บทที่ 1
วงและสนาม
(Rings and fields)

1.1 วง (Rings)

มีเซตที่เราคุ้นเคยหลายเซต เช่น Z, Q, R ซึ่งมีการดำเนินการทวิภาค 2 อย่าง คือ การบวก (+) และการคูณ (.) แม้ว่าเซตเหล่านี้จะเป็นกลุ่มภายใต้การดำเนินการบวกเพียงอย่างเดียว เซต Z, Q, R กับการดำเนินการคูณ (.) มีลักษณะเฉพาะที่แตกต่างอย่างมาก เซต $R - \{0\}$ และ $Q - \{0\}$ เป็นกลุ่มภายใต้การดำเนินการทวิภาค . ในขณะที่ $Z - \{0\}$ ไม่เป็น กฎการตัดออกภายใต้การคูณเป็นจริงสำหรับเซต $Z - \{0\}$

ในบทนี้และบทต่อ ๆ ไป เราจะศึกษาและพิจารณาเซตกับการดำเนินการทวิภาคซึ่งสอดคล้องกับคุณสมบัติที่แน่นอนชุดหนึ่ง เหมือนกับที่เราได้ทำไปแล้วในการศึกษาเรื่องกลุ่ม โครงสร้างทางพีชคณิตอันใหม่นี้เราเรียกว่า วง

นิยาม วง $(R, +, .)$ คือ เซต $R \neq \phi$ กับการดำเนินการทวิภาค ซึ่งนิยมเขียนแทนด้วย + (การบวก) และ . (การคูณ) ที่สอดคล้องกับคุณสมบัติต่อไปนี้

1. $(R, +)$ เป็นกลุ่มอาบีเลียน
2. ถ้า $a, b, c \in R$ แล้ว $(a . b) . c = a . (b . c)$
3. ถ้า $a, b, c \in R$ แล้ว $a . (b + c) = ab + ac$ และ $(a + b)c = ac + bc$

ขอให้สังเกตว่าจากนิยามการดำเนินการทวิภาค + และ . อาจจะสอดคล้องหรือไม่สอดคล้องกฎการสลับที่ และเนื่องจากการดำเนินการ . เป็นการดำเนินการทวิภาค ดังนั้น

การดำเนินการ . บน R สอดคล้องกฎการปิด และคุณสมบัติข้อ 2 คือ กฎการเปลี่ยนกลุ่มสำหรับการคูณ คุณสมบัติข้อ 3 คือ กฎการแจกแจง

ก่อนจะพิจารณาตัวอย่างขอให้นิยามอีก 2 นิยามดังนี้

นิยาม ให้ $(R, +, .)$ เป็นวง จะเรียก R ว่า วงที่สอดคล้องกฎการสลับที่ เมื่อ $a \cdot b = b \cdot a \ \forall a, b \in R$

นิยาม ให้ $(R, +, .)$ เป็นวง จะกล่าวว่า R เป็นวงที่มี unity เมื่อมี $e \in R$ ซึ่ง e ไม่ใช่เอกลักษณ์สำหรับการบวก และ $e \cdot r = r \cdot e = r \ \forall r \in R$

ตัวอย่าง 1.1.1 ถ้า $Z = \{$จำนวนเต็ม$\}$ แล้ว $(Z, +, .)$ เป็นวงอนันต์ (infinite) ที่มี unity และสอดคล้องกฎการสลับที่

ตัวอย่าง 1.1.2 ให้ $E = \{$จำนวนเต็มคู่$\} = \{2n | n \in Z\}$ แล้ว $(E, +, .)$ เป็นวงอนันต์ที่ไม่มี unity แต่สอดคล้องกฎการสลับที่

ตัวอย่าง 1.1.3 ให้ $Q = \{$จำนวนตรรกยะ$\}$, $R = \{$จำนวนจริง$\}$ และ $C = \{$จำนวนเชิงซ้อน$\}$ แล้ว $(Q, +, .)$, $(R, +, .)$, $(C, +, .)$ เป็นวงอนันต์ที่มี unity และสอดคล้องกฎการสลับที่

