พีชคณิตนามธรรม Abstract Algebra (กลางภาค)

ผศ.ดร.ธนัชยศ จำปาหวาย

สาขาวิชาคณิตศาสตร์ คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา

เนื้อหา Content

กลางภาค

- บทที่ 1 ความรู้พื้นฐาน
- บทที่ 2 กรุป
- บทที่ 3 กรุปย่อย
- บทที่ 4 กรุปย่อยปกติ

ปลายภาค

- บทที่ 5 สมสัณฐาน
- บทที่ 6 ริง
- บทที่ 7 โดเมนเชิงจำนวนเต็ม
- บทที่ 8 ริงพหุนาม

บทที่ 1 ความรู้พื้นฐาน

1.1 วิวัฒนาการของวิชาพีชคณิตนามธรรม

ภาษาไทย	ภาษาอังกฤษ	ภาษาอาหรับ
พีชคณิต	algebra	al jebr
		ศตวรรษที่ 9
	โอมาร์ เคย์แยม	มูฮัมหมัดแห่งคาริซม์
	(Omar Khayyam)	(Mohammed of Kharizm)

พีชคณิต

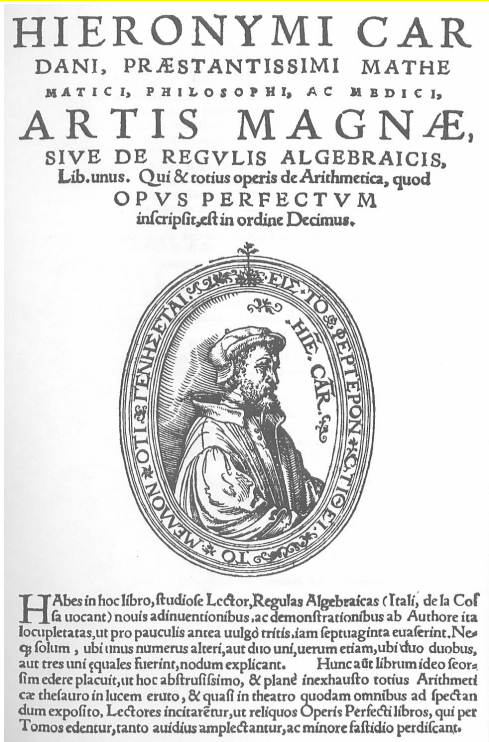
หมายถึงวิทยาการการหาคำตอบของสมการ (the science of sloving equations)

$ax + b = 0$	$ax^2 + bx + c = 0$	$x^3 + ax^2 + bx = c$	$x^4 + ax^3 + bx^2 + cx = d$

กิโรลาโม คาร์แดน (Girolamo Cardan)

Girolamo Cardano 1501

Ars Magna (The Great Art, 1545)



HIERONYMI CAR
DANI, PRÆSTANTISSIMI MATHE
MATICI, PHILOSOPHI, AC MEDICI,
ARTIS MAGNÆ,
SIVE DE REGVLIS ALGEBRAICIS,
Lib. unus. Qui & totius operis de Arithmetica, quod
OPVS PERFECTVM
inscripsit, est in ordine Decimus.

HAbes in hoc libro, studiose Lector, Regulas Algebraicas (Itali, de la Cosa uocant) nouis adinuentionibus, ac demonstrationibus ab Authore ita locupletatas, ut pro pauculis antea uulgo tritis, iam septuaginta euaserint. Ne eq; solum, ubi unus numerus alteri, aut duo uni, uerum etiam, ubi duo duobus, aut tres uni æquales fuerint, nodum explicant. Hunc aũt librum ideo foras sim edere placuit, ut hoc abstrusissimo, & planè inexhausto totius Arithmeticæ thesauro in lucem eruto, & quasi in theatro quodam omnibus ad spectandum exposito, Lectores incitarẽtur, ut reliquos Operis Perfecti libros, qui per Tomos edentur, tanto auidius amplectantur, ac minore fastidio perdiscant.

- ศตวรรษที่ 16 การหาคำตอบของสมการ $x^3 + ax + b = 0$

วิธีคาร์แดน (Cardan's method)

ตัวอย่าง (1.1.1)

จงหาคำตอบของสมการ $x^3 - 27x - 54 = 0$ โดยวิธีคาร์แดน

ตาร์แทกเลีย (Tartaglia)

Niccolò Fontana Tartaglia 1557

- รูปแบบทั่วไปของสมการกำลังสาม

  $x^3 + ax^2 + bx + c = 0$

  ลูโดวิโค เฟอร์รารี (Ludovico Ferrari)

- รูปแบบทั่วไปของสมการกำลังสี่

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

นีลส์ อาเบล (Niels Abel)

Neils Henrik Abel 1802

- ปี 1824
- พิสูจน์ว่าไม่สามารถหาคำตอบในรูปทั่วไปของสมการกำลังที่มากกว่าสี่

เอวาริสต์ กาลัว (Evariste Galois)

Evariste Galois 1811-1832

- ปี 1828 ตีพิมพ์ผลงานเกี่ยวกับ เศษส่วนต่อเนื่อง (continued fraction)
- ปี 1829 หาเงื่อนไขจำเป็นและเพียงพอสำหรับการหาคำตอบของพหุนามดีกรีใด ๆ ซึ่งเป็นรากฐานของ ทฤษฎีกาลัว (Galois Theory) ได้รับการติมพิพ์หลังเขาตายไปแล้วในปี 1846
- เป็นคนแรกที่ใช้คำว่า **กรุป (Group)** ในฐานะศัพท์เฉพาะทาง

สัญลักษณ์เกี่ยวกับเซต

$\mathbb{C}$	เซตของจำนวนเชิงซ้อน	$\mathbb{R}^+$	เซตของจำนวนจริงบวก
$\mathbb{R}$	เซตของจำนวนจริง	$\mathbb{R}^-$	เซตของจำนวนจริงลบ
$\mathbb{Q}$	เซตของจำนวนตรรกยะ	$\mathbb{Q}^+$	เซตของจำนวนตรรกยะบวก
$\mathbb{Q}^c$	เซตของจำนวนอตรรกยะ	$\mathbb{Q}^-$	เซตของจำนวนตรรกยะลบ
$\mathbb{Z}$	เซตของจำนวนเต็ม	$\mathbb{Z}^+$	เซตของจำนวนเต็มบวก
$\mathbb{N}$	แทนเซตของจำนวนนับ	$\mathbb{Z}^-$	เซตของจำนวนเต็มลบ
		$\mathbb{C}^*$	เซตของจำนวนเชิงซ้อนที่ไม่ใช่ศูนย์
		$\mathbb{R}^*$	เซตของจำนวนจริงที่ไม่ใช่ศูนย์
		$\mathbb{Q}^*$	เซตของจำนวนตรรกยะที่ไม่ใช่ศูนย์
		$\mathbb{Z}^*$	เซตของจำนวนเต็มที่ไม่ใช่ศูนย์

ช่วงบนจำนวนจริง

$\{x \in \mathbb{R} : a < x < b\}$ 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 $(-\infty, b]$

