e ว่าเอกลักษณ์ใน G

3. **การมีตัวผกผัน** กล่าวคือ ทุก ๆ $a \in G$ จะมี $b \in G$ ซึ่ง

$$a * b = e = b * a$$

   เรียก b ว่าตัวผกผันของ a เขียนแทนด้วย a^{-1}

ถ้า $(G, *)$ มีสมบัติข้อที่ 1 เท่านั้นเรียกว่า **กึ่งกรุป** (semigroup) ถ้ามีสมบัติข้อที่ 1 และข้อที่ 2 เรียกว่า **โมนอยด์** (monoid)

บทนิยาม 2.1.2 ถ้า $(G, *)$ มีสมบัติการสลับที่ นั่นคือ

$$a * b = b * a \qquad \text{สำหรับทุก ๆ } a, b \in G$$

เรียก $(G, *)$ ว่า**กรุปสลับที่** (commutative group) หรือ **กรุปอาบีเลียน** (abelian group) ซึ่งตั้งชื่อเพื่อเป็นเกียรติให้กับนักคณิตศาสตร์ชาวนอร์เวย์นามว่า นีลส์ อาเบล (Niels Abel)

บทนิยาม 2.1.3 ถ้า $(G, *)$ เป็นกรุปโดยที่ G เป็นเซตจำกัด เรียกว่า **กรุปจำกัด** (finite group) ถ้าสนใจจำนวนสมาชิกของเซต G จะกล่าวว่า $(G, *)$ เป็น**กรุปจำกัดอันดับ** $|G|$ (finite group of order $|G|$) ถ้า G เป็นเซตอนันต์เรียก $(G, *)$ ว่า **กรุปอนันต์** (infinite group)

ต่อไปคือตารางแสดงการมีสมบัติกับการเป็นกรุปของเซตที่เราคุ้นเคยกับการบวกและการคูณ

คู่อันดับ	สมบัติ การเปลี่ยนกลุ่ม	เอกลักษณ์	การมี ตัวผกผัน	ชนิด
$(\mathbb{Z}, +)$				
$(\mathbb{Q}, +)$				
$(\mathbb{R}, +)$				
$(\mathbb{C}, +)$				
$(\mathbb{Z}^+, +)$				
$(\mathbb{Q}^+, +)$				
$(\mathbb{R}^+, +)$				

คู่อันดับ	สมบัติ การเปลี่ยนกลุ่ม	เอกลักษณ์	การมี ตัวผกผัน	ชนิด
$(\mathbb{Z}, \cdot)$				
$(\mathbb{Q}, \cdot)$				
$(\mathbb{R}, \cdot)$				
$(\mathbb{C}, \cdot)$				
$(\mathbb{Z}^+, \cdot)$				
$(\mathbb{Q}^+, \cdot)$				
$(\mathbb{R}^+, \cdot)$				
$(\mathbb{Z}^*, \cdot)$				
$(\mathbb{Q}^*, \cdot)$				
$(\mathbb{R}^*, \cdot)$				
$(\mathbb{C}^*, \cdot)$				

ข้อสังเกต 2.1.4 $(\{0\}, +)$ เป็นกรุปการบวกที่เล็กที่สุด และ$(\{1\}, \cdot)$ เป็นกรุปการคูณที่เล็กที่สุด ซึ่งทั้งคู่เป็นกรุปแบบจำกัดอันดับ 1

ตัวอย่าง 2.1.5 จงตรวจสอบว่า $(\{-1, 1\}, \cdot)$ เป็นกรุปหรือไม่

ตัวอย่าง 2.1.6 จงตรวจสอบว่า $(G, \cdot)$ เป็นกรุปหรือไม่ โดยที่ $G = \{-1, 1, i, -i\}$ เมื่อ $i^2 = -1$

ตัวอย่าง 2.1.7 กำหนดให้

$$a * b = a + b + 2 \qquad \text{เมื่อ } a, b \in \mathbb{Z}$$

จงแสดงว่า $(\mathbb{Z}, *)$ เป็นกรุปอาบีเลียน

ตัวอย่าง 2.1.8 กำหนดให้

$$a * b = 3ab \qquad \text{เมื่อ } a, b \in \mathbb{Q}^+$$

แล้ว $(\mathbb{Q}^+, *)$ เป็นกรุปหรือไม่เพราะเหตุใด

ตัวอย่าง 2.1.9 กำหนดให้

$$a * b = a + b + ab \qquad \text{เมื่อ } a, b \in \mathbb{R}$$

จงแสดงว่า $(\mathbb{R}, *)$ เป็นโมนอยด์

ตัวอย่าง 2.1.10 ถ้า $G = (-1, 1)$ กำหนดให้

$$a * b = \frac{a+b}{ab+1} \qquad \text{ทุก ๆ } a, b \in G$$

แล้ว $(G, *)$ เป็นกรุปหรือไม่

ตัวอย่าง 2.1.11 ให้ $G = \{e, a\}$ และ e เป็นเอกลักษณ์ใน G ซึ่ง $a * a = e$
จงแสดงว่า $(G, *)$ เป็นกรุปแบบจำกัดอันดับ 2

กรุปไคลน์โฟว์

ต่อไปจะพิจารณากรุปลักษณะเดียวกันกับตัวอย่าง 2.1.11 แต่เพิ่มอันดับเป็น 4
ให้ $K_4 = \{e, a, b, c\}$ และ e เป็นเอกลักษณ์ใน K_4 ซึ่ง

$$a * a = b * b = c * c = a * b * c = e$$

แล้ว $(K_4, *)$ เป็นกรุป จะเรียกว่า **กรุปไคลน์โฟว์ (Klein 4-group)** ซึ่งจะเห็นว่าทุกสมาชิกในกรุปมีตัวผกผันของตัวเอง

พิจารณา

$$\begin{aligned} a * (a * b * c) * a &= a * e * a = a * a = e \\ (a * a) * (b * c * a) &= e \\ e * (b * c * a) &= e \\ b * c * a &= e \end{aligned}$$

ในทำนองเดียวกันจะได้ว่า $c * a * b = e$, $a * c * b = e$ และ $b * a * c = e$ จะได้ว่า

$$\begin{aligned} a * b &= (a * b) * e = (a * b) * (c * c) = (a * b * c) * c = e * c = c \\ a * c &= \\ b * a &= \\ b * c &= \\ c * a &= \\ c * b &= \end{aligned}$$

แสดงผลของการดำเนินการดังตาราง

$*$	e	a	b	c
e				
a				
b				
c				

สรุปได้ด้วยว่ากรุปไคลน์โฟว์เป็นกรุปอาบีเลียน

กรุปควอเทอร์เนียน

กำหนดให้ $Q_8 = \{1, -1, i, -i, j - j, k, -k\}$ นิยามการดำเนินการ $*$ ดังนี้

$$1 * a = a = a * 1 \text{ และ } (-1) * a = -a * (-1) = a \text{ สำหรับทุก } a \in Q_8$$

และ

$$\begin{gathered}(-1) * (-1) = 1, \qquad i * i = j * j = k * k = -1, \\ i * j = k, \qquad j * k = i, \qquad k * i = j, \\ j * i = -k, \qquad k * j = -i \qquad \text{และ} \qquad i * k = -j\end{gathered}$$

แล้ว $(Q_8, *)$ เป็นกรุป ซึ่งเรียกว่า **กรุปควอเทอร์เนียน** (Quaternion Group)
และเห็นได้ว่า Q_8 ไม่เป็นอาบีเลียนกรุป

กรุปของจำนวนเต็มมอดุโล n

ต่อไปจะพิจารณากรุปบนเซตของจำนวนเต็มมอดุโล n หรือ $\mathbb{Z}_n$ จากทฤษฎีบท 1.5.26 จะได้ว่า

$$\bar{a} + \bar{b} = \overline{a+b} \qquad \text{และ} \qquad \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

เป็นการดำเนินการทวิภาค และเรียกว่าการบวกและการคูณใน $\mathbb{Z}_n$ ตามลำดับ

ทฤษฎีบท 2.1.12 $(\mathbb{Z}_n, +)$ เป็นกรุปอาบีเลียนแบบจำกัด

ตัวอย่าง 2.1.13 จงหาตัวผกผันของทุกสมาชิกใน $(\mathbb{Z}_8, +)$

วิธีทำ แสดงได้ดังตาราง

สมาชิก	ตัวผกผันการบวก	เหตุผล
$\bar{0}$		
$\bar{1}$		
$\bar{2}$		
$\bar{3}$		
$\bar{4}$		
$\bar{5}$		
$\bar{6}$		
$\bar{7}$		

ทฤษฎีบท 2.1.14 $\mathbb{Z}_n$ มีสมบัติการสลับที่และสมบัติการเปลี่ยนกลุ่มภายใต้การคูณ และมี $\bar{1}$ เป็นเอกลักษณ์การคูณ

กำหนดให้ $\mathbb{Z}_n^*$ แทนเซตของจำนวนเต็มมอดุโลที่สมาชิกไม่ใช่ $\bar{0}$ นั่นคือ

$$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : x \neq \bar{0}\}$$

ตัวอย่าง 2.1.15 จงตรวจสอบว่า $\mathbb{Z}_4^*$ และ $\mathbb{Z}_5^*$ เป็นกรุปการคูณหรือไม่

ทฤษฎีบท 2.1.16 $(\mathbb{Z}_p^*, \cdot)$ เป็นกรุปอาบีเลียนแบบจำกัดอันดับ $p-1$

ตัวอย่าง 2.1.17 จงหาตัวผกผันการคูณของแต่ละสมาชิกใน $\mathbb{Z}_p^*$ เมื่อ $p = 2, 3$

วิธีทำ แสดงได้ดังตารางต่อไปนี้

เซตและสมาชิก	ตัวผกผันการคูณ	เหตุผล
$\mathbb{Z}_2^*$		
$\bar{1}$		
$\mathbb{Z}_3^*$		
$\bar{1}$		
$\bar{2}$		

ต่อไปจะเป็นตารางของตัวผกผันการคูณของแต่สมาชิกใน $(\mathbb{Z}_p^*, \cdot)$ เมื่อ $p = 2, 3, 5, 7$

เซตและสมาชิก	ตัวผกผันการคูณ	เหตุผล
$\mathbb{Z}_5^*$	$\bar{1}$	$\bar{1} \cdot \bar{1} = \bar{1}$
$\bar{1}$		
$\bar{2}$		
$\bar{3}$		
$\bar{4}$		
$\mathbb{Z}_7^*$	$\bar{1}$	$\bar{1} \cdot \bar{1} = \bar{1}$
$\bar{1}$		
$\bar{2}$		
$\bar{3}$		
$\bar{4}$		
$\bar{5}$		
$\bar{6}$		
$\mathbb{Z}_{11}^*$		
$\bar{1}$	$\bar{1}$	$\bar{1} \cdot \bar{1} = \bar{1}$
$\bar{2}$		
$\bar{3}$		
$\bar{4}$		
$\bar{5}$		
$\bar{6}$		
$\bar{7}$		
$\bar{8}$		
$\bar{9}$		
$\overline{10}$		

ตัวอย่าง 2.1.18 จงหาตัวผกผันการคูณของ $\overline{13}$ ใน $(\mathbb{Z}_{23}^*, \cdot)$

จากนี้เราจะขยายกรุปอาบีเลียน $\mathbb{Z}_p^*$ ไปยังกรณี $\mathbb{Z}_n^*$ โดยการเลือกสมาชิกใน $\mathbb{Z}_n^*$ ที่มีตัวผกผันการคูณเท่านั้น นั่นคือ $\bar{a} \in \mathbb{Z}_n^*$ จะมีตัวผกผันการคูณน่าจะสอดคล้องกับเงื่อนไข

$$\text{gcd}(a, n) = 1$$

ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.1.19 ให้ $\bar{a}$ เป็นสมาชิกใน $\mathbb{Z}_n^*$ จะได้ว่า

$$\bar{a} \quad \text{มีตัวผกผันการคูณ} \qquad \text{ก็ต่อเมื่อ} \qquad \text{gcd}(a, n) = 1$$

บทแทรก 2.1.20 กำหนดให้

$$\mathbb{Z}_n^\times = \{\bar{a} \in \mathbb{Z}_n \,:\, 0 < a < n \text{ และ } \mathrm{gcd}(a, n) = 1\}$$

แล้ว $(\mathbb{Z}_n^\times, \cdot)$ เป็นกรุปอาบีเลียนอันดับ $\phi(n)$

ตารางต่อไปนี้จะแสดงตัวอย่างการแจกแจงสมาชิกของ $\mathbb{Z}_n^\times$ เมื่อ $n = 2, 3, 4, ..., 10$

เซต	สมาชิก	จำนวนสมาชิก
$\mathbb{Z}_2^*$	$\{\bar{1}\}$	$\phi(2) = 1$
$\mathbb{Z}_3^*$	$\{\bar{1}, \bar{2}\}$	$\phi(3) = 2$
$\mathbb{Z}_4^*$	$\{\bar{1}, \bar{3}\}$	$\phi(4) = 2$
$\mathbb{Z}_5^*$	$\{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$	$\phi(5) = 4$
$\mathbb{Z}_6^*$	$\{\bar{1}, \bar{5}\}$	$\phi(6) = 2$
$\mathbb{Z}_7^*$	$\{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$	$\phi(7) = 6$
$\mathbb{Z}_8^*$	$\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$	$\phi(8) = 4$
$\mathbb{Z}_9^*$	$\{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$	$\phi(9) = 6$
$\mathbb{Z}_{10}^*$	$\{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$	$\phi(10) = 4$

ตัวอย่าง 2.1.21 จงหาจำนวนสมาชิกของ $\mathbb{Z}_{2500}^\times$

ตัวอย่าง 2.1.22 จงหาตัวผกผันการคูณของ $\overline{51}$ ใน $(\mathbb{Z}_{100}^\times, \cdot)$

กรุปของเมทริกซ์

เมทริกซ์ (Matrix) คือสี่เหลี่ยมผืนผ้าของจำนวนจริง หรือสมาชิกในริง (จะกล่าวถึงในบทที่ 6) โดยแนวนอนเรียกว่า **แถว** (row) แนวตั้งเรียกว่า **หลัก** (column) และเรียกจำนวนแถว $\times$ จำนวนหลักว่าขนาดของเมทริกซ์ ตัวอย่างเช่น

$$\begin{bmatrix} -1 & 3 & 0 & 2 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

เป็นเมทริกซ์ขนาด 2×4 เนื่องจากมี 2 แถว และ 4 หลัก รูปแบบทั่วไปของเมกทริกซ์ขนาด $m \times n$ เขียนได้เป็น

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

นิยมใช้อักษรภาษาอังกฤษตัวพิมพ์ใหญ่แทนเมทริกซ์ เช่นเมทริกซ์ A ขนาด $m \times n$ เขียนแทนด้วย

$$[a_{ij}]_{m\times n} \qquad \text{หรือ} \qquad [a_{ij}]$$

โดยที่ a_{ij} คือค่าของตัวเลขในแถวที่ i หลักที่ j และในกรณีที่จำนวนแถวเท่ากับจำนวนหลัก เรียกว่า **เมทริกซ์จตุรัส** (square matrix)

การเท่ากันของสองเมทริกซ์หมายถึงเมทริกซ์ที่มีขนาดเดียวกันและทุกตำแหน่งในเมทริกซ์ทั้งสองเท่ากัน และ**เมทริกซ์ศูนย์** (zero matrix) หมายถึงทุกตำแหน่งมีค่าเป็นศูนย์เขียนแทนด้วย $\underline{0}$

บทนิยาม 2.1.23 ให้ $A = [a_{ij}]$ และ $B = [b_{ij}]$ เป็นเมทริกซ์ที่มีขนาดเดียวกัน และ c เป็นจำนวนจริง แล้วนิยาม

1. $A + B = [a_{ij} + b_{ij}]$
2. $A - B = [a_{ij} - b_{ij}]$
3. $cA = [ca_{ij}]$

กำหนดให้เซตของเมทริกซ์ขนาด $m \times n$ เขียนแทนด้วย

$$M_{mn}(\mathbb{R}) = \{[a_{ij}]_{m\times n} \,:\, a_{ij} \in \mathbb{R}\}$$

ทฤษฎีบท 2.1.24 ให้ A และ B เป็นเมทริกซ์ที่มีขนาด $m \times n$ และ $\underline{0} = [0]_{m\times n}$ จะได้ว่า

1. $A + B = B + A$
2. $(A + B) + C = A + (B + C)$
3. $A + \underline{0} = A = \underline{0} + A$
4. $A + (-A) = \underline{0} = (-A) + A$

ทฤษฎีบท 2.1.25 $(M_{mn}(\mathbb{R}), +)$ เป็นกรุปอาบีเลียน

บทนิยาม 2.1.26 ให้ $A = [a_{ij}]$ เป็นเมทริกซ์ขนาด $m \times r$ และ $B = [b_{ij}]$ เป็นเมทริกซ์ขนาด $r \times n$ แล้ว

$$AB = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ir} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mr} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} & \cdots b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots b_{2n} \\ \vdots & \vdots & & \vdots & \vdots \\ b_{r1} & b_{r2} & \cdots & b_{rj} & \cdots b_{rn} \end{bmatrix} = [c_{ij}]_{m\times n}$$

โดยที่ $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ir}b_{rj}$

ตัวอย่าง 2.1.27 กำหนดให้

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \end{bmatrix} \qquad \text{และ} \qquad B = \begin{bmatrix} 2 & 3 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}$$

จงหา AB และ BA

วิธีทำ

$$AB = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 1 & 1 \\ 1 & 0 \end{bmatrix} =$$

$$BA = \begin{bmatrix} 2 & 3 \\ 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \end{bmatrix} =$$

จากตัวอย่าง 2.1.27 แสดงให้เห็นว่า AB ไม่เท่ากับ BA สำหรับ A, B และ C เป็นเมทริกซ์จตุรัสที่มีขนาดเดียวกัน จากสมบัติการคูณของเมทริกซ์จะได้ว่า

$$A(BC) = (AB)C$$

และนิยาม I เป็นเมทริกซ์เอกลักษณ์การคูณซึ่งมีขนาด $n \times n$ โดยที่

$$I = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$

ดังนั้นสำหรับเมทริกซ์ A ขนาด $n \times n$ จะได้ว่า $AI = A = IA$ ทำให้ได้ว่า $(M_{nn}(\mathbb{R}), \cdot)$ เป็นโมนอยด์

สำหรับเมทริกซ์ $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ เมื่อ $ad - bc \neq 0$ จะได้ว่า A มีตัวผกผันการคูณ เขียนแทนด้วย A^{-1} โดยที่

$$A^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

และเรียกค่า $ad - bc$ ว่า **ดีเทอร์มิแนนท์** (determinant) ของเมทริกซ์ A เขียนแทนด้วย $\det(A)$ ในทางเมทริกซ์จะนิยามดีเทอร์มิแนนท์สำหรับเมทริกซ์จตุรัสเท่านั้น และสามารถพิสูจน์

$$\text{เมเทริกซ์จตุรัส } A \text{ มีตัวผกผันการคูณ} \quad \text{ก็ต่อเมื่อ} \quad \det(A) \neq 0$$

จากสมบัติดังกล่าวทำให้ได้ข้อสรุปตามทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.1.28 $(GL_n(\mathbb{R}), \cdot)$ เป็นกรุป โดยที่

$$GL_n(\mathbb{R}) = \{A \in M_{nn}(\mathbb{R}) \,:\, \det(A) \neq 0\}$$

และเรียกว่า **กรุปเชิงเส้นทั่วไป** (the general linear group)

จะเห็นได้ว่ากรุปเชิงเส้นทั่วไปไม่เป็นกรุปอาบีเลียน เนื่องจากการคูณของเมทริกซ์ไม่มีสมบัติการสลับที่ แต่เมื่อจำกัดสมาชิกของกรุปและมีสมบัติสอดคล้องนิยามของกรุปไคลน์โฟว์จะได้กรุปอาบีเลียนดังตัวอย่างต่อไปนี้

ตัวอย่าง 2.1.29 ให้ $G = \{I, A, B, C\}$ ซึ่ง

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{และ} \quad C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

จงแสดงว่า $(G, \cdot)$ เป็นกรุปไคลน์โฟว์

กรุปของฟังก์ชัน

สำหรับ $A \subseteq \mathbb{R}$ โดยที่ $A \neq \varnothing$ กำหนดให้

$$C[A] = \{f : A \to \mathbb{R} \ : \ f \text{ เป็นฟังก์ชันต่อเนื่อง } \}$$

ให้ $f : A \to \mathbb{R}$ และ $g : A \to \mathbb{R}$ นิยามการบวกการคูณดังนี้

$$(f+g)(x) = f(x) + g(x) \quad \text{และ} \quad (f \cdot g)(x) = f(x) \cdot g(x) \qquad \text{ทุก ๆ } x \in A$$

ถ้า f, g เป็นฟังก์ชันต่อเนื่อง โดยสมบัติของฟังก์ชันจะได้ว่า $f + g$ และ fg เป็นฟังก์ชันต่อเนื่อง

ทฤษฎีบท 2.1.30 $(C[A], +)$ เป็นกรุปอาบีเลียน และ$(C[A], \cdot)$ เป็นโมนอยด์

ให้ $A \subseteq \mathbb{R}$ โดยที่ $A \neq \varnothing$ กำหนดให้

$$S_A = \{f : A \to A \ : \ f \text{ เป็นฟังก์ชัน 1-1 แบบทั่วถึง } \}$$

ตัวอย่าง 2.1.31 $(S_A, +)$ และ $(S_A, \cdot)$ เป็นกรุปหรือไม่

พิจารณาการดำเนินการคอมโพสิทตามบทนิยาม 1.4.16 นั่นคือ

$$(f \circ g)(x) = f(g(x))$$

ถ้า $f, g, h : A \to A$ เป็นฟังก์ชัน 1-1 แบบทั่วถึง โดยสมบัติของฟังก์ชันจะได้ว่า $f \circ g$ เป็นฟังก์ชัน 1-1 แบบทั่วถึง และ f^{-1} เป็นฟังก์ชัน 1-1 แบบทั่วถึง และ

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

การพิสูจน์เว้นไว้เป็นแบบฝึกหัด

จากสมบัติที่ได้ดังกล่าวทำให้ได้ว่าทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.1.32 $(S_A, \circ)$ เป็นกรุป ซึ่งเรียกว่า **กรุปสมมาตร** (symmetric group)

ข้อสังเกต 2.1.33 ถ้า A เป็นเซตจำกัด โดยที่ $|A| \geq 3$ จะได้ว่า $(S_A, \circ)$ เป็นกรุปไม่สลับที่แบบจำกัด

กรุปของเซตย่อย

สำหรับเซต D นิยาม $\mathcal{P}(D) = \{X : X \subseteq D\}$ เรียกว่า **เซตกำลัง** (power set) ของ D แล้วจะได้ว่าการดำเนินการ $\cup$, $\cap$ และ $-$ เป็นการดำเนินการทวิภาคบน $\mathcal{P}(D)$

ตัวอย่าง 2.1.34 ให้ $D \neq \varnothing$ จงตรวจสอบว่าข้อใดต่อไปนี้เป็นกรุป

1. $(\mathcal{P}(D), \cup)$

2. $(\mathcal{P}(D), \cap)$

3. $(\mathcal{P}(D), -)$

ให้ A และ B เป็นเซต นิยาม **ผลต่างสมมาตร** (symmetric difference) ของ A และ B เขียนแทนด้วย $A \bigtriangleup B$ โดย

$$A \bigtriangleup B = (A - B) \cup (B - A)$$

จะเห็นได้ว่า $B \bigtriangleup A = (B - A) \cup (A - B) = (A - B) \cup (B - A) = A \bigtriangleup B$ ดังนั้นผลต่างสมมาตรมีสมบัติการสลับที่ และ $\bigtriangleup$ เป็นการดำเนินการทวิภาคบน $\mathcal{P}(D)$

ทฤษฎีบท 2.1.35 ผลต่างสมมาตรมีสมบัติการเปลี่ยนกลุ่ม

ทฤษฎีบท 2.1.36 ให้ $D \neq \varnothing$ แล้ว $(\mathcal{P}(D), \bigtriangleup)$ เป็นกรุปอาบีเลียน

แบบฝึกหัด 2.1

1. พิจารณา $(G, *)$ ที่กำหนดให้ต่อไปนี้ เป็นกรุป กึ่งกรุป หรือโมนอยด์

   1.1 $G = \mathbb{Z}$ นิยาม $a * b = a + b - 3$

   1.2 $G = \mathbb{Z}$ นิยาม $a * b = a + 2b$

   1.3 $G = \mathbb{R}^*$ นิยาม $a * b = 5ab$

   1.4 $G = \mathbb{Q}$ นิยาม $a * b = \dfrac{ab}{4}$

   1.5 $G = \mathbb{Q}$ นิยาม $a * b = \dfrac{a+b}{7}$

   1.6 $G = \mathbb{Q}^+$ นิยาม $a * b = \dfrac{3a}{b}$

   1.7 $G = \mathbb{N}$ นิยาม $a * b = \min\{a, b\}$ หมายถึงสมาชิกตัวน้อยสุดใน $\{a, b\}$

   1.8 $G = \mathbb{N}$ นิยาม $a * b = \max\{a, b\}$ หมายถึงสมาชิกตัวมากสุดใน $\{a, b\}$

   1.9 $G = \mathbb{C}$ นิยาม $(a + bi) * (c + di) = (a + c) + (b + d)i$

   1.10 $G = \mathbb{Z}_n$ นิยาม $\bar{a} * \bar{b} = \overline{a + b + 1}$ เมื่อ $n = 3, 4, 5, 6$

   1.11 $G = \mathbb{Z}_n$ นิยาม $\bar{a} * \bar{b} = \overline{a - b}$ เมื่อ $n = 3, 4, 5, 6$

2. ให้ $G = \{x \in \mathbb{R} : x \neq -1\}$ นิยาม $a * b = a + b + ab$ จงแสดงว่า $(G, *)$ เป็นอกรุปอาบีเลียน

3. จงหาตัวผกผันการบวกของทุกสมาชิกใน $\mathbb{Z}_9$ และ $\mathbb{Z}_{12}$

4. จงหาตัวผกผันการคูณของทุกสมาชิกใน $\mathbb{Z}_{13}^*$ และ $\mathbb{Z}_{15}^\times$

5. จงหาตัวผกผันการคูณของสมาชิกต่อไปนี้ใน $(\mathbb{Z}_{100}^\times, \cdot)$

   5.1 $\overline{29}$ 5.2 $\overline{61}$ 5.3 $\overline{73}$ 5.4 $\overline{99}$

6. จงหาจำนวนสมาชิกของเซต

   6.1 $\mathbb{Z}_{600}^\times$ 6.2 $\mathbb{Z}_{1500}^\times$ 6.3 $\mathbb{Z}_{4900}^\times$ 6.4 $\mathbb{Z}_{625000}^\times$

7. ให้ $M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ และ $\mathcal{B} = \{X \in M_{22}(\mathbb{R}) \,:\, MX = XM\}$ แล้ว $(\mathcal{B}, \cdot)$ เป็นกรุปหรือไม่

8. ให้ a เป็นค่าคงตัว และ $G_a = \{f : \mathbb{R} \to \mathbb{R} \,:\, f(x) = ax\}$ แล้ว $(G_a, \circ)$ เป็นกรุปหรือไม่

9. ให้ $G = \{z \in \mathbb{C} \,:\, z^n = 1$ สำหรับบาง $n \in \mathbb{Z}^+\}$ แล้ว $(G, +)$ และ $(G, \cdot)$ เป็นกรุปหรือไม่

10. ให้ $G = \{a + b\sqrt{2} \,:\, a, b \in \mathbb{Q}\}$ แล้ว $(G, +)$ และ $(G - \{0\}, \cdot)$ เป็นกรุปหรือไม่

11. ให้ $G = \{A^n \,:\, A \in GL_2(\mathbb{R})$ และ $n \in \mathbb{N} \cup \{0\}\}$ และ $A^0 = I$ แล้ว $(G, \cdot)$ เป็นกรุปหรือไม่

12. ถ้า $D = \{a, b\}$ แล้ว $(\mathcal{P}(D), \triangle)$ เป็นกรุปไคลน์โฟว์ปหรือไม่

2.2 สมบัติเบื้องต้นของกรุป

ในหัวข้อนี้จะกล่าวถึงสมบัติเบื้องต้นเกี่ยวกับกรุปซึ่งจะนำไปใช้พิสูจน์ทฤษฎีบทที่สำคัญต่าง ๆ ต่อไป ในที่นี้การกล่าวถึงผลการดำเนินการ $a * b$ ในกรุป $(G, *)$ จะเขียนด้วย ab และกล่าวว่า G เป็นกรุปโดยไม่ใช้คู่อันดับแต่กล่าวถึงเฉพาะเซตเท่านั้น แต่ให้เข้าใจว่ามีตัวดำเนินการทวิภาคหนึ่งคู่กับเซตนี้เสมอ และใช้ e แทนด้วยเอกลักษณ์ของกรุป

ทฤษฎีบท 2.2.1 ให้ G เป็นกรุป จะได้ว่า

1. เอกลักษณ์ใน G มีเพียงตัวเดียว เขียนแทนด้วย e
2. สำหรับแต่ละ $a \in G$ จะมีตัวผกผันของ a เพียงตัวเดียว เขียนแทนด้วย a^{-1}

ทฤษฎีบท 2.2.2 ให้ G เป็นกรุป และ $a, b \in G$ จะได้ว่า

1. $(a^{-1})^{-1} = a$
2. $(ab)^{-1} = b^{-1}a^{-1}$

ตัวอย่าง 2.2.3 ให้ G เป็นกรุป และ $a, b, c \in G$ จงพิสูจน์ว่า $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$

ทฤษฎีบท 2.2.4 **กฎการตัดออก** (Law of Cancellation)
ให้ G เป็นกรุป และ $a, b, c \in G$

1. ถ้า $ac = bc$ แล้ว $a = b$
2. ถ้า $ca = cb$ แล้ว $a = b$

บทแทรก 2.2.5 ให้ G เป็นกรุป และ $a, b \in G$ จะได้ว่า

1. ถ้า $ab = a$ แล้ว $b = e$
2. ถ้า $ab = b$ แล้ว $a = e$

ทฤษฎีบท 2.2.6 ให้ G เป็นกรุป และ $a, b \in G$ จะได้ว่า

1. มี $x \in G$ เพียงตัวเดียวที่สอดคล้องสมการ $ax = b$
2. มี $y \in G$ เพียงตัวเดียวที่สอดคล้องสมการ $ya = b$

ทฤษฎีบท 2.2.7 ให้ G เป็นกึ่งกรุป จะได้ว่า G เป็นกรุป ก็ต่อเมื่อ ทุก ๆ $a, b \in G$

$$\text{มี } x \in G \text{ ซึ่ง } \quad ax = b \quad \text{และ มี } y \in G \text{ ซึ่ง } \quad ya = b$$

ตัวอย่าง 2.2.8 ให้ G เป็นกรุป และ $a, b \in G$ โดยที่ $c = c^{-1}$ จงแสดงว่า

$$ab = c \qquad \text{ก็ต่อเมื่อ} \qquad abc = e$$

สำหรับผลการดำเนินการของสมาชิกตัวเดียวกันเช่น $a * a$ หรือ aa จะเขียนแทนด้วย a^2 คล้ายการนิยามของเลขยกกำลัง ดังนั้นสำหรับกรุป G ให้ $a \in G$ และ $n \in \mathbb{Z}^+$ แล้ว

$$\underbrace{a * a * a * ... * a}_{n \text{ ตัว}} \qquad \text{เขียนแทนด้วย} \qquad a^n$$

และ a^0 หมายถึง e นั่นคือ $a^0 = e$ ในทำนองเดียวกันสำหรับตัวผกผัน

$$\underbrace{a^{-1} * a^{-1} * a^{-1} * ... * a^{-1}}_{n \text{ ตัว}} \qquad \text{เขียนแทนด้วย} \qquad a^{-n}$$

ในกรณีที่ a เป็นสมาชิกในกรุปการบวก แล้วตัวผกผัน a^{-1} นิยมเขียนแทนด้วย $-a$ โดยที่

$$\underbrace{a + a + \cdots + a}_{n \text{ ตัว}} \qquad \text{เขียนแทนด้วย} \qquad na$$
$$\underbrace{-a - a - \cdots - a}_{n \text{ ตัว}} \qquad \text{เขียนแทนด้วย} \qquad -na$$

นิยมเขียน 0 แทนเอกลักษณ์การบวก และ 1 แทนเอกลักษณ์การคูณ

จากการนิยามข้างต้นถ้า $a \in G$ โดย $m, n \in \mathbb{Z}^+$ จะได้สมบัติคล้ายสมบัติของเลขยกกำลังดังนี้

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

การพิสูจน์เว้นไว้เป็นแบบฝึกหัด 2.2 ข้อ 4

ตัวอย่าง 2.2.9 ให้ G เป็นกรุป และ $a \in G$ จงแสดงว่า

$$a^2 = a \qquad \text{ก็ต่อเมื่อ} \qquad a = e$$

บทนิยาม 2.2.10 ให้ G เป็นกรุป และ $a \in G$ ถ้ามีจำนวนเต็มบวก n ที่น้อยที่สุดที่ทำให้

$$a^n = e \qquad \text{หรือ} \qquad n = \min\{k \in \mathbb{N} : a^k = e\}$$

จะเรียก n ว่า **อันดับ** (order) ของ a เขียนแทนด้วย $\circ(a)$ ในกรณีที่ไม่มีจำนวนเต็มบวกที่สอดคล้องเงื่อนไขดังกล่าวให้เรียก a ว่ามี **อันดับอนันต์** (infinite order) เขียนแทนด้วย $\circ(a) = \infty$

ข้อสังเกต 2.2.11 $\circ(a) = 1$ ก็ต่อเมื่อ $a = e$

ตัวอย่าง 2.2.12 จงแสดงว่าทุกสมาชิกในกรุป $(\mathbb{Z}, +)$ มีอันดับอนันต์ ยกเว้น 0

ตัวอย่าง 2.2.13 จงแสดงว่าทุกสมาชิกในกรุป $(\mathbb{Q}^*, \cdot)$ มีอันดับอนันต์ ยกเว้น -1 และ 1 ในทำนองเดียวกันทุกสมาชิกในกรุป $(\mathbb{R}^*, \cdot)$ มีอันดับอนันต์ ยกเว้น -1 และ 1

ตัวอย่าง 2.2.14 จงหาอันดับของสมาชิกต่อไปในกรุป $(\mathbb{C}^*, \cdot)$

1. i และ $-i$

2. $\dfrac{\sqrt{2}}{2} + \dfrac{\sqrt{2}}{2}i$

3. $\dfrac{1}{2} - \dfrac{\sqrt{3}}{2}i$

ตัวอย่าง 2.2.15 จงหาอันดับของทุกสมาชิกใน $\mathbb{Z}_n$ เมื่อ $n = 2, 3, 4$ ภายใต้การบวก

วิธีทำ แสดงได้ดังตาราง

เซตและสมาชิก	อันดับ	เหตุผล
$\mathbb{Z}_2$		
$\bar{0}$		
$\bar{1}$		
$\mathbb{Z}_3$		
$\bar{0}$		
$\bar{1}$		
$\bar{2}$		
$\mathbb{Z}_4$		
$\bar{0}$		
$\bar{1}$		
$\bar{2}$		
$\bar{3}$		

ข้อสังเกต $2(\bar{1}) = \bar{1} + \bar{1} = \overline{1+1} = \overline{2(1)}$ ทำนองเดียวกันทำให้ได้ว่า $n(\bar{a}) = \overline{na}$

ต่อไปเป็นตัวอย่างอันดับของทุกสมาชิกใน $\mathbb{Z}_n$ เมื่อ $n = 5, 6$ ภายใต้การบวก

เซตและสมาชิก	อันดับ	เหตุผล
$\mathbb{Z}_5$		
$\bar{0}$	1	$\bar{0} = 1(\bar{0})$
$\bar{1}$		
$\bar{2}$		
$\bar{3}$		
$\bar{4}$		
$\mathbb{Z}_6$		
$\bar{0}$	1	$\bar{0} = 1(\bar{0})$
$\bar{1}$		
$\bar{2}$		
$\bar{3}$		
$\bar{4}$		
$\bar{5}$		

ทฤษฎีบท 2.2.16 ให้ a เป็นสมาชิกของกรุป G จะได้ว่า a และตัวผกผันของ a มีอันดับเดียวกัน

ตัวอย่าง 2.2.17 จงหาอันดับของทุกสมาชิกใน $\mathbb{Z}_p^*$ เมื่อ $p = 2, 3$ ภายใต้การคูณ

วิธีทำ แสดงได้ดังตาราง

เซตและสมาชิก	อันดับ	เหตุผล
$\mathbb{Z}_2^*$		
$\bar{1}$		
$\mathbb{Z}_3^*$		
$\bar{1}$		
$\bar{2}$		

ต่อไปเป็นตัวอย่างอันดับของทุกสมาชิกใน $\mathbb{Z}_p^*$ เมื่อ $n = 5, 7$ ภายใต้การคูณ

เซตและสมาชิก	อันดับ	เหตุผล
$\mathbb{Z}_5^*$		
$\bar{1}$	1	เนื่องจาก $\bar{1}$ เป็นเอกลักษณ์
$\bar{2}$		
$\bar{3}$		
$\bar{4}$		
$\mathbb{Z}_7^*$		
$\bar{1}$	1	เนื่องจาก $\bar{1}$ เป็นเอกลักษณ์
$\bar{2}$		
$\bar{3}$		
$\bar{4}$		
$\bar{5}$		
$\bar{6}$		

ตัวอย่าง 2.2.18 จงหาอันดับของสมาชิกต่อไปนี้ใน $(\mathbb{Z}_{12}, +)$

1. $\bar{2}$ 2. $\bar{3}$ 3. $\bar{5}$ 4. $\bar{9}$ 5. $\overline{10}$

วิธีทำ แสดงได้ดังตาราง

สมาชิก	อันดับ	เหตุผล
$\bar{2}$		
$\bar{3}$		
$\bar{5}$		
$\bar{9}$		
$\overline{10}$		

ตัวอย่าง 2.2.19 จงหาอันดับของสมาชิกต่อไปนี้ใน $(\mathbb{Z}_{40}^{\times}, \cdot)$

