บทที่ 4
ไอดีลและโควเชี่ยนริง
(Ideals and Quotient Rings)

สำหรับในบทนี้ จะกล่าวถึงไอดีลและโควเชี่ยนริง ซึ่งเป็นการสร้างริงอีกแบบหนึ่ง และจะกล่าวถึงแม็กซิมัลและไอดีลเฉพาะ (maximal and prime ideals)

4.1 ไอดีล (Ideals)

นิยาม 4.1.1 ให้ $\mathfrak{U}$ เป็นสับริงของริง R

1. $\mathfrak{U}$ จะเป็นไอดีลทางขวา (Right ideal) ของ A ถ้าทุก ๆ สมาชิก $a \varepsilon \mathfrak{U}, r \varepsilon R$ แล้ว $ar \varepsilon \mathfrak{U}$

2. $\mathfrak{U}$ จะเป็นไอดีลทางซ้าย (Left ideal) ของ R ถ้าทุก ๆ สมาชิก $a \varepsilon \mathfrak{U}, r \varepsilon R$ แล้ว $ra \varepsilon \mathfrak{U}$

3. $\mathfrak{U}$ จะเป็นไอดีล (Ideal) ของ R ถ้า $\mathfrak{U}$ เป็นทั้งไอดีลทางซ้ายและไอดีลทางขวาของ R นั่นคือ $\mathfrak{U}$ จะเป็นไอดีลของ R ถ้าสำหรับทุก ๆ $a \varepsilon \mathfrak{U}, r \varepsilon R$ แล้วจะได้ว่า ar และ $ra \varepsilon \mathfrak{U}$

หมายเหตุ 1. ถ้า R เป็นคอมมิวเททีฟริง แล้วไอดีลทางขวาและไอดีลทางซ้ายของ R จะเหมือนกัน

2. ทุก ๆ ริง R จะมีไอดีล 2 ไอดีลเสมอคือ R และ $\{0\}$ เรียกว่าทริเวียลไอดีล (Trivial Ideals) หรือ อิมพรอพเปอร์ไอดีล (Improper Ideals) สำหรับไอดีลอื่น ๆ ของ R ที่ไม่ใช่ 2 ไอดีลที่กล่าวมาแล้ว จะเรียกว่าไอดีลแท้ (Proper Ideals)

ตัวอย่าง 4.1.1 จากตัวอย่าง 2.1.1 ได้ว่า E เป็นสับริงของ I ซึ่งเป็นคอมมิวเทตีฟริง และ E จะเป็นไอดีลของ I ด้วย เพราะว่าผลคูณของจำนวนเต็มคู่กับจำนวนเต็มใด ๆ ของ I ยังคงเป็นจำนวนเต็มคู่

ตัวอย่าง 4.1.2 ให้ I เป็นริงของจำนวนเต็ม และ Q เป็นริงของจำนวนตรรกยะ จะได้ว่า I เป็นสับริงของ Q แต่ I ไม่เป็นไอดีลของ Q เนื่องจาก $3 \in I$, $\frac{1}{2} \in Q$ แต่ $3 \cdot \frac{1}{2} = \frac{3}{2} \notin I$

ตัวอย่าง 4.1.3 ให้ $K = \{a, b, c, d\}$ โดยนิยามการบวกและการคูณตามตารางต่อไปนี้

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	a	a	a
d	a	b	c	d

จากตารางการบวกและการคูณจะเห็นว่า K เป็นริง และเนื่องจาก $cd = a \neq c = dc$ ดังนั้น K ไม่เป็นคอมมิวเทตีฟริง

และพบว่าเซ็ต $\{a, b\}$ เป็นสับริงของ K

พิจารณา $aa = a$ และ $ab = a$

$ba = a$ และ $bb = b$

$ca = a$ และ $cb = a$

$da = a$ และ $db = b$

นั่นคือ $\{a, b\}$ เป็นไอดีลทางซ้ายของ K

พิจารณา $aa = a$ และ $ba = a$

$ab = a$ และ $bb = b$

$ac = a$ และ $bc = c$

$ad = a$ และ $bd = d$

ดังนั้น $\{a, b\}$ ไม่เป็นไอดีลทางขวาของ K เนื่องจาก $bc = c \notin \{a, b\}$ และ $bd = d \notin \{a, b\}$

แสดงว่า $\{a, b\}$ ไม่เป็นไอดีลของ K

<u>ตัวอย่าง 4.1.4</u> ให้ W เป็นริงของเมตริกซ์ขนาด 2×2 โดยมีสมาชิกในเมตริกซ์เป็นจำนวนเต็ม

ให้ $A = \{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \varepsilon W \;/\; a, b \;\varepsilon\; I$ โดยที่ $a \neq 0, b \neq 0\}$

จะแสดงว่า A ไม่เป็นไอดีลของ W

จากนิยามของ A ได้ว่า $A \subseteq W$ และ $A \neq \emptyset$

ให้ $\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} \varepsilon A$

เนื่องจาก $\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1-a_2 & b_1-b_2 \\ 0 & 0 \end{pmatrix} \varepsilon A$

และ $\begin{pmatrix} a_1 & b_1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 \\ 0 & 0 \end{pmatrix} \varepsilon A$

นั่นคือ A เป็นสับริงของ W

ให้ $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ เป็นสมาชิกใด ๆ ใน W และ $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \varepsilon A$

พิจารณา $\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} xa & xb \\ za & zb \end{pmatrix} \notin A$ เมื่อ $z \neq 0$

ดังนั้น A ไม่เป็นไอดีลของ W

<u>ตัวอย่าง 4.1.5</u> ให้ I เป็นคอมมิวเทฟริงของจำนวนเต็ม และ a เป็นสมาชิกของ I กำหนด $(a) = \{ar / r \in I\}$ จะแสดงว่า (a) เป็นไอดีลของ I