การดำเนินการบนเซต

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

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

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

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

ในกรณีที่ทราบจำนวนสมาชิกของเซต A เรียกว่า **เซตจำกัด (finite set)** เขียน

$|A|$ แทนจำนวนสมาชิกของ A

และเซตที่ไม่ใช่เซตจำกัดเรียกว่า **เซตอนันต์ (infinite set)**

1.2 พีชคณิตกับการจัดการเรียนรู้

สาระที่ 1: จำนวนและพีชคณิต

เรียนรู้เกี่ยวกับ ระบบจำนวนจริง สมบัติเกี่ยวกับจำนวนจริง อัตราส่วน ร้อยละ การประมาณค่า การแก้ปัญหาเกี่ยวกับจำนวน การใช้จำนวนในชีวิตจริง แบบรูปความสัมพันธ์ ฟังก์ชัน เซต ตรรกศาสตร์ นิพจน์ เอกนาม พหุนาม สมการ ระบบสมการ อสมการ กราฟ ดอกเบี้ยและมูลค่าของเงิน ลำดับและอนุกรม และการนำความรู้เกี่ยวกับจำนวนและพีชคณิตไปใช้ในสถานการณ์ต่าง ๆ

สาระและมาตรฐานการเรียนรู้

1. **มาตรฐาน ค 1.1** เข้าใจความหลากหลายของการแสดงจำนวน ระบบจำนวน การดำเนินการของจำนวน ผลที่เกิดขึ้นจากการดำเนินการ สมบัติของการดำเนินการ และนำไปใช้
2. **มาตรฐาน ค 1.2** เข้าใจและวิเคราะห์แบบรูป ความสัมพันธ์ ฟังก์ชัน ลำดับและอนุกรม และนำไปใช้
3. **มาตรฐาน ค 1.3** ใช้นิพจน์ สมการ และอสมการ อธิบายความสัมพันธ์หรือช่วยแก้ปัญหาที่กำหนดให้

1.3 อุปนัยเชิงคณิตศาสตร์

หลักการจัดอันดับดี (Well Ordering Principle : WOP)

ให้ $S \subseteq \mathbb{N}$ และ $S \neq \varnothing$ จะได้ว่า S มีสมาชิกตัวเล็กสุด หรือ

มี $m \in S$ ซึ่ง $m \leq s$ ทุก ๆ $s \in S$

หลักการอาร์คิมีดีส (Archimedean Principle : AP)

ทฤษฎีบท (1.3.1)

สำหรับจำนวนเต็มบวก a และ b ใด ๆ จะมีจำนวนเต็มบวก n ซึ่ง $na \geq b$

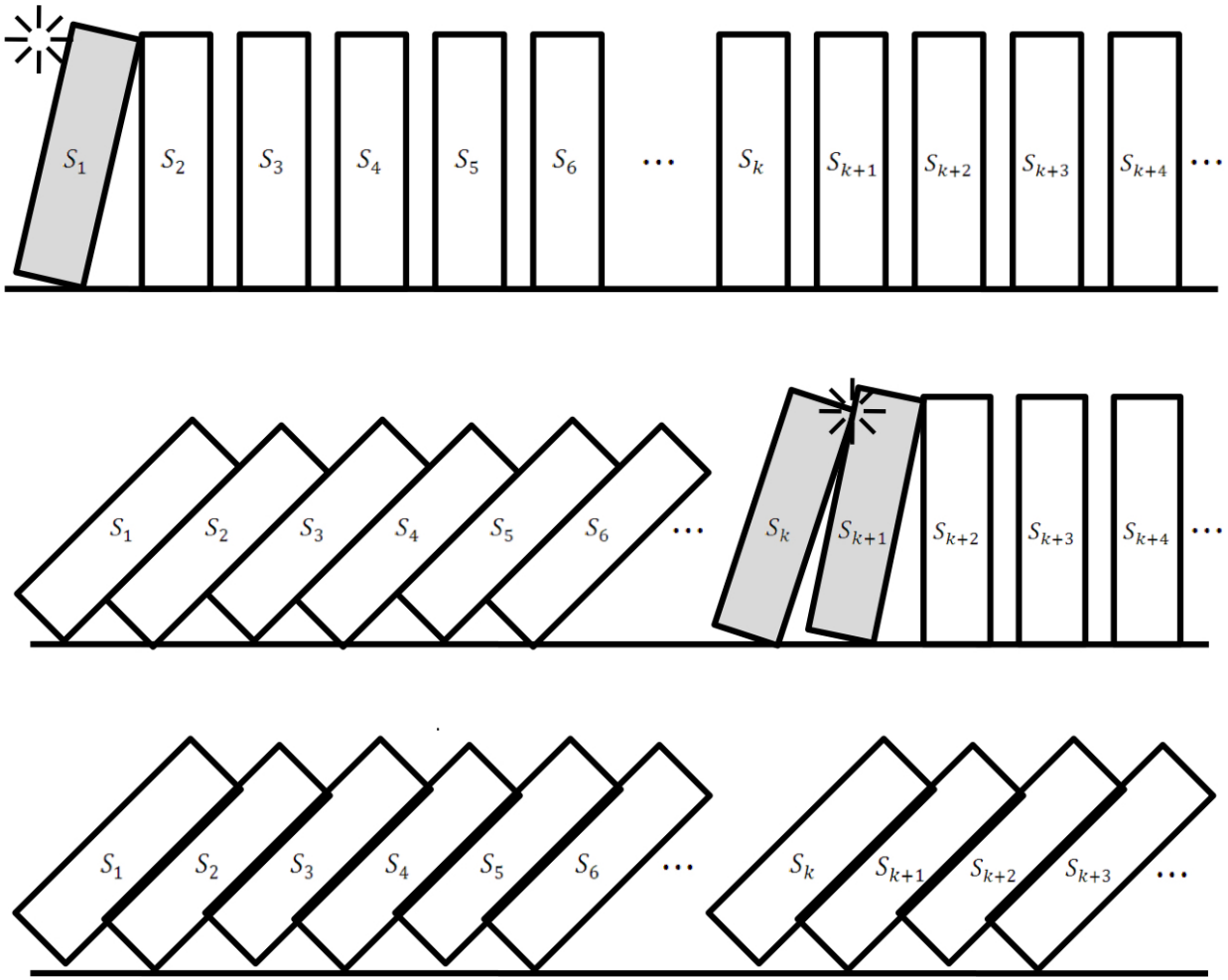
ทฤษฎีบท (1.3.2)

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

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

แล้วจะได้ว่า $S = \mathbb{N}$

หลักโดมิโน


S_1 S_2 S_3 S_4 S_5 S_6 ⋯ S_k S_{k+1} S_{k+2} S_{k+3} S_{k+4} ⋯
S_1 S_2 S_3 S_4 S_5 S_6 ⋯ S_k S_{k+1} S_{k+2} S_{k+3} S_{k+4} ⋯
S_1 S_2 S_3 S_4 S_5 S_6 ⋯ S_k S_{k+1} S_{k+2} S_{k+3} ⋯

