บทที่ 5
ฟังก์ชันถ่ายแบบและฟังก์ชันถอดแบบของวง
(Ring homomorphisms and isomorphisms)

ฟังก์ชันจากวง (R, +, .) ไปยังวง (S, +, .) ซึ่งยังคงรักษาการดำเนินการ + และ . ไว้เป็นเรื่องที่เรากำลังจะศึกษากันในบทนี้

5.1 ฟังก์ชันถ่ายแบบและฟังก์ชันถอดแบบของวง

(Homomorphism and isomorphism of Rings)

นิยาม

> ให้ (R, +, .) และ (S, +, .) เป็นวง $\psi : R \to S$ เป็นฟังก์ชัน จะเรียก ψ ว่าฟังก์ชันถ่ายแบบเมื่อ
>
> $\psi(x + y) = \psi(x) + \psi(y)$
>
> และ $\psi(xy) = \psi(x)\,\psi(y)$
>
> สำหรับทุก ๆ $x, y \in R$

ตัวอย่าง 5.1.1 กำหนด $f : Z_2 \to Z_6$ โดย $f(0) = 0$ และ $f(1) = 3$ แล้ว f เป็นฟังก์ชันถ่ายแบบของวง $(Z_2, +_2, \cdot_2)$ ไปใน $(Z_6, +_6, \cdot_6)$

ตัวอย่าง 5.1.2 ให้ (R, +, .) เป็นวง ถ้า f เป็นฟังก์ชันที่ส่งแต่ละสมาชิกของ r ไปบน R เองแล้ว f เป็นฟังก์ชันถ่ายแบบ

ทฤษฎี 5.1.1 ถ้า I เป็นกลุ่มอุดมคติของ R แล้วฟังก์ชันแบบบัญญัติ

$$\psi : R \to R/I \text{ กำหนดโดย } \psi(a) = a + I$$

สำหรับ $a \in R$ เป็นฟังก์ชันถ่ายแบบ

พิสูจน์

ให้ $a, b \in R$

$$\begin{aligned}\psi(a+b) &= (a+b)+I \\ &= (a+I)+(b+I) \\ &= \psi(a)+\psi(b)\end{aligned}$$

และ

$$\begin{aligned}\psi(ab) &= ab+I \\ &= (a+I)(b+I) \\ &= \psi(a)\,\psi(b)\end{aligned}$$

ψ เป็นฟังก์ชันถ่ายแบบของวง #

นิยาม ให้ $(R, +, .)$ และ $(S, +, .)$ เป็นวง ψ เป็นฟังก์ชันถ่ายแบบของวง R ไปยังวง S แล้ว จะเรียก ψ ว่า ฟังก์ชันถอดแบบของวง R ไปยังวง S ถ้า ψ เป็นฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึง (one to one และ onto)

นิยาม ถ้า ψ เป็นฟังก์ชันถ่ายแบบของวง R ไปยังวง S และเป็นฟังก์ชันหนึ่งต่อหนึ่ง เรียก ψ ว่า โมโนมอร์ฟิสซึม (monomorphism)

นิยาม ถ้า ψ เป็นฟังก์ชันถ่ายแบบของวง R ไปยังวง S และเป็นฟังก์ชันทั่วถึง เรียก ψ ว่า epimorphism

นิยาม

ให้ (R, +, .) และ (S, +, .) เป็นวง และถ้ามีฟังก์ชันถอดแบบจาก R ไปยัง-S เรากล่าวว่า วง R และวง S ถอดแบบกัน ใช้สัญลักษณ์ $R \cong S$

