บทที่ 5
อินติกรัลโดเมนและฟิลด์
(Integral Domains and Fields)

ในบทนี้จะศึกษาถึงระบบพีชคณิตที่เรียกว่า อินติกรัลโดเมนและฟิลด์ สำหรับในเรื่องอินติกรัลโดเมน จะกล่าวถึงคุณสมบัติที่เรียกว่า คาแรคเตอริสติก และออเดอร์อินติกรัลโดเมน ส่วนเรื่องฟิลด์ จะกล่าวถึงนิยามและคุณสมบัติเบื้องต้นของฟิลด์ของเศษส่วน ของอินติกรัลโดเมน

5.1 อินติกรัลโดเมน (Integral Domain)

ก่อนจะให้นิยามของอินติกรัลโดเมน จะกล่าวถึงนิยามของตัวหารศูนย์ พิจารณาริง I จะพบว่า ถ้า $a \neq 0, b \neq 0$ สำหรับทุก ๆ สมาชิก $a, b \in I$ แล้ว จะได้ $ab \neq 0$ แต่ในริงบางอัน ซึ่งมีสมาชิก 2 ตัว ที่ไม่ใช่สมาชิกศูนย์ จะได้ผลคูณเป็นศูนย์ เช่นริง I_6 ซึ่งมี $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$ เป็นสมาชิก มี $\bar{2}.\bar{3} = \bar{0}$ และ $\bar{3}\ \bar{4} = \bar{0}$ โดยที่ $\bar{2} \neq \bar{0}$, $\bar{3} \neq \bar{0}$ และ $\bar{4} \neq \bar{0}$ โดยทั่ว ๆ ไป จะเรียกสมาชิกของริงที่ไม่ใช่สมาชิกศูนย์ แต่มีผลคูณเป็นศูนย์ว่า ตัวหารศูนย์ (zero divisor) เช่น เรียก $\bar{2}$, $\bar{3}$ และ $\bar{4}$ ว่าเป็นตัวหารศูนย์ใน I_6 ซึ่งนิยามของตัวหารศูนย์กล่าวได้ดังนี้

นิยาม 5.1.1 ถ้า a, b เป็นสมาชิกที่ไม่ใช่ศูนย์ของริง R ซึ่ง $ab = 0$ แล้วจะเรียก a และ b ว่าเป็นตัวหารศูนย์ (zero divisors) และเรียก a ว่าเป็นตัวหารศูนย์ทางซ้าย (left zero divisor) และ b ว่าตัวหารศูนย์ทางขวา (right zero divisor)

นิยาม 5.1.2 ถ้าสมาชิกทุกตัวของริง R ไม่เป็นตัวหารศูนย์ จะกล่าวว่า R เป็นริงที่ไม่มีตัวหารศูนย์

ข้อสังเกตุ สำหรับในคอมมิวเททีฟริง ที่มีตัวหารศูนย์ จะได้ว่า ตัวหารศูนย์ทางซ้ายทุกตัวจะเป็นตัวหารศูนย์ทางขวาด้วย

ตัวอย่าง 5.1.1 ในริง I_{12} มี $\bar{2}$, $\bar{3}$, $\bar{4}$, $\bar{6}$, $\bar{8}$, $\bar{9}$ และ $\bar{10}$ เป็นสมาชิกตัวหารศูนย์

ตัวอย่าง 5.1.2 พิจารณาริง $M_2(I)$ ซึ่งมีสมาชิกเป็นเมตริกซ์ ขนาด 2×2 อยู่ในรูป $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ โดยที่ $a, b, c, d \in I$

พิจารณา $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

จะเห็นว่า $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ และ $\begin{pmatrix} 2 & 3 \\ 0 & 0 \end{pmatrix}$ ไม่ใช่เมตริกซ์ศูนย์ แต่ผลคูณเป็นเมตริกซ์ศูนย์

ดังนั้น $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ เป็นตัวหารศูนย์ทางซ้าย และ $\begin{pmatrix} 2 & 3 \\ 0 & 0 \end{pmatrix}$ เป็นตัวหารศูนย์ทางขวา

นิยาม 5.1.3 ให้ D เป็น คอมมิวเททีพริง ที่มียูนิตี้ จะเรียก D ว่าเป็น D อินติกรัลโดเมน ก็ต่อเมื่อ D ไม่มีตัวหารศูนย์

ตัวอย่าง 5.1.3 ริงของจำนวนเต็ม I , ริงของจำนวนตรรกยะ Q และริงของจำนวนจริง $\mathbb{R}$ เป็นอินติกรัลโดเมน แต่ริง $M_2(I)$ ไม่เป็นอินติกรัลโดเมน

นิยาม 5.1.4 ให้ D เป็นอินติกรัลโดเมน , D' เป็นสับเซ็ตของ D และ $D' \neq \emptyset$ จะเรียก D' ว่าเป็นอินติกรัลสับโดเมน (Integral subdomain) ของ D ก็ต่อเมื่อ D' เป็นอินติกรัลโดเมน ภายใต้โอเปอเรชันของ D

ตัวอย่าง 5.1.4 I เป็นอินติกรัลสับโคเมนของ Q และ Q เป็นอินติกรัลสับโคเมนของ $\mathbb{R}$

ตัวอย่าง 5.1.5 ให้ $D' = \{\pm 0, \pm 3, \pm 6, \pm 9, \ldots\}$ จะได้ว่า D' ไม่เป็นอินติกรัลสับโคเมนของ I เพราะว่า D' ไม่เป็นอินติกรัลโคเมน

ตัวอย่าง 5.1.6 ให้ $D' = \{a + b\sqrt{3} \mid a, b \in Q\}$ จะแสดงว่า D' เป็นอินติกรัลสับโคเมนของ $\mathbb{R}$ ภายใต้การบวกและการคูณธรรมดา

1. จะแสดงว่า D' เป็นสับริงของ $\mathbb{R}$

เห็นได้ชัดว่า $D' \subseteq \mathbb{R}$

เนื่องจาก $0 \in Q$ ดังนั้น $0 + 0\sqrt{3} = 0 \in D'$

นั่นคือ $D' \neq \emptyset$

ให้ $a + b\sqrt{3},\ c + d\sqrt{3} \in D'$

เนื่องจาก $(a + b\sqrt{3}) - (c + d\sqrt{3}) = a + b\sqrt{3} - c - d\sqrt{3}$

$= (a - c) + (b - d)\sqrt{3}$

และ $a - c,\ b - d \in Q$

ดังนั้น $(a - c) + (b - d)\sqrt{3} \in D'$

นั่นคือ $(a + b\sqrt{3}) - (c + d\sqrt{3}) \in D'$

และพิจารณา $(a + b\sqrt{3})(c + d\sqrt{3}) = ac + 3bd + bc\sqrt{3} + ad\sqrt{3}$

$= (ac + 3bd) + (bc + ad)\sqrt{3}$

เนื่องจาก $ac + 3bd,\ bc + ad \in Q$

ดังนั้น $(ac + 3bd) + (bc + ad)\sqrt{3} \in D'$

นั่นคือ $(a + b\sqrt{3})(c + d\sqrt{3}) \in D'$

แสดงว่า D' เป็นสับริงของ $\mathbb{R}$

2. จะแสดงว่า D' เป็นคอมมิวเททีฟริง

ให้ $a + b\sqrt{3}, c + d\sqrt{3} \in D'$

พิจารณา $(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (bc + ad)\sqrt{3}$

$= (ca + 3db) + (cb + da)\sqrt{3}$

โดยกฎการสลับที่สำหรับการคูณใน Q

$= (c + d\sqrt{3}) + (a + b\sqrt{3})$

นั่นคือกฎการสลับที่เป็นจริงใน D' สำหรับการคูณ

3. สำหรับทุก ๆ $a + b\sqrt{3} \in D'$ จะมี $1 = 1 + 0\sqrt{3}$ เป็นยูนิต้ใน D'

เนื่องจาก $(a + b\sqrt{3})1 = a + b\sqrt{3}$

และ $1(a + b\sqrt{3}) = a + b\sqrt{3}$

แสดงว่า D' เป็นริงที่มียูนิต้

4. จะแสดงว่า D' ไม่มีตัวหารศูนย์

พิจารณา $a + b\sqrt{3} \neq 0$ และ $c + d\sqrt{3} \neq 0$ ซึ่งเป็นสมาชิกใน D'

จะได้ว่า $(a + b\sqrt{3})(c + d\sqrt{3}) \neq 0$

แสดงว่า D' ไม่มีตัวหารศูนย์

จากคุณสมบัติทั้ง 4 ข้อนี้แสดงว่า D' เป็นอินติกรัลสับโดเมนของ R

จากการศึกษาคุณสมบัติของริงในบทที่ 2 ทราบว่ากฎการตัดออกสำหรับการบวกเป็นจริงในทุก ๆ ริง ต่อไปนี้จะเป็นกฎการตัดออกสำหรับการคูณ