เนื่องจาก $ar \in I$ สำหรับทุก ๆ $r \in I$

ดังนั้น $(a) \subseteq I$

และเนื่องจาก $0 \in I$ ซึ่งทำให้ $a0 = 0 \in (a)$

นั่นคือ $(a) \neq \emptyset$

ให้ $ar_1, ar_2 \in (a)$ สำหรับสมาชิก $r_1, r_2 \in I$

พิจารณา $ar_1 - ar_2 = a(r_1 - r_2)$

เนื่องจาก $r_1 - r_2 \in I$ ดังนั้น $a(r_1 - r_2) \in (a)$

นั่นคือ $ar_1 - ar_2 \in (a)$

พิจารณา $(ar_1)(ar_2) = a(r_1(ar_2))$

เนื่องจาก $r_1(ar_2) \in I$ ดังนั้น $a(r_1(ar_2)) \in (a)$

นั่นคือ $(ar_1)(ar_2) \in (a)$

ดังนั้น (a) เป็นสับริงของ I

ให้ $r \in I$ และ $as \in (a)$ สำหรับทุก ๆ สมาชิก $s \in I$

พิจารณา $r(as) = (ra)s$ (โดยกฎการรวมหมู่สำหรับการคูณ)

$= (ar)s$ (โดยกฎการสลับที่สำหรับการคูณ)

$= a(rs)$ (โดยกฎการรวมหมู่สำหรับการคูณ)

เนื่องจาก $rs \in I$ ดังนั้น $a(rs) \in (a)$

นั่นคือ $r(as) \in (a)$

ในทำนองเดียวกัน จะได้ว่า $(as)r = a(sr) \in (a)$

ดังนั้น (a) เป็นไอดีลของ I

<u>ทฤษฎี 4.1.1</u> กำหนดให้ R เป็นริงที่มียูนิตี้ e ถ้า U เป็นไอดีลของ R ซึ่ง $e \in U$ แล้วจะได้ว่า $U = R$

<u>พิสูจน์</u> เนื่องจาก U เป็นไอดีลของ R ดังนั้น $U \subseteq R$

ให้ r เป็นสมาชิกใด ๆ ของ R

ดังนั้น $r = re \in U$ (เพราะว่า U เป็นไอดีลของ R และ $e \in U$)

นั่นคือ $R \subseteq U$

ดังนั้น $U = R$

<u>ทฤษฎี 4.1.2</u> กำหนดให้ R เป็นริงที่มียูนิตี้ e ถ้า U เป็นไอดีลแท้ของ R แล้วจะไม่มีสมาชิกตัวใดของ U ที่มีอินเวอร์สสำหรับการคูณ

<u>พิสูจน์</u> เนื่องจาก U เป็นไอดีลแท้ของ R

ดังนั้น $U \neq R$ และ $U \neq \{0\}$

สมมุติว่ามีสมาชิกบางตัวของ U คือ a โดยที่ $a \neq 0 \ni a^{-1} \in R$

เนื่องจาก $a \in U$ และ $a^{-1} \in R$

ดังนั้น $aa^{-1} \in U$

นั่นคือ $e \in U$

จะได้ว่า $U = R$ (โดยทฤษฎี 4.1.1)

ซึ่งจะขัดแย้งกับที่กำหนดให้ U เป็นไอดีลแท้ของริง R

ดังนั้นจะไม่มีสมาชิกตัวใดของ U ที่มีอินเวอร์สสำหรับการคูณ

<u>ทฤษฎี 4.1.3</u> ให้ ϕ เป็นโฮโมมอร์ฟิซึมจากริง R ไปยังริง R' จะได้ว่า

1. ถ้า S เป็นไอดีลของ R แล้ว $\phi(S)$ จะเป็นไอดีลของ $\phi(R)$
2. ถ้า S' เป็นไอดีลของ $\phi(R)$ แล้ว $\phi^{-1}(S')$ จะเป็นไอดีลของ R

<u>พิสูจน์</u> ข้อ 1 จากทฤษฎี 2.3.1 ได้ว่า $\phi(S)$ เป็นสับริงของ R'

ให้ $s' \in \phi(S)$ และ $r' \in \phi(R)$

นั่นคือ $s' = \phi(s)$ และ $r' = \phi(r)$ สำหรับ $s \in S$ และ $r \in R$

เนื่องจาก S เป็นไอดีลของ R ดังนั้น $rs \in S$ และ $sr \in S$

พิจารณา $s'r' = \phi(s)\,\phi(r)$

$= \phi(sr)$ (เพราะว่า ϕ เป็นโฮโมมอร์ฟิซึม)

ดังนั้น $s'r' \in \phi(S)$ เพราะว่า $\phi(sr) \in \phi(S)$

ในทำนองเดียวกัน $r's' = \phi(r)\,\phi(s)$

$= \phi(rs)$

ดังนั้น $r's' \in \phi(S)$ เพราะว่า $\phi(rs) \in \phi(S)$

นั่นคือ $\phi(S)$ เป็นไอดีลของ $\phi(R)$

ข้อ 2 จากทฤษฎี 2.3.1 ได้ว่า $\phi^{-1}(S')$ เป็นสับริงของ R

ให้ $s \in \phi^{-1}(S')$ และ $r \in R$

เนื่องจาก $\phi(r) \in \phi(R)$ และ $\phi(s) \in S'$ และ S' เป็นไอดีลของ $\phi(R)$