ตัวอย่าง 5.1.3 ฟังก์ชันในตัวอย่าง 5.1.2 เป็นฟังก์ชันถอดแบบ

ตัวอย่าง 5.1.4 ฟังก์ชันในตัวอย่าง 5.1.1 เป็น ring monomorphism

นิยาม

ให้ ψ เป็นฟังก์ชันถ่ายแบบจากวง R ไปยังวง S ส่วนกลางของ Ψ (kernel of ψ) คือ เซตของสมาชิกทุกตัวของ R ที่ภายใต้ ψ ส่งไปที่เอกลักษณ์สำหรับการบวก (0) ของ S ใช้สัญลักษณ์ Ker (ψ) นั่นคือ $\ker(\psi) = \{x \in R \mid \psi(x) = 0_S\}$

ทฤษฎี 5.1.2

ให้ ψ เป็นฟังก์ชันถ่ายแบบจากวง R ไปยังวง S แล้ว 1. ถ้า O_R เป็นเอกลักษณ์สำหรับการบวกของ R แล้ว $\psi(O_R) = O_S$ จะเป็นเอกลักษณ์สำหรับการบวกของ S 2. ถ้า $a \in R$ แล้ว $\psi(-a) = -\psi(a)$ 3. ถ้า H เป็นวงย่อยของ R แล้ว $\psi(H)$ จะเป็นวงย่อยของ S 4. ถ้า H เป็นกลุ่มอุดมคติของ R แล้ว $\psi(H)$ จะเป็นกลุ่มอุดมคติของ $\psi(R)$ 5. ถ้า T เป็นวงย่อยของ S แล้ว $\psi^{-1}(T)$ จะเป็นวงย่อยของ R 6. ถ้า T เป็นกลุ่มอุดมคติของ $\psi(R)$ แล้ว $\psi^{-1}(T)$ จะเป็นกลุ่มอุดมคติของ R 7. ถ้า R มียูนิตี้ 1_R และ $\psi(1) \neq O_S$ แล้ว $\psi(1_R) = 1_S$ จะเป็น unity ของ $\psi(R)$

พิสูจน์ 1 และ 2

ให้ ψ เป็นฟังก์ชันถ่ายแบบของ R ไปใน S

$\therefore$ ψ เป็นฟังก์ชันถ่ายแบบ จากกลุ่ม (R +) ไปในกลุ่ม (S, +)

$\therefore$ $\psi(O_R) = O_S$ เป็นเอกลักษณ์สำหรับการบวกของ S

และ $\psi(-a) = -\psi(a)$ สำหรับ $a \in R$

พิสูจน์ 3

ถ้า H เป็นวงย่อยของวง R

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

$\therefore$ $(\psi(H), +)$ เป็นกลุ่มย่อยของกลุ่ม (S, +)

ให้ $\psi(h_1)\ \psi(h_2) \in \psi(H)$

$$\because\ \psi(h_1)\psi(h_2) = \psi(h_1h_2)$$

$$= \psi(h_3) \in \psi(H)$$

แสดงว่า การคูณบน $\psi(H)$ สอดคล้องกฎการปิด

$\therefore$ $(\psi(H), +, .)$ เป็นวงย่อยของ (S, +, .)

