# บทที่ 3

# ริงและสับริง

# (Ring and Subring)

ในบทนี้จะศึกษาเกี่ยวกับระบบพีชคณิตที่เรียกว่า ริง ซึ่งจะแตกต่างจากกรุ๊ปโดยที่ในริงจะมีไบนารี่โอเปอร์เรชันสองโอเปอร์เรชัน แต่ในกรุ๊ปจะมีเพียงหนึ่งไบนารี่โอเปอร์เรชันเท่านั้น ในบทนี้จะให้นิยามของริงและสับริง และพิสูจน์ทฤษฎีเบื้องต้นของริง พร้อมทั้งให้ตัวอย่าง และในหัวข้อสุดท้าย จะกล่าวถึงโฮโมมอร์ฟิซึมของริง

## 3.1 ริง (Ring)

**นิยาม 3.1.1** ให้ R เป็นเซ็ตที่ไม่ว่าง กำหนดให้ + และ . เป็นไบนารี่โอเปอร์เรชันที่เรียกว่า การบวก (addition) และการคูณ (Multiplication) ตามลำดับในเซ็ต R จะเรียก (R, +, .) ว่าเป็นริง ถ้า + และ . มีความสอดคล้องตามคุณสมบัติต่อไปนี้

1. $(a + b) + c = a + (b + c)$ สำหรับทุกๆ $a, b, c \in R$
2. มี $a' \in R$ ซึ่ง $a' + a = a = a + a'$ สำหรับทุกๆ $a \in R$ และเรียกสมาชิก $a'$ ว่าเป็นสมาชิกเอกลักษณ์สำหรับการบวก (additive identity) ซึ่งเขียนแทนด้วย 0
3. สำหรับแต่ละ $a \in R$ จะมี $x \in R$ ซึ่ง $x + a = 0 = a + x$ และเรียกสมาชิก x ว่าเป็นอินเวอร์สสำหรับการบวก (additive inverse) ของ a ซึ่งเขียนแทนด้วย $-a$
4. $a + b = b + a$ สำหรับทุกๆ $a, b \in R$
5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ สำหรับทุกๆ $a, b, c \in R$

6. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ และ $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ สำหรับทุกๆ $a, b, c \in R$

<u>หมายเหตุ</u> 1. เนื่องจากไบนารี่โอเปอร์เรชัน มีคุณสมบัติปิดแล้ว ดังนั้นจึงไม่ได้กล่าวถึงคุณสมบัติปิดในนิยาม 3.1.1

2. จะเขียนริง $(R, +, \cdot)$ แทนด้วย $R$

3. จะเขียน $a \cdot b$ แทนด้วย $ab$ สำหรับทุกๆ $a, b \in R$

4. สำหรับคุณสมบัติข้อ 1 – 4 แสดงว่า $(R, +)$ เป็นอบีเลียนกรุ๊ป

5. จากทฤษฎี 2.3.2 จะได้ว่าสมาชิกเอกลักษณ์สำหรับการบวก จะมีเพียงตัวเดียวเท่านั้น

6. จากทฤษฎี 2.3.2 จะได้ว่าอินเวอร์สของการบวกของแต่ละสมาชิกใน $R$ จะมีเพียงตัวเดียวเท่านั้น

<u>นิยาม 3.1.2</u> ให้ $R$ เป็นริง จะเรียกว่า $R$ เป็นริงที่มียูนิตี้ (unity) ถ้ามี $e \in R$ ซึ่ง $ae = a = ea$ สำหรับทุกๆ $a \in R$ และเรียก $e$ ว่ายูนิตี้ของ $R$

<u>นิยาม 3.1.3</u> ให้ $R$ เป็นริงที่มียูนิตี้ $e$ จะเรียก $R$ ว่าเป็นดิวิชันริง (Division Ring) ถ้าสำหรับแต่ละ $0 \neq a \in R$ จะมี $x \in R$ ซึ่ง $ax = e = xa$ และเรียก $x$ ว่าเป็นอินเวอร์สสำหรับการคูณของ $a$ (multiplicative inverse of $a$) ซึ่งจะเขียนแทนด้วย $a^{-1}$

<u>นิยาม 3.1.4</u> ให้ $R$ เป็นริงจะเรียก $R$ ว่าเป็นคอมมิวเทที่พริง (Commutative Ring) ถ้า $ab = ba$ สำหรับทุกๆ $a, b \in R$

ถ้า $cd \neq dc$ สำหรับบางสมาชิก $c, d \in R$ จะเรียก $R$ ว่า เป็นนอนคอมมิวเทที่พริง (Non - commutative Ring)

ตัวอย่าง 3.1.1 ให้ I เป็นเซ็ตของจำนวนเต็ม (integers) มีการบวกธรรมดา และการคูณธรรมดา เป็นไบนารี่โอเปอร์เรชัน จะได้ว่า I เป็นคอมมิวเทตีฟริงที่มียูนิตี้เป็น 1

ตัวอย่าง 3.1.2 ถ้าให้ E เป็นเซ็ตของจำนวนเต็มคู่ มีการบวกธรรมดา และการคูณธรรมดาเป็นไบนารี่โอเปอร์เรชัน จะได้ว่า E เป็นคอมมิวเทตีฟริงที่ไม่มียูนิตี้

ตัวอย่าง 3.1.3 ให้ Q เป็นเซ็ตของจำนวนตรรกยะ (rational numbers) ซึ่งมีการบวกธรรมดาและการคูณธรรมดา เป็นไบนารีโอเปอร์เรชัน จะได้ว่า Q เป็นคอมมิวเทตีฟริงที่มียูนิตี้เป็น 1

ตัวอย่าง 3.1.4 เซ็ตของจำนวนจริง (Real numbers) และเซ็ตของจำนวนเชิงซ้อน (Complex numbers) ซึ่งมีการบวกธรรมดา และการคูณธรรมดาเป็นไบนารี่โอเปอร์เรชันเป็นริงเช่นกัน

ตัวอย่าง 3.1.5 ให้ $R = \{x + 2y / x , y \in I\}$ เมื่อ I เป็นเซ็ตของจำนวนเต็ม ซึ่งมีการบวกธรรมดา และการคูณธรรมดา เป็นไบนารี่โอเปอร์เรชัน จะได้ว่า R เป็นคอมมิวเทตีฟริง ที่มียูนิตี้เป็น 1

ตัวอย่าง 3.1.6 ให้ $R = \{0\}$ ซึ่งกำหนดการบวกและการคูณเป็น $0 + 0 = 0$ และ $0 \cdot 0 = 0$ ตามลำดับ จะได้ว่า R เป็นริงซึ่งเรียกว่าทริเวียลริง (Trivial Ring) หรือซีโรริง (Zero ring)

หมายเหตุ จากตัวอย่าง 3.1.6 นี้จะเห็นว่า 0 ทำหน้าที่เป็นทั้งสมาชิกเอกลักษณ์ของการบวก และยูนิตี้ ซึ่งจะเป็นเพียงกรณีเดียวในริง $\{0\}$ นี้เท่านั้น เพราะฉะนั้นโดยทั่วๆไปเมื่อกล่าวถึงยูนิตี้ จะไม่รวมถึงกรณีที่เป็นทริเวียลริง โดยสมมุติว่ายูนิตี้เป็นสมาชิกที่ไม่ใช่ศูนย์

<u>ตัวอย่าง 3.1.7</u> ให้ $R = \{u,v,w,x\}$ โดยกำหนดการบวกและการคูณบนเซ็ต R ดังนี้ตารางต่อไปนี้

| + | u | v | w | x |
|---|---|---|---|---|
| u | u | v | w | x |
| v | v | u | x | w |
| w | w | x | u | v |
| x | x | w | v | u |

| • | u | v | w | x |
|---|---|---|---|---|
| u | u | u | u | u |
| v | u | v | w | x |
| w | u | w | w | u |
| x | u | x | u | x |

จะได้ว่า R เป็นคอมมิวเทที่พริงซึ่งมี u เป็นสมาชิกเอกลักษณ์สำหรับการบวกของ R และ v เป็นยูนิตี้

<u>ตัวอย่าง 3.1.8</u> ให้ R เป็นเซ็ตของอีควิวาเลนซ์คลาสของจำนวนเต็มมอดูโล 7 นั่นคือเซ็ต R ประกอบด้วยสมาชิก $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}$ จะได้ว่า R เป็นคอมมิวเทที่พริง และมียูนิตี้เป็น $\bar{1}$

<u>ทฤษฎี 3.1.1</u> กฎการตัดออกสำหรับการบวก (Cancellation Law of addition)

ให้ a , b และ c เป็นสมาชิกของริง R

1. ถ้า $a + c = b + c$ แล้วจะได้ $a = b$
2. ถ้า $c + a = c + b$ แล้วจะได้ $a = b$

<u>พิสูจน์</u> 1. เนื่องจาก $a + c = b + c$

และจากคุณสมบัติของริง จะมีสมาชิก $t \in R$ ซึ่ง

$$c + t = 0$$

ดังนั้น $(a + c) + t = (b + c) + t$

$a + (c + t) = b + (c + t)$

$a + 0 = b + 0$

$a = b$

2. พิสูจน์ในทำนองเดียวกันกับข้อ 1

<u>ทฤษฎี 3.1.2</u> ให้ R เป็นริงใดๆที่มี 0 เป็นสมาชิกเอกลักษณ์สำหรับการบวกจะได้ว่า

$a0 = 0a = 0$ สำหรับทุกๆ $a \in R$

<u>พิสูจน์</u> ให้ $a \in R$

ดังนั้น $a = a + 0 = 0 + a$

เอา a คูณทั้ง 2 ข้างของสมการข้างบนนี้

จะได้ $aa = (a + 0)a$

$= aa + 0a$

แต่ $aa + 0 = aa$

ดังนั้น $aa + 0 = aa + 0a$

จากทฤษฎี 3.1.1 จะได้ $0 = 0a$

ในทำนองเดียวกันพิสูจน์ได้ว่า $0 = a0$

<u>หมายเหตุ</u> ต่อไปจะเขียน $a - b$ แทน $a + (-b)$ สำหรับ a , b ที่เป็นสมาชิกใน ริง R

<u>ทฤษฎี 3.1.3</u> กำหนดให้ a , b , c เป็นสมาชิกของริง R จะได้ว่า

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

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

4. $a(b - c) = (ab) - (ac)$

5. $(a - b)c = (ac) - (bc)$

<u>พิสูจน์</u> 1. จะแสดงว่า $a(-b)$ เป็นอินเวอร์สสำหรับการบวกของ $ab$ หรือ

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

พิจารณา $ab + a(-b) = a[b + (-b)]$

$= a0$

$= 0$ โดยทฤษฎี 3.1.2

เนื่องจาก $ab + [-(ab)] = 0$

ดังนั้น $ab + a(-b) = ab + [-(ab)]$

โดยทฤษฎี 3.1.1. จะได้ว่า $a(-b) = -(ab)$

สำหรับข้อ 2, 3, 4, 5 เป็นแบบฝึกหัด

<u>ทฤษฎี 3.1.4</u> กำหนดให้ R เป็นริงที่มียูนิตี้ จะได้ว่ายูนิตี้ของริง R จะมีเพียงตัวเดียวเท่านั้น

<u>พิสูจน์</u> สมมุติให้ $e$ และ $e'$ เป็นยูนิตี้ใน R

เมื่อ $e$ ทำหน้าที่เป็นยูนิตี้จะได้ $ee' = e'$

และเมื่อ $e'$ ทำหน้าที่เป็นยูนิตี้จะได้ $ee' = e$

ดังนั้น $e' = e$

นั่นคือยูนิตี้ของริง R จะมีเพียงตัวเดียวเท่านั้น

<u>ทฤษฎี 3.1.5</u> กำหนดให้ R เป็นริงที่มียูนิตี้ e และ $a \in R$ โดยที่ $a \neq 0$ ถ้า a มีอินเวอร์สสำหรับการคูณแล้วจะได้ว่า อินเวอร์สสำหรับการคูณของ a มีเพียงตัวเดียวเท่านั้น

<u>พิสูจน์</u> สมมุติให้ s และ t เป็นอินเวอร์สสำหรับการคูณของ $a \in R$ ซึ่งจากนิยาม 2.1.3 จะได้ว่า

$$as = sa = e$$

และ

$$at = ta = e$$

เนื่องจาก

$$\begin{aligned} s &= se \\ &= s(at) \\ &= (sa)t \\ &= et \\ &= t \end{aligned}$$

