บทที่ 2
ความรู้พื้นฐาน

ในบทนี้จะขอทบทวนความรู้ในเรื่องของจำนวนเต็ม โดยจะกล่าวถึงคุณสมบัติบางประการของจำนวนเต็มที่จะนำไปใช้ในเรื่องของริง ไบนารี่โอเปอเรชัน (Binary Operation) โดยจะให้นิยามของไบนารี่โอเปอเรชัน และกฎต่างๆของไบนารี่โอเปอเรชัน นอกจากนี้จะทบทวนเรื่องกรุ๊ปโดยจะให้นิยาม และคุณสมบัติเบื้องต้นของกรุ๊ปเพียงเล็กน้อย

2.1. คุณสมบัติบางประการของจำนวนเต็ม

ให้ I เป็นเซ็ตของจำนวนเต็ม

การหารในจำนวนเต็ม

นิยาม 2.1.1 ถ้า $a, d \in I$ โดยที่ $d \neq 0$ จะกล่าวว่า d หาร a ได้ลงตัว ก็ต่อเมื่อมี $b \in I$ ซึ่ง $a = bd$ และเรียก d ว่าเป็นตัวหารของ a

สัญลักษณ์ เขียน d/a หมายความว่า d หาร a ได้ลงตัว
และ $d \nmid a$ หมายความว่า d หาร a ไม่ลงตัว

ข้อสังเกตุ
1. ให้ $a \in I$, ถ้า $a/1$ จะได้ว่า $a = \pm 1$
2. ถ้า b เป็นสมาชิกใดๆ ใน I แล้วจะได้ว่า $b/0$

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

ทฤษฎี 2.1.1 ดิวิชันอัลกอริทึมสำหรับจำนวนเต็มสำหรับจำนวนเต็ม

ให้ a, b เป็นจำนวนเต็มบวก จะมี $q, r \in I$ เพียงคู่เดียว ซึ่ง

$$a = bq + r \quad \text{เมื่อ} \quad 0 \leq r < b$$

พิสูจน์ ในตอนแรกจะพิสูจน์ว่า มี $q, r \in I$ ซึ่งสอดคล้องตามทฤษฎี

ให้ $S = \{a - bx / x \in I , a - bx \geq 0\}$

ถ้าให้ $x = 0$ ดังนั้น $a - bx = a > 0$

แสดงว่า $a \in S$ นั่นคือ $S \neq \emptyset$

เนื่องจากสมาชิกในเซ็ต S เป็นจำนวนเต็มบวก ดังนั้น S จะมีสมาชิกที่มีค่าน้อยที่สุด

ให้ r เป็นสมาชิกที่มีค่าน้อยที่สุดใน S

ดังนั้นจะมี $q \in I$ ซึ่ง $a - bq = r$

นั่นคือ $a = bq + r \qquad 0 \leq r$

สมมุติว่า $r \geq b$

ดังนั้น $r - b \geq 0$

และ $r - b = (a - bq) - b$

$= a - (q + 1)b$

แสดงว่า $r - b \in S$ ซึ่งจะทำให้เกิดการขัดแย้งกับที่ว่า r เป็นสมาชิกที่มีค่าน้อยที่สุดใน S

ดังนั้น $r < b$

นั่นคือ จะมี $q, r \in I$ ซึ่ง $a = bq + r$ เมื่อ $0 \leq r < b$

ต่อไปจะพิสูจน์ว่ามี q และ r เพียงคู่เดียว

สมมุติว่ามี q_1 และ r_1 ซึ่ง $a = bq_1 + r_1$ เมื่อ $0 \leq r_1 < b$

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

และเนื่องจาก $a = bq + r$ เมื่อ $0 \leq r < b$

ดังนั้น $bq_1 + r_1 = bq + r$

จะได้ $b(q_1 - q) = r - r_1$

สมมุติให้ $q_1 \geq q$

ดังนั้น $q_1 - q \geq 0$

ถ้า $q_1 - q \neq 0$ แสดงว่า $q_1 - q \geq 1$

ดังนั้น $b(q_1 - q) \geq b$

นั่นคือ $r - r_1 \geq b$

ซึ่งจะขัดแย้งกับที่ $b > r_1$ และ $b > r$

นั่นคือ $q_1 - q = 0$

ทำให้ได้ว่า $r - r_1 = 0$

นั่นคือ $q_1 = q$ และ $r = r_1$

แสดงว่าจะมี $q , r \in I$ เพียงค่าเดียวเท่านั้นที่ทำให้

$a = bq + r$ เมื่อ $0 \leq r < b$

<u>นิยาม 2.1.2</u> ให้ $a , b \in I$ โดยที่ $a \neq 0$, $b \neq 0$, d เป็นจำนวนเต็มบวก จะเรียกว่า d เป็นตัวหารร่วมมาก หรือ ห.ร.ม.ของ a และ b ก็ต่อเมื่อ

1. d/a และ d/b
2. ถ้า c/a และ c/b สำหรับ $c \in I$ แล้วจะได้ว่า c/d

<u>หมายเหตุ</u> จากนิยาม 2.1.2 ข้อ 1 แสดงให้เห็นว่า d เป็นตัวหารร่วมของ a และ b และข้อ 2 แสดงให้เห็นว่า d เป็นตัวที่มีค่ามากที่สุดในบรรดาตัวหารร่วมของ a และ b