พิสูจน์ 4

ถ้า H เป็นกลุ่มอุดมคติของ R แล้ว

สำหรับ $h \in H$ และ $r \in R$, $rh \in H$ และ $hr \in H$

ดังนั้น $\psi(rh) \in \psi(H)$ และ $\psi(hr) \in \psi(H)$

แต่ $\psi(rh) = \psi(r)\ \psi(h) \in \psi(H)$

และ $\psi(hr) = \psi(h)\ \psi(r) \in \psi(H)$

และจากพิสูจน์ 3 ได้ว่า $\psi(H)$ เป็นวงย่อยของ $\psi(R)$

$\therefore$ $\psi(H)$ เป็นกล่มอุดมคติของ $\psi(R)$

พิสูจน์ 5

ถ้า T เป็นวงย่อยของ S

$\therefore$ $(\psi^{-1}(T), +)$ จะเป็นกลุ่มย่อยของ $(R, +)$

ให้ $a, b \in \psi^{-1}(T)$

$\therefore$ $\psi(a), \psi(b) \in T$

$\therefore$ $\psi(a)\,\psi(b) \in T$

แต่ $\psi(a)\,\psi(b) = \psi(ab) \in T$

$\therefore$ $ab \in \psi^{-1}(T)$

การคูณบน $\psi^{-1}(T)$ สอดคล้องกฎการปิด

$\therefore$ $\psi^{-1}(T)$ เป็นวงย่อยของ R

พิสูจน์ 6

ถ้า T เป็นกลุ่มอุดมคติของ $\psi(R)$ แล้ว

สำหรับ $\psi(a) \in T$ และ $\psi(r) \in \psi(R)$

$\psi(a)\,\psi(r) \in T$

และ $\psi(r)\,\psi(a) \in T$

แต่ $\psi(a)\,\psi(r) = \psi(ar) \in T$

$\therefore$ $ar \in \psi^{-1}(T)$

และ $\psi(r)\,\psi(a) = \psi(ra) \in T$

$\therefore$ $ra \in \psi^{-1}(T)$

และจากพิสูจน์ 5 เราได้มาแล้วว่า

$\psi^{-1}(T)$ เป็นวงย่อยของ R

ดังนั้น $\psi^{-1}(T)$ เป็นกลุ่มอุดมคติของ R

พิสูจน์ 7

ถ้า R มียูนิตี้ 1_R

ดังนั้น สำหรับทุก ๆ $r \in R$ จะได้

$$r = r1_R$$

$$\psi(r) = \psi(r\ 1_R) = \psi(r)\psi(1_R) \qquad \text{..........(1)}$$

และ $r = 1_R r$

$$\psi(r) = \psi(1_R \cdot r) = \psi(1_R)\psi(r) \qquad \text{..........(2)}$$

จาก (1) และ (2) ได้ว่า

$\psi(1) = 1_S$ เป็นเอกลักษณ์สำหรับการคูณของ $\psi(R)$

ดังนั้น ถ้า $1_S \neq 0_S$ แล้ว $\psi(1_R) = 1_S$ เป็น unity ของ $\psi(R)$ #

บทแทรก ถ้า ψ เป็นฟังก์ชันถ่ายแบบของวง R ไปยังวง S แล้ว ker (ψ) เป็นกลุ่มอุดมคติของ R

ข้อพิสูจน์ละไว้ให้ น.ศ. ทำ

ข้อสังเกต

1. ให้ ψ เป็น ring epimorphism จากวง R ไปยังวง S ถ้า R เป็นวงที่สอดคล้องกฎการสลับที่แล้ว S จะเป็นวงที่สอดคล้องกฎการสลับที่ด้วย

ข้อพิสูจน์ละให้ น.ศ. ทำ

2. ถ้า R, S, T เป็นวง ψ เป็นฟังก์ชันถ่ายแบบ จาก R ไปยัง S และ ϕ เป็นฟังก์ชันถ่ายแบบจาก S ไปยัง T แล้ว $\phi \cdot \psi$ จะเป็นฟังก์ชันถ่ายแบบจาก R ไปยัง T

ข้อพิสูจน์ละไว้ให้ น.ศ. ทำ

ทฤษฎี 5.1.3 ให้ $(R, +, .)$ และ $(S, +, .)$ เป็นวง และให้ ψ เป็นฟังก์ชันถ่ายแบบจาก R ไปใน S แล้ว ψ จะเป็น ring monomorphism ก็ต่อเมื่อ $\ker(\psi) = \{0_R\}$