นั่นคืออินเวอร์สสำหรับการคูณของ a มีเพียงตัวเดียวเท่านั้น

<u>บทแทรก 3.1.6</u> กำหนดให้ R เป็นริงที่มียูนิตี้ e ถ้า R ไม่ใช่ทริเวียลริง แล้ว 0 และ e จะแตกต่างกัน

<u>พิสูจน์</u> เนื่องจาก $R \neq \{0\}$

ดังนั้นจะมี $a \in R$ ซึ่ง $a \neq 0$

เนื่องจาก $ae = a$

และ $a0 = 0$

ถ้า e และ 0 เป็นตัวเดียวกันจะได้ว่า $ae = a0$

ทำให้ $a = 0$

ซึ่งจะขัดแย้งกับสมมุติฐานข้างบน

ดังนั้น $0$ และ $e$ จะต้องแตกต่างกัน

## 3.2 <u>สับริง</u> (Subring)

<u>นิยาม 3.2.1</u> ให้ $R$ เป็นริง $S$ เป็นสับเซ็ตที่ไม่เป็นเซ็ตว่าง (non-empty subset) ของ $R$ จะเรียก $S$ ว่าเป็นสับริงของ $R$ ถ้า $S$ เป็นริงภายใต้ไบนารี่โอเปอร์เรชันการบวกและการคูณของ $R$

จากนิยาม .2.1 นี้ เมื่อต้องการทราบว่าสับเซ็ตใดเป็นสับริงนั้น จะต้องแสดงว่าสับเซ็ตนั้นสอดคล้องตามคุณสมบัติของริง เพื่อความรวดเร็วในการแสดงว่าสับเซ็ตเป็นสับริง จึงได้มีทฤษฎีต่อไปนี้ สำหรับแสดงว่าสับเซ็ตนั้นเป็นสับริง

<u>ทฤษฎี 3.2.1</u> กำหนดให้ $R$ เป็นริง และ $S$ เป็นสับเซ็ตที่ไม่ว่างของ $R$ จะได้ว่า $S$ เป็นสับริงของ $R$ ก็ต่อเมื่อ

1. สำหรับ $a, b \in S$ จะได้ $a - b \in S$
2. สำหรับ $a, b \in S$ จะได้ $ab \in S$

<u>พิสูจน์</u> <u>ตอนแรก</u> สมมุติให้ $S$ เป็นสับริงของ $R$

ดังนั้น ถ้า $a, b \in S$ จะได้ว่า $-b \in S$ และ $a - b \in S$ (จากคุณสมบัติของริง)

และถ้า $a, b \in S$ จะได้ว่า $ab \in S$ (จากคุณสมบัติของไบนารี่โอเปอร์เรชัน)

<u>ตอนสอง</u> สมมุติว่าข้อ 1 และ 2 ในทฤษฎีเป็นจริง จะแสดงว่า $S$ เป็นสับริงของ $R$ เนื่องจาก $S$ เป็นสับเซ็ตที่ไม่ว่างของ $R$ ดังนั้นทุกสมาชิกใน $S$ จะสอดคล้องกับคุณสมบัติของริงข้อ 1,4,5 และ 6 ในนิยามที่ 3.1.1

ถ้า $a \in S$ จะได้ว่า $a - a \in S$ (จากข้อ 1)

นั่นคือ $0 \in S$

ถ้า $0, a \in S$ จะได้ว่า $0 - a \in S$ (จากข้อ 1)

นั่นคือ $-a \in S$

ดังนั้น S เป็นสับริงของ R

<u>ข้อสังเกต</u> 1. ถ้า S เป็นสับริงของ R จะได้ว่าสมาชิกเอกลักษณ์ของ S คือสมาชิกเอกลักษณ์ของ R และแต่ละสมาชิกในสับริง S จะมีอินเวอร์สสำหรับการบวกใน S และ R เป็นตัวเดียวกัน

2. ทุกๆริง R จะมี R และ {0} เป็นสับริงเสมอ

<u>นิยาม 3.2.2</u> จะเรียกสับริง R และ {0} ของริง R ว่า ทริเวียลสับริง (trivial subring) สำหรับสับริงอื่นๆของ R จะเรียกว่านอนทริเวียลสับริง หรือสับริงแท้ (non - trivial subring or proper subring)

<u>ตัวอย่าง 3.2.1</u> ถ้าให้ E เป็นเซ็ตของจำนวนเต็มคู่จะได้ว่า E เป็นสับริงของริง I ซึ่งเป็นริงของจำนวนเต็ม

เนื่องจากถ้าให้ $2n, 2m \in E$ แล้วจะได้ว่า $2n - 2m = 2(n - m) \in E$

และ $(2n)(2m) = 2(2nm) \in E$

ดังนั้นโดยทฤษฎี .2.1 จะได้ว่า E เป็นสับริงของริง I

<u>นิยาม 3.2.3</u> เซนเตอร์ (Center) ของริง R เขียนแทนด้วย Cent R คือ $\{a \in R \mid ar = ra$ สำหรับทุกๆสมาชิก $r \in R\}$

<u>ข้อสังเกต</u> จากนิยาม 3.2.3 จะได้ว่า ริง R เป็นคอมมิวเทฑีพริงก็ต่อเมื่อ Cent R = R

<u>พิสูจน์</u> <u>ตอนแรก</u> สมมุติว่า R เป็นคอมมิวเททีพริง

ให้ $x \in R$

ดังนั้น $xr = rx$ สำหรับทุกๆสมาชิก $x , r \in R$

นั่นคือ $x \in \text{Cent } R$

ดังนั้น $R \subseteq \text{Cent } R$

และเนื่องจาก $\text{Cent } R \subseteq R$

จะได้ว่า $\text{Cent } R = R$

<u>ตอนสอง</u> สมมุติว่า $\text{Cent } R = R$

นั่นคือ $ar = ra$ สำหรับทุกๆสมาชิก $a , r \in R$

ดังนั้น R เป็นคอมมิวเททีพริง

<u>ทฤษฎี 3.2.2</u> สำหรับทุกๆริง R จะได้ว่า Cent R เป็นสับริงของ R

<u>พิสูจน์</u> จากนิยาม 3.2.3 จะได้ว่า $\text{Cent } R \subseteq R$ และไม่เป็นเซ็ตว่าง เพราะว่าอย่างน้อยจะมีสมาชิกเอกลักษณ์สำหรับการบวกของ R เป็นสมาชิกอยู่ใน Cent R

ให้ $a , b \in \text{Cent } R$

จากนิยาม 3.2.3 ได้ว่า $ar = ra$ และ $br = rb$ สำหรับทุกๆสมาชิก $r \in R$

พิจารณา
$$\begin{aligned}(a - b)r &= ar - br \\ &= ra - rb \\ &= r(a - b)\end{aligned}$$

นั่นคือ $a - b \in \text{Cent } R$

ในทำนองเดียวกันจะได้ว่า
$$\begin{aligned}(ab)r &= a(br) \\ &= a(rb) \\ &= (ar)b\end{aligned}$$

$$= (ra)b$$

$$= r(ab)$$

นั่นคือ $ab \in \text{Cent } R$

จากทฤษฎี 3.2.1 จะได้ว่า Cent R เป็นสับริงของ R

<u>หมายเหตุ</u> 1. ริงบางริงมียูนิตี้ แต่สับริงอาจจะไม่มียูนิตี้ก็ได้ เช่นริงของจำนวนเต็ม I มียูนิตี้เป็น 1 แต่ริงของเลขจำนวนเต็มคู่ ซึ่งเป็นสับริงของ I ไม่มียูนิตี้

2. ถ้าริงและสับริงต่างก็มียูนิตี้ ไม่จำเป็นจะต้องเป็นตัวเดียวกัน ดังตัวอย่างต่อไปนี้

<u>ตัวอย่าง 3.2.2</u> พิจารณาเซ็ต I x I ซึ่งประกอบด้วยสมาชิกที่เป็นคู่ลำดับของจำนวนเต็ม นั่นคือ $I \times I = \{(a, b) / a, b \in I\}$

กำหนดการบวกและการคูณบนเซ็ต I x I ดังนี้

การบวก : สำหรับ $(a, b), (c, d) \in I \times I$

$$(a, b) + (c, d) = (a + c, b + d)$$

การคูณ : สำหรับ $(a, b), (c, d) \in I \times I$

$$(a, b)(c, d) = (ac, bd)$$

จะได้ว่า I x I เป็นริงที่มียูนิตี้เป็น (1, 1) เพราะว่าสำหรับทุกๆสมาชิก $(a, b) \in I \times I$

$$(a, b)(1, 1) = (a1, b1)$$

$$= (a, b)$$

และ $$(1, 1)(a, b) = (1a, 1b)$$

$$= (a, b)$$

ต่อไปพิจารณา $I \times \{0\} = \{(a, 0) / a \in I\}$

เนื่องจาก $0 \in I$ ดังนั้นอย่างน้อยจะต้องมี $(0, 0) \in I \times \{0\}$

ดังนั้น $I \times \{0\}$ ไม่เป็นเซ็ทว่าง และ $I \times \{0\} \subsetneq I \times I$

เนื่องจาก $(0, 0)$ เป็นสมาชิกเอกลักษณ์สำหรับการบวกของ $I \times I$

สำหรับทุกๆ $(a, 0) \in I \times I$ จะมี $(-a, -0)$ เป็นอินเวอร์สสำหรับการบวกของ $(a, 0)$

เพราะว่า $(a, 0) + (-a, -0) = (0, 0)$

ดังนั้น $(-a, -0) = -(a, 0)$

หรือ $-(a, 0)$ คือ อินเวอร์สสำหรับการบวกของ $(a, 0)$

ต่อไปจะแสดงว่า $I \times \{0\}$ เป็นสับริงของ $I \times I$

สำหรับทุกๆ $(a, 0), (b, 0) \in I \times \{0\}$

พิจารณา
$$\begin{aligned}(a, 0) - (b, 0) &= (a, 0) + [-(b, 0)] \\ &= (a, 0) + (-b, -0) \\ &= (a - b), 0 - 0) \\ &= (a - b, 0)\end{aligned}$$

เนื่องจาก $a - b \in I$ ดังนั้น $(a - b, 0) \in I \times \{0\}$

พิจารณา
$$\begin{aligned}(a, 0)(b, 0) &= (ab, 00) \\ &= (ab, 0)\end{aligned}$$

เนื่องจาก $ab \in I$ ดังนั้น $(ab, 0) \in I \times \{0\}$

ดังนั้น $I \times \{0\}$ เป็นสับริงของ $I \times I$

และ $I \times \{0\}$ มียูนิตี้เป็น $(1, 0)$ เพราะว่าสำหรับทุกๆ $(a, 0) \in I \times \{0\}$

จะได้
$$\begin{aligned}(a, 0)(1, 0) &= (a1, 00) \\ &= (a, 0)\end{aligned}$$

และ $(1, 0)(a , 0) = (1a , 00)$

$= (a , 0)$

จากตัวอย่างนี้จะเห็นว่าริง $I \times I$ และสับริง $I \times \{0\}$ ของ $I \times I$ ต่างก็มียูนิตี้ซึ่งแตกต่างกัน

แบบฝึกหัด 3 ก

1. กำหนดให้ $I$ เป็นเซ็ตของจำนวนเต็ม จงพิจารณาว่าเซ็ตและไบนารี่โอเปอร์เรชันซึ่งกำหนดให้ในแต่ละข้อต่อไปนี้ เซ็ตใดเป็นริง , เซ็ตใดเป็นริงที่มียูนิตี้, เซ็ตใดเป็นดิวิชันริง, และเซ็ตใดเป็นคอมมิวเทฟริง

ก. $M = \{m - n\sqrt{2} / m , n \in I\}$ มีการบวกและการคูณเป็นไบนารี่โอเปอร์เรชัน

ข. $K =$ เซ็ตของเมตริกซ์ขนาด $2 \times 2$ ซึ่งอยู่ในรูป $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$

โดยที่ $a , b , c \in I$ มีการบวกและการคูณของเมตริกซ์เป็นไบนารี่โอเปอร์เรชัน

ค. $T = \{(s , t , u)/s,t,u \in I\}$ กำหนดการบวกและการคูณดังต่อไปนี้

$(s , t , u) + (x , y , z) = (s + x , t + y, u + z)$

และ $(s , t , u)(x , y , z) = (sx , sy + tz , uz)$

สำหรับทุกๆสมาชิก $(s , t , u) , (x , y , z) \in T$

2. ตารางต่อไปนี้ คือตารางของการบวก และการคูณของริง $\{a, b, c, d\}$

| $+$ | a | b | c | d |
|---|---|---|---|---|
| a | a | b | c | d |
| b | b | c | d | a |
| c | c | d | a | b |
| d | d | a | b | c |

| $\cdot$ | a | b | c | d |
|---|---|---|---|---|
| a | a | a | a | a |
| b | a | – | a | c |
| c | a | a | a | – |
| d | a | c | a | – |