ตัวอย่าง 1.1.4 ให้ $Z_6 = \{0, 1, 2, 3, 4, 5\}$ แล้ว $(Z_6, +_6, .6)$ เป็นวงจำกัดที่มี unity และสอดคล้องกฎการสลับที่ โดยที่ $+_6$ และ $.6$ เป็นการบวกและการคูณ modulo 6

ตัวอย่าง 1.1.5 ให้ $A = \{0, 2, 4\}$ แล้ว $A \subset Z_6$ และ $(A, +_6, .6)$ เป็นวงจำกัดที่มี unity และสอดคล้องกฎการสลับที่ (นักศึกษาทราบไหมว่า unity คือ สมาชิกตัวใดของ A)

ตัวอย่าง 1.1.6 ให้ $A \subset Z_8$ และกำหนด $A = \{0, 2, 4, 6\}$ แล้ว $(A, +_8, \cdot_8)$ เป็นวงจำกัดที่ไม่มี unity แต่สอดคล้องกฎการสลับที่

ข้อสังเกต ถ้า n เป็นจำนวนเต็มบวกแล้ว $(Z_n, +_n, \cdot_n)$ เป็นวงอนันต์ที่มี unity และสอดคล้องกฎการสลับที่

ทฤษฎี 1.1.1

ถ้า R เป็นวงแล้ว

1) $a0 = 0a = 0$ สำหรับทุก ๆ $a \in R$

2) $a(-b) = (-a)b = -(ab)$ สำหรับทุก ๆ $a, b \in R$

3) $(-a)(-b) = ab$ สำหรับทุก ๆ $a, b \in R$

พิสูจน์

ถ้า $a \in R$ แล้ว

$$a0 = a(0 + 0)$$
$$= a0 + a0$$

ดังนั้น $0 = a \cdot 0$

ทำนองเดียวกัน เราจะได้

$$0 = 0a$$

$\therefore \quad a0 = 0a = 0$

ถ้า $a, b \in R$ แล้ว

$$a(-b) + ab = a[(-b) + b]$$
$$= a0$$
$$= 0$$

ดังนั้น $\quad a(-b) = -(ab)$

และ $(-a)b + ab = (-a + a)b$

$= Ob$

$= 0$

$(-a)b = -(ab)$

. $a(-b) = (-a)b = -(ab)$

ถ้า $a, b \in R'$

$(-a)(-b) = -[a(-b)]$

$= -[-(ab)]$

$= ab$ #

นิยาม ให้ $(R, +, .)$ เป็นวงที่มี unity จะเรียก $0 \neq u \in R$ ว่า unit ก็ต่อเมื่อ u มีตัวผกผันสำหรับการดำเนินการ . ใน R

1.2 วงย่อย (Subrings)

ในตอนที่ศึกษาเรื่องกลุ่มนักศึกษาคงพบหลักว่า ถ้า H เป็นเซตย่อยของกลุ่ม $(G, *)$ แล้วเพื่อจะดูว่า $(H, *)$ เป็นกลุ่มย่อยของ $(G, *)$ หรือไม่ เราทำเพียงตรวจสอบเงื่อนไขพิเศษเงื่อนไขเดียว คือ $a * b^{-1} \in H$ สำหรับ $a, b \in H$ (เพื่อดูว่า H เองภายใต้ * เป็นกลุ่มหรือไม่) ในกรณีที่ขยายกลุ่มขึ้นมาเป็นวงก็เช่นเดียวกัน เราจะพยายามหาเงื่อนไขที่น้อยที่สุดที่เซตย่อยของวงใด ๆ จะเป็นวงย่อยของวงนั้น

นิยาม ให้ $(R, +, .)$ เป็นวงแล้วเซตย่อย S ของ R จะเป็นวงย่อยของ R ก็ต่อเมื่อ $(S, +, .)$ เป็นวง