พิสูจน์

$\Rightarrow$ สมมติ ψ เป็น ring monomorphism

$\therefore$ ψ เป็นฟังก์ชันถ่ายแบบ และเป็นฟังก์ชันหนึ่งต่อหนึ่ง

$\therefore$ $\psi(0_R) = 0_S$

และ 0_R เป็นสมาชิกเพียงตัวเดียวที่ถูกส่งไปบน 0_S

ดังนั้น $\psi^{-1}(0_S) = \{0_R\}$

แต่ $\psi^{-1}(0_S) = \ker(\psi)$

$\therefore$ $\ker(\psi) = \{0_R\}$

$\Leftarrow$ สมมติ $\ker(\psi) = \{0_R\}$

ถ้า $r_1, r_2 \in R \ni \psi(r_1) = \psi(r_2)$ แล้ว

$$\begin{aligned} 0_S &= \psi(r_1) + (-\psi(r_2)) \\ &= \psi(r_1) + \psi(-r_2) \\ &= \psi(r_1 + (-r_2)) \end{aligned}$$

$\therefore$ $r_1 + (-r_2) \in \ker(\psi)$

แต่ $\ker(\psi) = \{0_R\}$

$\therefore$ $r_1 + (-r_2) = 0_R$

$\therefore$ $r_1 = r_2$

$\therefore$ ψ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

$\therefore$ ψ เป็น monomorphism #

ถ้ามี epimorphism จากวงหนึ่งไปยังวงอื่น ๆ แล้ว **จะมีการสมนัยหนึ่งต่อหนึ่งระหว่าง**โคเซตที่ก่อกำเนิดโดยส่วนกลาง (kernel) **และสมาชิกในพิสัยของฟังก์ชันถ่ายแบบ การเกี่ยวข้อง**นี้ส่งผลให้เราได้ฟังก์ชันถอดแบบระหว่างวงปันส่วนและภาพ (image) **ของฟังก์ชันถ่ายแบบ** ทฤษฎีต่อไปนี้จะช่วยให้เห็นแนวความคิดนี้เด่นชัดขึ้น

ทฤษฎี 5.1.4 | ถ้า ψ เป็น ring epimorphism จากวง R ไปยังวง S แล้ว $R/\ker(\psi) \cong S$

พิสูจน์

ถ้า ψ เป็น ring epimorphism

กำหนด $\phi : R/\ker(\psi) \to S$ โดย $\phi(r + \ker(\psi)) = \psi(r)$

สำหรับแต่ละ $r + \ker(\psi) \in R/\ker(\psi)$

จะต้องแสดงว่า ϕ เป็นฟังก์ชันถอดแบบ

ก่อนอื่นจะแสดงว่า ϕ ที่กำหนดแบบนี้เป็นฟังก์ชัน

สมมติ $x + \ker(\psi) = y + \ker(\psi)$

$\therefore x - y \in \ker(\psi)$

$$\psi(x \quad y) = 0_S$$

$$\psi(x) + (\psi(-y)) = 0_S$$

$$\psi(x) + (-\psi(y)) = 0_S$$

ดังนั้น $\psi(x) = \psi(y)$

$$\phi[x + \ker(\psi)] = \phi[y + \ker(\psi)]$$

แสดงว่า ϕ เป็นฟังก์ชัน

$$\phi\,[(x + \ker(\psi)) + (y + \ker(\psi))] = \phi[(x + y) + \ker(\psi)]$$

$$= \psi(x + y)$$

$$= \psi(x) + \psi(y)$$
$$= \phi[x + \ker(\psi)] + \phi[y + \ker(\psi)]$$

และ $\phi[x + \ker(\psi) \cdot y + \ker(\psi)] = \phi[xy + \ker(\psi)]$
$$= \psi(xy)$$
$$= \psi(x)\ \psi(y)$$
$$= \phi[x + \ker(\psi)]\ \phi[y + \ker(\psi)]$$

ดังนั้น ϕ เป็นฟังก์ชันถ่ายแบบ

เนื่องจาก ψ เป็นฟังก์ชันทั่วถึง

ถ้า $s \in S$ แล้ว $\exists r \in R \ni \psi(r) = s$

แต่ $\phi(r + \ker(\psi)) = \psi(r)$
$$= s$$

แสดงว่า สำหรับแต่ละ $s \in S$ $\exists x + \ker(\psi) \in R/\ker(\psi) \ni \phi(r + \ker(\psi)) = s$