ดังนั้น $\phi(rs) = \phi(r)\,\phi(s) \in S'$

และ $\phi(sr) = \phi(s)\,\phi(r) \in S'$

นั่นคือ $rs \in \phi^{-1}(S')$

และ $sr \in \phi^{-1}(S')$

ดังนั้น $\phi^{-1}(S')$ เป็นไอดีลของ R

<u>ทฤษฎี 4.1.4</u> ถ้า R และ R' เป็นริงใด ๆ และ $\emptyset : R \longrightarrow R'$ เป็นโฮโมมอร์ฟิซึม จะได้ว่า $Ker(\emptyset)$ เป็นไอดีลของ R

<u>พิสูจน์</u> เนื่องจาก $Ker(\emptyset) = \{r \in R \,/\, \emptyset(r) = 0'\}$

ดังนั้น $Ker(\emptyset) \subseteq R$

เนื่องจาก $0 \in R$ และ $\emptyset(0) = 0'$ โดยทฤษฎี 2.3.1 ข้อ 1

ดังนั้น $0 \in Ker(\emptyset)$

นั่นคือ $Ker(\emptyset) \neq \emptyset$

ให้ $r, s \in Ker(\emptyset)$ นั่นคือ $\emptyset(r) = 0'$ และ $\emptyset(s) = 0'$

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

ดังนั้น $r - s \in Ker(\emptyset)$

และ
$$\begin{aligned} \emptyset(rs) &= \emptyset(r)\,\emptyset(s) \\ &= 0'0' \\ &= 0' \end{aligned}$$

ดังนั้น $rs \in Ker(\emptyset)$

นั่นคือ $Ker(\emptyset)$ เป็นสับริงของ R

สำหรับทุก ๆ สมาชิก $a \in Ker(\emptyset),\ r \in R$

พิจารณา
$$\begin{aligned} \emptyset(ar) &= \emptyset(a)\,\emptyset(r) \\ &= 0'\,\emptyset(r) \\ &= 0' \end{aligned}$$

และ $\phi(ra) = \phi(r)\,\phi(a)$

$= \phi(r)0'$

$= 0'$

ดังนั้น ar และ $ra \in \text{Ker}(\phi)$ นั่นคือ $\text{Ker}(\phi)$ เป็นไอดีลของ R

4.2 <u>โควเชี่ยนริง</u> (Quotient Ring)

กำหนดให้ U เป็นไอดีลของริง R จากนิยามของไอดีล ทราบว่า U จะต้องเป็นสับริงของ R นั่นคือ สำหรับทุก ๆสมาชิก $a, b \in U$ แล้ว $a-b \in U$ ซึ่งคุณสมบัตินี้แสดงว่า U เป็นอบีเลี่ยน สับกรุปของ R ภายใต้การบวก

พิจารณาโคเซ็ต (Coset) ของ U ใน R ดังต่อไปนี้

สำหรับ $r \in R,\ r + U = \{r + a \,/\, a \in U\}$

$= \{a + r \,/\, a \in U\}$

$= U + r$

ให้ $R/_U$ เป็นเซ็ตของโคเซ็ตของ U ใน R ทั้งหมดที่แตกต่างกัน ซึ่งโคเซ็ตเหล่านี้จะอยู่ในรูปของ $r + U$ เมื่อ $r \in R$

กำหนดการบวกและการคูณในเซ็ตของ $R/_U$ ดังต่อไปนี้

<u>เล็มม่า 4.2.1</u> ถ้า U เป็นไอดีลของริง R และ $a, b \in R$ จงพิสูจน์ว่า

ก. $a + U = U$ ก็ต่อเมื่อ $a \in U$

ข. $a + U = b + U$ ก็ต่อเมื่อ $a - b \in U$

<u>พิสูจน์</u> ก. <u>ตอนแรก</u> ให้ $a + U = U$ จะพิสูจน์ว่า $a \in U$

สมมุติให้ $a + U \in U$

เนื่องจาก $a + U = U$

ดังนั้น $a + u \in U$

เนื่องจาก U เป็นสับริง ดังนั้นจะมี $-u \in U$

แล้วได้ว่า $(a + u) + (-u) \in U$

พิจารณา $a + [u + (-u)] = a + 0$

$= a$

ดังนั้น $a \in U$

<u>ตอนสอง</u> ให้ $a \in U$ แล้วจะพิสูจน์ว่า $a + U = U$

สมมุติให้ $a + u_1$ เป็นสมาชิกใดๆ ใน $a + U$

เนื่องจาก $a \in U$ ดังนั้น $a + u_1 \in U$ (โดยคุณสมบัติของสับริง)

นั่นคือ $a + U \subseteq U$

ต่อไปสมมุติให้ $u_2 \in U$

เนื่องจาก $a \in U$ จะได้ว่า $a + u_2 \in U$

แต่ $a + u_2 \in a + U$ (จากนิยามของโคเซ็ต)

ดังนั้น $U \subseteq a + U$ --------(2)

จาก (1) และ (2) จะได้ว่า $a + U = U$ เมื่อ $a \in U$

ข. <u>ตอนแรก</u> สมมุติให้ $a + U = b + U$ จะพิสูจน์ $a - b \varepsilon U$

ให้ $a + u_1 \varepsilon a + U$

เนื่องจาก $a + U = b + U$

ดังนั้นจะมี $u_2 \varepsilon U$ ซึ่งทำให้ $a + u_1 = b + u_2$

และได้ว่า $a - b = u_2 - u_1$

แต่ $u_2 - u_1 \varepsilon U$ ดังนั้น $a - b \varepsilon U$

<u>ตอนสอง</u> สมมุติให้ $a - b \varepsilon U$ จะพิสูจน์ว่า $a + U = b + U$

เนื่องจาก $a - b \varepsilon U$

สมมุติให้ $a - b = u$ โดยที่ $u \varepsilon U$

และให้ $a + u_1 \varepsilon a + U$

พิจารณา $a + u_1 = (u + b) + u_1$ (เพราะว่า $a - b = u$)