1. $\bar{3}$

2. $\bar{7}$

3. $\overline{11}$

4. $\overline{13}$

5. $\overline{29}$

ตัวอย่าง 2.2.20 จงหาอันดับของสมาชิกต่อไปนี้ใน $(GL_2(\mathbb{R}), \cdot)$

1. $A = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$

2. $B = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$

3. $C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

ทฤษฎีบท 2.2.21 ให้ a เป็นสมาชิกของกรุป G ถ้า $\circ(a) = m$ แล้วจะได้ว่า

สำหรับ $k \in \mathbb{Z}$ ซึ่ง $a^k = e$ ก็ต่อเมื่อ $m \mid k$

แบบฝึกหัด 2.2

1. ให้ G เป็นกรุป และ $a_1, a_2, ..., a_n \in G$ จงแสดงว่า $(a_1 a_2 ... a_n)^{-1} = a_n^{-1} ... a_2^{-1} a_1^{-1}$

2. ให้ $x \in G$ จงพิสูจน์ว่า $x^2 = e$ ก็ต่อเมื่อ $\circ(x)$ เท่ากับ 1 หรือ 2

3. ให้ G เป็นกรุป และ $x, y \in G$ จงพิสูจน์ว่าข้อความทั้ง 3 ข้อสมมูลกัน

   (1) $xy = yx$ (2) $y^{-1}xy = x$ (3) $x^{-1}y^{-1}xy = 1$

4. ให้ G เป็นกรุป และ $a \in G$ โดยที่ $m, n \in \mathbb{Z}^+$ จงแสดงว่า

   4.1 $a^m a^n = a^{m+n}$ 4.2 $(a^m)^n = a^{mn}$ 4.3 $(a^m)^{-1} = (a^{-1})^m$

5. ให้ G เป็นกรุป และ $a, x, y \in G$ จงพิสูจน์ว่า

   5.1 $a = a^{-1}$ ก็ต่อเมื่อ $a^2 = e$ 5.2 ถ้า $xya = a^{-1}$ แล้ว $yax = a^{-1}$

6. จงพิสูจน์ว่า ถ้า $x^2 = e$ ทุก ๆ $x \in G$ แล้ว G เป็นกรุปอาบีเลียน

7. จงพิสูจน์ว่า ถ้า $(G, *)$ เป็นกึ่งกรุป ที่สอดคล้อง 2 เงื่อนไขต่อไปนี้

   (1) มี $x \in G$ ซึ่ง $x * a = a$ ทุก ๆ $a \in G$

   (2) สำหรับแต่ละ $a \in G$ มี $b \in G$ ซึ่ง $b * a = x$

   แล้ว $(G, *)$ เป็นกรุป

8. จงหาอันดับของสมาชิกต่อไปในกรุป $(\mathbb{C}^*, \cdot)$

   8.1 $\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$ 8.2 $-\frac{\sqrt{3}}{2} + \frac{1}{2}i$ 8.3 $\frac{1}{2} + \frac{\sqrt{3}}{2}i$

9. ให้ $\bar{a} \neq \bar{0}$ เป็นสมาชิกของกรุป $(\mathbb{Z}_n, +)$ จงแสดงว่า

   $$\circ(\bar{a}) = n \quad \text{ก็ต่อเมื่อ} \quad \gcd(a, n) = 1$$

10. จงหาอันดับของทุกสมาชิกใน $(\mathbb{Z}_{15}, +)$ และ $(\mathbb{Z}_{11}^*, \cdot)$

11. จงหาอันดับของสมาชิกต่อไปนี้ใน $\mathbb{Z}_{19}$

    $$\bar{3},\ \bar{5},\ \bar{7},\ \bar{9},\ \overline{12},\ \overline{16},\ \overline{23},\ \overline{-5},\ \overline{-11},\ \overline{-19},\ \overline{-14}$$

12. จงหาอันดับของสมาชิกต่อไปนี้ใน $\mathbb{Z}_{45}^{\times}$

    $$\bar{1},\ \bar{7},\ \bar{9},\ \overline{11},\ \overline{13},\ \overline{31},\ \overline{27},\ \overline{-7},\ \overline{-21},\ \overline{-39},\ \overline{-41}$$

13. จงหา $x \in \mathbb{R}$ เมทริกซ์ $\begin{bmatrix} \sin x & \cos x \\ \cos x & -\sin x \end{bmatrix}$ ใน $(GL_2(\mathbb{R}), \cdot)$ มีอันดับเป็น 2

2.3 ผลคูณตรงของกรุป

สำหรับจำนวนจริง a และ b โดยที่ $i^2 = -1$ จะได้ว่า $z = a + bi$ เป็นจำนวนเชิงซ้อน เมื่อเขียนในรูป (a, b) จะหมายถึงคู่อันดับในระนาบเชิงซ้อน นั่นหมายความว่า $(a, b) \in \mathbb{R} \times \mathbb{R}$ โดยนิยามการบวกและการคูณดังนี้

$$\begin{aligned}(a, b) + (c, d) &= (a + c, b + d)\\ (a, b) \cdot (c, d) &= (ac - bd, ad + bc)\end{aligned}$$

ซึ่งสอดคล้องกับการบวกและการคูณในจำนวนเชิงซ้อน เนื่องจาก $(\mathbb{C}, +)$ เป็นกรุป เราจะได้ว่า $\mathbb{R}\times\mathbb{R}$ กับการบวกดังกล่าวเป็นกรุปด้วย ในหัวข้อนี้จึงขยายแนวคิดไปยังการดำเนินการใด ๆ บนผลคูณคาร์ทีเซียน

ตัวอย่าง 2.3.1 ให้ $G = \mathbb{R} \times \mathbb{R}^*$ กำหนดให้

$$(a, b) * (c, d) = (ad + bc, bd)$$

จงแสดงว่า $(G, *)$ เป็นกรุปอาบีเลียน

ตัวอย่าง 2.3.2 ให้ $G = \mathbb{R}^* \times \mathbb{R}$ กำหนดให้

$$(a, b) * (c, d) = (ac, bc + d)$$

แล้ว $(G, *)$ เป็นกรุปหรือไม่

การขยายแนวคิดไปยังการพิจารณา $G_1 \times G_2$ เมื่อ $(G_1, \diamond)$ และ $(G_2, \circledast)$ เป็นกรุป โดยนิยาม

$$(a, b) * (c, d) = (a \diamond c, b \circledast d) \tag{2.1}$$

จากนั้นจะพิสูจน์ได้โดยง่ายว่า $(G_1 \times G_2, *)$ เป็นกรุป ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 2.3.3 ให้ $(G_1, \diamond)$ และ $(G_2, \circledast)$ เป็นกรุป ถ้านิยามการดำเนิน $*$ ดังสมการ 2.1 แล้ว $(G_1 \times G_2, *)$ เป็นกรุป และเรียก $G_1 \times G_2$ ว่า **ผลคูณตรงของกรุป** (direct product of group)

สำหรับกรุปการบวกใน $\mathbb{Z}_n \times \mathbb{Z}_m$ นิยาม

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

และสำหรับกรุปการคูณใน $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$ นิยาม

$$(\bar{a}, \bar{b}) \cdot (\bar{c}, \bar{d}) = (\bar{a} \cdot \bar{c}, \bar{b} \cdot \bar{d})$$

ตัวอย่าง 2.3.4 จงหาตัวผกผันและอันดับของทุกสมาชิกในกรุป $\mathbb{Z}_2 \times \mathbb{Z}_3$

ตัวอย่าง 2.3.5 จงหาตัวผกผันและอันดับ $(\bar{3}, \bar{7})$ ในกรุปการคูณ $\mathbb{Z}_5^* \times \mathbb{Z}_{11}^*$

แบบฝึกหัด 2.2

1. จงตรวจสอบ $(G,*)$ เป็นกรุปหรือไม่

   1.1 $G=\mathbb{Z}\times\mathbb{Z}$ กำหนดให้ $(a,b)*(c,d)=(a+b,ab)$

   1.2 $G=\mathbb{Z}\times\mathbb{Z}$ กำหนดให้ $(a,b)*(c,d)=(a+c,b+d)$

   1.3 $G=\mathbb{R}^*\times\mathbb{R}^*$ กำหนดให้ $(a,b)*(c,d)=(ac,bd)$

   1.4 $G=\mathbb{Q}\times\mathbb{Q}^*$ กำหนดให้ $(a,b)*(c,d)=(a+b+1,2ab)$

   1.5 $G=\mathbb{Q}\times\mathbb{Q}$ กำหนดให้ $(a,b)*(c,d)=(a+c-3,b+d+3)$

   1.6 $G=\mathbb{R}\times\mathbb{R}$ กำหนดให้ $(a,b)*(c,d)=(a+b+ab,ab+1)$

   1.7 $G=\mathbb{R}\times\mathbb{R}$ กำหนดให้ $(a,b)*(c,d)=(ac-bd,ad+bc)$

2. จงหาตัวผกผันและอันดับของทุกสมาชิกใน

   2.1 กรุปการบวก $\mathbb{Z}_2\times\mathbb{Z}_4$

   2.2 กรุปการคูณ $\mathbb{Z}_3^*\times\mathbb{Z}_4^\times$

3. จงหาตัวผกผันและอันดับ $(\bar{5},\bar{9})$ ในกรุปการคูณ $\mathbb{Z}_7^*\times\mathbb{Z}_{13}^*$

4. ให้ G_1 เมื่อ G_2 เป็นกรุป โดยที่ $(a,b)\in G_1\times G_2$ ถ้า $\circ(a)=m$ และ $\circ(b)=n$ จงแสดงว่า

$$\circ((a,b))=\ell\text{cm}(n,m)$$

2.4 กรุปการเรียงสับเปลี่ยน

ในหัวข้อนี้จะศึกษากรุปสมมาตร $(S_A, \circ)$ ตามทฤษฎีบท 2.1.32 โดยสนใจกรณีที่ A เป็นเซตจำกัด ดังบทนิยามต่อไปนี้

บทนิยาม 2.4.1 ให้ A เป็นเซตจำกัดที่ไม่ใช่เซตว่าง กำหนดให้

$$S_A = \{\sigma : A \to A \,:\, \sigma \text{ เป็นฟังก์ชัน 1-1 แบบทั่วถึง } \}$$

แล้ว S_A เป็นกรุปภายใต้การดำเนินการ $\circ$ เรียกว่า **กรุปการเรียงสับเปลี่ยน** (permutation group) สมาชิก σ ใน S_A จะเรียกว่า **วิธีเรียงสับเปลี่ยน** (permutation) ของ A

สำหรับกรณี $A = \{1, 2, ..., n\}$ กรุปสมมาตร A เขียนแทนด้วย S_n และเขียน $\sigma : A \to A$ โดย

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

จะได้ตัวผกผันของ σ คือ $\sigma^{-1} : A \to A$ เขียนได้เป็น

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

เอกลักษณ์ของ S_n เขียนแทนด้วย (1) หมายถึง

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

ตัวอย่าง S_n เมื่อ $n = 1, 2, 3$

$$S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$$

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

เมื่อพิจารณา $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ และ $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ แล้ว

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

ผลของ $\alpha \circ \beta$ หาได้จากขวาไปซ้าย ดังนั้นถ้านิยาม $\beta\alpha = \alpha \circ \beta$ จะทำให้การหาผลดังกล่าวจากซ้ายไปขวาได้ ดังบทนิยามต่อไปนี้

บทนิยาม 2.4.2 ให้ $\alpha, \beta \in S_n$ เมื่อ $n \in \mathbb{N}$ แล้ว **ผลคูณ** (product) ของ α และ β คือ $\beta \circ \alpha$ เขียนแทนด้วย $\alpha\beta$ นั่นคือ

$$\alpha\beta = \beta \circ \alpha$$

สำหรับ $k \in \mathbb{N}$ ผลคูณของ α จำนวน k ตัวเขียนแทนด้วย α^k และ $\alpha^0 = (1)$
α^{-1} เขียนแทนตัวผกผันของ α และผลคูณของ α^{-1} จำนวน k ตัวเขียนแทนด้วย α^{-k}

ข้อสังเกต 2.4.3 $(S_n, \cdot)$ เป็นกรุปที่มีอันดับเป็น $n!$ นั่นคือ $|S_n| = n!$

ตัวอย่าง 2.4.4 ให้ $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ และ $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ เป็นสมาชิกใน S_3 จงหาผลคูณต่อไปนี้

1. $\alpha\beta$

2. $\beta\alpha$

3. α^{-1}

4. β^{-1}

5. α^2

6. β^3

7. α^{-3}

8. α^6

บทนิยาม 2.4.5 ให้ $A = \{1, 2, 3, ..., n\}$ โดยที่ $a_1, a_2, ..., a_m$ เป็นสมาชิกของ A ที่แตกต่างกัน จะเรียก $(a_1\, a_2 ... a_m)$ ว่า **วัฏจักร (cycle)** ซึ่งความหมายว่า

$$a_1 \mapsto a_2,\ a_2 \mapsto a_3,\ ...,\ a_{m-1} \mapsto a_m \text{ และ } a_m \mapsto a_1$$

เขียนแทนด้วย

$$a_1 \mapsto a_2 \mapsto a_3 \mapsto \cdots \mapsto a_m \mapsto a_1$$

โดยที่ทุก ๆ สมาชิก $a \in A - \{a_1, a_2, ..., a_m\}$ จะส่งค่าฟังก์ชันไปยังค่าเดิมหรือ $a \mapsto a$
เรียก m ว่า **ความยาว (length)** ของวัฏจักร $(a_1\, a_2 ... a_m)$ สำหรับเอกลักษณ์เขียนแทนด้วย (1)

ตัวอย่างใน S_5 วัฏจักร $(1\ 2\ 4)$ หมายถึง

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

โดยนิยามจะได้ว่าวัฏจักร $(1\ 2\ 4)$ มีความหมายเดียวกับ $(4\ 1\ 2)$ และ $(2\ 4\ 1)$
สำหรับตัวผกผันของวัฏจักร $(a_1 a_2 ... a_m)$ คือ

$$(a_1 a_2 ... a_m)^{-1} = (a_m\, a_{m-1} ... a_1)$$

ตัวอย่างเช่น $(2\ 1\ 5\ 3)^{-1} = (3\ 5\ 1\ 2)$

ตัวอย่าง 2.4.6 จงเขียนวัฏจักรต่อไปนี้ในรูปวิธีเรียงสับเปลี่ยน

1. $(1\ 3\ 2) \in S_3$
2. $(1\ 3\ 4\ 2) \in S_4$
3. $(1\ 4\ 5) \in S_5$
4. $(1\ 5\ 3\ 6) \in S_7$

ตัวอย่าง 2.4.7 จงเขียนวัฏจักรต่อไปนี้ในรูปวิธีเรียงสับเปลี่ยน

1. $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
2. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$
3. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 3 & 5 & 4 \end{pmatrix}$
4. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 3 & 7 & 5 & 6 & 2 \end{pmatrix}$

ตัวอย่าง 2.4.8 จงหาผลคูณของวัฏจักรต่อไปนี้ ใน S_5

1. $(1\ 2\ 3)(4\ 5)$

2. $(1\ 3)^{-1}(2\ 5)$

3. $(2\ 3\ 4)(5\ 3\ 1)$

4. $(1\ 4)(1\,3\ 4)^{-1}$

การเขียนวิธีเรียงสับเปลี่ยนบางครั้งอาจไม่สามารถเขียนในรูปวัฏจักรเดียวได้ เช่น

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

เขียนได้เป็นในรูปผลคูณสองวัฏจักรคือ $(1\ 3)(4\ 5)$

บทนิยาม 2.4.9 ถ้า α และ β เป็นวัฏจักรไม่มีสมาชิกซ้ำกันจะกล่าวว่า α และ β เป็น **วัฏจักรไม่มีส่วนร่วม** (disjoint cycle)

ตัวอย่าง 2.4.10 จงเขียนฟังก์ชันต่อไปนี้ในรูปวัฏจักรไม่มีส่วนร่วม

1. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$

3. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 2 & 7 & 3 & 5 & 4 \end{pmatrix}$

4. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 3 & 6 & 2 & 4 & 1 & 8 \end{pmatrix}$

ต่อไปจะแสดงสมาชิกในรูปวัฏจักรไม่มีส่วนร่วม ของ S_n เมื่อ $n = 1, 2, 3, 4$ ดังตารางต่อไปนี้

เซต	$\|S_n\|$	สมาชิก
S_1	1	(1)
S_2	2	(1) (1 2)
S_3	6	(1) (1 2), (1 3), (2 3) (1 2 3), (1 3 2)
S_4	24	(1) (1 2), (1 3), (1 4), (2 3), (2 4), (3 4) (1 2 3), (1 2 4), (1 3 4), (2 3 4), (1 3 2), (1 4 2), (1 4 3), (2 4 3) (1 2 3 4), (1 3 4 2), (1 4 2 3), (4 3 2 1), (2 4 3 1), (3 2 4 1) (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)

ทฤษฎีบท 2.4.11 ถ้า $\alpha, \beta \in S_n$ เป็นวัฏจักรไม่มีส่วนร่วม จะได้ว่า

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

ตัวอย่าง 2.4.12 จงหาอันดับของสมาชิกต่อไปนี้

1. $(1\,2) \in S_2$

2. $(1\,2\,3) \in S_3$

ทฤษฎีบท 2.4.13 ถ้า α มีความยาว m แล้วจะได้ว่า $\circ(\alpha) = m$

ตัวอย่าง 2.4.14 จงหาอันดับของสมาชิกต่อไปนี้ S_5

1. $(1\,2)$
2. $(1\,2\,3)$
3. $(1\,2\,3\;5)$

ตัวอย่าง 2.4.15 จงหาอันดับของสมาชิกต่อไปนี้ใน S_5

1. $(1\,2)(3\;4\;5)$

2. $(1\;2)(3\;2\;1)$

ทฤษฎีบท 2.4.16 ให้ α และ β เป็นวัฏจักรไม่มีส่วนร่วม โดยแต่ละวัฏจักรมีความยาว m และ k ตามลำดับ แล้ว

$$\circ(\alpha\beta) = \ell\text{cm}(m, k)$$

บทแทรก 2.4.17 ให้ α_1, α_2, ..., α_k เป็นวัฏจักรไม่มีส่วนร่วม กัน โดยแต่ละวัฏจักรมีความยาว m_1, m_2,..., m_k ตามลำดับ แล้ว

$$\circ(\alpha_1\alpha_2\cdots\alpha_k) = \ell\text{cm}(m_1, m_2, ..., m_k)$$

ตัวอย่าง 2.4.18 จงหาอันดับของสมาชิกต่อไปนี้ใน S_6

1. $(1\ 2\ 4)(3\ 6)$

2. $(1\ 2\ 4)(3\ 5\ 6)$

3. $(1\ 2)(3\ 4)(5\ 6)$

4. $(1\ 2)(3\ 4)(1\ 5)$

ตัวอย่าง 2.4.19 จงหาอันดับ $(1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$ ใน S_{13}

แบบฝึกหัด 2.4

1. ให้ α, β และ γ เป็นวิธีเรียงสับเปลี่ยน จงหา

ก. $\alpha\beta$	ง. α^{-1}	ช. $\beta\alpha^{-1}\gamma$
ข. $\beta\alpha$	จ. β^{-1}	ซ. $\alpha^2\gamma\beta^{-1}$
ค. $\alpha\gamma$	ฉ. γ^{-1}	ฌ. $\alpha^{-2}\gamma\beta^{-1}$

เมื่อกำหนดให้

1.1 $\alpha = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$ $\quad \beta = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$ $\quad \gamma = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$

1.2 $\alpha = \begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 2 & 1 & 4\end{pmatrix}$ $\quad \beta = \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}$ $\quad \gamma = \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix}$

1.3 $\alpha = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 5 & 3 & 2 & 1 & 4\end{pmatrix}$ $\quad \alpha = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 4 & 3 & 5 & 1 & 2\end{pmatrix}$ $\quad \alpha = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 5 & 1 & 4\end{pmatrix}$

2. จงเขียนวิธีสับเปลี่ยนต่อไปนี้ในรูปวัฏจักรหรือผลคูณของวัฏจักร

2.1 $\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$

2.2 $\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 4 & 2 & 5 & 1\end{pmatrix}$

2.3 $\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 5 & 4 & 3 & 3 & 2\end{pmatrix}$

2.4 $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 1 & 5 & 2 & 4 & 6 & 3\end{pmatrix}$

2.5 $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 2 & 1 & 5 & 3 & 6 & 4\end{pmatrix}$

2.6 $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 1 & 5 & 2 & 3 & 6 & 7 & 4\end{pmatrix}$

2.7 $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 6 & 4 & 5 & 2 & 7 & 3 & 1\end{pmatrix}$

2.8 $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 8 & 3 & 6 & 5 & 4 & 7 & 2 & 1\end{pmatrix}$

2.9 $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 3 & 7 & 2 & 9 & 4 & 5 & 6 & 1 & 8\end{pmatrix}$

2.10 $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 2 & 8 & 3 & 1 & 3 & 6 & 4 & 5 & 7\end{pmatrix}$

3. จงหาตัวผกผันของวิธีสับเปลี่ยนต่อไปนี้

3.1 $(1\,4\,5\,2)$

3.2 $(3\,1\,5\,4)$

3.3 $(2\,1\,4\,2)(1\,5\,6)$

3.4 $(1\,4)(3\,1)(5\,2)(2\,3)$

4. จงหาอันดับของวิธีสับเปลี่ยนต่อไปนี้

4.1 $(1\,3\,4\,5)$

4.2 $(2\,3)(3\,4)$

4.3 $(4\,5\,3\,1)$

4.4 $(1\,2)(1\,3)(2\,4)$

4.5 $(5\,4)(1\,2)(1\,4)(2\,3)$

4.6 $(1\,9)(2\,3\,5)(3\,7\,8)$

5. ให้ α_1, α_2, ..., α_k เป็นวัฏจักรไม่มีส่วนร่วม กัน โดยแต่ละวัฏจักรมีความยาว m_1, m_2,..., m_k ตามลำดับ แล้ว

$$\circ(\alpha_1\alpha_2\cdots\alpha_k) = \ell\text{cm}(m_1, m_2, ..., m_k)$$

6. ให้ α และ β เป็นวัฏจักรไม่มีส่วนร่วม กัน โดยแต่ละวัฏจักรมีความยาว m และ k ตามลำดับ ให้ d เป็นจำนวนเต็มบวก จงแสดงว่า

   6.1 $(\alpha\beta)^d = (1)$ ก็ต่อเมื่อ $\alpha^d = (1)$ และ $\beta^d = (1)$

   6.2 ถ้า $(\alpha\beta)^d = (1)$ แล้ว $d \geq m$ และ $d \geq k$

บทที่ 3

กรุปย่อย

ในบทนี้เราสนใจเซตย่อยของกรุปซึ่งยังคงเป็นกรุปเรียกว่า **กรุปย่อย** (Subgroup) และศึกษาว่าในกรณีกรุปจำกัดจะวิธีการเช่นใดที่จะทำให้ทราบจำนวนทั้งหมดของกรุปย่อย และกรุปย่อยในแต่ละกรุปจะมีรูปแบบเช่นใด อันนำไปสู่สมบัติต่าง ๆ ที่จะอธิบายโครงสร้างเกี่ยวกับกรุปได้อย่างสมบูรณ์

3.1 นิยามและตัวอย่างของกรุปย่อย

บทนิยาม 3.1.1 ให้ $(G, *)$ เป็นกรุป และ $H \subseteq G$ จะกล่าวว่า H เป็น **กรุปย่อย** (subgroup) ของ G เขียนแทนด้วย $H \leq G$ ถ้า $(H, *)$ เป็นกรุป

ข้อสังเกต 3.1.2 ให้ $H \subseteq G$ เมื่อ $(G, *)$ เป็นกรุป

1. ถ้า $H \leq G$ แล้ว $H \neq \varnothing$
2. $*$ มีสมบัติการเปลี่ยนกลุ่มใน H
3. ถ้า G เป็นกรุปอาบีเลียน แล้วทุก ๆ กรุปย่อยของ G เป็นกรุปอาบีเลียน
4. $H = \{e\}$ เป็นกรุปย่อยเสมอ เรียกว่า **กรุปย่อยแบบแจ่มชัด** (trivial subgroup) ของ G
5. ถ้า $H = G$ แล้ว $H \leq G$

ตัวอย่างกรุปย่อยภายใต้การดำเนินการบวก

$$\mathbb{Z} \leq \mathbb{Q}, \quad \mathbb{Z} \leq \mathbb{R}, \quad \mathbb{Q} \leq \mathbb{R}, \quad \mathbb{Q} \leq \mathbb{C} \quad \text{และ} \quad \mathbb{R} \leq \mathbb{C}$$

ตัวอย่างกรุปย่อยภายใต้การดำเนินการคูณ

$$\mathbb{Z}^* \leq \mathbb{Q}^*, \quad \mathbb{Q}^+ \leq \mathbb{R}^* \quad \text{และ} \quad \mathbb{R}^* \leq \mathbb{C}^*$$

เมื่อกล่าวถึงกรุปของ $\mathbb{Z}_n$ จะหมายถึงกรุปของเซตดังกล่าวกับการบวก และ $\mathbb{Z}_p^*$ หรือ $\mathbb{Z}_n^\times$ จะหมายถึงกรุปของเซตเซตดังกล่าวการคูณ สำหรับ p เป็นจำนวนเฉพาะ และ n เป็นจำนวนนับ

ตัวอย่าง 3.1.3 จงหากรุปย่อยทั้งหมดของ $\mathbb{Z}_3$

ตัวอย่าง 3.1.4 จงตรวจสอบว่าเซตย่อยในข้อใดต่อไปนี้เป็นกรุปย่อยของ $\mathbb{Z}_6$

1. $H_1 = \{\bar{0}, \bar{3}\}$

2. $H_2 = \{\bar{0}, \bar{1}, \bar{4}\}$

3. $H_3 = \{\bar{0}, \bar{2}, \bar{4}\}$

ตัวอย่าง 3.1.5 จงหากรุปย่อยทั้งหมดของ S_2

ตัวอย่าง 3.1.6 จงแสดงว่า $H = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ เป็นกรุปย่อย S_3

ต่อไปเป็นการแสดงกรุปย่อยทั้งหมดของ S_3

กรุปย่อย	จำนวนสมาชิก (อันดับ)
$\{(1)\}$	1
$\{(1), (1\ 2)\}$	2
$\{(1), (1\ 3)\}$	2
$\{(1), (2\ 3)\}$	2
$\{(1), (1\ 2\ 3), (1\ 3\ 2)\}$	3

ทฤษฎีบท 3.1.7 เกณฑ์การพิจารณากรุปย่อย (The Subgroup Criterion)
ให้ H เป็นเซตย่อยของกรุป G โดยที่ $H \neq \varnothing$ แล้วจะได้ว่าข้อความต่อไปนี้สมมูลกัน

1. $H \leq G$
2. $ab^{-1} \in H$ สำหรับทุก ๆ $a, b \in H$
3. $ab \in H$ และ $a^{-1} \in H$ สำหรับทุก ๆ $a, b \in H$

จากทฤษฎีบท 3.1.7 จะได้ว่ากรุปย่อย H มีเอกลักษณ์ตัวเดียวกับ G และสรุปการตรวจสอบว่า H กรุปย่อยด้วยสมบัติ 3 ข้อต่อไปนี้

1. $e \in H$
2. H มีสมบัติปิด
3. ตัวผกผันทุกตัวของสมาชิกใน H เป็นสมาชิกใน H

ตัวอย่าง 3.1.8 จงหากรุปย่อยทั้งหมดของ $\mathbb{Z}_4$

ต่อไปจะเป็นตัวอย่างของกรุปย่อยทั้งหมดของกรุป $\mathbb{Z}_n$ เมื่อ $n = 1, 2, 3, ..., 12$

$\mathbb{Z}_n$	กรุปย่อยทั้งหมด	จำนวนกรุปย่อย
$n = 1$	$\mathbb{Z}_1$	1
$n = 2$	$\{\bar{0}\}$, $\mathbb{Z}_2$	2
$n = 3$	$\{\bar{0}\}$, $\mathbb{Z}_3$	2
$n = 4$	$\{\bar{0}\}$, $\{\bar{0}, \bar{2}\}$, $\mathbb{Z}_4$	3
$n = 5$	$\{\bar{0}\}$, $\mathbb{Z}_5$	2
$n = 6$	$\{\bar{0}\}$, $\{\bar{0}, \bar{3}\}$, $\{\bar{0}, \bar{2}, \bar{4}\}$, $\mathbb{Z}_6$	4
$n = 7$	$\{\bar{0}\}$, $\mathbb{Z}_7$	2
$n = 8$	$\{\bar{0}\}$, $\{\bar{0}, \bar{4}\}$, $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$, $\mathbb{Z}_8$	4
$n = 9$	$\{\bar{0}\}$, $\{\bar{0}, \bar{3}, \bar{6}\}$, $\mathbb{Z}_9$	3
$n = 10$	$\{\bar{0}\}$, $\{\bar{0}, \bar{5}\}$, $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$, $\mathbb{Z}_{10}$	4
$n = 11$	$\{\bar{0}\}$, $\mathbb{Z}_{11}$	2
$n = 12$	$\{\bar{0}\}$, $\{\bar{0}, \bar{6}\}$, $\{\bar{0}, \bar{4}, \bar{8}\}$, $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\}$, $\{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$, $\mathbb{Z}_{12}$	6

ตัวอย่าง 3.1.9 จงหากรุปย่อยทั้งหมดของ $\mathbb{Z}_5^*$

ต่อไปจะเป็นตัวอย่างของกรุปย่อยทั้งหมดของกรุป $\mathbb{Z}_n^\times$ เมื่อ $n = 2, 3, ..., 12$

$\mathbb{Z}_n^\times$	กรุปย่อยทั้งหมด	จำนวนกรุปย่อย
$n = 2$	$\mathbb{Z}_2^\times$	1
$n = 3$	$\{\bar{1}\}$, $\mathbb{Z}_3^\times$	2
$n = 4$	$\{\bar{1}\}$, $\mathbb{Z}_4^\times$	2
$n = 5$	$\{\bar{1}\}$, $\{\bar{1}, \bar{4}\}$, $\mathbb{Z}_5^\times$	3
$n = 6$	$\{\bar{1}\}$, $\mathbb{Z}_6^\times$	2
$n = 7$	$\{\bar{1}\}$, $\{\bar{1}, \bar{6}\}$, $\{\bar{1}, \bar{2}, \bar{4}\}$, $\mathbb{Z}_7^\times$	4
$n = 8$	$\{\bar{1}\}$, $\{\bar{1}, \bar{3}\}$, $\mathbb{Z}_8^\times$	3
$n = 9$	$\{\bar{1}\}$, $\{\bar{1}, \bar{8}\}$, $\{\bar{1}, \bar{4}, \bar{7}\}$, $\mathbb{Z}_9^\times$	4
$n = 10$	$\{\bar{1}\}$, $\{\bar{1}, \bar{9}\}$, $\mathbb{Z}_{10}^\times$	3
$n = 11$	$\{\bar{1}\}$, $\{\bar{1}, \overline{10}\}$, $\{\bar{1}, \bar{3}, \bar{4}, \bar{5}, \bar{9}\}$, $\mathbb{Z}_{11}^\times$	4
$n = 12$	$\{\bar{1}\}$, $\{\bar{1}, \bar{5}\}$, $\mathbb{Z}_{12}^\times$	3

ทฤษฎีบท 3.1.10 ให้ $n\mathbb{Z} = \{nk \,:\, k \in \mathbb{Z}\}$ เมื่อ $n \in \mathbb{Z}$ จะได้ว่า $n\mathbb{Z}$ เป็นกรุปย่อยของ $(\mathbb{Z}, +)$

มากไปกว่านั้นเราพิสูจน์ได้ว่ากรุปย่อยของ $\mathbb{Z}$ จะมีรูปแบบเป็น $n\mathbb{Z}$ เสมอ (แบบฝึกหัด) หรือกล่าวอีกนัยได้ว่า ทุก ๆ กรุปย่อยของ $\mathbb{Z}$ จะมีรูปแบบเดียวคือ $n\mathbb{Z}$ สำหรับบางจำนวนเต็ม n

ตัวอย่าง 3.1.11 ให้ $H = \{2^n : n \in \mathbb{Z}\}$ จงพิสูจน์ว่า $H \leq \mathbb{R}^*$ ภายใต้การคูณ

ตัวอย่าง 3.1.12 ให้ $H = \{\ell\text{n}a : a \in \mathbb{Q}^+\}$ จงพิสูจน์ว่า $H \leq \mathbb{R}$ ภายใต้การบวก

ตัวอย่าง 3.1.13 จงพิสูจน์ว่า $H \leq G$ เมื่อกำหนดให้

1. $H = \{a + b\sqrt{2} \,:\, a, b \in \mathbb{Q}\}$ และ $G = \mathbb{R}$ ภายใต้การบวก

2. $H = \{a + b\sqrt{2} \,:\, a, b \in \mathbb{Q}, a \neq 0$ หรือ $b \neq 0\}$ และ $G = \mathbb{R}^*$ ภายใต้การคูณ

ตัวอย่าง 3.1.14 จงตรวจสอบว่าเซตย่อยต่อไปนี้เป็นกรุปย่อยของ $(GL_2(\mathbb{R}), \cdot)$ หรือไม่

1. $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \neq 0 \right\}$

2. $H = \left\{ \begin{bmatrix} a & a \\ 0 & b \end{bmatrix} : a \neq 0 \text{ และ } b \neq 0 \right\}$

ทฤษฎีบท 3.1.15 ให้ G เป็นกรุป ถ้า H และ K เป็นกรุปย่อยของ G แล้ว

$$H \cap K \text{ เป็นกรุปย่อยของ } G$$

ทฤษฎีบท 3.1.16 ให้ G เป็นกรุป และ $\{H_\alpha\}_{\alpha\in\Lambda}$ เป็นกลุ่มของกรุปย่อยของ G เมื่อ Λ เป็นเซตดัชนี จะได้ว่า

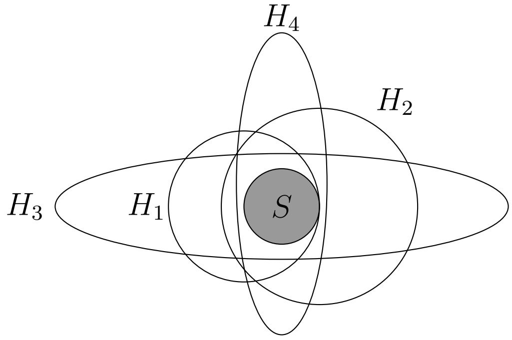
$$\bigcap_{\alpha\in\Lambda} H_\alpha = \{x : x \in H_\alpha \text{ ทุก ๆ } \alpha \in \Lambda\} \quad \text{กรุปย่อยของ } G$$

บทนิยาม 3.1.17 ให้ G เป็นกรุป และ S เป็นเซตย่อยของ G ที่ไม่ใช่เซตว่าง $\{H_\alpha\}_{\alpha\in\Lambda}$ เป็นกลุ่มของกรุปย่อยของ G เมื่อ Λ เป็นเซตดัชนี โดยที่ $S \subseteq H_\alpha$ ทุก ๆ $\alpha \in \Lambda$ แล้วนิยาม

$$\langle S\rangle = \bigcap_{\alpha\in\Lambda} H_\alpha$$

เรียกว่า **กรุปย่อยของ** G **ที่ก่อกำเนิดโดย** S (subgroup of G generated by S)
ในกรณี $S = \{a_1, a_2, ..., a_k\}$ เขียนแทน $\langle S\rangle$ ด้วย $\langle a_1, a_2, ..., a_k\rangle$

ในกรณีมีกรุปย่อยของ G คือ H_1, H_2, H_3 และ H_4 ที่บรรจุ S เพื่อให้เรามองเห็นภาพมากยิ่งขึ้น อาจแสดงตัวอย่างให้เห็นได้ดังรูปต่อไปนี้



ข้อสังเกต 3.1.18 ให้ G เป็นกรุป และ S เป็นเซตย่อยของ G ที่ไม่ใช่เซตว่าง

1. $S \subseteq \langle S \rangle$
2. เนื่องจาก e เป็นสมาชิกของทุก ๆ กรุปย่อยของ G ดังนั้น $\langle e \rangle = \{e\}$
3. ถ้า $H \leq G$ และ $S \subseteq H$ แล้ว $\langle S \rangle \subseteq H$ หรือกล่าวได้ว่า $\langle S \rangle$ คือ**กรุปย่อยที่เล็กที่สุดของ** G **ที่บรรจุ** S

จากตัวอย่าง 3.1.8 จะได้ว่า $\mathbb{Z}_4$ มีกรุปย่อยทั้งหมดคือ $\{\bar{0}\}$, $\{\bar{0}, \bar{2}\}$ และ $\mathbb{Z}_4$ จะได้ว่า $\langle \bar{0} \rangle = \{\bar{0}\} \cap \{\bar{0}, \bar{2}\} \cap \mathbb{Z}_4 = \{\bar{0}\}$ และ $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}\} \cap \mathbb{Z}_4 = \{\bar{0}, \bar{2}\}$ และ $\langle \bar{0}, \bar{2} \rangle = \{\bar{0}, \bar{2}\}$ เป็นต้น

ตัวอย่าง 3.1.19 จงหาแจกแจงสมาชิกของเซตต่อไปนี้ ใน $(\mathbb{Z}_{12}, +)$

1. $\langle \bar{2} \rangle$ 2. $\langle \bar{4} \rangle$ 3. $\langle \bar{6} \rangle$ 4. $\langle \bar{2}, \bar{3} \rangle$ 5. $\langle \bar{2}, \bar{4} \rangle$

วิธีทำ จากกรุปย่อยทั้งหมดของ $\mathbb{Z}_{12}$ คือ

$$\{\bar{0}\},\ \{\bar{0}, \bar{6}\},\ \{\bar{0}, \bar{4}, \bar{8}\},\ \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \overline{10}\},\ \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} \text{ และ } \mathbb{Z}_{12}$$

ทฤษฎีบท 3.1.20 ให้ S และ T เป็นเซตย่อยที่ไม่ใช่เซตว่างของกรุป G จะได้ว่า

$$\langle S \rangle = \langle T \rangle \quad \text{ก็ต่อเมื่อ} \quad S \subseteq \langle T \rangle \text{ และ } T \subseteq \langle S \rangle$$

ทฤษฎีบท 3.1.21 ให้ S เป็นเซตย่อยที่ไม่ใช่เซตว่างของกรุป G แล้ว

$$\langle S\rangle = \{a_1^{r_1}a_2^{r_2}...a_n^{r_n} \,:\, a_i \in S, r_i \in \mathbb{Z},\ \text{เมื่อ } 1 \le i \le n \text{ และ } n \in \mathbb{N}\}$$