$\therefore$ ϕ เป็นฟังก์ชันทั่วถึง

ต่อไปจะแสดงว่า ϕ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

ถ้า $x + \ker(\psi) \in \ker(\phi)$

$$\phi(x + \ker(\psi)) = 0_S$$

แต่ $\phi(x + \ker(\psi)) = \psi(x)$
$$\psi(x) = 0_S$$
$$x \in \ker(\psi)$$
$$x + \ker(\psi) = \ker(\psi)$$

และ $0_R + \ker(\psi) = \ker(\psi)$

$\therefore$ $x + \ker(\psi) = 0_R + \ker(\psi)$

$$\ker(\psi) \subseteq \{0_R + \ker(\psi)\} \qquad (1)$$

และเนื่องจาก $0_R + \ker(\psi) \in \ker(\phi)$ แน่นอน

$\therefore \quad \{0_R + \ker(\psi)\} \subseteq \ker(\phi)$ ....(2)

ดังนั้น จาก (1) และ (2) ได้ว่า

$$\ker(\phi) = \{0_R + \ker(\psi)\}$$

แสดงว่า ϕ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

ดังนั้น ϕ เป็นฟังก์ชันถอดแบบ #

ทฤษฎี 5.1.5 ถ้า R เป็นวงที่มี I และ J เป็นกลุ่มอุดมคติ ซึ่ง $I \subseteq J$ แล้ว $(R/I)/(J/I) \cong R/J$

พิสูจน์

กำหนด $\psi : R/I \to R/J$ โดย $\psi(r + I) = r + J$

สำหรับแต่ละ $r \in R$

ก่อนอื่นจะแสดงก่อนว่า ψ เป็นฟังก์ชัน

สมมติ $x + I = y + I$

$x-y \in I$

tad $1 \subseteq J$

$x-y \in J$

$x + J = y + J$

$\psi(x + I) = \psi(y + I)$

แสดงว่า ψ เป็นฟังก์ชัน

เนื่องจาก $\psi[(x + I) + (y + I)] = \psi[(x + y) + I]$

$= (x + y) + J$

$$= (x + J) + (y + J)$$

$$= \psi(x + I) + \psi(y + I)$$

และ $\psi[(x + I)(y + I)] = \psi[xy + I]$

$$= xy + J$$

$$= (x + J)(y + J)$$

$$= \psi(x + I)\,\psi(y + I)$$

$\therefore$ ψ เป็นฟังก์ชันถ่ายแบบ

เนื่องจาก ถ้า $x + J \in R/J$ แล้ว

$x \in R$ และ $x + I \in R/I$

ดังนั้น $\psi(x + I) = x + J$

แสดงว่า ψ เป็นฟังก์ชันทั่วถึง

เนื่องจาก ψ เป็นฟังก์ชันถ่ายแบบและทั่วถึง ดังนั้นโดยทฤษฎี 5.1.4 เราจึงได้ว่า $(R/I)/\ker(\psi) \cong R/J$

ดังนั้น ถ้าเราสามารถหาได้ว่า $\ker(\psi) = J/I$ เราก็จะได้ข้อพิสูจน์ที่สมบูรณ์ของทฤษฎีนี้

ให้ $x + I \in \ker(\psi)$

$$\psi(x + I) = 0 + J$$

แต่ $\psi(x + I) = x + J$

$\therefore$ $0 + J = x + J$

$$x - 0 \in J$$

$$x \in J$$

ดังนั้น $x + I \in J/I$

$$\ker(\psi) \subseteq J/I \qquad \text{..........(1)}$$

ให้ $a + I \in J/I$

$$\psi(a + I) = a + J$$

$$= \quad e + J$$

$$a + I \in \ker(\psi)$$

$$J/I \subseteq \ker(\psi) \qquad \ldots\ldots\ldots\ldots (2)$$

จาก (1) และ (2) ทำให้ได้ว่า

$$\ker(\psi) = J/I$$

$$(R/I)/(J/I) \cong R/J \qquad \#$$

หมายเหตุ ในการพิสูจน์ทฤษฎี 5.1.5 นี้ ก่อนอื่นเราหาก่อนว่ามีฟังก์ชันถ่ายแบบและทั่วถึงจาก R/I ไปยัง R/J ต่อจากนั้น โดยอาศัยทฤษฎี 5.1.4 เราก็เหลือแต่เพียงแสดงว่า $\ker(\psi) = J/I$