ให้ R เป็นริง และ $a, b, c \in R$ ถ้า $ab = ac$ และ $ba = ca$ ซึ่ง $a \neq 0$ แล้วทำให้ $b = c$ กฎนี้เรียกว่ากฎการตัดออกสำหรับการคูณ (cancellation law of Multiplication)

ต่อไปนี้เป็นคุณสมบัติบางประการของริงที่ไม่มีตัวหารศูนย์

<u>ทฤษฎี 5.1.1</u> ให้ R เป็นริงใด ๆ กฎการตัดออกสำหรับการคูณจะเป็นจริงใน R ก็ต่อเมื่อ R ไม่มีตัวหารศูนย์

<u>พิสูจน์</u> <u>ตอนแรก</u> สมมุติให้กฎการตัดออกสำหรับการคูณเป็นจริงใน R จะพิสูจน์ว่า R ไม่มีตัวหารศูนย์

สมมุติให้ $ab = 0$ สำหรับ $a, b \in R$

ถ้า $a \neq 0$ ดังนั้น $ab = 0 = a0$

เนื่องจากกฎการตัดออกสำหรับการคูณเป็นจริงใน R

ดังนั้น $b = 0$

ในทำนองเดียวกัน ถ้า $b \neq 0$ แล้วสามารถพิสูจน์ได้ว่า $a = 0$

นั่นคือ ถ้ากฎการตัดออกสำหรับการคูณเป็นจริงใน R แล้วจะได้ว่า R ไม่มีตัวหารศูนย์

<u>ตอนสอง</u> สมมุติให้ R เป็นริงที่ไม่มีตัวหารศูนย์

ให้ $ab = ac$ สำหรับ $a, b, c \in R$ และ $a \neq 0$

ดังนั้น $ab - ac = 0$

และ $a(b - c) = 0$

เนื่องจาก $a \neq 0$ และ R ไม่มีตัวหารศูนย์

จะได้ $b - c = 0$

นั่นคือ $b = c$

พิสูจน์ได้ในทำนองเดียวกันว่า ถ้า $ba = ca$ สำหรับ $a, b, c \in R$ และ $a \neq 0$

แล้วจะได้ว่า $b = c$

นั่นคือ ถ้า R ไม่มีตัวหารศูนย์แล้วจะได้ว่ากฎการตัดออกสำหรับการคูณเป็นจริงใน R

<u>ทฤษฎี 5.1.2</u> ให้ D เป็นคอมมิวเททีพริงที่มียูนิตี้ จะได้ว่า D เป็นอินติกรัลโดเมน ก็ต่อเมื่อกฎการตัดออกสำหรับการคูณเป็นจริงใน D

<u>พิสูจน์</u> โดยนิยาม 5.1.3 ได้ว่า D เป็นอินติกรัลโดเมนก็ต่อเมื่อ D ไม่มีตัวหารศูนย์ และโดยทฤษฎี 5.1.1 ได้ว่า D ไม่มีตัวหารศูนย์ก็ต่อเมื่อ กฎการตัดออกสำหรับการคูณเป็นจริงใน D

นั่นคือ D จะเป็นอินติกรัลโดเมน ก็ต่อเมื่อกฎการตัดออกสำหรับการคูณเป็นจริงใน D

<u>ทฤษฎี 5.1.3</u> ให้ R เป็นคอมมิวเททีพริงที่มียูนิตี้ และ U เป็นไอดีลแท้ของ R จะได้ U จะเป็นไอดีลเฉพาะก็ต่อเมื่อ โควเชี่ยนริง $R/_U$ เป็นอินติกรัลโดเมน

<u>พิสูจน์</u> <u>ตอนแรก</u> ให้ U เป็นไอดีลเฉพาะของ R จะพิสูจน์ว่า $R/_U$ เป็นอินติกรัลโดเมน

เนื่องจาก R เป็นคอมมิวเททีพริง ที่มียูนิตี้
ดังนั้น $R/_U$ ก็จะเป็นคอมมิวเททีพริงที่มียูนิตี้
ต่อไปจะแสดงว่า $R/_U$ ไม่มีตัวหารศูนย์
สมมุติ $(a + U)(b + U) = U$ สำหรับ $(a + U), (b + U) \in R/_U$
และ U คือสมาชิกศูนย์ของ $R/_U$

จะได้ $ab + U = U$
นั่นคือ $ab \in U$
เนื่องจาก U เป็นไอดีลเฉพาะของ R จะได้ว่า $a \in U$ หรือ $b \in U$
นั่นคือ $a + U = U$ หรือ $b + U = U$
แสดงว่า $R/_U$ ไม่มีตัวหารศูนย์
ดังนั้น $R/_U$ เป็นอินติกรัลโดเมน

<u>ตอนสอง</u> สมมุติว่า $R/_U$ เป็นอินติกรัลโดเมน จะพิสูจน์ว่า U เป็นไอดีลเฉพาะของ R

ให้ $ab \in U$ สำหรับ $a, b \in R$

ดังนั้น $ab + U = U$

นั่นคือ $(a + U)(b + U) = U$

เนื่องจาก $R/_U$ เป็นอินติกรัลโดเมน ดังนั้น $R/_U$ ไม่มีตัวหารศูนย์

นั่นคือ $a + U = U$ หรือ $b + U = U$

ดังนั้น $a \in U$ หรือ $b \in U$

นั่นคือ U เป็นไอดีลเฉพาะของ R

<u>แบบฝึกหัด 5 ก.</u>

1. จงพิสูจน์ว่าอินเตอร์เซคชัน (intersection) ของอินติกรัลสับโดเมนของอินติกรัลโดเมน D เป็นอินติกรัลสับโดเมนของ D
2. จงพิสูจน์ว่า ริง R ซึ่งมีจำนวนสมาชิกจำกัด มียูนิตี้และไม่มีตัวหารศูนย์เป็นดิวิชันริง
3. จงแสดงว่า ถ้า D เป็นอินติกรัลโดเมนแล้ว $\{ne/ n \in I\}$ เป็นสับโดเมนของ D ซึ่งจะอยู่ในทุก ๆ สับโดเมนของ D
4. ให้ D เป็นอินติกรัลโดเมน $a, b \in D$ สมมุติว่า $a^n = b^n$ และ $a^m = b^m$ ซึ่ง m, n เป็นจำนวนเต็มบวก และ $(m,n) = 1$ จงพิสูจน์ว่า $a = b$
5. ถ้า $R = \{a + b\sqrt{2}/ a, b \in I\}$ แล้วจงแสดงว่า R เป็นอินติกรัลโดเมนภายใต้การบวกและการคูณ

6. ถ้า a เป็นตัวหารศูนย์ของคอมมิวเททีพริง R จงแสดงว่า ar เมื่อ r เป็นสมาชิกใดๆ ใน R จะเป็นตัวหารศูนย์ใน R เช่นกัน
7. จงพิสูจน์ว่า ถ้า a มีอินเวอร์สสำหรับการคูณคือ a^{-1} อยู่ในริง R แล้ว a จะไม่เป็นตัวหารศูนย์ใน R
8. จงแสดงให้เห็นว่า เมตริกซ์ต่อไปนี้เป็นตัวหารศูนย์ในริง $M_2(I)$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$$

9. จงพิสูจน์ว่าเซ็ตของจำนวนเต็มมอดูโล p (I_p) เมื่อ p เป็นจำนวนเฉพาะเป็นอินติกรัลโดเมน

5.2. คาแรคเตอริสติก (Characteristics)

สำหรับหัวข้อนี้ จะศึกษาคุณสมบัติของริง และอินติกรัลโดเมน โดยพิจารณาจากกรุ๊ปภายใต้การบวก สำหรับสัญลักษณ์ที่ใช้ในหัวข้อมีดังนี้

สำหรับ a ที่เป็นสมาชิกใดๆ ในริง R และ n เป็นจำนวนเต็มบวก

na หมายถึง $a + a + \cdots + a$ (n ครั้ง)

และ $(-n)a$ หมายถึง $(-a) + (-a) + \cdots + (-a)$ (n ครั้ง)

พิจารณา $I_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

เนื่องจาก $\bar{1} + \bar{1} + \bar{1} + \bar{1} = 4\bar{1} = \bar{0}$

$\bar{2} + \bar{2} + \bar{2} + \bar{2} = 4\bar{2} = \bar{0}$

$\bar{3} + \bar{3} + \bar{3} + \bar{3} = 4\bar{3} = \bar{0}$

ทำนองเดียวกันจะได้

$$4\bar{1} = (-4)\bar{1} = 8\bar{1} = 16\bar{1} = (-16)\bar{1} = \cdots = \bar{0}$$
$$2\bar{2} = 4\bar{2} = (-4)\bar{2} = 6\bar{2} = (-6)\bar{2} = \cdots = \bar{0}$$
$$4\bar{3} = (-4)\bar{3} = \bar{0}$$