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

สัญลักษณ์ เขียน (a,b) หมายถึง ห.ร.ม. ของ a และ b

ตัวอย่าง 2.1.1 เนื่องจากกำหนดให้ ห.ร.ม. เป็นจำนวนเต็มบวก ดังนั้นจะได้ว่า

$$(60, 24) = (60, -24) = 12$$

ทฤษฎี 2.1.2 ให้ a และ b เป็นสมาชิกที่ไม่เท่ากับ 0 ใน I แล้วจะได้ว่าจะมี d เป็น ห.ร.ม. ของ a และ b และจะมี m , n เป็นจำนวนเต็ม ซึ่ง

$$d = am + bn$$

พิสูจน์ ให้ $S = \{ax + by / x , y \in I , ax + by > 0\}$

ถ้าให้ $x = a$ และ $y = b$ จะได้ว่า $a^2 + b^2 \in S$ เนื่องจาก $a^2 + b^2 > 0$

นั่นคือ $S \neq \emptyset$

เนื่องจากทุกๆสมาชิกใน S เป็นจำนวนเต็มบวก ดังนั้น S จะมีสมาชิกที่มีค่าน้อยที่สุด

ให้ d เป็นสมาชิกที่มีค่าน้อยที่สุดใน S นั่นคือ $d \in S$

ดังนั้น $d = am + bn$ สำหรับบาง $m , n \in I$

ต่อไปจะแสดงว่า d เป็น ห.ร.ม. ของ a และ b

โดยดิวิชันอัลกอริทึมของ I สำหรับ $a , d \in I$ จะมี $q, r \in I$ ซึ่ง

$$a = qd + r \quad \text{เมื่อ} \quad 0 \leq r < d$$

ดังนั้น $a = q(am + bn) + r$

$$r = a - qam - qbn$$

$$= a(1 - qm) + (-nq)b$$

ถ้า $r \neq 0$ จะได้ว่า $r \in S$

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

เนื่องจาก $r < d$ ดังนั้นจะขัดแย้งกับที่ให้ d เป็นสมาชิกใน S ที่มีค่าน้อยที่สุด

นั่นคือ $r = 0$

ดังนั้น $a = qd$

แสดงว่า d/a

ในทำนองเดียวกัน พิสูจน์ได้ว่า d/b

ต่อไปสมมุติให้มี $c \in I$ ซึ่ง c/a และ c/b

นั่นคือจะมี $u, v \in I$ ซึ่ง $a = cu$ และ $b = cv$

ดังนั้น $d = (cu)m + (cv)n$

$= c(um + vn)$

แสดงว่า c/d

นั่นคือ d เป็น ห.ร.ม. ของ a และ b

<u>นิยาม 2.1.3</u> ถ้า $a, b \in I$ แล้ว a และ b จะเป็น relatively prime เมื่อ $(a, b) = 1$

<u>บทแทรก 2.1.3</u> ถ้า a และ b เป็น relatively prime แล้วจะมี $m,n \in I$ ซึ่ง $am + bn = 1$

<u>นิยาม 2.1.4</u> ให้ $p \in I$ และ $p > 1$ จะเรียกว่า p เป็นจำนวนเฉพาะ (prime number) ก็ต่อเมื่อตัวหารของ p คือ ± 1 และ $\pm p$ เท่านั้น

<u>ทฤษฎี 2.1.4</u> ถ้า p เป็นจำนวนเฉพาะ และ p/ab สำหรับ $a,b \in I$ แล้วจะได้ว่า p/a หรือ p/b

<u>พิสูจน์</u> ให้ p/ab และสมมุติว่า $p \not/ a$

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

เนื่องจาก p เป็นจำนวนเฉพาะ และ $(p , a) = 1$
โดยบทแทรก 1.1.3 จะได้ว่า มี $r, s \in I$ ซึ่ง

$$pr + as = 1$$

ดังนั้น $$b = prb + asb$$
$$= prb + abs$$

เนื่องจาก p/prb และ p/abs ทำให้ได้ว่า p/b

<u>บทแทรก 2.1.5</u> ถ้า n เป็นจำนวนเต็มบวก , p เป็นจำนวนเต็มเฉพาะ และ $p/a_1a_2\cdots\cdots a_n$ สำหรับ $a_i \in I$ แล้วจะได้ว่าจะมีอย่างน้อยค่า i หนึ่งค่าซึ่ง p/a_i เมื่อ $1 \leq i \leq n$

<u>พิสูจน์</u> แบบฝึกหัด

<u>นิยาม 2.1.5</u> ให้ n เป็นจำนวนเต็มที่มีค่าคงที่ และ $n > 0$ แล้วจะกล่าวว่า a คอนกรุเอนต์กับ b มอดูโล n (a is congruent to b modulo n) ก็ต่อเมื่อ $n/(a - b)$ สำหรับ $a , b \in I$

<u>สัญลักษณ์</u> เขียน $a \equiv b \pmod{n}$ หมายความว่า a คอนกรุเอนต์กับ b มอดูโล n

<u>ตัวอย่าง 2.1.2</u> $73 \equiv 4 \pmod{23}$
และ $21 \equiv -9 \pmod{10}$

<u>ทฤษฎี 2.1.6</u> 1. ความสัมพันธ์คอนกรุเอนต์มอดูโล n เป็นความสัมพันธ์สมมูลย์

2. ถ้า $a \equiv b \pmod{n}$ และ $c \equiv d \pmod{n}$ แล้วจะได้ว่า

$$a + c \equiv b + d \pmod{n}$$

และ $$ac \equiv bd \pmod{n}$$

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

พิสูจน์ 1. จะแสดงว่าความสัมพันธ์คอนกรูเอนต์มอดูโล n เป็นความสัมพันธ์สมมูลย์ คือ จะต้องแสดงว่าความสัมพันธ์คอนกรูเอนต์มอดูโล n สอดคล้องคุณสมบัติสะท้อน (reflexive) คุณสมบัติสมมาตร (symmetry) และคุณสมบัติถ่ายทอด (transitive)