ในการพิจารณาว่าเซตย่อย S ของวง R จะเป็นวงย่อยของวง R หรือไม่ ก่อนอื่นเลยเราจะต้องตรวจสอบดูก่อนว่า (S, +) เป็นกลุ่มย่อยของ (R, +) หรือไม่ นักศึกษาคงยังจำได้จากการศึกษาเรื่องกลุ่มว่า (S, +) จะเป็นกลุ่มย่อยของ (R, +) ก็ต่อเมื่อ $a + (-b) = a - b \in S$ สำหรับทุก ๆ $a, b \in S$ จึงน่าคิดต่อไปว่ามีคุณสมบัติอื่นใดอีกที่เราจะต้องตรวจสอบเพื่อแสดงว่า (S, +, .) เป็นวง

ตัวอย่าง 1.2.1 ถ้า R = {จำนวนจริง} แล้ว Q และ Z เป็นวงย่อยของ R

ตัวอย่าง 1.2.2 วง E ตามตัวอย่าง 1.1.2 เป็นวงย่อยของวง (Z, +, .)

ตัวอย่าง 1.2.3 วง $(A_6, +_6, .6)$ ตามตัวอย่าง 1.1.5 เป็นวงย่อยของวง $(Z_6, +_6, .6)$

ตัวอย่าง 1.2.4 วง $(A_8, +_8, .8)$ ตามตัวอย่าง 1.1.6 เป็นวงย่อยของวง $(Z_8, +_8, .8)$

นิยาม วงย่อย S ของวง R จะเป็นวงย่อยแท้ (proper subring) ก็ต่อเมื่อ $S \neq \{0\}$ และ $S \neq R$

ทฤษฎี 1.2.1 ให้ (R, +, .) เป็นวง เซตย่อย S ของ R จะเป็นวงย่อยของ R ก็ต่อเมื่อ

1. $0 \in S$
2. $(a - b) \in S$ สำหรับทุก ๆ $a, b \in S$
3. $ab \in S$ สำหรับทุก ๆ $a, b \in S$

พิสูจน์ $\Rightarrow$ สมมติ (S, +, .) เป็นวงย่อยของวง (R, +, .)

$\therefore$ (S, +) เป็นกลุ่มย่อยของ (R, +)

