บทที่ 2
โดเมนเชิงจำนวนเต็ม
(Integral domain)

2.1 ตัวหารของศูนย์และการตัดออก

(Divisors of zero and cancellation)

คุณสมบัติทางพีชคณิตที่สำคัญมากที่สุด คุณสมบัติหนึ่งของระบบจำนวน ก็คือ ผลคูณระหว่างจำนวน 2 จำนวนจะเป็นศูนย์ได้ก็ต่อเมื่ออย่างน้อยที่สุดจำนวนใดจำนวนหนึ่งต้องเป็นศูนย์ ซึ่งคุณสมบัตินี้นักศึกษาคงพบและใช้อยู่ประจำ ตัวอย่างเช่น ต้องการจะแก้สมการ

$$x^2 - 5x + 6 = 0$$

สิ่งแรกที่เราจะทำก็คือ แยกแฟคเตอร์ของด้านซ้ายของสมการ ซึ่งจะได้

$$x^2 - 5x + 6 = (x - 2)(x - 3)$$

แล้วเราก็สรุปว่า $x = 2$ และ $x = 3$

ทำไมเราจึงสรุปเช่นนี้

คำตอบก็คือ ถ้า x ถูกแทนที่ด้วยจำนวน a แล้ว

$(a - 2)(a - 3) = 0$ ก็ต่อเมื่อ $a - 2 = 0$ หรือ $a - 3 = 0$

ตัวอย่าง 2.1.1 จงแก้สมการ $x^2 - 5x + 6 = 0$ ใน Z_{12}

วิธีทำ

$\because (x^2 - 5x + 6) = (x - 2)(x - 3)$

แต่ใน Z_{12} จะพบว่าไม่แต่เพียง $(0)a = a(0) = 0$ สำหรับทุก ๆ $a \in Z_{12}$ เท่านั้น แต่ยังมีจำนวนอื่น ๆ ที่คูณกัน แล้วได้ผลลัพธ์ 0 อีก คือ

$$(2)(6) = (6)(2) = 0$$

$$(3)(4) = (4)(3) = 0$$

$(3)(8) = (8)(3) = 0$

$(4)(6) = (6)(4) = 0$

$(4)(9) = (9)(4) = 0$

$(6)(6) = 0$

$(6)(8) = (8)(6) \quad 0$

$(6)(10) = (10)(6) = 0$

$(8)(9) = (9)(8) = 0$

ดังนั้นคำตอบสำหรับสมการนี้จึงไม่ใช่แต่เพียง $x = 2$ และ $x = 3$ เท่านั้น แต่ $x = 6$ และ $x = 11$ ก็เป็นคำตอบของสมการด้วยเช่นกัน เพราะ

$(6 - 2)(6 - 3) = (4)(3) = 0$ ใน Z_{12}

และ $(11 - 2)(11 - 3) = (9)(8) = 0$ ใน Z_{12}

จากแนวความคิดอันนี้ทำให้เราสร้างนิยามของตัวหารของศูนย์ดังนี้

นิยาม ถ้า a และ b เป็นสมาชิกที่ไม่ใช่ศูนย์ของวง R ซึ่ง $ab = 0$ แล้ว a และ b เป็นตัวหารของศูนย์ (divisor of zero)

a เป็นตัวหารซ้ายของศูนย์ (left divisor of zero)

b เป็นตัวหารขวาของศูนย์ (right divisor of zero)

ในวง (ring) ที่สอดคล้องกฎการสลับที่ ทุก ๆ ตัวหารซ้ายของศูนย์ ก็จะเป็นตัวหารขวาของศูนย์ด้วยเช่นกัน และในทางกลับกันตัวหารขวาของศูนย์ก็จะเป็นตัวหารซ้ายของศูนย์ด้วยเช่นกัน ดังนั้นจึงไม่มีความแตกต่างระหว่างตัวหารซ้ายของศูนย์และตัวหารขวาของศูนย์ ในวงที่สอดคล้องกฎการสลับที่

ตัวอย่างที่ 2.1.1 แสดงให้เห็นว่า ใน Z_{12} สมาชิก 2, 3, 4, 6, 8, 9 และ 10 เป็นตัวหารของศูนย์ ขอให้สังเกตด้วยว่า สมาชิกทั้งหมดที่กล่าวนี้ เป็นจำนวนใน Z_{12} ที่ไม่ใช่จำนวน**เฉพาะสัมพัทธ์** (relatively prime) กับ 12 นั่นคือ ห.ร.ม. ของ 12 และสมาชิกแต่ละตัวที่กล่าวข้างต้น ไม่ใช่ 1