บทแทรก 3.1.22 ให้ G เป็นกรุป และ $a, b \in G$ จะได้ว่า

1. $\langle a\rangle = \{a^r \,:\, r \in \mathbb{Z}\}$
2. ถ้า G เป็นกรุปอาบีเลียน แล้ว $\langle a, b\rangle = \{a^i b^j \,:\, i, j \in \mathbb{Z}\}$

จากบทแทรก 3.1.22 ข้อ 1 สำหรับกรุป $(\mathbb{Z}, +)$ เมื่อ $n \in \mathbb{Z}$ จะได้ว่า

$$\langle n\rangle = \{kn : k \in \mathbb{Z}\} = n\mathbb{Z}$$

หรือกล่าวได้ว่ากรุปย่อยของ $\mathbb{Z}$ อยู่ในรูปแบบ $\langle n\rangle$ เท่านั้น และได้ด้วยว่า

$$\langle -n\rangle = \{k(-n) : k \in \mathbb{Z}\} = \{(-k)n : k \in \mathbb{Z}\} = \{(-k)n : -k \in \mathbb{Z}\} = \langle n\rangle$$

ทฤษฎีบท 3.1.23 ให้ m และ n เป็นสมาชิกในกรุป $(\mathbb{Z}, +)$ โดยที่ $n \neq 0$ จะได้ว่า

$$\langle m\rangle \subseteq \langle n\rangle \quad \text{ก็ต่อเมื่อ} \quad n \mid m$$

ข้อสังเกต 3.1.24 ให้ m เป็นสมาชิกในกรุป $(\mathbb{Z}, +)$ ถ้า $\langle m \rangle \subseteq \langle 0 \rangle$ แล้ว $m = 0$

บทแทรก 3.1.25 ให้ m และ n เป็นสมาชิกในกรุป $(\mathbb{Z}, +)$ โดยที่ $n \neq 0$ จะได้ว่า

$$\langle m \rangle = \langle n \rangle \quad \text{ก็ต่อเมื่อ} \quad n = \pm m$$

ตัวอย่าง 3.1.26 ให้ K_4 เป็นกรุปไคลน์โฟว์ ถ้า a และ b เป็นสมาชิกที่ไม่ใช้เอกลักษณ์ของ K_4 จงแสดงว่า

$$\langle a, b \rangle = \{e, a, b, ab\} = K_4$$

ทฤษฎีบท 3.1.27 ให้ G เป็นกรุป และ $a, b \in G$ โดยที่ $\circ(a) = n$ และ $\circ(b) = m$ จะได้ว่า

1. $\langle a \rangle = \{e, a, a^2, ..., a^{n-1}\}$
2. ถ้า G เป็นกรุปอาบีเลียน แล้ว

$$\langle a, b \rangle = \{a^i b^j \,:\, i \in \{0, 1, ..., n-1\}, j \in \{0, 1, ..., m-1\}\}$$

ข้อสังเกต 3.1.28 ให้ a เป็นสมาชิกในกรุป G และมีอันดับจำกัด จะได้ว่า $\circ(a) = |\langle a \rangle|$

ตัวอย่าง 3.1.29 จงแจกแจงสมาชิกของเซตต่อไปนี้

1. $\langle\bar{2}\rangle$ ใน $(\mathbb{Z}_6, +)$

2. $\langle\bar{3}\rangle$ ใน $(\mathbb{Z}_6, +)$

3. $\langle\bar{1}\rangle$ ใน $(\mathbb{Z}_5, +)$

4. $\langle\bar{4}, \bar{6}\rangle$ ใน $(\mathbb{Z}_{12}, +)$

ตัวอย่าง 3.1.30 จงแจกแจงสมาชิกของเซตต่อไปนี้

1. $\langle\bar{2}\rangle$ ใน $(\mathbb{Z}_5^*, \cdot)$

2. $\langle\bar{3}\rangle$ ใน $(\mathbb{Z}_7^*, \cdot)$

3. $\langle\bar{3}, \bar{7}\rangle$ ใน $(\mathbb{Z}_8^\times, \cdot)$

ตัวอย่าง 3.1.31 จงแจกแจงสมาชิกของเซตต่อไปนี้

1. $\langle (1\,2\,3) \rangle$ ใน S_3

2. $\langle (1\,2), (3\,4) \rangle$ ใน S_4

ตัวอย่าง 3.1.32 กำหนดให้ $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ ใน $GL_2(\mathbb{R})$ จงเขียนเซต $\langle A \rangle$ ในรูปแบบมีเงื่อนไข

ทฤษฎีบท 3.1.33 ให้ H เป็นเซตย่อยที่ไม่ใช่เซตว่างของกรุป G โดยที่ H เป็นเซตจำกัด

$$\text{ถ้าทุก ๆ } x, y \in H \text{ ซึ่ง } xy \in H \text{ จะได้ว่า } H \leq G$$

แบบฝึกหัด 3.1

1. จงตรวจสอบว่าเซตย่อย H ต่อไปนี้เป็นกรุปย่อยของ $(GL_2(\mathbb{R}), \cdot)$ หรือไม่

   1.1 $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \in \mathbb{R} \right\}$

   1.2 $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & \frac{1}{a} \end{bmatrix} : a \neq 0 \right\}$

   1.3 $H = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : ac \neq 0 \right\}$

   1.4 $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc = 1 \right\}$

   1.5 $H = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a \neq 0 \right\}$

   1.6 $H = \left\{ \begin{bmatrix} a & 0 \\ b & \frac{1}{a} \end{bmatrix} : a \neq 0 \right\}$

2. จงแจกแจงสมาชิกของเซตต่อไปนี้

   2.1 $\langle \bar{2} \rangle$ ใน $\mathbb{Z}_{10}$

   2.2 $\langle \bar{3}, \bar{6} \rangle$ ใน $\mathbb{Z}_9$

   2.3 $\langle \bar{4} \rangle$ ใน $\mathbb{Z}_{16}$

   2.4 $\langle (1\ 3) \rangle$ ใน S_4

   2.5 $\langle (1\ 2\ 3) \rangle$ ใน S_5

   2.6 $\langle (1\ 5\ 6\ 4) \rangle$ ใน S_6

3. กำหนดให้ $A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ และ $B = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ ใน $GL_2(\mathbb{R})$
   จงเขียนเซตต่อไปนี้ในรูปแบบมีเงื่อนไข

   3.1 $\langle A \rangle$

   3.2 $\langle B \rangle$

   3.3 $\langle A, B \rangle$

4. จงหากรุปย่อยทั้งหมดของ $\mathbb{Z}_{18}$ และ $\mathbb{Z}_{24}$

5. ให้ G เป็นกรุปและ $a, b \in G$ จงแสดงว่า

   5.1 $\circ(ab) = \circ(ba)$

   5.2 $\circ(a) = \circ(b^{-1}ab)$

6. จงแสดงว่ากรุปที่มีอันดับน้อยกว่าหรือเท่ากับ 5 จะเป็นกรุปอาบีเลียน

7. ให้ a และ bเป็นสมาชิกที่ไม่ใช่เอกลักษณ์ของกรุป G ซึ่งสอดคล้อง $a^5 = e$ และ $ab^{-1}a = b^2$
   จงหา $\circ(b)$

8. จงพิสูจน์ว่าถ้า H เป็นเซตย่อยของกรุป G แล้ว $\langle H \rangle = H$

9. จงพิสูจน์ว่าถ้า $A \subseteq B$ และ B เป็นเซตย่อยของกรุป G แล้ว $\langle A \rangle \subseteq \langle B \rangle$

10. จงแสดงว่า $S_4 = \langle (1\,2\,3\,4), (1\,2\,4\,3) \rangle$ เป็นกรุปไคลน์โฟว์

11. จงแสดงว่า $H = \{(1), (1\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(2\ 4)\}$ เป็นกรุปย่อยของ S_4 และเป็นกรุปไคลน์โฟว์

12. ใน S_4 ให้ $a = (1\ 2)(3\ 4)$ และ $b = (1\ 3)(2\ 4)$ จงแจกแจงสมาชิก $K_4 = \langle a, b \rangle$

13. ใน S_8 ถ้า $a = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$ และ $b = (1\ 5\ 3\ 7)(2\ 8\ 4\ 6)$
    จงแสดงว่า $\langle a, b \rangle$ เป็นกรุปควอเทอร์เนียน

14. จงสร้างตารางการดำเนินการของกรุปควอเทอร์เนียน

3.2 กรุปวัฏจักร

บทนิยาม 3.2.1 ให้ G เป็นกรุป จะกล่าวว่า G เป็น **กรุปวัฏจักร** (cyclic group) ถ้ามี $a \in G$ ซึ่ง

$$G = \langle a \rangle$$

เรียก a ว่า **ตัวก่อกำเนิด** (generator) ของ G

ตัวอย่างเช่น $(\mathbb{Z}, +)$ เป็นกรุปวัฏจักร โดยมี 1 เป็นตัวก่อกำเนิดเนื่องจาก

$$\langle 1 \rangle = \{k1 : k \in \mathbb{Z}\} = \mathbb{Z}$$

และเห็นได้ว่า $\langle -1 \rangle = \{k(-1) : k \in \mathbb{Z}\} = \mathbb{Z}$ นั่นคือ -1 เป็นตัวก่อกำเนิดอีกตัวของ $\mathbb{Z}$
สำหรับ $n \in \mathbb{Z}$ จะได้ว่า

$$\langle n \rangle = \{kn : k \in \mathbb{Z}\} = n\mathbb{Z}$$

ทำให้สรุปได้ว่า $n\mathbb{Z}$ เป็นกรุปวัฏจักร โดยมี n เป็นตัวก่อกำเนิด

ข้อสังเกต 3.2.2 ตัวก่อกำเนิดของกรุปวัฏจักรอาจมีมากกว่าหนึ่งตัว

ตัวอย่าง 3.2.3 จงตรวจสอบว่ากรุปต่อไปนี้เป็นกรุปวัฏจักรหรือไม่

1. $(\mathbb{Z}_3, +)$
2. $(\mathbb{Z}_6, +)$
3. $(\mathbb{Z}_5^*, \cdot)$
4. $(\mathbb{Z}_8^*, \cdot)$

จากตัวอย่าง 3.2.3 จะเห็นได้ว่า $(\mathbb{Z}_n, +)$ เป็นกรุปวัฏจักรทุก ๆ $n \in \mathbb{N}$ เนื่องจาก

$$\langle \bar{1} \rangle = \mathbb{Z}_n$$

ทฤษฎีบท 3.2.4 กรุปวัฏจักรเป็นกรุปอาบีเลียน

จากทฤษฎีบท 3.2.4 โดยกฎการแย้งสลับที่กล่าวได้อีกนัยว่า

ถ้า G ไม่เป็นกรุปอาบีเลียน แล้ว G ไม่เป็นกรุปวัฏจักร

ตัวอย่างเช่น S_3 และ Q_4 ไม่เป็นกรุปวัฏจักร เนื่องจากกรุปทั้งสองไม่เป็นกรุปอาบีเลียน

ทฤษฎีบท 3.2.5 ให้ G เป็นกรุปจำกัด และ $a \in G$ จะได้ว่า

a เป็นตัวก่อกำเนิดของ G ก็ต่อเมื่อ $\circ(a) = |G|$

ข้อสังเกต 3.2.6 โดยทฤษฎีบท 3.2.5 จะได้ว่า

1. G เป็นกรุปวัฏจักร ก็ต่อเมื่อ มี $a \in G$ ซึ่ง $\circ(a) = |G|$
2. ถ้า a เป็นตัวก่อกำเนิดของ G แล้ว a^{-1} เป็นตัวก่อกำเนิด G เนื่องจาก $\circ(a) = \circ(a^{-1})$

ตัวอย่าง 3.2.7 จงหาตัวก่อกำเนิดทั้งหมดของกรุปต่อไปนี้

1. $\mathbb{Z}_5$

2. $\mathbb{Z}_6$

3. $\mathbb{Z}_5^*$

ทฤษฎีบท 3.2.8 ทุก ๆ กรุปย่อยของกรุปวัฏจักรย่อมเป็นกรุปวัฏจักร

ตัวอย่าง 3.2.9 จงหากรุปย่อยทั้งหมดของ $\mathbb{Z}_6$

ต่อไปจะพิสูจน์สมบัติเกี่ยวกับผลคาร์ทีเซียนของกรุปวัฏจักรเป็นกรุปวัฏจักร (ทฤษฎีบท 3.2.10) ซึ่งอาศัยทฤษฎีบท 2.2.21 ที่ว่าสำหรับ a ที่เป็นสมาชิกของกรุป G และ a มีอันดับจำกัด จะได้ว่า

$$\text{สำหรับ } k \in \mathbb{Z} \text{ ซึ่ง } \quad a^k = e \quad \text{ ก็ต่อเมื่อ } \quad \circ(a) \mid k$$

ทฤษฎีบท 3.2.10 ให้ G_1 และ G_2 เป็นกรุปวัฏจักร โดย a_1 a_2 เป็นตัวก่อกำเนิดของ G_1 และ G_2 ตามลำดับ สมมติ $\circ(a_1) = m$ และ $\circ(a_2) = n$ โดยที่ $\gcd(m, n) = 1$ จะได้ว่า

$$G_1 \times G_2 \text{ เป็นกรุปวัฏจักรซึ่งมี } (a_1, a_2) \text{ เป็นตัวก่อกำเนิดซึ่ง } |G_1 \times G_2| = mn$$

ตัวอย่าง 3.2.11 จงตรวจสอบว่ากรุปต่อไปนี้เป็นกรุปวัฏจักรหรือไม่

1. $\mathbb{Z}_2 \times \mathbb{Z}_3$
2. $\mathbb{Z}_2 \times \mathbb{Z}_2$

บทแทรก 3.2.12 ให้ $m, n \in \mathbb{N}$ ถ้า $\text{gcd}(m,n) = 1$ แล้ว $\mathbb{Z}_n \times \mathbb{Z}_m$ เป็นกรุปวัฏจักร

ทฤษฎีบท 3.2.13 ให้ G เป็นกรุปวัฏจักร โดย $|G| = n$ และ a เป็นตัวก่อกำเนิดของ G สำหรับ $1 \leq k < n$ เมื่อ $k \in \mathbb{N}$ จะได้ว่า

$$a^k \text{ เป็นตัวก่อกำเนิด } G \quad \text{ ก็ต่อเมื่อ } \quad \text{gcd}(k,n) = 1$$

ตัวอย่าง 3.2.14 จงหาตัวก่อกำเนิดทั้งหมดของกรุปวัฏจักรต่อไปนี้

1. $\mathbb{Z}_5$

2. $\mathbb{Z}_8$

3. $\mathbb{Z}_{12}$

จากทฤษฎีบท 3.2.13 และ $\bar{1}$ เป็นตัวก่อกำเนิดของ $\mathbb{Z}_n$ เมื่อ $n \in \mathbb{N}$ ทำให้ได้ข้อสรุปดังต่อไปนี้

1. ตัวก่อกำเนิดของ $\mathbb{Z}_n$ คือ $\bar{k}$ เมื่อ $1 \leq k < n$ และ $\gcd(k, n) = 1$
2. ถ้า p เป็นจำนวนเฉพาะ จะได้ว่าตัวก่อกำเนิดของ $\mathbb{Z}_p$ คือ $\bar{1}, \bar{2}, \bar{3}, ..., \overline{p-1}$

ตัวอย่าง 3.2.15 จงหาตัวก่อกำเนิดทั้งหมดของกรุปวัฏจักรต่อไปนี้

1. $\mathbb{Z}_5^*$
2. $\mathbb{Z}_{10}^\times$

ตัวอย่าง 3.2.16 จงหาตัวก่อกำเนิดทั้งหมดของ $\mathbb{Z}_2 \times \mathbb{Z}_5$

ข้อสังเกต 3.2.17 จากทฤษฎีบท 3.2.13 เมื่อ G เป็นกรุปวัฏจักรซึ่ง $|G| = n$ จะได้ว่า

จำนวนตัวก่อกำเนิดของ G เท่ากับ $\phi(n)$

ตัวอย่าง 3.2.18 จงหาจำนวนตัวก่อกำเนิดทั้งหมดกรุปวัฏจักรต่อไปนี้

1. $\mathbb{Z}_{12}$
2. $\mathbb{Z}_{25}$
3. $\mathbb{Z}_{36}$
4. $\mathbb{Z}_{144}$
5. $\mathbb{Z}_{5000}$
6. $\mathbb{Z}_{25} \times \mathbb{Z}_{36}$

ตัวอย่าง 3.2.19 จงหาจำนวนตัวก่อกำเนิดของ $\mathbb{Z}_{25}^*$

สำหรับ $n \in \mathbb{N}$ ถ้า $\mathbb{Z}_n^\times$ เป็นกรุปวัฏจักร แล้วจำนวนตัวก่อกำเนิดของ $\mathbb{Z}_n^\times$ เท่ากับ

$$\phi(\phi(n))$$

ดังแสดงตัวอย่างดังตารางต่อไปนี้

กรุป	ตัวก่อกำเนิด	จำนวนตัวก่อกำเนิด
$\mathbb{Z}_2^\times$	$\bar{1}$	$\phi(\phi(2)) = \phi(1) = 1$
$\mathbb{Z}_3^\times$	$\bar{2}$	$\phi(\phi(3)) = \phi(2) = 1$
$\mathbb{Z}_4^\times$	$\bar{3}$	$\phi(\phi(4)) = \phi(2) = 1$
$\mathbb{Z}_5^\times$	$\bar{2}, \bar{3}$	$\phi(\phi(5)) = \phi(4) = 2$
$\mathbb{Z}_6^\times$	$\bar{5}$	$\phi(\phi(6)) = \phi(2) = 1$
$\mathbb{Z}_7^\times$	$\bar{3}, \bar{5}$	$\phi(\phi(7)) = \phi(6) = 2$
$\mathbb{Z}_8^\times$	ไม่มี	ไม่มี
$\mathbb{Z}_9^\times$	$\bar{2}, \bar{5}$	$\phi(\phi(9)) = \phi(6) = 2$
$\mathbb{Z}_{10}^\times$	$\bar{3}, \bar{7}$	$\phi(\phi(10)) = \phi(4) = 2$

ทฤษฎีบท 3.2.20 ถ้า $\langle a \rangle$ เป็นกรุปอนันต์ แล้ว

$$a^m = a^n \quad \text{ก็ต่อเมื่อ} \quad m = n$$

ทฤษฎีบท 3.2.21 ตัวก่อกำเนิดของกรุปวัฏจักรอนันต์มีเพียง 2 ตัวซึ่งเป็นตัวผกผันกันและกัน

จากทฤษฎีบท 3.2.21 จะได้ว่า $(\mathbb{Z}, +)$ มีตัวก่อกำเนิด 2 ตัวเท่านั้นคือ 1 และ -1 สำหรับ $n \in \mathbb{N}$ จะได้ว่า $n\mathbb{Z}$ มีตัวก่อกำเนิด 2 ตัวคือ n และ $-n$

ทฤษฎีบท 3.2.22 ให้ G เป็นกรุปวัฏจักรจำกัด ถ้า $d \in \mathbb{Z}^+$ ซึ่ง d หาร $|G|$ ลงตัว แล้ว

G จะมีกรุปย่อยอันดับ d เพียงกรุปเดียว

จากการพิสูจน์ทฤษฎีบท 3.2.22 ถ้า $G = \langle a \rangle$ และ $|G| = n$ ซึ่ง $d_1 d_2, .., d_m$ เป็นตัวหารทั้งหมดของ n กรุปย่อยที่มีอันดับ $d_1 d_2, .., d_m$ คือ

$$\left\langle a^{\frac{n}{d_1}} \right\rangle, \left\langle a^{\frac{n}{d_2}} \right\rangle, ... , \left\langle a^{\frac{n}{d_m}} \right\rangle \text{ ตามลำดับ}$$

ตัวอย่างเช่นในกรุป $\mathbb{Z}_6$ ตัวหารของ 6 คือ $1, 2, 3$ และ 6 เนื่องจาก $\langle \bar{1} \rangle = \mathbb{Z}_6$ กรุปย่อยที่มีอันดับ $1, 2, 3$ และ 6 คือ $\left\langle \frac{6}{1}(\bar{1}) \right\rangle$, $\left\langle \frac{6}{2}(\bar{1}) \right\rangle$, $\left\langle \frac{6}{3}(\bar{1}) \right\rangle$ และ $\left\langle \frac{6}{3}(\bar{1}) \right\rangle$ ตามลำดับเขียนใหม่ได้เป็น

$$\langle \bar{0} \rangle, \langle \bar{3} \rangle, \langle \bar{2} \rangle \text{ และ } \langle \bar{1} \rangle \quad \text{ตามลำดับ}$$

ตัวอย่าง 3.2.23 จงหากรุปย่อยทั้งหมดของกรุปต่อไปนี้

1. $(\mathbb{Z}_8, +)$

2. $(\mathbb{Z}_{12}, +)$

ตัวอย่าง 3.2.24 จงหากรุปย่อยทั้งหมดของกรุป $\mathbb{Z}_{25}^{\times}$

ตัวอย่าง 3.2.25 จงหากรุปย่อยทั้งหมดของกรุป $\mathbb{Z}_2 \times \mathbb{Z}_3$

บทแทรก 3.2.26 ให้ G เป็นกรุปวัฏจักรจำกัด โดยที่ $|G| = n$ แล้ว

จำนวนกรุปย่อยทั้งหมดของ G เท่ากับ $\tau(n)$

เมื่อ $\tau(n)$ คือจำนวนตัวหารทั้งหมดของ n เรียกว่าฟังก์ชันเทา (Tau function)

สำหรับ $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ เป็นรูปแบบบัญญัติ โดยสมบัติของฟังก์ชันเทาจะได้ว่า

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

ข้อสังเกต 3.2.27 ให้ p เป็นจำนวนเฉพาะ และ n เป็นจำนวนนับ จะได้ว่า

1. กรุปย่อยของ $\mathbb{Z}_p$ มี 2 กรุปคือ

$$\{\bar{0}\} = \langle \bar{p} \rangle \quad \text{และ} \quad \langle \bar{1} \rangle = \mathbb{Z}_p$$

เนื่องจากตัวหารของ p มี 2 ตัวคือ 1 และ p

2. กรุปย่อยของ $\mathbb{Z}_{p^n}$ มี $p+1$ กรุปคือ

$$\{\bar{0}\} = \langle \bar{p}^n \rangle, \langle \bar{p}^{n-1} \rangle, \text{ .... }, \langle \bar{p}^2 \rangle, \langle \bar{p} \rangle \text{ และ } \langle \bar{1} \rangle = \mathbb{Z}_p$$

เนื่องจากตัวหารของ p^n มี $p+1$ ตัวคือ $1, p, p^2, ..., p^n$

ตัวอย่าง 3.2.28 จงหากรุปย่อยทั้งหมดของ $\mathbb{Z}_{625}$

ตัวอย่าง 3.2.29 จงหาจำนวนกรุปย่อยทั้งหมดของกรุปวัฏจักรต่อไปนี้

1. $\mathbb{Z}_{100}$
2. $\mathbb{Z}_{10} \times \mathbb{Z}_{25}$

จะเห็นได้ว่าใน S_3 ซึ่งไม่เป็นกรุปวัฏจักรจะไม่สอดคล้องกับทฤษฎีบท 3.2.22 เนื่องจากกรุปย่อยทั้งหมดคือ

กรุปย่อย	จำนวนสมาชิก (อันดับ)
$\langle(1)\rangle = \{(1)\}$	1
$\langle(1\ 2)\rangle =$	
$\langle(1\ 3)\rangle =$	
$\langle(2\ 3)\rangle =$	
$\langle(1\ 2\ 3)\rangle =$	

เห็นได้ว่ามีกรุปย่อยอันดับ 2 มากกว่าหนึ่งกรุป

บทแทรก 3.2.30 ให้ G เป็นกรุปวัฏจักรจำกัด ซึ่ง d หาร $|G|$ ลงตัว แล้ว

G จะมีสมาชิกอันดับ d จำนวน $\phi(d)$ ตัว

ตัวอย่าง 3.2.31 จงหาตัวก่อกำเนิดทั้งหมดของกรุปย่อยทุกกรุปของ $\mathbb{Z}_{12}$

วิธีทำ ให้ d เป็นตัวหารของ 12 พิจารณาได้จากตารางต่อไปนี้

d	กรุปย่อย	ตัวก่อกำเนิด	จำนวนตัวก่อกำเนิด
1	$\langle\bar{0}\rangle = \{\bar{0}\}$	$\bar{0}$	$\phi(1) = 1$
2			
3			
4			
6			
12			

ตัวอย่าง 3.2.32 จงหาตัวก่อกำเนิดทั้งหมดของกรุปย่อยทุกกรุปของ $\mathbb{Z}_{10}^{\times}$

ตัวอย่าง 3.2.33 จงหาตัวก่อกำเนิดทั้งหมดของกรุปย่อยทุกกรุปของ $\mathbb{Z}_2 \times \mathbb{Z}_5$

แบบฝึกหัด 3.2

1. จงหาตัวก่อกำเนิดทุกตัวของกรุปวัฏจักรต่อไปนี้

   1.1 $\mathbb{Z}_9$ 1.4 $\mathbb{Z}_{25}$ 1.7 $\mathbb{Z}_9^\times$ 1.10 $\mathbb{Z}_3 \times \mathbb{Z}_5$

   1.2 $\mathbb{Z}_{16}$ 1.5 $\mathbb{Z}_{45}$ 1.8 $\mathbb{Z}_{20}^\times$ 1.11 $\mathbb{Z}_4 \times \mathbb{Z}_7$

   1.3 $\mathbb{Z}_{17}$ 1.6 $\mathbb{Z}_{48}$ 1.9 $\mathbb{Z}_2 \times \mathbb{Z}_3$ 1.12 $\mathbb{Z}_4 \times \mathbb{Z}_9$

2. จงหาจำนวนตัวก่อกำเนิดทั้งหมดของกรุปวัฏจักรต่อไปนี้

   2.1 $\mathbb{Z}_{125}$ 2.3 $\mathbb{Z}_{3600}$ 2.5 $\mathbb{Z}_{18000}$ 2.7 $\mathbb{Z}_9 \times \mathbb{Z}_{32}$

   2.2 $\mathbb{Z}_{555}$ 2.4 $\mathbb{Z}_{11250}$ 2.6 $\mathbb{Z}_{49000}$ 2.8 $\mathbb{Z}_{100} \times \mathbb{Z}_{343}$

3. จงแสดงว่า $\mathbb{Z}_{25}^*$ เป็นกรุปวัฏจักร โดยมี $\bar{2}$ เป็นตัวก่อกำเนิด

4. จงตรวจสอบว่ากรุปไคลน์โฟว์เป็นกรุปวัฏจักรหรือไม่ พร้อมยกเหตุผลประกอบ

5. ให้ G เป็นกรุป และ $x \in G$ และ $m, n \in \mathbb{Z}$ จงพิสูจน์ว่า

   $$\text{ถ้า } x^m = 1 \text{ และ } x^n = 1 \text{ แล้ว } x^d = 1 \text{ เมื่อ } d = \gcd(m, n)$$

6. ให้ Gเป็นกรุป และ x เป็นสมาชิกที่ไม่ใช่เอกลักษณ์ของกรุปจำกัด G จงพิสูจน์ว่า

   $$\text{ถ้า } \circ(x) = n \text{ แล้ว } \circ(x^a) = \frac{n}{\gcd(a, n)} \text{ เมื่อ } a \text{ เป็นจำนวนเต็มที่ไม่ใช่ศูนย์}$$

7. จงหากรุปย่อยทั้งหมดของ

   7.1 $\mathbb{Z}_{10}$ 7.3 $\mathbb{Z}_{36}$ 7.5 $\mathbb{Z}_{10}^\times$ 7.7 $\mathbb{Z}_6 \times \mathbb{Z}_2$

   7.2 $\mathbb{Z}_{16}$ 7.4 $\mathbb{Z}_{60}$ 7.6 $\mathbb{Z}_{25}^\times$ 7.8 $\mathbb{Z}_3 \times \mathbb{Z}_8$

8. จงหาตัวก่อกำเนิดทั้งหมดของกรุปย่อยทุกกรุปของ

   8.1 $\mathbb{Z}_8$ 8.3 $\mathbb{Z}_{21}$ 8.5 $\mathbb{Z}_{10}^\times$ 8.7 $\mathbb{Z}_9 \times \mathbb{Z}_6$

   8.2 $\mathbb{Z}_{15}$ 8.4 $\mathbb{Z}_{32}$ 8.6 $\mathbb{Z}_{25}^\times$ 8.8 $\mathbb{Z}_{12} \times \mathbb{Z}_4$

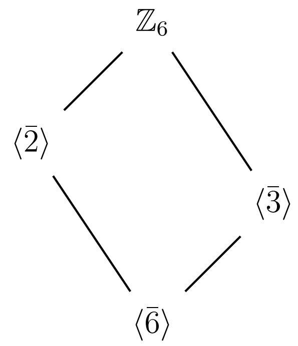
9. จงหาจำนวนกรุปย่อยของกรุปต่อไปนี้

   9.1 $\mathbb{Z}_{72}$ 9.2 $\mathbb{Z}_{150}$ 9.3 $\mathbb{Z}_{2019}$ 9.4 $\mathbb{Z}_{120} \times \mathbb{Z}_{32}$

10. จงหาตัวก่อกำเนิดทั้งหมดของ $\mathbb{Z}_{443171}$

3.3 แลตทิซของกรุปย่อย

ในหัวข้อนี้จะกล่าวถึงการแผนภาพการแสดงกรุปย่อยทั้งหมดของกรุปจำกัดซึ่งเรียกว่า **แลตทิซของกรุปย่อย** (the lattice of subgroups) ของกรุปจำกัด G หรือเรียกสั้น ๆ ว่า **แลตทิซ** (lattice) ซึ่งประกอบไปด้วย กรุปย่อยของ G และส่วนของเส้นตรงเชื่อมระหว่างกรุปย่อย A และ B เมื่อ $A \leq B$ และไม่มี $C \leq G$ ซึ่ง $A \leq C \leq B$ ($A \leq C$ และ $C \leq B$) โดย B จะถูกเขียนไว้เหนือ A ดังตัวอย่างต่อไปนี้ แลตทิซของ $\mathbb{Z}_6$



รูปที่ 2 แลตทิซของ $\mathbb{Z}_6$

เนื่องจาก $\mathbb{Z}_6$ เป็นกรุปวัฏจักรจึงมักนิยมเขียนแทนกรุปย่อยในรูปตัวก่อกำเนิด จะเห็นได้ว่ากรุปย่อย $\langle\bar{6}\rangle = \langle\bar{0}\rangle = \{\bar{0}\}$ จะเป็นกรุปย่อยที่อยู่ด้านล่างสุดของแลตทิซเสมอ และ กรุปย่อย $\mathbb{Z}_6 = \langle\bar{1}\rangle$ จะเป็นกรุปย่อยที่อยู่ด้านบนสุดของแลตทิซเสมอ

ข้อสังเกต 3.3.1 แลตทิซของกรุปจำกัด G จะมีกรุปย่อย $\{e\}$ อยู่ที่ด้านล่างสุดของแลตทิซเสมอ และกรุปย่อย G อยู่ด้านบนสุดของแลตทิซเสมอ

ตัวอย่าง 3.3.2 จงเขียนแลตทิซของ $\mathbb{Z}_{12}$

พิจารณาแลตทิซของกรุป $\mathbb{Z}_p$ เมื่อ p เป็นจำนวนเฉพาะ ซึ่งมีกรุปย่อยเพียง 2 กรุปเท่านั้นคือ $\langle \bar{p} \rangle$ และ $\mathbb{Z}_p$ จะเขียนแลตทิซได้ดังนี้

$$\begin{tikzcd}
\mathbb{Z}_2 \arrow[d, dash] & \mathbb{Z}_3 \arrow[d, dash] & \mathbb{Z}_5 \arrow[d, dash] & & \mathbb{Z}_p \arrow[d, dash] \\
\langle \overline{2} \rangle & \langle \overline{3} \rangle & \langle \overline{5} \rangle & \cdots & \langle \overline{p} \rangle
\end{tikzcd}$$

รูปที่ 4 แลตทิซของ $\mathbb{Z}_p$ เมื่อ p เป็นจำนวนเฉพาะ

สำหรับแลตทิซของกรุป $\mathbb{Z}_{p^n}$ เมื่อ p เป็นจำนวนเฉพาะ และ n เป็นจำนวนนับ ซึ่งมีกรุปย่อย $\langle \bar{p}^n \rangle$, $\langle \bar{p}^{n-1} \rangle$, ... , $\langle \bar{p}^2 \rangle$, $\langle \bar{p} \rangle$ และ $\mathbb{Z}_{p^n}$ เป็นจำนวนเฉพาะจะเขียนแลตทิซ ได้ดังนี้

$$\begin{tikzcd}
 & & & & \mathbb{Z}_{p^n} \arrow[d, dash] \\
 & & \mathbb{Z}_8 \arrow[d, dash] & & \langle \bar{p} \rangle \arrow[d, dash] \\
 & \mathbb{Z}_4 \arrow[d, dash] & \langle \bar{2} \rangle \arrow[d, dash] & & \langle \bar{p}^2 \rangle \arrow[d, dash, dashed] \\
\mathbb{Z}_2 \arrow[d, dash] & \langle \bar{2} \rangle \arrow[d, dash] & \langle \bar{4} \rangle \arrow[d, dash] & & \langle \bar{p}^{n-1} \rangle \arrow[d, dash] \\
\langle \overline{2} \rangle & \langle \bar{4} \rangle & \langle \bar{8} \rangle & \cdots & \langle \bar{p}^n \rangle
\end{tikzcd}$$

รูปที่ 5 แลตทิซของ $\mathbb{Z}_{p^n}$ เมื่อ p เป็นจำนวนเฉพาะ

ตัวอย่าง 3.3.3 จงเขียนแลตทิซของ $\mathbb{Z}_{81}$

ตัวอย่าง 3.3.4 จงเขียนแลตทิชของ $\mathbb{Z}_{36}$

ตัวอย่าง 3.3.5 จงเขียนแลตทิชของ $\mathbb{Z}_{10}^{\times}$

ตัวอย่าง 3.3.6 จงเขียนแลตทิซของ $\mathbb{Z}_7^*$

ตัวอย่าง 3.3.7 จงเขียนแลตทิซของ S_3

แบบฝึกหัด 3.3

1. จงเขียนแลตทิซของกรุปต่อไปนี้

   1.1 $\mathbb{Z}_3$ 1.3 $\mathbb{Z}_{24}$ 1.5 $\mathbb{Z}_{48}$ 1.7 $\mathbb{Z}_{225}$

   1.2 $\mathbb{Z}_{14}$ 1.4 $\mathbb{Z}_{25}$ 1.6 $\mathbb{Z}_{52}$ 1.8 $\mathbb{Z}_{1024}$

2. จงเขียนแลตทิซของกรุปต่อไปนี้

   2.1 $\mathbb{Z}_8^\times$ 2.2 $\mathbb{Z}_{11}^*$ 2.3 $\mathbb{Z}_{20}^\times$ 2.4 $\mathbb{Z}_{30}^\times$

3. จงเขียนแลตทิซของกรุปไคลน์โฟว์ K_4

4. จงเขียนแลตทิซของกรุปควอเทอร์เนียน Q_4

5. ให้ $G = \{1, -1, i, -i\} \subseteq \mathbb{C}$ จงเขียนแลตทิซของ $(G, \cdot)$

บทที่ 4

กรุปย่อยปกติ

ในส่วนแรกของบทนี้จะกล่าวถึงกรุปจำกัด G ความสัมพันธ์ของอันดับของกรุปย่อยกับอันดับของ G ซึ่งจะได้ข้อสรุปในทฤษฎีบทของลากรานจ์ จากนั้นศึกษากรุปย่อยปกติเพื่อนำไปสร้างกรุปชนิดที่แรกว่ากรุปผลหาร

4.1 โคเซตและทฤษฎีบทของลากรานจ์

ทฤษฎีบท 4.1.1 ให้ G เป็นกรุปและ $H \leq G$ นิยามความสัมพันธ์ $\sim$ ใน G โดย

$$a \sim b \qquad \text{ก็ต่อเมื่อ} \qquad ab^{-1} \in H$$

แล้วจะได้ว่า $\sim$ เป็นความสัมพันธ์สมมูล

ให้ $a \in G$ ชั้นสมมูลของ a มอดุโล $\sim$ เขียนแทนด้วย Ha คือ

$$Ha = \{x \in G : xa^{-1} \in H\} = \{x \in G : xa^{-1} = h \text{ เมื่อ } h \in H\} = \{ha : h \in H\}$$

ต่อไปจะเรียกว่าโคเซตขวาและขยายไปยังโคเซตซ้าย ดังนิยามต่อไปนี้

บทนิยาม 4.1.2 ให้ $(G, *)$ เป็นกรุปและ $H \leq G$ โดยที่ $a \in G$ กำหนดให้

$$H * a = \{h * a \,:\, h \in H\} \qquad \text{และ} \qquad a * H = \{a * h \,:\, h \in H\}$$

เรียกว่า **โคเซตขวา** (right coset) สำหรับ a ของ H ใน G และ **โคเซตซ้าย** (left coset) สำหรับ a ของ H ใน G ตามลำดับ และเรียก **โคเซต** (coset) เมื่อเป็นโคเซตขวาหรือโคเซตซ้าย

เรานิยมเขียน Ha และ aH แทน $H * a$ และ $a * H$ เช่นเดียวกับ ab แทน $a * b$

ข้อสังเกต 4.1.3 ให้ G เป็นกรุป จะได้ว่า

1. ถ้า G เป็นกรุปอาบีเลียน แล้ว $Ha = aH$ ทุก ๆ $a \in G$
2. $He = H = He$

ตัวอย่าง 4.1.4 ให้ $H = \langle \bar{2} \rangle$ โดยที่ $H \leq \mathbb{Z}_6$ จงแจกแจงสมาชิกของโคเซตต่อไปนี้

1. $\bar{1} + H$
2. $H + \bar{2}$
3. $H + \bar{3}$
4. $H + \bar{5}$

ตัวอย่าง 4.1.5 ให้ $H = 2\mathbb{Z}$ โดยที่ $H \leq \mathbb{Z}$ จงแจกแจงสมาชิกของโคเซตต่อไปนี้

1. $1 + H$
2. $H + 2$
3. $3 + H$
4. $4 + H$

ตัวอย่าง 4.1.6 ให้ $H = \langle (1\ 3) \rangle$ โดยที่ $H \leq S_3$ จงแจกแจงสมาชิกของโคเซตต่อไปนี้