จะเห็นได้ว่า 4 เป็นจำนวนเต็มบวกที่น้อยที่สุดที่ทำให้ $4\bar{a} = \bar{0}$ สำหรับทุกๆสมาชิก $\bar{a} \neq \bar{0}$ ใน I_4 กรณีเช่นนี้จะกล่าวว่าริง I_4 มีคาแรคเตอริสติกเป็น 4
ต่อไปจะให้นิยามของคาแรคเตอริสติก

<u>นิยาม 5.2.1</u> ให้ R เป็นริงใดๆ ถ้ามีจำนวนเต็มบวก n ที่น้อยที่สุดซึ่งทำให้ $na = 0$ สำหรับทุกๆ สมาชิก $a \in R$ แล้วจะกล่าวว่าริง R มีคาแรคเตอริสติกเป็น n ถ้าไม่มีจำนวนเต็มบวก n ดังกล่าว จะเรียกว่า R มีคาแรคเตอริสติกเป็นศูนย์

<u>ตัวอย่าง 5.2.1</u> ริง I_n มีคาแรคเตอริสติกเป็น n

<u>ตัวอย่าง 5.2.2</u> ริง I , Q , R และ C มีคาแรคเตอริสติกเป็น 0

<u>หมายเหตุ</u> ต่อไปจะเขียน char R แทนคาแรคเตอริสติกของ R

<u>ทฤษฎี 5.2.1</u> ให้ R เป็นริงที่มียูนิตี้ e จะได้ว่า R จะมีคาแรคเตอริสติก $n > 0$ ก็ต่อเมื่อ n เป็นจำนวนเต็มบวกที่น้อยที่สุด ซึ่งทำให้ $ne = 0$

<u>พิสูจน์</u> <u>ตอนแรก</u> สมมุติว่า char R = $n > 0$
นั่นคือ $na = 0$ สำหรับทุกๆ สมาชิก $a \in R$
เนื่องจาก R เป็นริงที่มียูนิตี้ e
ดังนั้น $ne = 0$

<u>ตอนสอง</u> สมมุติว่า n เป็นจำนวนเต็มบวกที่น้อยที่สุด ซึ่ง $ne = 0$ สำหรับสมาชิก a ใดๆ ของ R จะได้

$$na = a + a + \cdots + a \quad (n \text{ ครั้ง})$$
$$= ae + ae + \cdots + ae \quad (n \text{ ครั้ง})$$

$$na = a(e + e + \cdots + e) \quad (n \text{ ครั้ง})$$
$$= a(ne)$$
$$= a0$$
$$= 0$$

นั่นคือ char R = n

<u>ทฤษฎี 5.2.2</u> คาแรคเตอริสติกของอินติกรัลโดเมน จะเป็น 0 หรือจำนวนเฉพาะ

<u>พิสูจน์</u> ให้ D เป็นอินติกรัลโดเมน ซึ่งมีคาแรคเตอริสติกเป็นจำนวนบวก n จะพิสูจน์ว่า n เป็นจำนวนเฉพาะ

สมมุติว่า n ไม่เป็นจำนวนเฉพาะ

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

โดยทฤษฎี 5.2.1 ได้ว่า n เป็นจำนวนเต็มบวกที่น้อยที่สุดที่ทำให้

$$0 = ne$$
$$= (n_1n_2)e$$
$$= (n_1n_2)ee \qquad \text{เพราะว่า } ee = e$$
$$= (n_1e)(n_2e)$$

เนื่องจาก D ไม่มีตัวหารศูนย์

ดังนั้น $n_1e = 0$ หรือ $n_2e = 0$

พิจารณา กรณี $n_1e = 0$

เนื่องจาก $n_1 < n$ ทำให้ขัดแย้งกับที่ว่า n เป็นจำนวนเต็มบวกที่น้อยที่สุด ที่ทำให้ $ne = 0$

ในทำนองเดียวกัน กรณีที่ $n_2e = 0$ ทำให้เกิดข้อขัดแย้งเช่นกัน

นั่นคือ n เป็นจำนวนเฉพาะ

ตัวอย่าง 5.2.4 อินติกรัลโดเมน I, Q และ $\mathbb{R}$ มีคาแรคเตอริสติกเป็น 0 และอินติกรัลโดเมนของจำนวนเต็มมอดูโล p เมื่อ p เป็นจำนวนเฉพาะ มีคาแรคเตอริสติกเป็น p

ทฤษฎี 5.2.3 ถ้า D เป็นอินติกรัลโดเมน ซึ่งมีคาแรกเตอริสติก 0 แล้ว D จะมีสับริงซึ่งไอโซมอร์ฟิก (isomorphic) กับอินติกรัลโดเมน I

พิสูจน์ ให้ D เป็นอินติกรัลโดเมนที่มียูนิตี้ e

และให้ $Ie = \{xe / x \in I\}$

จะแสดงว่า Ie เป็นสับริงของ D

เนื่องจาก $0 \in I$ ดังนั้น $0e = 0 \in Ie$

นั่นคือ $Ie \neq \emptyset$

จากการกำหนดเซ็ต Ie จะได้ว่า $Ie \subseteq D$

ให้ $x_1e, x_2e \in Ie$ สำหรับ $x_1x_2 \in I$

พิจารณา $x_1e - x_2e = (x_1 - x_2)e$

เนื่องจาก $x_1 - x_2 \in I$

ดังนั้น $(x_1 - x_2)e \in Ie$

พิจารณา $(x_1e)(x_2e) = (x_1x_2)(ee)$

$= (x_1x_2)e$

เนื่องจาก $x_1x_2 \in I$

ดังนั้น $(x_1x_2)e \in Ie$ นั่นคือ $(x_1e)(x_2e) \in Ie$

แสดงว่า Ie เป็นสับริงของ D

กำหนดฟังก์ชัน $\theta : I \longrightarrow Ie$

โดย $\theta(x) = xe$ สำหรับทุก ๆ $x \in I$

จะแสดงว่า θ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

สมมุติให้ $\theta(x_1) = \theta(x_2)$ สำหรับ $x_1, x_2 \in I$ และ $x_1 \geq x_2$

จะได้ $x_1e = x_2e$

ดังนั้น $(x_1 - x_2)e = 0$ และ $x_1 - x_2 \geq 0$

เนื่องจาก D มีคาแรคเตอริสติก 0 ดังนั้น $x_1 - x_2 > 0$ เป็นไปไม่ได้

นั่นคือ $x_1 - x_2 = 0$

ดังนั้น $x_1 = x_2$

แสดงว่า θ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

จากนิยาม θ เห็นได้ชัดว่า θ เป็นฟังก์ชันออนทูจาก I ไปยัง Ie

ต่อไปจะแสดงว่า θ เป็นโฮโมมอร์ฟิซึม

ให้ $x_1, x_2 \in I$

พิจารณา
$$\begin{aligned}\theta(x_1 + x_2) &= (x_1 + x_2)e \\ &= x_1e + x_2e \\ &= \theta(x_1) + \theta(x_2)\end{aligned}$$

และ
$$\begin{aligned}\theta(x_1x_2) &= (x_1x_2)e \\ &= (x_1x_2)ee \\ &= (x_1e)(x_2e) \\ &= \theta(x_1)\theta(x_2)\end{aligned}$$

แสดงว่า θ เป็นโฮโมมอร์ฟิซึมจาก I ไปยัง Ie

ดังนั้น θ เป็นไอโซมอร์ฟิซึมจาก I ไปยัง Ie

นั่นคือ $I \cong Ie$

<u>ทฤษฎี 5.2.4</u> ถ้า D เป็นอินติกรัลโดเมน ซึ่งมีคาแรคเตอริสติกเป็นจำนวนเฉพาะ p แล้ว D จะมีสับริง ซึ่งไอโซมอร์ฟิกกับอินติกรัลโดเมน ของจำนวนเต็มมอดูโล p (I_p)

<u>พิสูจน์</u> สมมุติให้ D เป็นอินติกรัลโดเมน ที่มียูนิตี้ e และ char D = p

กำหนด $Ie = \{xe / x \in I\}$

เช่นเดียวกับทฤษฎี 5.2.3 ได้ว่า Ie เป็นสับริงของ D

กำหนดฟังก์ชัน $\phi : I_p \longrightarrow Ie$

โดย $\phi(\bar{x}) = xe$ สำหรับ $x \in I$

จะแสดงว่า ϕ เป็นฟังก์ชันที่กำหนดขึ้นถูกต้องแล้ว

ให้ $\bar{x}_1 = \bar{x}_2$ สำหรับ $x_1, x_2 \in I$ และเลือกให้ $x_1 \geq x_2$

ดังนั้น $x_1 \equiv x_2 \pmod{p}$

นั่นคือ $p / x_1 - x_2$

จะได้ $x_1 - x_2 = ap$ สำหรับบางสมาชิก $a \in I$

ดังนั้น $(x_1 - x_2)e = (ap)e$

$= a(pe)$

$= a0$ (โดยทฤษฎี 5.2.1)