เนื่องจาก $n/0$ ดังนั้น $n/(a - a)$

นั่นคือ $a \equiv a \pmod{n}$ เรียกว่าคุณสมบัติสะท้อน

ถ้า $a \equiv b \pmod{n}$ จะต้องแสดงว่า $b \equiv a \pmod{n}$

ให้ $a \equiv b \pmod{n}$

นั่นคือ $n/(a - b)$

จะได้ว่า $n/[-(a - b)]$ หรือ $n/(b - a)$

นั่นคือ $b \equiv a \pmod{n}$

แสดงว่า ถ้า $a \equiv b \pmod{n}$ แล้วจะได้ว่า $b \equiv a \pmod{n}$

เรียกว่าคุณสมบัติสมมาตร

ต่อไปจะแสดงว่า ถ้า $a \equiv b \pmod{n}$ และ $b \equiv c \pmod{n}$

แล้วจะได้ว่า $a \equiv c \pmod{n}$

เนื่องจาก $a \equiv b \pmod{n}$ และ $b \equiv c \pmod{n}$

นั่นคือ $n/(a - b)$ และ $n/(b - c)$

ดังนั้น $n/(a - b) + (b - c)$ จะได้ว่า $n/(a - c)$

นั่นคือ $a \equiv c \pmod{n}$

ดังนั้น ถ้า $a \equiv b \pmod{n}$ และ $b \equiv c \pmod{n}$

จะได้ว่า $a \equiv c \pmod{n}$ เรียกว่าคุณสมบัติถ่ายทอด

แสดงว่า ความสัมพันธ์คอนกรูเอนต์มอดูโล n เป็นความสัมพันธ์สมมูลย์

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

2. สมมุติ $a \equiv b \pmod n$ และ $c \equiv d \pmod n$

ดังนั้น $n/(a-b)$ และ $n/(c-d)$

จะได้ว่า $n/[(a-b)+(c-d)]$

นั่นคือ $n/[(a+c)-(b+d)]$

แสดงว่า $a+c \equiv b+d \pmod n$

และจาก $n/[(a-b)+(c-d)]$

จะได้ว่า $n/[(a-b)c+(c-d)b]$ นั่นคือ $n/(ac-bd)$

แสดงว่า $ac \equiv bd \pmod n$

นิยาม 2.1.6 ให้ $a \in I$ และ $\bar{a} = \{x \in I / x \equiv a \pmod n\}$

แล้วจะเรียก $\bar{a}$ ว่าเป็นอีควิวาเลนซ์คลาส (Equivalence class) ของ a

ข้อสังเกต 1. เนื่องจาก $a \equiv a \pmod n$ สำหรับ $a \in \bar{a}$ แสดงว่า $\bar{a}$ จะไม่เป็นเซ็ตว่าง

2. จากนิยาม 2.1.6 จะได้ว่า

$$\bar{a} = \{x \in I / x - a = nq, q \in I\}$$

$$= \{x \in I / x = nq + a, q \in I\}$$

นั่นคือ $\bar{a}$ จะเป็นเซ็ตของจำนวนเต็มซึ่งหารด้วย n แล้วเหลือเศษ a

ตัวอย่าง 2.1.3 พิจารณา $a \equiv b \pmod 5$ สำหรับ $a, b \in I$ จะหาอีควิวาเลนซ์คลาสของความสัมพันธ์นี้

จากนิยาม $\bar{a} = \{x \in I / x \equiv a \pmod n\}$

ถ้า $a = 0$, $\bar{0} = \{x \in I / x \equiv 0 \pmod 5\}$

$= \{x \in I /$ 5 หาร x ลงตัว $\}$

$= \{x \in I / x = 5q$ สำหรับ $q \in I\}$

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

$= \{\ldots -15, -10, 0, 5, 10, 15, \ldots\}$

ถ้า $a = 5$, $\bar{5} = \{x \in I / x \equiv 5 \pmod 5\}$

$= \{x \in I / 5$ หาร $x - 5$ ลงตัว $\}$

$= \{\ldots - 15, -10, 0, 5, 10, 15, \ldots\}$

ดังนั้นจะได้ว่า

$\bar{0} = \bar{5} = \overline{(-5)} = \ldots = \{\ldots -15, -10, 0, 5, 10, 15, \ldots\}$

$=$ เซ็ตของจำนวนเต็มที่หารด้วย 5 ลงตัว

ถ้า $a = 1$, $\bar{1} = \{x \in I / x \equiv 1 \pmod 5\}$

$= \{x \in I / x - 1 = 5q$, $q \in I\}$

$= \{x \in I / x = 5q + 1$, $q \in I\}$

$= \{\ldots -14, -9, -4, 1, 6, 11, 16, \ldots\}$

ถ้า $a = 6$, $\bar{6} = \{x \in I / x \equiv 6 \pmod 5\}$

$= \{\ldots -14, -9, -4, 1, 6, 11, 16, \ldots\}$

ดังนั้นจะได้ว่า

$\bar{1} = \bar{6} = \overline{(-4)} = \ldots = \{\ldots -14, -9, -4, 1, 6, 11, 16, \ldots\}$

$=$ เซ็ตของจำนวนเต็มที่หารด้วย 5 แล้วเหลือเศษเป็น 1

ในทำนองเดียวกันจะได้ว่า

$\bar{2} = \bar{7} = \overline{(-3)} = \ldots = \{\ldots -13, -8, -3, 2, 7, 12, 17, \ldots\}$

$=$ เซ็ตของจำนวนเต็มที่หารด้วย 5 แล้วเหลือเศษเป็น 2

$\bar{3} = \bar{8} = \overline{(-2)} = \ldots = \{\ldots -12, -7, -2, 3, 8, 13, 18, \ldots\}$