ทฤษฎี 2.1.1 ในวง Z_n, ตัวหารของศูนย์ ก็คือ สมาชิกของ Z_n ตัวที่ไม่ใช่จำนวนเฉพาะสัมพัทธ์กับ n

พิสูจน์

ให้ $m \in Z_n$ โดยที่ $m \neq 0$

และให้ ห.ร.ม. ของ m กับ $n = d \neq 1$

$\because \quad m\left(\frac{n}{d}\right) = \left(\frac{m}{d}\right)n$

และถ้า $\frac{m}{d} = 0$

$\left(\frac{m}{d}\right)n = 0n = 0$

จึงได้ $m\left(\frac{n}{d}\right) = 0$

ดังนั้น $m\left(\frac{n}{d}\right) = 0$ ใน Z_n ในขณะที่ทั้ง $m \neq 0$ และ $\frac{n}{d} \neq 0$

$\therefore$ m เป็นตัวหารของศูนย์

หรือสมมติ $m \in Z_n$ เป็นจำนวนเฉพาะสัมพัทธ์กับ n

ถ้าสำหรับ $s \in Z_n$ เรามี $ms = 0$

$\because \; ms = 0$

ดังนั้น n หาร ms ลงตัว โดยที่ $m, s \in Z_n$

แต่ n ไม่มีตัวหารร่วมกับ m ที่ > 1

ดังนั้น n ต้องหาร s ลงตัว

$\therefore$ $s = 0$ ใน Z_n

$\therefore$ ไม่มีตัวหารของศูนย์ #

บทแทรก | ถ้า p เป็นจำนวนเฉพาะ แล้ว Z_p ไม่มีตัวหารของศูนย์

พิจารณา ให้ R เป็นวง, $a, b, c \in R$ แล้ว

กฎการตัดออกสำหรับการคูณจะเป็นจริงใน R ถ้า

$ab = ac$ และ $a \neq 0 \Rightarrow b = c$

และ $ba = ca$ และ $a \neq 0 \Rightarrow b = c$

ส่วนกฎการตัดออกสำหรับการบวกเป็นจริงในวง R อยู่แล้ว เพราะ $(R, +)$ เป็นกลุ่ม

ทฤษฎี 2.1.2 | กฎการตัดออก (cancellation law) จะเป็นจริงในวง R ก็ต่อเมื่อ R ไม่มีตัวหารทางซ้ายของศูนย์หรือตัวหารทางขวาของศูนย์

พิสูจน์ $\Rightarrow$

ให้ R เป็นวงซึ่งกฎการตัดออกเป็นจริง

และสมมติ $ab = 0$ สำหรับ a, b บางตัวใน R

เราจะต้องแสดงว่า $a = 0$ หรือ $b = 0$

ถ้า $a \neq 0$

$$ab = a0$$

โดยกฎการตัดออก

$$b = 0$$

ในทำนองเดียวกัน

ถ้า $b \neq 0$

$$ab = 0b$$

$$a = 0$$

แสดงว่าไม่มีตัวหารของศูนย์ (ทั้งขวาและซ้าย) ถ้ากฎการตัดออกเป็นจริงในวง R

$\Leftarrow$ สมมติวง R ไม่มีตัวหารซ้ายของศูนย์หรือตัวหารขวาของศูนย์

และสมมติ $ab = ac$ โดยที่ $a \neq 0$

$$\therefore \quad ab - ac = 0$$

$$a(b - c) = 0$$

เนื่องจาก $a \neq 0$ และ R ไม่มีตัวหารร่วมซ้ายของศูนย์

เราจะต้องได้ $b - c = 0$

$$\therefore \quad b = c$$

ในทำนองเดียวกัน จะพิสูจน์ได้ว่า

$ba = ca$ และ $a \neq 0 \Rightarrow b = c$ #

สมมติว่า R เป็นวงที่ไม่มีตัวหารของศูนย์ แล้วสมการ $ax = b$ โดยที่ $a \neq 0$ ใน R จะมีผลเฉลย (solution) ได้อย่างมากเพียงคำตอบเดียว

เพราะ ถ้า $ax_1 = b$

และ $ax_2 = b$

$$\therefore \quad ax_1 = ax_2$$

$$x_1 = x_2$$

ถ้า R มียูนิตี้ 1 และ a เป็น unit ใน R

แล้ว ผลเฉลยของสมการ $ax = b$ คือ

$$x = a^{-1}b$$

ในกรณีที่วง R เป็นวงที่สอดคล้องกฎการสลับที่ โดยเฉพาะในกรณีที่ R เป็นสนาม (field) เรามักเขียนแทน $a^{-1}b$ และ ba^{-1} โดยสัญลักษณ์ $\frac{b}{a}$ แต่สัญลักษณ์นี้จะต้องไม่ใช้ในกรณีที่ R ไม่ใช่วงที่สอดคล้องกฎการสลับที่