$= (b + u) + u_1$

$= b + (u + u_1)$

แต่ $b + (u + u_1) \varepsilon b + U$

ดังนั้น $a + u_1 \varepsilon b + U$

จะได้ว่า $a + U \subseteq b + U$ --------- (1)

ต่อไปสมมุติให้ $b + u_2 \varepsilon b + U$

พิจารณา $b + u_2 = [a + (-u)] + u_2$ (เพราะว่า $a - b = u$)

$= a + [(-u) + u_2]$

แต่ $a + [(-u) + u_2] \varepsilon a + U$

ดังนั้น $b + u_2 \varepsilon a + U$

แสดงว่า $b + U \quad a + U$ --------(2)

จาก (1) และ (2) จะได้ว่า $a + U = b + U$

นิยาม 4.2.1 ให้ $r+U$ และ $s+U$ เป็นสมาชิกของ $R/_U$
กำหนดการบวกใน $R/_U$ ดังนี้

$$(r+U)+(s+U) = (r+s)+U$$

กำหนดการคูณใน $R/_U$ ดังนี้

$$(r + U)(s + U) = rs + U$$

จะแสดงว่าการบวกและการคูณของโคเซ็ตของ U ใน R กำหนดถูกต้องแล้ว (Well defined)

สมมุติว่า $r + U = r' + U$ และ $s + U = s' + U$ สำหรับ $r + U,\ r' + U,\ s + U$ และ $s' + U \in R/_U$

เนื่องจาก $(r + U) + (s + U) = (r + s) + U$

และ $(r' + U) + (s' + U) = (r' + s') + U$

เนื่องจาก $r + U = r' + U$

ดังนั้นจะมี $a_1 \in U$ ซึ่ง

$$r + 0 = r' + a_1$$

นั่นคือ $r = r' + a_1$

และเนื่องจาก $s + U = s' + U$

ดังนั้นจะมี $a_2 \in U$ ซึ่ง

$$s + 0 = s' + a_2$$

นั่นคือ $s = s' + a_2$

ดังนั้น
$$\begin{aligned} r + s &= (r' + a_1) + (s' + a_2) \\ &= (r' + s') + (a_1 + a_2) \end{aligned}$$

ให้ $a = a_1 + a_2$ จะได้ว่า $a \in U$ (เพราะว่า U เป็นไอดีลของ R)

ดังนั้นจะได้ $r + s = (r' + s') + a$

และ $(r + s) + U = (r' + s') + a + U$

เนื่องจาก $a \in U$ ดังนั้นจะได้ว่า $a + U = U$ (โดยเล็มม่า 4.2.1 ข้อ ก.)

ดังนั้น $(r + s) + U = (r' + s') + U$

นั่นคือ การบวกของโคเซ็ตกำหนดถูกต้องแล้ว

เนื่องจาก $rs = (r' + a_1)(s' + a_2)$

$= r's' + a_1s' + r'a_2 + a_1a_2$

เนื่องจาก U เป็นไอดีลของ R ดังนั้น $a_1s, r'a_2, a_1a_2 \in U$

ให้ $b = a_1s' + r'a_2 + a_1a_2$

ดังนั้น $rs = r's' + b$

และ $rs + U = r's' + b + U$

เนื่องจาก $b \in U$ ดังนั้นจะได้ว่า $b + U = U$

ดังนั้น $rs + U = r's' + U$

นั่นคือ การคูณของโคเซ็ตกำหนดถูกต้องแล้ว

<u>ทฤษฎี 4.2.1</u> กำหนดให้ $R/_U$ เป็นเซ็ตของโคเซ็ตของไอดีล U ในริง R จะได้ว่า $R/_U$ เป็นริงภายใต้การบวกและการคูณของโคเซ็ต

<u>พิสูจน์</u> 1. จะแสดงว่าการบวกของโคเซ็ตเป็นไบนารี่โอเปอเรชันในเซ็ต $R/_U$

ให้ $a + U, b + U \in R/_U$ สำหรับ $a, b \in R$ และ U เป็นไอดีลของ R

พิจารณา $(a + U) + (b + U) = (a + b) + U$

เนื่องจาก $a + b \in R$ ดังนั้น $(a + b) + U \in R/_U$

นั่นคือ การบวกของโคเซ็ตเป็นไบนารี่โอเปอเรชันบนเซ็ต $R/_U$

2. จะแสดงว่าการบวกของโคเซ็ตสอดคล้องกฎการรวมหมู่

ให้ $a + U$, $b + U$ และ $c + U \in R/_U$ เมื่อ $a, b, c \in R$

พิจารณา $[(a + U) + (b + U)] + (c + U) = [(a + b) + U] + (c + U)$

$= [(a + b) + c] + U$

$= [a + (b + c)] + U$

(โดยกฎการรวมหมู่สำหรับการบวกใน R)

$= (a + U) + [(b + c) + U]$

$= (a + U) + [(b + U) + (c + U)]$

นั่นคือ การบวกของโคเซ็ตสอดคล้องกฎการรวมหมู่

3. จะมี $0 + U$ เป็นสมาชิกศูนย์ใน $R/_U$

ซึ่ง $(a + U) + (0 + U) = (a + 0) + U$ สำหรับ $a \in R$ และ 0 คือสมาชิกศูนย์ใน R

$= a + U$

และ $(0 + U) + (a + U) = (0 + a) + U$

$= a + U$

นั่นคือ $0 + U$ หรือ U คือสมาชิกศูนย์ใน $R/_U$

4. สำหรับ $a + U \in R/_U$ จะมี $(-a) + U$ เป็นอินเวอร์ส สำหรับการบวกของ $a + U$ ใน $R/_U$ เพราะว่า