$=$ เซ็ตของจำนวนเต็มที่หารด้วย 5 แล้วเหลือเศษเป็น 3

$\bar{4} = \bar{9} = \overline{(-1)} = \ldots = \{\ldots -11, -6, -1, 4, 9, 14, 19, \ldots\}$

$=$ เซ็ตของจำนวนเต็มที่หารด้วย 5 แล้วเหลือเศษเป็น 4

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

ข้อสังเกตุ จากตัวอย่าง 2.1.3 ที่ผ่านมาสำหรับ $n = 5$ จะได้อีควิวาเลนซ์คลาสที่แตกต่างกันทั้งหมดคือ $\bar{0}$, $\bar{1}$, $\bar{2}$, $\bar{3}$, $\bar{4}$ ซึ่งมีคุณสมบัติดังนี้คือ

1. $\bar{0} \cup \bar{1} \cup \bar{2} \cup \bar{3} \cup \bar{4} = I$
2. $\bar{a} \cap \bar{b} = \phi$ สำหรับ $\bar{a}$, $\bar{b} \in I_5$

ในกรณีทั่วไปถ้ากำหนด $\bar{a} = \{x \in I \mid x \equiv a \pmod n\}$
จะได้เซ็ตของอีควิวาเลนซ์ หรือเซ็ตของจำนวนเต็มมอดูโล n ซึ่งเขียนแทนด้วย

I_n คือ $\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$ โดยที่

$\bar{0} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$

$\bar{1} = \{\ldots, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\}$

$\bar{2} = \{\ldots, -2n+2, -n+2, 2, n+2, 2n+2, \ldots\}$

.....

.....

$\bar{x} = \{\ldots, -2n+x, -n+x, x, n-x, 2n+x, \ldots\}$

.....

$\overline{n-1} = \{\ldots, -n-1, -1, n-1, 2n-1, 3n-1, \ldots\}$

ทฤษฎี 2.1.7 ให้ $a , b \in I$

1. ถ้า $a \in b$ แล้วจะได้ว่า $\bar{a} = \bar{b}$
2. $\bar{a} = \bar{b}$ ก็ต่อเมื่อ $a \equiv b \pmod n$
3. ถ้า $\bar{a} \cap \bar{b} \neq \phi$ แล้วจะได้ว่า $a \equiv b \pmod n$

พิสูจน์ 1. จะพิสูจน์ว่า $\bar{a} = \bar{b}$ โดยการแสดงว่า $\bar{a} \subseteq \bar{b}$ และ $\bar{b} \subseteq \bar{a}$

สมมุติให้ $a \in \bar{b}$ นั่นคือ $a \equiv b \pmod n$

ให้ $x \in \bar{a}$ นั่นคือ $x \equiv a \pmod n$

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

เนื่องจากความสัมพันธ์คอนกรูเอนต์สอดคล้องคุณสมบัติถ่ายทอด

ดังนั้น $x \equiv b \pmod{n}$

นั่นคือ $x \in \bar{b}$

แสดงว่า $\bar{a} \subseteq \bar{b}$

ต่อไปให้ $y \in \bar{b}$ นั่นคือ $y \equiv b \pmod{n}$

เนื่องจากความสัมพันธ์คอนกรูเอนต์สอดคล้องคุณสมบัติสมมาตร

ดังนั้น $b \equiv y \pmod{n}$

และเนื่องจาก $a \equiv b \pmod{n}$

โดยคุณสมบัติถ่ายทอดจะได้ $a \equiv y \pmod{n}$

โดยคุณสมบัติสมมาตรจะได้ $y \equiv a \pmod{n}$

นั่นคือ $y \in \bar{a}$

แสดงว่า $\bar{b} \subseteq \bar{a}$

นั่นคือ $\bar{a} = \bar{b}$

สำหรับการพิสูจน์ข้อ 2 และ 3 ให้ทำเป็นแบบฝึกหัด

ต่อไปจะนิยามการบวก และการคูณใน I_n ดังนี้

<u>การบวก</u> ให้ $\bar{a}$ และ $\bar{b}$ เป็นสมาชิกใน I_n จะได้ว่า

$\bar{a} + \bar{b} = \bar{r}$ ต่อเมื่อ $a + b \in qn + r$ โดยที่ $q, r \in I$ และ

$0 \leq r < n$

<u>การคูณ</u> ให้ $\bar{a}$ และ $\bar{b}$ เป็นสมาชิกใน I_n จะได้ว่า

$\bar{a} \cdot \bar{b} = \bar{r}$ ต่อเมื่อ $a.b = qn + r$ โดยที่ $q, r \in I$ และ

$0 \leq r < n$

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

<u>ตัวอย่าง 2.1.4</u> พิจารณาการบวก และการคูณของสมาชิกใน $I_3 = \{ \bar{0}, \bar{1}, \bar{2} \}$

<u>การบวก</u>

$$\bar{0} + \bar{0} = \bar{0}$$
$$\bar{0} + \bar{1} = \bar{1}$$
$$\bar{0} + \bar{2} = \bar{2}$$
$$\bar{1} + \bar{0} = \bar{1}$$
$$\bar{1} + \bar{1} = \bar{2}$$
$$\bar{2} + \bar{1} = \bar{0}$$

<u>การคูณ</u>

$$\bar{0}.\bar{0} = \bar{0}$$
$$\bar{0}.\bar{1} = \bar{0}$$
$$\bar{1}.\bar{2} = \bar{2}$$
$$\bar{1}.\bar{1} = \bar{1}$$