1. $(1\ 2)H$

2. $H(1\ 2)$

3. $(2\ 3)H$

4. $H(2\ 3)$

ตัวอย่าง 4.1.7 จงแจกแจงสมาชิกของโคเซตต่อไปนี้

1. $\langle \bar{8} \rangle + \bar{1}$ ใน $\mathbb{Z}_{12}$

2. $\langle \bar{6} \rangle\, \bar{4}$ ใน $\mathbb{Z}_7^*$

3. $\langle (\bar{0}, \bar{2}) \rangle + (\bar{1}, \bar{3})$ ใน $\mathbb{Z}_2 \times \mathbb{Z}_6$

4. $1 + 5\mathbb{Z}$ ใน $\mathbb{Z}$

5. $(1\ 3)\,\langle (2\ 3) \rangle$ ใน S_3

ตัวอย่าง 4.1.8 ให้ $H = \langle A \rangle$ เมื่อ $A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ โดยที่ $H \leq GL_2(\mathbb{R})$

จงเขียนโคเซตต่อไปนี้ในรูปแบบมีเงื่อนไข

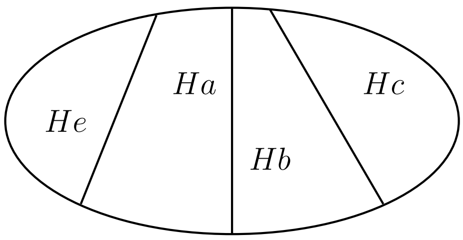
1. $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} H$

2. $H \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$

จากทฤษฎีบท 4.1.1 จะได้ว่าโคเซตเป็นชั้นสมมูล ดังนั้นเซตของโคเซตเป็นผลแบ่งกันของกรุป G นั่นคือ

$$G = \bigcup_{a \in G} Ha \qquad \text{และ} \qquad G = \bigcup_{a \in G} aH$$

สำหรับกรุป G ที่มีโคเซตขวาที่แตกต่างกันทั้งหมด 4 เซตคือ He, Ha, Hb และ Hc อาจแสดงตัวอย่างการแบ่งกั้นได้ดังรูปต่อไปนี้



สำหรับ $a, b \in G$ ใด ๆ ผลจากทฤษฎีบท 1.4.7 จะได้สมบัติดังต่อไปนี้

1. $Ha \cap Hb \neq \varnothing \quad \longleftrightarrow \quad ab^{-1} \in H \quad \longleftrightarrow \quad Ha = Hb$

2. $aH \cap bH \neq \varnothing \quad \longleftrightarrow \quad a^{-1}b \in H \quad \longleftrightarrow \quad aH = bH$

ทฤษฎีบท 4.1.9 ให้ H เป็นกรุปย่อยของกรุป G โดยที่ $a, b \in G$
สำหรับโคเซตขวา ข้อความต่อไปนี้สมมูลกัน

1. $ab^{-1} \in H$
2. มี $h \in H$ ซึ่ง $a = hb$
3. $a \in Hb$
4. $Ha = Hb$

สำหรับโคเซตซ้าย ข้อความต่อไปนี้สมมูลกัน

1. $a^{-1}b \in H$
2. มี $h \in H$ ซึ่ง $b = ah$
3. $b \in aH$
4. $aH = bH$

ตัวอย่าง 4.1.10 ให้ $H = \langle \bar{4} \rangle$ โดยที่ $H \leq \mathbb{Z}_{12}$ จงหาโคเซตทั้งหมดที่เท่ากับโคเซต $\bar{1} + H$

ตัวอย่าง 4.1.11 ให้ $H = \langle (1\ 3) \rangle$ โดยที่ $H \leq S_3$ จงหาโคเซตทั้งหมดที่เท่ากับโคเซต $(1\ 2)H$

ต่อไปจะสนใจจำนวนอันดับหรือจำนวนสมาชิกของโคเซต โดยการสังเกตจากอย่างที่ผ่านมา สำหรับกรุปจำกัดแล้วจะได้ว่า

$$|Ha| = |H| = |bH|$$

ดังที่จะได้ตามบทแทรก 4.1.13

ทฤษฎีบท 4.1.12 ให้ H เป็นกรุปย่อยของกรุป G และ $a, b \in G$ จะได้ว่า

มีฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึงจาก aH ไป Hb

บทแทรก 4.1.13 ให้ H เป็นกรุปย่อยของกรุปจำกัด G และ $a, b \in G$ จะได้ว่า

$$|Ha| = |H| = |bH|$$

ตัวอย่าง 4.1.14 จงหาโคเซตทั้งหมดของ $\langle \bar{3} \rangle$ ใน $\mathbb{Z}_{12}$

ตัวอย่าง 4.1.15 จงหาโคเซตทั้งหมดของ $\langle(1\ 2)\rangle$ ใน S_3

จากตัวอย่าง 4.1.15 จะเห็นได้ว่าจำนวนที่แตกต่างกันของโคเซตซ้ายเท่ากับโคเซตขวา ดังจะได้ดังทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.1.16 ให้ H เป็นกรุปย่อยของกรุป G กำหนดให้

$$\mathcal{R}(H) = \{Ha \,:\, a \in G\} \qquad \text{และ} \qquad \mathcal{L}(H) = \{aH \,:\, a \in G\}$$

จะได้ว่ามีฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึงจาก $\mathcal{R}(H)$ ไป $\mathcal{L}(H)$

บทนิยาม 4.1.17 ให้ H เป็นกรุปย่อยของกรุปจำกัด G แล้วจำนวนสมาชิกของ $\mathcal{R}(H)$ หรือ $\mathcal{L}(H)$ จะเรียกว่า **ดรรชนี** (index) ของ H ใน G เขียนแทนด้วย $[G : H]$

ตัวอย่าง 4.1.18 จงหาดรรชนี $[G : H]$ เมื่อกำหนดให้

1. $G = \mathbb{Z}_{12}$ และ $H = \langle \bar{4} \rangle$

2. $G = \mathbb{Z}_7^*$ และ $H = \langle \bar{2} \rangle$

3. $G = \mathbb{Z}_2 \times \mathbb{Z}_4$ และ $H = \langle (\bar{0}, \bar{2}) \rangle$

จากตัวอย่าง 4.1.18 เห็นได้ว่าการหาจำนวนโคเซตจะมีความยุ่งยากมากขึ้นเมื่อกรุปจำกัดมีอันดับมากขึ้น ได้มีนักคณิตศาสตร์ชาวฝรั่งเศสผู้โด่งดังนามว่า โฌแซฟ-หลุยส์ ลากรานจ์ (Joseph-Louis Lagrange) ได้ค้นพบความสัมพันธ์ของอันดับของกรุปย่อยกับกรุปของมันเอง ซึ่งถูกเรียกว่า ทฤษฎีบทของลากรานจ์ ทำให้เราเข้าใจโครงสร้างเกี่ยวกับกรุปมากยิ่งขึ้น ดังจะกล่าวต่อไปนี้

ทฤษฎีบท 4.1.19 **ทฤษฎีบทของลากรานจ์** (Lagrange's Theorem)
ให้ H เป็นกรุปย่อยของกรุปจำกัด G แล้วจะได้ว่า $|H|$ หาร $|G|$ ลงตัว และ

$$[G : H] = \frac{|G|}{|H|}$$

บทแทรก 4.1.20 ให้ G เป็นกรุปจำกัดที่มีอันเป็นจำนวนเฉพาะ แล้ว

1. G มีกรุปย่อยเพียง 2 กรุปเท่านั้นคือ $\{e\}$ และ G
2. G เป็นกรุปวัฏจักร
3. สมาชิกทุกตัวที่ไม่ใช่เอกลักษณ์เป็นตัวก่อกำเนิดของ G

บทแทรก 4.1.21 ให้ a เป็นสมาชิกของกรุป G โดยที่ $|G| = n$ จะได้ว่า $a^n = e$

ตัวอย่าง 4.1.22 จงหาดรรชนี $[G : H]$ ที่กำหนดให้ต่อไปนี้โดยใช้ทฤษฎีบทของลากรานจ์

1. $G = \mathbb{Z}_{12}$ และ $H = \langle \bar{3} \rangle$
2. $G = \mathbb{Z}_{30}$ และ $H = \langle \overline{10} \rangle$
3. $G = \mathbb{Z}_{20}^{\times}$ และ $H = \langle \overline{11} \rangle$
4. $G = \mathbb{Z}_3 \times \mathbb{Z}_6$ และ $H = \langle (\bar{0}, \bar{2}) \rangle$
5. $G = S_3$ และ $H = \langle (1\,2) \rangle$
6. $G = S_7$ และ $H = \langle (1\ 3\,4\ 5\ 6) \rangle$

ตัวอย่าง 4.1.23 จงหา $[\mathbb{Z}_{25}^{\times} : \langle \bar{7} \rangle]$

แบบฝึกหัด 4.1

1. ให้ H เป็นกรุปย่อยของกรุป G โดยที่ $a, b \in G$ จงแสดงว่าข้อความต่อไปนี้สมมูลกัน

   1. $ab^{-1} \in H$
   2. มี $h \in H$ ซึ่ง $a = hb$
   3. $a \in Hb$
   4. $Ha = Hb$

2. จงแจกแจงสมาชิกของโคเซตต่อไปนี้

   2.1 $\bar{2} + \langle \bar{3} \rangle$ ใน $\mathbb{Z}_{12}$
   2.2 $\bar{4} + \langle \bar{2} \rangle$ ใน $\mathbb{Z}_{18}$
   2.3 $\bar{6} + \langle \bar{8} \rangle$ ใน $\mathbb{Z}_{21}$
   2.4 $\langle \bar{5} \rangle + \bar{3}$ ใน $\mathbb{Z}_{20}$
   2.5 $\langle \overline{11} \rangle + \bar{7}$ ใน $\mathbb{Z}_{30}^{\times}$
   2.6 $\bar{8} + \langle \bar{7} \rangle$ ใน $\mathbb{Z}_{25}^{*}$
   2.7 $\langle (\bar{2}, \bar{3}) \rangle + (\bar{1}, \bar{4})$ ใน $\mathbb{Z}_4 \times \mathbb{Z}_6$
   2.8 $(\bar{2}, \bar{3}) + \langle (\bar{0}, \bar{4}) \rangle$ ใน $\mathbb{Z}_3 \times \mathbb{Z}_{12}$
   2.9 $7\mathbb{Z} + 2$ ใน $\mathbb{Z}$
   2.10 $6\mathbb{Z} + 15$ ใน $\mathbb{Z}$
   2.11 $(1\ 3\ 2)\, \langle (1\ 2) \rangle$ ใน S_3
   2.12 $\langle (3\ 2) \rangle\, (3\ 4)$ ใน S_4

3. ให้ $H = \langle A \rangle$ เมื่อ $A = \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}$ โดยที่ $H \leq GL_2(\mathbb{R})$ จงแจกแจงสมาชิกของโคเซต

   3.1 $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} H$
   3.2 $H \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
   3.3 $\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} H$
   3.4 $H \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$
   3.5 $\begin{bmatrix} 1 & 3 \\ 0 & 3 \end{bmatrix} H$
   3.6 $H \begin{bmatrix} 1 & 3 \\ 0 & 3 \end{bmatrix}$

4. จงหาดรรชนี $[G : H]$ เมื่อกำหนดให้

   4.1 $G = \mathbb{Z}_{24}$ และ $H = \langle \bar{4} \rangle$
   4.2 $G = \mathbb{Z}_{27}$ และ $H = \langle \bar{3} \rangle$
   4.3 $G = \mathbb{Z}_{30}$ และ $H = \langle \bar{6} \rangle$
   4.4 $G = \mathbb{Z}_{36}$ และ $H = \langle \overline{12} \rangle$
   4.5 $G = \mathbb{Z}_{20}^{\times}$ และ $H = \langle \overline{13} \rangle$
   4.6 $G = \mathbb{Z}_8 \times \mathbb{Z}_{10}$ และ $H = \langle (\bar{2}, \bar{2}) \rangle$
   4.7 $G = S_5$ และ $H = \langle (1\ 3\ 5) \rangle$
   4.8 $G = S_6$ และ $H = \langle (2\ 3\ 4) \rangle$

5. จงหาดรรชนีต่อไปนี้

   5.1 $[\mathbb{Z}_{12} : \langle \bar{6} \rangle]$
   5.2 $[\mathbb{Z}_{18} : \langle \bar{3} \rangle]$
   5.3 $[\mathbb{Z}_{50} : \langle \overline{15} \rangle]$
   5.4 $[\mathbb{Z}_{30}^{\times} : \langle \bar{7} \rangle]$
   5.5 $[\mathbb{Z}_{12} \times \mathbb{Z}_{10} : \langle (\bar{3}, \bar{5}) \rangle]$
   5.6 $[S_9 : \langle (1\ 3)(5\ 6)(2\ 7\ 9) \rangle]$

6. ให้ G เป็นกรุปจำกัดโดยที่ $|G| = n$ จงพิสูจน์ว่า $a^k = e$ ก็ต่อเมื่อ $k \mid n$

7. ให้ H เป็นกรุปย่อยของกรุป G กำหนดให้

$$f : \mathcal{R}(H) \to \mathcal{L}(H) \quad \text{นิยามโดย} \quad f(Ha) = b^{-1}H \quad \text{เมื่อ } a \in G$$

   จงพิสูจน์ว่า f เป็นฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึงจาก $\mathcal{R}(H)$ ไป $\mathcal{L}(H)$

4.2 นิยามและสมบัติของกรุปย่อยปกติ

บทนิยาม 4.2.1 ให้ H และ K เป็นเซตย่อยของ G โดยที่ $g \in G$ กำหนดให้

$$gHg^{-1} = \{ghg^{-1} : h \in H\} \qquad \text{และ} \qquad HK = \{hk : h \in H \text{ และ } k \in K\}$$

ข้อสังเกต 4.2.2 ให้ H และ K เป็นเซตย่อยของ G แล้ว

1. ถ้า $H \subseteq K$ แล้ว $gHg^{-1} \subseteq gKg^{-1}$ ทุก ๆ $g \in G$
2. ถ้า G เป็นกรุปอาบีเลียน $gHg^{-1} = H$ ทุก ๆ $g \in G$
3. ถ้า H และ K เป็นกรุปย่อยของกรุปอาบีเลียน แล้ว $HK = KH$

ตัวอย่าง 4.2.3 จงหา gHg^{-1}, HK และ KH ใน $\mathbb{Z}_{12}$ เมื่อกำหนดให้

$$H = \{\bar{1}, \bar{4}, \bar{8}\}, \quad K = \{\bar{2}, \bar{3}\} \quad \text{และ} \quad g = \bar{7}$$

ตัวอย่าง 4.2.4 จงหา gHg^{-1} ใน S_3 เมื่อ $H = \langle(1\ 2\ 3)\rangle$ และ $g = (1\ 3\ 2)$

ตัวอย่าง 4.2.5 จงหา gHg^{-1}, HK และ KH ใน S_3 เมื่อกำหนดให้

$$H = \langle(2\ 3)\rangle, \quad K = \langle(1\ 3)\rangle \quad \text{และ} \quad g = (1\ 2\ 3)$$

ข้อสังเกต 4.2.6 ให้ H และ K เป็นเซตย่อยของ G แล้ว

1. ถ้า $g \in H$ และ $H \leq G$ แล้ว $gHg^{-1} = H$
2. $HK = \bigcup_{h \in H} hK = \bigcup_{k \in K} Hk$

บทนิยาม 4.2.7 ให้ N กรุปย่อยของกรุป G จะกล่าวว่า N เป็น **กรุปย่อยปกติ** (normal subgroup) เขียนแทนด้วย $N \trianglelefteq G$ ก็ต่อเมื่อ

$$gNg^{-1} = N \qquad \text{ทุก ๆ } g \in G$$

ข้อสังเกต 4.2.8 ให้ $N \leq G$ จะได้ว่า

1. $\{e\}$ และ G เป็นกรุปย่อยปกติเสมอ
2. ถ้า G กรุปอาบีเลียน แล้ว $N \trianglelefteq G$ ทุก $N \leq G$

ตัวอย่าง 4.2.9 จงตรวจสอบว่ากรุปย่อย $\langle(1\ 2)\rangle$ และ $\langle(1\ 2\ 3)\rangle$ เป็นกรุปย่อยปกติของ S_3 หรือไม่

ทฤษฎีบท 4.2.10 **เกณฑ์การพิจารณากรุปย่อยปกติ** (The Normal Subgroup Criterion)
ให้ N เป็นกรุปย่อยของกรุป G แล้วข้อความต่อไปนี้สมมูลกัน

(1) $N \trianglelefteq G$

(2) $gNg^{-1} = N$ ทุก ๆ $g \in G$

(3) $gN = Ng$ ทุก ๆ $g \in G$

(4) $(Ng)(Nh) = N(gh)$ ทุก ๆ $g, h \in G$

(5) $(gN)(hN) = (gh)N$ ทุก ๆ $g, h \in G$

(6) $gNg^{-1} \subseteq N$ ทุก ๆ $g \in G$

ทฤษฎีบท 4.2.11 ให้ G เป็นกรุป ถ้า $N \trianglelefteq G$ และ $K \trianglelefteq G$ แล้ว $N \cap K \trianglelefteq G$

เมื่อพิจารณากรุป S_3 ให้ $H = \langle (1\ 2) \rangle$ และ $K = \langle (1\ 3) \rangle$ จะได้ว่า

$$HK = \langle (1\ 2) \rangle \langle (1\ 3) \rangle = \{(1), (1\ 2)\}\{(1), (1\ 3)\} = \{\{(1), (1\ 2), (1\ 3), (1\ 2\ 3)\}$$

จะเห็นได้ว่า HK ไม่เป็นกรุปย่อยของ S_3 นั่นหมายความว่าถ้า H และ K เป็นกรุปย่อยของ G ไม่จำเป็นว่า $HK \leq G$ ข้อความดังกล่าวจะเป็นจริงถ้าสอดคล้องทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.2.12 ให้ H และ K เป็นกรุปย่อยของกรุป G จะได้ว่า

$$HK \leq G \qquad \text{ก็ต่อเมื่อ} \qquad HK = KH$$

ถ้า G เป็นกรุปอาบีเลียน จะได้ว่า $HK = KH$ โดยทฤษฎีบท 4.2.12 สรุปได้ว่า $HK \leq G$ นั่นหมายความว่าสำหรับกรุปอาบีเลียน G จะได้ว่า

$$HK \leq G \qquad \text{ทุก ๆ } H \leq G \text{ และ } K \leq G$$

บทแทรก 4.2.13 ให้ H และ K เป็นกรุปย่อยของกรุป G จะได้ว่า

1. ถ้า $H \trianglelefteq G$ หรือ $K \trianglelefteq G$ แล้ว $HK \leq G$
2. ถ้า $K \trianglelefteq G$ แล้ว $H \cap K \trianglelefteq K$ และ $K \trianglelefteq HK$

ทฤษฎีบท 4.2.14 ให้ H และ K เป็นกรุปย่อยจำกัดของกรุป G แล้ว

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

ทฤษฎีบท 4.2.15 ให้ N เป็นกรุปย่อยของกรุป G จะได้ว่า

$$\text{ถ้า} \quad [G:N]=2 \quad \text{แล้ว} \quad N \trianglelefteq G$$

ตัวอย่าง 4.2.16 กรุปย่อย $\langle(1\ 3\ 2)\rangle$ เป็นกรุปย่อยปกติของ S_3 หรือไม่

แบบฝึกหัด 4.2

1. จงหา gHg^{-1}, HK และ KH เมื่อกำหนดให้

   1.1 $H = \{\bar{0}, \bar{1}, \bar{2}\}$, $K = \{\bar{2}, \bar{3}, \bar{4}\}$ และ $g = \bar{3}$ ใน $\mathbb{Z}_5$

   1.2 $H = \langle \bar{4} \rangle$, $K = \{\bar{0}, \bar{7}, \bar{8}\}$, และ $g = \bar{2}$ ใน $\mathbb{Z}_{15}$

   1.3 $H = \langle \bar{8} \rangle$, $K = \langle \bar{3} \rangle$ และ $g = \overline{13}$ ใน $\mathbb{Z}_{18}$

   1.4 $H = \langle \bar{3} \rangle$, $K = \langle \bar{5} \rangle$ และ $g = \bar{8}$ ใน $\mathbb{Z}_{20}^{\times}$

   1.5 $H = \langle (\bar{0}, \bar{2}) \rangle$, $K = \langle (\bar{2}, \bar{0}) \rangle$ และ $g = (\bar{1}, \bar{3})$ ใน $\mathbb{Z}_4 \times \mathbb{Z}_6$

   1.6 $H = \langle (1\,3\,2) \rangle$, $K = \langle (2\,3) \rangle$ และ $g = (1\,3)$ ใน S_3

2. กำหนดให้ $H = \langle A \rangle$ และ $K = \langle B \rangle$ โดยที่ $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ และ $B = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ ใน $GL_2(\mathbb{R})$ ถ้า $C = \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}$ และ $D = \begin{bmatrix} 1 & 1 \\ 4 & 3 \end{bmatrix}$ จงเขียนเซตต่อไปนี้ในรูปแบบมีเงื่อนไข

   2.1 HK 2.2 KH 2.3 CHC^{-1} 2.4 DKD^{-1}

3. จงหากรุปย่อยปกติทั้งหมดของ

   3.1 $\mathbb{Z}_{18}$ 3.2 $\mathbb{Z}_{20}^{\times}$ 3.3 $\mathbb{Z}_4 \times \mathbb{Z}_6$ 3.4 S_3

4. เรียกกรุป G ว่า **กรุปเชิงเดี่ยว (simple group)** ถ้ากรุปย่อยปกติของ G มีเพียง 2 กรุปเท่านั้น คือ $\{e\}$ และ G จงแสดงว่า $\mathbb{Z}_p$ กรุปเชิงเดี่ยว เมื่อ p เป็นจำนวนเฉพาะที่มากกว่า 2

5. จงตรวจสอบว่า S_3 เป็นกรุปเชิงเดี่ยวหรือไม่

6. จงพิสูจน์ว่า ถ้า G เป็นกรุปอาบีเลียนซึ่งมีกรุปย่อยอันดับ n และ m แล้ว G จะมีกรุปย่อยอันดับ $\ell\mathrm{cm}(m, n)$

7. ให้ G เป็นกรุป จงพิสูจน์ว่า ถ้า $N \trianglelefteq G$ และ N เป็นกรุปวัฏจักร แล้วทุกกรุปย่อยของ N จะเป็นกรุปย่อยปกติของ G

8. ให้ G เป็นกรุปจำกัด และ $N \trianglelefteq G$ โดยที่ $[G : N]$ และ $|N|$ เป็นจำนวนเฉพาะสัมพัทธ์ จงพิสูจน์ว่า ถ้า $x \in G$ ซึ่ง $x^{|N|} = e$ แล้ว $x \in N$

9. ให้ G เป็นกรุป จงแสดงว่า ถ้า $M \trianglelefteq G$ และ $N \trianglelefteq G$ แล้ว $MN \trianglelefteq G$.

10. ให้ H และ K เป็นกรุปย่อยของกรุป G จงพิสูจน์ว่า

$$\text{ถ้า } K \trianglelefteq G \text{ แล้ว } H \cap K \trianglelefteq K \text{ และ } K \trianglelefteq HK$$

4.3 กรุปผลหาร

ในหัวข้อนี้จะกล่าวถึงการสร้างกรุปบนเซตของโคเซตขวาของ N ในกรุป G โดยที่ $N \trianglelefteq G$ เพื่อที่จะนิยามการดำเนินทวิภาคให้สอดคล้องกับทฤษฎีบท 4.2.10 ข้อ 4 ซึ่งจะเรียกว่ากรุปผลหาร จากนั้นศึกษาสมบัติของกรุปผลหาร โดยเริ่มต้นจากทฤษฎีบทต่อไปนี้

ทฤษฎีบท 4.3.1 ให้ G เป็นกรุป และ $N \trianglelefteq G$ นิยามการดำเนินการทวิภาค $*$ ใน $\mathcal{R}(N)$ โดย

$$(Ng) * (Nh) = (Ng)(Nh) \qquad \text{เมื่อ } g, h \in G$$

จะได้ว่า

1. $(\mathcal{R}(N), *)$ เป็นกรุป
2. ถ้า G เป็นกรุปอาบีเลียน แล้ว $(\mathcal{R}(N), *)$ เป็นกรุปอาบีเลียน
3. ถ้า G เป็นกรุปวัฏจักร แล้ว $(\mathcal{R}(N), *)$ เป็นกรุปวัฏจักร

จากบทพิสูจน์ของทฤษฎีบท 4.3.1 จะได้ว่า

1. N เป็นเอกลักษณ์ในกรุป $(\mathcal{R}(N), *)$
2. ตัวผกผันของ Ng คือ Ng^{-1} ดังนั้น $(Ng)^{-1} = Ng^{-1}$
3. $(Ng)^n = Ng^n$ เมื่อ $n \in \mathbb{Z}$
4. ถ้า G เป็นกรุปวัฏจักรซึ่งมี a เป็นตัวก่อกำเนิด แล้ว Na เป็นตัวก่อกำเนิดของ $\mathcal{R}(N)$

จากนี้ไปจะเขียน $(Ng)(Nh)$ แทน $(Ng) * (Nh)$ เมื่อกล่าวถึงกรุป $(\mathcal{R}(N), *)$

บทนิยาม 4.3.2 ให้ G เป็นกรุป และ $N \trianglelefteq G$ แล้วกรุป $(\mathcal{R}(N), *)$ ในทฤษฎีบท 4.3.1 จะเรียกว่า **กรุปผลหาร** (quotient group) ของ G เขียนแทนด้วย G/N

ข้อสังเกต 4.3.3 ถ้า G เป็นกรุปจำกัด และ $N \trianglelefteq G$ แล้ว

$$|G/N| = [G : N] = \frac{|G|}{|N|}$$

ตัวอย่าง 4.3.4 จงแจกแจงสมาชิกของกรุปผลหารต่อไปนี้

1. $\mathbb{Z}_6/\langle\bar{3}\rangle$
2. $\mathbb{Z}_{12}/\langle\bar{4}\rangle$
3. $\mathbb{Z}_7^*/\langle\bar{2}\rangle$
4. $\mathbb{Z}_{10}^*/\langle\bar{3}\rangle$
5. $\mathbb{Z}_2 \times \mathbb{Z}_6/\langle(\bar{0}, \bar{2})\rangle$
6. $S_3/\langle(1\,2\,3)\rangle$

ตัวอย่าง 4.3.5 จงแจกแจงสมาชิกของกรุปผลหารต่อไปนี้

1. $\mathbb{Z}/3\mathbb{Z}$

2. $\mathbb{Z}/4\mathbb{Z}$

3. $\mathbb{Z}/7\mathbb{Z}$

ตัวอย่าง 4.3.6 จงหาตัวก่อกำเนิดทั้งหมดของกรุปผลหารต่อไปนี้

1. $\mathbb{Z}_{12}/\langle\bar{3}\rangle$

2. $\mathbb{Z}_7^*/\langle\bar{2}\rangle$

3. $\mathbb{Z}_2 \times \mathbb{Z}_5/\langle(\bar{1},\bar{0})\rangle$

ทฤษฎีบท 4.3.7 ให้ $n, r \in \mathbb{N}$ โดยที่ $0 \leq r < n$ สมมติว่า $n\mathbb{Z} + r$ เป็นตัวก่อกำเนิด $\mathbb{Z}/n\mathbb{Z}$ ถ้า $k \in \mathbb{N}$ ซึ่ง $1 \leq k < n$ จะได้ว่า

$$n\mathbb{Z} + kr \text{ เป็นตัวก่อกำเนิดของ } \mathbb{Z}/n\mathbb{Z} \qquad \text{ก็ต่อเมื่อ} \qquad \gcd(n, k) = 1$$

ตัวอย่าง 4.3.8 จงหาตัวก่อกำเนิดทั้งหมดของ $\mathbb{Z}/6\mathbb{Z}$

ทฤษฎีบท 4.3.9 ให้ G เป็นกรุป และ $N \trianglelefteq G$ และ $[G : N] = n$ จะได้ว่า

1. $a^n = N$ สำหรับทุก ๆ $a \in G/N$
2. $g^n \in N$ สำหรับทุก ๆ $g \in G$

บทแทรก 4.3.10 ให้ G เป็นกรุป และ $N \leq G$ ซึ่ง $[G : N] = 2$ จะได้ว่า

$$g^2 \in N \qquad \text{ทุก ๆ } g \in G$$

แบบฝึกหัด 4.3

1. จงแจกแจงสมาชิกของกรุปผลหารต่อไปนี้

   1.1 $\mathbb{Z}_6/\langle\bar{2}\rangle$ 1.3 $\mathbb{Z}_{24}/\langle\bar{4}\rangle$ 1.5 $\mathbb{Z}_{20}^{\times}/\left\langle\overline{11}\right\rangle$

   1.2 $\mathbb{Z}_{12}/\langle\bar{8}\rangle$ 1.4 $\mathbb{Z}_{25}^{\times}/\left\langle\bar{7}\right\rangle$ 1.6 $S_3/\langle(1\,3\,2)\rangle$

2. จงหาตัวก่อกำเนิดทั้งหมดของกรุปผลหารต่อไปนี้

   2.1 $\mathbb{Z}_8/\langle\bar{2}\rangle$ 2.3 $\mathbb{Z}_{24}/\langle\bar{4}\rangle$ 2.5 $\mathbb{Z}_{20}^{\times}/\left\langle\overline{11}\right\rangle$

   2.2 $\mathbb{Z}_{12}/\langle\bar{6}\rangle$ 2.4 $\mathbb{Z}_{25}^{\times}/\left\langle\bar{7}\right\rangle$ 2.6 $\mathbb{Z}_4 \times \mathbb{Z}_9/\langle(\bar{2},\bar{3})\rangle$

3. ให้ G เป็นกรุป จงพิสูจน์ว่า

   ถ้า $N \trianglelefteq G$, $M \trianglelefteq G$ และ $N \cap M = \{e\}$ แล้ว $nm = mn$ ทุก ๆ $n, m \in N$

4. ให้ G เป็นกรุป และ $H \leq G$ จงแสดงว่า $\displaystyle\bigcap_{g\in G} gHg^{-1} \trianglelefteq G$

5. จงแสดงว่ามีกรุปอันดับ 9 เป็นกรุปอาบีเลียน

บทที่ 5

สมสัณฐาน

กรุปแต่ละกรุปนั้นมีโครงสร้างที่แตกต่างกัน แต่อาจสัมพันธ์กันได้เช่นกรุปวัฏจักรจำกัดที่มีสมาชิกเท่ากันจะมีจำนวนตัวก่อกำเนิดเท่ากัน มากไปกว่านั้นนักคณิตศาสตร์อยากทราบว่าสองกรุปใด ๆ จะมีความสัมพันธ์กันเรื่องใดบ้าง เช่น เอกลักษณ์ ตัวผกผัน ตัวก่อกำเนิด หรือแม้กระทั่งกรุปย่อย ซึ่งเราจะศึกษาสมบัติต่าง ๆ ที่จะเกิดขึ้นในบทเรียนนี้

5.1 ฟังก์ชันสาทิสสัณฐาน

บทนิยาม 5.1.1 ให้ $(G, *)$ และ $(G', \circledast)$ เป็นกรุป
เรียกฟังก์ชัน $\varphi : G \to G'$ ว่า **ฟังก์ชันสาทิสสัณฐาน** (homomorphism) ถ้า

$$\varphi(x * y) = \varphi(x) \circledast \varphi(y) \qquad \text{ทุก ๆ } x, y \in G$$

และ **เคอร์เนล** (kernel) ของ φ เขียนแทนด้วย Ker(φ) นิยามโดย

$$\text{Ker}(\varphi) = \{x \in G \,:\, \varphi(x) = e'\}$$

เมื่อ e' เป็นเอกลักษณ์ของ G'

บางครั้งอาจละการเขียนเครื่องหมายการดำเนินทวิภาค โดยเขียน $\varphi(xy) = \varphi(x)\varphi(y)$ แทนการเขียน $\varphi(x * y) = \varphi(x) \circledast \varphi(y)$

ตัวอย่าง 5.1.2 ให้ G และ G' เป็นกรุป เมื่อ e' เป็นเอกลักษณ์ของ G'
จงตรวจสอบว่า φ เป็นฟังก์ชันสาทิสสัณฐานหรือไม่

1. ให้ $\varphi : G \to G'$ นิยามโดย $\quad \varphi(x) = e' \quad$ เมื่อ $x \in G$

2. ให้ $\varphi : G \to G$ นิยามโดย $\quad \varphi(x) = x^{-1} \quad$ เมื่อ $x \in G$

จากตัวอย่าง 5.1.2 ข้อ 2 จึงสรุปได้ว่าถ้า G เป็นกรุปอาบีเลียนแล้ว

$$\varphi : G \to G \quad \text{นิยามโดย } \varphi(x) = x^{-1}$$

เป็นฟังก์ชันสาทิสสัณฐาน

ตัวอย่าง 5.1.3 จงตรวจสอบว่า φ เป็นฟังก์ชันสาทิสสัณฐานหรือไม่

1. ให้ $\varphi : (GL_2(\mathbb{R}), \cdot) \to (\mathbb{R}^*, \cdot)$ นิยามโดย $\varphi(A) = \det(A)$

2. ให้ $\varphi : (M_{nn}(\mathbb{R}), +) \to (\mathbb{R}, +)$ นิยามโดย $\varphi(A) = \det(A)$

ตัวอย่าง 5.1.4 จงตรวจสอบว่า φ เป็นฟังก์ชันสาทิสสัณฐานหรือไม่ และหา Ker(φ)

1. ให้ $\varphi : (\mathbb{C}^*, \cdot) \to (\mathbb{R}^*, \cdot)$ นิยามโดย $\varphi(z) = |z|$ เมื่อ $z \in \mathbb{C}^*$

2. ให้ $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}_6, +)$ นิยามโดย $\varphi(x) = \bar{x}$ เมื่อ $x \in \mathbb{Z}$

ขยายแนวคิดจากตัวอย่าง 5.1.4 ข้อ 2 สำหรับ $n \in \mathbb{N}$ จะได้ว่า

$$\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +) \quad \text{นิยามโดย} \quad \varphi(x) = \bar{x}$$

เป็นฟังก์ชันสาทิสสัณฐาน โดยมี Ker$(\varphi) = n\mathbb{Z}$

ตัวอย่าง 5.1.5 ให้ $\varphi : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ นิยามโดย $\varphi(x) = \cos x + i \sin x$ เมื่อ $x \in \mathbb{R}$ จงแสดงว่า φ เป็นฟังก์ชันสาทิสสัณฐาน และหา Ker(φ)

ตัวอย่าง 5.1.6 ให้ $\varphi : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ นิยามโดย $\varphi(x) = \ell n(x)$ เมื่อ $x \in \mathbb{R}^+$ จงแสดงว่า φ เป็นฟังก์ชันสาทิสสัณฐาน และหา Ker(φ)

ตัวอย่าง 5.1.7 ให้ $\varphi : (\mathbb{R}^2, +) \to (\mathbb{R}, +)$ นิยามโดย $\varphi((x, y)) = x + y$ เมื่อ $x, y \in \mathbb{R}$ จงแสดงว่า φ เป็นฟังก์ชันสาทิสสัณฐาน และหา Ker(φ)

ทฤษฎีบท 5.1.8 ให้ G เป็นกรุป และ $N \trianglelefteq G$ ให้ $\pi : G \to G/N$ นิยามโดย

$$\pi(g) = Ng \qquad \text{ทุก ๆ } g \in G$$

แล้ว π เป็นฟังก์ชันสาทิสสัณฐานแบบทั่วถึง
ซึ่งจะเรียกว่า **ฟังก์ชันสาทิสสัณฐานธรรมชาติ** (natural homomorphism)

ทฤษฎีบท 5.1.9 ให้ G และ G' เป็นกรุป โดยที่ e และ e' เป็นเอกลักษณ์ของ G และ G' ตามลำดับ ให้ $\varphi : G \to G'$ เป็นฟังก์ชันสาทิสสัณฐาน และ $a \in G$ ซึ่งมีอันดับจำกัด และ $n \in \mathbb{Z}$ จะได้ว่า

1. $\varphi(e) = e'$
2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$
3. $\varphi(a^n) = (\varphi(a))^n$
4. $\circ(\varphi(a)) \mid \circ(a)$

ทฤษฎีบท 5.1.10 ให้ G และ G' เป็นกรุป โดยที่ $\varphi : G \to G'$ เป็นฟังก์ชันสาทิสสัณฐาน จะได้ว่า

1. Ker$(\varphi) \trianglelefteq G$
2. Ran$(\varphi) \leq G'$
3. ถ้า G เป็นกรุปวัฏจักร แล้ว Ran(φ) เป็นกรุปวัฏจักร

ทฤษฎีบท 5.1.11 ให้ G และ G' เป็นกรุป โดยที่ $\varphi : G \to G'$ เป็นฟังก์ชันสาทิสสัณฐาน จะได้ว่า

φ เป็นฟังก์ชัน 1-1 ก็ต่อเมื่อ $\text{Ker}(\varphi) = \{e\}$

ตัวอย่าง 5.1.12 ให้ $\varphi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ นิยามโดย $\varphi(x) = e^x$
จะแสดงว่า $\varphi(x)$ เป็นฟังก์ชันสาทิสสัณฐานแบบหนึ่งต่อหนึ่ง

แบบฝึกหัด 5.1

1. จงตรวจสอบว่า φ เป็นฟังก์ชันสาทิสสัณฐานหรือไม่

   1.1 ให้ $\varphi : (\mathbb{R}^*, \cdot) \to (\mathbb{Z}_2, +)$ นิยามโดย $\varphi(x) = \begin{cases} \bar{0} & \text{ถ้า } x > 0 \\ \bar{1} & \text{ถ้า } x < 0 \end{cases}$

   1.2 ให้ $\varphi : \mathbb{R} \to \mathbb{Z}$ นิยามโดย $\varphi(x) = [x]$ คือจำนวนเต็มมากสุดที่น้อยกว่าหรือเท่ากับ x

   1.3 ให้ $\varphi : \mathbb{Z} \to \mathbb{R}$ นิยามโดย $\varphi(x) = x$

   1.4 ให้ $\varphi : \mathbb{Z}_2 \to \mathbb{Z}_6$ นิยามโดย $\varphi(x) = x^{-1}$

   1.5 ให้ $\varphi : \mathbb{Z} \to \mathbb{Z}_{12}$ นิยามโดย $\varphi(x) = \overline{4 + x}$

   1.6 ให้ $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_6$ นิยามโดย $\varphi(x) = (x)^2$