$\therefore 0 \in S$

และ $(a - b) \in S$ สำหรับทุก ๆ $a, b \in S$

ให้ $a, b \in S$

แต่ $(S, +, .)$ เป็นวงย่อย

ดังนั้น $(S, +, .)$ เป็นวง

$\therefore ab \in S$

$\Leftarrow$ สมมติเงื่อนไขต่อไปนี้เป็นจริงคือ

1) $0 \in S$

2) $(a - b) \in S$ สำหรับทุก ๆ $a, b \in S$

3) $ab \in S$ สำหรับทุก ๆ $a, b \in S$

$\because 0 \in S$

$\therefore S \neq \phi$

และ $(a - b) \in S$ สำหรับทุก ๆ $a, b \in S$

$\therefore (S, +)$ เป็นกลุ่มย่อยของ $(R, +)$

ให้ $a, b \in S$

$\therefore a, b \in R$

ดังนั้น $a + b = b + a$

$\therefore$ การบวกบน S สอดคล้องกฎการสลับที่

$(S, +)$ เป็นกลุ่มอาบีเลียน

ให้ $a, b, c \in S$

$\therefore a, b, c \in R$

$a(bc) = (ab)c$

การ . สอดคล้องกฎการเปลี่ยนกลุ่มบน S

และ $a(b + c) = ab + ac$

และ $(a + b)c = ac + bc$

แสดงว่า กฎการแจกแจงเป็นจริงบน S

$\therefore (S, +, .)$ เป็นวง

เนื่องจาก $S \subseteq R$

$\therefore (S, +, .)$ เป็นวงย่อยของ $(R, +, .)$

ทฤษฎี 1.2.2

ถ้า R เป็นวงแล้วเงื่อนไขต่อไปนี้สมมูลกัน คือ

1) S เป็นวงย่อยของ R

2) (ก) $(S, -)$ เป็นกลุ่มย่อยของ R

(ข) $ab \in S$ สำหรับ ทุก ๆ $a, b \in S$

3) (ก) S เป็นเซตย่อยที่ไม่ใช่เซตว่างของ R

(ข) $(a + b) \in S$ สำหรับ ทุก ๆ $a, b \in S$

(ค) $-a \in S$ สำหรับ ทุก ๆ $a \in S$

(ง) $ab \in S$ สำหรับ ทุก ๆ $a, b \in S$

4) (ก) S เป็นเซตย่อยที่ไม่ใช่เซตว่างของ R

(ข) $(a - b) \in S$ สำหรับ ทุก ๆ $a, b \in S$

(ค) $ab \in S$ สำหรับ ทุก ๆ $a, b \in S$

พิสูจน์ (1) $\Rightarrow$ (2)

สมมติ S เป็นวงย่อยของวง R

$\therefore$ $(S, +)$ เป็นกลุ่มย่อยของกลุ่ม $(R, +)$

ให้ $a, b \in S$

เนื่องจาก $(S, +, .)$ เป็นวงย่อยของวง $(R, +, .)$

ดังนั้น $(S, +, .)$ เป็นวง

$\therefore$ $ab \in S$

พิสูจน์ (2) $\Rightarrow$ (3)

สมมติ คุณสมบัติต่อไปนี้เป็นจริงคือ

(ก) $(S, +)$ เป็นกลุ่มย่อยของ $(R, +)$

(ข) $ab \in S$ สำหรับทุก ๆ $a, b \in S$

$\because$ $(S, +)$ เป็นกลุ่มย่อยของ $(R, +)$

$\therefore$ $(S, +)$ เป็นกลุ่ม

ดังนั้น $S \neq \phi$ และ $S \subseteq R$

และ $(a + b) \in S$ สำหรับทุก ๆ $a, b \in S$

และ สำหรับแต่ละ $a \in S$ จะต้องมี $-a \in S$

พิสูจน์ (3) $\Rightarrow$ (4)

สมมติคุณสมบัติต่อไปนี้เป็นจริงคือ

(ก) S เป็นเซตย่อยที่ไม่ใช่เซตว่างของ R

(ข) $a + b \in S$ สำหรับทุก ๆ $a, b \in S$

(ค) $-a \in S$ สำหรับทุก ๆ $a \in S$

(ง) $ab \in S$ สำหรับทุก ๆ $a, b \in S$

เนื่องจาก S เป็นเซตย่อยที่ไม่ใช่เซตว่างของ R

และจากข้อ ข และ ค

ให้ $a, b \in S \Rightarrow -a \in S$

$\therefore a + (-a) = 0 \in S$

$\therefore (S, +)$ เป็นกลุ่มย่อยของ $(R, +)$

$\therefore (a - b) \in S$ สำหรับทุก $a, b \in S$

พิสูจน์ (4) $\Rightarrow$ (1)