ในสนาม F บ่อยครั้งที่เรานิยามเศษส่วน $\frac{b}{a}$ โดยที่ $a \neq 0$ ให้เป็นผลเฉลย x ใน F ของสมการ $ax = b$

2.2 **โดเมนเชิงจำนวนเต็ม** (Integral domains)

นิยาม โดเมนเชิงจำนวนเต็ม D คือ วงที่มี unity, สอดคล้องกฎการสลับที่ และไม่มีตัวหารของศูนย์

ตัวอย่าง 2.2.1 (R, +, .), (Q, +, .), (Z, +, .) เป็นโดเมนเชิงจำนวนเต็ม

จากนิยามจะได้ข้อสังเกตว่า ถ้าสัมประสิทธิ์ของ polynomial มาจากโดเมนเชิงจำนวนเต็มแล้ว เราสามารถจะแก้สมการโพลิโนเมียลโดยการแยกตัวประกอบออกมาให้เหลือ x มีกำลังหนึ่ง แล้วเทียบให้แต่ละตัวประกอบมีค่าเท่ากับศูนย์ ก็จะได้ค่า x

ทฤษฎี 2.2.1 ทุก ๆ สนาม F เป็นโดเมนเชิงจำนวนเต็ม

พิสูจน์

ให้ F เป็นสนาม $a, b \in F$ โดยที่ $a \neq 0$

และ $ab = 0$

$$\frac{1}{a}(ab) = \frac{1}{a}(0)$$

$$= 0$$

แต่ $$\frac{1}{a}(ab) = \left(\frac{1}{a}a\right)b$$

$$= 1b$$

$$= b$$

$\therefore \quad b = 0$

$\therefore$ F ไม่มีตัวหารของศูนย์

และเนื่องจาก F เป็นสนาม

$\therefore$ F เป็นวงที่มี unity และสอดคล้องกฎการสลับที่

ดังนั้น F เป็นโดเมนเชิงจำนวนเต็ม #

ทฤษฎี 2.2.2 ทุก ๆ โดเมนเชิงจำนวนเต็มที่มีสมาชิกจำกัดเป็นสนาม

พิสูจน์

ให้ D เป็นโดเมนเชิงจำนวนเต็มที่มีสมาชิกจำกัด

$0, 1, a_1, a_2, \ldots, a_n \in D$

จะต้องแสดงว่า สำหรับ $a \in D$ ที่ $a \neq 0 \ \exists\, b \in D \ni ab = 1$

พิจารณา เราถือว่า $1, a_1, a_2, \ldots, a_n \in D$ เป็นสมาชิกที่แยกกันเด็ดขาด (distinct)

สำหรับ $aa_i = aa_j$

โดย กฎการตัดออก

$a_i = a_j$

เนื่องจาก D ไม่มีตัวหารของศูนย์

$\therefore$ สมาชิกทุกตัวของ D ไม่ใช่ศูนย์

ด้วยเหตุนี้โดยการนับ เราพบว่า

$a1, aa_1, \ldots, aa_n$ คือ สมาชิก $1, a_1, \ldots, a_n$

ดังนั้น $a1 = 1$

$a = 1$

หรือ $aa_i = 1$ สำหรับ บาง i

ดังนั้น a มีตัวผกผันสำหรับการคูณ #

บทแทรก | ถ้า p เป็นจำนวนเฉพาะแล้ว Z_p เป็นสนาม |

2.3 ลักษณะเฉพาะของวง (The characteristic of a ring)

ถ้าให้ R เป็นวง เราอาจจะมีคำถามขึ้นมาว่า มีจำนวนเต็มบวก n ที่มีคุณสมบัติว่า $n \cdot a = 0$ สำหรับทุก ๆ $a \in R$ หรือไม่ โดยที่ $n \cdot a$ หมายความว่า $a + a + \ldots + a$ ทั้งหมด n ตัว ตัวอย่างเช่น จำนวนเต็มบวก m มีคุณสมบัตินี้ในวง Z_m