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

แบบฝึกหัด 2 ก

1. ให้ a , b และ $d \neq 0$ เป็นสมาชิกในเซ็ตของจำนวนเต็ม I จงพิสูจน์
   ก. ถ้า d/a และ a/b แล้วจะได้ว่า d/b
   ข. d/a ก็ต่อเมื่อ d/(-a)
   ค. $\pm$ 1/a สำหรับทุกๆจำนวนเต็ม a
   ง. ถ้า a/b และ b/a แล้วจะได้ว่า $a = \pm b$
   จ. ถ้า d/a และ d/b แล้วจะได้ว่า d/ (ax + by) สำหรับ $x , y \in I$
2. จงพิสูจน์ว่า ถ้า $x = y + z$ เมื่อ $x, y, z \in I$ และ $d \neq 0 \in I$ เมื่อ d เป็นตัวหารของ 2 ตัว ใดๆของ x , y และ z แล้วจะได้ว่า d จะเป็นตัวหารของตัวที่สามด้วย
3. ถ้า p และ q ต่างก็เป็นจำนวนเฉพาะ ซึ่ง p/q แล้วจงแสดงว่า p = q
4. จงพิสูจน์บทแทรก 2.1.5
5. ถ้า a/x และ b/x และ (a , b) = 1 จงพิสูจน์ว่า ab/x
6. จงแสดงว่า n > 1 จะเป็นจำนวนเฉพาะ ก็ต่อเมื่อสำหรับ a ใดๆ แล้ว (a , n) = 1 หรือ n/a
7. จงพิสูจน์ทฤษฎีบท 2.1.7 ข้อ 2, 3
8. ถ้า (a , n) = 1 จงพิสูจน์ว่า จะมี $\bar{b} \in I_n$ ซึ่ง $\bar{a}\bar{b} = \bar{1}$ ใน I_n
9. ถ้า (m , n) = 1 และ a , b เป็นสมาชิกใดๆใน I แล้วจงพิสูจน์ว่าจะมี $x \in I$ ซึ่ง $x \equiv a \pmod n$ และ $x \equiv b \pmod n$

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

2.2. ไบนารี่โอเปอร์เรชัน (Binary Operation)

นิยาม 2.2.1 ให้ S เป็นเซ็ตใดๆ ไบนารี่โอเปอร์เรชันบนเซ็ต S คือฟังก์ชันจากเซ็ต

$S \times S$ ไปยัง S

นั่นคือ $* : S \times S \longrightarrow S$ เมื่อ $*$ เป็นไบนารี่โอเปอร์เรชันบนเซ็ต S

ตัวอย่าง 2.2.1 ให้ $\mathbb{R}$ เป็นเซ็ตของจำนวนจริง

กำหนด $+ : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$

โดย $(a, b) \longrightarrow a + b$ สำหรับทุกๆ $a, b \in R$

จะได้ว่า + (เรียกว่าการบวก) เป็นไบนารี่โอเปอร์เรชันบนเซ็ต R

ตัวอย่าง 2.2.2 ให้ $\mathbb{R}$ เป็นเซ็ตของจำนวนจริง

กำหนด $\cdot : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$

โดย $(a, b) \longrightarrow a \cdot b$ สำหรับทุกๆ $a, b \in R$

จะได้ว่า $\cdot$ (เรียกว่าการคูณ) เป็นไบนารี่โอเปอร์เรชันบนเซ็ต $\mathbb{R}$

ตัวอย่าง 2.2.3 ให้ I เป็นเซ็ตของจำนวนเต็ม

กำหนด $\div : I \times I \longrightarrow I$

โดย $(a, b) \longrightarrow \frac{a}{b}$

จะได้ว่า $(3, 4) \longrightarrow \frac{3}{4}$

เนื่องจาก $\frac{3}{4} \notin I$ ดังนั้น $\div$ ไม่เป็นไบนารี่โอเปอร์เรชันบนเซ็ต I

หมายเหตุ สัญลักษณ์ของไบนารี่โอเปอร์เรชัน โดยทั่วๆไปมักจะใช้เครื่องหมาย $*$ หรือ $\circ$

เช่น $a * b$ หรือ $a \circ b$

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

ตัวอย่าง 2.2.4 ให้ I^+ เป็นเซ็ตของจำนวนเต็มบวก กำหนดให้ $a * b$ คือ ค่าที่น้อยกว่าระหว่าง a กับ b หรือค่าที่เท่ากันในกรณีที่ $a = b$ สำหรับทุกๆ $a, b \in I$ เช่น $2 * 5 = 2$, $15 * 10 = 10$, $5 * 5 = 5$ จะได้ว่า $*$ เป็นไบนารี่โอเปอร์เรชันบนเซ็ต I^+

ตัวอย่าง 2.2.5 ให้ I^+ เป็นเซ็ตของจำนวนเต็มบวก กำหนดให้ $a \circ b$ คือสมาชิกตัวหน้าเรชัน โดย $a \circ b = a$ สำหรับ $a, b \in I^+$ ดังนั้น $3 \circ 5 = 3$, $25 \circ 10 = 25$ จะได้ว่า เป็นไบนารี่โอเปอร์เรชันบน I^+

นิยาม 2.2.2 ให้ $*$ เป็นไบนารี่โอเปอร์เรชันบนเซ็ต S

1. ถ้า $a * b = b * a$ สำหรับทุกๆ $a, b \in S$ แล้วจะเรียกว่า $*$ สอดคล้องกฎการสลับที่ (commutative law)
2. ถ้า $(a * b) * c = a * (b * c)$ สำหรับทุกๆ $a, b, c \in$ แล้วจะเรียกว่า $*$ สอดคล้องกฎการรวมหมู่ (associative law)

ตัวอย่าง 2.2.6 จากตัวอย่าง 2.2.1 ได้ว่า $+$ เป็นไบนารี่โอเปอร์เรชันบนเซ็ต $\mathbb{R}$ จะได้ว่า $+$ สอดคล้องกฎการสลับที่ และกฎการรวมหมู่ เนื่องจาก $a + b = b + a$ สำหรับทุกๆ $a, b, c \in R$ และ $a + (b + c) = (a + b) + c$