สมมติคุณสมบัติต่อไปนี้เป็นจริงคือ

(ก) S เป็นเซตย่อยที่ไม่ใช่เซตว่างของ R

(ข) $(a - b) \in S$ สำหรับ $a, b \in S$

(ค) $ab \in S$ สำหรับ $a, b \in S$

$\because$ S เป็นเซตย่อยที่ไม่ใช่เซตว่างของ R

และ $(a - b) \in S$ สำหรับ $a, b \in S$

$\therefore$ $(S, +)$ เป็นกลุ่มย่อยของ $(S, +)$

ให้ $a, b \in S$

$\therefore$ $a, b \in R$

$\therefore$ $a + b = b + a$

$\therefore$ การบวกบน S สอดคล้องกฎการสลับที่

$(S, +)$ เป็นกลุ่มอาบีเลียน

ให้ $a, b, c \in S$

$\therefore$ $a, b, c \in R$

$\therefore$ $a(bc) = a(bc)$

และ $a(b + c) = ab + ac$

และ $(a + b)c = ac + bc$

$\therefore$ การคูณบน S สอดคล้องกฎการเปลี่ยนกลุ่ม

และ กฎการแจกแจงบน S เป็นจริง

$\therefore$ $(S, +, .)$ เป็นวงย่อยของ $(R, +, .)$

ข้อสังเกต ถ้า R เป็นวงแล้ว

1. R เป็นวงย่อยของ R
2. $\{0\}$ เป็นวงย่อยของ R
3. ถ้า S เป็นวงย่อยของวงที่สอดคล้องกฎการสลับที่แล้ว S เป็นวงที่สอดคล้องกฎการสลับที่ด้วย
4. ถ้า S เป็นวงย่อยของ R แล้ว เอกลักษณ์สำหรับการบวกของ S คือ เอกลักษณ์สำหรับการบวกของ R

5. ถ้า S เป็นวงย่อยของ R และ T เป็นวงย่อยของ S แล้ว T เป็นวงย่อยของ R

1.3 สนาม (Fields)

จากตัวอย่างในเรื่องวง นักศึกษาพบแล้วว่ามีวงบางวงที่เป็นวงที่มี unity และสอดคล้องกฎการสลับที่ และยิ่งกว่านั้นสมาชิกตัวที่ไม่ใช่เอกลักษณ์สำหรับการดำเนินการบวกทุกตัวยังมีตัวผกผันสำหรับการคูณด้วย วงที่มีคุณสมบัติพิเศษอย่างนี้มีชื่อเรียกว่า สนาม (field)

นิยาม ให้ (R, +, .) เป็นวงที่มี unity จะเรียก R ว่าวงการหาร (Division ring) ก็ต่อเมื่อสมาชิกที่ไม่ใช่ศูนย์ของ R ทุกตัวเป็น unit

วงการหารบางครั้ง เรียก skew field

นิยาม ให้ (F, +, .) เป็นวงที่สอดคล้องกฎการสลับที่ จะเรียก F ว่า สนาม (field) ก็ต่อเมื่อ (F, +, .) เป็นวงการหาร

ตัวหาร 1.3.1 ให้ Q = {จำนวนตรรกยะ} แล้ว (Q, +, .) เป็นสนาม

ตัวอย่าง 1.3.2 ให้ Z = {จำนวนเต็ม} แล้ว (Z, +, .) ไม่เป็นสนาม (ทำไม)

ตัวอย่าง 1.3.3 ให้ R = {จำนวนจริง} แล้ว (R, +, .) เป็นสนาม

ตัวอย่าง 1.3.4 ให้ C = {จำนวนเชิงซ้อน} แล้ว (C, +, .) เป็นสนาม

ทฤษฎี 1.3.1 ให้ R เป็นวงที่มี unity และสอดคล้องกฎการสลับที่ แล้ว R จะเป็นสนามก็ต่อเมื่อสำหรับทุก ๆ a, b $\in$ R ซึ่ง a $\neq$ 0 สมการ ax = b มีคำตอบ x $\in$ R

$\Rightarrow$ สมมติ $(R, +, .)$ เป็นสนาม

ให้ $a, b \in R$ โดยที่ $a \neq 0$

เนื่องจาก R เป็นสนาม

$\therefore$ a เป็น unit $\in R \Rightarrow$ มี $a^{-1} \in R$

ดังนั้น สมการ $ax = b$

$x = a^{-1}b \in R$

$\Leftarrow$ สมมติสำหรับ $a, b \in R$ ซึ่ง $a \neq 0$ สมการ $ax = b$

$x = a^{-1}b \in R$

แต่ R เป็นวงที่มี unity

$\because$ R ต้องปิดภายใต้การ .