จงเติมลงในช่องว่างในตารางของการคูณ โดยคำนวณจากกฎของการกระจาย

3. ถ้า a และ b เป็นสมาชิกในริง R จงพิสูจน์ว่าสมการ $a + x = b$ ใน R จะมีคำตอบเพียงแบบเดียวเท่านั้นคือ $x = b - a$

4. กำหนดให้ R เป็นริงที่มียูนิตี้ ถ้า a และ b เป็นสมาชิกของ R ซึ่งมีอินเวอร์สสำหรับการคูณ จงแสดงว่า ab มีอินเวอร์สสำหรับการคูณ

5. จงแสดงตัวอย่างของสมาชิก a และ b ของริง R ซึ่งมี $a^{-1}$ และ $b^{-1}$ แต่ $(ab)^{-1} \neq a^{-1}b^{-1}$

6. กำหนดการบวก $+$ และการคูณ $\cdot$ บนเซ็ตของจำนวนเต็ม I ดังต่อไปนี้

$$m + n = m + n - 1$$

และ

$$m \cdot n = m + n - mn$$

สำหรับทุกๆสมาชิก $m, n \in I$ จงพิสูจน์ว่า I เป็นคอมมิวเททีฟริงที่มียูนิตี้

7. จงแสดงว่าอินเตอร์เซคชันของสับริงของริง R เป็นสับริงของ R

8. จงแสดงตัวอย่างของริง R ซึ่งมี S เป็นสับริงโดยมีข้อกำหนดต่อไปนี้

ก. R มียูนิตี้ แต่ S ไม่มียูนิตี้

ข. R ไม่มียูนิตี้ แต่ S มียูนิตี้

ค. R และ S มียูนิตี้ตัวเดียวกัน

ง. R และ S มียูนิตี้ที่แตกต่างกัน

จ. R เป็นนอนคอมมิวเทที่พริง และ S เป็นคอมมิวเทที่พริง

9. กำหนดให้ R เป็นคอมมิวเทที่พริง และ $a \varepsilon R$ จงพิสูจน์ว่าเซ็ต $\{x, x \varepsilon R, ax = 0\}$ เป็นสับริงของ R

10. จงพิสูจน์ว่าริง R ซึ่งมีโอเปอร์เรชันทั้งสองเหมือนกัน (นั่นคือ $a + b = ab$ สำหรับทุกๆสมาชิก $a, b \varepsilon R$) จะต้องเป็นทริเวียลริง นั่นคือ $R = \{0\}$

11. จงพิสูจน์ทฤษฎี 3.1.3 ข้อ 2, 3, 4, 5

12. จงพิสูจน์ว่า $I_n$ เป็นริง

## 3.3 <u>โฮโมมอร์ฟิซึมของริง</u> (Homomorphism of Ring)

<u>นิยาม 3.3.1</u> ให้ $\phi$ เป็นฟังก์ชันจากริง R ไปยังริง R' จะเรียก $\phi$ ว่าเป็นโฮโมมอร์ฟิซึม (Homomorphism) ถ้า

1. $\phi(a + b) = \phi(a) + \phi(b)$

2. $\phi(ab) = \phi(a)\phi(b)$

สำหรับทุกๆสมาชิก $a, b \varepsilon R$

<u>นิยาม 3.3.2</u> ถ้า $\phi$ เป็นโฮโมมอร์ฟิซึมจากริง R ไปยังริง R' แล้วเคอร์เนล(Kernel) ของ $\phi$ เขียนแทนด้วย Ker ($\phi$) คือ เซ็ตซึ่งประกอบด้วยสมาชิก $a \varepsilon R$ ซึ่ง $\phi(a) = 0'$

เมื่อ 0' คือ สมาชิกเอกลักษณ์สำหรับการบวกของ R'

นั่นคือ $\text{Ker}(\phi) = \{a \varepsilon R \,/\, \phi(a) = 0'\}$

<u>ตัวอย่าง 3.3.1</u> ให้ R เป็นริงใดๆและ $\phi$ เป็นฟังก์ชันจาก R ไปยัง R โดยกำหนด $\phi(a) = a$ สำหรับทุกๆสมาชิก $a \varepsilon R$ จงแสดงว่า $\phi$ เป็นโฮโมมอร์ฟิซึมแล้วจงหา Ker ($\phi$)

ให้ a , b ε R, พิจารณา $\emptyset(a + b) = a + b$

$= \emptyset(a) + \emptyset(b)$

และ $\emptyset(ab) = ab$

$= \emptyset(a)\,\emptyset(b)$

นั่นคือ $\phi$ เป็นโฮโมมอร์ฟิซึม

เนื่องจาก $\emptyset(0) = 0$

ดังนั้น $\mathrm{Ker}\,(\emptyset) = \{0\}$

<u>ตัวอย่าง 3.3.2</u> ให้ R และ R' เป็นริงใดๆ , $\phi$ เป็นฟังก์ชันจาก R ไปยัง R' โดยกำหนด $\emptyset(a) = 0'$ สำหรับทุกๆสมาชิก $a \in R$ และ $0'$ คือสมาชิกเอกลักษณ์ของ R'

จงแสดงว่า $\phi$ เป็นโฮโมมอร์ฟิซึมแล้ว จงหา $\mathrm{Ker}\,(\emptyset)$

ให้ $a , b \in R$

เนื่องจาก $\emptyset(a + b) = 0'$

และ $\emptyset(a) + \emptyset(b) = 0' + 0' = 0'$

ดังนั้น $\emptyset(a + b) = \emptyset(a) + \emptyset(b)$

และ $\emptyset(ab) = 0'$

$\emptyset(a)\,\emptyset(b) = 0'0' = 0'$

ดังนั้น $\emptyset(ab) = \emptyset(a)\,\emptyset(b)$

นั่นคือ $\phi$ เป็นโฮโมมอร์ฟิซึม และเรียก $\phi$ ว่าเป็นทริเวียลโฮโมมอร์ฟิซึม

เนื่องจาก $\emptyset(a) = 0'$ สำหรับทุกๆสมาชิก $a \in R$

ดังนั้น $\mathrm{Ker}\,(\emptyset) = R$

<u>ตัวอย่าง 3.3.3</u> ให้ R เป็นเซ็ตของจำนวนจริงที่อยู่ในรูป $m + n\sqrt{2}$ ซึ่ง $m, n \in I$ จะได้ว่า R เป็นริงภายใต้การบวก และการคูณ ถ้าให้ $\phi$ เป็นฟังก์ชันจาก R ไปยัง R โดยกำหนด $\phi(m + n\sqrt{2}) = m - n\sqrt{2}$ จงแสดงว่า $\phi$ เป็นโฮโมมอร์ฟิซึม และจงหา $\mathrm{Ker}(\phi)$

ให้ $m_1 + n_1\sqrt{2}, m_2 + n_2\sqrt{2} \in R$

พิจารณา

$$\begin{aligned}\phi\left((m_1 + n_1\sqrt{2}) + (m_2 + n_2\sqrt{2})\right) &= \phi[(m_1 + m_2) + (n_1 + n_2)\sqrt{2}] \\ &= (m_1 + m_2) - (n_1 + n_2)\sqrt{2} \\ &= (m_1 - n_1\sqrt{2}) + (m_2 - n_2\sqrt{2}) \\ &= \phi(m_1 + n_1\sqrt{2}) + \phi(m_2 + n_2\sqrt{2})\end{aligned}$$

และ

$$\begin{aligned}\phi\left((m_1 + n_1\sqrt{2})(m_2 + n_2\sqrt{2})\right) &= \phi\left((m_1m_2 + 2n_1n_2) + (n_1m_2 + m_1n_2)\sqrt{2}\right) \\ &= (m_1m_2 + 2n_1n_2) - (n_1m_2 + n_2m_1)\sqrt{2} \\ &= (m_1 - n_1\sqrt{2})(m_2 - n_2\sqrt{2}) \\ &= \phi(m_1 + n_1\sqrt{2})\,\phi(m_2 + n_2\sqrt{2})\end{aligned}$$

ดังนั้น $\phi$ เป็นโฮโมมอร์ฟิซึม

เนื่องจาก $\phi(0 + 0\sqrt{2}) = 0 - 0\sqrt{2}$

หรือ $\phi(0) = 0$

นั่นคือ $\mathrm{Ker}(\phi) = \{0\}$

<u>ตัวอย่าง 3.3.4</u> ให้ I เป็นริงของจำนวนเต็ม และให้ $I_n$ เป็นริงของจำนวนเต็มมอดูโล n ให้ $\theta : I \longrightarrow I_n$ ซึ่งกำหนดโดย $\theta(m) = \bar{r}, \bar{r} \in I_n$ จงแสดงว่า $\theta$ เป็นโฮโมมอร์ฟิซึม

1. จะแสดงว่า $\theta(s+t) = \theta(s) + \theta(t)$ สำหรับทุกๆ $s, t \in I$

ให้ $s, t \in I$ โดยอาศัย ดิวิชันอัลกอริทึม ใน $I$ จะได้

$$s = q_1n + r_1 \quad \text{สำหรับ} \quad 0 \leq r_1, r_2 < n$$

และ $$t = q_2n + r_2$$

นั่นคือ $$\theta(s) = \bar{r}_1 \quad \text{และ} \quad \theta(t) = \bar{r}_2$$

ดังนั้น $$\theta(s) + \theta(t) = r_1 + r_2 \quad (\text{มอดูโล } n)$$

โดยอาศัย ดิวิชันอัลกอริทึม ใน $I$ จะได้

$$r_1 + r_2 = q_3n + r_3 \quad \text{สำหรับ} \quad 0 \leq r_3 < n$$

ดังนั้น $$\theta(s) + \theta(t) = \bar{r}_3$$

พิจารณา $$s + t = (q_1 + q_2)n + (r_1 + r_2)$$

$$= (q_1 + q_2 + q_3)n + r_3 \quad \text{สำหรับ} \quad 0 \leq r_3 < n$$

ดังนั้น $$\theta(s+t) = \bar{r}_3$$

นั่นคือ $$\theta(s+t) = \theta(s) + \theta(t)$$

2. จะแสดงว่า $\theta(st) = \theta(s)\theta(t)$

จากการพิสูจน์ในตอนที่ 1 จะได้ว่า

$$\theta(s) = \bar{r}_1 \quad \text{และ} \quad \theta(t) = \bar{r}_2$$

ดังนั้น $$\theta(s)\theta(t) \equiv r_1r_2 \quad (\text{มอดูโล } n)$$

จาก ดิวิชันอัลกอริทึม จะได้ว่า

$$r_1r_2 = q_4n + r_4 \quad \text{สำหรับ} \quad 0 \leq r_4 < n$$

ดังนั้น $$\theta(s)\,\theta(t) = \bar{r}_4$$

พิจารณา $\quad st = (q_1q_2n + r_1q_2 + q_1r_2)n + r_1r_2$

$\quad\quad = (q_1q_2n + r_1q_2 + q_1r_2 + q_4)n + r_4, \; 0 \le r_4 < n$

ดังนั้น $\quad \theta(st) = \bar{r}_4$

นั่นคือ $\quad \theta(st) = \theta(s)\,\theta(t)$

ดังนั้น $\theta$ เป็นโฮโมมอร์ฟิซึม

<u>ทฤษฎี 3.3.1</u> ให้ $\phi$ เป็นโฮโมมอร์ฟิซึมจากริง R ไปยังริง R' จะได้ว่า

1. $\phi(0) = 0'$ โดยที่ 0 และ 0' เป็นสมาชิกเอกลักษณ์สำหรับการบวกของ R และ R' ตามลำดับ

2. $\phi(-a) = -\phi(a)$ สำหรับสมาชิก $a \in R$

3. ถ้า S เป็นสับริงของ R แล้ว $\phi(S)$ จะเป็นสับริงของ R'
เมื่อ $\phi(S) = \{s' \in R' / \phi(s) = s'$ เมื่อ $s \in S\}$

4. ถ้า S' เป็นสับริงของ R' แล้ว $\phi^{-1}(S')$ จะเป็นสับริงของ R
เมื่อ $\phi^{-1}(S') = \{s \in R / \phi(s) = s'$ เมื่อ $s' \in S'\}$

5. ถ้า R มียูนิตี้ e และ $\phi(e) \neq 0'$ แล้วจะได้ว่า $\phi(e)$ เป็นยูนิตี้ของ $\phi(R)$