การพิสูจน์โดยหลักอุปนัยเชิงคณิตศาสตร์

อุปนัยเชิงคณิตศาสตร์

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

การพิสูจน์ทำได้ 2 ขั้นตอนดังนี้

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

แล้วสรุปได้ว่า $P(n)$ เป็นจริงสำหรับทุก ๆ จำนวนนับ n

ตัวอย่าง (1.3.3)

จงพิสูจน์ข้อความต่อไปนี้โดยหลักอุปนัยเชิงคณิตศาสตร์

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

อุปนัยเชิงคณิตศาสตร์ที่ขั้นฐานเริ่มต้นที่ $n_0 \in \mathbb{Z}$

อุปนัยเชิงคณิตศาสตร์

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

การพิสูจน์ทำได้ 2 ขั้นตอนดังนี้

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 (1.3.4)

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

อุปนัยเชิงคณิตศาสตร์แบบเข้ม Strong Mathematical Induction

อุปนัยเชิงคณิตศาสตร์แบบเข้ม

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

การพิสูจน์ทำได้ 2 ขั้นตอนดังนี้

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 (1.3.5)

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

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

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

1.4 ทฤษฎีจำนวนเบื้องต้น

บทนิยาม (1.4.1)

ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ จะกล่าวว่า a **หาร** b **ลงตัว** เขียนแทนด้วยสัญลักษณ์ $a \mid b$ 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 (1.4.2)

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 (1.4.3)

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 (1.4.4)

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 (1.4.5)

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 (1.4.6)

ให้ a, b และ c เป็นจำนวนเต็ม

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

ขั้นตอนวิธีการหาร (The Division Algorithm : DA)

ทฤษฎีบท (1.4.7)

ให้ a และ b เป็นจำนวนเต็ม โดยที่ $a \neq 0$ แล้วมีจำนวนเต็ม q และ r เพียงคู่เดียวที่ทำให้

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

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

ตัวหารร่วมมาก (Greatest Common Divisior : G.C.D)

บทนิยาม (1.4.8)

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)**

สมบัติเชิงเส้นของตัวหารร่วมมาก

ทฤษฎีบท (1.4.9)

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

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

ทฤษฎีบท (1.4.10)

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

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

ทฤษฎีบท (1.4.11)

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

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

บทแทรก (1.4.12)

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

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

Theorem (1.4.13)

ให้ a, b, c *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* $(ab) \mid c$

ตัวคูณร่วมน้อย (Least Common Multiple : L.C.M)

บทนิยาม (1.4.14)

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 $m \leq c$

ความสัมพันธ์ของ G.C.D. และ L.C.M

ทฤษฎีบท (1.4.15)

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

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

จำนวนเฉพาะ (Prime)

บทนิยาม (1.4.16)

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

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

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

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

ข้อสังเกตที่ได้จากบทนิยามของจำนวนเฉพาะ

ข้อสังเกต (1.4.17)

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 $a = bc$

ทฤษฎีบท (1.4.18)

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

ทฤษฎีบท (1.4.19)

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

$$\text{ถ้า} \quad p \mid ab \quad \text{แล้ว} \quad p \mid a \quad \text{หรือ} \quad p \mid b$$

ทฤษฎีบท (1.4.20)

ให้ p เป็นจำนวนเฉพาะ และ $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ เมื่อ $n \in \mathbb{N}$ จะได้ว่า

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

ทฤษฎีบทหลักมูลเลขคณิต (The Fundamental Theorem of Arithmematic)

ทฤษฎีบท (1.4.21)

จำนวนเต็มที่มากกว่า 1 สามารถเขียนในรูปผลคูณของจำนวนเฉพาะได้ และถ้าไม่คิดลำดับเป็นสำคัญแล้วการเขียนนี้ทำได้เพียงวิธีเดียวเท่านั้น หรือกล่าวได้ว่าจำนวนเต็ม $n > 1$ 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*

ตัวอย่างจำนวนที่เขียนในรูปแบบบัญญัติ

36

1225

150^2

4725

ฟังก์ชันฟี (Phi Function)

บทนิยาม (1.4.22)

ให้ $n \in \mathbb{N}$ เรียก ϕ ว่า**ฟังก์ชันฟี (phi function)** นิยามโดย

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

ข้อสังเกต (1.4.23)

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

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

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

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

ตัวอย่างการหาค่าฟังก์ชันฟี

$\phi(100)$

$\phi(360)$

$\phi(300)$

$\phi(133^2 - 130^2)$

ฟังก์ชันเทา (Tau Function)

บทนิยาม (1.4.24)

ให้ $n \in \mathbb{N}$ เรียก τ ว่า **ฟังก์ชันเทา (tau function)** นิยามโดย

$$\tau(n) = \text{จำนวนของตัวหารที่เป็นบวกของ } n$$

ข้อสังเกต (1.4.25)

$\tau(1) = 1$ และ $\tau(p) = 2$ เมื่อ p เป็นจำนวนเฉพาะ

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

$$\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$$

ตัวอย่างการหาค่าฟังก์ชันเทา

$\tau(72)$

$\tau(150^2)$

$\tau(100)$

$\tau(10!)$

1.5 ความสัมพันธ์และฟังก์ชัน

บทนิยาม (1.5.1)

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

ตัวอย่าง (1.5.2)

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

ความสัมพันธ์ (Relation)

บทนิยาม (1.5.4)

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

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

ในกรณีที่ R เป็นความสัมพันธ์จาก A ไป A จะเรียก r ว่าความสัมพันธ์ใน A

ความสัมพันธ์สมมูล (Equivalence Relation)

บทนิยาม (1.5.5)

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

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

ชั้นสมมูล (Eequivalence Class)

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

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

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

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

ตัวอย่าง (1.5.6)

ให้ $x, y \in \mathbb{Z}$ กำหนดให้

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

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

$\mathbb{Z}$ มอดุโล R หรือ $\mathbb{Z}/R$

$$[-3] = \{x \in \mathbb{Z} : 3 \mid (-3 - x)\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\} = \{3k : k \in \mathbb{Z}\}$$

$$[-2] = \{x \in \mathbb{Z} : 3 \mid (-2 - x)\} = \{\ldots, -8, -5, -2, 1, 4, 7, \ldots\} = \{3k + 1 : k \in \mathbb{Z}\}$$

$$[-1] = \{x \in \mathbb{Z} : 3 \mid (-1 - x)\} = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\} = \{3k + 2 : k \in \mathbb{Z}\}$$

$$[0] = \{x \in \mathbb{Z} : 3 \mid (0 - x)\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\} = \{3k : k \in \mathbb{Z}\}$$

$$[1] = \{x \in \mathbb{Z} : 3 \mid (1 - x)\} = \{\ldots, -8, -5, -2, 1, 4, 7, \ldots\} = \{3k + 1 : k \in \mathbb{Z}\}$$

$$[2] = \{x \in \mathbb{Z} : 3 \mid (2 - x)\} = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\} = \{3k + 2 : k \in \mathbb{Z}\}$$

$$[3] = \{x \in \mathbb{Z} : 3 \mid (0 - 3)\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\} = \{3k : k \in \mathbb{Z}\}$$