$(a + U) + [(-a) + U] = [a + (-a)] + U$

$= 0 + U$

$= U$

และ $\left[(-a) + U\right] + (a + U) = \left[(-a) + a\right] + U$

$$= 0 + U$$

$$= U$$

ดังนั้น $(-a) + U$ เป็นอินเวอร์สสำหรับการบวกของ $a + U$ ใน $R/_U$

5. จะแสดงว่าการบวกของโคเซ็ตสอดคล้องกฎการสลับที่

ให้ $a + U,\ b + U \in R/_U$

ดังนั้น $(a + U) + (b + U) = (a + b) + U$

$= (b + a) + U$ (โดยกฎการสลับที่ สำหรับการบวกใน R)

$= (b + U) + (a + U)$

นั่นคือ กฎการสลับที่สำหรับการบวกเป็นจริงใน $R/_U$

6. จะแสดงว่าการคูณของโคเซ็ตเป็นไบนารี่โอเปอเรชันใน $R/_U$

ให้ $a + U,\ b + U \in R/_U$

พิจารณา $(a + U)(b + U) = ab + U$

เนื่องจาก $ab \in R$ ดังนั้น $ab + U \in R/_U$

นั่นคือ การคูณของโคเซ็ตเป็นไบนารี่โอเปอเรชันบนเซ็ต $R/_U$

7. จะแสดงว่าการคูณของโคเซ็ตสอดคล้องกฎการรวมหมู่

ให้ $a + U,\ b + U,\ c + U \in R/_U$ สำหรับ $a, b, c \in R$

พิจารณา $\left[(a+U)(b+U)\right](c+U) = (ab+U)(c+U)$

$= \left[(ab)c + U\right]$

$= \left[a(bc) + U\right]$

(โดยกฎการรวมหมู่สำหรับการคูณใน R)

$= (a+U)(bc+U)$

$= (a+U)\left[(b+U)(c+U)\right]$

8. จะแสดงว่ากฎการกระจายเป็นจริงใน $R/_U$

ให้ $a+U$, $b+U$ และ $c+U \in R/_U$

พิจารณา $(a+U)\left[(b+U)+(c+U)\right] = (a+U)\left[(b+c)+U\right]$

$= a(b+c) + U$

$= (ab+ac) + U$

(โดยกฎการกระจายใน R)

$= (ab+U) + (ac+U)$

$= (a+U)(b+U)$

$+ (a+U)(c+U)$

นั่นคือกฎการกระจายเป็นจริงใน $R/_U$

แสดงว่า $R/_U$ เป็นริงภายใต้การบวกและการคูณของโคเซ็ต

<u>นิยาม 4.2.3</u> ริง $R/_U$ ในทฤษฎี 4.2.1 เรียกว่าโควเชี่ยนริง หรือแฟคเตอร์ริง (Quotient Ring or Factor Ring)

<u>หมายเหตุ</u> 1. ถ้า R เป็นริงที่มียูนิตี้ e แล้วจะได้ว่า $R/_U$ เป็นริงที่มียูนิตี้คือ e + U เพราะว่า สำหรับทุก ๆ สมาชิก (e + U), (r + U) ε $R/_U$ แล้วจะได้ว่า

$$\begin{aligned}(e + U)(r + U) &= er + U \\ &= r + U \\ &= re + U \\ &= (r + U)(e + U)\end{aligned}$$

2. ถ้า R เป็นคอมมิวเททีพริง จะได้ว่า $R/_U$ เป็นคอมมิวเททีพริงด้วย เพราะว่าสำหรับทุก ๆ สมาชิก (r + U), (s + U) ε $R/_U$ จะได้ว่า

$$\begin{aligned}(r + U)(s + U) &= rs + U \\ &= sr + U \\ &= (s + U)(r + U)\end{aligned}$$

3. เนื่องจากทุก ๆ ริง R จะมีอย่างน้อย 2 ไอดีลคือ R และ {0} ดังนั้นจะมีโควเชี่ยนที่เกิดจาก 2 ไอดีลนี้คือ $R/_R$ ซึ่งมีสมาชิกเพียง 1 โคเซ็ตคือ r + R สำหรับ r ε R และ $R/_{\{0\}}$ ซึ่งก็คือริง R นั่นเอง

<u>ตัวอย่าง 4.2.1</u> จากตัวอย่าง4.1.5 ได้ว่า (a) เป็นไอดีลของ I ดังนั้น $I/_{(a)}$ เป็นโควเชี่ยนริง

แบบฝึกหัด 4 ก

1. จงพิสูจน์ว่าโควเชี่ยนริงของไอดีล U ใน R เป็นคอมมิวเทตีฟ ก็ต่อเมื่อ $(rs - sr) \varepsilon U$ สำหรับทุก ๆ สมาชิก $r, s \varepsilon R$

2. จงพิสูจน์ว่า ถ้า R เป็นริงที่มียูนิตี้ และ U เป็นไอดีลของ R โดยที่ $U \neq R$ แล้ว $R/_U$ จะเป็นริงที่มียูนิตี้

3. จงแสดงว่าอินเตอร์เซคชันของไอดีลของริง R เป็นไอดีลของริง R

4. ให้ R เป็นคอมมิวเทตีฟริง และให้ $a \varepsilon R$ จงแสดงว่า

   $I_a = \{x \varepsilon R/ ax = 0\}$ เป็นไอดีลของ R

5. ถ้า A และ B เป็นไอดีลของริง R กำหนดผลบวกของ A กับ B คือ $A + B$ ดังนี้ $A + B = \{a + b/ a \varepsilon A, b \varepsilon B\}$