<u>พิสูจน์</u>

1. ให้ $a \in R$ ดังนั้น $\phi(a) \in R'$

และเนื่องจาก $\quad \phi(a) + 0' = \phi(a)$

$\quad\quad = \phi(a + 0)$

$\quad\quad = \phi(a) + \phi(0)$ (เพราะว่า $\phi$ เป็นโฮโมมอร์ฟิซึม)

จึงทำให้ได้ว่า $\emptyset(a) + 0' = \emptyset(a) + \emptyset(0)$

ดังนั้น $0' = \emptyset(0)$ (โดยทฤษฎี 3.1.1)

2. จาก ข้อ 1 ได้ว่า $0' = \emptyset(0)$

$= \emptyset(a + (-a))$ สำหรับ $a \in R$

$= \emptyset(a) + \emptyset(-a)$ (เพราะว่า $\phi$ เป็นโฮโมมอร์ฟิซึม)

แต่ $\emptyset(a) + [-\emptyset(a)] = 0'$

ดังนั้น $\emptyset(a) + \emptyset(-a) = \emptyset(a) + [-\emptyset(a)]$

นั่นคือ $\emptyset(-a) = -\emptyset(a)$ (โดยทฤษฎี 3.1.1)

3. เนื่องจาก $\emptyset(S) = \{s' \in R' / \emptyset(s) = s'$ เมื่อ $s \in S\}$

ดังนั้น $\emptyset(S) \subseteq R'$

เนื่องจาก $0 \in S$ ซึ่งทำให้ได้ว่า $\phi(0) = 0' \in \phi(S)$

ดังนั้น $\emptyset(S) \neq \emptyset$

ให้ $\emptyset(s), \emptyset(t) \in \emptyset(S)$ เมื่อ $s, t \in S$

เนื่องจาก S เป็นสับริงของ R ดังนั้น $s - t \in S$ และ $st \in S$

พิจารณา $\emptyset(s) - \emptyset(t) = \emptyset(s) + (-\emptyset(t))$

$= \emptyset(s) + \emptyset(-t)$ (จากข้อ 2)

$= \emptyset(s - t) \in \emptyset(S)$

ดังนั้น $\emptyset(s) - \emptyset(t) \in \emptyset(S)$

เนื่องจาก $\emptyset(s)\emptyset(t) = \emptyset(st) \in \emptyset(S)$

นั่นคือ $\emptyset(s)\emptyset(t) \in \emptyset(S)$

ดังนั้น $\emptyset(S)$ เป็นสับริงของ $R'$ โดยทฤษฎี 3.2.1

4. เนื่องจาก $\emptyset^{-1}(S') = \{s \in R / \phi(s) = s'$ เมื่อ $s' \in S'\}$

ดังนั้น $\emptyset^{-1}(S') \subseteq R$

เนื่องจาก $0' \in S'$ ทำให้ได้ว่า $\emptyset^{-1}(0') \in \emptyset^{-1}(S')$

ดังนั้น $\phi^{-1}(S') \neq \phi$

ให้ $s, t \in \phi^{-1}(S')$ ดังนั้น $\phi(s), \phi(t) \in S'$

เนื่องจาก $S'$ เป็นสับริงของ $R'$ ดังนั้น $\phi(s) - \phi(t) \in S'$ และ $\phi(s)\phi(t) \in S'$

พิจารณา $\phi(s - t) = \phi(s + (-t))$

$= \phi(s) + \phi(-t)$

$= \phi(s) - \phi(t)$

ดังนั้น $\phi(s - t) \in S'$

นั่นคือ $s - t \in \phi^{-1}(S')$

เนื่องจาก $\phi(st) = \phi(s)\phi(t)$

ดังนั้น $\phi(st) \in S'$

นั่นคือ $st \in \phi^{-1}(S')$

ดังนั้น $\phi^{-1}(S')$ เป็นสับริงของ $R$ (โดยทฤษฎี 3 2.1)

5. ถ้า $R$ มียูนิตี้ $e$

ดังนั้น สำหรับทุกๆสมาชิก $r \in R$

$\phi(r) = \phi(er)$

$= \phi(e)\phi(r)$

ในทำนองเดียวกันจะได้

$\phi(r) = \phi(re)$

$= \phi(r)\phi(e)$

เนื่องจาก $\phi(e) \neq 0'$

ดังนั้น $\phi(e)$ คือยูนิตี้ของ $\phi(R)$

ทฤษฎี 3.3.2 ให้ $\phi$ เป็นโฮโมมอร์ฟิซึมจากริง R ไปยังริง R' จะได้ว่า $\phi$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง ก็ต่อเมื่อ $\mathrm{Ker}(\phi) = \{0\}$

พิสูจน์ (===>) ให้ $\phi$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง และเป็นโฮโมมอร์ฟิซึมจากริง R ไปยังริง R'

โดยทฤษฎี 2.3.1 ข้อ 1 ได้ว่า $\phi(0) = 0'$

ให้ $a \in \mathrm{Ker}(\phi)$ ดังนั้น $\phi(a) = 0'$

เนื่องจาก $\phi$ เป็นฟังก์ชันหนึ่งต่อหนึ่งจะได้ว่า $a = 0$

ดังนั้น $\mathrm{Ker}(\phi) = \{0\}$

(<===) ให้ $\mathrm{Ker}(\phi) = \{0\}$

จะแสดงว่า $\phi$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

ให้ $r, s \in R$ และ $\phi(r) = \phi(s)$

พิจารณา
$$\begin{aligned}\phi(r - s) &= \phi(r + (-s)) \\ &= \phi(r) + \phi(-s) \\ &= \phi(r) - \phi(s) \\ &= \phi(s) - \phi(s) \\ &= 0'\end{aligned}$$

นั่นคือ $r - s \in \mathrm{Ker}(\phi)$

ดังนั้น $r - s = 0$

นั่นคือ $r = s$

แสดงว่า $\phi$ เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก R ไปยัง R'

ตัวอย่าง 3.3.5 จากตัวอย่าง 3.3.3 $R = \{m + n\sqrt{2} \mid m, n \in I\}$ เป็นริงภายใต้การบวกธรรมดา และการคูณธรรมดา

ให้ $\emptyset : R \dashrightarrow R$ ซึ่งกำหนดโดย $\emptyset(m + n\sqrt{2}) = m - n\sqrt{2}$

ได้ว่า $Ker(\emptyset) = \{0\}$ จะแสดงว่า $\emptyset$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

<u>พิสูจน์</u> ให้ $m_1 + n_1\sqrt{2}$ และ $m_2 + n_2\sqrt{2}$ เป็นสมาชิกใดๆใน R

และให้ $\emptyset(m_1 + n_1\sqrt{2}) = \emptyset(m_2 + n_2\sqrt{2})$

พิจารณา
$$\begin{aligned}\emptyset((m_1 + n_1\sqrt{2}) - (m_2 + n_2\sqrt{2})) &= \emptyset((m_1+n_1\sqrt{2})+(-(m_2+n_2\sqrt{2}))\\ &= \emptyset(m_1+n_1\sqrt{2}) + \emptyset(-(m_2+n_2\sqrt{2}))\\ &= \emptyset(m_1+n_1\sqrt{2}) - \emptyset(m_2+n_2\sqrt{2}))\\ &= 0\end{aligned}$$

ดังนั้น $(m_1 + n_1\sqrt{2}) - (m_2 + n_2\sqrt{2}) \in Ker(\emptyset)$

เนื่องจาก $Ker(\emptyset) = \{0\}$

ดังนั้น $(m_1 + n_1\sqrt{2}) - (m_2 + n_2\sqrt{2}) = 0$

นั่นคือ $m_1 + n_1\sqrt{2} = m_2 + n_2\sqrt{2}$

แสดงว่า $\emptyset$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

<u>นิยาม 3.3.3</u> ให้ $\emptyset$ เป็นโฮโมมอร์ฟิซึมจากริง R ไปยังริง R' จะกล่าวว่า $\emptyset$ เป็น ไอโซมอร์ฟิซึม (isomorphism) ก็ต่อเมื่อ $\emptyset$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง และเป็น ออนทูจาก R ไปยัง R' และจะเรียกว่าริง R เป็นไอโซมอร์ฟิค(isomorphic) กับริง R' ซึ่งใช้สัญลักษณ์แทนด้วย $R \cong R'$

<u>ตัวอย่าง 3.3.6</u> ให้ I เป็นริงของจำนวนเต็ม และกำหนดให้

$$2I = \{2n \,/\, n \in I\}$$

ซึ่งเซ็ต 2I จะเป็นริงภายใต้การบวก และการคูณ

ให้ $\phi : I \longrightarrow 2I$ ซึ่งกำหนดโดย $\phi(x) = 2x$ สำหรับ $x \in I$

$\phi$ จะไม่เป็นไอโซมอร์ฟิซึม เพราะว่า $\phi(xy) = 2xy$ สำหรับ $x, y \in I$

แต่ $\phi(x)\,\phi(y) = (2x)(2y)$

$= 4xy$

ดังนั้น $\phi$ ไม่เป็นโฮโมมอร์ฟิซึม

ตัวอย่าง 3.3.7 ให้ R เป็นริงใดๆ และ $\phi$ เป็นฟังก์ชั่นจาก R ไปยัง R โดยกำหนด

$\phi(a) = a$ สำหรับทุกๆสมาชิก $a \in R$ จะแสดงว่า $\phi$ เป็นไอโซมอร์ฟิซึม

จากตัวอย่าง 3.3.1 จะได้ว่า $\phi$ เป็นโฮโมมอร์ฟิซึม และ $\text{Ker}(\phi) = \{0\}$

ดังนั้น $\phi$ เป็นฟังก์ชั่นหนึ่งต่อหนึ่งจาก R ไปยัง R'

เนื่องจากสำหรับทุกๆสมาชิก $x \in R$ จะมี $x \in R$ ซึ่ง $\phi(x) = x$

แสดงว่า $\phi$ เป็นฟังก์ชั่นออนทู

ดังนั้น $\phi$ เป็นไอโซมอร์ฟิซึมจากริง R ไปยังริง R

แบบฝึกหัด 3 ข

1. จงแสดงว่า ถ้า R , R' และ R'' เป็นริงและ $\phi : R \longrightarrow R'$ และ $\psi : R' \longrightarrow R''$ เป็นโฮโมมอร์ฟิซึมแล้วจะได้ว่าคอมโพสิชันของฟังก์ชั่น (composition function) $\psi \circ \phi : R \longrightarrow R''$ เป็นโฮโมมอร์ฟิซึมด้วย

2. จงแสดงว่า ถ้า $\phi : C \longrightarrow M_2(R)$ เมื่อ C คือเซ็ตของจำนวนเชิงซ้อน และ $M_2(R)$ เป็นเซ็ตซึ่งประกอบด้วยสมาชิกที่เป็นเมตริกซ์ขนาด 2 x 2 โดย

$\phi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ สำหรับ $a, b \in R$ แล้ว $\phi$ จะเป็นโฮโมมอร์ฟิซึม

3. ให้ $\theta$ เป็นฟังก์ชันจากริง $I_2$ ไปยังริง $I_6$ โดยกำหนด $\theta(\bar{0}) = \bar{0}$ และ $\theta(\bar{1}) = \bar{3}$ จงแสดงว่า $\theta$ เป็นโฮโมมอร์ฟิซึมจาก $I_2$ ไปยัง $I_6$ และ $Ker(\theta) = \{\bar{0}\}$

4. ให้ $\theta : I \dashrightarrow S''$ เมื่อ $I$ คือ เซ็ตของจำนวนเต็ม และ / $S'' = \{3n \,/\, n \in I\}$ จงแสดงว่า $\theta$ ไม่เป็นไอโซมอร์ฟิซึม เมื่อกำหนด $\theta(n) = 3n$ สำหรับทุกๆ $n \in I$

5. ให้ $\theta : \mathbb{R} \dashrightarrow \mathbb{R}$ เมื่อ $\mathbb{R}$ คือ ริงของจำนวนจริง โดยกำหนด $\theta(x) = |x|$ สำหรับทุกๆ $x \in R$ จงทดสอบว่า $\theta$ เป็นโฮโมมอร์ฟิซึมหรือไม่

----------

## 3.4. การสร้างริงใหม่ (Construction of New Ring)

การสร้างริงใหม่จากริงเดิมที่มีอยู่แล้ว ทำได้โดยการให้นิยามโอเปอเรชันการบวกและการคูณ แล้วทดสอบคุณสมบัติให้สอดคล้องตามนิยามของริง ก็จะได้ริงใหม่ ริงใหม่ที่สร้างจากริงที่มีอยู่แล้ว ซึ่งจะศึกษากันต่อไปได้แก่ โปรดักหรือไดเรคซัมของริง (Product or Direct Sum of Rings) ฟังก์ชันริง ( Function Ring) เอนโดมอร์ฟิซึมริง ( Endomorphism Ring) เมตริกซ์ริง ( Matrix Ring) และโพลีโนเมียลริง ( Polynomial Ring) เป็นต้น