   1.7 ให้ $\varphi : \mathbb{Z}_5^* \to \mathbb{Z}_7^*$ นิยามโดย $\varphi(x) = 5x$

   1.8 ให้ $\varphi : S_4 \to S_4$ นิยามโดย $\varphi(x) = x^{-2}$

   1.9 ให้ $\varphi : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ นิยามโดย $\varphi(x) = \cos x - i \sin x$

   1.10 ให้ $f : (\mathbb{R}, +) \to (\mathbb{R}, +)$ นิยามโดย $f(x) = \tan x$

   1.11 ให้ $P : \mathbb{R}^2 \to \mathbb{R}$ นิยามโดย $P((x, y)) = y$

2. จงหา Ker(φ) ของฟังก์ชันสาทิสสัณฐานต่อไปนี้

   2.1 $\varphi : \mathbb{Z} \to \mathbb{R}$ นิยามโดย $\varphi(a) = -a$

   2.2 $\varphi : S_5 \to S_5$ นิยามโดย $\varphi(x) = (1\,3\,2)x(1\,2\,3)$

   2.3 $\varphi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ นิยามโดย $\varphi(x) = e^x$

   2.4 $\varphi : \mathbb{Z} \to \mathbb{Z}_{12}$ นิยามโดย $\varphi(x) = \overline{4x}$

3. ให้ G เป็นกรุป และ $\varphi : G \to G$ นิยามโดย $\varphi(x) = x^2$ จงพิสูจน์ว่า

   φ เป็นฟังก์ชันสาทิสสัณฐาน ก็ต่อเมื่อ G เป็นกรุปอาบีเลียน

4. ให้ A และ B เป็นกรุป จงพิสูจน์ว่า f เป็นฟังก์ชันสาทิสสัณฐาน และหา Ker(f)

   4.1 $f : A \times B \to A$ นิยามโดย $f(a, b) = a$

   4.2 $f : A \times B \to B$ นิยามโดย $f(a, b) = b$

5. พิสูจน์ทฤษฎีบท 5.1.9 ข้อ 3

5.2 ฟังก์ชันสมสัณฐาน

บทนิยาม 5.2.1 ให้ G และ G' เป็นกรุป จะเรียกฟังก์ชัน $\varphi : G \to G'$ ว่าเป็น **ฟังก์ชันสมสัณฐาน** (isomorphism) ก็ต่อเมื่อ

φ เป็นฟังก์ชันสาทิสสัณฐานแบบหนึ่งต่อหนึ่งและทั่วถึง

ถ้า φ เป็นฟังก์ชันสมสัณฐาน จะกล่าวว่า G **สมสัณฐาน** (isomoephic) กับ G' เขียนแทน $G \cong G'$

ข้อสังเกต 5.2.2 $G \cong G'$ ก็ต่อเมื่อ มีฟังก์ชัน $\varphi : G \to G'$ เป็นฟังก์ชันสมสัณฐาน

ตัวอย่าง 5.2.3 จงตรวจสอบว่าฟังก์ชันสาทิสสัณฐาน φ เป็นฟังก์ชันสมสัณฐานหรือไม่

1. $\varphi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ นิยามโดย $\varphi(x) = 2^x$

2. $\varphi : (GL_2(\mathbb{R}), \cdot) \to (\mathbb{R}^*, \cdot)$ นิยามโดย $\varphi(A) = \det(A)$

ทฤษฎีบท 5.2.4 ให้ G และ G' เป็นกรุป และ $a \in G$ ถ้า $\varphi : G \to G'$ เป็นฟังก์ชันสมสัณฐาน แล้ว

1. φ^{-1} เป็นฟังก์ชันสมสัณฐานจาก G' ไป G
2. ถ้า $\circ(a)$ เป็นอันดับจำกัด แล้ว $\circ(a) = \circ(\varphi(a))$

ทฤษฎีบท 5.2.5 สมบัติสมมาตรของสมสัณฐาน
ให้ G_1 และ G_2 เป็นกรุป

$$\text{ถ้า} \quad G_1 \cong G_2 \quad \text{แล้ว} \quad G_2 \cong G_1$$

ทฤษฎีบท 5.2.6 สมบัติการถ่ายทอดของสมสัณฐาน
ให้ G_1, G_2 และ G_3 เป็นกรุป

$$\text{ถ้า} \quad G_1 \cong G_2 \quad \text{และ} \quad G_2 \cong G_3 \quad \text{แล้ว} \quad G_1 \cong G_3$$

ทฤษฎีบท 5.2.7 ให้ G เป็นกรุปวัฏจักร จะได้ว่า

1. ถ้า G เป็นกรุปอนันต์ แล้ว $G \cong \mathbb{Z}$
2. ถ้า G เป็นกรุปจำกัดที่มีอันดับเป็น n แล้ว $G \cong \mathbb{Z}_n$

บทแทรก 5.2.8 ให้ G เป็นกรุป ซึ่ง $|G| = p$ เมื่อ p เป็นจำนวนเฉพาะ จะได้ว่า $G \cong \mathbb{Z}_p$

บทแทรก 5.2.9 ให้ $m, n \in \mathbb{N}$ ถ้า m และ n เป็นจำนวนเฉพาะสัมพัทธ์กันแล้ว

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

ทฤษฎีบท 5.2.10 ให้ G และ G' เป็นกรุป ซึ่ง $G \cong G'$ จะได้ว่า

1. G เป็นกรุปอาบีเลียน ก็ต่อเมื่อ G' เป็นกรุปอาบีเลียน
2. G เป็นกรุปวัฏจักร ก็ต่อเมื่อ G' เป็นกรุปวัฏจักร
3. G มีกรุปย่อยอันดับ n ก็ต่อเมื่อ G' มีกรุปย่อยอันดับ n
4. G มีสมาชิกอันดับ n ก็ต่อเมื่อ G' มีสมาชิกอันดับ n
5. ทุกสมาชิกของ G เป็นอันดับจำกัด ก็ต่อเมื่อ ทุกสมาชิกของ G' เป็นอันดับจำกัด

ทฤษฎีบท 5.2.11 ให้ G_1 และ G_2 เป็นกรุป

$$\text{ถ้า} \quad G_1 \cong G_1' \quad \text{และ} \quad G_2 \cong G_2' \quad \text{แล้ว} \quad G_1 \times G_2 \cong G_1' \times G_2'$$

ต่อไปจะกล่าวถึงทฤษฎีบทที่โดงดังที่กล่าวไว้ว่า ทุก ๆ กรุป G จะสมสัณฐานกับกรุปการเรียงสับเปลี่ยนของ G เสมอ คิดค้นโดยนักคณิตศาสตร์ชาวอังกฤษผู้เลื่องชื่อนามว่า อาร์เทอร์ เคย์เลย์ (Arthur Cayley) โดยเฉพาะกรุปจำกัดที่มี $|G| = n$ จะได้สมสัณฐานกับ H สำหรับบาง $H \leq S_n$

จากหัวข้อ 2.4 และตามทฤษฎีบท 2.1.32 กรุปสมมาตร S_G จะหมายถึงเซต

$$S_G = \{ f : G \to G : f \text{ เป็นฟังก์ชัน 1-1 แบบทั่วถึง } \}$$

สมาชิกใน S_G เรียกว่าวิธีเรียงสับเปลี่ยนของ G และกรุปย่อยของ S_G เรียกว่ากรุปการเรียงสับเปลี่ยน

บทตั้ง 5.2.12 ให้ G เป็นกรุป และ $a \in G$ กำหนดให้ $T_a : G \to G$ นิยามโดย

$$T_a(x) = ax \qquad \text{ทุก ๆ } x \in G$$

แล้ว T_a เป็นวิธีเรียงสับเปลี่ยนของ G หรือ $T_a \in S_G$

ทฤษฎีบท 5.2.13 **ทฤษฎีบทเคย์เลย์** (Cayley's Theorem)
ให้ G เป็นกรุป แล้ว

$$G \text{ สมสัณฐานกับกรุปการเรียงสับเปลี่ยนของ } G$$

บทแทรก 5.2.14 ให้ G เป็นกรุปจำกัดที่มีอันดับเท่ากับ n แล้วจะได้ว่ามี $H \leq S_n$ ซึ่ง $G \cong H$

ตัวอย่าง 5.2.15 จงหากรุปการเรียงสับเปลี่ยนที่สมสัณฐานกับ $\mathbb{Z}_3$ และเป็นกรุปย่อยของ S_3

แบบฝึกหัด 5.2

1. จงตรวจสอบว่า φ เป็นฟังก์ชันสมสัณฐานหรือไม่

   1.1 $\varphi : (\mathbb{R}^*, \cdot) \to (\mathbb{R}^+, \cdot)$ นิยามโดย $\varphi(x) = |x|$

   1.2 $\varphi : \mathbb{Z} \to \mathbb{Z}$ นิยามโดย $\varphi(x) = 3x$

   1.3 $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_{12}$ นิยามโดย $\varphi(x) = 2x$

   1.4 $\varphi : \mathbb{Z} \to \mathbb{Z}_2$ นิยามโดย $\varphi(x) = \bar{x}$

   1.5 $\varphi : (\mathbb{Z}, +) \to (\mathbb{R}^+, \cdot)$ นิยามโดย $\varphi(x) = e^x$

   1.6 $\varphi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ นิยามโดย $\varphi(x) = 3^{-x}$

   1.7 $\varphi : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ นิยามโดย $\varphi(x) = \ell\mathrm{n}(x)$

   1.8 $\varphi : S_4 \to S_4$ นิยามโดย $\varphi(x) = x^2$

   1.9 $\varphi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ นิยามโดย $\varphi(A) = \det(A)$

2. จงตรวจสอบเซตคู่ใดสมสัณฐานกันบ้าง

   2.1 $\mathbb{Z}_5$ และ $\mathbb{Z}_6$
   2.2 $\mathbb{Z}_6$ และ $\mathbb{Z}_3$
   2.3 $\mathbb{Z}$ และ $\mathbb{Q}$
   2.4 $\mathbb{R}^+$ และ $\mathbb{R}$
   2.5 $\mathbb{Z}/6\mathbb{Z}$ และ $\mathbb{Z}_6$
   2.6 $\mathbb{Z}/10\mathbb{Z}$ และ $\mathbb{Z}_2 \times \mathbb{Z}_5$
   2.7 $\mathbb{Z}_2 \times \mathbb{Z}_3$ และ $\mathbb{Z}_6$
   2.8 $\mathbb{Z}_2 \times \mathbb{Z}_5$ และ $\mathbb{Z}_{11}^*$
   2.9 $\mathbb{Z}_2 \times \mathbb{Z}_4$ และ $\mathbb{Z}_8$

3. ให้ G และ G' เป็นกรุป จงแสดงว่า $G \times G' \cong G' \times G$

4. จงหากรุปการเรียงสับเปลี่ยนที่สมสัณฐานกับ

   4.1 $\mathbb{Z}_4$
   4.2 $\mathbb{Z}_5$
   4.3 $\mathbb{Z}_7^*$
   4.4 $\mathbb{Z}_2 \times \mathbb{Z}_3$
   4.5 $\mathbb{Z}_{10}^\times$
   4.6 $\mathbb{Z}/6\mathbb{Z}$
   4.7 $\mathbb{Z}$
   4.8 $\mathbb{R}$

5. ให้ a เป็นสมาชิกในกรุป G จงแสดงว่า

$$f_a : G \to G \quad \text{นิยามโดย} \quad f_a(x) = axa^{-1} \quad \text{ทุก ๆ } x \in G$$

   เป็นฟังก์ชันสมสัณฐาน

6. จงพิสูจน์ทฤษฎีบท 5.2.7

7. จงพิสูจน์ทฤษฎีบท 5.2.11

8. ให้ G_1, G_2 และ G_3 เป็นกรุป ถ้า $G_1 \cong G_2$ และ $G_2 \cong G_3$ แล้ว $G_1 \cong G_3$

9. ให้ $a, b \in \mathbb{R}^*$ กำหนด $T_{ab} : \mathbb{R} \to \mathbb{R}$ นิยามโดย $T_{ab}(x) = ax + b$ ให้

$$G = \{T_{ab} : a, b \in \mathbb{R}^*\} \qquad \text{และ} \qquad N = \{T_{1b} : b \in \mathbb{R}\}$$

   จงแสดงว่า $(G, \circ)$ เป็นกรุป และ $N \trianglelefteq G$ และ $G/N \cong \mathbb{R}^*$

5.3 ทฤษฎีบทฟังก์ชันสมสัณฐาน

ทฤษฎีบท 5.3.1 **ทฤษฎีบทฟังก์ชันสมสัณฐานบทที่หนึ่ง** (The First Isomorphism Theorem) ให้ G และ G' เป็นกรุป โดยที่ $\varphi : G \to G'$ เป็นฟังก์ชันสาทิสสัณฐาน จะได้ว่า

$$G/\mathrm{Ker}(\varphi) \cong \mathrm{Ran}(\varphi)$$

ข้อสังเกต 5.3.2 ให้ G และ G' เป็นกรุป

1. ถ้า $\varphi : G \to G'$ เป็นฟังก์ชันสาทิสสัณฐานแบบทั่วถึง แล้ว $G/\mathrm{Ker}(\varphi) \cong G'$
2. $\psi \circ \pi = \varphi$ เมื่อ π เป็นฟังก์ชันสาทิสสัณฐานธรรมชาติ

ต่อไปเป็นแผนภาพแสดงความสัมพันธ์ของ G, $\mathrm{Ran}(\varphi)$ และ $G/\mathrm{Ker}(\varphi)$ ตามทฤษฎีบทฟังก์ชันสมสัณฐานบทที่หนึ่ง

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \mathrm{Ran}(\varphi) \\
G/\mathrm{Ker}(\varphi) \arrow[ur, "\psi"'] &
\end{tikzcd}$$

ทฤษฎีบท 5.3.3 ให้ $n \in \mathbb{N}$แล้ว $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

จากทฤษฎีบท 5.3.3 เห็นได้ว่า $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ นั่นหมายความว่าเราอาจเขียนกรุป $\mathbb{Z}/n\mathbb{Z}$ ใช้แทน $\mathbb{Z}_n$ ซึ่งในหนังสือบางเล่มจะใช้ในลักษณะดังกล่าว เช่น $\mathbb{Z}/6\mathbb{Z}$ จะหมายถึง $\mathbb{Z}_6$

ตัวอย่าง 5.3.4 ให้ $\varphi : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ นิยามโดย $\varphi(x) = \text{cos}x + i\text{sin}x$ เมื่อ $x \in \mathbb{R}$ จงแสดงว่า $\mathbb{R}/\langle 2\pi \rangle \cong \{\text{cos}x + i\text{sin}x : x \in \mathbb{R}\}$

ตัวอย่าง 5.3.5 ให้ $\varphi : (\mathbb{R}^2, +) \to (\mathbb{R}, +)$ นิยามโดย $\varphi((x, y)) = x + y$ เมื่อ $x, y \in \mathbb{R}$ จงแสดงว่า $\mathbb{R}^2/\{(x, -x) : x \in \mathbb{R}\} \cong \mathbb{R}$

ทฤษฎีบท 5.3.6 ให้ G เป็นกรุป และ $K \trianglelefteq G$ แล้วจะได้ว่า

มีกรุป G' และ $f : G \to G'$ เป็นฟังก์ชันสาทิสสัณฐาน ซึ่ง $\text{Ker}(f) = K$

ทฤษฎีบท 5.3.7 **ทฤษฎีบทฟังก์ชันสมสัณฐานบทที่สอง** (The Second Isomorphism Theorem) ให้ G เป็นกรุป โดยที่ $H \leq G$ และ $K \trianglelefteq G$ จะได้ว่า

$$H/H \cap K \cong HK/K$$

โดยทฤษฎีบทฟังก์ชันสมสัณฐานบทที่สอง แสดงความสัมพันธ์ของ H, K, $H \cap K$ และ HK ได้ดังนี้

$$\begin{tikzcd}
 & HK \arrow[dl, dash, "\leq"'] \arrow[dr, dash, "\trianglelefteq"] & \\
H \arrow[dr, dash, "\trianglelefteq"'] & & K \arrow[dl, dash, "\leq"] \\
 & H \cap K &
\end{tikzcd}$$

ทฤษฎีบท 5.3.8 ทฤษฎีบทฟังก์ชันสมสัณฐานบทที่สาม (The Third Isomorphism Theorem)
ให้ G เป็นกรุป โดยที่ $H \trianglelefteq G$, $K \trianglelefteq G$ และ $K \subseteq H$ จะได้ว่า

$$H/K \trianglelefteq G/K \qquad \text{และ} \qquad (G/K)/(H/K) \cong G/H$$

แบบฝึกหัด 5.3

1. ให้ G เป็นกรุปอาบีเลียนที่มีอันดับ n ให้ $m \in \mathbb{N}$ ซึ่ง $\gcd(n,m) = 1$ จงแสดงว่า

$$\text{ทุก ๆ} \quad g \in G \quad \text{จะมี} \quad x \in G \quad \text{ซึ่ง} \quad g = x^m$$

2. จงแสดงว่า $\mathbb{Z}_{18}/\left\langle \bar{3} \right\rangle \cong \mathbb{Z}_3$

3. จงพิสูจน์ว่า ถ้า H เป็นกรุปย่อยปกติของกรุป G ซึ่ง $|G| = p$ แล้วจะได้ว่า ทุก ๆ $K \leq G$ จะสอดคล้องข้อใดข้อหนึ่งเพียงข้อเดียวจาก 2 ต่อไปนี้

   (ก) $K \leq H$ หรือ

   (ข) $G = HK$ และ $[K : K \cap H] = p$

4. ให้ M และ N เป็นกรุปย่อยปกติของกรุป G ซึ่ง $G = MN$ จงแสดงว่า

$$G/(M \cap N) \cong (G/M) \times (G/N)$$

5. ให้ C และ D เป็นกรุปย่อยปกติของกรุป A และ B ตามลำดับ จงพิสูจน์ว่า

$$(C \times D) \trianglelefteq (A \times B) \qquad \text{และ} \qquad (A \times B)/(C \times D) \cong (A/C) \times (B/D)$$

5.4 ฟังก์ชันอัตสัณฐาน

บทนิยาม 5.4.1 ให้ G เป็นกรุป ถ้า $\varphi : G \to G$ เป็นฟังก์ชันสมสัณฐาน
จะเรียก φ ว่าเป็น **ฟังก์ชันอัตสัณฐาน** (automorphism) ของ G เซตของฟังก์ชันอัตสัณฐานของ G เขียนแทนด้วย Aut(G) นั่นคือ

$$\text{Aut}(G) = \{\varphi : G \to G \ : \ \varphi \text{ เป็นฟังก์ชันสมสัณฐาน } \}$$

เห็นได้ชัดว่าฟังก์ชันเอกลักษณ์ i_G เป็นฟังก์ชัน 1-1 แบบทั่วถึง และสำหรับ $x, y \in G$ จะได้ว่า

$$i_G(xy) = xy = i_G(x)i_G(y)$$

ดังนั้น i_G เป็นฟังก์ชันอัตสัณฐานของ G

ตัวอย่าง 5.4.2 ให้ G เป็นกรุปอาบีเลียน และ

$$\varphi : G \to G \quad \text{นิยามโดย} \quad \varphi(x) = x^{-1}$$

จงแสดงว่า φ ฟังก์ชันอัตสัณฐานของ G

ทฤษฎีบท 5.4.3 ให้ G เป็นกรุปวัฏจักร โดยที่ a และ b เป็นตัวก่อกำเนิดของ G กำหนดให้

$$\varphi : G \to G \quad \text{นิยามโดย} \quad \varphi(a^k) = b^k \quad \text{เมื่อ } k \in \mathbb{Z}$$

แล้ว φ เป็นฟังก์ชันอัตสัณฐานของ G

ทฤษฎีบท 5.4.4 ให้ G เป็นกรุป แล้ว $(\mathrm{Aut}(G), \circ)$ เป็นกรุป

จะเห็นว่ากรุป $(\mathrm{Aut}, \circ)$ มี i_G เป็นเอกลักษณ์ และ φ มีตัวผกผันคือ φ^{-1}

ทฤษฎีบท 5.4.5 ให้ G เป็นกรุป และ $a \in G$ กำหนดให้

$$f_a : G \to G \quad \text{นิยามโดย} \quad f_a(x) = a^{-1}xa$$

แล้ว f_a เป็นฟังก์ชันอัตสัณฐานของ G

บทนิยาม 5.4.6 ให้ G เป็นกรุป และ $a \in G$ จะเรียก f_a ในทฤษฎีบท 5.4.5 ว่า **ฟังก์ชันอัตสัณฐานภายใน** (inner automorphism) ของ G ซึ่งสมนัยกับ a และเซตของฟังก์ชันอัตสัณฐานภายในของ G เขียนแทนด้วย $\mathrm{Inn}(G)$ นั่นคือ

$$\mathrm{Inn}(G) = \{f_a \in \mathrm{Aut}(G) \,:\, a \in G\}$$

ข้อสังเกต 5.4.7 ถ้า G เป็นกรุปอาบีเลียน จะได้ว่า f_a คือ i_G สำหรับทุก ๆ $a \in G$

ตัวอย่าง 5.4.8 จงหา $f_a(x) \in \mathrm{Inn}(S_3)$ เมื่อ $a = (1\,2)$

ทฤษฎีบท 5.4.9 ให้ G เป็นกรุป จะได้ว่า

$$G/Z(G) \cong \mathsf{Inn}(G) \qquad \text{และ} \qquad \mathsf{Inn}(G) \trianglelefteq \mathsf{Aut}(G)$$

เมื่อ $Z(G) = \{a \in G : ax = xa$ ทุก ๆ $x \in G\}$

แบบฝึกหัด 5.4

1. จงตรวจสอบว่า φ เป็นฟังก์ชันอัตสัณฐานหรือไม่

   1.1 $\varphi : \mathbb{R}^* \to \mathbb{R}^*$ นิยามโดย $\varphi(x) = |x|$

   1.2 $\varphi : S_2 \to S_2$ นิยามโดย $\varphi(x) = x^{-1}$

   1.3 $\varphi : S_n \to S_n$ นิยามโดย $\varphi(x) = x^{-1}$ เมื่อ $n \in \mathbb{N}$

   1.4 $\varphi : G \to G$ นิยามโดย $\varphi(x) = xax^{-1}$ เมื่อ a เป็นสมาชิกในกรุป G

2. จงหาฟังก์ชันอัตสัณฐานทั้งหมดของกรุปต่อไปนี้

   2.1 $\mathbb{R}$
   2.2 $\mathbb{R}^+$
   2.3 S_3
   2.4 $\mathbb{Z}_4$
   2.5 $\mathbb{Z}_6$
   2.6 $\mathbb{Z}_5^*$

3. ให้ p เป็นจำนวนเฉพาะ จงพิสูจน์ว่า

   3.1 $|\text{Aut}(\mathbb{Z}_2)| = 1$
   3.2 $\text{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$
   3.3 $\text{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$
   3.4 $\text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$

4. จงหาฟังก์ชันอัตสัณฐานภายใน $f_a(x) \in \text{Inn}(S_3)$ เมื่อกำหนดให้

   4.1 $a = (1\ 3)$
   4.2 $a = (2\ 3)$
   4.3 $a = (1\ 3\ 2)$

5. ให้ G เป็นกรุป จงพิสูจน์ว่า $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$

บทที่ 6

ริง

เมื่อใดก็ตามที่กล่าวถึงกรุปจะทราบทันทีว่ามีการดำเนินการทวิภาคเพียงหนึ่งเดียวบนกรุปนั้น ในบทนี้จะเพิ่มอีกหนึ่งการดำเนินการทวิภาคในกรุป โดยให้ $+$ แทนการดำเนินการแรก และ $\cdot$ แทนการดำเนินการที่เพิ่ม และให้การดำเนินการทั้งสองมีความสัมพันธ์กัน ดังจะศึกษาได้จากบทเรียนนี้

6.1 ริงและฟีลด์

บทนิยาม 6.1.1 ให้ R เป็นเซตที่ไม่ใช่เซตว่าง โดยที่ $+$ และ $\cdot$ เป็นการดำเนินการทวิภาคใน R จะเรียกว่า **ริง** (ring) เขียนแทนด้วย $(R, +, \cdot)$ ถ้าสอดคล้อง 3 ข้อต่อไปนี้

(ก) $(R, +)$ เป็นกรุปอาบีเลียน

(ข) $(R, \cdot)$ เป็นกึ่งกรุป

(ค) สำหรับ $a, b, c \in R$ จะได้ว่า

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{และ} \qquad (b + c) \cdot a = b \cdot a + c \cdot a$$

เรียกว่า **สมบัติการแจกแจง** (distributive law) ใน R

เขียน R แทนริง $(R, +, \cdot)$ และ $a \cdot b$ เขียนแทนด้วย ab

We write a ring R instead of $(R, +, \cdot)$ and ab instead of $a \cdot b$.
ถ้า $(R+, \cdot)$ เป็นริง แล้ว

1. เอกลักษณ์ใน $(R, +)$ เขียนแทนด้วย 0 เรียกว่า **ศูนย์** (zero element) และสำหรับ $a \in R$ เขียนตัวผกผันของ a ด้วย $-a$
2. ถ้ากึ่งกรุป $(R, \cdot)$ มีเอกลักษณ์ เขียนแทนด้วย 1 เรียกว่า **ยูนิตี** (unity) และเรียก $(R, +, \cdot)$ ว่า **ริงซึ่งมียูนิตี** (ring with unity)
3. ถ้ากึ่งกรุป $(R, \cdot)$ มีสมบัติการสลับที่ เรียก $(R, +, \cdot)$ ว่า **ริงสลับที่** (commutative ring)

ข้อสังเกต 6.1.2 ถ้าวง $(R, +, \cdot)$ มีสมาชิกเพียงตัวเดียว จะได้ว่า $R = \{0\}$ และศูนย์ทำหน้าที่เป็นยูนิตี นั่นคือ $0 = 1$ โดยเรียก $(\{0\}, +, \cdot)$ ว่า **ริงชัด** (trivial ring)

จากความรู้เรื่องกรุปถ้า $+$ เป็นการบวก และ $\cdot$ เป็นการคูณ จะได้ว่า

1. $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ และ $(\mathbb{C},+,\cdot)$ เป็นริงสลับที่ซึ่งมียูนิตีคือ 1
2. สำหรับ $n \in \mathbb{N}$ จะได้ว่า $(\mathbb{Z}_n,+,\cdot)$ เป็นริงสลับที่ซึ่งมียูนิตีคือ $\bar{1}$
3. สำหรับ $n \in \mathbb{N}$ จะได้ว่า $(M_{nn}(\mathbb{R}),+,\cdot)$ เป็นริงที่ไม่สลับที่ซึ่งมียูนิตีคือ I

ตัวอย่าง 6.1.3 กำหนดให้

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \,:\, a, b \in \mathbb{Q}\}$$

จงแสดงว่า $(\mathbb{Q}[\sqrt{2}],+,\cdot)$ เป็นริงสลับที่ซึ่งมียูนิตี

ตัวอย่าง 6.1.4 ให้ $a, b \in \mathbb{Z}$ นิยามโดย

$$\begin{aligned} a \oplus b &= a + b + 2 \\ a \odot b &= 2ab \end{aligned}$$

จงตรวจสอบว่า $(\mathbb{Z},\oplus,\odot)$ เป็นริง หรือไม่

ตัวอย่าง 6.1.5 ให้ $a, b \in \mathbb{R}$ นิยามโดย

$$a \oplus b = a + b + 1$$
$$a \odot b = a + b + ab$$

จงแสดงว่า $(\mathbb{R}, \oplus, \odot)$ เป็นริงสลับที่ซึ่งมียูนิตี

ตัวอย่าง 6.1.6 ให้ $a, b, c, d \in \mathbb{R}$ นิยามโดย

$$(a, b) \oplus (c, d) = (a + c, b + d)$$
$$(a, b) \odot (c, d) = (a \cdot c, b \cdot d)$$

จงแสดงว่า $(\mathbb{R} \times \mathbb{R}, \oplus, \odot)$ เป็นริงสลับที่ซึ่งมียูนิตี

จากตัวอย่าง 6.1.6 จะเห็นได้ว่า $\mathbb{R}$ เป็นริง แล้ว $\mathbb{R} \times \mathbb{R}$ เป็นริง ขยายแนวคิดนี้ไปยัง 2 ริงใด ๆ ถ้า R และ S เป็นริง สำหรับ $(a, b), (c, d) \in R \times S$ โดยนิยาม

$$(a, b) + (c, d) = (a + c, b + d) \tag{6.1}$$

$$(a, b) \cdot (c, d) = (a \cdot c, b \cdot d) \tag{6.2}$$

จะพิสูจน์ได้ว่า $(R \times S, +, \cdot)$ เป็นริงด้วย

ทฤษฎีบท 6.1.7 ให้ R และ S เป็นริง จะได้ว่า $R \times S$ เป็นริง เมื่อนิยาม $+$ และ $\cdot$ ดังสมการ (6.1) และ (6.2) ตามลำดับ และเรียกริง $R \times S$ ว่า **ผลคูณตรงของริง** (direct product of ring)

บทแทรก 6.1.8 ให้ R และ S เป็นริงซึ่งมียูนิตี จะได้ว่า $R \times S$ เป็นริงซึ่งมียูนิตี

บทแทรก 6.1.9 ให้ R และ S เป็นริงซึ่งมียูนิตี ถ้า R และ S มีหน่วย แล้ว $R \times S$ มีหน่วย

ทฤษฎีบท 6.1.10 ให้ R เป็นริง และ $a, b \in R$ จะได้ว่า

1. $a0 = 0a = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$

บทแทรก 6.1.11 ให้ R เป็นริงซึ่งมียูนิตี และ $a \in R$ จะได้ว่า

1. $(-1)a = -a$
2. $(-1)(-1) = 1$

บทแทรก 6.1.12 ถ้า R เป็นริงซึ่งมียูนิตี และ $R \neq \{0\}$ แล้ว $0 \neq 1$

บทนิยาม 6.1.13 ให้ $(R, +, \cdot)$ เป็นริง โดยที่ $x \in R$ และ $n \in \mathbb{N}$ กำหนดให้

1. $nx = x + (n-1)x$
2. $0x = 0$ เมื่อ 0 ทางขวามือเป็นเอกลักษณ์ใน $(R, +)$ และ 0 ทางซ้ายมือเป็นจำนวนเต็ม
3. $(-n)x = n(-x)$
4. $x^0 = 1$ เมื่อ $0 \in \mathbb{Z}$ และ 1 เป็นเอกลักษณ์ใน $(R, \cdot)$ โดยที่ x ไม่เป็นเอกลักษณ์ใน $(R, +)$
5. $x^n = xx^{n-1}$ เมื่อ x ไม่เป็นเอกลักษณ์ใน $(R, +)$

ทฤษฎีบท 6.1.14 ให้ $(R, +, \cdot)$ เป็นริง โดยที่ $x, y \in R$ และ $n, m \in \mathbb{Z}$ จะได้ว่า

1. $-(nx) = n(-x)$
2. $nx + mx = (n+m)x$
3. $n(x+y) = nx + ny$
4. $n(xy) = (nx)y = x(ny)$
5. $(nx)(my) = (nm)xy$
6. $(xy)^n = x^n y^n$ เมื่อ xy ไม่เป็นเอกลักษณ์ใน $(R, +)$

บทนิยาม 6.1.15 ให้ R เป็นริง ถ้ามี $k \in \mathbb{N}$ ซึ่ง $ka = 0$ ทุก $a \in R$ และ

$$n = \min\{k \in \mathbb{N} : ka = 0 \text{ ทุก ๆ } a \in R\}$$

เรากล่าวว่า R มี **แคแรกเทอริสติก** (characteristic) เท่ากับ n เขียนแทนด้วย $\mathrm{Char}(R)$
ถ้าไม่มี $k \in \mathbb{N}$ ซึ่ง $ka = 0$ ทุก $a \in R$ จะกล่าวว่า R มีแคแรกเทอริสติกเท่ากับ 0

ข้อสังเกต 6.1.16 จะได้ว่า $\mathrm{Char}(R) > 0$ ก็ต่อเมื่อ $\min\{k \in \mathbb{N} : ka = 0 \text{ ทุก ๆ } a \in R\} \neq \varnothing$

ตัวอย่าง 6.1.17 จงหาแคแรกเทอริสติกของ

1. $\mathbb{Z}_3$

2. $\mathbb{Z}_6$

3. $\mathbb{Z}_2 \times \mathbb{Z}_3$

สำหรับริง $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ และ $\mathbb{C}$ เห็นได้ชัดว่าไม่มี $k \in \mathbb{N}$ ซึ่ง $ka = 0$ ทุก a ที่เป็นสมาชิกของริงนั้น ดังนั้น Char($\mathbb{Z}$) $= 0$, Char($\mathbb{Q}$) $= 0$, Char($\mathbb{R}$) $= 0$ และ Char($\mathbb{C}$) $= 0$

ทฤษฎีบท 6.1.18 ให้ R เป็นริงซึ่งมียูนิตี และ Char$(R) = n$ จะได้ว่า

$$n > 0 \qquad \text{ก็ต่อเมื่อ} \qquad \{k \in \mathbb{N} : k1 = 0\} \neq \varnothing$$

บทแทรก 6.1.19 ให้ R เป็นริงซึ่งมียูนิตี และ Char$(R) > 0$ จะได้ว่า

$$\text{Char}(R) = \{k \in \mathbb{N} : k1 = 0\}$$

บทนิยาม 6.1.20 ให้ R เป็นริงซึ่งมียูนิตี และ $a \in R$ จะเรียก a ว่า **หน่วย** (unit) ถ้า

$$\text{มี } b \in R \quad \text{ซึ่ง} \quad ab = 1 = ba$$

หรือกล่าวได้ว่า a เป็นหน่วย ก็ต่อเมื่อ a มีตัวผกผันในกึ่งกรุป $(R, \cdot)$
และเซตของหน่วยของ R เขียนแทนด้วย $\mathcal{U}(R)$ นั่นคือ

$$\mathcal{U}(R) = \{a \in R : \text{ มี } b \in R \text{ ซึ่ง } ab = 1 = ba\}$$

ตัวอย่าง 6.1.21 จงหา $\mathcal{U}(R)$ ของริงต่อไปนี้

1. $\mathbb{Z}_6$
2. $\mathbb{Z}_7$

จากความรู้เรื่องกรุป สำหรับริง $(R, +, \cdot)$ เมื่อ $+$ คือการบวก และ $\cdot$ คือการคูณ จะได้ว่า

R	เซตของหน่วยของ R หรือ $\mathcal{U}(R)$	
$\mathbb{Z}_n$	$\mathbb{Z}_n^{\times}$	เมื่อ $n \in \mathbb{N}$
$\mathbb{Z}_p$	$\mathbb{Z}_p^*$	เมื่อ p เป็นจำนวนเฉพาะ
$\mathbb{Z}$	$\{-1, 1\}$	
$\mathbb{Q}$	$\mathbb{Q}^*$	
$\mathbb{R}$	$\mathbb{R}^*$	
$\mathbb{C}$	$\mathbb{C}^*$	
$M_{nn}(\mathbb{R})$	$GL_n(\mathbb{R})$	เมื่อ $n \in \mathbb{N}$

ในทำนองเดียวกันกับตัวอย่าง 6.1.3 พิสูจน์ได้ว่า $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ เป็นริง เมื่อ

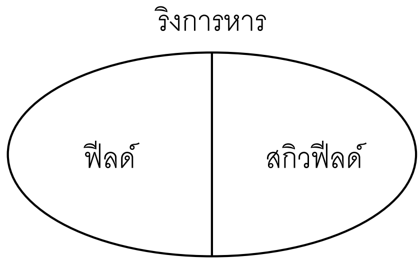
$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$$

ตัวอย่าง 6.1.22 จงหาเซตของหน่วยของริง $(\mathbb{Z}[\sqrt{2}], +, \cdot)$

บทนิยาม 6.1.23 ให้ R เป็นริงซึ่งมียูนิตี โดยที่ $1 \neq 0$ แล้วเรียก R ว่า

1. **ริงการหาร** (division ring) ถ้าทุกสมาชิกที่ไม่ใช่ศูนย์ใน R เป็นหน่วย
2. **ฟีลด์** (field) ถ้า R เป็นริงการหารสลับที่ (commutative division ring)
3. **สกิวฟีลด์** (skew field) ถ้า R เป็นริงการหารไม่สลับที่

จากนิยามข้างต้นแสดงความสัมพันธ์ของริงการหาร ฟีลด์ และสกิวฟีลด์ ได้ดังต่อไปนี้



ข้อสังเกต 6.1.24 ให้ R เป็นริงซึ่งมียูนิตี โดยที่ $1 \neq 0$ จะได้ว่า

$$R \text{ เป็นริงการหาร} \quad \text{ก็ต่อเมื่อ} \quad \mathcal{U}(R) = R - \{0\}$$

จากตารางที่ 15 เมื่อ p เป็นจำนวนเฉพาะ จะได้ว่า

$$\mathbb{Z}_p, \quad \mathbb{Q}, \quad \mathbb{R} \quad \text{และ} \quad \mathbb{C}$$

เป็นริงการหาร เนื่องจากริงดังกล่าวเป็นริงสลับที่ได้ ดังนั้นทั้ง 4 ริงเป็นฟีลด์ด้วย

จากนี้จะกล่าวถึงตัวอย่างของริงการหารที่ไม่สลับที่ที่เรียกว่าสกิวฟีลด์
ให้ $Q = \mathbb{R}^4$ โดยที่ $x = (x_1, x_2, x_3, x_4)$ และ $y = (y_1, y_2, y_3, y_4)$ นิยามการดำเนินการโดย

$$x + y = (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4) \tag{6.3}$$

$$\begin{aligned} x \cdot y = (&x_1y_1 - x_2y_2 - x_3y_3, x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3, \\ &x_1y_3 + x_3y_1 + x_4y_2 - x_2y_4, x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2) \end{aligned} \tag{6.4}$$

แล้ว $(Q, +, \cdot)$ เป็นริงไม่สลับที่ (พิสูจน์เป็นแบบฝึกหัด) ซึ่งเรียกว่า **ริงควอเทอร์เนียน** (**quaternion ring**) สำหรับ $x = (x_1, x_2, x_3, x_4)$ ที่ไม่ใช่ศูนย์ใน Q จะได้ว่า

$$x^{-1} = \left(\frac{x_1}{s}, -\frac{x_2}{s}, -\frac{x_3}{s}, -\frac{x_4}{s}\right)$$

เมื่อ $s = x_1^2 + x_2^2 + x_3^2 + x_4^2$
ดังนั้นสมาชิกทุกตัวที่ไม่ใช่ศูนย์เป็นหน่วย สรุปได้ว่า $(Q, +, \cdot)$ เป็นสกิวฟีลด์

ถ้ากำหนดให้ $\mathbf{1} = (1, 0, 0, 0)$, $\boldsymbol{i} = (0, 1, 0, 0)$, $\boldsymbol{j} = (0, 0, 1, 0)$ และ $\boldsymbol{k} = (0, 0, 0, 1)$ โดยที่

$$Q_4 = \{\mathbf{1}, -\mathbf{1}, \boldsymbol{i}, -\boldsymbol{i}, \boldsymbol{j}, -\boldsymbol{j}, \boldsymbol{k}, -\boldsymbol{k}\}$$

จะได้ว่า

$$\begin{aligned} &\boldsymbol{i}^2 = \boldsymbol{i}^2 = \boldsymbol{k}^2 = \boldsymbol{ijk} = -\mathbf{1} \\ &\boldsymbol{ij} = -\boldsymbol{ji} = \boldsymbol{k}, \quad \boldsymbol{jk} = -\boldsymbol{kj} = \boldsymbol{i}, \quad \boldsymbol{ki} = -\boldsymbol{ki} = \boldsymbol{j} \end{aligned} \tag{6.5}$$

โดยนิยาม $\cdot$ ดังสมการ (6.4) จะเห็นว่า $\mathbf{1}$ เป็นเอกลักษณ์ และ

$$\mathbf{1}, -\mathbf{1}, -\boldsymbol{i}, -\boldsymbol{j}, -\boldsymbol{k} \text{ เป็นตัวผกผันของ } \mathbf{1}, -\mathbf{1}, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k} \text{ ตามลำดับ}$$

ดังนั้น $(Q_4, \cdot)$ เป็นกรุปควอเทอร์เนียนหรือกรุปไม่สลับที่ (สอดคล้องตามเงื่อนไขของตัวอย่าง ??)