   จงพิสูจน์ว่า $A + B$ เป็นไอดีลของ R

6. กำหนดให้ A และ B เป็นไอดีลของริง R กำหนดผลคูณของ A และ B ดังนี้

   $$AB = \{ \sum_{i=1}^{n} a_i b_i / a_i \varepsilon A, b_i \varepsilon B, n \varepsilon I^+\}$$

   จงแสดงว่า AB เป็นไอดีลของ R

7. ถ้า U เป็นไอดีลของริง R และ $a, b \varepsilon R$ จงพิสูจน์ว่า

   ก. $a + U = U$ ก็ต่อเมื่อ $a \varepsilon U$

   ข. $a + U = b + U$ ก็ต่อเมื่อ $a - b \varepsilon U$

<u>ทฤษฎี 4.2.2</u> ถ้า U เป็นไอดีลของริง R แล้ว จะได้ว่า $\alpha : R \longrightarrow R/_U$ ซึ่งกำหนดโดย $\alpha(r) = r + U$ สำหรับสมาชิก $r \in R$ เป็นโฮโมมอร์ฟิซึม

<u>พิสูจน์</u> ให้ $r, s \in R$

ดังนั้น
$$\begin{aligned}\alpha(r + s) &= (r + s) + U \\ &= (r + U) + (s + U) \\ &= \alpha(r) + \alpha(s)\end{aligned}$$

และ
$$\begin{aligned}\alpha(rs) &= rs + U \\ &= (r + U)(s + U) \\ &= \alpha(r)\alpha(s)\end{aligned}$$

นั่นคือ α เป็นโฮโมมอร์ฟิซึม

<u>หมายเหตุ</u> ฟังก์ชัน α ในทฤษฎี 4.2.2 เรียกว่าฟังก์ชันธรรมชาติ (natural function หรือ canonical function)

<u>ทฤษฎี 4.2.3</u> ทฤษฎีหลักมูลโฮโมมอร์ฟิซึม (Fundamental Homomorphism Theorem)

ให้ ϕ เป็นโฮโมมอร์ฟิซึมจากริง R ไปยัง R' ถ้า ϕ เป็นออนทู และ $\mathrm{Ker}\,(\phi) = K$ แล้วจะได้ว่า $R/_K \cong R'$

<u>พิสูจน์</u> กำหนดฟังก์ชัน $\psi : R/_K \longrightarrow R'$

โดย $\psi(r + K) = \phi(r)$ สำหรับ $r + K \in R/_K$

1. จะแสดงว่า ψ เป็นโฮโมมอร์ฟิซึม

ให้ $r_1 + K, r_2 + K \in R/_K$

พิจารณา $(r_1+K) + (r_2+K) = \Psi[(r_1+r_2) + K]$

$= \phi(r_1+r_2)$

$= \phi(r_1) + \phi(r_2)$

(เพราะว่า ϕ เป็นโฮโมมอร์ฟิซึม)

$= \Psi(r_1+K) + \Psi(r_2+K)$

และ $\Psi[(r_1+K)(r_2+K)] = \Psi(r_1r_2+K)$

$= \phi(r_1r_2)$

$= \phi(r_1)\,\phi(r_2)$

$= \Psi(r_1+K)\,\Psi(r_2+K)$

นั่นคือ Ψ เป็นโฮโมมอร์ฟิซึม

2. จะแสดงว่า Ψ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

นั่นคือต้องแสดงว่า ถ้า $\Psi(r_1+K) = \Psi(r_2+K)$ แล้วจะได้ $r_1+K = r_2+K$

สำหรับ $r_1, r_2 \in R$

สมมุติให้ $\Psi(r_1 + K) = \Psi(r_2 + K)$

นั่นคือ $\phi(r_1) = \phi(r_2)$

เนื่องจาก $\phi(r_2) + [-\phi(r_2)] = 0'$

ดังนั้น $\phi(r_2) + [-\phi(r_1)] = 0'$

จะได้ $\phi(r_2) + \phi(-r_1) = 0'$ (โดยทฤษฎี 2.3.1 ข้อ 2)

ดังนั้น $\phi(r_2 - r_1) = 0'$

นั่นคือ $r_2 - r_1 \in K$

ดังนั้น $r_1 + K = r_2 + K$ (โดยเล็มม่า 4.2.1 ข้อ ข)

นั่นคือ Ψ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

3. จะแสดงว่า ψ เป็นฟังก์ชันออนทู

ให้ $r' \in R'$

ดังนั้น จะมี $r \in R$ โดยที่ $r' = \phi(r)$

$= \psi(r + K)$

นั่นคือ ψ เป็นฟังก์ชันออนทู

ดังนั้น ψ เป็นไอโซมอร์ฟิซึม ψ นั่นคือ $R/_K \cong R'$

<u>แบบฝึกหัด 4 ข.</u>

1. (First Isomorphism Theorem for Rings) ให้ M และ N เป็นไอดีลของริง R โดยที่ M เป็นสับกรุ๊ปของ N จงพิสูจน์ว่า
$R/_N \cong (R/_M)/(N/_M)$

2. (Second Isomorphism Theorem for Rings) ให้ M และ N เป็นไอดีลของริง R และให้ $M + N = \{m+n \mid m \in M, n \in N\}$ จงพิสูจน์ว่า $M + N$ เป็นไอดีลของ R และ $(M + N)_{/N} \cong M_{/(M \cap N)}$