นั่นคือ $x_1e - x_2e = 0$

จะได้ $x_1e = x_2e$

นั่นคือ $\phi(\bar{x}_1) = \phi(\bar{x}_2)$

แสดงว่า กำหนดฟังก์ชันถูกต้องแล้ว และจากการกำหนดฟังก์ชัน ϕ จะเห็นได้ชัดว่า ϕ เป็นฟังก์ชันออนทูจาก I_p ไปยัง Ie

ต่อไปจะแสดงว่า ϕ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

สมมุติให้ $x_1, x_2 \in I$ และ $x_1 \geq x_2$ ซึ่ง $\phi(\bar{x}_1) = \phi(\bar{x}_2)$

นั่นคือ $x_1 e = x_2 e$

ดังนั้น $(x_1 - x_2)e = 0$

เนื่องจาก $x_1 - x_2 \geq 0$ และ $p > 0$

โดย ดิวิชันอัลกอริทึม จะได้ว่ามีจำนวนเต็ม q และ r ซึ่งทำให้

$$x_1 - x_2 = pq + r \qquad 0 \leq r \leq p$$

ดังนั้น
$$\begin{aligned}(x_1 - x_2)e &= (qp + r)e \\ &= (qp)e + re \\ &= q(pe) + re \\ &= 0 + re \qquad \text{(โดยทฤษฎี 5.2.1)} \\ &= re\end{aligned}$$

จะได้ว่า $re = 0$ (เพราะว่า $x_1 e = x_2 e$)

ถ้า $r < p$ และจากทฤษฎี 5.2.1 จะได้ว่า r เป็นคาแรกเตอริสติกของ D ซึ่งขัดแย้งกับสมมุติฐานที่ว่า char D = p

ดังนั้น $r = 0$

จะได้ $x_1 - x_2 = qp$

แสดงว่า $p / x_1 - x_2$

นั่นคือ $x_1 \equiv x_2 \pmod{p}$

จะได้ $\bar{x}_1 = \bar{x}_2$

แสดงว่า ϕ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

ต่อไปจะแสดงว่า ϕ เป็นโฮโมมอร์ฟิซึม

ให้ $\bar{x}_1 , \bar{x}_2 \in I_p$

พิจารณา $\phi(\bar{x}_1 + \bar{x}_2) = \phi(\overline{x_1 + x_2})$

$= (x_1 + x_2)e$

$= x_1e + x_2e$

$= \phi(\bar{x}_1) + \phi(\bar{x}_2)$

และ $\phi(\bar{x}_1\bar{x}_2) = \phi(\overline{x_1x_2})$

$= (x_1x_2)e$

$= (x_1x_2)ee$

$= (x_1e)(x_2e)$

$= \phi(\bar{x}_1)\,\phi(\bar{x}_2)$

นั่นคือ ϕ เป็นโฮโมมอร์ฟิซึมจาก I_p ไปยัง Ie

แสดงว่า ϕ เป็นไอโซมอร์ฟิซึมจาก I_p ไปยัง Ie

ดังนั้น $I_p \cong Ie$

แบบฝึกหัดที่ 5 ข.

1. จงหาคาแรคเตอริสติกของริงต่อไปนี้

   ก. $2I$ ข. $I + I$ ค. $I_3 + I_3$

2. จงแสดงว่าคาแรคเตอริสติกของสับโดเมนของอินติกรัลโดเมน D เท่ากับคาแรคเตอริสติกของ D

3. ถ้า R เป็นริงที่มีคาแรคเตอริสติก 2 สำหรับ $a, b, c \in R$ จงแสดงว่า

ก. $(a + b)^2 = a^2 + b^2$

ข. $(a + b + c)^2 = a^2 + b^2 + c^2$

4. ถ้า R เป็นริงที่มีคาแรคเตอริสติก 5 สำหรับ $a, b \in R$ จงแสดงว่า

ก. $(a + b)^5 = a^5 + b^5$

ข. $(a + b)^{25} = a^{25} + b^{25}$

5. ถ้า D เป็นอินติกรัลโดเมน ซึ่งมีคาแรคเตอริสติก 0 แล้ว D จะมีสับโดเมนไอโซมอร์ฟิกกับอินติกรัลโดเมนของจำนวนเต็ม

6. ถ้า D เป็นอินติกรัลโดเมน ซึ่งมีคาแรคเตอริสติก เป็นจำนวนเฉพาะ p แล้ว D จะมีสับโดเมน ไอโซมอร์ฟิกกับอินติกรัลโดเมนของจำนวนเต็มมอดูโล p

---

5.3 <u>ออเดอร์อินติกรัลโดเมน</u> (Ordered Integral Domain)

ในหัวข้อนี้จะศึกษาถึงอินติกรัลโดเมนที่เรียกว่าออเดอร์อินติกรัลโดเมน โดยจะกล่าวถึงนิยามและคุณสมบัติของออเดอร์อินติกรัลโดเมน

<u>นิยาม 5.3.1</u> ให้ D เป็นอินติกรัลโดเมน จะเรียกว่า D เป็นออเดอร์อินติกรัลโดเมน ก็ต่อเมื่อ D มีสับเซ็ต D_p ซึ่งไม่เป็นเซ็ตว่าง และสอดคล้องตามคุณสมบัติต่อไปนี้

1. ถ้า $a, b \in D_p$ แล้วจะได้ $a + b \in D_p$
2. ถ้า $a, b \in D_p$ แล้วจะได้ $ab \in D_p$
3. สำหรับแต่ละสมาชิก $a \in D$ จะได้ว่า $a = 0$ หรือ $a \in D_p$ หรือ $-a \in D_p$ สำหรับสมาชิกใน D_p เรียกว่าสมาชิกบวก (positive element) ของ D และอินเวอร์สสำหรับการบวกของสมาชิกใน D_p เรียกว่าสมาชิกลบ (negative element)

ตัวอย่าง 5.3.1 พิจารณาอินติกรัลโดเมน I จะได้ว่า I เป็นออเดอร์อินติกรัลโดเมน โดยมีเซ็ตของจำนวนเต็มบวกเป็นสับเซ็ต D_p ซึ่งสอดคล้องคุณสมบัติในนิยาม 5.3.1

นิยาม 5.3.2 ให้ D เป็นออเดอร์อินติกรัลโดเมน ซึ่งมี D_p เป็นเซ็ตของสมาชิกบวกของ D

1. จะกล่าวว่า $a < b$ หรือ $b > a$ (อ่านว่า a น้อยกว่า b หรือ b มากกว่า a) ก็ต่อเมื่อ $b + (-a) = b - a \in D_p$

2. $a > 0$ หมายความว่า $a \in D_p$ และ $a < 0$ หมายความว่า $0 - a \in D_p$ หรือ $-a \in D_p$

ดังนั้นจากนิยาม 5.3.1 เขียนใหม่ได้ว่า

อินติกรัลโดเมน D จะเป็นออเดอร์อินติกรัลโดเมนก็ต่อเมื่อ D มีสับเซ็ต D_p ซึ่งไม่เป็นเซ็ตว่าง และสอดคล้องตามคุณสมบัติต่อไปนี้

1. ถ้า $a > 0$ และ $b > 0$ แล้วจะได้ว่า $a + b > 0$
2. ถ้า $a > 0$ และ $b > 0$ แล้วจะได้ว่า $ab > 0$
3. ถ้า $a \in D$ แล้วจะมีเพียง 1 กรณีต่อไปนี้เท่านั้นที่เป็นจริง คือ $a = 0$, $a > 0$ หรือ $a < 0$

ต่อไปจะกล่าวถึงคุณสมบัติของออเดอร์ อินติกรัลโดเมน

ทฤษฎี 5.3.1 ให้ a, b และ c เป็นสมาชิกของออเดอร์ อินติกรัลโดเมน D ถ้า $a > b$ และ $c > 0$ แล้วจะได้ว่า $ac > bc$

พิสูจน์ พิจารณา
$$\begin{aligned} ac - bc &= ac + [-(bc)] \\ &= ac + [(-b)c] \\ &= [a + (-b)]\, c \end{aligned}$$

เนื่องจาก $a > b$

ดังนั้น $a - b > 0$ และ $c > 0$

จะได้ $(a - b)c > 0$

หรือ $[a + (-b)]c > 0$

นั่นคือ $ac - bc > 0$

ดังนั้น $ac > bc$

<u>ทฤษฎี 5.3.2</u> ให้ a เป็นสมาชิกของ ออเดอร์ อินติกรัลโดเมน D
ถ้า $a \neq 0$ แล้วจะได้ว่า $a^2 > 0$ นั่นคือ $a^2 \in D_p$