สำหรับ $x = (x_1, x_2, x_3, x_4)$ สามารถเขียนในรูป $\mathbf{1}, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ ได้เป็น

$$x = x_1\mathbf{1} + x_2\boldsymbol{i} + x_3\boldsymbol{j} + x_4\boldsymbol{k}$$

เราอาจนิยาม (6.3) และ (6.4) ได้ดังนี้

$$x + y = (x_1\mathbf{1} + x_2\boldsymbol{i} + x_3\boldsymbol{j} + x_4\boldsymbol{k}) + (x_1\mathbf{1} + x_2\boldsymbol{i} + x_3\boldsymbol{j} + x_4\boldsymbol{k}) \tag{6.6}$$

$$x \cdot y = (x_1\mathbf{1} + x_2\boldsymbol{i} + x_3\boldsymbol{j} + x_4\boldsymbol{k})(y_1\mathbf{1} + y_2\boldsymbol{i} + y_3\boldsymbol{j} + y_4\boldsymbol{k}) \tag{6.7}$$

เมื่อ $x = (x_1, x_2, x_3, x_4)$ และ $y = (y_1, y_2, y_3, y_4)$ โดยที่ $\mathbf{1}, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ สอดคล้องเงื่อไข (6.5)
สำหรับ $x = (x_1, x_2, x_3, x_4)$ ที่ไม่ใช่ศูนย์ใน Q จะได้ว่า

$$x^{-1} = \frac{x_1\mathbf{1} - x_2\boldsymbol{i} - x_3\boldsymbol{j} - x_4\boldsymbol{k}}{x_1^2 + x_2^2 + x_3^2 + x_4^2}$$

แบบฝึกหัด 6.1

1. ให้ $a, b \in \mathbb{R}$ นิยามโดย

$$a \oplus b = a + b - 1 \qquad \text{และ} \qquad a \odot b = ab - (a + b) + 2$$

จงตรวจสอบว่า $(\mathbb{R}, \oplus, \odot)$ เป็นริงสลับที่ซึ่งมียูนิตีหรือไม่

2. ให้ $a, b, c, d \in \mathbb{Q}$ นิยามโดย

$$(a, b) \oplus (c, d) = (a + c, b + d) \qquad \text{และ} \qquad (a, b) \odot (c, d) = (ac - bd, ad + bc)$$

จงตรวจสอบว่า $(\mathbb{Q} \times \mathbb{Q}, \oplus, \odot)$ เป็นริงสลับที่ซึ่งมียูนิตีหรือไม่

3. ให้ $(R, +, \cdot)$ เป็นริงที่สอดคล้องเงื่อนไข $x \cdot x = x$ ทุก ๆ $x \in R$ จงแสดงว่า

   3.1 $x + x = 0$ ทุก ๆ $x \in R$ 3.2 $x \cdot y = y \cdot x$ ทุก ๆ $x, y \in R$

4. ให้ $(R, +, \cdot)$ เป็นริงสลับที่ ให้ $a, b \in R$ จงพิสูจน์ว่า

   4.1 $a^2 - b^2 = (a - b)(a + b)$ 4.2 $(a + b)^2 = a^2 + 2ab + b^2$

5. จงหาเซตของหน่วยของริง $\mathbb{Q}[\sqrt{2}]$
6. จงแสดงว่า $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ เป็นริง
7. ให้ $(R, +, \cdot)$ เป็นริงซึ่งมียูนิตี จงพิสูจน์ว่า $(\mathcal{U}(R), \cdot)$ เป็นกรุป
8. ให้ R และ S เป็นริงซึ่งมียูนิตี จงแสดงว่า $\mathcal{U}(R \times S) = \mathcal{U}(R) \times \mathcal{U}(S)$
9. ให้ R เป็นริงการหาร และ $a \in R$ กำหนดให้ $C(a) = \{r \in R : ra = ar\}$ จงพิสูจน์ว่า $C(a)$ เป็นริงการหารทุก ๆ $a \in R$
10. จะเรียกริง R ว่า **ริงบูลีน (Boolean ring)** ถ้า $a^2 = a$ ทุก ๆ $a \in R$
    จงพิสูจน์ว่าริงบูลีนเป็นริงสลับที่
11. ให้ X เป็นเซตที่ไม่ใช่เซตว่าง กำหนดให้

$$A + B = (A \cup B) - (A \cap B) \qquad \text{และ} \qquad A \cdot B = A \cap B$$

จงแสดงว่า $(\mathcal{P}(X), +, \cdot)$ เป็นริงบูลีน

12. จงแสดงว่า Char$(\mathbb{Z}_n) = n$ เมื่อ $n \in \mathbb{N}$
13. ให้ R เป็นริงที่มีสามชิกมากกว่า 1 ตัว ถ้าทุก ๆ $a \in R - \{0\}$ มี $x \in R$ ซึ่ง $axa = x$
    จงแสดงว่า R เป็นวงการหาร
14. ถ้า R และ S เป็นฟีลด์ แล้ว $R \times S$ เป็นฟีลด์ หรือไม่เพราะเหตุใด
15. จงแสดงว่า $(Q, +, \cdot)$ เป็นสกิวฟีลด์ โดยใช้นิยาม (6.6) และ (6.7)
16. จงสร้างตารางของกรุปควอเทอร์เนียน $(Q_4, \cdot)$ โดย $Q_4 = \{\mathbf{1}, -\mathbf{1}, \boldsymbol{i}, -\boldsymbol{i}, \boldsymbol{j}, -\boldsymbol{j}, \boldsymbol{k}, -\boldsymbol{k}\}$

6.2 ริงย่อย ไอดีล และริงผลหาร

บทนิยาม 6.2.1 ให้ $(R,+,\cdot)$ เป็นริง และ $S \subseteq R$ ถ้า $(S,+,\cdot)$ เป็นริง จะเรียก S ว่า **ริงย่อย** (subring) ของ R

จากหัวข้อ 6.1 จะได้ว่า

$(\mathbb{Z},+,\cdot)$	เป็นริงย่อยของ	$(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ และ $(\mathbb{C},+,\cdot)$
$(\mathbb{Q},+,\cdot)$	เป็นริงย่อยของ	$(\mathbb{R},+,\cdot)$ และ $(\mathbb{C},+,\cdot)$
$(\mathbb{R},+,\cdot)$	เป็นริงย่อยของ	$(\mathbb{C},+,\cdot)$
$(n\mathbb{Z},+,\cdot)$	เป็นริงย่อยของ	$(\mathbb{Z},+,\cdot)$ เมื่อ $n \in \mathbb{N}$

ตัวอย่าง 6.2.2 จงหาริงย่อยทั้งหมดของ $(\mathbb{Z}_6,+,\cdot)$

วิธีทำ พิจารณากรุปย่อยทั้งหมดของ $(\mathbb{Z}_6,+)$ คือ $\langle \bar{d} \rangle$ เมื่อ $d = 0,1,2,3$

$\langle \bar{d} \rangle$	$(\langle \bar{d} \rangle, \cdot)$	ริงย่อยของ $\mathbb{Z}_6$	ยูนิตี
$\langle \bar{0} \rangle = \{\bar{0}\}$	เป็นกึ่งกรุป	ใช่	$\bar{0}$
$\langle \bar{3} \rangle = \{\bar{0},\bar{3}\}$			
$\langle \bar{2} \rangle = \{\bar{0},\bar{2},\bar{4}\}$			
$\langle \bar{1} \rangle = \mathbb{Z}_6$			

จากตัวอย่าง 6.2.2 จะสังเกตได้ว่า

1. กรุปย่อยของ $(\mathbb{Z}_6,+)$ เป็นริงย่อยของ $\mathbb{Z}_6$
2. ยูนิตีของริ่งย่อยไม่จำเป็นต้องเท่ากับยูนิตีใน $\mathbb{Z}_6$
3. $\mathbb{Z}_6$ เป็นริงซึ่งมียูนิตี แต่ริงย่อยของ $\mathbb{Z}_6$ ไม่จำเป็นต้องมียูนิตี

ทฤษฎีบท 6.2.3 เกณฑ์การพิจารณาริงย่อย (The Subring Criterion)
ให้ $(R,+,\cdot)$ เป็นริง และ $S \subseteq R$ โดยที่ $S \neq \varnothing$ ข้อความต่อไปนี้สมมูลกัน

1. $(S,+,\cdot)$ เป็นริงย่อยของ $(R,+,\cdot)$
2. $(S,+)$ เป็นกรุปย่อยของ $(R,+)$ และ $ab \in S$ ทุก ๆ $a,b \in S$
3. $a-b \in S$ และ $ab \in S$ ทุก ๆ $a,b \in S$

ตัวอย่าง 6.2.4 จงตรวจสอบว่าเซตต่อไปนี้เป็นริงย่อยของ $M_{22}(\mathbb{R})$ หรือไม่

1. $S = \left\{ \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} : x, y \in \mathbb{R} \right\}$

2. $T = \left\{ \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} : x \in \mathbb{R} \right\}$

ตัวอย่าง 6.2.5 จงตรวจสอบว่า S เป็นริงย่อยของ $\mathbb{Z} \times \mathbb{Z}$ หรือไม่

1. $S = \{(x, x) : x \in \mathbb{Z}\}$

2. $T = \{(x, 0) : x \in \mathbb{Z}\}$

3. $U = \{(x, 1) : x \in \mathbb{Z}\}$

ทฤษฎีบท 6.2.6 ให้ S_1 และ S_2 เป็นริงย่อยของ R จะได้ว่า $S_1 \cap S_2$ เป็นริงย่อยของ R

บทนิยาม 6.2.7 ให้ $(R, +, \cdot)$ เป็นริง และ $(I, +)$ เป็นกรุปย่อยของ $(R, +)$ แล้ว

1. เรียก I ว่า **ไอดีลซ้าย (left ideal)** ของ R ถ้า $RI \subseteq I$
2. เรียก I ว่า **ไอดีลขวา (right ideal)** ของ R ถ้า $IR \subseteq I$
3. เรียก I ว่า **ไอดีล (ideal)** ของ R ถ้า $RI \subseteq I$ และ $IR \subseteq I$

ข้อสังเกต 6.2.8 สำหรับริง R ใด ๆ จะได้ว่า $\{0\}$ และ R เป็นไอดีลของ R

เนื่องจาก $\mathbb{Z}_p$ เมื่อ p เป็นจำนวนเฉพาะ มีกรุปย่อยเพียง 2 กรุป ดังนั้น $\mathbb{Z}_p$ มีเพียง 2 ไอดีลเท่านั้น คือ $\{\bar{0}\}$ และ $\mathbb{Z}_p$ เช่นเดียวกับฟิลด์จะมีเพียง 2 ไอดีลดังจะพิสูจน์ในทฤษฎีบท 6.2.23

ทฤษฎีบท 6.2.9 ไอดีลซ้าย ไอดีลขวา และไอดีล ของริง R ย่อมเป็นริงย่อยของ R

ทฤษฎีบท 6.2.10 ให้ R เป็นริงซึ่งมี 1 และ I เป็นไอดีลของ R จะได้ว่า

$$\text{ถ้า} \quad 1 \in I \quad \text{แล้ว} \quad I = R$$

ตัวอย่าง 6.2.11 จงหาไอดีลของ $\mathbb{Z}_6$

ในทำนองเดียวกับตัวอย่าง 6.2.11 ทุก ๆ กรุปย่อยของ $(\mathbb{Z}_n, +)$ เป็นไอดีลของ $\mathbb{Z}_n$ เมื่อ $n \in \mathbb{N}$

ตัวอย่าง 6.2.12 จงแสดงว่า $n\mathbb{Z}$ เป็นไอดีลของ $\mathbb{Z}$ เมื่อ $n \in \mathbb{N}$

ข้อสังเกต 6.2.13 ให้ R เป็นริงสลับที่ จะได้ว่า

1. ถ้า I เป็นไอดีลซ้ายของ R แล้ว I เป็นไอดีลขวา และไอดีลของ R
2. ถ้า I เป็นไอดีลขวาของ R แล้ว I เป็นไอดีลซ้าย และไอดีลของ R

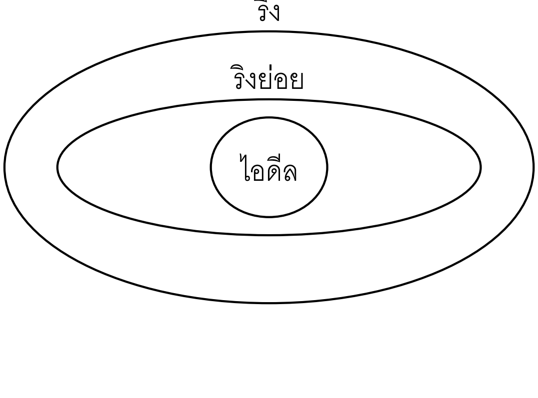
ตัวอย่าง 6.2.14 จงแสดงว่า $I = \{(x, 0) : x \in \mathbb{Z}\}$ เป็นไอดีลของ $\mathbb{Z} \times \mathbb{Z}$

ตัวอย่าง 6.2.15 จงตรวจสอบว่ากรุปย่อยของ $M_{22}(\mathbb{R})$ ต่อไปนี้ว่าเป็นไอดีลซ้าย ไอดีลขวา ไอดีล หรือเป็นอย่างอื่น

1. $I = \left\{ \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} : x, y \in \mathbb{R} \right\}$

2. $J = \left\{ \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} : x \in \mathbb{R} \right\}$

โดยทฤษฎีบท 6.2.9 ทุก ๆ ไอดีลเป็นริงย่อย แต่ในทางกลับกันตัวอย่าง 6.2.15 ข้อ 2 แสดงให้เห็นว่า J เป็นริงย่อยของ $M_{22}(\mathbb{R})$ แต่ไม่เป็นไอดีลของ $M_{22}(\mathbb{R})$ เพื่อให้เข้าใจยิ่งขึ้นจะแสดงให้เห็นความสัมพันธ์ของ ริง ริงย่อย และไอดีล ดังรูปต่อไปนี้



ทฤษฎีบท 6.2.16 ให้ I และ J เป็นไอดีลซ้าย (ไอดีลขวา, ไอดีล) ของ R แล้ว

$I \cap J$ เป็นไอดีลซ้าย (ไอดีลขวา, ไอดีล) ของ R

ทฤษฎีบท 6.2.17 ให้ R เป็นริง และ $a \in R$ จะได้ว่า

Ra เป็นไอดีลซ้าย และ aR เป็นไอดีลขวาของ R

ทฤษฎีบท 6.2.18 ให้ R เป็นริงสลับที่และมียูนิตี และ $a \in R$ จะได้ว่า

Ra เป็นไอดีลที่มี a เป็นสมาชิก

บทนิยาม 6.2.19 ให้ R เป็นริงสลับที่และมียูนิตี และ $a \in R$ จะเรียก

$$Ra = \{ra : r \in R\}$$

ว่า **ไอดีลมุขสำคัญ** (principal ideal) เขียนแทนด้วย $\langle a \rangle$

ตัวอย่าง 6.2.20 จงแจกแจงสมาชิกของไอดีลมุขสำคัญใน $\mathbb{Z}_6$

1. $\langle \bar{1} \rangle$

2. $\langle \bar{2} \rangle$

3. $\langle \bar{3} \rangle$

ในทำนองเดียวกันสำหรับริง $\mathbb{Z}$ เมื่อ $n \in \mathbb{Z}$ เห็นได้ชัดว่า

$$\langle n \rangle = n\mathbb{Z}$$

ทฤษฎีบท 6.2.21 ให้ I และ J เป็นไอดีลซ้าย (ไอดีลขวา, ไอดีล) ของ R และ S ตามลำดับ แล้ว

$I \times J$ เป็นไอดีลซ้าย (ไอดีลขวา, ไอดีล) ของ $R \times S$

ในทางกลับกับของทฤษฎีบท 6.2.21 เมื่อ R และ S เป็นริง เราแสดงได้ว่าไอดีลของ $R \times S$ อยู่ในรูป $I \times S$ เมื่อ I และ J เป็นไอดีลของ R และ S ตามลำดับ

ตัวอย่าง 6.2.22 จงหาไอดีลทั้งหมดของ $\mathbb{Z}_2 \times \mathbb{Z}_6$

ทฤษฎีบท 6.2.23 ให้ R เป็นริงสลับที่ซึ่งมียูนิตี และ $R \neq \{0\}$ จะได้ว่า

R เป็นฟีลด์ ก็ต่อเมื่อ R มีเพียง 2 ไอดีลเท่านั้นคือ R และ $\{0\}$

ทฤษฎีบท 6.2.24 ให้ I เป็นไอดีลของริง R และ $R/I = \{I + a \,:\, a \in R\}$ กำหนดให้

$$(I + a) + (I + b) = I + (a + b)$$
$$(I + a) \cdot (I + b) = I + (ab)$$

แล้ว $(R/I, +, \cdot)$ เป็นริง และเรียกว่า **ริงผลหาร** (quotient ring)

ข้อสังเกต 6.2.25 ถ้า R เป็นริงสลับที่ซึ่งมียูนิตี และ I เป็นไอดีลของ R จะได้ว่า R/I เป็นริงสลับที่ซึ่งมียูนิตี โดยที่

I เป็นศูนย์ และ $I + 1$ เป็นยูนิตี ในริงผลหาร R/I

ตัวอย่างเช่นใน $\mathbb{Z}_6$ พิจารณา $\langle\bar{3}\rangle$ ซึ่งเป็นไอดีลมุขสำคัญ จะได้ว่า

$$\mathbb{Z}_6/\langle\bar{3}\rangle = \{\langle\bar{3}\rangle, \langle\bar{3}\rangle + \bar{1}, \langle\bar{3}\rangle + \bar{2}\}$$

แสดงตารางการดำเนินการได้ดังนี้

$+$	$\langle\bar{3}\rangle$	$\langle\bar{3}\rangle + \bar{1}$	$\langle\bar{3}\rangle + \bar{2}$
$\langle\bar{3}\rangle$			
$\langle\bar{3}\rangle + \bar{1}$			
$\langle\bar{3}\rangle + \bar{2}$			

$\cdot$	$\langle\bar{3}\rangle$	$\langle\bar{3}\rangle + \bar{1}$	$\langle\bar{3}\rangle + \bar{2}$
$\langle\bar{3}\rangle$			
$\langle\bar{3}\rangle + \bar{1}$			
$\langle\bar{3}\rangle + \bar{2}$			

ทฤษฎีบท 6.2.26 ให้ I, J เป็นไอดีลของริง R โดยที่ I เป็นเซตย่อยของ J จะได้ว่า

$$J/I = \{I\} \quad \text{ก็ต่อเมื่อ} \quad J = I$$

ทฤษฎีบท 6.2.27 ให้ I, J, K เป็นไอดีลของริง R โดยที่ I เป็นเซตย่อยของ J และ K จะได้ว่า

$$K/I = J/I \quad \text{ก็ต่อเมื่อ} \quad K = J$$

แบบฝึกหัด 6.2

1. จงตรวจสอบว่ากรุปย่อยของ $M_{22}(\mathbb{R})$ ต่อไปนี้ว่าเป็นไอดีลซ้าย ไอดีลขวา ไอดีล หรือเป็นอย่างอื่น

    1.1 $A = \left\{ \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} : x, y \in \mathbb{R} \right\}$

    1.2 $B = \left\{ \begin{bmatrix} x & y \\ z & 0 \end{bmatrix} : x, y, z \in \mathbb{R} \right\}$

    1.3 $C = \left\{ \begin{bmatrix} x & 0 \\ 0 & y \end{bmatrix} : x, y \in \mathbb{R} \right\}$

    1.4 $D = \left\{ \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} : x, y \in \mathbb{R} \right\}$

    1.5 $E = \left\{ \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} : x \in \mathbb{R} \right\}$

    1.6 $F = \left\{ \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} : x \in \mathbb{R} \right\}$

2. จงตรวจสอบว่าเซตต่อไปนี้เป็น ริงย่อย หรือ ไอดีลของ $\mathbb{Z} \times \mathbb{Z}$ หรือไม่

    2.1 $I = \{(a, a) \,:\, a \in \mathbb{Z}\}$

    2.2 $J = \{(2a, 2b) \,:\, a, b \in \mathbb{Z}\}$

    2.3 $K = \{(2a, 0) \,:\, a \in \mathbb{Z}\}$

    2.4 $L = \{(0, -a) \,:\, a \in \mathbb{Z}\}$

3. จงหาริงย่อยทั้งหมดและยูนิตี (ถ้ามี) ของริงต่อไปนี้

    3.1 $\mathbb{Z}_8$ 3.2 $\mathbb{Z}_{12}$ 3.3 $\mathbb{Z}_{15}$ 3.4 $\mathbb{Z}_{36}$

4. ถ้า p เป็นจำนวนเฉพาะจงให้เหตุผลว่าทำไม $\mathbb{Z}_p$ มีไอดีลเพียง 2 เซตเท่านั้นคือ $\{\bar{0}\}$ และ $\mathbb{Z}_p$

5. ให้ $R = \{f : \mathbb{R} \to \mathbb{R} \,:\, f$ เป็นฟังก์ชันต่อเนื่อง $\}$ กำหนดโดย

$$(f + g)(x) = f(x) + g(x) \qquad \text{และ} \qquad (f \cdot g)(x) = f(x) \cdot g(x)$$

    5.1 จงพิสูจน์ว่า $(R, +, \cdot)$ เป็นริง

    5.2 $I = \{f \in R \,:\, f(1) = 0\}$เป็นไอดีลของ R

6. ให้ R เป็นริงและ I_i เป็นไอดีลของ R ทุก ๆ $i \in \mathbb{N}$ โดยที่

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$$

    จงแสดงว่า $\bigcup_{i \in \mathbb{N}} I_i$ เป็นไอดีลของ R

7. จงยกตัวอย่างไอดีล I และ J ของริง R ซึ่ง $I \cup J$ ไม่เป็นไอดีลของริง R

8. จงหาหน่วยทั้งหมดของ $\mathbb{Z}_6/\left\langle \bar{2} \right\rangle$

9. กำหนดให้ R และ S เป็นริง จงแสดงว่าไอดีลของ $R \times S$ อยู่ในรูป $I \times J$ เมื่อ I และ J เป็นไอดีลของ R และ S ตามลำดับ

10. จงพิสูจน์ว่าไอดีลมุขสำคัญ $\langle \bar{a} \rangle$ ในริง R มีสมาชิกเหมือนกับกรุปย่อย $\langle \bar{a} \rangle$ ใน $(R, +)$

6.3 ฟังก์ชันสาทิสสัณฐานของริง

บทนิยาม 6.3.1 ให้ $(R, +, \cdot)$ และ $(S, \oplus, \odot)$ เป็นริง และ $\varphi : R \to S$

1. เรียก φ ว่า **ฟังก์ชันสาทิสสัณฐานของริง** (ring homomorphism) ถ้าทุก ๆ $a, b \in R$ สอดคล้อง 2 เงื่อนไขต่อไปนี้

$$\varphi(a + b) = \varphi(a) \oplus \varphi(b)$$
$$\varphi(a \cdot b) = \varphi(a) \odot \varphi(b)$$

2. เรียก φ ว่า **ฟังก์ชันสมสัณฐานของริง** (ring isomorphism) ถ้า φ เป็นฟังก์ชันสาทิสสัณฐานของริงซึ่งเป็นฟังก์ชัน 1-1 แบบทั่วถึง และกล่าวว่า R **สมสัณฐาน** (isomorphic) กับ S เขียนแทนด้วย $R \cong S$

3. **เคอร์เนล** (Kernel) ของ φ เขียนแทนด้วย นิยามโดย

$$\text{Ker}(\varphi) = \{x \in R : \varphi(x) = 0_S\}$$

เมื่อ 0_S เป็นศูนย์ใน S

สำหรับ $(R, +, \cdot)$ และ $(S, \oplus, \odot)$ เป็นริง ถ้า $\varphi : R \to S$ เป็นฟังก์ชันสาทิสสัณฐานของริง จะได้ว่า $\varphi : (R, +) \to (S, \oplus)$ เป็นฟังก์ชันสาทิสสัณฐาน เพราะว่า $(R, +)$ และ $(S, \oplus)$ เป็นกรุปอาบีเลียน จากสมบัติของฟังก์ชันสาทิสสัณฐาน ทำให้ได้ว่า

1. $\varphi(0_R) = 0_S$ เมื่อ 0_R และ 0_S เป็นศูนย์ใน R และ S ตามลำดับ
2. $\varphi(-x) = -\varphi(x)$ ทุก ๆ $x \in R$

ตัวอย่าง 6.3.2 จงแสดงว่า φ เป็นฟังก์ชันสาทิสสัณฐานของริง และหา $\text{Ker}(\varphi)$

1. กำหนดให้ $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ นิยามโดย $\varphi(x) = \bar{x}$ เมื่อ $n \in \mathbb{N}$

2. กำหนดให้ $\varphi : \mathbb{C} \to \mathbb{C}$ นิยามโดย $\varphi(x + yi) = x - yi$ เมื่อ $x, y \in \mathbb{R}$

ตัวอย่าง 6.3.3 จงตรวจสอบว่า φ เป็นฟังก์ชันสาทิสสัณฐานของริงหรือไม่

1. กำหนดให้ $\varphi : \mathbb{Z} \to \mathbb{Z}_2$ นิยามโดย $\varphi(x) = (\bar{x})^2$

2. กำหนดให้ $\varphi : \mathbb{Z} \to \mathbb{Z}_3$ นิยามโดย $\varphi(x) = (\bar{x})^2$

ทฤษฎีบท 6.3.4 ให้ R และ S เป็นริง และ φ เป็นฟังก์ชันสมสัณฐานของริงจาก R ไป S จะได้ว่า

$$\varphi \text{ เป็นฟังก์ชัน 1-1 } \quad \text{ก็ต่อเมื่อ} \quad \text{Ker}(\varphi) = \{0_R\}$$

ตัวอย่าง 6.3.5 ให้ $\varphi : \mathbb{R} \to M_{22}(\mathbb{R})$ นิยามโดย

$$\varphi(a) = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$$

จงแสดงว่า φ เป็นฟังก์ชันสาทิสสัณฐานของริงแบบ 1-1

จากตัวอย่าง 6.3.5 จะเห็นว่า $\varphi(1) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ฉะนั้น $\varphi(1_R) = 1_S$ ไม่เป็นจริง เมื่อ 1_R และ 1_S เป็นยูนิตีใน R และ S ตามลำดับ เมื่อกำหนดให้

$$T = \text{Ran}(\varphi) = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in \mathbb{R} \right\}$$

จะได้ว่า T เป็นริงย่อยของ $\mathbb{M}_{22}(\mathbb{R})$ และ $\varphi : \mathbb{R} \to T$ เป็นฟังก์ชันสมสัณฐานของริง นั่นคือ $\mathbb{R} \cong T$

ข้อสังเกต 6.3.6 ให้ R และ S เป็นริง และ φ เป็นฟังก์ชันสาทิสสัณฐานของริงจาก R ไป S
ถ้า φ เป็นฟังก์ชัน 1-1 แล้ว $R \cong \text{Ran}(\varphi)$

ตัวอย่าง 6.3.7 ให้ $S = \{(x, x) : x \in \mathbb{Z}\}$ เป็นริงย่อยของ $\mathbb{Z}$ จงแสดงว่า $S \cong \mathbb{Z}$

ทฤษฎีบท 6.3.8 ให้ R และ S เป็นริง และ φ เป็นฟังก์ชันสาทิสสัณฐานของริงจาก R ไป S จะได้ว่า

1. Ker(φ) เป็นริงย่อยของ R
2. Ran(φ) เป็นริงย่อยของ S
3. Ker(φ) เป็นไอดีลของ R
4. ถ้า R มียูนิตีคือ 1_R แล้ว $\varphi(1_R)$ เป็นยูนิตีใน Ran(φ)

ทฤษฎีบท 6.3.9 ให้ I เป็นไอดีลของริง R กำหนดให้

$$\pi : R \to R/I \quad \text{นิยามโดย} \quad \pi(a) = I + a$$

แล้ว π เป็นภาวะสาทิสัณฐานของริงแบบทั่วถึง
ซึ่งจะเรียกว่า **ฟังก์ชันสาทิสสัณฐานของริงธรรมชาติ** (natural ring homomorphism)

ทฤษฎีบท 6.3.10 **ทฤษฎีบทฟังก์ชันสมสัณฐานของริงบทที่หนึ่ง**
ให้ R และ S เป็นริง โดยที่ $\varphi : R \to S$ เป็นฟังก์ชันสาทิสสัณฐานของริง จะได้ว่า

$$R/\mathrm{Ker}(\varphi) \cong \mathrm{Ran}(\varphi)$$

ข้อสังเกต 6.3.11 ให้ R และ S เป็นริง

1. ถ้า $\varphi : R \to S$ เป็นฟังก์ชันสาทิสสัณฐานของริงแบบทั่วถึง แล้ว $R/\mathrm{Ker}(\varphi) \cong S$
2. $\psi \circ \pi = \varphi$ เมื่อ π เป็นฟังก์ชันสาทิสสัณฐานของริงธรรมชาติ

ต่อไปเป็นแผนภาพแสดงความสัมพันธ์ของ R, $\mathrm{Ran}(\varphi)$ และ $R/\mathrm{Ker}(\varphi)$ ตามทฤษฎีบทฟังก์ชันสมสัณฐานของริงบทที่หนึ่ง

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \mathrm{Ran}(\varphi) \\
R/\mathrm{Ker}(\varphi) \arrow[ur, "\psi"'] &
\end{tikzcd}$$

ตัวอย่าง 6.3.12 จงแสดงว่า $\mathbb{Z}/\langle n\rangle \cong \mathbb{Z}_n$

ทฤษฎีบท 6.3.13 **ทฤษฎีบทฟังก์ชันสมสัณฐานของริงบทที่สอง**
ให้ A เป็นริงย่อยของ R และ B เป็นไอดีลของ R แล้ว $A+B=\{a+b : a\in A \text{ และ } b\in B\}$ เป็นริงย่อยของ R และ $A\cap B$ เป็นไอดีลของ A และ

$$(A+B)/B \cong A/(A\cap B)$$

ทฤษฎีบท 6.3.14 ทฤษฎีบทฟังก์ชันสมสัณฐานของริงบทที่สาม
ให้ I และ J เป็นไอดีลของ R โดยที่ $I \subseteq J$ แล้ว J/I เป็นไอดีลของ R/I และ

$$(R/I)/(J/I) \cong R/J$$

แบบฝึกหัด 6.3

1. จงตรวจสอบว่า φ เป็นฟังก์ชันสาทิสสัณฐานของริงหรือไม่

   1.1 กำหนดให้ $\varphi : \mathbb{Z} \to \mathbb{Z}_3$ นิยามโดย $\varphi(x) = (\bar{x})^3$

   1.2 กำหนดให้ $\varphi : \mathbb{Z} \to \mathbb{Z}_{12}$ นิยามโดย $\varphi(x) = \overline{4x}$

   1.3 กำหนดให้ $\varphi : \mathbb{C} \to \mathbb{R}$ นิยามโดย $\varphi(x+yi) = x^2 + y^2$ เมื่อ $x, y \in \mathbb{R}$

2. ให้ R เป็นริงสลับที่ และ $I = \{x \in R : \text{ มี } n \in \mathbb{N} \text{ ซึ่ง } x^n = 0\}$ จงพิสูจน์ว่า

   2.1 I เป็นไอดีลของ R

   2.2 ใน R/I จะได้ว่ามี $m \in I$ ซึ่ง $x^{-m} = 0 \to x = 0$

3. จงแสดงว่าริง $2\mathbb{Z}$ และ $3\mathbb{Z}$ ไม่สมสัณฐานกัน

4. จงหาฟังก์ชันสมสัณฐานจาก $\mathbb{Z}$ ไป $\mathbb{Z}/30\mathbb{Z}$ พร้อมทั้งหาเคอร์เนล และเรนจ์

5. จงหาฟังก์ชันสมสัณฐานจาก $\mathbb{Z} \times \mathbb{Z}$ ไป $\mathbb{Z}$ พร้อมทั้งหาเคอร์เนล และเรนจ์

6. จงตรวจสอบว่าฟังก์ชันต่อไปนี้ว่าเป็นฟังก์ชันสาทิสสัณฐานของริงจาก $M_{22}(\mathbb{Z})$ ไป $\mathbb{Z}$ หรือไม่

   6.1 $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto a$ 6.2 $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto a+d$ 6.3 $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto ad-bc$

7. ให้ $R = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, b, d \in \mathbb{Z} \right\}$ เป็นริงย่อยของ $M_{22}(\mathbb{Z})$ จงพิสูจน์ว่า

   $$\varphi : R \to \mathbb{Z} \times \mathbb{Z} \text{ นิยามโดย } \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mapsto (a, d)$$

   เป็นเป็นฟังก์ชันสาทิสสัณฐานของริงแบบทั่วถึง และหาเคอร์เนลของ φ

8. จงแสดงว่า $S = \{(x, 0) : x \in \mathbb{Z}\}$ เป็นริงย่อยของ $\mathbb{Z}$ และ $S \cong \mathbb{Z}$

9. จงแสดงว่า $\mathcal{M} \cong \mathbb{C}$ เมื่อ $\mathcal{M} = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$ และนิยาม $\varphi : \mathbb{C} \to \mathcal{M}$ โดย

   $$\varphi(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

10. ให้ R และ S เป็นริง และ φ เป็นฟังก์ชันสาทิสสัณฐานของริงจาก R ไป S จงแสดงว่า Ran(φ) เป็นริงย่อยของ S แต่ไม่เป็นไอดีลของ S

11. จงพิสูจน์ทฤษฎีบทฟังก์ชันสมสัณฐานของริงบทที่สาม

12. ให้ R เป็นริงซึ่งมียูนิตี และ S เป็นริง กำหนดให้ $\varphi : R \to S$ เป็นฟังก์ชันสาทิสสัณฐาน และ u เป็นหน่วยของ R จงแสดงว่า

    $$\varphi(u) \text{ เป็นหน่วยของ } S \text{ ก็ต่อเมื่อ } u \notin \text{Ker}(\varphi)$$

บทที่ 7

อินทิกรัลโดเมน

จำนวนเต็มเต็มที่เรารู้จักกันมานานนั้นมีสมบัติมากมายที่น่าสนใจซึ่งจะเห็นว่า $(\mathbb{Z}, +, \cdot)$ เป็นริงชนิดหนึ่ง ดังนั้นในบทนี้เราจะขยายแนวคิดนี้ให้ทั่วไปมากยิ่งขึ้นเพื่อใช้ตรวจสอบว่าริงต่าง ๆ มีสมบัติดังกล่าวหรือไม่ โดยความสนในเรื่องนี้ เกิดขึ้นพร้อม ๆ กับการพัฒนาวิชาพีชคณิตนามธรรมในช่วงเริ่มต้น

7.1 ตัวหารศูนย์และอินทิกรัลโดเมน

บทนิยาม 7.1.1 ให้ R เป็นริงสลับที่ และ a เป็นสมาชิกที่ไม่ใช่ศูนย์ใน R แล้ว

เรียก a ว่า **ตัวหารศูนย์** (zero divisor) ถ้ามี b ซึ่งเป็น สมาชิกที่ไม่ใช่ศูนย์ใน R ที่ทำให้ $ab = 0$

ข้อสังเกต 7.1.2 ถ้า R ริงสลับที่ซึ่งไม่มีตัวหารศูนย์ แล้วทุก ๆ ริงย่อยของ R ไม่มีตัวหารศูนย์

สำหรับ $a, b \in \mathbb{C}$ โดยสมบัติของจำนวนเชิงซ้อนจะได้ว่า

$$a \neq 0 \quad \text{และ} \quad b \neq 0 \quad \text{ก็ต่อเมื่อ} \quad ab \neq 0$$

สรุปได้ว่า $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ และ $\mathbb{C}$ ไม่มีตัวหารศูนย์

ตัวอย่าง 7.1.3 จงหาตัวหารศูนย์ทั้งหมดของ $\mathbb{Z}_6$

ทฤษฎีบท 7.1.4 ให้ $a \in \{1, 2, 3, ..., n-1\}$ เมื่อ $n \in \mathbb{N}$ จะได้ว่า

$\bar{a}$ เป็นตัวหารศูนย์ใน $\mathbb{Z}_n$ ก็ต่อเมื่อ $\gcd(a, n) \neq 1$

ตัวอย่าง 7.1.5 จงหาตัวหารศูนย์ทั้งหมดของริงต่อไปนี้

1. $\mathbb{Z}_{12}$

2. $\mathbb{Z}_{18}$

3. $\mathbb{Z}_{20}$

บทแทรก 7.1.6 จำนวนตัวหารศูนย์ของ $\mathbb{Z}_n$ เท่ากับ $(n-1)-\phi(n)$ เมื่อ $n \in \mathbb{N}$