จะสังเกตเห็นว่า $[0] = [3k]$, $[1] = [3k + 1]$ และ $[2] = [3k + 2]$ ทุกจำนวนเต็ม k ดังนั้น

$$\mathbb{Z}/R = \{[0], [1], [2]\}$$

สมบัติชั้นสมมูล

ทฤษฎีบท (1.5.7)

ให้ R เป็นความสัมพันธ์สมมูลในเซต $A \neq \varnothing$ แล้ว

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

ผลแบ่งกั้น (Partition)

บทนิยาม (1.5.8)

ให้ A เป็นเซตที่ไม่ใช่เซตว่าง และ Λ เป็นเซตดรรชนี จะกล่าวว่า

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

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

(1) $A = \bigcup_{\alpha\in\Lambda} A_\alpha := \{x : x \in A_\alpha \text{ สำหรับบาง } \alpha \in \Lambda\}$

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

ทฤษฎีบท (1.5.9)

ให้ A เป็นเซตไม่ใช่เซตว่าง และ R เป็นความสัมพันธ์สมมูลใน A แล้ว A/R เป็นผลแบ่งกั้นหนึ่งของ A

จำนวนเต็มมอดุโล n

ให้ $\sim$ เป็นความสัมพันธ์ใน $\mathbb{Z}$ นิยามโดย

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

เมื่อ n เป็นจำนวนเต็มบวก จะได้ว่า $\sim$ เป็นความสัมพันธ์สมมูลใน $\mathbb{Z}$
ชั้นสมมูลของ $a \in \mathbb{Z}$ มอดุโล $\sim$ เขียนแทนด้วย $\bar{a}$ นั่นคือ

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

ข้อสังเกต (1.5.10)

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

เซตของจำนวนเต็มมอดุโล n

ชั้นสมมูลที่แตกต่างกันมีทั้งหมด n เซตดังนี้

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

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

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

ตัวอย่างเซตของจำนวนเต็มมอดุโล n

เซตของจำนวนเต็มมอดุโล n	แจกแจงสมาชิก
$\mathbb{Z}_1$	
$\mathbb{Z}_2$	
$\mathbb{Z}_3$	
$\mathbb{Z}_4$	
$\mathbb{Z}_5$	
$\mathbb{Z}_6$	
$\mathbb{Z}_7$	
$\mathbb{Z}_{11}$	

ตัวอย่าง (1.5.11)

จงเขียนสมาชิกต่อไปนี้ให้อยู่ในรูปสมาชิกในตาราง 1.2

1. $\overline{1265}$ และ $\overline{78961}$ ใน $\mathbb{Z}_3$
2. $\overline{2564}$ และ $\overline{20261}$ ใน $\mathbb{Z}_4$
3. $\overline{11698}$ และ $\overline{5523}$ ใน $\mathbb{Z}_9$
4. $\overline{11236}$ และ $\overline{66337}$ ใน $\mathbb{Z}_{11}$

ตัวอย่าง (1.5.12)

จงเขียนสมาชิกใน $\mathbb{Z}_7$ ต่อไปนี้ให้อยู่ในรูปสมาชิกในตาราง 1.2

1. $\overline{121415}$
2. $\overline{1234321}$
3. $\overline{11223344}$

ฟังก์ชัน (Function)

บทนิยาม (1.5.13)

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

$$\text{แต่ละ } (x_1, y_1) \text{ และ } (x_2, y_2) \text{ ใน } f \text{ ถ้า } x_1 = x_2 \text{ แล้ว } y_1 = y_2$$

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

ฟังก์ชันจาก A ไป B

บทนิยาม (1.5.14)

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

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

เมื่อ $\mathrm{Dom}(f) = \{x \in A : (x, y) \in f\}$ เรียกว่า **โดเมน (domain)** ของ f

และ $\mathrm{Ran}(f) = \{y \in A : (x, y) \in f\}$ เรียกว่า **เรนจ์ (range)** ของ f

ฟังก์ชันหนึ่งต่อหนึ่งและฟังก์ชันทั่วถึง

บทนิยาม (1.5.15)

กำหนดให้ $f : A \to B$ จะกล่าวว่า

1. f เป็น**ฟังก์ชันหนึ่งต่อหนึ่ง (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 (surjection)** ก็ต่อเมื่อ $\text{Ran}(f) = B$
3. f เป็น**ฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึง (bijection)** ก็ต่อเมื่อ f เป็นฟังก์ชันหนึ่งต่อหนึ่งและเป็นฟังก์ชันทั่วถึง

ข้อสังเกต (1.5.16)

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

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

ตัวอย่างการเขียนฟังก์ชันแทนด้วยแผนภาพ

ตัวอย่าง (1.5.17)

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

ฟังก์ชันประกอบ (Composite Function)

บทนิยาม (1.5.18)

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 (1.5.19)

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. $f \circ f$

ฟังก์ชันผกผันได้ (Invertible Function)

บทนิยาม (1.5.20)

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 (1.5.21)

ให้ $f : A \to B$ *แล้วจะได้ว่า*

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

ทฤษฎีบท (1.5.22)

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

ตัวอย่าง (1.5.23)

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

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

จงหาฟังก์ชันต่อไปนี้

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

ทฤษฎีบท (1.5.24)

ให้ $f : A \to B$ *แล้ว*

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

ทฤษฎีบท (1.5.25)

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

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

1.6 การดำเนินการทวิภาค

บทนิยาม (1.6.1)

ให้ G เป็นเซตที่ไม่ใช่เซตว่าง แล้ว $*$ เป็น **การดำเนินการทวิภาค (binary operation)** บน G ก็ต่อเมื่อ

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

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

ข้อสังเกต

ถ้า $*$ เป็นการดำเนินการทวิภาคบน G แล้ว

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

ตัวอย่าง

ต่อไปนี้เป็นตัวอย่างการดำเนินการทวิภาคที่คุ้นเคย เช่น

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

ตัวอย่าง

จงตรวจสอบว่า $*$ เป็นการดำเนินการทวิภาคหรือไม่

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

ตารางเคย์เลย์ (Cayley 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	$c*a$	$c*b$	$c*c$

ตัวอย่าง

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 $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

สมบัติการปิด (closure property)

บทนิยาม

ให้ $*$ เป็นการดำเนินการทวิภาคบนเซต G และให้ $A \subseteq G$ และ $A \neq \varnothing$ ถ้า

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

แล้วจะกล่าวว่า A มี**สมบัติการปิด (closure property)** ภายใต้ $*$ หรือ $*$ มีสมบัติการปิดบน A

ตัวอย่าง

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

1. เซตของจำนวนคู่ $\mathbb{E}$
2. เซตของจำนวนคี่ $\mathbb{O}$

สมบัติการสลับที่ (commutative property)

บทนิยาม

ให้ $*$ เป็นการดำเนินการทวิภาคบนเซต G ถ้า

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

จะกล่าวว่า G มี**สมบัติการสลับที่ (commutative property)** ภายใต้ $*$ หรือ $*$ มีสมบัติการสลับที่บน G