ทฤษฎี 5.1.6 ถ้า R เป็นวง S เป็นวงย่อยของ R และ I เป็นกลุ่มอุดมคติของ R แล้ว $S/(S \cap I) \cong (S + I)/I$

พิสูจน์

กำหนด $\psi : S \to S/I$ โดย $\psi(s) = s + I$ สำหรับแต่ละ $s \in S$

ถ้า $s_1, s_2 \in S$ แล้ว

$$\begin{aligned} \psi(s_1 \ t \ s_2) &= (s_1 + s_2) + I \\ &= (s_1 + 1) + (s_2 + 1) \\ &= \psi(s_1) + \psi(s_2) \end{aligned}$$

และ

$$\begin{aligned} \psi(s_1 s_2) &= s_1 s_2 + I \\ &= (s_1 + I)(s_2 + I) \\ &= \psi(s_1)\ \psi(s_2) \end{aligned}$$

ดังนั้น ψ เป็นฟังก์ชันถ่ายแบบ

ให้ $(s + i) + I \in (S + I)/I$ แล้ว

$$\begin{aligned} \psi(s) &= s + I \\ &= s + (i + I) \\ &= (s + i) + I \end{aligned}$$

ดังนั้น ψ เป็นฟังก์ชันทั่วถึง

โดยทฤษฎี 5.1.4

$$S/\ker(\psi) \cong (S + I)/I$$

ข้อพิสูจน์จะสมบูรณ์ถ้าสามารถหาได้ว่า $\ker(\psi) = S \cap I$

ให้ $x \in \ker(\psi)$

$$\begin{aligned} \psi(x) &= 0 + I = x + I \\ 0 + x &\in I \\ x &\in I \end{aligned}$$

และ $\ker(\psi)$ เป็นวงย่อยของ S ด้วย

ดังนั้น $x \in S$

$$x \in S \cap I$$

$$\ker(\psi) \subseteq S \cap I \qquad .(1)$$

ให้ $y \in S \cap I$

$$y \in S \text{ และ } Y \in I$$

เนื่องจาก $y \in S$

$\therefore \quad \psi(y) = y + I$

แต่ $y \in I$ ด้วย

$$y + I = 0 + I$$

$$\psi(y) = 0 + I$$

$$y \in \ker(\psi)$$

$$S \cap I \subseteq \ker(\psi) \qquad \text{.........(2)}$$

จาก (1) และ (2) ได้ว่า

$$\ker(\psi) = S \cap I$$

$$\therefore \frac{S}{S \cap I} \cong \frac{S + I}{I}$$

#

ทฤษฎี 5.1.7 (Fundamental homomorphism theory)

> ให้ ψ เป็นฟังก์ชันถ่ายแบบของวง R ไปในวง R′ โดยมี kernel K แล้ว $\psi(R)$ เป็นวง และจะมีฟังก์ชันถอดแบบแบบบัญญัติ (canonical isomorphism ของ $\psi(R)$ กับ R/K

พิสูจน์

ทฤษฎี 5.1.2 แสดงแล้วว่า $\psi(R)$ เป็นวง

ให้ $(a + K) \in R/K$ และ

กำหนด $\phi(R/K) \to \psi(R)$ โดย $\phi(a + K) = \psi(a)$

ก่อนอื่น จะต้องแสดงก่อนว่า ϕ แจ่มชัด (well defined) โดยให้ $b \in a + K$ แล้วจะต้องแสดงว่า $\phi(a) = \phi(b)$