### 3.4.1 โปรดักหรือไดเรคซัมของริง ( Product or Direct Sum of Rings)

กำหนดริง $R$ และ $R'$ เป็นริงที่มียูนิตี้ $e$ และ $e'$ ตามลำดับ ต้องการสร้างริง $R \times R'$

ให้ $R \times R'$ เป็นเซ็ตของคู่ลำดับ $(r, r')$ ซึ่ง $r \in R$ และ $r' \in R'$ นั่นคือ $R \times R' = \{(r,r') / r \in R, r' \in R'\}$

ให้นิยามของการบวกและการคูณใน $R \times R'$ ดังต่อไปนี้

การบวก สำหรับทุก ๆ $(r,r'), (s,s') \in R \times R'$

$$(r,r') + (s,s') = (r + s, r' + s')$$

การคูณ สำหรับทุก ๆ $(r,r'), (s,s') \in R \times R'$

$$(r,r')(s,s') = (rs, r's')$$

จะเรียกโอเปอเรชันทั้งสองนี้ว่า "เทอมไวซ์" ("termwise" operation) ต่อไปจะแสดงว่า $R \times R'$ และโอเปอเรชันเทอมไวซ์เป็นริง

1. จากนิยามการบวกและการคูณ สำหรับทุก ๆ

$(r,r'), (s,s') \in R \times R'$

จะได้ $(r,r') + (s,s') = (r + s, r' + s')$

และ $(r,r')(s,s') = (rs, r's')$

ซึ่ง $(r + s, r' + s')$ และ $(rs, r's') \in R \times R'$ ( เพราะว่า

$r + s, rs \in R$ และ $r' + s', r's' \in R')$

นั่นคือ การบวกและการคูณนี้เป็นไบนารี่โอเปอเรชันบนเซ็ต $R \times R'$

2. สำหรับทุก ๆ $(r,r'), (s,s')$ และ $(t,t') \in R \times R'$

$$[(r,r') + (s,s')] + (t,t') = (r + s, r' + s') + (t,t')$$

$$= ((r + s) + t, (r' + s') + t')$$

$$= (r + (s + t), r' + (s' + t'))$$

( โดยกฎการรวมหมู่สำหรับการบวกใน $R$ และ $R'$)

$$= (r,r') + (s + t, s' + t')$$

$$= (r,r') + [(s,s') + (t,t')]$$

นั่นคือ กฎการรวมหมู่สำหรับการบวกเป็นจริงใน $R \times R'$

3. สำหรับทุก ๆ $(r,r') \in R \times R'$ จะมี $(0, 0')$ เป็นสมาชิกเอกลักษณ์สำหรับการบวกใน $R \times R'$ เมื่อ $0,0'$ เป็นสมาชิกเอกลักษณ์ใน $R$ และ $R'$ ตามลำดับ

เพราะว่า $(r,r') + (0,0') = (r + 0, r' + 0')$

$$= (r,r')$$ (โดยคุณสมบัติสมาชิกเอกลักษณ์ใน $R$ และ $R'$)

และ $(0,0') + (r,r') = (0 + r, 0' + r')$

$= (r,r')$ (โดยคุณสมบัติสมาชิกเอกลักษณ์ใน R และ R')

4. สำหรับแต่ละ $(r,r') \in R \times R'$ จะมี $(-r,-r') \in R \times R'$

โดยที่ $(r,r') + (-r, -r') = (r + (-r), r' + (-r'))$

$= (r-r, r'-r')$

$= (0,0')$ (โดยคุณสมบัติของอินเวอร์สของการบวกใน R และ R')

และ $(-r,-r') + (r,r') = ((-r) + r, (-r') + r')$

$= (-r + r, -r' + r')$

$= (0,0')$ (โดยคุณสมบัติของอินเวอร์สของการบวกใน R และ R')

นั่นคือ $(-r, -r')$ เป็นอินเวอร์สของการบวกของ $(r,r')$

5. สำหรับทุก ๆ $(r,r'), (s,s') \in R \times R'$

จะได้ $(r,r') + (s,s') = (r + s, r' + s')$

$= (s + r, s' + r')$

(โดยกฎการสลับที่สำหรับการบวกใน R และR')

$= (s,s') + (r,r')$

ดังนั้นกฎการสลับที่สำหรับการบวกเป็นจริงใน $R \times R'$

6. สำหรับทุก ๆ $(r,r')$, $(s,s')$ และ $(t,t') \in R \times R'$

จะได้ว่า $[(r,r')(s,s')](t,t') = (rs, r's')(t,t')$

$= ((rs)t, (r's')t')$

$= (r(st), r'(s't'))$

(โดยกฎการรวมหมู่สำหรับการคูณ ใน $R$ และ $R'$)

$= (r,r')(st, s't')$

$= (r,r')[(s,t)(t,t')]$

ดังนั้นกฎการรวมหมู่สำหรับการคูณเป็นจริงใน $R \times R'$

7. สำหรับทุก ๆ $(r,r')$, $(s,s')$ และ $(t,t') \in R \times R'$

$(r,r')[(s,s') + (t,t')] = (r,r')(s + t, s' + t')$

$= (r(s + t), r'(s' + t'))$

$= (rs + rt, r's' + r't')$

(โดยกฎการกระจายใน $R$ และ $R'$)

$= (rs, r's') + (rt, r't')$

$= (r,r')(s,s') + (r,r')(t,t')$

ในทำนองเดียวกันจะได้ว่า

$[(r,r') + (s,s')](t,t') = (r,r')(t,t') + (s,s')(t,t')$

นั่นคือ กฎการกระจายเป็นจริงใน $R \times R'$

จากคุณสมบัติทั้ง 7 ข้อนี้แสดงว่า $R \times R'$ เป็น ริงภายใต้โอเปอเรชันเหอมไวซ์

หมายเหตุ จะเรียกว่า $R \times R'$ นี้ว่าโปรดักของริง R และ $R'$ (Product of R and $R'$) หรือไดเรคซัมของ R และ $R'$ (Direct Sum of R and $R'$)

นอกจากนี้ถ้าริง R และ $R'$ มียูนิตี้เป็น e และ $e'$ ตามลำดับ จะได้ว่าริง $R \times R'$ มี $(e,e')$ เป็นยูนิตี้

เพราะว่า สำหรับทุก ๆ $(r,r') \in R \times R'$

$$(r,r')(e,e') = (r,r')$$

และ

$$(e,e')(r,r') = (r,r')$$

ถ้า R และ $R'$ เป็นคอมมิวเทที่ฟริง จะได้ว่าโปรดักของริง R และ $R'$ ยังคงเป็นคอมมิวเทที่ฟริง เพราะว่าสำหรับทุก ๆ $(r,r')$ และ $(s,s') \in R \times R'$

$$(r,r')(s,s') = (rs, r's')$$

$$= (sr, s'r') \quad \text{( โดยกฎการสลับที่สำหรับการคูณใน R และ } R')$$

$$= (s,s')(r,r')$$

ตัวอย่าง 3.4.1 ให้ $I_2$ เป็นริงของจำนวนเต็มมอดูโล 2 จะพบว่า $I_2$ เป็นคอมมิวเทที่ฟริงที่มียูนิตี้ คือ $\bar{1}$

ดังนั้น $I_2 \times I_2 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{0}), (\bar{1},\bar{1})\}$ เป็นคอมมิวเทที่ฟริงมี $(\bar{1},\bar{1})$ เป็นยูนิตี้

---

### 3.4.2 ฟังก์ชันริง (Function Ring)

ต่อไปจะสร้าง "ฟังก์ชันริง"

ให้ $R^X$ แทนเซ็ตของฟังก์ชันจากเซ็ต $X$ ซึ่งไม่เป็นเซ็ตว่างไปยังริง $R$

นั่นคือ $R^X = \{f/f$ เป็นฟังก์ชันจากเซ็ต $X$ ไปยังริง $R\}$

ให้ $f$ และ $g$ เป็นสมาชิกใน $R^X$

กำหนดการบวกและการคูณใน $R^X$ ดังต่อไปนี้

<u>การบวก</u> $(f + g)(x) = f(x) + g(x)$ สำหรับแต่ละสมาชิก $x \in X$

เรียกการบวกนี้ว่าพอยท์ไวซ์ซัม (pointwise sum) หรือเทอมไวซ์ซัม (term-wise sum)

<u>การคูณ</u> $(fg)(x) = f(x)g(x)$ สำหรับแต่ละสมาชิก $x \in X$

เรียกการคูณนี้ว่าพอยท์ไวซ์โปรดัก (pointwise product)

<u>ทฤษฎี 3.4.1</u> ถ้า $R$ เป็นริง และ $X$ เป็นเซ็ตใด ๆ ที่ไม่ใช่เซ็ตว่าง แล้ว $R^X$ จะเป็นริงภายใต้พอยท์ไวซ์ซัมและพอยท์ไวซ์โปรดัก

<u>พิสูจน์</u> 1. จากนิยามพอยท์ไวซ์ซัม สำหรับทุก ๆ $f, g \in R^X$ ได้ว่า

$(f + g)(x) = f(x) + g(x)$ สำหรับแต่ละสมาชิก $x \in X$

ซึ่ง $f(x) + g(x) \in R$ ดังนั้น $f + g \in R^X$

นั่นคือพอยท์ไวซ์ซัมเป็นไบนารี่โอเปอเรชันบน $R^X$

2. จากนิยามพอยท์ไวซ์โปรดัก สำหรับทุก ๆ $f, g \in R^X$ ได้ว่า

$(fg)(x) = f(x)g(x)$ สำหรับแต่ละสมาชิก $x \in X$

ซึ่ง $f(x)g(x) \in R$ ดังนั้น $fg \in R^X$

นั่นคือ พอยท์ไวซ์โปรดัก เป็นไบนารี่โอเปอเรชันบน $R^X$

3. กฎการรวมหมู่สำหรับพอยท์ไวซ์ซัม ให้พิสูจน์เป็นแบบฝึกหัด

4. จะแสดงว่า $R^X$ มีสมาชิกเอกลักษณ์สำหรับพอยท์ไวซ์ซัม

ให้ $\sigma(x) = 0$ สำหรับทุกสมาชิก $x \varepsilon X$ และ $0$ เป็นสมาชิกเอกลักษณ์ใน $R$

จะได้ว่าฟังก์ชัน $\sigma$ เป็นสมาชิกเอกลักษณ์สำหรับพอยท์ไวซ์ซัมของ $R^X$ เพราะว่า สำหรับทุกๆสมาชิก $f \varepsilon R^X$ และ $x \varepsilon X$

$$\begin{aligned}(\sigma + f)(x) &= \sigma(x) + f(x)\\ &= 0 + f(x)\\ &= f(x)\end{aligned}$$

นั่นคือ $\sigma + f = f$

ในทำนองเดียวกันจะได้ว่า

$$f + \sigma = f$$

5. จะแสดงว่าแต่ละสมาชิก $f \varepsilon R^X$ มีอินเวอร์สสำหรับพอยท์ไวซ์ซัม

เนื่องจาก $f(x) \varepsilon R$ สำหรับสมาชิก $x \varepsilon X$ ดังนั้น $f(x)$ จะต้องมีอินเวอร์สสำหรับพอยท์ไวซ์ซัมคือ $-f(x)$

ให้ $-f(x) = (-f)(x)$ สำหรับแต่ละสมาชิก $x \varepsilon X$

เนื่องจากสำหรับทุก ๆ สมาชิก $f \varepsilon R^X$

$$\begin{aligned}[(-f) + f](x) &= (-f)(x) + f(x)\\ &= -f(x) + f(x)\\ &= 0\end{aligned}$$

แต่ $\sigma(x) = 0$

ดังนั้น $\sigma(x) = [(-f) + f](x)$

นั่นคือ $\sigma = (-f) + f$

ในทำนองเดียวกัน จะได้ว่า $\phi = f + (-f)$

นั่นคือ $-f$ เป็นอินเวอร์สสำหรับพอยท์ไวซ์ซัมของ $f$

โดยที่ $(-f)(x) = -f(x)$

6. จะแสดงว่ากฎการสลับที่สำหรับพอยท์ไวซ์ซัมเป็นจริงใน $R^X$ สำหรับทุก ๆ สมาชิก $f, g \in R^X$