3. จงแสดงว่า $\phi : C \longrightarrow M_2(R)$ กำหนดโดย

$$\phi(a + b_i) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

สำหรับ $a, b \in R$ เป็นไอโซมอร์ฟิซึมจาก C ไปยัง $M_2(R)$

4. ถ้า U เป็นไอดีลของริง R จงพิสูจน์ว่า เมตริกซ์ริง

$M_n(R/_U) \cong M_n(R) / M_n(U)$

[Hint : พิจารณาฟังก์ชัน $\emptyset : M_n(R) \dashrightarrow M_n(R/_U)$ กำหนดโดย

$\emptyset((a_{ij})) = (a_{ij} + U)$]

5. สมมุติ S เป็นสับริง และ U เป็นไอดีลของริง R ถ้า $S \quad U = \{0\}$ จงพิสูจน์ว่า S ไอโซมอร์ฟิคกับสับริงของโควเชี่ยนริง $R/_U$

(Hint : ใช้ฟังก์ชัน $\emptyset(a) = a + U$ เมื่อ $a \in S$)

- - - - -

4.3 แม็กซิมัลและไอดีลเฉพาะ (Maximal and Prime Ideals)

4.3.1 แม็กซิมัลไอดีล (Maximal Ideal)

นิยาม 4.3.1 ให้ M เป็นไอดีลของริง R ใดๆ และ $M \neq R$ จะกล่าวว่า M เป็นแม็กซิมัลไอดีลของริง R ต่อเมื่อ U เป็นไอดีลใดๆ ของ R ซึ่ง $M \subsetneq U \subsetneq R$ แล้วได้ว่า $R = U$ หรือ $U = M$ อย่างใดอย่างหนึ่ง

เล็มมา 4.3.1 ให้ I เป็นริงของจำนวนเต็ม กำหนดให้ $(a) = \{ar \,/\, r \in I\}$ และ $(ab) = \{(ab)r \,/\, r \in I\}$ สำหรับ $a, b \in I$ จะได้ว่า $(ab) \subsetneq (a)$

พิสูจน์ สมมุติให้ m เป็นสมาชิกใดใน (ab)

ดังนั้น $m = (ab)r$ เมื่อ $r \in I$

$= a(br)$

เนื่องจาก $b, r \varepsilon I$ จะได้ว่า $br \varepsilon I$

สมมุติให้ $br = r_1$

ดังนั้น $m = ar_1$ โดยที่ $r_1 \varepsilon I$

นั่นคือ $m \varepsilon (a)$

แสดงว่า $(ab) \subseteq (a)$

<u>ตัวอย่าง 4.3.1</u> ให้ I เป็นริงของจำนวนเต็ม และ $(a) = \{ar / r \varepsilon I\}$

สำหรับ $a \varepsilon I$ จงหาค่า a ที่ทำให้ (a) เป็นแม็กซิมัลไอดีล

จากตัวอย่าง 4.1.5 ได้ว่า (a) เป็นไอดีลของ I สำหรับ $a \varepsilon I$

ตอนแรกจะแสดงว่า ถ้าให้ p เป็นจำนวนเฉพาะ (prime number)

แล้วจะได้ว่า $A = (p)$ เป็นแม็กซิมัลไอดีลของ I

ให้ U เป็นไอดีลของ I และ $A \subseteq U$ โดย

$U = (a)$ เมื่อ a เป็นจำนวนเต็ม

เนื่องจาก $p \varepsilon A \subseteq U$

(ดูหน้าต่อไป)

ดังนั้น $p \varepsilon U$ และ $p = ma$ เมื่อ m เป็นจำนวนเต็ม

เนื่องจาก p เป็นจำนวนเฉพาะดังนั้น $a = 1$ หรือ $a = p$

ถ้า $a = p$ จะได้ว่า $U = (a) = (p) = A$

นั่นคือ $A = U$

ถ้า $a = 1$ ดังนั้น $1 \varepsilon U$

โดยทฤษฎี 4.1.1 จะได้ $U = I$

ดังนั้น A เป็นแม็กซิมัลไอดีลของ I

ในทางกลับกัน ถ้า $M = (a)$ เป็นแม็กซิมัลไอดีลของ I แล้วจะแสดงว่า a เป็นจำนวนเฉพาะ

ให้ $a = xy$ โดยที่ x, y เป็นจำนวนเต็มบวก

ถ้าให้ $U = (x)$ จะได้ว่า U เป็นไอดีลของ I

เนื่องจาก $M = (xy)$ และ $U = (x)$

ดังนั้น $M \subseteq U$

เนื่องจาก M เป็นแม็กซิมัลไอดีล ดังนั้น $U = M$ หรือ $U = I$

ถ้า $U = I$ แสดงว่า $U = (1)$ (เพราะว่า $(1) = \{1n/n \varepsilon I\} = I$)

นั่นคือ $x = 1$ ดังนั้น $a = 1y$

ถ้า $U = M$ จะได้ว่า $x \varepsilon M$

นั่นคือ $x = ar$ สำหรับบางสมาชิก $r \varepsilon I$

ดังนั้น $a = xy = (ar)y$

จะได้ $1 = ry$

นั่นคือ $y = 1$

ดังนั้น $a = x1$

แสดงว่า a เป็นจำนวนเฉพาะ

ดังนั้น (a) จะเป็นแม็กซิมัลไอดีลของ I ก็ต่อเมื่อ a เป็นจำนวนเฉพาะ

4.3.2 <u>ไอดีลเฉพาะ</u> (Prime Ideal)

<u>นิยาม 4.3.2</u> ให้ R เป็นคอมมิวเทที่ฟริงและ P เป็นไอดีลของ R จะกล่าวว่า P เป็นไอดีลเฉพาะของ R ถ้า $ab \in P$ สำหรับทุก ๆ $a,b \in R$ แล้ว ได้ว่า $a \in P$ หรือ $b \in P$ อย่างใดอย่างหนึ่ง