ตัวอย่าง 2.2.7 ไบนารี่โอเปอร์เรชัน $*$ ในตัวอย่าง 2.2.4 สอดคล้องกฎการสลับที่และการรวมหมู่

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

ตัวอย่าง 2.2.8 ไบนารี่โอเปอร์เรชัน $\circ$ ในตัวอย่าง 2.2.5 ไม่สอดคล้องกฎการสลับที่ แต่จะสอดคล้องกับกฎการรวมหมู่

เนื่องจาก $a \circ b = a$ แต่ $b \circ a = b$ แสดงว่า

$a \circ b \neq b \circ a$

แต่ $a \circ (b \circ c) = a \circ b = a$

และ $(a \circ b) \circ c = a \circ c = a$

แสดงว่า $a \circ (b \circ c) = (a \circ b) \circ c$

นิยาม 2.2.3 ให้ $*$ และ $\circ$ เป็นไบนารี่โอเปอร์เรชันบนเซ็ต S

1. ถ้า $a * (b \circ c) = (a * b) \circ (a * c)$ สำหรับทุกๆ $a,b,c \in S$ เรียกว่ากฎการกระจายทางซ้ายของ $*$ บน $\circ$ (left distributive law)
2. ถ้า $(a \circ b) * c = (a * c) \circ (b * c)$ สำหรับทุกๆ $a,b,c \in S$ เรียกว่ากฎการกระจายทางขวาของ $*$ บน $\circ$ (right distributive law) ถ้าสอดคล้องทั้งซ้ายและขวา เรียกว่ากฎการกระจาย (distributive law)

ตัวอย่าง 2.2.9 ให้ I เป็นเซ็ตของจำนวนเต็มมี $+$ และ $\cdot$ คือการบวก และการคูณเป็นไบนารี่โอเปอร์เรชันบนเซ็ต I แล้วจะได้ว่ากฎการกระจายทั้งซ้ายและขวาของ $\cdot$ บน $+$ เป็นจริงในเซ็ต I

เช่น $3 \cdot (2 + 4) = (3 \cdot 2) + (3 \cdot 4)$

และ $(2 + 4) \cdot 5 = (2 \cdot 5) + (4 \cdot 5)$

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

แบบฝึกหัด 2 ข

1. จงพิสูจน์ว่า โอเปอร์เรชันในข้อต่อไปนี้ ข้อใดเป็น หรือไม่เป็นไบนารี่โอเปอร์เรชัน ของเซ็ต S ในแต่ละข้อต่อไปนี้

   ก. S = เซ็ตของจำนวนเต็มคู่ , $x * y = x + y$

   ข. S = เซ็ตของจำนวนเต็มคู่ , $x * y = x \cdot y$

   ค. S = เซ็ตของสับเซ็ตของเซ็ตของจำนวนเต็ม , $x * y = x \cap y$

   ง. S = เซ็ตของจำนวนเต็มบวก $x * y = x - y$

   จ. S = {0 , 1} , $x * y = x + y$

2. จงพิจารณาว่า โอเปอร์เรชันในแต่ละข้อต่อไปนี้ ข้อใดเป็นไบนารี่โอเปอร์เรชัน และข้อใดไม่เป็นไบนารี่โอเปอร์เรชัน

   ก. การบวกในเซ็ตของจำนวนเต็มคี่

   ข. ให้ I เป็นเซ็ตของจำนวนเต็ม กำหนดให้ $a \not| b$ เป็น ค.ร.น. ของ a และ b สำหรับทุกๆ $a , b \in I$

3. ให้ * เป็นไบนารี่โอเปอร์เรชัน ตามที่กำหนดให้ในข้อต่อไปนี้ จงพิจารณาว่า * ในข้อใดสอดคล้องกฎการสลับที่ และข้อใดสอดคล้องกฎการรวมหมู่

   ก. I = เซ็ตของจำนวนเต็ม , $a * b = a - b$

   ข. Q = เซ็ตของจำนวนตรรกยะ , $a * b = ab + 1$

   ค. I^+ = เซ็ตของจำนวนเต็มบวก , $a * b = 2^{ab}$

   ง. I^+ = เซ็ตของจำนวนเต็มบวก , $a * b = a^b$

   จ. Q = เซ็ตของจำนวนตรรกยะ , $a * b = \frac{ab}{2}$

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

4. I เป็นเซ็ตของจำนวนเต็ม จงพิจารณาว่าไบนารี่โอเปอร์เรชันในแต่ละข้อต่อไปนี้สอดคล้องการกระจายทางซ้ายของการคูณหรือไม่

   ก. $a * b = a - b$ สำหรับทุกๆ $a, b \in I$

   ข. $a \# b = a + b + 1$ สำหรับทุกๆ $a, b \in I$

   ค. $a * b = a + b - ab$ สำหรับทุกๆ $a, b \in I$

5. ให้ I_n เป็นเซ็ตของอีควิวาเลนซ์คลาสของจำนวนเต็มมอดูโล n แล้วจงพิสูจน์ว่าการบวก และการคูณใน I_n สอดคล้องกฎการสลับที่ และกฎการรวมหมู่ และกฎการกระจายของการคูณบนการบวก

2.3. กรุ๊ป (Group)

ในเรื่องกรุ๊ปจะทบทวนแต่นิยามของกรุ๊ป อบีเลียนกรุ๊ป พร้อมทั้งตัวอย่าง และคุณสมบัติเบื้องต้นเท่านั้น

นิยาม 2.3.1 ให้ G เป็นเซ็ตที่ไม่ว่าง , $\circ$ เป็นไบนารี่โอเปอร์เรชันบนเซ็ต G ซึ่งสอดคล้อง