<u>หมายเหตุ</u> a^2 หมายถึง aa

<u>พิสูจน์</u> เนื่องจาก $a \in D$ และ $a \neq 0$

ดังนั้น $a > 0$ หรือ $a < 0$ อย่างใดอย่างหนึ่ง

ถ้า $a > 0$ จะได้ว่า $a \in D_p$

ดังนั้น $aa = a^2 \in D_p$

นั่นคือ $a^2 > 0$

ถ้า $a < 0$ หรือ $-a > 0$

นั่นคือ $-a \in D_p$ จะได้ว่า $(-a)(-a) = (-a)^2 \in D_p$

หรือ $(-a)^2 > 0$

เนื่องจาก $(-a)^2 = (-a)(-a)$

$= -[a(-a)]$

$= -(-a^2)$

$= a^2$

ดังนั้น $a^2 > 0$ นั่นคือ $a^2 \in D_p$

ข้อสังเกตุ จากทฤษฎี 5.3.2 นี้จะได้ว่ายูนิตี้ของออเดอร์ อินติกรัลโดเมนจะเป็นสมาชิกบวก เพราะว่า $e^2 = e > 0$ นั่นคือ $e \in D_p$

นิยาม 5.3.3 ริง R จะเป็นออเดอร์ริง (Oedered Ring) ถ้า R มีสับเซ็ต P ซึ่งไม่เป็นเซ็ตว่าง และสอดคล้องคุณสมบัติต่อไปนี้

1. ถ้า $a \in P$ และ $b \in P$ แล้วจะได้ $a + b \in P$ และ $ab \in P$

2. สำหรับแต่ละสมาชิก $a \in R$ จะได้ว่า $a \in P$, $a = 0$, $-a \in P$ อย่างใดอย่างหนึ่งเท่านั้น ซึ่งคุณสมบัติข้อนี้เรียกว่ากฎไตรวิภาค (Trichotomy law)

ทฤษฎี 5.3.3 ออเดอร์ คอมมิวเททีพริง R ที่มียูนิตี้ จะเป็นอินติกรัลโดเมนที่มีคาแรคเตอริสติก 0

พิสูจน์ สมมุติให้ $a, b \in R$ โดยที่ $a \neq 0$, $b \neq 0$ และ $ab = 0$

ดังนั้น $(\pm a)(\pm b) = ab = 0$

จากข้อ 2 ของนิยาม 5.3.3 มีสับเซ็ต P ของ R ที่

$+a$ หรือ $-a$ และ $+b$ หรือ $-b$ เป็นสมาชิกของ P

ดังนั้น $(\pm a)(\pm b) = 0 \in P$ (โดยข้อ 1 นิยาม 5.3.3)

ซึ่งจะขัดแย้งกับที่ว่า $0 \notin P$ (โดยข้อ 2 นิยาม 5.3.3)

ดังนั้นที่สมมุติว่า $a \neq 0$, $b \neq 0$ แล้ว $ab = 0$ เป็นไปไม่ได้

นั่นคือ R ไม่มีตัวหารศูนย์

แสดงว่า R เป็น (ออเดอร์) อินติกรัลโดเมน

ต่อไปจะพิสูจน์ว่า คาแรคเตอริสติกของ R คือ 0

เนื่องจาก $e \in P$ (โดยทฤษฎี 5.3.2)

ดังนั้น $e + e + \ldots + e + \ldots \in P$ (โดยข้อ 1 นิยาม 5.3.3)
จะเห็นได้ชัดว่าผลบวกนี้จะไม่มีโอกาสเป็น 0
ดังนั้นคาแรคเตอริสติกของ R คือ 0

แบบฝึกหัด 5 ค.

1. ให้ D เป็นออเดอร์ อินติกรัลโดเมน และให้ $a, b, c \in D$ จงพิสูจน์ว่า
   ก. ถ้า $a > b$ แล้ว $a + c > b + c$ สำหรับทุก $c \in D$
   ข. ถ้า $a > b$ และ $c < 0$ แล้วจะทำให้ $ac < bc$
   ค. ถ้า $a > b$ และ $b > c$ แล้วจะทำให้ $a > c$

2. ให้ u, v, x, y เป็นสมาชิกของออเดอร์ อินติกรัลโดเมน D จงพิสูจน์ว่า
   ก. ถ้า $u > x$ แล้ว $-u < -x$
   ข. ถ้า $u > v$ และ $x > y$ แล้ว $u + x > v + y$
   ค. ถ้า $uv > ux$ และ $u > 0$ แล้ว $v > x$

3. ให้ a เป็นสมาชิกของออเดอร์อินติกรัลโดเมน นิยาม a ซึ่งจะเรียกว่า ค่าสัมบูรณ์ของ a (absolute value of a) ดังต่อไปนี้

$$|a| = \begin{cases} a & \text{ถ้า } a \geq 0 \\ -a & \text{ถ้า } a < 0 \end{cases}$$

ในที่นี้ $a \geq 0$ หมายความว่า $a > 0$ หรือ $a = 0$ จงพิสูจน์ว่า
สำหรับทุก $a, b \in D$ แล้ว
   ก. $|ab| = |a||b|$
   ข. $-|a| \leq a \leq |a|$
   ค. $|a + b| \leq |a| + |b|$

5.4 ฟิลด์ (Field)

นิยาม 5.4.1 F จะเป็นฟิลด์ก็ต่อเมื่อ F เป็นคอมมิวเททีพริงที่มียูนิตี้ ซึ่งสมาชิกทุกตัวที่ไม่ใช่สมาชิกศูนย์ของ F จะต้องมีอินเวอร์สสำหรับการคูณอยู่ใน F

ตัวอย่าง 5.4.1 $\mathbb{C}$, $\mathbb{R}$ และ $\mathbb{Q}$ เป็นฟิลด์

ตัวอย่าง 5.4.2 พิจารณา $I_7 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6} \}$ ซึ่งเป็นริงของจำนวนเต็มมอดูโล 7 ภายใต้การบวกและการคูณมอดูโล 7

จากตัวอย่าง 2.4.8 ได้ว่า I_7 เป็นคอมมิวเททีพริง และมี $\bar{1}$ เป็นยูนิตี้

เนื่องจาก $\bar{1}\,\bar{1} = \bar{1} = \bar{6}\,\bar{6}$

$\bar{2}\,\bar{4} = \bar{1} = \bar{4}\,\bar{2}$

$\bar{3}\,\bar{5} = \bar{1} = \bar{5}\,\bar{3}$

นั่นคือ สมาชิกที่ไม่ใช่สมาชิกศูนย์ของ I_7 ทุกตัวมีอินเวอร์สสำหรับการคูณ

ดังนั้น I_7 เป็นฟิลด์

หมายเหตุ I_7 ในตัวอย่าง 5.4.2 เป็นฟิลด์ที่มีสมาชิกจำนวนจำกัด (finite field)

ตัวอย่าง 5.4.3 พิจารณา I_6 ซึ่งเป็นริงของจำนวนเต็มมอดูโล 6 ภายใต้การบวกและการคูณมอดูโล 6 จะได้ว่ามีสมาชิกที่ไม่ใช่ศูนย์ของ I_6 ที่ไม่มีอินเวอร์สสำหรับการคูณ ดังนั้น I_6 ไม่เป็นฟิลด์

ทฤษฎี 5.4.1 ให้ R เป็นคอมมิวเททีพริงที่มียูนิตี้ จะได้ว่า R เป็นฟิลด์ก็ต่อเมื่อ R ไม่มีไอดีลแท้

พิสูจน์ ตอนแรก สมมุติว่า R ไม่มีไอดีลแท้ แล้วจะพิสูจน์ว่า R เป็นฟิลด์ นั่นคือ ต้องแสดงว่าสำหรับทุกสมาชิก $0 \neq a \in R$ มีอินเวอร์สสำหรับการคูณ ให้ $a \in R$ ซึ่ง $a \neq 0$

พิจารณา $Ra = \{xa / x \in R\}$

จะแสดงว่า Ra เป็นไอดีลของ R

จากนิยามของ Ra จะได้ว่า $Ra \subseteq R$

เนื่องจาก $e \in R$ ดังนั้น $ea = a \in Ra$ นั่นคือ $Ra \neq \emptyset$

ให้ $r_1a, r_2a \in Ra$ เมื่อ $r_1, r_2 \in R$

เนื่องจาก $r_1 - r_2 \in R$

และ $r_1a - r_2a = (r_1 - r_2)a$

จะได้ว่า $r_1a - r_2a \in Ra$

และ $(r_1a)(r_2a) = r_1(a(r_2a))$

$= r_1(r_2(aa))$

$= (r_1r_2a)a$

เนื่องจาก $r_1r_2a \in R$ ดังนั้น $(r_1a)(r_2a) \in Ra$

นั่นคือ Ra เป็นสับริงของ R

ให้ $ra \in Ra$ และ $x \in R$

พิจารณา $x(ra) = (xr)a$

และ $(ra)x = r(ax)$

$= r(xa)$

$= (rx)a$

เนื่องจาก $xr, rx \in R$

ดังนั้น $(xr)a, (rx)a \in Ra$

นั่นคือ $x(ra), (ra)x \in Ra$

แสดงว่า Ra เป็นไอดีลของ R

เนื่องจาก R ไม่มีไอดีลแท้ ดังนั้น $Ra = \{0\}$ หรือ $Ra = R$
เนื่องจาก $ea = a \neq 0 \in Ra$