ตัวอย่าง

พิจารณาการดำเนินทวิภาคต่อไปนี้

1. กำหนดให้ $a * b = a + b + 5$ เมื่อ $a, b \in \mathbb{N}$
2. กำหนดให้ $a * b = a^2 + ab$ เมื่อ $a, b \in \mathbb{Z}$

สมบัติการเปลี่ยนหมู่ (associative property)

บทนิยาม

ให้ $*$ เป็นการดำเนินการทวิภาคบนเซต G ถ้า

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

แล้วจะกล่าวว่า G มี**สมบัติการเปลี่ยนหมู่ (associative property)** ที่ภายใต้ $*$ หรือ $*$ มีสมบัติการเปลี่ยนหมู่บน G

ตัวอย่าง

จงตรวจสอบสมบัติการเปลี่ยนหมู่ของการดำเนินทวิภาคต่อไปนี้

1. กำหนดให้ $a*b = a+b+1$ เมื่อ $a,b \in \mathbb{N}$
2. กำหนดให้ $a*b = a+2b$ เมื่อ $a,b \in \mathbb{Z}$

เอกลักษณ์ (identity)

บทนิยาม

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

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

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

ตัวอย่าง

จงหาเอกลักษณ์ (ถ้ามี) ของการดำเนินการบนเซตในแต่ละข้อต่อไปนี้

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

ถ้า G มีเอกลักษณ์ภายใต้การดำเนินการ $*$ จะมีได้เพียงตัวเดียวเท่านั้น

ตัวผกผัน (inverse)

บทนิยาม

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

ตัวอย่าง

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

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

ทฤษฎีบท

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*

ตัวอย่าง

จงหาตัวผกผันสำหรับการบวกและการคูณของแต่ละสมาชิกใน $\mathbb{Z}_5$

บทที่ 2 กรุป

2.1 นิยามและตัวอย่างของกรุป

บทนิยาม

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

1. **สมบัติการเปลี่ยนหมู่** กล่าวคือ $a*(b*c)=(a*b)*c$ สำหรับทุก ๆ $a,b,c\in G$
2. **การมีเอกลักษณ์** กล่าวคือ มี $e\in G$ ซึ่ง $a*e=a=e*a$ 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

ถ้ากรุป $(G, *)$ 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

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)**

คู่อันดับ	สมบัติ การเปลี่ยนหมู่	เอกลักษณ์	การมี ตัวผกผัน	ชนิด
$(\mathbb{Z}, +)$	✓	0	✓	กรุป
$(\mathbb{Q}, +)$	✓	0	✓	กรุป
$(\mathbb{R}, +)$	✓	0	✓	กรุป
$(\mathbb{C}, +)$	✓	0	✓	กรุป
$(\mathbb{Z}^+, +)$	✓	ไม่มี	×	กึ่งกรุป
$(\mathbb{Q}^+, +)$	✓	ไม่มี	×	กึ่งกรุป
$(\mathbb{R}^+, +)$	✓	ไม่มี	×	กึ่งกรุป

คู่อันดับ	สมบัติการเปลี่ยนหมู่	เอกลักษณ์	การมีตัวผกผัน	ชนิด
$(\mathbb{Z}, \cdot)$	✓	1	×	โมนอยด์
$(\mathbb{Q}, \cdot)$	✓	1	×	โมนอยด์
$(\mathbb{R}, \cdot)$	✓	1	×	โมนอยด์
$(\mathbb{C}, \cdot)$	✓	1	×	โมนอยด์
$(\mathbb{Z}^+, \cdot)$	✓	1	×	โมนอยด์
$(\mathbb{Q}^+, \cdot)$	✓	1	✓	กรุป
$(\mathbb{R}^+, \cdot)$	✓	1	✓	กรุป
$(\mathbb{Z}^*, \cdot)$	✓	1	×	โมนอยด์
$(\mathbb{Q}^*, \cdot)$	✓	1	✓	กรุป
$(\mathbb{R}^*, \cdot)$	✓	1	✓	กรุป
$(\mathbb{C}^*, \cdot)$	✓	1	✓	กรุป

ตัวอย่าง

กำหนดให้

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

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

ตัวอย่าง

กำหนดให้

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

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

กรุปไคลน์โฟว์ (Klein 4-group)

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

กรุปควอเทอร์เนียน (Quaternion Group)

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 $(-1) * (-1) = 1$, $i * i = j * j = k * k = -1$, $i * j = k$, $j * k = i$, $k * i = j$, $j * i = -k$, $k * j = -i$ และ $i * k = -j$ แล้ว $(Q_8, *)$ เป็นกรุป ซึ่งเรียกว่า **กรุปควอเทอร์เนียน (Quaternion Group)** และเห็นได้ว่า Q_8 ไม่เป็นอาบีเลียนกรุป

กรุปของจำนวนเต็มมอดุโล *n*

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

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

ทฤษฎีบท

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

ทฤษฎีบท

$\mathbb{Z}_n$ *มีสมบัติการสลับที่และสมบัติการเปลี่ยนหมู่ภายใต้การคูณ*
และมี $\bar{1}$ *เป็นเอกลักษณ์การคูณ*

ทฤษฎีบท

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

ทฤษฎีบท

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

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

บทแทรก

กำหนดให้

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

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

กรุปของเมทริกซ์

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

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

เป็นเมทริกซ์ขนาด 2×4 เนื่องจากมี 2 แถว และ 4 หลัก หรือกล่าวย่อ ๆ ว่า เมทริกซ์ 2×4 จะเรียก 3 ที่อยู่แถวที่ 1 หลักที่ 2 ว่า**สมาชิก (element)** ของเมทริกซ์

รูปแบบทั่วไปของเมทริกซ์ขนาด $m \times n$ หรือ เมทริกซ์ $m \times n$ 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} คือสมาชิกของเมทริกซ์ที่อยู่แถวที่ i หลักที่ j และในกรณีที่จำนวนแถวเท่ากับจำนวนหลัก เรียกว่า **เมทริกซ์จตุรัส (square matrix)**

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

บทนิยาม

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. $cA = [ca_{ij}]$

ทฤษฎีบท

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

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

บทนิยาม

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

ทฤษฎีบท

ให้ $n \in \mathbb{N}$ *แล้ว* $(GL_n(\mathbb{R}), \cdot)$ *เป็นกรุป โดยที่*

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

กรุปของฟังก์ชัน

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

$$S_A = \{ f : A \to A \ : \ f \text{ เป็นฟังก์ชันหนึ่งต่อหนึ่งทั่วถึง } \}$$

ตัวอย่าง

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

2.2 สมบัติกรุปเบื้องต้น

ทฤษฎีบท

ให้ G เป็นกรุป จะได้ว่า

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

ทฤษฎีบท

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

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

ทฤษฎีบท

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* $a = b$

ทฤษฎีบท

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

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

อันดับของสมาชิกกรุป

บทนิยาม

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 $\circ(a)$ หรือเรียกว่า a มี**อันดับจำกัด (finite order)** ในกรณีที่ไม่มีจำนวนเต็มบวกที่สอดคล้องเงื่อนไขดังกล่าวให้เรียก a ว่ามี**อันดับอนันต์ (infinite order)** เขียนแทนด้วย $\circ(a) = \infty$