$(f + g)(x) = f(x) + g(x)$

$= g(x) + f(x)$ ( โดยกฎการสลับที่สำหรับการบวกใน R)

$= (g + f)(x)$

นั่นคือ $f + g = g + f$

7. กฎการรวมหมู่สำหรับพอยท์ไวซ์โปรดักใน $R^X$ ให้พิสูจน์เป็นแบบฝึกหัด

8. จะแสดงว่ากฎการกระจายเป็นจริงใน $R^X$ สำหรับทุก ๆ $f, g$ และ $h$ เป็นสมาชิกใด ๆ ใน $R^X$ จะได้ว่า

$f(x)\left[g(x) + h(x)\right] = f(x)g(x) + f(x)h(x)$ สำหรับทุก ๆ $x \in X$ เพราะว่า $f(x)$, $g(x)$ และ $h(x)$ เป็นสมาชิกในริง $R^X$

ดังนั้น $f(x)\left[(g + h)(x)\right] = (fg)(x) + (fh)(x)$

$\left[f(g + h)\right](x) = (fg + fh)(x)$

นั่นคือ $f(g + h) = fg + fh$

ในทำนองเดียวกันพิสูจน์ได้ว่า

$(f + g)h = fh + gh$

แสดงว่ากฎการกระจายเป็นจริงใน $R^X$

จากคุณสมบัติทั้ง 8 ข้อนี้ แสดงว่า $R^X$ เป็นริงภายใต้พอยท์ไวซ์ซัมและพอยท์ไวซ์โปรดัก

<u>หมายเหตุ</u> 1. เรียกริง $R^X$ นี้ว่าฟังก์ชันริง (Function Ring)

2. ถ้า R เป็นริงที่มียูนิตี้ e จะได้ว่า $R^X$ มี $e'$ เป็นยูนิตี้

โดยที่ $e'(x) = e$ สำหรับทุก ๆ $x \in X$

เพราะว่าสำหรับแต่ละสมาชิก $f \in R^X$

$$(fe')(x) = f(x)e'(x)$$
$$= f(x)e$$
$$= f(x)$$

นั่นคือ $fe' = f$

ในทำนองเดียวกันพิสูจน์ได้ว่า

$$e'f = f$$

3. ถ้า R เป็นคอมมิวเทฟริง จะได้ว่า $R^X$ เป็นคอมมิวเทฟริงด้วย เพราะว่าสำหรับทุก ๆ $f, g \in R^X$ และ $x \in X$

$$f(x)g(x) = g(x)f(x) \quad \text{(โดยกฎการสลับที่สำหรับการคูณใน R)}$$

นั่นคือ $fg = gf$

4. สำหรับฟังก์ชัน $\sigma$ และ $e' \in R^X$ โดยที่

$\sigma(x) = 0$ สำหรับทุก $x \in X$

และ $e'(x) = e$ สำหรับทุก $x \in X$

จะเรียกฟังก์ชันคงที่ (constant functions)

---

3.4.3 เอนโดมอร์ฟิซึมริง (Endomorphism Ring)

นิยาม 3.4.1 ให้ G และ G' เป็นกรุ๊ป มี . และ * เป็นไบนารี่โอเปอเรชันตามลำดับ และ θ เป็นฟังก์ชันจาก G ไปยัง G' จะเรียก θ ว่าเป็นโฮโมมอร์ฟิซึม (homomorphism) ของกรุ๊ป G และ G' ก็ต่อเมื่อ

$\theta(x \cdot y) = \theta(x) * \theta(y)$ สำหรับทุก ๆ $x, y \in G$

นิยาม 3.4.2 ให้ A เป็นอบีเลียนกรุ๊ป เอนโดมอร์ฟิซึม (Endomorphism) ของ A หมายถึงโฮโมมอร์ฟิซึมของ A ไปยัง A ใช้สัญลักษณ์ Hom(A) แทนเซ็ตของเอนโดมอร์ฟิซึมของ A ทั้งหมด

นิยามการบวกและการคูณบนเซ็ต Hom(A) ดังนี้

การบวก สำหรับ $\phi, \psi \in \mathrm{Hom}(A)$ และทุก ๆ สมาชิก $a \in A$

$(\phi + \psi)(a) = \phi(a) + \psi(a)$

การคูณ สำหรับการคูณใน Hom(A) หมายถึงคอมโพสิชันของฟังก์ชัน (Function composition)

นั่นคือ สำหรับ $\phi, \theta \in \mathrm{Hom}(A)$ และทุก ๆ สมาชิก $a \in A$

$(\phi \circ \theta)(a) = \phi(\theta(a))$

ทฤษฎี 3.4.2 Hom(A) จะเป็นริงภายใต้การบวกและการคูณใน Hom(A) และเรียกว่าเอนโดมอร์ฟิซึมริง (Endomorphism Ring)

พิสูจน์ 1. จะแสดงว่าการบวกเป็นไบนารี่โอเปอเรชันบน Hom(A)

ให้ $\phi, \psi \in \mathrm{Hom}(A)$ และ $a, b \in A$

พิจารณา $(\phi + \psi)(a + b) = \phi(a + b) + \psi(a + b)$ (จากนิยามการบวก)

$= [\phi(a) + \phi(b)] + [\psi(a) + \psi(b)]$

(เพราะว่า $\phi, \psi \in \mathrm{Hom}(A)$)

$= [\phi(a) + \psi(a)] + [\phi(b) + \psi(b)]$

(เพราะว่า A เป็นอบีเลียนกรุป)

$= (\phi + \psi)(a) + (\phi + \psi)(b)$

(จากนิยามการบวก)

ดังนั้น $\phi + \psi \in \mathrm{Hom}(A)$

2. จะแสดงว่ากฎการรวมหมู่สำหรับการบวกเป็นจริงใน Hom(A)

ให้ $\phi$, $\psi$ และ $\theta \in \mathrm{Hom}(A)$ และ $a \in A$

$[\phi + (\psi + \theta)](a) = \phi(a) + (\psi + \theta)(a)$ (จากนิยามการบวก)

$= \phi(a) + [\psi(a) + \theta(a)]$ (จากนิยามการบวก)

$= [\phi(a) + \psi(a)] + \theta(a)$

(จากกฎการรวมหมู่ใน A)

$= (\phi + \psi)(a) + \theta(a)$

$= [(\phi + \psi) + \theta](a)$

นั่นคือ $\phi + (\psi + \theta) = (\phi + \psi) + \theta$

ดังนั้นกฎการรวมหมู่สำหรับการบวกเป็นจริงใน Hom(A)

3. จะแสดงว่ากฎการสลับที่สำหรับการบวกเป็นจริงใน Hom(A)

ให้ $\phi, \psi \in \mathrm{Hom}(A)$ และ $a \in A$

พิจารณา $(\emptyset + \psi)(a) = \emptyset(a) + \psi(a)$ (จากนิยามการบวก)

$= \psi(a) + \emptyset(a)$ (เพราะว่า A เป็นอบีเลียนกรุ๊ป)

$= (\psi + \emptyset)(a)$ (จากนิยามการบวก)

นั่นคือ $\emptyset + \psi = \psi + \emptyset$

4. จะแสดงว่า Hom(A) มีสมาชิกเอกลักษณ์สำหรับการบวก

ให้ $0$ เป็นสมาชิกเอกลักษณ์ใน $A$ และ $0'$ เป็นฟังก์ชันจาก $A$ ไปยัง $A$ ซึ่งกำหนดโดย $0'(a) = 0$ สำหรับทุก ๆ สมาชิก $a \in A$

ดังนั้น $0' \in \text{Hom}(A)$

ให้ $\emptyset \in \text{Hom}(A)$ และ $a \in A$

พิจารณา $(\emptyset + 0')(a) = \emptyset(a) + 0'(a)$ (จากนิยามการบวก)

$= \emptyset(a) + 0$

$= \emptyset(a)$

ดังนั้น $\emptyset + 0' = \emptyset$

ในทำนองเดียวกัน พิสูจน์ได้ว่า

$0' + \emptyset = \emptyset$

นั่นคือ $0'$ เป็นสมาชิกเอกลักษณ์สำหรับการบวกของ Hom(A)

5. จะแสดงว่าทุก ๆ สมาชิก $\emptyset \in \text{Hom}(A)$ มีอินเวอร์สสำหรับการบวกใน Hom(A) ให้ $\emptyset \in \text{Hom}(A)$

กำหนด $-\emptyset$ โดย $(-\emptyset)(a) = -(\emptyset(a))$ สำหรับ $a \in A$

จะแสดง $-\emptyset \in \text{Hom}(A)$

เนื่องจาก $(-\emptyset)(a+b) = -(\emptyset(a+b))$

$= -(\emptyset(a) + \emptyset(b))$

$= -\emptyset(a) + (-\emptyset(b))$

$= (-\emptyset)(a) + (-\emptyset)(b)$

ดังนั้น $-\emptyset \in \text{Hom}(A)$

ต่อไปพิจารณา

$(\emptyset + (-\emptyset))(a) = \emptyset(a) + (-\emptyset)(a)$

$= \emptyset(a) - \emptyset(a)$

$= 0$

$= 0'(a)$

ดังนั้น $\emptyset + (-\emptyset) = 0'$

ในทำนองเดียวกันจะได้ว่า

$(-\emptyset) + \emptyset = 0'$

นั่นคือ $-\emptyset$ เป็นอินเวอร์สสำหรับการบวกของ $\emptyset$

6. จะแสดงว่าการคูณเป็นไบนารี่โอเปอเรชันบน Hom (A)

ให้ $\emptyset, \psi \in \text{Hom}(A)$ และ $a, b \in A$

เนื่องจาก $\emptyset : A \to A$ และ $\psi : A \to A$

จะได้ $\emptyset \circ \psi : A \to A$

พิจารณา $(\emptyset \circ \psi)(ab) = \emptyset(\psi(ab))$ ( จากนิยามคอมโพสิชันของฟังก์ชัน)

$= \emptyset(\psi(a)\psi(b))$ (เพราะว่า $\psi \in \text{Hom}(A)$)

$= \emptyset(\psi(a))\emptyset(\psi(b))$ (เพราะว่า $\emptyset \in \text{Hom}(A)$)

$= (\emptyset \circ \psi)(a)(\emptyset \circ \psi)(b)$

ดังนั้น $\emptyset \circ \psi \in \text{Hom}(A)$

7. จะแสดงว่ากฎการรวมหมู่สำหรับการคูณเป็นจริงใน Hom(A)

ให้ $\phi$, $\psi$ และ $\theta \varepsilon$ Hom (A)

$$[(\phi\circ\psi)\circ\theta](a) = (\phi\circ\psi)(\theta(a)) \qquad \text{(นิยามคอมโพสิชันของฟังก์ชั่น)}$$

$$= \phi(\psi(\theta(a)) \qquad \text{(นิยามคอมโพสิชันของฟังก์ชั่น)}$$

$$= \phi(\psi\circ\theta(a)) \qquad \text{(นิยามคอมโพสิชันของฟังก์ชั่น)}$$

$$= [\phi\circ(\psi\circ\theta)](a) \qquad \text{(นิยามคอมโพสิชันของฟังก์ชั่น)}$$

ดังนั้น $(\phi\circ\psi)\circ\theta) = \phi\circ(\psi\circ\theta)$

8. จะแสดงว่ากฎการกระจายเป็นจริงใน Hom(A)

ให้ $\phi$, $\psi$ และ $\theta \varepsilon$ Hom(A) และ $a \varepsilon A$

$$(\phi+\psi)\circ\theta\ (a) = (\phi+\psi)(\theta(a)) \qquad \text{(นิยามคอมโพสิชันของฟังก์ชั่น)}$$

$$= [\phi(\theta(a))] + [\psi(\theta(a))] \text{(นิยามการบวก)}$$

$$= (\phi\circ\theta)(a) + (\psi\circ\theta)(a)$$

$$= (\phi\circ\theta + \psi\circ\theta)(a)$$

ดังนั้น $(\phi+\psi)\circ\theta = \phi\circ\theta + \psi\circ\theta$

ในทำนองเดียวกันพิสูจน์ได้ว่า

$$\phi\circ(\psi+\theta) = \phi\circ\psi + \phi\circ\theta$$

จากคุณสมบัติทั้ง 8 ข้อแสดงว่า Hom(A) เป็นริง

---

<u>หมายเหตุ</u> โดยทั่วไปแล้วคอมโพสิชันของฟังก์ชันจะไม่เป็นคอมมิวเทที่พ เพราะฉะนั้นเอนโดมอร์ฟิซึมริง ไม่จำเป็นจะต้องเป็นคอมมิวเทที่ฟริงเสมอไป