1. $(a \circ b) \circ c = a \circ (b \circ c)$ สำหรับทุกๆ $a, b, c \in G$
2. จะมีสมาชิก $e \in G$ ซึ่ง $a \circ e = a = e \circ a$ สำหรับทุก $a \in G$ เรียก e ว่าเป็นสมาชิกเอกลักษณ์สำหรับไบนารี่โอเปอร์เรชัน $\circ$
3. สำหรับทุกๆ $a \in G$ จะมีสมาชิก $b \in G$ ซึ่ง $a \circ b = e = b \circ a$ เรียก b ว่าเป็นอินเวอร์สของ a

จะเรียก G ว่าเป็นกรุ๊ปภายใต้ไบนารี่โอเปอร์เรชัน $\circ$

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

นิยาม 2.3.2 ให้ G เป็นกรุ๊ป, และ o เป็นไบนารี่โอเปอร์เรชันบน G จะกล่าวว่า G เป็นอบีเลี่ยนกรุ๊ป(abelian or commutative group) ถ้า a o b = b o a สำหรับทุกๆ a , b ε G

ตัวอย่าง 2.3.1 ให้ I เป็นเซ็ตของจำนวนเต็ม มี + (การบวก) เป็นไบนารี่โอเปอร์เรชันบนเซ็ต I จะได้ว่า

1. + สอดคล้องกฎการรวมหมู่ใน I
นั่นคือ (a + b) + c = a + (b + c) สำหรับทุกๆ a,b,c ε I
2. มี 0 ε I ซึ่ง a + 0 = a = 0 + a สำหรับทุกๆ a ε I
นั่นคือ 0 เป็นสมาชิกเอกลักษณ์สำหรับการบวกใน I
3. สำหรับทุกๆ a ε I จะมี -a ε I ซึ่ง a + (-a) = 0 = (-a)+a
นั่นคือ -a เป็นอินเวอร์สสำหรับการบวกของ a
4. สำหรับทุกๆ a,b ε I จะได้ว่า a + b = b + a
แสดงว่า I เป็นอบีเลี่ยนกรุ๊ป ภายใต้ไบนารี่โอเปอร์เรชัน +

ตัวอย่าง 2.3.2 ให้ I เป็นเซ็ตของจำนวนเต็ม มี • (การคูณ) เป็นไบนารี่โอเปอร์เรชัน เนื่องจาก อินเวอร์สสำหรับการคูณของ 3 ε I คือ $\frac{1}{3}$ ไม่เป็นสมาชิกใน I นั่นคือ I ไม่เป็นกรุ๊ปภายใต้ไบนารี่โอเปอร์เรชัน •

ตัวอย่าง 2.3.3 ให้ G = {u,v,w,x} กำหนด • เป็นโอเปอร์เรชันบนเซ็ต G ตามตารางข้างล่างนี้

•	u	v	w	x
u	u	v	w	x
v	v	u	x	w
w	w	x	v	u
x	x	w	u	v

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

1. จากตารางจะเห็นว่า $\circ$ เป็นไบนารี่โอเปอร์เรชันบนเซ็ต G คือ
สำหรับทุกๆ $a,b \in G$ แล้วจะได้ว่า $a \circ b \in G$

2. พิจารณา $(u \circ v) \circ w = v \circ w = x$
และ $u \circ (v \circ w) = u \circ x = x$
แสดงว่า $(u \circ v) \circ w = u \circ (v \circ w)$
จะต้องทดสอบว่าทุกๆสมาชิกสอดคล้องกฎการรวมหมู่ ให้ทำเป็นแบบฝึกหัด

3. จากตารางจะได้ว่ามี $u \in G$ ซึ่งสำหรับทุกๆ $g \in G$ แล้วจะได้ว่า
$g \circ u = g = u \circ g$
นั่นคือ u เป็นสมาชิกเอกลักษณ์

4. สำหรับทุกๆ $a \in G$ จะมี $b \in G$ ซึ่ง $a \circ b = u = b \circ a$ เช่น
$w \circ x = u = x \circ w$ สำหรับ $w, x \in G$
จากการทดสอบดูทุกสมาชิก $a \in G$ จะมีอินเวอร์สสำหรับไบนารี่โอเปอร์เรชัน

5. สำหรับทุกๆ $a,b \in G$ จะได้ว่า $a \circ b = b \circ a$ เช่น
$w \circ v = x = v \circ w$
จากการทดสอบดูทุกคู่จะสอดคล้องกฎการสลับที่ สำหรับไบนารี่โอเปอร์เรชัน
นั่นคือ G เป็นกรุ๊ปภายใต้ไบนารี่โอเปอร์เรชัน $\circ$ และ G เป็นอบีเลี่ยนกรุ๊ป

<u>ตัวอย่าง 2.3.4</u> ให้ $\mathbb{R}$ เป็นเซ็ตของจำนวนจริง , Q เป็นเซ็ตของจำนวนตรรกยะ
จะได้ว่า $\mathbb{R}$ และ Q จะเป็นกรุ๊ปภายใต้ไบนารี่โอเปอร์เรชัน +

<u>ทฤษฎี 2.3.1</u> ให้ a,b,c เป็นสมาชิกในกรุ๊ป G ซึ่งมี $\circ$ เป็นไบนารี่โอเปอร์เรชัน
แล้วจะได้ว่า
1. ถ้า $a \circ b = a \circ c$ แล้วจะได้ว่า $b = c$
2. ถ้า $a \circ c = b \circ c$ แล้วจะได้ว่า $a = b$