นิยาม ถ้าในวง R มีจำนวนเต็มบวก n ซึ่ง $n \cdot a = 0$ สำหรับทุก ๆ $a \in R$ แล้ว จำนวนเต็มบวก n ตัวที่เล็กที่สุดที่มีคุณสมบัติแบบนี้ใน R คือ ลักษณะเฉพาะของวง R (Characteristic of the ring R) ใช้สัญลักษณ์ Char (R) = n ถ้าไม่มีจำนวนเต็มบวก n ที่มีคุณสมบัติอย่างนี้แล้ว ลักษณะเฉพาะของ R เป็น 0 (Char (R) = 0)

ตัวอย่าง 2.3.1 as $(Z, +, \cdot)$ มี Char(Z) = 0

ตัวอย่าง 2.3.2 วง $(Z_6, +_6, \cdot_6)$ มี Char $(Z_6) = 6$ เพราะ $6 \cdot r = 0$ $\forall r \in Z_6$

นั่นคือ $0 + 0 + 0 + 0 + 0 + 0 = 0$

$1 + 1 + 1 + 1 + 1 + 1 = 0$

$2 + 2 + 2 + 2 + 2 + 2 = 0$

$3 + 3 + 3 + 3 + 3 + 3 = 0$

$4 + 4 + 4 + 4 + 4 + 4 = 0$

$5 + 5 + 5 + 5 + 5 + 5 = 0$

ตัวอย่าง 2.3.3 วง $(Z_n, +_n, \cdot_n)$ มี Char $(Z_n) = n$

ทฤษฎี 2.3.1 ถ้า R เป็นวงที่มี unity 1 และ n เป็นจำนวนเต็มบวกที่เล็กที่สุดที่ $n \cdot 1 = 0$ แล้ว Char (R) = n ถ้าไม่มีจำนวนเต็มบวกที่เล็กที่สุด n ซึ่ง $n \cdot 1 = 0$ แล้ว Char (R) = 0

พิสูจน์

ถ้าไม่มีจำนวนเต็มบวก n ที่ $n \cdot 1 = 0$

$\therefore$ จะไม่มีจำนวนเต็มบวกที่เล็กที่สุด ที่ $n \cdot r = 0 \ \forall r \in R$

$\therefore$ Char (R) = 0

ถ้ามีจำนวนเต็มบวกที่เล็กที่สุด n ที่ทำให้ $n \cdot 1 = 0$

ให้ $r \in R$

$$\begin{aligned} \because \quad nr &= (n1)r \\ &= 0r \\ &= 0 \end{aligned}$$

ถ้า $0 < k < n$ แล้ว $k1 \neq 0$

$\therefore$ n เป็นจำนวนเต็มบวกที่เล็กที่สุด ที่ $nr = 0 \ \forall r \in R$

แบบฝึกหัดที่ 2

1) จงพิจารณาข้อความแต่ละข้อต่อไปนี้เป็นจริงหรือเป็นเท็จ

..............ก) วง nZ จะมีตัวหารของศูนย์ ถ้า n ไม่ใช่จำนวนเฉพาะ

..............ข) ทุก ๆ สนามเป็นโดเมนเชิงจำนวนเต็ม

..............ค) ลักษณะเฉพาะของ nZ คือ n

..............ง) วง Z และวง nZ ถอดแบบกัน สำหรับทุก ๆ $n \geqslant 1$

..............จ) กฎการตัดออกเป็นจริงในทุก ๆ วงที่ถอดแบบกับโดเมนเชิงจำนวนเต็ม

..............ฉ) ทุก ๆ โดเมนเชิงจำนวนเต็มที่มีลักษณะเฉพาะ 0 มีสมาชิกเป็นจำนวนอนันต์

..............ช) ตัวหารของศูนย์ในวงซึ่งสอดคล้องกฎการสลับที่ที่มี unity สามารถจะไม่มีตัวผกผันสำหรับการคูณ

..............ซ) nZ เป็นโดเมนย่อยของ Z

..............ฌ) Z เป็นสนามย่อยของ Q

2) จงหาคำตอบของสมการ $x^3 - 2x^2 - 3x = 0$ ใน Z_{12}

3) จงหาค่าของ x ที่สอดคล้องกับสมการ $3x = 2$ ในสนาม Z_7 และสนาม Z_{23}

4) จงหาลักษณะเฉพาะของแต่ละวงต่อไปนี้

ก) $2Z$

ข) $Z + Z$

ค) $Z_3 + 3Z$

ง) $Z_3 + Z_3$

จ) $Z_3 + Z_4$

ฉ) $Z_6 + Z_{15}$

5) จงหาคำตอบทั้งหมดของสมการ (1) $x^2 + 2x + 2 = 0$ ใน Z_6

(2) $x^2 + 2x + 4 = 0$ ใน Z_6