<u>ตัวอย่าง 4.3.2</u> สำหรับไอดีล (n) ของริง I ถ้า n ไม่เป็นจำนวนเฉพาะ จะแสดงได้ว่า (n) ไม่เป็นไอดีลเฉพาะของ I

ให้ $n = n_1n_2$ เมื่อ $1 < n_1, n_2 < n$

ดังนั้น $n_1n_2 \in (n)$

เนื่องจาก ทั้ง n_1 และ n_2 ไม่สามารถเขียนเป็นผลคูณของจำนวนเต็มกับ n (integeral multiple of n)

นั่นคือ $n_1 \neq an$ และ $n_2 \neq bn$ สำหรับ $a, b \in I$

ดังนั้น $n_1 \notin (n)$ และ $n_2 \notin (n)$

นั่นคือ (n) ไม่เป็นไอดีลเฉพาะของ I

<u>ตัวอย่าง 4.3.3</u> สำหรับ {0} และ I ซึ่งเป็นทริเวียลไอดีลของ I จะได้ว่า {0} และ I เป็นไอดีลเฉพาะของ I

<u>เลมมา 4.3.1</u> ถ้า R เป็นคอมมิวเทที่ฟริงที่มียูนิตี้และ M เป็นแมกซิมัลไอดีลของ R ให้ $N = \{ra + m /\ a, r \in R, m \in M$ และ $a \notin M\}$ แล้วจะได้ว่า N เป็นไอดีลของ R และ $N = R$

<u>พิสูจน์</u> แบบฝึกหัด

<u>ทฤษฎี 4.3.2</u> ทุก ๆ แม็กซิมัลไอดีลของคอมมิวเทฟริง ที่มียูนิตี้ จะเป็นไอดีล-เฉพาะ

<u>พิสูจน์</u> ให้ R เป็นคอมมิวเทฟริง ที่มียูนิตี้ e และ M เป็นแม็กซิมัลไอดีลของ R

ให้ $ab \in M$ สำหรับ $a, b \in R$ และ $a \notin M$

จะต้องแสดงว่า $b \in M$ ซึ่งทำให้ได้ว่า M เป็นไอดีลเฉพาะ

ให้ $N = \{ra + m / r \in R, m \in M\}$

โดยเลมม่า 4.4.1 จะได้ $N = R$

ดังนั้น จะมี $m \in M, r \in R$ ซึ่ง $e = ra + m$

เนื่องจาก $ab \in M$ และ $m \in M$

ดังนั้น
$$\begin{aligned} b &= eb \\ &= (ra + m)b \\ &= r(ab) + mb \in M \end{aligned}$$
(เพราะว่า M เป็นไอดีลของ R)

นั่นคือ M เป็นไอดีลเฉพาะของ R

<u>ตัวอย่าง 4.3.4</u> สำหรับไอดีล (n) ของ I ถ้า n เป็นจำนวนเฉพาะ แล้วจะได้ว่า (n) เป็นไอดีลเฉพาะ

จากตัวอย่าง 4.4.1 ถ้า n เป็นจำนวนเฉพาะแล้วจะได้ว่า(n) เป็นแม็กซิมัลไอดีลของ I และจากทฤษฎี 4.4.2 ทำให้ได้ว่า (n) เป็นไอดีลเฉพาะ

แบบฝึกหัด 4 ค.

1. จงแสดงว่า N เป็นแม็กซิมัลไอดีลของริง R ก็ต่อเมื่อ R/N ไม่มีไอดีลแท้
2. จงพิสูจน์เลมมา 4.3.1
3. จงแสดงตัวอย่างของริงที่มีไอดีลเฉพาะบางอันที่ไม่เป็นแม็กซิมัลไอดีลของ R
4. ถ้า R เป็นคอมมิวเททีฟริงที่มีสมาชิกจำนวนจำกัด และ R มียูนิตี้ จงพิสูจน์ว่าทุก ๆ ไอดีลเฉพาะของ R จะเป็นแม็กซิมัลไอดีลของ R
5. จงพิสูจน์ว่า M เป็นไอดีลแท้ของริง R แล้ว M จะเป็นแม็กซิมัลไอดีล ก็ต่อเมื่อ สำหรับทุก ๆ สมาชิก $r \notin M$ แล้ว จะมีบางสมาชิก $a \in R$ ซึ่ง $1 + ra \in M$
6. ถ้า M_1 และ M_2 เป็นแม็กซิมัลไอดีลของริง R โดยที่ $M_1 \neq M_2$ แล้วจงพิสูจน์ว่า $M_1M_2 = M_1 \cap M_2$
7. ให้ M เป็นไอดีลแท้ของริง R, จงพิสูจน์ว่า M เป็นแม็กซิมัลไอดีล ก็ต่อเมื่อ สำหรับแต่ละไอดีล U ของ R แล้วจะได้ $U \subseteq M$ หรือ $U + M = R$
8. ไอดีล N ของริง R จะเรียกว่าเป็นมินิมัลไอดีล (minimal ideal) ของ R ถ้า $N \neq \{0\}$ และไม่มีไอดีล U ของ R ซึ่ง $\{0\} \subsetneq U \subsetneq N$

    ก. จงพิสูจน์ว่าไอดีล N ของ R ซึ่ง $N \neq \{0\}$ แล้ว N จะเป็นมินิมัลไอดีล ก็ต่อเมื่อ $N = (a)$ สำหรับสมาชิก $a \neq 0 \in N$

    ข. จงแสดงว่าริง I ไม่มีมินิมัลไอดีล.