<u>ตัวอย่าง 3.4.1</u> จะแสดงว่า $Hom(I \times I)$ ไม่เป็นคอมมิวเทที่ฟริง

พิจารณา $I \times I = \{(a,b) / a,b \in I\}$

จากหัวข้อ 3.4.1 ได้ว่า $I \times I$ เป็นริง ดังนั้น $I \times I$ เป็นอบีเลียนกรุ๊ปภายใต้การบวก

จากทฤษฎี 3.4.2 จะได้ $Hom(I \times I)$ เป็นริง

ต่อไปจะแสดงว่า $Hom(I \times I)$ ไม่เป็นคอมมิวเทที่ฟริง

พิจารณา $\emptyset, \theta \in Hom(I \times I)$

ซึ่งกำหนดโดย $\emptyset(r,s) = (s,r)$

และ $\theta(r,s) = (r,0)$

สำหรับทุก ๆ $r,s \in I$ และ $0$ เป็นสมาชิกเอกลักษณ์ของ $I$

พิจารณา

$$\begin{aligned}(\emptyset \circ \theta)(r,s) &= \emptyset(\theta(r,s)) \\ &= \emptyset(r,0) \\ &= (0,r)\end{aligned}$$

และ

$$\begin{aligned}(\theta \circ \emptyset)(r,s) &= \theta(\emptyset(r,s)) \\ &= \theta(s,r) \\ &= (s,0)\end{aligned}$$

ดังนั้น $\emptyset \circ \theta \neq \theta \circ \emptyset$

นั่นคือ $Hom(I \times I)$ ไม่เป็นคอมมิวเทที่ฟริง

---

### 3.4.4 <u>เมตริกซ์ริง</u> (Matrix Ring)

ให้ $R$ เป็นริงใด ๆ

พิจารณาเซ็ต $M_2(R)$ เป็นเซ็ตของเมตริกซ์ที่มีขนาด $2 \times 2$ ใช้สัญลักษณ์เขียนแทนดังนี้

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

โดยที่สมาชิก $a_{ij}$ ในเมตริกซ์เป็นสมาชิกในริง $R$

<u>สัญลักษณ์</u> $a_{ij}$ เขียนแทนสมาชิกในเมตริกซ์แสดงตำแหน่งของสมาชิกดังนั้น

$i$ แสดงว่าอยู่ในตำแหน่งแถว (row) ที่ $i$

$j$ แสดงว่าอยู่ในตำแหน่งหลัก (column) ที่ $j$

เช่น $a_{12}$ คือสมาชิกในเมตริกซ์ที่อยู่ในตำแหน่งแถวที่ 1 คอลัมน์ที่ 2

จะเรียก $M_2(R)$ ว่าเป็นเซ็ตของ $2 \times 2$ เมตริกซ์บน $R$

นิยามการบวกของเมตริกซ์ใน $M_2(R)$ ดังนี้

สำหรับ $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in M_2(R)$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

นิยามการคูณของเมตริกซ์ใน $M_2(R)$ ดังนี้

สำหรับ $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in M_2(R)$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

นั่นคือ $(a_{ij})(b_{ij}) = (c_{ij})$

โดยที่ $c_{ij} = \sum_{k=1}^{2} a_{ik}\, b_{kj}$

ต่อไปจะแสดงว่า $M_2(R)$ เป็นริงภายใต้การบวกและการคูณของเมตริกซ์

1. จะแสดงว่าการบวกของเมตริกซ์ขนาด $2 \times 2$ เป็นไบนารี่โอเปอเรชันบน $M_2(R)$

ให้ $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \varepsilon M_2(R)$

ให้ $C = A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$

จะได้ว่า $C \varepsilon M_2(R)$ เนื่องจาก $a_{11} + b_{11}$, $a_{12} + b_{12}$, $a_{21} + b_{21}$ และ $a_{22} + b_{22} \varepsilon R$

2. จะแสดงว่ากฎการรวมหมู่สำหรับการบวกเป็นจริงใน $M_2(R)$

ให้ $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$

และ $C = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \varepsilon M_2(R)$

$$(A + B) + C = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix} + \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$$

$$= \begin{pmatrix} (a_{11} + b_{11}) + c_{11} & (a_{12} + b_{12}) + c_{12} \\ (a_{21} + b_{21}) + c_{21} & (a_{22} + b_{22}) + c_{22} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11} + (b_{11} + c_{11}) & a_{12} + (b_{12} + c_{12}) \\ a_{21} + (b_{21} + c_{21}) & a_{22} + (b_{22} + c_{22}) \end{pmatrix}$$

$$= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} + c_{11} & b_{12} + c_{12} \\ b_{21} + c_{21} & b_{22} + c_{22} \end{pmatrix}$$

$$= A + (B + C)$$

ดังนั้น $(A + B) + C = A + (B + C)$

3. จะแสดงว่า $M_2(R)$ มีสมาชิกเอกลักษณ์สำหรับการบวก

ให้ $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ โดยที่ $0$ เป็นสมาชิกเอกลักษณ์ของ $R$

จะได้ $O \in M_2(R)$

พิจารณา $A + O = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

$$= \begin{pmatrix} a_{11} + 0 & a_{12} + 0 \\ a_{21} + 0 & a_{22} + 0 \end{pmatrix}$$

$$= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

ดังนั้น $A + O = A$

ในทำนองเดียวกันพิสูจน์ได้ว่า

$$O + A = A$$

นั่นคือ $O$ เป็นสมาชิกเอกลักษณ์สำหรับการบวกใน $M_2(R)$

4. จะแสดงว่าแต่ละสมาชิก $A \varepsilon M_2(R)$ มีอินเวอร์สสำหรับการบวก

ให้ $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ จะมี $-A = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix} \varepsilon M_2(R)$

ซึ่ง $$A + (-A) = \begin{pmatrix} a_{11} + (-a_{11}) & a_{12} + (-a_{12}) \\ a_{21} + (-a_{21}) & a_{22} + (-a_{22}) \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

ดังนั้น $A + (-A) = O$

ในทำนองเดียวกัน จะได้ว่า

$$(-A) + A = O$$

นั่นคือ $-A$ เป็นอินเวอร์สสำหรับการบวกของ $A$

5. จะแสดงว่ากฎการสลับที่สำหรับการบวกเป็นจริงใน $M_2(R)$

ให้ $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \varepsilon M_2(R)$

$$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

$$= \begin{pmatrix} b_{11} + a_{11} & b_{12} + a_{12} \\ b_{21} + a_{21} & b_{22} + a_{22} \end{pmatrix}$$

$$= B + A$$

6. จะแสดงว่าการคูณเมตริกซ์เป็นไบนารี่โอเปอเรชันบน $M_2(R)$

ให้ $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \varepsilon M_2(R)$

$$AB = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

ดังนั้น $AB \varepsilon M_2(R)$

7. จะแสดงว่ากฎการรวมหมู่สำหรับการคูณเป็นจริงใน $M_2(R)$

ให้ $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij}) \varepsilon M_2(R)$

ถ้า $d_{rs}$ เป็นสมาชิกใน $(a_{ij}) \left[ (b_{ij})(c_{ij}) \right]$ จะได้ว่า

$$d_{rs} = \sum_{k=1}^{2} a_{rk} \left( \sum_{j=1}^{2} b_{kj} c_{js} \right)$$

$$= \sum_{j=1}^{2} \left( \sum_{k=1}^{2} a_{rk} b_{kj} \right) c_{js}$$

$$= e_{rs}$$

ซึ่ง $e_{rs}$ คือสมาชิกในแถวที่ r และหลักที่ s ของ $[(a_{ij})(b_{ij})](c_{ij})$

8. สำหรับกฎการกระจายเป็นจริงใน $M_2(R)$ ให้พิสูจน์เป็นแบบฝึกหัด

จากคุณสมบัติทั้ง 8 ข้อนี้แสดงว่า $M_2(R)$ เป็นริงภายใต้การบวกและการคูณของเมตริกซ์

--------------------

ให้ R เป็นริงใด ๆ และกำหนด $M_n(R)$ เป็นเซ็ตของเมตริกซ์ขนาด $n \times n$ บน R และนิยามการบวกและการคูณของเมตริกซ์ใน $M_n(R)$ ดังนี้

<u>การบวก</u> ให้ A และ B เป็นเมตริกซ์ขนาด $n \times n$ โดยให้ $A = (a_{ij})$ และ $B = (b_{ij})$

$$A + B = (a_{ij}) + (b_{ij})$$
$$= (a_{ij} + b_{ij}) \quad \text{สำหรับทุก ๆ } i, j$$

<u>การคูณ</u> ให้ A และ B เป็นเมตริกซ์ขนาด $n \times n$ โดยให้ $A = (a_{ij})$ และ $B = (b_{ij})$

$$AB = (a_{ij})(b_{ij})$$
$$= (c_{ij})$$

โดยที่ $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$

__ทฤษฎี 3.4.1__ ให้ $R$ เป็นริง และ $M_n(R)$ เป็นเซ็ตของเมตริกซ์ขนาด $n \times n$ ทั้งหมด ซึ่งมีสมาชิกในเมตริกซ์อยู่ในริง $R$ จะได้ว่า $M_n(R)$ เป็นริงภายใต้การบวกและการคูณของเมตริกซ์ และเรียกว่าเมตริกซ์ริง (Matrix Ring)

__พิสูจน์__ เป็นแบบฝึกหัด

-------------

__ข้อสังเกต__ สำหรับการคูณของเมตริกซ์ไม่เป็นคอมมิวเททีฟ เพราะฉะนั้นเมตริกซ์ริง $M_n(R)$ ไม่เป็นคอมมิวเททีฟสำหรับ $n \geq 2$

-------------

### 3.4.5 โพลิโนเมียลริง (Polynomial Ring)

การสร้างริงเรื่องสุดท้ายที่จะศึกษาในบทนี้คือ โพลิโนเมียลริง ซึ่งแต่ละสมาชิกของริงนี้ จะอยู่ในรูปของโพลิโนเมียล

นิยาม 3.4.3 ให้ R เป็นริงใดๆ จะเรียก $f(x)$ ว่าเป็นโพลิโนเมียลที่มีสัมประสิทธิ์ (coefficient) อยู่ใน R หรือกล่าวสั้นๆว่าโพลิโนเมียลของ x ใน R ถ้า $f(x)$ เป็นนิพจนที่เขียนได้ในรูป

$$f(x) = a_o + a_1x + a_2x^2 + \dots + a_nx^n$$

โดยที่ $a_o , a_1, \dots, a_n \in R$ และ $n$ เป็นจำนวนเต็มที่ไม่น้อยกว่า 0
เรียก $a_i$ ว่าสัมประสิทธิ์ของ $x^i$ สำหรับ $i = 1, 2, \dots, n$

สำหรับสัญลักษณ์ x ไม่ได้แทนเลขจำนวน หรือสมาชิกในเซ็ตเดียวกับสัมประสิทธิ์ แต่ใช้เป็นสัญลักษณ์ทั่วๆไปไม่จำเพาะเจาะจง

ถ้า $f(x) = a_o + a_1x + \dots + a_nx^n$ และ $a_n \neq 0$
จะเรียกว่า $f(x)$ มีดีกรี (degree) เป็น $n$

ถ้า $f(x) = 0 + 0x + 0x^2 + \dots + 0x^n$ หรือ $f(x) = 0$
จะเรียก $f(x)$ ว่าเป็นโพลิโนเมียลศูนย์ (Zero polynomial)

ถ้า $f(x) = c$ ซึ่ง $c$ เป็นสมาชิกใน R จะเรียก $f(x)$ นี้ว่าโพลิโนเมียลคงที่ (constant polynomial)

ถ้า $f(x)$ เป็นโพลิโนเมียลคงที่ไม่เป็นศูนย์ จะกล่าวว่าโพลิโนเมียล $f(x)$ มีดีกรี 0

กรณีที่ $ex^i$ เมื่อ $i = 0, 1, 2, \ldots\ldots, n$ และ $e$ คือยูนิตี้ ใน $R$ จะเขียนแทนด้วย $x^i$ สำหรับเทอมใดที่เป็น $0x^i$ หรือ $a_o = 0$ (แต่ไม่ใช่ทุกค่าของ $a_i = 0$ ) จะไม่เขียนบ่งไว้ เช่น $2 + 0x + ex^2$ เขียนเป็น $2 + x^2$

<u>สัญลักษณ์</u> เซ็ทของโพลี่โนเมี่ยลทั้งหมดของ $x$ ในริง $R$ จะเขียนแทนด้วย $R[x]$