และ $0 \neq a \in R, b \in R, a^{-1}b \in R$

$\therefore$ $a^{-1} \in R$

แต่ $a^{-1}a = aa^{-1} = 1$

$\therefore$ a เป็น unit

แสดงว่า R เป็นวงที่มี unity, สอดคล้องกฎการสลับที่และสมาชิกที่ไม่ใช่ 0 เป็น unit

ดังนั้น R เป็นสนาม #

นิยาม เซตย่อย S ของสนาม $(F, +, .)$ จะเรียกว่าสนามย่อย (subfield) ของ F ก็ต่อเมื่อ $(S, +, .)$ เป็นสนาม

นิยาม ถ้า F เป็นสนาม K เป็นสนามย่อยของ F $\ni$ K อยู่ในทุก ๆ สนามย่อยของ F แล้ว เรียก K ว่า สนามย่อยจำนวนเฉพาะ (prime subfield) ของ F

นิยาม ฟังก์ชัน monomorhism ψ ของวง R กับวง S คือ ฟังก์ชันหนึ่งต่อหนึ่งจาก R ไปยัง S และสำหรับทุก ๆ a, b $\in$ R

1. $\psi(a + b) = w(a) + \psi(b)$
2. $\psi(ab) = \psi(a)\,\psi(b)$

นิยาม ถ้า ψ เป็นฟังก์ชัน monomorphism จากวง R ไปในวง S และเป็นฟังก์ชันทั่วถึง จะเรียก ψ ว่า ฟังก์ชันถอดแบบ และเรียกวง R และ S ว่า วงถอดแบบกัน ใช้สัญลักษณ์ $R \cong S$

แบบฝึกหัดที่ 1

1) จงพิจารณาข้อความแต่ละข้อต่อไปนี้เป็นจริงหรือเป็นเท็จ

.....ก) ทุกสนามเป็นวงด้วย

.....ข) ทุก ๆ วงมีเอกลักษณ์สำหรับการคูณ

.....ค) ทุก ๆ วงที่มียูนิตี้มียูนิตอย่างน้อยสองตัว

.....ง) ทุก ๆ วงที่มียูนิตี้มียูนิตอย่างมากที่สุดสองตัว

.....จ) เป็นไปได้ที่เซตย่อยของสนามบางสนามอาจเป็นวงแต่ไม่เป็นสนามย่อย

.....ฉ) กฎการแจกแจงไม่สำคัญสำหรับการเป็นวง

.....ช) การคูณในสนามสอดคล้องกฎการสลับที่

.....ซ) เซตสมาชิกที่ไม่ใช่ 0 ของสนามเป็นกลุ่มภายใต้การคูณ

.....ฌ) การบวกในทุก ๆ วงสอดคล้องกฎการสลับที่

.....ญ) ทุก ๆ สมาชิกในวงมีตัวผกผันสำหรับการบวก

2) จงพิจารณาว่าเซตใดต่อไปนี้ กับการดำเนินการที่กำหนดเป็นวง และถ้าไม่เป็นวงให้บอกเหตุผลด้วย

ก) nZ กับการบวก และการคูณธรรมดา

ข) Z^+ กับการบวกและการคูณธรรมดา

ค) $Z + Z$ กับการบวกและการคูณ (เป็นส่วน)

ง) $2Z + Z$ กับการบวกและการคูณ (เป็นส่วน)

จ) $\{a + b\sqrt{2} | a, b \in Z\}$ กับการบวกและการคูณธรรมดา

ฉ) $\{a + b\sqrt{2} | a, b \in Q\}$ กับการบวกและการคูณธรรมดา

3) สำหรับแต่ละข้อในข้อ 2 ที่เป็นวง จงบอกว่าเป็นวงที่สอดคล้องกฎการสลับที่, มี *unity* และเป็นสนามหรือไม่

4) จงบอก unit ของแต่ละวงต่อไปนี้

ก) Z

ข) $Z + Z$

ค) Z_5

ง) Q

จ) $Z + Q + Z$

ฉ) Z_4

4) จงแสดงว่า ถ้า U เป็นเซตของ unit ทั้งหมดของวง $(R, +, .)$ ซึ่งเป็นวงที่มี unity แล้ว $(U, .)$ เป็นกลุ่ม

5) จงยกตัวอย่างวงที่มี unity 1 ซึ่งมีวงย่อยที่มี unity $1' \neq 1$