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

<u>พิสูจน์</u> เนื่องจาก $a \circ b = a \circ c$

จากนิยามของกรุ๊ปจะมีอินเวอร์สของ a เป็นสมาชิกใน G

ให้ s เป็นอินเวอร์สของ a

ดังนั้น $s \circ a = e = a \circ s$ เมื่อ e คือสมาชิกเอกลักษณ์ใน G

ดังนั้น $s \circ (a \circ b) = s \circ (a \circ c)$

โดยกฎการรวมหมู่จะได้ $(s \circ a) \circ b = (s \circ a) \circ c$

ดังนั้น $e \circ b = e \circ c$

นั่นคือ $b = c$

2. พิสูจน์เป็นแบบฝึกหัด

<u>หมายเหตุ</u> คุณสมบัติในทฤษฎี 2.3.1 นี้เรียกว่ากฎของการตัดออก (cancellation law)

<u>ทฤษฎี 2.3.2</u> ให้ G เป็นกรุ๊ปภายใต้ไบนารี่โอเปอร์เรชัน $\circ$ แล้วจะได้ว่า

1. สมาชิกเอกลักษณ์ของ G จะมีได้เพียงตัวเดียว
2. สำหรับทุกๆ $a \in G$ จะมีอินเวอร์สของ a ได้เพียงตัวเดียว

<u>พิสูจน์</u> 1. สมมุติ e และ e' เป็นสมาชิกเอกลักษณ์ของ G

เนื่องจาก e เป็นสมาชิกเอกลักษณ์ของ G

ดังนั้น $a \circ e = a = e \circ a$ สำหรับทุกๆ $a \in G$

ถ้าให้ $a = e'$ ดังนั้น $e' \circ e = e' = e \circ e'$ สำหรับ $e' \in G$ ---(1)

เนื่องจาก e' เป็นสมาชิกเอกลักษณ์ของ G

ดังนั้น $a \circ e' = a = e' \circ a$ สำหรับทุกๆ $a \in G$

ให้ $a = e$ จะได้ว่า $e \circ e' = e = e' \circ e$ สำหรับ $e \in G$ ---(2)

จาก (1) และ (2) จะได้ว่า $e = e'$

นั่นคือ สมาชิกเอกลักษณ์ของ G จะมีได้เพียงตัวเดียวเท่านั้น

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

2. สมมุติให้ทั้ง b และ c เป็นอินเวอร์สของ a

ดังนั้น $a \circ b = e = b \circ a$

และ $a \circ c = e = c \circ a$

ดังนั้น $a \circ b = a \circ c$

โดยทฤษฎี 23.1 จะได้ $b = c$

นั่นคืออินเวอร์สของ a จะมีได้เพียงตัวเดียวเท่านั้น

แบบฝึกหัด 2 ค

1. จงพิสูจน์ทฤษฎี 23.1 ข้อ 2
2. ให้ G เป็นกรุ๊ปและ $\circ$ เป็นไบนารี่โอเปอร์เรชันในกรุ๊ป G และให้ a^{-1} เป็นอินเวอร์สของ a สำหรับทุกๆ $a \in G$ จงพิสูจน์ว่า $(a^{-1})^{-1} = a$ สำหรับทุกๆ $a \in G$
3. ให้ G เป็นกรุ๊ป, $\circ$ เป็นไบนารี่โอเปอร์เรชันในกรุ๊ป G แล้วจะได้ว่า $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$ สำหรับทุกๆ $a, b \in G$
4. G เป็นอบีเลี่ยนกรุ๊ป ก็ต่อเมื่อ $(ab)^2 = a^2b^2$ สำหรับทุกๆ $a, b \in G$
5. G เป็นกรุ๊ปใดๆ จงพิสูจน์ว่า G จะเป็นอบีเลี่ยนกรุ๊ป ถ้า $x^2 = e$ สำหรับทุกๆ $x \in G$
6. จงพิจารณาเซ็ตต่อไปนี้ พร้อมด้วยโอเปอร์เรชันเซ็ตใดเป็นกรุ๊ป ถ้าเป็นกรุ๊ปจงหาสมาชิกเอกลักษณ์ และอินเวอร์สของแต่ละสมาชิกในเซ็ตนั้น

   ก. เซ็ต $\{ \bar{0}, \bar{2}, \bar{4}, \bar{6} \}$, โอเปอร์เรชันคือ การบวก

   ข. เซ็ต $\{a + b\sqrt{2} / a, b \in I \}$, โอเปอร์เรชันคือ การคูณ

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved

6. (ต่อ)

ค. เซ็ต $\{a + b\sqrt{2} / a , b \in I\}$, โอเปอร์เรชันคือ การคูณ

ง. เซ็ต N ซึ่งเป็นเซ็ตของจำนวนเต็มที่ไม่เป็นลบ , โอเปอร์เรชันคือ การบวก

จ. เซ็ตของจำนวนเต็ม I , โอเปอร์เรชัน $\circ$ ซึ่งกำหนดโดย $a \circ b = a^2 - b$ สำหรับทุกๆ $a , b \in I$

ช. เซ็ตของจำนวนเต็ม I , โอเปอร์เรชัน $\bullet$ ซึ่งกำหนดโดย $a \bullet b = a + b + 1$ สำหรับทุกๆ $a , b \in I$

ซ. เซ็ตของจำนวนเต็ม I , โอเปอร์เรชัน $\bullet$ ซึ่งกำหนดโดย $a \bullet b = a + b - ab$ สำหรับทุกๆ $a , b \in I$

ฌ. เซ็ต $\{a , b , c , d\}$, โอเปอร์เรชัน $\bullet$ ซึ่งกำหนดโดยตาราง

$\bullet$	a	b	c	d
a	a	b	c	d
b	b	c	d	b
c	c	d	a	b
d	d	a	c	a

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright© by Chiang Mai University
All rights reserved