ดังนั้น $Ra \neq \{0\}$
นั่นคือ $Ra = R$

แสดงว่าสมาชิกทุกตัวของ R สามารถเขียนเป็นผลคูณของสมาชิกใน R กับ $a \neq 0$ ได้เสมอ

เนื่องจาก $e \in R$ ดังนั้นจะมีสมาชิก $b \in R$ ซึ่ง $ba = e = ab$
นั่นคือ $b = a^{-1}$

แสดงว่าสมาชิกของ R ที่ไม่ใช่สมาชิกศูนย์จะมีอินเวอร์สสำหรับการคูณ
นั่นคือ R เป็นฟิลด์

<u>ตอนสอง</u> สมมุติว่า R เป็นฟิลด์ จะพิสูจน์ว่า R ไม่มีไอดีลแท้
เนื่องจาก R เป็นฟิลด์
ดังนั้นสมาชิกทุกตัวที่ไม่ใช่สมาชิกศูนย์ของ R จะมีอินเวอร์สสำหรับการคูณอยู่ใน R
ให้ U เป็นไอดีลใด ๆ ของ R และ $a \in U$ โดยที่ $a \neq 0$
ดังนั้น $aa^{-1} = e \in U$ เมื่อ $a^{-1} \in R$
ดังนั้น $U = R$ (โดยทฤษฎี 4.1.1)
นั่นคือ ถ้า R เป็นฟิลด์แล้ว R จะไม่มีไอดีลแท้

<u>ทฤษฎี 5.4.2</u> ให้ R เป็นคอมมิวเททีพริง ซึ่งมียูนิตี้ และ M เป็นไอดีลของ R จะได้ว่า M เป็นแม็กซิมัลไอดีลของ R ก็ต่อเมื่อ $R/_M$ เป็นฟิลด์

พิสูจน์ <u>ตอนแรก</u> สมมุติ M เป็นแม็กซิมัลไอดีลของ R จะต้องพิสูจน์ว่า $R/_M$ เป็นฟิลด์
นั่นคือ จะต้องแสดงว่า $R/_M$ เป็นคอมมิวเททีพริงที่มียูนิตี้ และสมาชิกทุกตัวของ $R/_M$ ที่ไม่ใช่สมาชิกศูนย์จะมีอินเวอร์สสำหรับการคูณ

เนื่องจาก R เป็นคอมมิวเททีพริงที่มียูนิตี้ e
ดังนั้น $R/_M$ เป็นคอมมิวเททีพริง และมี $e + M$ เป็นยูนิตี้
เพราะว่า M เป็นแม็กซิมัลไอดีลของ R ดังนั้น $M \neq R$
ให้ $a + M \in R/_M$ โดยที่ $a \in R$ และ $a \notin M$
นั่นคือ $a + M \neq M$
แสดงว่า $a + M$ ไม่ใช่สมาชิกศูนย์ใน $R/_M$
จะพิสูจน์ว่า $a + M$ มีอินเวอร์สสำหรับการคูณอยู่ใน $R/_M$
ให้ $N = \{ra + m / r \in R, m \in M\}$
โดยเลมม่า 4.3.1 จะได้ว่า N เป็นไอดีลของ R และ $N = R$
ดังนั้น $e \in N$
จากการกำหนดเซ็ต N จะต้องมี $b \in R, m \in M$ ซึ่ง

$$\begin{aligned} e &= ba + m \\ e + M &= (ba + m) + M \\ &= ba + (m + M) \\ &= ba + M \\ &= (b + M)(a + M) \end{aligned}$$

เนื่องจาก $R/_M$ เป็นคอมมิวเททีพริง
ดังนั้น $(a + M)(b + M) = (b + M)(a + M) = e + M$
นั่นคือ $b + M$ เป็นอินเวอร์สสำหรับการคูณของ $a + M$
แสดงว่า $R/_M$ เป็นฟิลด์

<u>ตอนสอง</u> สมมุติ $R/_M$ เป็นฟิลด์ จะต้องแสดงว่า M เป็นแม็กซิมัลไอดีลของ R
ให้ N เป็นไอดีลใด ๆ ของ R ซึ่ง $M \subsetneq N \subseteq R$

และให้ θ เป็นฟังก์ชันธรรมชาติ
นั่นคือ $\theta : R \longrightarrow R/_M$

โดย $\theta(r) = r + M$ สำหรับทุก ๆ สมาชิก $r \in R$

ซึ่ง θ เป็นฟังก์ชันออนทูและโฮโมมอร์ฟิซึม จะได้ว่า
$\theta(N)$ เป็นไอดีลของ $R/_M$ (ไดอกรุ่ 4.1.3)

และมี $\theta(M) \subseteq \theta(N) \subseteq \theta(R)$

นั่นคือ $\{(0 + M)\} \subseteq \theta(N) \subseteq R/_M$

ซึ่งจะขัดแย้งกับทฤษฎี 5.4.1 ซึ่งกล่าวว่า ฟิลด์จะไม่มีไอดีลแท้
ดังนั้น ถ้า $R/_M$ เป็นฟิลด์ แล้วจะได้ว่า M เป็นแม็กซิมัลไอดีลของ R

<u>บทแทรก 5.4.3</u> ริง $I/_{(n)}$ จะเป็นฟิลด์ ก็ต่อเมื่อ n เป็นจำนวนเฉพาะ
<u>พิสูจน์</u> แบบฝึกหัด

<u>ทฤษฎี 5.4.4</u> ทุก ๆ ฟิลด์ F จะเป็นอินติกรัลโดเมน
<u>พิสูจน์</u> จากนิยามของฟิลด์ ได้ว่า F เป็นคอมมิวเททีพริงที่มียูนิตี้ ดังนั้นจะต้องแสดงว่า F ไม่มีตัวหารศูนย์
ให้ $a, b \in F$ โดยที่ $a \neq 0$ และ $ab = 0$
เนื่องจาก $a \in F$ และ $a \neq 0$ ดังนั้นจะมี $a^{-1} \in F$

จาก $ab = 0$

$a^{-1}(ab) = a^{-1}(0)$

$(a^{-1}a)b = 0$

$eb = 0$

$b = 0$

นั่นคือ ถ้า $ab = 0$ โดย $a \neq 0$ แล้วจะได้ว่า $b = 0$
ดังนั้น F ไม่มีตัวหารศูนย์ แสดงว่า F เป็นอินติกรัลโดเมน