ตัวอย่าง 7.1.7 จงหาจำนวนตัวหารศูนย์ทั้งหมดของริงต่อไปนี้

1. $\mathbb{Z}_{15}$
2. $\mathbb{Z}_{23}$
3. $\mathbb{Z}_{36}$
4. $\mathbb{Z}_{100}$

บทแทรก 7.1.8 ถ้า p เป็นจำนวนเฉพาะ แล้ว $\mathbb{Z}_p$ ไม่มีตัวหารศูนย์

ทฤษฎีบท 7.1.9 ให้ R และ R เป็นริงสลับที่ จะได้ว่า

ถ้า a หรือ b เป็นตัวหารศูนย์ของ R และ S ตามลำดับ แล้ว (a, b) เป็นตัวหารศูนย์ของ $R \times S$

ให้ R และ S เป็นริงสลับที่ จะเห็นได้ชัดว่า $x \in R - \{0\}$ และ $y \in S - \{0\}$ จะได้ว่า

$$(x, 0_S) \text{ และ } (0_R, y) \text{ เป็นตัวหารศูนย์ของ } R \times S$$

ตัวอย่างเช่นตัวหารศูนย์ของ $\mathbb{Z}_2 \times \mathbb{Z}_3$ คือ $(\bar{0}, \bar{1})$, $(\bar{0}, \bar{2})$ และ $(\bar{1}, \bar{0})$

ทฤษฎีบท 7.1.10 ให้ R และ R เป็นริงสลับที่ ให้ $a \in R - \{0\}$ และ $b \in S - \{0\}$ จะได้ว่า

ถ้า (a, b) เป็นตัวหารศูนย์ของ $R \times S$ แล้ว a หรือ b เป็นตัวหารศูนย์ของ R และ S ตามลำดับ

ตัวอย่าง 7.1.11 จงหาตัวหารศูนย์ของ $\mathbb{Z}_3 \times \mathbb{Z}_4$

ตัวอย่าง 7.1.12 จงหาจำนวนตัวหารศูนย์ของ $\mathbb{Z}_5 \times \mathbb{Z}_6$

บทนิยาม 7.1.13 จะเรียกริงสลับที่ซึ่งไม่มีตัวหารศูนย์ว่า **อินทิกรัลโดเมน** (integral domain)

จากบทนิยามข้างต้น ให้ R เป็นริงสลับที่จะได้ว่า

$$R \text{ เป็นอินทิกรัลโดเมน ก็ต่อเมื่อ } ab \neq 0 \text{ ทุก ๆ } a, b \in R - \{0\}$$

หรือกล่าวอีกนัยได้ว่า R เป็นอินทิกรัลโดเมน ก็ต่อเมื่อ ทุก ๆ $a, b \in R$

$$\text{ถ้า } ab = 0 \text{ แล้ว } a = 0 \text{ หรือ } b = 0$$

หรือกล่าวได้ว่า R เป็นอินทิกรัลโดเมน ก็ต่อเมื่อ ทุก ๆ $a, b \in R$

$$\text{ถ้า } a \neq 0 \text{ และ } b \neq 0 \text{ แล้ว } ab \neq 0$$

เนื่องจาก $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ และ $\mathbb{C}$ ไม่มีตัวหารศูนย์ ดังนั้นริงดังกล่าวเป็นอินทิกรัลโดเมน

ตัวอย่าง 7.1.14 จงตรวจสอบว่าริงต่อไปนี้เป็นอินทิกรัลโดเมนหรือไม่

1. $\mathbb{Z}_5$
2. $\mathbb{Z}_6$
3. $\mathbb{Z}_7$
4. $\mathbb{Z}_8$

ทฤษฎีบท 7.1.15 $\mathbb{Z}_n$ เป็นอินทิกรัลโดเมน ก็ต่อเมื่อ n เป็นจำนวนเฉพาะ

ทฤษฎีบท 7.1.16 ให้ R เป็นริงสลับที่ จะได้ว่า

R เป็นอินทิกรัลโดเมน ก็ต่อเมื่อ R สอดคล้องเงื่อนไขการตัดออกสำหรับ $\cdot$

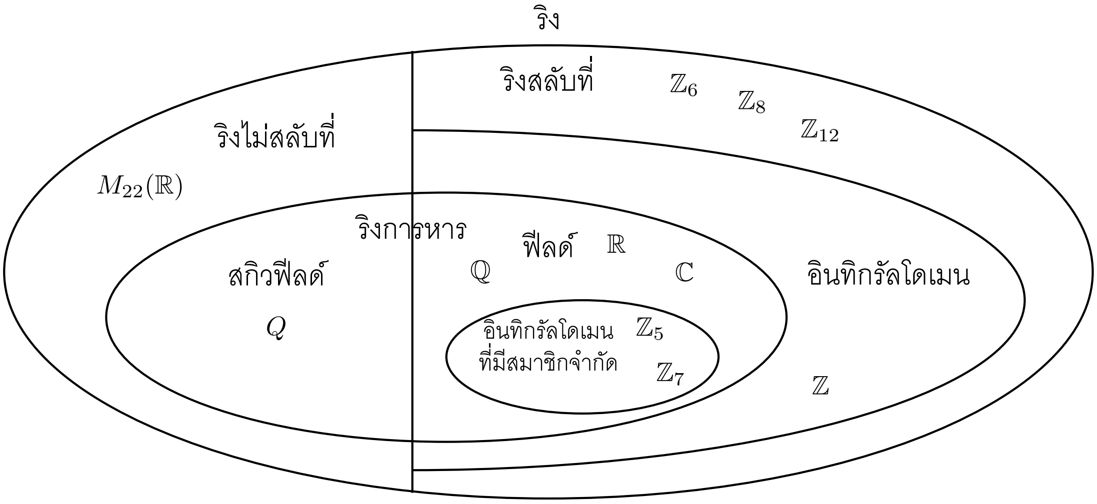
ทฤษฎีบท 7.1.17 ฟีลด์เป็นอินทิกรัลโดเมน

บทกลับของทฤษฎีบท 7.1.17 ไม่เป็นจริง ตัวอย่างคือ $\mathbb{Z}$ เป็นอินทิกรัลโดเมนแต่ไม่เป็นฟิลด์ เพราะหน่วยใน $\mathbb{Z}$ มีแค่ 2 ตัวเท่านั้นคือ 1 และ -1 บทกลับจะเป็นจริงต้องเพิ่มเงื่อนไขว่าอินทิกรัลโดเมนต้องเป็นเซตจำกัด จะกล่าวในทฤษฎีบทต่อไปนี้

ทฤษฎีบท 7.1.18 อินทิกรัลโดเมนที่มีสมาชิกจำกัดเป็นฟิลด์

บทแทรก 7.1.19 $\mathbb{Z}_n$ เป็นฟิลด์ ก็ต่อเมื่อ n เป็นจำนวนเฉพาะ

จากการนิยามและทฤษฎีบทต่างที่ได้สามารถแสดงความสัมพันธ์ส่วนต่าง ๆ ของริงพร้อมตัวอย่างประกอบได้ดังนี้



บทแทรก 7.1.20 ทฤษฎีบทของแฟร์มาต์ (Fermat's Theorem)
ให้ $a \in \mathbb{Z}$ และ p เป็นจำนวนเฉพาะ โดยที่ $p \nmid a$ จะได้ว่า

$$p \mid (a^{p-1} - 1)$$

ตัวอย่างที่ได้จากทฤษฎีบทของแฟร์มาต์

1. เนื่องจาก $5 \nmid 1011$ จะได้ว่า $5 \mid (1011^4 - 1)$
2. เนื่องจาก $7 \nmid 30$ จะได้ว่า $7 \mid (30^6 - 1)$
3. เนื่องจาก $11 \nmid 131$ จะได้ว่า $11 \mid (131^{10} - 1)$

ทฤษฎีบท 7.1.21 ให้ R เป็นอินทิกรัลโดเมนซึ่งมียูนิตี และ $a \in R - \{0\}$ โดยที่ $\circ(a)$ คืออันดับใน $(R, +)$ จะได้ว่า

1. $\circ(a) = \text{Char}(R)$ ถ้า $\text{Char}(R) > 0$
2. $\circ(a) = \infty$ ถ้า $\text{Char}(R) = 0$

ทฤษฎีบท 7.1.22 ให้ R เป็นอินทิกรัลโดเมนซึ่งมียูนิตี แล้ว

$$\text{Char}(R) > 0 \quad \text{ก็ต่อเมื่อ} \quad \text{มี } n \in \mathbb{N} \text{ และมี } a \in R - \{0\} \text{ ซึ่ง } na = 0$$

ทฤษฎีบท 7.1.23 ให้ R เป็นอินทิกรัลโดเมนซึ่งมียูนิตี แล้ว

$$\text{Char}(R) = 0 \quad \text{หรือ} \quad \text{Char}(R) = p \quad \text{เมื่อ } p \text{ เป็นจำนวนเฉพาะ}$$

บทแทรก 7.1.24 ถ้า R เป็นอินทิกรัลโดเมนซึ่งมียูนิตีและจำกัด แล้ว

$$\text{Char}(R) \text{ เป็นจำนวนเฉพาะเท่านั้น}$$

แบบฝึกหัด 7.1

1. จงหาตัวหารศูนย์ของริงต่อไปนี้

1.1 $\mathbb{Z}_9$	1.4 $\mathbb{Z}_{24}$	1.7 $\mathbb{Z}_3 \times \mathbb{Z}_4$
1.2 $\mathbb{Z}_{14}$	1.5 $\mathbb{Z}_{51}$	1.8 $\mathbb{Z}_2 \times \mathbb{Z}_5$
1.3 $\mathbb{Z}_{16}$	1.6 $\mathbb{Z}_2 \times \mathbb{Z}_3$	1.9 $\mathbb{Z}_4 \times \mathbb{Z}_6$

2. จงหาจำนวนตัวหารศูนย์ทั้งหมดของริงต่อไปนี้

2.1 $\mathbb{Z}_{50}$	2.3 $\mathbb{Z}_{625}$	2.5 $\mathbb{Z}_7 \times \mathbb{Z}_6$
2.2 $\mathbb{Z}_{250}$	2.4 $\mathbb{Z}_{1500}$	2.6 $\mathbb{Z}_8 \times \mathbb{Z}_9$

3. ให้ R และ R เป็นริงสลับที่ ให้ $a \in R - \{0\}$ และ $b \in S - \{0\}$ จงพิสูจน์ว่า

   ถ้า (a, b) เป็นตัวหารศูนย์ของ $R \times S$ แล้ว a หรือ b เป็นตัวหารศูนย์ของ R และ S ตามลำดับ

4. จงยกตัวอย่างอินทิกรัลโดเมนที่มีสมาชิก 7 ตัวและ 10 ตัว

5. จงแสดงว่า $101 \mid (1000^{100} - 1)$

6. ให้ D เป็นอินทิกรัลโดเมน $a, b \in D$ และ $n, m \in \mathbb{N}$ โดยที่ m และ n เป็นจำนวนเฉพาะสัมพัทธ์กัน จงแสดงว่า

$$\text{ถ้า} \quad a^n = b^n \quad \text{และ} \quad a^m = b^m \quad \text{แล้ว} \quad a = b$$

7. ให้ R เป็นอินทิกรัลโดเมนซึ่งมียูนิตี และ $a \in R - \{0\}$ จงแสดงว่า

   7.1 $\{k \in \mathbb{N} : ka = 0\} \subseteq \{k \in \mathbb{N} : k1 = 0\}$

   7.2 $\{n \in \mathbb{N} :$ มี $a \in R - \{0\}$ ซึ่ง $na = 0\} \subseteq \{n \in \mathbb{N} : n1 = 0\}$

8. จงพิสูจน์ทฤษฎีบท 7.1.23

7.2 ไอดีลใหญ่สุดและไอดีลเฉพาะ

ในหัวข้อนี้จะกล่าวถึงไอดีล 2 ชนิดซึ่งมีความคล้ายคลึงกันและชี้ให้เห็นถึงความแตกต่างกันบางประการจากสมบัติของไอดีลทั้ง 2 แบบ ทำให้ได้ริงผลหารที่น่าสนใจ

บทนิยาม 7.2.1 ให้ M เป็นไอดีลของริง R โดยที่ $M \neq R$ จะกล่าวว่า M เป็น **ไอดีลใหญ่สุด** (maximal ideal) ก็ต่อเมื่อ

$$\text{ทุก ๆ ไอดีล } I \text{ ของ } R \text{ ถ้า } \quad M \subseteq I \subseteq R \quad \text{แล้ว} \quad I = M \quad \text{หรือ} \quad I = R$$

จากบทนิยามจะได้ว่าฟีลด์ F มีไอดีลใหญ่สุดคือ $\{0\}$ เท่านั้น เนื่องจากฟีลด์ F มี 2 ไอดีลเท่านั้น คือ $\{0\}$ และ F โดยทฤษฎีบท 6.2.23 ดังนั้น $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ มีไอดีลใหญ่สุดคือ $\{0\}$ เท่านั้น และ และ $\mathbb{Z}_p$ มีไอดีลใหญ่สุดคือ $\{0\}$ เท่านั้น p เป็นจำนวนเฉพาะ

ตัวอย่าง 7.2.2 จงหาไอดีลใหญ่สุดของริงต่อไปนี้

1. $\mathbb{Z}_6$

2. $\mathbb{Z}_8$

3. $\mathbb{Z}_{12}$

ตัวอย่าง 7.2.3 จงตรวจสอบว่า $\langle 4 \rangle$ และ $\langle 5 \rangle$ เป็นไอดีลใหญ่สุดของ $\mathbb{Z}$ หรือไม่

ทฤษฎีบท 7.2.4 ให้ $p \in \mathbb{N}$ จะได้ว่า

$$\langle p \rangle \text{ เป็นไอดีลใหญ่สุดของ } \mathbb{Z} \quad \text{ก็ต่อเมื่อ} \quad p \text{ เป็นจำนวนเฉพาะ}$$

บทแทรก 7.2.5 สำหรับริง $\mathbb{Z}$ จะได้ว่า

$$\text{ถ้า} \quad M \text{ เป็นไอดีลใหญ่สุดของ } \mathbb{Z} \quad \text{แล้ว} \quad M = \langle p \rangle \quad \text{เมื่อ } p \text{ เป็นจำนวนเฉพาะ}$$

ตัวอย่าง 7.2.6 จงหา $n \in \mathbb{N}$ ซึ่ง $100 < n < 110$ ที่ทำให้ $\langle n \rangle$ เป็นไอดีลใหญ่สุดของ $\mathbb{Z}$

บทตั้ง 7.2.7 ให้ I เป็นไอดีลของริง R และ $I \subseteq J \subseteq R$ จะได้ว่า

J เป็นไอดีลของ R ก็ต่อเมื่อ J/I เป็นไอดีลของ R/I

ทฤษฎีบท 7.2.8 ให้ R เป็นริงสลับที่ซึ่งมียูนิตี และ M เป็นไอดีลของ R โดยที่ $M \neq R$

M เป็นไอดีลใหญ่สุดของ R ก็ต่อเมื่อ R/M เป็นฟีลด์

ตัวอย่าง 7.2.9 จงหาไอดีลใหญ่สุดทั้งหมดของ $\mathbb{Z}_8$ โดยใช้ทฤษฎีบท 7.2.8

บทแทรก 7.2.10 ให้ $n \in \mathbb{N}$ จะได้ว่า

$$\mathbb{Z}/\langle n\rangle \text{ เป็นฟีลด์ ก็ต่อเมื่อ } n \text{ เป็นจำนวนเฉพาะ}$$

ข้อสังเกต 7.2.11 ไอดีลใหญ่สุดของ $\mathbb{Z}_{p^n}$ มีเพียง $\langle \bar{p} \rangle$ เท่านั้น เมื่อ p เป็นจำนวนเฉพาะ และ $n \in \mathbb{N}$

สำหรับ $n \in N$ ซึ่ง $n > 1$ เขียนในรูปแบบบัญญัติคือ

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

จะได้ว่า $\langle \overline{p_1} \rangle, \langle \overline{p_2} \rangle, ..., \langle \overline{p_k} \rangle$ เป็นไอดีลใหญ่สุดของ $\mathbb{Z}_n$ (พิสูจน์เป็นแบบฝึกหัด)

ตัวอย่าง 7.2.12 จงหาไอดีลใหญ่สุดทั้งหมดของริงต่อไปนี้

1. $\mathbb{Z}_{81}$
2. $\mathbb{Z}_{50}$
3. $\mathbb{Z}_{144}$
4. $\mathbb{Z}_{3575}$

ตัวอย่าง 7.2.13 จงหาไอดีลใหญ่สุดทั้งหมดของ $\mathbb{Z}_2 \times \mathbb{Z}_6$

บทนิยาม 7.2.14 ให้ P เป็นไอดีลของริงสลับที่ R และ $P \neq R$ จะกล่าวว่า P เป็น **ไอดีลเฉพาะ** (prime ideal) ก็ต่อเมื่อ

$$\text{ทุก ๆ } a, b \in R \quad \text{ถ้า} \quad ab \in P \quad \text{แล้ว} \quad a \in P \quad \text{หรือ} \quad b \in P$$

หรือกล่าวได้อีกอย่างคือ

$$\text{ทุก ๆ } a, b \in R \quad \text{ถ้า} \quad a \notin P \quad \text{และ} \quad b \notin P \quad \text{แล้ว} \quad ab \notin P$$

ข้อสังเกต 7.2.15 $\{0\}$ เป็นไอดีลเฉพาะของอินทิกรัลโดเมน เนื่องจาก

$$\text{ถ้า} \quad a \neq 0 \quad \text{และ} \quad b \neq 0 \quad \text{แล้ว} \quad ab \neq 0$$

ทฤษฎีบท 7.2.16 ฟีลด์มีไอดีลเฉพาะเพียงตัวเดียวคือ $\{0\}$

ตัวอย่างเช่น $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ มีไอดีลเพียงตัวเดียวคือ $\{0\}$ และ $\mathbb{Z}_p$ มีไอดีลเพียงตัวเดียวคือ $\{\bar{0}\}$ เมื่อ p เป็นจำนวนเฉพาะ เนื่องจากริงเหล่านั้นเป็นฟีลด์ แต่จะเห็นว่า $\{\bar{0}\}$ ไม่เป็นไอดีลเฉพาะของ $\mathbb{Z}_6$ เนื่องจาก

$$\bar{2} \cdot \bar{3} \in \{\bar{0}\} \quad \text{แต่} \quad \bar{2} \notin \{\bar{0}\} \quad \text{และ} \quad \bar{3} \notin \{\bar{0}\}$$

ตัวอย่าง 7.2.17 จงหาไอดีลเฉพาะทั้งหมดของ $\mathbb{Z}_6$

ตัวอย่าง 7.2.18 จงตรวจสอบว่า $\langle 2\rangle$ และ $\langle 10\rangle$ เป็นไอดีลเฉพาะของ $\mathbb{Z}$ หรือไม่

ทฤษฎีบท 7.2.19 ให้ R เป็นริงสลับที่ และ P เป็นไอดีลของ R โดยที่ $P \neq R$ จะได้ว่า

P เป็นไอดีลเฉพาะของ R ก็ต่อเมื่อ R/P เป็นอินทิกรัลโดเมน

บทแทรก 7.2.20 ให้ R เป็นริงสลับที่ซึ่งมียูนิตี

ถ้า M เป็นไอดีลใหญ่สุดของ R แล้ว M เป็นไอดีลเฉพาะ

ตัวอย่าง 7.2.21 จงแสดงว่า $\langle 4 \rangle$ เป็นไอดีลใหญ่สุดแต่ไม่เป็นไอดีลเฉพาะของ (2)

ตัวอย่าง 7.2.22 จงแสดงว่า $\mathbb{Z} \times \{0\}$ เป็นไอดีลเฉพาะแต่ไม่เป็นไอดีลใหญ่สุดของ $\mathbb{Z} \times \mathbb{Z}$

จากตัวอย่าง 7.2.22 บทกลับของบทแทรก 7.2.20 ไม่เป็นจริง ต้องอาศัยการเพิ่มเงื่อนไขให้ริงนั้นมีสมาชิกจำกัดตัวจะทำให้บทกลับเป็นจริงดังทฤษฎีบทต่อไปนี้

บทแทรก 7.2.23 ให้ R เป็นริงจำกัดสลับที่ซึ่งมียูนิตี จะได้ว่า

$$M \text{ เป็นไอดีลใหญ่สุดของ } R \text{ ก็ต่อเมื่อ } M \text{ เป็นไอดีลเฉพาะ}$$

บทแทรก 7.2.24 ให้ $p \in \mathbb{N}$ จะได้ว่า

1. $\langle p \rangle$ เป็นไอดีลเฉพาะของ $\mathbb{Z}$ ก็ต่อเมื่อ p เป็นจำนวนเฉพาะ
2. ถ้า P เป็นไอดีลเฉพาะของ $\mathbb{Z}$ แล้ว $P = \langle p \rangle$ เมื่อ p เป็นจำนวนเฉพาะ

แบบฝึกหัด 7.2

1. จงหาไอดีลใหญ่สุดของริงต่อไปนี้โดยเขียนแลตทิช

   1.1 $\mathbb{Z}_9$ 1.2 $\mathbb{Z}_{15}$ 1.3 $\mathbb{Z}_{24}$ 1.4 $\mathbb{Z}_{36}$ 1.5 $\mathbb{Z}_{48}$

2. จงหาไอดีลใหญ่สุดทั้งหมดของริงต่อไปนี้ พร้อมเขียนแลตทิชประกอบ

   2.1 $\mathbb{Z}_2 \times \mathbb{Z}_3$ 2.2 $\mathbb{Z}_2 \times \mathbb{Z}_5$ 2.3 $\mathbb{Z}_6 \times \mathbb{Z}_4$

3. จงหา $n \in \mathbb{N}$ ซึ่ง $50 < n < 100$ ที่ทำให้ $\langle n \rangle$ เป็นไอดีลใหญ่สุดของ $\mathbb{Z}$

4. จงหาไอดีลเฉพาะทั้งหมดของริงต่อไปนี้

   4.1 $\mathbb{Z}_{64}$ 4.3 $\mathbb{Z}_{275}$ 4.5 $\mathbb{Z}_{1331}$ 4.7 $\mathbb{Z}_{26880}$

   4.2 $\mathbb{Z}_{100}$ 4.4 $\mathbb{Z}_{1300}$ 4.6 $\mathbb{Z}_{1800}$ 4.8 $\mathbb{Z}_{111271}$

5. จงหาจำนวนไอดีลใหญ่สุดของ $\mathbb{Z}_{1600}$

6. ไอดีลที่ไม่เป็นไอดีลเฉพาะของ $\mathbb{Z}_{1000}$ มีทั้งหมดกี่ไอดีล

7. จงยกตัวอย่างของไอดีลใหญ่สุด และไอดีลเฉพาะ ของริงต่อไปนี้

   7.1 $\mathbb{Z}_2 \times \mathbb{Z}$ 7.3 $\mathbb{Z} \times \mathbb{Z}_5$ 7.5 $\mathbb{Z} \times 2\mathbb{Z}$

   7.2 $\mathbb{Z} \times \mathbb{Z}$ 7.4 $\mathbb{Z} \times \mathbb{Q}$ 7.6 $\mathbb{Z}_6 \times \mathbb{Z}_5$

8. จงยกตัวอย่างฟีลด์อันดับ 4, 9 และ 25

9. จงแสดงว่า ถ้า P เป็นไอดีลเฉพาะของ $\mathbb{Z}$ แล้ว $P = \langle p \rangle$ เมื่อ p เป็นจำนวนเฉพะ

10. จงพิสูจน์ว่า $\mathbb{Z} \times p\mathbb{Z}$ เป็นไอดีลใหญ่สุดของ $\mathbb{Z} \times \mathbb{Z}$ ก็ต่อเมื่อ p เป็นจำนวนเฉพาะ

11. จงแสดงว่า $\mathbb{Z} \times 2\mathbb{Z}$ เป็นไอดีลเฉพาะและไอดีลใหญ่สุดของ $\mathbb{Z} \times \mathbb{Z}$

12. จงแสดงว่า $2\mathbb{Z} \times 3\mathbb{Z}$ ไม่เป็นไอดีลใหญ่สุดของ $\mathbb{Z} \times \mathbb{Z}$

13. จงยกตัวอย่างค้านข้อความที่ว่า ถ้า M_1 และ M_2 เป็นไอดีลใหญ่สุดของริง R_1 และ R_2 ตามลำดับ แล้ว $M_1 \times M_2$ เป็นไอดีลใหญ่สุดของ $R_1 \times R_2$

14. จงตรวจสอบว่าข้อความต่อไปนี้เป็นจริงหรือไม่

    ถ้า P_1 และ P_2 เป็นไอดีลเฉพาะของริง R_1 และ R_2 ตามลำดับ
    แล้ว $P_1 \times P_2$ เป็นไอดีลเฉพาะของ $R_1 \times R_2$

7.3 โดเมนซึ่งแยกตัวประกอบได้อย่างเดียว

เมื่อกล่าวถึงอินทิกรัลโดเมน $\mathbb{Z}$ เราทราบกันดีว่าสมาชิกทุกตัวใน สามารถแยกเป็นผลคูณของจำนวนเฉพาะได้เสมอ และจำนวนเต็มที่มากกว่า 1 สามารถเขียนในรูปแบบบัญญัติได้เพียงแบบเดียวเท่านั้น เราจะขยายแนวคิดนี้ไปยังอินทิกรัลโดเมนอื่น ๆ ซึ่งมีสมบัติพิเศษดังกล่าว โดยเริ่มจากการนิยามการหารลงบทนิยามต่อไปนี้

บทนิยาม 7.3.1 ให้ R เป็นริงสลับที่ซึ่งมียูนิตี และ $a, b \in R$
จะกล่าวว่า $\boldsymbol{a}$ **หาร** $\boldsymbol{b}$ **ลงตัว** ($\boldsymbol{a}$ divides $\boldsymbol{b}$) เขียนแทนด้วย $a \mid b$ ก็ต่อเมื่อ

$$\text{มี} \quad c \in R \quad \text{ซึ่ง} \quad b = ac$$

ตัวอย่างเช่น

ใน $\mathbb{Z}$ จะได้ว่า $2 \mid 4$ เนื่องจาก $4 = 2 \cdot 2$

ใน $\mathbb{R}$ จะได้ว่า $2 \mid 1.2$ เนื่องจาก $1.2 = 2 \cdot 0.6$

ข้อสังเกต 7.3.2 ให้ R เป็นริงสลับที่ซึ่งมียูนิตี และ $a, b \in R$ จะได้ว่า

1. $a \mid 0$, $1 \mid a$ และ $a \mid a$ เนื่องจาก $0 = 0a$ และ $a = 1a$
2. $a \mid b$ ก็ต่อเมื่อ มี $k \in R$ ซึ่ง $b = ak$ ก็ต่อเมื่อ $b \in \langle a \rangle$

เราจะทบทวนว่า a เป็นหน่วยในริง R ซึ่งมียูนิตี (ดูบทนิยาม 6.1.20) หมายถึง

$$\text{มี } b \in R \quad \text{ซึ่ง} \quad ab = 1 = ba$$

จากนี้เราจะศึกษาเฉพาะสมาชิกที่ไม่ใช่หน่วยในอินทิกรัลโดเมนซึ่งมียูนิตี เพื่อนำไปศึกษาสมบัติการแยกตัวประกอบได้อย่างเดียวต่อไป

บทนิยาม 7.3.3 ให้ D เป็นอินทิกรัลโดเมนซึ่งมียูนิตี ให้ $r \in D - \{0\}$ และ r ไม่เป็นหน่วย
จะกล่าวว่า r **ลดทอนไม่ได้** (irreducible) ก็ต่อเมื่อ

$$\text{ถ้า} \quad r = ab \quad \text{แล้ว} \quad a \quad \text{หรือ} \quad b \quad \text{เป็นหน่วย}$$

ถ้าเป็นอย่างอื่นเรียก r ว่า **ลดทอนได้** (reducible) นั่นคือ r ลดทอนได้ ก็ต่อเมื่อ

$$r = ab \quad \text{โดยที่} \quad a \quad \text{และ} \quad b \quad \text{ไม่เป็นหน่วย}$$

ข้อสังเกต 7.3.4 เนื่องจากฟีลด์สมาชิกทุกตัวที่ไม่ใช่ศูนย์เป็นหน่วย ดังนั้นจะไม่กล่าวถึงลดทอนได้หรือไม่ได้ของสมาชิกในฟีลด์

เนื่องจาก $\mathbb{Z}_n$ เป็นอินทิกรัลโดเมนก็ต่อเมื่อ p เป็นจำนวนเฉพาะ นั่นคือ $\mathbb{Z}_p$ เป็นฟีลด์ ดังนั้นจะไม่กล่าวถึงลดทอนได้หรือไม่ได้ของสมาชิกใน $\mathbb{Z}_p$

สำหรับริง $\mathbb{Z}$ จะเห็นว่ามีหน่วยคือ 1 และ -1 เท่านั้น จากบทนิยามของการลดทอนไม่ได้ จะได้ว่า

$$p \quad \text{ลดทอนไม่ได้} \qquad \text{ก็ต่อเมื่อ} \qquad p \quad \text{เป็นจำนวนเฉพาะ}$$

สำหรับ $T \in \mathbb{Z}$ กำหนดให้

$$\mathbb{Z}[\sqrt{T}] = \{a + b\sqrt{T} : a, b \in \mathbb{Z}\}$$

แล้วจะได้ว่า $\mathbb{Z}[\sqrt{T}]$ เป็นริงย่อยของ $\mathbb{C}$ และเป็นอินทิกรัลโดเมนที่มียูนิตี (เป็นแบบฝึกหัด)

ทฤษฎีบท 7.3.5 ให้ $a, b \in \mathbb{Z}$ และ $K \in \mathbb{Z}$ โดยที่ $K > 0$ จะได้ว่า

$$a + b\sqrt{-K} \quad \text{เป็นหน่วยใน} \quad \mathbb{Z}[\sqrt{-K}] \quad \text{ก็ต่อเมื่อ} \quad a^2 + Kb^2 = 1$$

ตัวอย่าง 7.3.6 จงแสดงว่า 2 และ 3 ลดทอนไม่ได้ใน $\mathbb{Z}[\sqrt{-5}]$

ตัวอย่าง 7.3.7 จงแสดงว่า $1 + \sqrt{-5}$ ลดทอนไม่ได้ใน $\mathbb{Z}[\sqrt{-5}]$

บทนิยาม 7.3.8 ให้ D เป็นอินทิกรัลโดเมนซึ่งมียูนิตี ให้ $p \in D - \{0\}$ และ p ไม่เป็นหน่วย จะกล่าวว่า p เป็น **สมาชิกเฉพาะ** (prime element) ของ D ก็ต่อเมื่อ

$$\text{ถ้า} \quad p \mid ab \quad \text{แล้ว} \quad p \mid a \quad \text{หรือ} \quad p \mid b$$

สำหรับริง $\mathbb{Z}$ จะได้ว่าจำนวนเฉพาะเป็นสมาชิกเฉพาะของ $\mathbb{Z}$

ทฤษฎีบท 7.3.9 ให้ D เป็นอินทิกรัลโดเมนซึ่งมียูนิตี จะได้ว่า

ถ้า p เป็นสมาชิกเฉพาะของ D แล้ว p ลดทอนไม่ได้

ตัวอย่าง 7.3.10 จงแสดงว่า 3 ลดทอนไม่ได้ใน $\mathbb{Z}[\sqrt{-5}]$ แต่ไม่เป็นสมาชิกเฉพาะ

บทนิยาม 7.3.11 ให้ D เป็นอินทิกรัลโดเมนซึ่งมียูนิตี
จะกล่าวว่า D เป็น **โดเมนซึ่งแยกตัวประกอบได้อย่างเดียว** (Unique Factorization Domain) เขียนสั้น ๆ ว่า U.F.D. ก็ต่อเมื่อ สำหรับ $d \in D - \{0\}$ และ d ไม่เป็นหน่วย สอดคล้อง 2 เงื่อนไขดังนี้

1. มี $p_1, p_2, ..., p_n \in D$ ซึ่งลดทอนไม่ได้ และ $d = p_1p_2...p_n$
2. ถ้า $d = p_1p_2...p_n = q_1q_2...q_m$ เมื่อ $q_1, q_2, ..., q_m \in D$

   แล้ว $n = m$ และสำหรับ i จะมี j ซึ่ง $p_i = uq_j$ โดยที่ u เป็นหน่วย

   เมื่อ $i, j \in \{1, 2, ..., n\}$

โดยทฤษฎีบทหลักมูลเลขคณิต (ทฤษฎีบท 1.3.25) สรุปได้ว่า $\mathbb{Z}$ เป็น U.F.D. และฟีลด์เป็น U.F.D. เสมอเนื่องจากทุกสมาชิกที่ไม่ใช่ศูนย์เป็นหน่วย ดังนั้น $\mathbb{Q}$, $\mathbb{R}$ และ $\mathbb{C}$ เป็น U.F.D.

ตัวอย่าง 7.3.12 จงแสดงว่า $\mathbb{Z}[\sqrt{-5}]$ ไม่เป็น U.F.D.

ทฤษฎีบท 7.3.13 สมาชิกซึ่งลดทอนไม่ได้ของ U.F.D. จะเป็นสมาชิกเฉพาะ

บทนิยาม 7.3.14 ให้ D อินทิกรัลโดเมนซึ่งมียูนิตี
จะกล่าวว่า D เป็น **โดเมนไอดีลมุขสำคัญ (Principal Ideal Domain)** เขียนแทนด้วย P.I.D.
ก็ต่อเมื่อ ทุกไอดีลของ D เป็นไอดีลมุขสำคัญ

ตัวอย่างเช่น $\mathbb{Z}$ เป็น P.I.D. เนื่องจากทุกไอดีลของ $\mathbb{Z}$ อยู่ในรูป $n\mathbb{Z}$ หรือ (n) และสนามเป็น P.I.D. เสมอเนื่องจากมี 2 ไอดีลเท่านั้นคือ $\langle 0\rangle$ และ $\langle 1\rangle$

ทฤษฎีบท 7.3.15 สมาชิกลดทอนไม่ได้ใน P.I.D. จะเป็นสมาชิกเฉพาะ

บทแทรก 7.3.16 ให้ D เป็น P.I.D. โดยที่ p ลดทอนไม่ได้ใน D และ $a_1, a_2, ..., a_n \in D$

ถ้า $p \mid (a_1 a_2 ... a_n)$ แล้ว มี $i \in \{1, 2, ..., n\}$ ซึ่ง $p \mid a_i$

ทฤษฎีบท 7.3.17 ให้ D เป็น P.I.D. และ $p \in D - \{0\}$ ซึ่งไม่ใช่สมาชิกหน่วย แล้ว

$$\langle p \rangle \text{ เป็นไอดีลใหญ่สุดของ } D \quad \text{ก็ต่อเมื่อ} \quad p \text{ ลดทอนไม่ได้ใน } D$$

ต่อไปเราสามารถพิสูจน์ได้ว่า P.I.D. เป็น U.F.D. เสมอ ทำให้เห็นถึงความสัมพันธ์ระหว่าง P.I.D. และ U.F.D. สำหรับการพิสูจน์จะขอเว้นไว้ในรายวิชานี้

ทฤษฎีบท 7.3.18 P.I.D. เป็น U.F.D.

บทนิยาม 7.3.19 ให้ E อินทิกรัลโดเมนซึ่งมียูนิตี
จะกล่าวว่า E เป็น **ริงแบบยุคลิด** (Euclidean ring) ก็ต่อเมื่อ มีฟังก์ชัน $d : E - \{0\} \to \mathbb{N}_0$
ซึ่งสำหรับทุก $a, b \in E - \{0\}$ สอดคล้อง 2 เงื่อนไขต่อไปนี้

1. $d(b) \leq d(ab)$
2. มี $q, r \in E$ ซึ่ง $\;b = aq + r\;$ โดยที่ $r = 0$ หรือ $d(r) < d(a)$

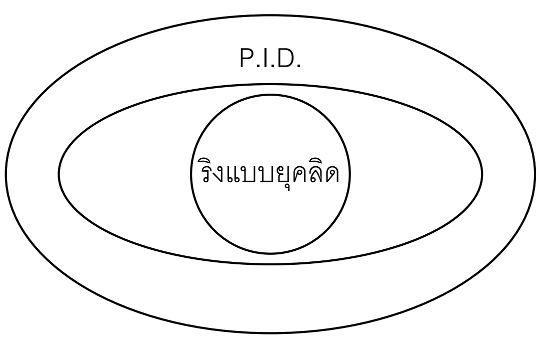
ตัวอย่าง 7.3.20 จงแสดงว่า $\mathbb{Z}$ เป็นริงแบบยุคลิด

ทฤษฎีบท 7.3.21 ฟีลด์เป็นริงแบบยุคลิด

สรุปได้ว่า $\mathbb{Q}$, $\mathbb{R}$ และ $\mathbb{C}$ เป็นริงแบบยุคลิด

ทฤษฎีบท 7.3.22 ริงแบบยุคลิดเป็น P.I.D.

จากทฤษฎีบทที่ผ่านมาของ ริงยุคลิด P.I.D และ U.F.D. อาจแสดงความสัมพันธ์ได้ดังนี้



แบบฝึกหัด 7.3

1. ให้ D เป็นอินทิกรัลโดเมนซึ่งมียูนิตี ให้ $a, b \in D - \{0\}$ จงพิสูจน์ว่า

$$a \mid b \quad \text{และ} \quad b \mid a \quad \text{ก็ต่อเมื่อ} \quad \langle a \rangle = \langle b \rangle$$

2. ให้ $T \in \mathbb{Z}$ จงแสดงว่า $\mathbb{Z}[\sqrt{T}]$ เป็นอินทิกรัลโดเมนที่มียูนิตี

3. สามารถนิยาม $0 \mid 0$ ได้หรือไม่ในอินทิกรัลโดเมนซึ่งมียูนิตี จงให้เหตุผลประกอบ

4. จงหาหน่วยทั้งหมดของ

   4.1 $\mathbb{Z}[\sqrt{-1}]$

   4.2 $\mathbb{Z}[\sqrt{-3}]$

   4.3 $\mathbb{Z}[\sqrt{-5}]$

   4.4 $\mathbb{Z}[\sqrt{-6}]$

   4.5 $\mathbb{Z}[\sqrt{-7}]$

   4.6 $\mathbb{Z}[\sqrt{-8}]$

5. จงยกตัวอย่างหน่วยใน $\mathbb{Z}[\sqrt{3}]$ มาอย่างน้อย 2 ตัว ที่ไม่ใช่ 1 และ -1

6. จงแสดงว่า 2 และ 7 ไม่เป็นสมาชิกเฉพาะของ $\mathbb{Z}[\sqrt{-5}]$

7. จงแสดงว่า $1 - \sqrt{-5}$ ลดทอนไม่ได้ใน $\mathbb{Z}[\sqrt{-5}]$

8. จงแสดงว่า 7 และ 13 ลดทอนไม่ได้ใน $\mathbb{Z}[\sqrt{-5}]$

9. จงยกตัวอย่างสมาชิกใน $\mathbb{Z}[\sqrt{-3}]$ ซึ่งลดทอนไม่ได้

10. จงแสดงว่า $\mathbb{Z}[\sqrt{-3}]$ เป็นอินทิกรัลโดเมนแต่ไม่เป็น U.F.D.