ข้อสังเกต

ให้ a มีอันดับจำกัด จากบทนิยามของอันดับจะได้ว่า

1. $\circ(a) = 1$ ก็ต่อเมื่อ $a = e$
2. ถ้า $a^m = e$ แล้ว $\circ(a) \leq m$
3. $\circ(a) = n$ ก็ต่อเมื่อ ทุก ๆ $k \in \mathbb{N}$ ซึ่ง $a^k = e$ จะได้ว่า $n \leq k$
4. จากบทนิยาม 0.96 อันดับของ a คือจำนวนเต็มบวก n น้อยสุดที่ทำให้ $a^n = e$

ตัวอย่าง

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

ตัวอย่าง

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

ตัวอย่าง

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

1. i และ $-i$
2. $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$
3. $\frac{1}{2} - \frac{\sqrt{3}}{2}i$

ทฤษฎีบท

ให้ a เป็นสมาชิกของกรุป G จะได้ว่า a และตัวผกผันของ a มีอันดับเดียวกัน

ตัวอย่าง

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

ตัวอย่าง

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

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

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

2.3 ผลคูณตรงของกรุป (direct product of groups)

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

$$(a, b) * (c, d) = (a \diamond c, b \circledast d) \tag{1}$$

ทฤษฎีบท

ให้ $(G_1, \diamond)$ และ $(G_2, \circledast)$ เป็นกรุป ถ้านิยามการดำเนินการ $*$ ดังสมการ (1) แล้ว

$(G_1 \times G_2, *)$ เป็นกรุป และเรียก $G_1 \times G_2$ ว่า ***ผลคูณตรงของกรุป (direct product of groups)***

ข้อสังเกต

1. (e_1, e_2) เป็นเอกลักษณ์ของ $G_1 \times G_2$ เมื่อ e_1 และ e_2 เป็นเอกลักษณ์ของ G_1 และ G_2
2. (a^{-1}, b^{-1}) เป็นตัวผกผันของ $(a, b) \in G_1 \times G_2$ เมื่อ a^{-1} และ b^{-1} เป็นตัวผกผันของ a และ b ตามลำดับ

ตัวอย่าง

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

ทฤษฎีบท

ให้ G_1 *และ* G_2 *เป็นกรุป โดยที่* $a \in G_1$ *และ* $b \in G_2$ *มีอันดับจำกัด*

จะได้ว่า $(a, b) \in G_1 \times G_2$ *มีอันดับจำกัด และ*

$$\circ((a, b)) = \ell cm(\circ(a), \circ(b))$$

ตัวอย่าง

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

2.4 กรุปการเรียงสับเปลี่ยน (permutation group)

บทนิยาม

ให้ A เป็นเซตจำกัดที่ไม่ใช่เซตว่าง กำหนดให้

$$S_A = \{\sigma : A \to A : \sigma \text{ เป็นฟังก์ชันหนึ่งต่อหนึ่งทั่วถึง } \}$$

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

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

เอกลักษณ์ของ S_n เขียนแทนด้วย (1) หมายถึง

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

ตัวอย่าง S_n เมื่อ $n = 1, 2, 3$

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

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

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

บทนิยาม

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

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

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

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

ตัวอย่าง

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

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

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

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

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

ตัวอย่าง

จงเขียนวัฏจักรต่อไปนี้ในรูปการเรียงสับเปลี่ยน

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

จงเขียนวัฏจักรต่อไปนี้ในรูปการเรียงสับเปลี่ยน

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

วัฏจักรไม่มีส่วนร่วม (disjoint cycle)

บทนิยาม

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

ข้อสังเกต

ถ้า α และ β เป็นวัฏจักรต่างสมาชิก แล้ว

$$\alpha^k \text{ และ } \beta^d \text{ เป็นวัฏจักรต่างสมาชิก ทุก ๆ } k, d \in \mathbb{Z}$$

ตัวอย่าง

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

ทฤษฎีบท

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

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

ทฤษฎีบท

ถ้า $\alpha, \beta \in S_n$ เป็นวัฏจักรไม่มีส่วนร่วม และ $k \in \mathbb{N}$ จะได้ว่า

$$(\alpha\beta)^k = \alpha^k\beta^k$$

ตัวอย่าง

จงหาอันดับของสมาชิกต่อไปนี้

1. $(1\,2) \in S_2$
2. $(1\,2\,3) \in S_3$

ทฤษฎีบท

ถ้าวัฏจักร α มีความยาว m แล้วจะได้ว่า $\circ(\alpha) = m$

ตัวอย่าง

จงหาอันดับของสมาชิกต่อไปนี้ S_5

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

ทฤษฎีบท

ให้ α และ β เป็นวัฏจักรไม่มีส่วนร่วมกัน โดยแต่ละวัฏจักรมีความยาว m และ k ตามลำดับ แล้ว

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

ตัวอย่าง

จงหาอันดับของสมาชิกต่อไปนี้ใน S_6

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

บทที่ 3 กรุปย่อย

3.1 นิยามและตัวอย่างของกรุปย่อย

บทนิยาม

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

ข้อสังเกต

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

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

ตัวอย่างกรุปย่อยภายใต้การบวก

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

ตัวอย่างกรุปย่อยภายใต้การคูณ

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

เมื่อกล่าวถึงกรุป $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ให้หมายถึงกรุปของเซตเหล่านั้นกับการบวก และเมื่อกล่าวถึงกรุป $\mathbb{Q}^+, \mathbb{R}^+, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ ให้หมายถึงกรุปของเซตเหล่านั้นกับการคูณ เมื่อกล่าวถึงกรุปของ $\mathbb{Z}_n$ จะหมายถึงกรุปของเซตดังกล่าวกับการบวก และ $\mathbb{Z}_p^*$, $\mathbb{Z}_n^\times$ จะหมายถึงกรุปของเซตดังกล่าวกับการคูณ เมื่อ p เป็นจำนวนเฉพาะ และ n เป็นจำนวนนับ

ตัวอย่าง

จงหากรุปย่อยทั้งหมดของ $\mathbb{Z}_3$

ตัวอย่าง

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

จงหากรุปย่อยทั้งหมดของ S_2

ตัวอย่าง

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

เกณฑ์การพิจารณากรุปย่อย (Subgroup Criterion)

ทฤษฎีบท

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 จะได้ว่ากรุปย่อย H มีเอกลักษณ์ตัวเดียวกับ G และสรุปการตรวจสอบว่า H กรุปย่อยด้วยสมบัติ 3 ข้อต่อไปนี้