<u>นิยาม 3.4.4</u> ให้ $f(x), g(x) \in R[x]$ โดยที่

$$f(x) = a_o + a_1x + \ldots\ldots + a_nx^n$$

และ

$$g(x) = b_o + b_1x + \ldots\ldots + b_mx^m$$

กำหนดการเท่ากันของโพลี่โนเมี่ยลดังนี้

$$f(x) = g(x) \text{ ก็ต่อเมื่อ } a_i = b_i \text{ สำหรับทุกจำนวนเต็ม } i \geq 0$$

กำหนดการบวกของโพลี่โนเมี่ยลดังนี้

$$f(x) + g(x) = c_o + c_1x + c_2x^2 + \ldots\ldots + c_nx^n$$

โดยที่ $c_i = a_i + b_i$ สำหรับทุกๆจำนวนเต็ม $i \geq 0$

กำหนดการคูณของโพลี่โนเมี่ยลดังนี้

$$f(x)\,g(x) = d_o + d_1x + \ldots\ldots + d_{n+m}x^{n+m}$$

โดยที่

$$d_i = a_ob_i + a_1b_{i-1} + a_2b_{i-2} + \ldots\ldots + a_{i-1}b_1 + a_ib_o$$

สำหรับทุกๆจำนวนเต็ม $i \geq 0$

<u>ข้อสังเกตุ</u> จากนิยามการคูณของโพลี่โนเมี่ยล จะเห็นว่าสัมประสิทธิ์ของ $x^i$ ในผลคูณ $f(x)g(x)$ เป็นรูปผลบวกของ $a_sb_r$ เมื่อ $s + r = i$

<u>ตัวอย่าง 3.4.3</u> ให้ $I[x]$ เป็นเซ็ตของโพลิโนเมียลทั้งหมดของ $x$ ใน $I$

กำหนด $f(x) = 1 + x + x^2 \in I[x]$ และ $g(x) = 3 - 2x \in I[x]$

ดังนั้น $f(x) + g(x) = 4 - x + x^2$

<u>ตัวอย่าง 3.4.4</u> กำหนดให้ $p(x)$ และ $q(x) \in I[x]$ โดยที่

$$p(x) = 1 + x - x^2 \quad \text{และ} \quad g(x) = 2 + x^2 + x^3$$

ในที่นี้ $a_o = 1$, $a_1 = 1$, $a_2 = -1$, $a_i = 0$ สำหรับ $i > 2$

และ $b_o = 2$, $b_1 = 0$, $b_2 = 1$, $b_3 = 1$, $b_i = 0$ สำหรับ $i > 3$

จากนิยามการคูณ

$$d_o = a_ob_o = (1)(2) = 2$$

$$d_1 = a_ob_1 + a_1b_o = (1)(0) + (1)(2) = 2$$

$$d_2 = a_ob_2 + a_1b_1 + a_2b_o = (1)(1) + (1)(0) + (-1)(2) = -1$$

$$d_3 = a_ob_3 + a_1b_2 + a_2b_1 + a_3b_o = (1)(1)+(1)(1)+(-1)(0)+(0)(2) = 2$$

$$d_4 = a_ob_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_4b_o = (1)(0) + (1)(1) + (-1)(1) + (0)(0) + (0)(2) = 0$$

$$d_5 = a_ob_5 + a_1b_4 + a_2b_3 + a_3b_2 + a_4b_1 + a_5b_o$$

$$= (1)(0) + (1)(0) + (-1)(1) + (0)(1) + (0)(0) + (0)(2) = -1$$

$$d_6 = a_ob_6 + a_1b_5 + a_2b_4 + a_3b_3 + a_4b_2 + a_5b_1 + a_6b_o$$

$$= (1)(0) + (1)(0) + (-1)(0) + (0)(1) + (0)(1) + (0)(0) + (0)(2) = 0$$

$$d_7 = d_8 = \cdots = 0$$

ดังนั้น $p(x)\, q(x) = (1 + x - x^2)(2 + x^2 + x^3)$

$$= d_o + d_1 x + \cdots + d_5 x^5$$

$$= 2 + 2x - x^2 + 2x^3 - x^5$$

<u>ตัวอย่าง 3.4.5</u> กำหนด $f(x) = x + \bar{1} \in I_2[x]$

จะได้ $(x + \bar{1}) + (x + \bar{1}) = \bar{2}x + \bar{2}$

$$= \bar{0}x + \bar{0}$$

$$= \bar{0}$$

และ $(x + \bar{1})^2 = (x + \bar{1})(x + \bar{1})$

$$= x^2 + \bar{2}x + \bar{1}$$

$$= x^2 + \bar{1}$$

<u>ทฤษฎี 3.4.4</u> ให้ R เป็นริงใดๆ และ $R[x]$ เป็นเซ็ตของโพลี่โนเมี่ยลของ $x$ ทั้งหมดใน R จะได้ว่า $R[x]$ เป็นริงภายใต้การบวก และการคูณโพลี่โนเมี่ยล

1. จากนิยามการบวกของโพลี่โนเมี่ยล จะได้ว่าการบวกของโพลี่โนเมี่ยล เป็นไบนารี่โอเปอร์เรชันบน $R[x]$

2. สำหรับกฎการรวมหมู่ และกฎการสลับที่สำหรับการบวกของโพลี่โนเมี่ยล เป็นจริง พิสูจน์ได้โดยอาศัยนิยามการบวกของโพลี่โนเมี่ยล และคุณสมบัติของริง

3. จะแสดงว่าโพลี่โนเมี่ยลเป็นสมาชิกเอกลักษณ์ใน $R[x]$

ให้ $f(x) \in R[x]$ โดยที่

$$f(x) = a_o + a_1 x + \cdots + a_n x^n$$

จะมี $z(x) = 0 + 0x + \dots + 0x^n$ เป็นสมาชิกใน $R[x]$

ซึ่ง $f(x) + z(x) = (a_0 + 0) + (a_1 + 0)x + \dots + (a_n + 0)x^n$

$$= a_0 + a_1x + \dots + a_nx^n$$

$$= f(x)$$

ในทำนองเดียวกันพิสูจน์ได้ว่า

$$z(x) + f(x) = f(x)$$

นั่นคือ $z(x)$ เป็นสมาชิกเอกลักษณ์ใน $R[x]$

4. จะแสดงว่าแต่ละ $f(x) \in R[x]$ จะมีอินเวอร์สสำหรับการบวก

ให้ $f(x) \in R[x]$ โดยที่ $f(x) = a_0 + a_1x + \dots + a_nx^n$

เนื่องจาก $a_i \in R$ ดังนั้น $-a \in R$ สำหรับ $i = 0, 1, 2, \dots, n$

ดังนั้นจะมี $-f(x) = (-a_0) + (-a_1)x + \dots + (-a_n)x^n \in R[x]$

ซึ่ง $f(x) + (-f(x)) = (a_0 - a_0) + (a_1 - a_1)x + \dots + (a_n - a_n)x^n$

$$= 0 + 0x + \dots + 0x^n$$

$$= z(x)$$

ในทำนองเดียวกันพิสูจน์ได้ว่า

$$(-f(x)) + f(x) = z(x)$$

นั่นคือ $-f(x)$ เป็นอินเวอร์สสำหรับการบวกของ $f(x)$

5. จากนิยามการคูณของโพลีโนเมียลจะได้ว่า การคูณของโพลีโนเมียลเป็นไบนารีโอเปอร์เรชันบน $R[x]$

6. จะแสดงว่ากฎการรวมหมู่สำหรับการคูณเป็นจริงใน $R[x]$

ให้ $f(x)$ , $g(x)$ , $h(x) \in R[x]$

โดยที่ $f(x) = a_o + a_1x + a_2x^2 + \dots + a_nx^n$

$g(x) = b_o + b_1x + b_2x^2 + \dots + b_mx^m$

และ $h(x) = c_o + c_1x + c_2x^2 + \dots + c_px^p$

จะแสดงว่า $[f(x)g(x)]\, h(x) = f(x)\, [g(x)h(x)]$

จากนิยามการคูณได้ว่าผลบวกของ $(a_ib_j)c_k$ โดยที่ $i + j + k = t$

คือสัมประสิทธิ์ของ $x^t$ ในผลคูณ $[f(x)\ g(x)]\ h(x)$

และผลบวกของ $a_i(b_jc_k)$ โดย $i + j + k = t$ เป็นสัมประสิทธิ์ของ $x^t$

ในผลคูณ $f(x)[\,g(x)\ h(x)\,]$

เนื่องจาก $a_i$ , $b_j$ , $c_k \in R$

ดังนั้น $(a_ib_j)c_k = a_i(b_jc_k)$ โดยที่ $i + j + k = t$

แสดงว่าสัมประสิทธิ์ของ $x^t$ ในผลคูณ $[f(x)\ g(x)\,]\,h(x)$ เท่ากับสัมประสิทธิ์ของ $x^t$

ในผลคูณ $f(x)\ [g(x)\ h(x)]$

ในทำนองเดียวกันสัมประสิทธิ์ของ $x^s$ ในผลคูณ $f(x)[(g(x)h(x))]$ เป็นสัมประสิทธิ์

ของ $x^s$ ในผลคูณ $\{f(x)\ g(x)\}\ h(x)$

นั่นคือ $\{f(x)\ g(x)\}\ h(x) = f(x)\{g(x)h(x)\}$

แสดงว่ากฎการรวมหมู่สำหรับการคูณเป็นจริงใน $R\{x\}$

7. การแสดงว่ากฎการกระจายเป็นจริงใน $R\{x\}$ ให้เป็นแบบฝึกหัด

ดังนั้น $R\{x\}$ จะเป็นริง ภายใต้การบวก และการคูณของโพลีโนเมียล

<u>หมายเหตุ</u> ถ้า $R$ เป็นคอมมิวเทที่พริง จะได้ว่า $R\{x\}$ เป็นคอมมิวเทที่พริง และถ้า $R$ มียูนิตี้เป็น $e$ จะได้ว่า $f(x) = e$ เป็นยูนิตี้ของ $R\{x\}$

## แบบฝึกหัด 3 ก

1. ให้ $S, T$ เป็นเซ็ตที่มี $\square$ และ $\square'$ เป็นไบนารี่โอเปอเรชัน สำหรับโปรดักเซ็ต $S \times T$ , นิยามไบนารี่โอเปอเรชัน $\square''$ ดังนี้คือ

$$(s_1, t_1) \; \square'' \; (s_2, t_2) = (s_1 \square s_2, \; t_1 \square' t_2)$$

สำหรับทุก ๆ $s_1, s_2 \in S$ และ $t_1, t_2 \in T$

ก. จงแสดงว่า $\square''$ เป็นคอมมิวเททีฟ ก็ต่อเมื่อทั้ง $\square$ และ $\square'$ เป็นคอมมิวเททีฟ

ข. จงแสดงว่า $\square''$ เป็นไปตามกฎของการรวมหมู่ ก็ต่อเมื่อทั้ง $\square$ และ $\square'$ เป็นไปตามกฎการรวมหมู่

ค. จงแสดงว่า $\square''$ มียูนิตี้ ก็ต่อเมื่อทั้ง $\square$ และ $\square'$ มียูนิตี้

2. จงคำนวณ $\begin{pmatrix} 3 & -4 \\ 1 & 5 \end{pmatrix} + \begin{pmatrix} 4 & 17 \\ 5 & -3 \end{pmatrix}$ และ $\begin{pmatrix} 3 & -4 \\ 1 & 5 \end{pmatrix}\begin{pmatrix} 4 & 17 \\ 5 & -3 \end{pmatrix}$

ในเซ็ต $M_2(Q)$ เมื่อ $Q$ คือริงของจำนวนตรรกยะ

3. จงแสดงว่า $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ เป็นยูนิตี้ใน $M_2(R)$ และจงหาว่ายูนิตี้ใน $M_n(R)$ คืออะไร

4. จงคำนวณผลบวกและผลคูณของ $f(x) = 2x^3 + 4x^2 + 3x + 2$ และ $g(x) = 3x^4 + 2x + 4$ โดยที่ $f(x), g(x) \in I[x]$

5. จงคำนวณผลบวกและผลคูณของ $f(x) = \bar{2}x^3 + \bar{4}x^2 + \bar{3}x + \bar{2}$ และ $g(x) = \bar{3}x^4 + \bar{2}x + \bar{4}$ กำหนดให้ $f(x), g(x) \in I_5[x]$

6. จงพิสูจน์ทฤษฎี 3.2.1 ข้อ 3, 7

7. จงพิสูจน์ทฤษฎี 3.4.1

8. จงพิสูจน์ทฤษฎี 3.5.1 ข้อ 8

---