11. ให้ D เป็น P.I.D. และ $p \in D - \{0\}$ ซึ่งไม่ใช่สมาชิกหน่วย จงแสดงว่า

$$\text{ถ้า } p \text{ ลดทอนไม่ได้ใน } D \text{ แล้ว } \langle p \rangle \text{ เป็นไอดีลใหญ่สุดของ } D$$

12. พิสูจน์บทแทรก 7.3.16 โดยอุปนัยเชิงคณิตศาสตร์

13. จงแสดงว่า $\mathbb{Z}[i]$ เป็นริงแบบยุคลิด

14. จงพิสูจน์ว่า ริงแบบยุคลิดมีหน่วยเสมอ

15. จงแสดงว่า $\mathbb{Z}[\sqrt{-5}]$ ไม่เป็นริงแบบยุคลิด

บทที่ 8

ริงพหุนาม

การศึกพหุนามนั้นมีมาช้านานตั้งแต่ยุคแรกเริ่มในสมัยกรีกโรมัน จนเป็นที่สนใจมากขึ้นในสมัยของคาร์ดานผู้บุกเบิกวิชาพีชคณิตที่สนในการหาคำตอบในรูปทั่วของของพหนุนามกำลังสาม เป็นจุดเริ่มต้นของวิชาพีชคณิตนามธรรม ในบทนี้เราจะขยายบทนิยามของพหุนามให้ทั่วไปมากยิ่งขึ้นที่เรียกว่าริงพหุนาม และศึกษาสมบัติต่าง ๆ ที่เกิดขึ้นดังจะกล่าวต่อไปนี้

8.1 พหุนาม

บทนิยาม 8.1.1 ให้ R เป็นริงสลับที่ซึ่งมียูนิตี กำหนดให้

$$R[x] = \{a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \, : \, a_i \in R, \, n \in \mathbb{N}_0\}$$

เรียกสมาชิก $p(x)$ ใน $R[x]$ ว่า **พหุนาม** (polynomial) ซึ่งอยู่ในรูป

$$p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = \sum_{i=0}^{n} a_ix^i$$

โดยนิยามส่วนต่าง ๆ ดังนี้

- $a_n, a_{n-1}, ..., a_1, a_0$ เรียกว่า **สัมประสิทธิ์** (coefficient) ของ $x^n, x^{n-1}, ..., x, 1$ ตามลำดับ
- เรียก $a_n \neq 0$ ว่า **สัมประสิทธิ์ตัวนำ** (leading coefficient) ถ้า $a_i \neq 0$ เรียกแต่ละ a_ix^i ว่า **พจน์** (term) ของพหุนาม $p(x)$ หรือ **เอกนาม** (monomial)
- ถ้า $a_n \neq 0$ เรียก $p(x)$ ว่า **พหุนามระดับขั้น** n (polynomial of degree n) และเขียน n แทนด้วย deg $p(x)$ นั่นคือ deg $p(x) = n$
- ถ้า $a_n = 1$ เรียก $p(x)$ ว่า **พหุนามโมนิก** (monic polynomial)
- ถ้า $p(x) = a_0$ เรียก $p(x)$ ว่า **พหุนามคงตัว** (constant polynomial)
ให้ deg $p(x) = 0$ เมื่อ $a_0 \neq 0$
- กรณี $p(x) = 0$ เรียก **พหุนามศูนย์** (zero polynomaial) และไม่นิยามระดับขั้น

ข้อสังเกต 8.1.2 ให้ R เป็นริงสลับที่ซึ่งมียูนิตี เห็นได้ชัดว่า $R \subseteq R[x]$

ตัวอย่างเช่น $p(x) = 5x^2 - 2x + 3 \in \mathbb{Z}[x]$ เป็นพหุนามระดับขั้น 2 มี 5 เป็นสัมประสิทธิ์ตัวนำ และ $5, -2, 3$ เป็นสัมประสิทธิ์ของ $x^2, x, 1$ ตามลำดับ เนื่องจาก $a_2 = 5 \neq 1$ จะได้ว่า $p(x)$ ไม่เป็นพหุนามโมนิก และ $q(x) = 1 + x^7 \in \mathbb{Z}[x]$ เป็นพหุนามโมนิกระดับขั้น 7 เนื่องจาก $a_7 = 1$

ถ้า 1 เป็นยูนิตีใน R เราจะเขียนพจน์ x^i และ $-x^i$ แทนด้วยพจน์ $1x^i$ และ $-1x^i$ ตามลำดับ สำหรับ $i \in \mathbb{N}$

ตัวอย่าง 8.1.3 จงเขียนสมาชิกทั้งหมดของพหุนามระดับขั้น 2 ใน $\mathbb{Z}_2[x]$

ตัวอย่าง 8.1.4 จงเขียนสมาชิกทั้งหมดของพหุนามที่มีระดับขั้นไม่เกิน 1 ใน $\mathbb{Z}_3[x]$

จากตัวอย่าง 8.1.3 จะเห็นว่า a ที่เป็นไปได้คือ $\bar{1}$ เพียงแบบเดียวใน $\mathbb{Z}_2[x]$ เนื่องจาก เพราะเป็นสัมประสิทธิ์ตัวนำ สำหรับ b และ c อาจจะเป็น $\bar{0}$ หรือ $\bar{1}$ ดังนั้น จำนวนพหุนามระดับขั้น 2 ใน $\mathbb{Z}_2[x]$ เท่ากับ $1 \cdot 2 \cdot 2 = 4$ แบบ ดังนั้นไปยังจำนวนพหุนามระดับขั้น m ใน $\mathbb{Z}_2[x]$ จะมีทั้งหมด

$$1 \cdot \underbrace{2 \cdot 2 \cdot \dots \cdot 2}_{m \text{ ตัว}} = 2^m$$

และจำนวนพหุนามระดับขั้น m ใน $\mathbb{Z}_n[x]$ จะเท่ากับ

$$(n-1) \cdot \underbrace{n \cdot n \cdot \dots \cdot n}_{m \text{ ตัว}} = (n-1) \cdot n^m$$

สำหรับจำนวนพหุนามระดับขั้นน้อยกว่า m ใน $\mathbb{Z}_n[x]$ รวมพหุนามศูนย์จะเท่ากับ

$$n \cdot \underbrace{n \cdot n \cdot \dots \cdot n}_{m \text{ ตัว}} = n^{m+1}$$

บทนิยาม 8.1.5 ให้ R เป็นริงสลับที่ซึ่งมียูนิตี ให้ $p(x)$ และ $q(x)$ เป็นพหุนามที่ไม่ใช่พหุนามศูนย์ใน $R[x]$ จะได้ว่า $p(x) = q(x)$ ก็ต่อเมื่อ $\deg p(x) = \deg q(x)$ และอยู่ในรูป

$$p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$
$$q(x) = b_nx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$$

เมื่อ $n \in \mathbb{N}_0$ และ $a_i = b_i$ ทุก ๆ $i \in \{1, 2, ..., n\}$

ตัวอย่าง 8.1.6 ให้ $p(x) = \bar{2}x^2 + x + \bar{1}$ และ $q(x) = ax^2 + bx + c$ เป็นพหุนามใน $\mathbb{Z}_2[x]$ ถ้า $p(x) = q(x)$ จงหา a, b และ c

บทนิยาม 8.1.7 ให้ R เป็นริงสลับที่ซึ่งมียูนิตี ถ้า $p(x)$ และ $q(x)$ เป็นพหุนามใน $R[x]$ ซึ่ง

$$p(x) = a_mx^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$$
$$q(x) = b_nx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$$

เมื่อ $m, n \in \mathbb{N}_0$ และ $m \leq n$ แล้ว

$$p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_{m+1}x^{m+1} + a_mx^m + \cdots + a_1x + a_0$$

โดยที่ $a_{m+1} = a_{m+2} = ... = a_n = 0$ เมื่อ $m < n$ นิยามการบวกและการคูณ $p(x)$ และ $q(x)$ คือ

$$p(x) + q(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$
$$p(x) \cdot q(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_kx^k + \cdots + c_1x + c_0$$

เมื่อ $c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0$ โดยที่ $k = 0, 1, 2, ..., m+n$ ซึ่ง $a_k = b_k = 0$ ทุก ๆ $k > n$

สำหรับ $p(x) \cdot q(x)$ จะเขียนแทนด้วย $p(x)q(x)$ และจากบทนิยามข้างต้นจะได้ข้อสังเกตต่อไปนี้

ข้อสังเกต 8.1.8 ให้ R เป็นริงสลับที่ซึ่งมียูนิตี ถ้า $p(x)$ และ $q(x)$ เป็นพหุนามที่ไม่ใช่พหุนามศูนย์ใน $R[x]$ แล้วจะได้ว่า

1. $\deg\,(p(x) + q(x)) \leq \max\{\deg p(x), \deg q(x)\}$ หรือ $p(x) + q(x) = 0$
2. $\deg\,(p(x)q(x)) \leq \deg p(x) + \deg q(x)$ หรือ $p(x) \cdot q(x) = 0$

จะเห็นว่าการบวกพหุนามทำได้โดยง่าย แต่การคูณพหุนามสามารถหาโดยใช้บทนิยามมีความยุ่งยาก เราอาจจะหาผลคูณพหุนามโดยจากการแจกแจง หรือสร้างตารางการคูณแต่ละพจน์ ดังจะแสดงในตัวอย่างต่อไปนี้

ตัวอย่าง 8.1.9 กำหนดให้ $p(x) = x^3 + x^2 - 3x + 1$ และ $q(x) = x^2 - 3$ เป็นพหุนามใน $\mathbb{Z}[x]$ จงหา $p(x) + q(x)$ และ $p(x)q(x)$ โดยบทนิยาม การแจกแจง และใช้ตาราง

ตัวอย่าง 8.1.10 กำหนดให้

$p(x) = Ax^3 + Bx^2 + Cx + D$ และ $q(x) = (x-2)(x+3)(x+1) + 5$ เป็นพหุนามใน $\mathbb{Z}[x]$ ถ้า $p(x) = q(x)$ จงหาค่าของ A, B, C และ D

ตัวอย่าง 8.1.11 ให้ $p(x) = x^2 + ax + b$ และ $q(x) = x^4 + x^3 + x + \bar{1}$ เป็นพหุนามใน $\mathbb{Z}_3[x]$ ถ้า $[p(x)]^2 = q(x)$ จงหา a และ b

ทฤษฎีบท 8.1.12 ให้ R เป็นริงสลับที่ซึ่งมียูนิตี แล้ว

$R[x]$ ซึ่งนิยามการบวกและการคูณในบทนิยาม 8.1.7 เป็นริงสลับที่ซึ่งมียูนิตี และเรียก $R[x]$ ว่า **ริงพหุนาม (polynomial ring)**

ถ้า R เป็นริงสลับที่ซึ่งมียูนิตี จะได้ว่า

- ศูนย์ใน $R[x]$ คือพหุนามศูนย์เขียนแทนด้วย 0
- ยูนิตีใน $R[x]$ คือพหุนามคงตัวยูนิตี เขียนแทนด้วย 1

นั่นคือริง $R[x]$ มีศูนย์และยูนิตีเป็นตัวเดียวกับ R

ตัวอย่าง 8.1.13 ให้ $p(x), q(x), r(x)$ เป็นพหุนามใน $\mathbb{Z}_4[x]$ โดยที่

$$p(x) = \bar{2}x^2 + x + \bar{2}, \quad q(x) = \bar{2}x^2 + \bar{2} \quad \text{และ} \quad r(x) = \bar{2}x^3 + \bar{1}$$

จงหา $p(x) + q(x)$, $q(x) + r(x)$, $[q(x)]^2$ และ $q(x)r(x)$

ทฤษฎีบท 8.1.14 ถ้า R เป็นอินทิกรัลโดเมนซึ่งมียูนิตี แล้ว

$$R[x] \text{ เป็นอินทิกรัลโดเมนซึ่งมียูนิตี}$$

ทฤษฎีบท 8.1.15 ให้ R เป็นอินทิกรัลโดเมนซึ่งมียูนิตี
ถ้า $p(x)$ และ $q(x)$ เป็นพหุนามที่ไม่ใช่พหุนามศูนย์ใน $R[x]$ แล้วจะได้ว่า

1. deg $(p(x)q(x))$ = deg $p(x)$ + deg $q(x)$
2. deg $p(x) \leq$ deg $(p(x)q(x))$

ทฤษฎีบท 8.1.16 ให้ R เป็นอินทิกรัลโดเมนซึ่งมียูนิตีจะได้ว่า

หน่วยใน R และ $R[x]$ คือตัวเดียวกัน

บทแทรก 8.1.17 ให้ R เป็นอินทิกรัลโดเมนซึ่งมียูนิตี แล้ว $\mathcal{U}(R[x]) = \mathcal{U}(R)$

ข้อสังเกต 8.1.18 สำหรับอินทิกรัลโดเมน $R[x]$ พหุนามที่ไม่ใช่ศูนย์ที่ระดับขั้นมากกว่า 0 ไม่เป็นหน่วยใน $R[x]$

แบบฝึกหัด 8.1

1. จงเขียนสมาชิกทั้งหมดของพหุนามระดับขั้น 3 ใน $\mathbb{Z}_2[x]$
2. จงเขียนสมาชิกทั้งหมดของพหุนามระดับขั้น 2 และ 3 ใน $\mathbb{Z}_3[x]$
3. จงหาจำนวนพหุนามระดับขั้น 5 ทั้งหมดใน $\mathbb{Z}_7[x]$
4. จงหาจำนวนพหุนามระดับขั้นไม่เกิน 3 ทั้งหมดใน $\mathbb{Z}_5[x]$
5. จงหาจำนวนของพหุนาม $p(x)$ ใน $\mathbb{Z}_n[x]$ ซึ่ง $\deg p(x) \leq k$ โดยที่ $k, n \in \mathbb{N}$
6. จงหาหน่วยทั้งหมดในริงพหุนามต่อไปนี้

   6.1 $\mathbb{Z}_3[x]$ 6.3 $\mathbb{Z}_6[x]$ 6.5 $\mathbb{Z}[x]$

   6.2 $\mathbb{Z}_5[x]$ 6.4 $\mathbb{Z}_{13}[x]$ 6.6 $\mathbb{Q}[x]$

7. ใน $\mathbb{Z}_6[x]$

   7.1 จงหาพหุนามระดับขั้นหนึ่งทั้งหมดใน $\mathbb{Z}_6[x]$

   7.2 จงหา $x \in \mathbb{Z}_6$ ที่สอดคล้อง $\bar{2}x^2 + \bar{3}x + \bar{1} = \bar{0}$

   7.3 จงเขียน $(\bar{2}x^2 + \bar{3}x + \bar{1})^2$ ในรูป $ax^4 + bx^3 + cx^2 + dx + e$

8. ให้ R เป็นริงสลับที่ซึ่งมียูนิตี จงแสดงว่า

   $R[x]$ ซึ่งนิยามการบวกและการคูณในบทนิยาม 8.1.7 เป็นริงสลับที่ซึ่งมียูนิตี

9. ให้ R เป็นอินทิกรัลโดเมนซึ่งมียูนิตี ถ้า $p(x)$ และ $q(x)$ เป็นพหุนามที่ไม่ใช่พหุนามศูนย์ใน $R[x]$ จงแสดงว่า

   $$\deg p(x) \leq \deg\,(p(x) \cdot q(x))$$

10. จงยกตัวอย่างฟีลด์ F ที่ทำให้ $F[x]$ ไม่เป็นฟีลด์

8.2 ริงพหุนามบนฟีลด์

ในหัวข้อนี้จะศึกษาริงพหุหนาม $F[x]$ เมื่อ F เป็นฟีลด์ เรียกว่า **ริงพหุนามบนฟีลด์** (polynomial ring on field)

ทฤษฎีบท 8.2.1 **ขั้นตอนวิธีการหารสำหรับพหุนาม** (The Division Algorithm for Polynomial) ให้ F เป็นฟีลด์ และ $a(x)$, $b(x)$ เป็นพหุนามใน $F[x]$ โดยที่ $a(x)$ ไม่เป็นพหุนามศูนย์ แล้วจะได้ว่ามีพหุนาม $q(x)$ และ $r(x)$ เพียงคู่เดียวเท่านั้นใน $F[x]$ ที่สอดคล้อง

$$b(x) = q(x)a(x) + r(x) \qquad \text{เมื่อ } \; r(x) = 0 \quad \text{หรือ} \quad \deg r(x) < \deg a(x)$$

เรียก $r(x)$ ว่า **เศษเหลือ** (remainder) และ $q(x)$ ว่า **ผลหาร** (quotient) ของการหาร $b(x)$ ด้วย $a(x)$

ในกรณี $r(x) = 0$ โดยบทนิยาม 7.3.1 จะได้ว่า $a(x)$ หาร $b(x)$ ได้ หรือเขียนแทนด้วย $a(x) \mid b(x)$ โดยเรียก $a(x)$ ว่า **ตัวประกอบ** (factor) ของ $b(x)$ ใน $F[x]$

ตัวอย่าง 8.2.2 จงหาผลหารและเศษเหลือที่เกิดจากการหาร

$$b(x) = x^3 + 1 \text{ ด้วย } a(x) = x^2 - 1 \text{ ใน } \mathbb{Z}[x]$$

ทฤษฎีบท 8.2.3 ถ้า F เป็นฟีลด์ แล้ว $F[x]$ เป็นริงแบบยุคลิด

บทแทรก 8.2.4 ถ้า F เป็นฟีลด์ แล้ว $F[x]$ เป็น P.I.D. และ U.F.D.

ทฤษฎีบท 8.2.5 ให้ F เป็นฟีลด์ และ $p(x)$ เป็นพหุนามที่ไม่ใช่พหุนามศูนย์ใน $F[x]$ แล้วข้อความต่อไปนี้สมมูลกัน

1. $p(x)$ เป็นหน่วยใน $F[x]$
2. $p(x)$ เป็นพหุนามคงตัวที่ไม่ใช่พหุนามศูนย์ใน $F[x]$
3. deg $p(x) = 0$

เนื่องจาก $F[x]$ เป็นอินทิกรัลโดเมน เมื่อ F เป็นฟีลด์ เราสามารถกล่าวถึงการลดทอนได้หรือไม่ได้ของพหุนาม

ตัวอย่าง 8.2.6 จงแสดงว่า

1. $x^2 + 1$ ลดทอนไม่ได้ใน $\mathbb{R}[x]$ แต่ลดทอนได้ใน $\mathbb{C}[x]$

2. $2x + 4$ ลดทอนไม่ได้ใน $\mathbb{R}[x]$ แต่ลดทอนได้ใน $\mathbb{Z}[x]$

3. $x^2 + x + \bar{1}$ ลดทอนไม่ได้ใน $\mathbb{Z}_2[x]$

บทแทรก 8.2.7 ให้ F เป็นฟีลด์และ $p(x)$ เป็นพหุนามซึ่งไม่ใช่พหุนามศูนย์ใน $F[x]$ โดยที่ $f(x)$ และ $g(x)$ เป็นพหุนาใน $F[x]$ แล้วข้อความต่อไปนี้สมมูลกัน

1. $p(x)$ ลดทอนไม่ได้ใน $F[x]$

2. ถ้า $p(x) = f(x) \cdot g(x)$ แล้ว deg $f(x) = 0$ หรือ deg $g(x) = 0$

ทฤษฎีบท 8.2.8 ให้ F เป็นฟีลด์และ $p(x)$ เป็นพหุนามระดับขั้น 1 ใน $F[x]$ จะได้ว่า

$$p(x) \text{ ลดทอนไม่ได้ใน } F[x]$$

ทฤษฎีบท 8.2.9 ให้ F เป็นฟีลด์ และ $p(x)$ เป็นพหุนามใน $F[x]$ แล้วข้อความต่อไปนี้สมมูลกัน

1. $\langle p(x) \rangle$ เป็นไอดีลใหญ่สุด
2. $p(x)$ ลดทอนไม่ได้ใน $F[x]$
3. $F[x]/\langle p(x) \rangle$ เป็นฟีลด์

ตัวอย่าง 8.2.10 จงตรวจสอบว่า $\mathbb{Z}_3[x]/\langle x^2 + \bar{1} \rangle$ เป็นฟีลด์หรือไม่

ทฤษฎีบท 8.2.11 ให้ F เป็นฟีลด์ และ $p(x)$ ลดทอนไม่ได้ใน $F[x]$ โดยที่ deg $p(x) = n$ จะได้ว่า

$$F[x]/\langle p(x)\rangle = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 + \langle p(x)\rangle \, : \, a_i \in F \text{ ทุก ๆ } i\}$$

ตัวอย่าง 8.2.12 จงเขียนรูปแบบสมาชิกของฟีลด์ต่อไปนี้

1. $\mathbb{C}[x]/\langle x+1\rangle =$
2. $\mathbb{R}[x]/\langle x^2+1\rangle =$

ตัวอย่าง 8.2.13 จงแจกแจงสมาชิกของ $\mathbb{Z}_3/\langle x^2+\bar{1}\rangle$

บทแทรก 8.2.14 ให้ p เป็นจำนวนเฉพาะ และ $g(x)$ ลดทอนไม่ได้ใน $\mathbb{Z}_p[x]$ โดยที่ deg $g(x) = n$ แล้ว

$$\mathbb{Z}_p[x]/\langle g(x)\rangle \text{ เป็นฟีลด์อันดับ } p^n$$

ตัวอย่าง 8.2.15 จงหาจำนวนสมาชิกของ $\mathbb{Z}_2/\langle x^2 + x + \bar{1}\rangle$

ตัวอย่าง 8.2.16 จงยกตัวอย่างฟีลด์อันดับ 25

ตัวอย่าง 8.2.17 จงสร้างตารางกรุปการคูณของ $\mathbb{Z}_2[x]/\left\langle x^2+x+\bar{1}\right\rangle$ พร้อมหาตัวผกผันการคูณของสมาชิก

ตัวอย่าง 8.2.18 จงหาตัวผกผันการคูณของ $x+1+\left\langle x^2+1\right\rangle$ ใน $\mathbb{R}[x]/\left\langle x^2+1\right\rangle$

แบบฝึกหัด 8.2

1. จงตรวจสอบว่าสมาชิกต่อไปนี้ลดทอนได้หรือไม่ในริงที่กำหนด

1.1 $x^2 + x + \bar{4}$	ใน $\mathbb{Z}_{11}[x]$	1.6 $x^3 + x^2 + x + 1$	ใน $\mathbb{R}[x]$
1.2 $\bar{2}x^3 + x^2 + \bar{2}x + \bar{2}$	ใน $\mathbb{Z}_5[x]$	1.7 $x^3 - x^2 - 2x + 2$	ใน $\mathbb{R}[x]$
1.3 $x^2 + \bar{1}$	ใน $\mathbb{Z}_7[x]$	1.8 $x^3 - x^2 - 2x + 2$	ใน $\mathbb{Q}[x]$
1.4 $x^2 + \bar{4}$	ใน $\mathbb{Z}_{11}[x]$	1.9 $x^3 - x^2 - 2x + 2$	ใน $\mathbb{Z}[x]$
1.5 $x^3 + \bar{2}x + \bar{3}$	ใน $\mathbb{Z}_5[x]$	1.10 $x^3 - x^2 + x - 1$	ใน $\mathbb{C}[x]$

2. จงยกตัวอย่างฟีลด์อันดับ 49, 81 และ 125

3. จงแสดงว่า $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$

4. จงแสดงว่า $\mathbb{Z}_{11}[x]/\langle x^2+x+\bar{4}\rangle \cong \mathbb{Z}_{12}[x]/\langle x^2+\bar{1}\rangle$

5. จงพิสูจน์ว่า $x^4 + x^3 + x + 1$ ลดทอนได้ใน $F[x]$ เมื่อ F เป็นฟีลด์

6. จงสร้างตารางกรุปการคูณของ $\mathbb{Z}_3[x]/\langle x^2+\bar{1}\rangle$ พร้อมหาตัวผกผันของสมาชิก

7. จงหาตัวผกผันการคูณของ $2x + 1 + \langle x^2+2\rangle$ ใน $\mathbb{R}[x]/\langle x^2+2\rangle$

8. ให้ F เป็นฟีลด์ และ $f(x), g(x) \in F[x]$ โดยที่ $f(x) \neq 0$ หรือ $g(x) \neq 0$ แล้ว **ตัวหารร่วมมาก (greatest common divisor)** ของ $f(x)$ และ $g(x)$ เขียนแทนด้วย gcd$(f(x), g(x))$ คือพหุนาม $d(x)$ ใน $F[x]$ ที่สอดคล้อง 3 เงื่อนไขต่อไปนี้

   (1) $d(x)$ เป็นพหุนามโมนิก

   (2) $d(x) \mid f(x)$ และ $d(x) \mid g(x)$

   (3) ถ้า $c(x) \in F[x]$ ซึ่ง $c(x) \mid f(x)$ และ $c(x) \mid g(x)$ แล้ว $c(x) \mid d(x)$

   จงหาตัวหารร่วมมากของ

   8.1 $x^2 - 1$ และ $x^3 - 1$ ใน $\mathbb{Q}[x]$

   8.2 $x^5 - 1$ และ $x^8 - 1$ ใน $\mathbb{Q}[x]$

   8.3 2 และ $4x - 6$ in $\mathbb{Z}[x]$

   8.4 $2x^2 + 6x + 4$ และ $8x^3 + 18x^2 + 4x$ ใน $\mathbb{Z}[x]$

8.3 ริงพหุนามบนฟีลด์ตรรกยะ

ในหัวข้อนี้จะศึกษาริงพหุนามบนฟีลด์ $\mathbb{Q}$ หรือ $\mathbb{Q}[x]$ ซึ่งสนใจความสัมพันธ์ของพหุนามลดทอนได้หรือลดทอนไม่ได้ใน $\mathbb{Q}[x]$ และ $\mathbb{Z}[x]$

บทนิยาม 8.3.1 ให้ $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ เป็นพหุนามซึ่ง $a_i \in \mathbb{Z}$ ทุก $i \in \{0, 1, ..., n\}$ จะเรียก $f(x)$ ว่า **พหุนามปฐมฐาน** (primitive polynomial) ก็ต่อเมื่อ

$$\text{gcd}(a_0, a_1, ..., a_n) = 1$$

ข้อสังเกต 8.3.2 ให้ $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ เป็นพหุนามซึ่ง $a_i \in \mathbb{Z}$
ถ้า $f(x)$ ไม่เป็นพหุนามปฐมฐาน ก็ต่อเมื่อ gcd$(a_0, a_1, ..., a_n) \neq 1$ หรือมี $a \in \mathbb{Z}$ โดยที่ $a \neq 1$ ซึ่ง

$$f(x) = ag(x) \quad \text{เมื่อ } g(x) \text{ เป็นพหุนามปฐมฐาน}$$

ตัวอย่างเช่น $a =$ gcd$(a_0, a_1, ..., a_n)$ ซึ่ง $a \neq 1$ และ $b_i = \dfrac{a_i}{a} \in \mathbb{Z}$ ทุก $i \in \{0, 1, ..., n\}$ จะได้ว่า

$$f(x) = ab_nx^n + ab_{n-1}x^{n-1} + \cdots + ab_1x + ab_0 = ag(x)$$

เมื่อ $g(x) = b_nx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$ โดยบทแทรก 1.3.15 จะได้ว่า

$$\text{gcd}(b_0, b_1, ..., b_n) = \text{gcd}\left(\frac{a_0}{a}, \frac{a_1}{a}, ..., \frac{a_n}{a}\right) = 1$$

นั่นคือ $g(x)$ เป็นพหุนามปฐมฐาน

ทฤษฎีบท 8.3.3 ให้ $f(x)$ และ $g(x)$ เป็นพหุนามปฐมฐาน แล้ว $f(x)g(x)$ เป็นพหุนามปฐมฐาน

ถ้า $p(x) = x^2$ เป็นพหุนามใน $\mathbb{Q}[x]$ สามารถเขียนเป็น $x^2 = x \cdot x$ ซึ่งเป็นผลคูณของพหุนามใน $\mathbb{Z}[x]$ แต่ถ้า

$$x^2 = 2x \cdot \frac{1}{2}x$$

ไม่ใช่ผลคูณของพหุนามใน $\mathbb{Z}[x]$ ต่อไปจะศึกษาสมบัติการแยกตัวประกอบในลักษณะดังกล่าว

บทตั้ง 8.3.4 บทตั้งของเกาส์ (Gauss' Lemma)
ให้ $f(x) \in \mathbb{Q}[x]$ โดยที่ $f(x)$ เป็นพหุนามปฐมฐาน ถ้า $f(x) = u(x)v(x)$ เมื่อ $u(x), v(x) \in \mathbb{Q}[x]$

$$\text{แล้วจะมี } g(x), h(x) \in \mathbb{Z}[x] \text{ ซึ่ง } f(x) = g(x)h(x)$$

จากบทตั้งของเกาส์สรุปได้ว่า สำหรับพหุนามปฐมฐาน $f(x)$ จะได้ว่า

$$f(x) \text{ ลดทอนไม่ได้ใน } \mathbb{Q}[x] \qquad \text{ก็ต่อเมื่อ} \qquad f(x) \text{ ลดทอนไม่ได้ } \mathbb{Z}[x]$$

ถ้า $f(x)$ ไม่เป็นพหุนามปฐมฐานบทตั้งของเกาส์จะไม่จริงดังตัวอย่างต่อไปนี้

ตัวอย่าง 8.3.5 จงแสดงว่า $4x+2$ ลดทอนได้ใน $\mathbb{Z}[x]$ แต่ลดทอนไม่ได้ $\mathbb{Q}[x]$

บทแทรก 8.3.6 ให้ $f(x) \in \mathbb{Q}[x]$ โดยที่สัมประสิทธิ์ทุกตัวเป็นจำนวนเต็ม
ถ้า $f(x) = u(x)v(x)$ เมื่อ $u(x), v(x) \in \mathbb{Q}[x]$

$$\text{แล้วจะมี } g(x), h(x) \in \mathbb{Z}[x] \text{ ซึ่ง } f(x) = g(x)h(x)$$

บทแทรก 8.3.7 $\mathbb{Z}[x]$ เป็น U.F.D.

ทฤษฎีบท 8.3.8 เกณฑ์การพิจารณาของไอเซนสไตน์ (Eisenstein's Criterion)
ให้ $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Q}[x]$ โดยที่ $a_i \in \mathbb{Z}$ ทุก $i \in \{0, 1, 2, ..., n\}$
มีจำนวนเฉพาะ p ซึ่ง

1. $p \mid a_i$ ทุก $i \in \{0, 1, ..., n-1\}$
2. $p \nmid a_n$ และ $p^2 \nmid a_0$

แล้ว $f(x)$ ลดทอนไม่ได้ใน $\mathbb{Q}[x]$

ตัวอย่าง 8.3.9 จงตรวจสอบว่าพหุนามต่อไปนี้ลดทอนได้หรือไม่ใน $\mathbb{Q}[x]$

1. $x^4 + 10x + 5$

2. $3x^3 + 4x + 2$

3. $x^2 - x - 12$

4. $5x^5 + 9x + 6$

5. $x^7 + 7$

6. $x^7 + 5^3$

7. $(x+1)^4 + 1$

ข้อสังเกต 8.3.10 ถ้า $n \in \mathbb{N}$ และ p เป็นจำนวนเฉพาะ จะได้ว่า $x^n + p$ ลดทอนไม่ได้ใน $\mathbb{Q}[x]$

แบบฝึกหัด 8.3

1. จงตรวจสอบว่าพหุนามต่อไปนี้เป็นพหุนามปฐมฐานหรือไม่

   1.1 $x^3 + 5x^2 - x + 1$

   1.2 $2x^5 + 4x^4 - 2x + 6$

   1.3 $(x^2 + x - 3)(2x^3 - 3x + 1)$

   1.4 $(x - 1)(2x^2 - 3x + 3)(2x - 1)$

2. จงตรวจสอบว่าพหุนามต่อไปนี้ลดทอนได้หรือไม่

   2.1 $x^4 + 6x^3 - 10x + 2$ ใน $\mathbb{Q}[x]$

   2.2 $x^5 - 3x^2 + 6x^3 - 9x + 3$ ใน $\mathbb{Q}[x]$

   2.3 $x^7 + 5$ ใน $\mathbb{Q}[x]$

   2.4 $(x^2 + 1)^2 + 1$ ใน $\mathbb{Q}[x]$

   2.5 $x^3 + x + 1$ ใน $\mathbb{Z}_3[x]$

   2.6 $x^4 + 1$ ใน $\mathbb{Z}_5[x]$

   2.7 $x^4 + 10x^2 + 1$ ใน $\mathbb{Z}[x]$

   2.8 $x^6 + x - 1$ ใน $\mathbb{Q}[x]$

   2.9 $x^4 + 4x + 1$ ใน $\mathbb{Q}[x]$

   2.10 $\dfrac{1}{2}x^3 + 2x - \dfrac{3}{2}$ ใน $\mathbb{Q}[x]$

3. ถ้า $n, m \in \mathbb{N}$ และ p เป็นจำนวนเฉพาะ จงให้เหตุผลว่าทำไม $x^n + p^m$ ลดทอนไม่ได้ใน $\mathbb{Q}[x]$

4. จงพิสูจน์ว่าพหุนามต่อไปนี้ลดทอนไม่ได้ใน $\mathbb{Z}[x]$

   4.1 $x^4 - 4x^3 + 6$

   4.2 $x^6 + 30x^5 - 15x^3 + 6x - 120$

   4.3 $x^4 + 4x^3 + 6x^2 + 2x + 1$

   4.4 $\dfrac{(x+2)^p - 2^p}{p}$ เมื่อ p เป็นจำนวนเฉพาะคี่

5. จงพิสูจน์ว่า $1 + x + x^2 + \cdots + x^p$ ลดทอนไม่ได้ใน $\mathbb{Q}[x]$ เมื่อ p เป็นจำนวนเฉพาะ

6. ให้ $a \in \mathbb{Z}_p$ เมื่อ p เป็นจำนวนเฉพาะ จงพิสูจน์ว่า $x^p + a$ ลดทอนไม่ได้ใน $\mathbb{Z}_p[x]$

7. จงยกตัวอย่างพหุนามระดับขั้น 8 ซึ่งลดทอนได้ใน $\mathbb{Q}[x]$

8. จงแสดงว่า $x^2 - \sqrt{2}$ ลดทอนไม่ได้ใน $\mathbb{Z}[\sqrt{2}][x]$

9. จงตรวจสอบว่า $\mathbb{Q}[x]/\langle x^4 + 2x^2 + 6x + 1\rangle$ เป็นฟีลด์หรือไม่

บรรณานุกรม

กระทรวงศึกษาธิการ. (2555). **เอกสารเสริมความรู้ วิชาคณิตศาสตร์ เรื่องพีชคณิต**. กรุงเทพฯ : บริษัท ไฮเอ็ดพับลิชชิ่ง จำกัด

จิตจวบ เปาอินทร์. (2537). **พีชคณิตนามธรรม**. ภาควิชาคณิตศาสตร์ คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ฉวีวรรณ รัตนประเสริฐ. (2548). **พีชคณิต**. กรุงเทพฯ : มูลนิธิ สอวน.

พัฒนี อุดมกะวานิช. (2559). **หลักคณิตศาสตร์**. กรุงเทพฯ: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

ธนัชยศ จำปาหวาย. (2565). **ทฤษฎีจำนวน**. www.mebmarket.com.

ธนัชยศ จำปาหวาย. (2565). **หลักการคณิตศาสตร์สำหรับครู**. www.mebmarket.com.

อัจฉรา หาญชูวงศ์. (2542). **ทฤษฎีจำนวน**. กรุงเทพฯ : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

Charles C. Pinter. (2016). **A Book of Abstract Algebra**. New York: McGraw-Hill Publishing Company, Inc.

David S. Dummit and Richard M. Foote. (2004). **Abstract Algebra**. Hoboken, NJ : John Wiley & Sons, Inc.

ประวัติผู้เขียน

นายธนัชยศ จำปาหวาย

- ปริญญาเอก วิทยาศาสตร์ดุษฎีบัณฑิต (คณิตศาสาตร์), จุฬาลงกรณ์มหาวิทยาลัย, 2557
  Ph.D. (Mathematics), Chulalongkorn University, 2014
- ปริญญาโท วิทยาศาสตร์มหาบัณฑิต (คณิตศาสาตร์), จุฬาลงกรณ์มหาวิทยาลัย, 2552
  M.Sc. (Mathematics), Chulalongkorn University, 2009
- ปริญญาตรี วิทยาศาสตร์บัณฑิต (คณิตศาสาตร์, เกียรตินิยมอันดับสอง),
  จุฬาลงกรณ์มหาวิทยาลัย, 2549
  B.Sc. (Mathematics, 2nd class honours),Chulalongkorn University, 2006
- ปัจจุบันดำรงตำแหน่งผู้ช่วยศาสตราจารย์ประจำสาขาวิชาคณิตศาสตร์ คณะครุศาสตร์
  มหาวิทยาลัยราชภัฏสวนสุนันทา

Email: thanatyod.ja@ssru.ac.th
Office: 1144
Facebook: www.facebook.com/Jampawai
Block: www.eledu.ssru.ac.th/thanatyod_ja

ผลงานทางวิชาการ

ธนัชยศ จำปาหวาย. (2565). **พีชคณิตนามธรรม**. www.mebmarket.com.

ธนัชยศ จำปาหวาย. (2565). **ทฤษฎีจำนวน**. www.mebmarket.com.

ธนัชยศ จำปาหวาย. (2565). **หลักการคณิตศาสตร์สำหรับครู**. www.mebmarket.com.

ธนัชยศ จำปาหวาย. (2565). **ความน่าจะเป็นและสถิติ**. www.mebmarket.com.

ธนัชยศ จำปาหวาย. (2560). **ความจริงที่ต้องพิสูจน์**. มหาวิทยาลัยราชภัฏสวนสุนันทา.