<u>ทฤษฎี 5.4.5</u> ทุก ๆ อินติกรัลโดเมน ที่มีสมาชิกจำนวนจำกัดเป็นฟิลด์

<u>พิสูจน์</u> ให้ D เป็นอินติกรัลโดเมน ซึ่งมีสมาชิกแตกต่างกันทั้งหมดคือ

$$D = \{a_1, a_2, \ldots, a_n\}$$

ให้ $0 \neq a \in D$ จะแสดงว่า a มีอินเวอร์สสำหรับการคูณ

พิจารณา $P = \{a_1a, a_2a, \ldots, a_na\} \subseteq D$

ต่อไปจะแสดงว่าสมาชิกใน P แตกต่างกันทั้งหมด

สมมุติว่าใน P มีสมาชิกบางคู่เท่ากัน นั่นคือ

$$a_ia = a_ja \quad \text{สำหรับ } i \neq j$$

$$a_ia - a_ja = 0$$

$$(a_i - a_j)a = 0$$

เนื่องจาก D ไม่มีตัวหารศูนย์ และ $a \neq 0$

ดังนั้น $a_i - a_j = 0$

นั่นคือ $a_i = a_j$ โดยที่ $i \neq j$

ซึ่งจะขัดแย้งกับที่ว่าสมาชิกใน D ต้องแตกต่างกันทั้งหมด

ดังนั้น $a_1a, a_2a, \ldots, a_na$ แตกต่างกันทั้งหมด

จะได้ว่า $P = D$

เนื่องจาก D เป็นคอมมิวเททีพริงที่มียูนิตี้

ฉะนั้นจะมี $e = a_ia = aa_i$ สำหรับบาง $a_i \in D$

นั่นคือ a_i เป็นอินเวอร์สสำหรับการคูณของ a

ดังนั้น D เป็นฟิลด์

<u>บทแทรก 5.4.6</u> ถ้า p เป็นจำนวนเฉพาะแล้วริง I_p เป็นฟิลด์

<u>พิสูจน์</u> เนื่องจาก I_p เป็นคอมมิวเททีพริงที่มียูนิตี้

จะแสดงว่า I_p เป็นอินติกรัลโดเมน นั่นคือต้องพิสูจน์ว่า I_p ไม่มีตัวหารศูนย์

ให้ $\bar{a}, \bar{b} \in I$ ซึ่ง $\bar{a}\bar{b} = \bar{0}$

ดังนั้น $\overline{ab} = \bar{0}$

แสดงว่า p หาร ab ลงตัว

แต่ p เป็นจำนวนเฉพาะ

ดังนั้น p จะต้องหาร a หรือ b อย่างใดอย่างหนึ่ง

นั่นคือ $a \equiv 0 \pmod{p}$ หรือ $b \equiv 0 \pmod{p}$

เพราะฉะนั้น $\bar{a} = \bar{0}$ หรือ $\bar{b} = \bar{0}$

จะได้ว่า I_p เป็นอินติกรัลโดเมน

และเนื่องจาก I_p มีสมาชิกจำนวนจำกัด

โดยทฤษฎี 5.4.5 จะได้ว่า I_p เป็นฟิลด์

แบบฝึกหัด 5 ง

1. ถ้า R เป็นดิวิชันริง จงพิสูจน์ว่า cent R เป็นฟิลด์
2. จงพิสูจน์ว่าทุก ๆ สับริงของฟิลด์ที่มียูนิตี้จะเป็นอินติกรัลโดเมน
3. ถ้า R เป็นคอมมิวเททีพริงที่มียูนิตี้ แล้ว R จะเป็นอินติกรัลโดเมน ก็ต่อเมื่อ {0} เป็นไอดีลเฉพาะของ R
4. จงพิสูจน์บทแทรก 5.4.3
5. จงยกตัวอย่างแสดงว่าส่วนกลับ (converse) ของทฤษฎี 5.4.4 ไม่เป็นจริงเสมอไป

6. จงพิสูจน์ว่า ถ้า I_p เป็นฟิลด์แล้วจะได้ว่า p เป็นจำนวนเฉพาะ

7. ให้ R เป็นริงที่มียูนิต์ โดยที่ R ไม่เป็นคอมมิวเททีพริง และ R มีเพียง {0} และ R เท่านั้นที่เป็นไอดีลทางขวา จงพิสูจน์ว่า R เป็นดิวิชันริง

8. ให้ R เป็นริงที่มี {0} และ R เป็นไอดีลทางขวา จงพิสูจน์ว่า R เป็นดิวิชันริง หรือ R เป็นริงที่มีจำนวนของสมาชิกเป็นจำนวนเฉพาะ ซึ่ง $ab = 0$ สำหรับทุก ๆ $a, b \in R$

5.5 ฟิลด์เศษส่วนของอินติกรัลโดเมน (The Field of Quotient of an Integral Domain)

ถ้า D เป็นอินติกรัลโดเมนแล้วสมาชิกที่ไม่ใช่ศูนย์ของ D อาจจะมีหรือไม่มีอินเวอร์ส สำหรับการคูณใน D ต้องการจะสร้างระบบพีชคณิตขึ้นมาระบบหนึ่งให้เป็น F ซึ่ง F จะบรรจุ D ไว้ภายใน และ F มีคุณสมบัติที่ว่าสมาชิกทุกตัวที่ไม่ใช่ศูนย์ของ F จะมีอินเวอร์สสำหรับการคูณใน F นั่นคือ จะสร้างฟิลด์ F ซึ่งมีอินติกรัลโดเมน D อยู่ใน F ฟิลด์ F นี้จะเรียกว่าฟิลด์เศษส่วนของอินติกรัลโดเมน D เช่น ฟิลด์เศษส่วนของอินติกรัลโดเมน I คือฟิลด์ของจำนวนตรรกยะ

ต่อไปจะพิจารณาโครงสร้างของ Heuristic Description ซึ่งมีรากฐานมาจากฟิลด์ของจำนวนตรรกยะ เพื่อเป็นแนวทางในการสร้างฟิลด์เศษส่วนอินติกรัลโดเมน

ให้ D เป็นอินติกรัลโดเมนที่กำหนดให้ ฟิลด์เศษส่วน F ของ D คือเซ็ตของเศษส่วน (fraction) $\frac{a}{b}$ ทั้งหมดซึ่ง $a, b \in D, b \neq 0$ ซึ่งเศษส่วนนี้จะต้องมีคุณสมบัติต่อไปนี้คือ $\frac{a}{b} = \frac{ac}{bc}$ สำหรับทุก ๆ $a, b, c \in D, b \neq 0, c \neq 0$

นิยาม 5.5.1 สำหรับ $\frac{a}{b}, \frac{c}{d} \in F$ (นั่นคือ $a,b,c,d \in D$, $b \neq 0$, $d \neq 0$)

กำหนด $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$

และ $\frac{a}{b} \frac{c}{d} = \frac{ac}{bd}$

สามารถพิสูจน์ได้ว่า F เป็นฟิลด์ภายใต้การบวกและการคูณที่นิยามข้างบนนี้ นอกจากนั้นถ้าคิดว่าสมาชิก d ใน D คือเศษส่วนที่อยู่ในรูป $\frac{d}{1}$ แล้วจะได้ D บรรจุอยู่ใน F

ฟิลด์เศษส่วนของอินติกรัลโดเมน

ให้ D เป็นอินติกรัลโดเมน และให้

$$E = \{(a,b) / a,b \in D, b \neq 0\}$$

นั่นคือ E เป็นเซ็ตของคู่ลำดับ (ordered pairs) ของสมาชิกใน D ซึ่งสมาชิกตัวที่สองในคู่ลำดับไม่เท่ากับ 0

หมายเหตุ คู่ลำดับ (a,b) ไม่ใช่เศษส่วนที่ต้องการ เพราะว่า $(a, b) \neq (ax, bx)$ ถ้า $x \neq 1$

นิยามความสัมพันธ์ $\sim$ (relation) ในเซ็ต E ดังนี้

$(a, b) \sim (c,d)$ ก็ต่อเมื่อ $ad = bc$ สำหรับทุก ๆ $(a,b),(c,d) \in E$

ทฤษฎี 5.5.1 $\sim$ เป็นความสัมพันธ์สมมูลย์ (Equivalence Relation) บน E

พิสูจน์ ให้ $(a, b), (c,d), (f,g) \in E$

1. จะได้ว่า $(a,b) \sim (a,b)$

เพราะว่า $ab = ba$

ดังนั้น มีคุณสมบัติสะท้อน (Reflexive)

2. สมมุติ $(a,b) \sim (c,d)$

จะได้ $ad = bc$

เนื่องจาก D เป็นคอมมิวเททีพริง

ดังนั้น $da = cb$

นั่นคือ $(c,d) \sim (a,b)$

ฉะนั้น $\sim$ มีคุณสมบัติสมมาตร (Symmetric)

3. สมมุติให้ $(a,b) \sim (c,d)$ และ $(c,d) \sim (f,g)$

จะได้ $ad = bc$ และ $cg = df$

ดังนั้น $adg = bcg$ และ $cgb = dfb$

นั่นคือ $(ag)d = (bf)d$

เนื่องจาก $(c,d) \in E$, $d \neq 0$ และ D เป็นอินติกรัลโดเมน

ดังนั้นกฎการตัดออกสำหรับการคูณเป็นจริง จะทำให้ได้ว่า

$$ag = bf$$

ฉะนั้น $(a,d) \sim (f,g)$

นั่นคือ $\sim$ มีคุณสมบัติถ่ายทอด (Transitive)

จาก 1, 2, 3 ได้ว่า $\sim$ เป็นความสัมพันธ์สมมูลย์บน E

ต่อไปจะกำหนดอีควิวาเลนซ์ คลาส (Equivalence class) ของ $(a, b) \in E$ ซึ่งจะเขียนแทนด้วย $[a,b]$ ดังนี้

$$[a,b] = \{(c,d) \in E / (c,d) \sim (a,b)\}$$

$$= \{(c,d) \in E / ad = bc\}$$

นิยาม 5.5.2 การเท่ากันของอีควิวาเลนซ์คลาส

อีควิวาเลนซ์คลาส $[a,b]$ และ $[c,d]$ จะเท่ากัน ถ้า $(a, b) \sim (c,d)$ หรือ $ad = bc$

นั่นคือ $[a,b] = [ax,bx]$ สำหรับทุก ๆ สมาชิก $x \in D$ และ $x \neq 0$

เพราะฉะนั้นจึงใช้อีควิวาเลนซ์คลาส $[a,b]$ เป็นเศษส่วนตามที่กล่าวไว้ใน Heuristic Description ได้เพราะว่า $[a,b] = [ax, bx]$ สำหรับทุก ๆ $(a,b) \in E$ และทุก $x \in D$ และ $x \neq 0$

ข้อสังเกต สำหรับทุก ๆ สมาชิก $x, y \in D$ และ $x \neq 0, y \neq 0$ จะได้ว่า

$$[0,x] = [0,y]$$

และ $$[x,x] = [y,y]$$

ต่อไปให้ F เป็นเซ็ตของอีควิวาเลนซ์คลาส $[a,b]$ ซึ่ง $a,b \in D$, $b \neq 0$ นิยามการบวกและการคูณใน F ดังนี้