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

ตัวอย่าง

จงหากรุปย่อยทั้งหมดของ $\mathbb{Z}_4$

ตัวอย่าง

จงหากรุปย่อยทั้งหมดของ $\mathbb{Z}_5^*$

ทฤษฎีบท

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

ตัวอย่าง

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

ให้ G เป็นกรุป ถ้า H และ K เป็นกรุปย่อยของ G แล้ว

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

ทฤษฎีบท

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

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

บทนิยาม

ให้ G เป็นกรุป และ S เป็นเซตย่อยของ G ที่ไม่ใช่เซตว่าง และให้ $\{H_\alpha\}_{\alpha\in\Lambda}$ เป็นเซตของกรุปย่อยของ G เมื่อ Λ เป็นเซตดรรชนี โดยที่ $S \subseteq H_\alpha$ ทุก ๆ $\alpha \in \Lambda$ หรือจะกล่าวว่า H_α เป็นกรุปย่อยของ G ที่บรรจุ S 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 $\langle a_1, a_2, ..., a_k\rangle$ ฉะนั้น $\langle a\rangle = \langle\{a\}\rangle$

ตัวอย่าง

จงแจกแจงสมาชิกของเซตต่อไปนี้ 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. $\langle \bar{2}, \bar{4} \rangle$

ทฤษฎีบท

ให้ S และ T เป็นเซตย่อยที่ไม่ใช่เซตว่างของกรุป G จะได้ว่า

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

Theorem

ให้ S เป็นเซตย่อยที่ไม่ใช่เซตว่างของกรุป G แล้ว

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

บทแทรก

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

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

ทฤษฎีบท

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

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

บทแทรก

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

ให้ K_4 เป็นกรุปไคลน์โฟว์ ถ้า a และ b เป็นสมาชิกที่ไม่ใช่เอกลักษณ์ของ K_4

จงแสดงว่า

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

ทฤษฎีบท

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*

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

ข้อสังเกต

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

3.2 กรุปวัฏจักร

บทนิยาม

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

ข้อสังเกต

ตัวก่อกำเนิดของกรุปวัฏจักรอาจมีมากกว่าหนึ่งตัว

ตัวอย่าง

จงตรวจสอบว่ากรุปต่อไปนี้เป็นกรุปวัฏจักรหรือไม่

1. $\mathbb{Z}_3$
2. $\mathbb{Z}_6$
3. $\mathbb{Z}_5^*$
4. $\mathbb{Z}_8^\times$

ทฤษฎีบท

กรุปวัฏจักรเป็นกรุปอาบีเลียน

ทฤษฎีบท

ให้ G เป็นกรุปจำกัด และ $a \in G$ จะได้ว่า

$$a \text{ เป็นตัวก่อกำเนิดของ } G \qquad \text{ก็ต่อเมื่อ} \qquad \circ(a) = |G|$$

ข้อสังเกต

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

จงหาตัวก่อกำเนิดทั้งหมดของกรุปต่อไปนี้

1. $\mathbb{Z}_5$
2. $\mathbb{Z}_6$
3. $\mathbb{Z}_5^*$

ทฤษฎีบท

ทุก ๆ กรุปย่อยของกรุปวัฏจักรย่อมเป็นกรุปวัฏจักร

ตัวอย่าง

จงหากรุปย่อยทั้งหมดของ $\mathbb{Z}_6$

ทฤษฎีบท

ให้ G_1 และ G_2 เป็นกรุปวัฏจักรจำกัด โดย a_1 และ a_2 เป็นตัวก่อกำเนิดของ G_1 และ G_2 ตามลำดับ สมมติว่า $\circ(a_1) = m$ และ $\circ(a_2) = n$ โดยที่ $gcd(m, n) = 1$ จะได้ว่า

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

ตัวอย่าง

จงตรวจสอบว่ากรุปต่อไปนี้เป็นกรุปวัฏจักรหรือไม่

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

บทแทรก

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

ทฤษฎีบท

ให้ G เป็นกรุปวัฏจักร โดย $|G| = n$ และ a เป็นตัวก่อกำเนิดของ G

สำหรับ $1 \leq k < n$ เมื่อ $k \in \mathbb{N}$ จะได้ว่า

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

ตัวอย่าง

จงหาตัวก่อกำเนิดทั้งหมดของกรุปวัฏจักรต่อไปนี้

1. $\mathbb{Z}_5$
2. $\mathbb{Z}_8$
3. $\mathbb{Z}_{12}$

ตัวอย่าง

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

ตัวอย่าง

จงหาจำนวนตัวก่อกำเนิดทั้งหมดกรุปวัฏจักรต่อไปนี้

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

ตัวอย่าง

จงหาจำนวนตัวก่อกำเนิดของ $\mathbb{Z}_{25}^{\times}$

ทฤษฎีบท

ถ้า $\langle a \rangle$ เป็นกรุปอนันต์ แล้ว

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

ทฤษฎีบท

ตัวก่อกำเนิดของกรุปวัฏจักรอนันต์มีเพียง 2 ตัวซึ่งเป็นตัวผกผันกันและกัน

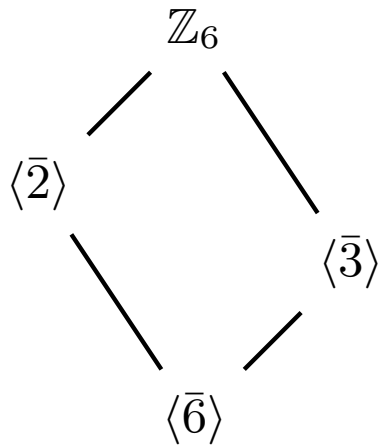
ทฤษฎีบท

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

$$G \text{ จะมีกรุปย่อยอันดับ } d \text{ เพียงกรุปเดียว}$$

3.3 แลตทิชของกรุป

ในหัวข้อนี้จะกล่าวถึงแผนภาพการแสดงกรุปย่อยทั้งหมดของกรุปจำกัดซึ่งเรียกว่า **แลตทิชของกรุปย่อย (lattice of subgroups)** ของกรุปจำกัด G หรือเรียกสั้น ๆ ว่า **แลตทิช (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 แลตทิชของ $\mathbb{Z}_6$



ตัวอย่าง

จงเขียนแลตทิชของ $\mathbb{Z}_{12}$

ตัวอย่าง

จงเขียนแลตทิชของ $\mathbb{Z}_{10}^{\times}$

ตัวอย่าง

จงเขียนแลตทิชของ $\mathbb{Z}_7^*$

ตัวอย่าง

จงเขียนแลตทิชของ S_3

บทที่ 4 กรุปย่อยปกติ

4.1 โคเซตและทฤษฎีบทลากรานจ์

บทนิยาม

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

ข้อสังเกต

ให้ G เป็นกรุป จะได้ว่า

1. ถ้า G เป็นกรุปอาบีเลียน แล้ว $Ha = aH$ ทุก ๆ $a \in G$
2. $He = H = He$

ตัวอย่าง

ให้ $H = \langle \bar{2} \rangle$ โดยที่ $H \leq \mathbb{Z}_6$ จงแจกแจงสมาชิกของโคเซตต่อไปนี้

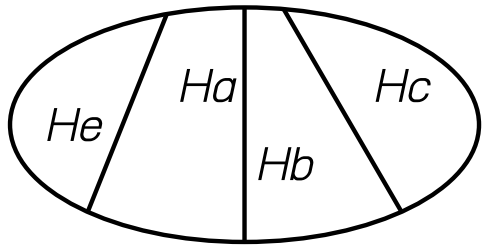
ตัวอย่าง

ให้ $H = \langle (1\ 3) \rangle$ โดยที่ $H \leq S_3$ จงแจกแจงสมาชิกของโคเซตต่อไปนี้