ให้ $[a, b]$, $[c, d] \in F$

การบวก $[a, b) + [c,d) = [ad + bc, bd]$

การคูณ $[a,b] [c,d] = [ac, bd]$

ทฤษฎี 5.5.2 การบวกและการคูณใน F ที่นิยามข้างบนนี้ กำหนดไว้ถูกต้องแล้ว (well defined)

พิสูจน์ จะแสดงว่าการบวกใน F กำหนดไว้ถูกต้องแล้ว

สมมุติ $[a,b] = [a_1, b_1)$

และ $[c,d] = [c_1, d_1]$

โดยที่ $[a,b]$, $[a_1, b_1]$, $[c,d]$, $[c_1, d_1] \in F$

ดังนั้น $ab_1 = a_1b$ .....(1)

และ $cd_1 = dc_1$ .....(2)

คูณ (1) ด้วย dd_1 และ (2) ด้วย bb_1 จะได้

$$adb_1d_1 = a_1d_1bd$$

และ $$bcb_1d_1 = b_1c_1bd$$

ดังนั้น $(ad + bc)b_1d_1 = (a_1d_1 + b_1c_1)bd$

แสดงว่า $[ad + bc, bd] = [a_1d_1 + b_1c_1, b_1d_1]$

ดังนั้น $[a,b] + [c,d] = [a_1,b_1] + [c_1,d_1]$

สำหรับการแสดงว่าการคูณใน F กำหนดไว้ถูกต้องแล้วให้ทำเป็นแบบฝึกหัด

<u>ทฤษฎี 5.5.3</u> F เป็นฟิลด์ภายใต้การบวกและการคูณข้างต้น

<u>พิสูจน์</u> <u>ตอนแรก</u> จะพิสูจน์ว่า F เป็นคอมมิวเททีพริงที่มียูนิตี้ และสมาชิกทุกตัวที่ไม่เป็นศูนย์ของ F จะต้องมีอินเวอร์สสำหรับการคูณใน F

จะแสดงคุณสมบัติบางข้อ ส่วนคุณสมบัติข้อใดที่ไม่ได้พิสูจน์ให้ทำเป็นแบบฝึกหัด

1. จะแสดงว่าสมาชิกศูนย์ของ F คือ $[0,x]$ เมื่อ x คือสมาชิกที่ไม่ใช่ศูนย์ใน D เพราะว่าสำหรับทุก ๆ สมาชิก $[a,b] \in F$

$$[a,b] + [0,x] = [ax + b0, bx]$$
$$= [ax, bx]$$
$$= [a,b]$$

และ $[0,x]+[a,b] = [0b + xa, xb]$

$= [xa, xb]$

$= [a,b]$

2. จะแสดงว่าอินเวอร์สสำหรับการบวกของ $[a,b]$ คือ $[-a, b]$

เพราะว่า สำหรับทุก ๆ $[a,b] \varepsilon F$

$[a,b]+[-a, b] = [ab - ba, bb]$

$= [0, bb]$

และ $[-a, b] + [a,b] = [-ab + ba, bb]$

$= [0, bb]$

3. จะแสดงว่ากฎการกระจายเป็นจริงใน F

สำหรับทุก ๆ $[a,b]$, $[c,d]$ และ $[f,g] \varepsilon F$

$[a,b]([c,d]+[f,g]) = [a,b][cg + df, dg]$

$= [acg + adf, bdg]$

$= [acgb + adfb, bbdg]$

$= [ac, bd]+[af, bg]$

$= [a,b][c,d]+[a,b][f,g]$

4. F มียูนิตี้คือ $[x, x]$ ซึ่ง x เป็นสมาชิกที่ไม่ใช่ศูนย์ของ D

เพราะว่า สำหรับทุก ๆ $[a,b] \varepsilon F$

$[a,b][x,x] = [ax, bx]$

$= [a, b]$

และ $[x,x][a,b] = [xa, xb]$

$= [a, b]$

5. จะแสดงว่าสมาชิกทุกตัวที่ไม่ใช่ศูนย์ของ F จะต้องมีอินเวอร์ส
สำหรับการคูณอยู่ใน F

ให้ $[m,n]$ เป็นสมาชิกที่ไม่ใช่ศูนย์ของ F ดังนั้น $m,n \in D$
และ $n \neq 0$, $m \neq 0$
ดังนั้น $[n,m]$ เป็นสมาชิกใน F
และ $[m,n]\,[n,m] = [mn, mn]$
ซึ่ง $[mn, mn]$ คือยูนิตี้ของ F
ดังนั้น อินเวอร์สสำหรับการคูณของ $[m,n]$ คือ $[n,m] \in F$
นั่นคือ F เป็นฟิลด์

<u>ทฤษฎี 5.5.4</u> ในฟิลด์เศษส่วน F ของอินติกรัลโดเมน D จะมีสับริง R ซึ่ง
ไอโซมอร์ฟิกกับอินติกรัลโดเมน D

<u>พิสูจน์</u> ให้ $R = \{[a, e] / a,e \in D\}$
จะแสดงว่า R เป็นสับริงของ F
เห็นได้ชัดว่า $R \subseteq F$
เนื่องจาก $e \in D$ ดังนั้นจะมี $[e,e] \in R$ นั่นคือ $R \neq \emptyset$
ให้ $[a,e]$, $[b,e] \in R$
จะได้ว่า $[-b , e]$ เป็นอินเวอร์สสำหรับการบวกของ $[b, e]$
ดังนั้น $[a,e] - [b,e] = [a,e] + [-b, e]$

$= [a - b, e] \in R$

และ $[a,e][b,e] = [ab, e] \in R$
นั่นคือ R เป็นสับริงของ F
ต่อไปจะต้องพิสูจน์ว่า D ไอโซมอร์ฟิกกับ R

กำหนด $\alpha : D \longrightarrow R$

โดย $\alpha(d) = [d,e]$ สำหรับทุก ๆ $d \in D$

จะแสดงว่า α กำหนดถูกต้องดีแล้ว

เนื่องจาก $\alpha(d_1) = [d_1,e]$ และ $\alpha(d_2) = [d_2, e]$

ถ้า $d_1 = d_2$

หรือ $d_1 e = d_2 e$

ดังนั้น $[d_1, e] = [d_2, e]$

นั่นคือ α กำหนดถูกต้องดีแล้ว

ต่อไปจะแสดงว่า α เป็นโฮโมมอร์ฟิซึม

พิจารณา $\alpha(c + d) = [c + d, e]$

$= [c,e] + [d,e]$

$= \alpha(c) + \alpha(d)$

และ $\alpha(cd) = [cd, e]$

$= [c,e]\,[d,e]$

$= \alpha(c)\,\alpha(d)$

นั่นคือ α เป็นโฮโมมอร์ฟิซึม

ให้ $[d,e] \in R$

จะได้ $d \in D$ และ $\alpha(d) = [d,e]$

ดังนั้น α เป็นฟังก์ชันออนทู

ต่อไปสมมุติให้ $\alpha(d) = \alpha(c)$ โดยที่ $d,c \in D$

นั่นคือ $[d,e] = [c,e]$

$de = ce$

$d = c$

ดังนั้น α เป็นฟังก์ชันหนึ่งต่อหนึ่ง
นั่นคือ α เป็นไอโซมอร์ฟิซึมของ D กับ R
แสดงว่า R ไอโซมอร์ฟิกกับ D

แบบฝึกหัด 5 จ.

1. สมมุติให้ R เป็นดิวิชันริง จงพิสูจน์ว่า cent R เป็นฟิลด์
2. จงพิสูจน์ว่าทุก ๆ สับริงที่มียูนิตี้ของฟิลด์ จะเป็นอินทิกรัลโดเมน
3. ในฟิลด์ของจำนวนเชิงซ้อน C , นิยามฟังก์ชัน $\alpha : C \longrightarrow C$ โดย $\alpha(a + bi) = a - bi$ สำหรับ $a + bi \in C$ จงแสดงว่า α เป็นออโตมอร์ฟิซึม (automorphism) ของ C
4. กำหนดให้ r, s เป็นสมาชิกของฟิลด์ F และ $r \neq 0$ จงแสดงว่ามีสมาชิก $x, y \in F$ ซึ่ง $rx = s$ และ $yr = s$
5. จงพิสูจน์ว่าฟิลด์เศษส่วน F ของอินทิกรัลโดเมน D เป็นฟิลด์ที่เล็กที่สุดที่บรรจุ D ไว้ นั่นคือต้องแสดงว่า ฟิลด์ใด ๆ ที่บรรจุ D ไว้จะต้องบรรจุ F ไว้ด้วย
6. จงพิสูจน์ว่าฟิลด์เศษส่วนของอินทิกรัลโดเมน D เป็นอินเตอร์เซคชันของฟิลด์ทั้งหมดที่บรรจุ D ไว้