โคเซตเป็นผลแบ่งกั้นของกรุป 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 จะได้สมบัติดังต่อไปนี้

1. $Ha \cap Hb \neq \varnothing \quad \longleftrightarrow \quad ab^{-1} \in H \quad \longleftrightarrow \quad Ha = Hb$
2. $aH \cap bH \neq \varnothing \quad \longleftrightarrow \quad a^{-1}b \in H \quad \longleftrightarrow \quad aH = bH$

Theorem

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

ให้ $H = \langle \bar{4} \rangle$ โดยที่ $H \leq \mathbb{Z}_{12}$ จงหาโคเซตทั้งหมดที่เท่ากับโคเซต $\bar{1} + H$

ตัวอย่าง

ให้ $H = \langle (1\ 3) \rangle$ โดยที่ $H \leq S_3$ จงหาโคเซตทั้งหมดที่เท่ากับโคเซต $(1\ 2)H$

ทฤษฎีบท

ให้ H เป็นกรุปย่อยของกรุป G และ $a, b \in G$ จะได้ว่า

มีฟังก์ชันหนึ่งต่อหนึ่งทั่วถึงจาก aH ไป Hb

บทแทรก

ให้ H เป็นกรุปย่อยของกรุปจำกัด G และ $a, b \in G$ จะได้ว่า

$$|Ha| = |H| = |bH|$$

ตัวอย่าง

จงหาโคเซตทั้งหมดของ $\langle \bar{3} \rangle$ ใน $\mathbb{Z}_{12}$

ทฤษฎีบท

ให้ H เป็นกรุปย่อยของกรุป G กำหนดให้

$$\mathcal{R}(H) = \{Ha : a \in G\} \qquad \text{และ} \qquad \mathcal{L}(H) = \{aH : a \in G\}$$

จะได้ว่ามีฟังก์ชันหนึ่งต่อหนึ่งทั่วถึงจาก $\mathcal{R}(H)$ ไป $\mathcal{L}(H)$

ทฤษฎีบทลากรานจ์ (Lagrange's Theorem)

บทนิยาม

ให้ H เป็นกรุปย่อยของกรุปจำกัด G แล้วจำนวนสมาชิกของ $\mathcal{R}(H)$ หรือ $\mathcal{L}(H)$ จะเรียกว่า **ดรรชนี (index)** ของ H ใน G เขียนแทนด้วย $[G : H]$

ทฤษฎีบท

ทฤษฎีบทลากรานจ์ (Lagrange's Theorem)

ให้ H เป็นกรุปย่อยของกรุปจำกัด G แล้วจะได้ว่า $|H|$ หาร $|G|$ ลงตัว และ

$$[G : H] = \frac{|G|}{|H|}$$

บทแทรก

ให้ G เป็นกรุปจำกัดที่มีอันดับเป็นจำนวนเฉพาะ แล้ว

1. G มีกรุปย่อยเพียง 2 กรุปเท่านั้นคือ $\{e\}$ และ G

บทแทรก

ให้ a เป็นสมาชิกของกรุป G โดยที่ $|G| = n$ จะได้ว่า $a^n = e$

ตัวอย่าง

จงหาดรรชนี $[G : H]$ ที่กำหนดให้ต่อไปนี้โดยใช้ทฤษฎีบทลากรานจ์

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 $H = \langle (1\ 3\,4\ 5\ 6) \rangle$

4.2 นิยามและตัวอย่างของกรุปย่อยปกติ

บทนิยาม

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

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 แล้ว $gHg^{-1} = H$ ทุก ๆ $g \in G$
3. ถ้า H และ K เป็นกรุปย่อยของกรุปอาบีเลียน แล้ว $HK = KH$

ตัวอย่าง

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

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

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

ให้ N กรุปย่อยของกรุป G จะกล่าวว่า N เป็น **กรุปย่อยปกติ (normal subgroup)** ของ G เขียนแทนด้วย $N \trianglelefteq G$ ก็ต่อเมื่อ

$$gNg^{-1} = N \qquad \text{ทุก ๆ } g \in G$$

ข้อสังเกต

ให้ $N \leq G$ จะได้ว่า

1. $\{e\}$ และ G เป็นกรุปย่อยปกติของ G เสมอ
2. ถ้า G กรุปอาบีเลียน แล้ว $N \trianglelefteq G$ ทุก $N \leq G$

ตัวอย่าง

จงตรวจสอบว่ากรุปย่อย $\langle (1\ 2) \rangle$ และ $\langle (1\ 2\ 3) \rangle$ เป็นกรุปย่อยปกติของ S_3 หรือไม่

เกณฑ์การพิจารณากรุปย่อยปกติ (Normal Subgroup Criterion)

ทฤษฎีบท

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

ให้ G เป็นกรุป ถ้า $N \trianglelefteq G$ และ $K \trianglelefteq G$ แล้ว $N \cap K \trianglelefteq G$

ทฤษฎีบท

ให้ H และ K เป็นกรุปย่อยของกรุป G จะได้ว่า

$$HK \leq G \qquad \text{ก็ต่อเมื่อ} \qquad HK = KH$$

บทแทรก

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

ให้ H และ K เป็นกรุปย่อยจำกัดของกรุป G แล้ว

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

ทฤษฎีบท

ให้ N เป็นกรุปย่อยของกรุป G จะได้ว่า

$$\text{ถ้า} \quad [G : N] = 2 \quad \text{แล้ว} \quad N \trianglelefteq G$$

ตัวอย่าง

กรุปย่อย $\langle (1\ 3\ 2) \rangle$ เป็นกรุปย่อยปกติของ S_3 หรือไม่

4.3 กรุปผลหาร (quotient group)

ทฤษฎีบท

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*

บทนิยาม

ให้ G เป็นกรุป และ $N \trianglelefteq G$ แล้วกรุป $(\mathcal{R}(N), *)$ จะเรียกว่า **กรุปผลหาร (quotient group)** ของ G เขียนแทนด้วย G/N

ข้อสังเกต

ถ้า G เป็นกรุปจำกัด และ $N \trianglelefteq G$ แล้ว

$$|G/N| = [G : N] = \frac{|G|}{|N|}$$

ตัวอย่าง

จงแจกแจงสมาชิกของกรุปผลหารต่อไปนี้

1. $\mathbb{Z}/3\mathbb{Z}$
2. $\mathbb{Z}/4\mathbb{Z}$
3. $\mathbb{Z}/7\mathbb{Z}$

ทฤษฎีบท

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

จงหาตัวก่อกำเนิดทั้งหมดของ $\mathbb{Z}/6\mathbb{Z}$

ทฤษฎีบท

ให้ G *เป็นกรุป และ* $N \trianglelefteq G$ *และ* $[G : N] = n$ *จะได้ว่า*

1. $a^n = N \quad$ *สำหรับทุก ๆ* $\quad a \in G/N$
2. $g^n \in N \quad$ *สำหรับทุก ๆ* $\quad g \in G$