$\because b \in a + K$

$\therefore$ มี $k_1 \in K \ni b = a + k_1$

$-a + b = k_1$

$$e' = \phi(k_1) = \phi(-a + b)$$

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

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

$$e' + \phi(a) = \phi(b)$$

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

$\therefore$ ϕ แจ่มชัด

ต่อไปจะแสดงว่า ϕ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

ให้ $a + K, b + K \in R/K$ โดยที่ $\phi(a + K) = \phi(b + K)$

$$\therefore \quad \psi(a) = \psi(b)$$

$$e' = -(\psi(a)) + (\psi(b))$$

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

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

$$\therefore \quad -a + b \in K$$

$$a + K = b + K$$

$\therefore$ ϕ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

ปราศจากข้อสงสัย (obvious) ϕ เป็นฟังก์ชันทั่วถึงบน $\psi(R)$

เพราะถ้าให้ $\psi(a) \in \psi(R)$

$\therefore$ $a \in R \Rightarrow$ มี $a + K \in R/K \ni \phi(a + K) = \psi(a)$

$$\because \quad \phi|(a + K) + (b + K)| = \psi(a + b)$$

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

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

และ $$\phi|(a + K)(b + K)| = \psi(ab)$$

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

$$= \phi(a + K)\,\phi(b)$$

$\therefore$ ϕ เป็นฟังก์ชันถอดแบบของวง

และ ϕ เป็น canonical ในแง่ที่ว่า $\gamma : R \to R/K$ เป็น canonical map แล้ว $\psi = \gamma\phi$ #

5.2 กลุ่มอุดมคติใหญ่สุดและกลุ่มอุดมคติจำนวนเฉพาะ
(Maximal and Prime ideals)

ในหัวข้อนี้ เราจะมากำหนดเงื่อนไขที่จำเป็นสำหรับ R/S ที่จะเป็นสนาม และจะมาดูกันว่าเมื่อไร R/S จะเป็นโดเมนเชิงจำนวนเต็ม

ถ้า R เป็นวงที่มี unity และสอดคล้องกฎการสลับที่แล้ว วงบันส่วน R/S เป็นวงที่มี unity $1 + S$ และสอดคล้องกฎการสลับที่ด้วย ในกรณีนี้เราจำเป็นที่จะต้องสร้างเงื่อนไขที่จำเป็นและเพียงพอสำหรับแต่ละสมาชิก $a + S \neq 0 + S$ ที่จะมีตัวผกผันสำหรับการคูณ การมีของตัวผกผันสำหรับการคูณใน R/S นี้ ขึ้นอยู่กับ S เป็นกลุ่มอุดมคติชนิดพิเศษ ที่เรียกว่า กลุ่มอุดมคติใหญ่สุด (maximal ideal)

นิยาม กลุ่มอุดมคติ S ของวง R จะเป็นกลุ่มอุดมคติใหญ่สุดก็ต่อเมื่อ

1. $S \neq R$ และ
2. ไม่มีกลุ่มอุดมคติ J ใน $R \ni S \subset J \subset R$

ข้อสังเกต จากนิยามจะพบว่า

1. ถ้า J เป็นกลุ่มอุดมคติของ R และ $S \subsetneq J$, $S \neq J$ แล้ว $J = R$
2. ถ้า J เป็นกลุ่มอุดมคติของ R และ $S \subseteq J \subseteq R$ แล้ว $S = J$ หรือมิฉะนั้นก็ $J = R$
3. ถ้าวง R มีกลุ่มอุดมคติใหญ่สุด R จะต้องไม่ใช่ $\{0\}$

ตัวอย่าง 5.2.1 กลุ่มอุดมคติ $<2>$ และ $<3>$ เป็นกลุ่มอุดมคติใหญ่สุดของวง Z

ตัวอย่าง 5.2.2 ให้ $E = \{2n \mid n \in Z\}$

$(E, +, .)$ เป็นวง

$<4>$ เป็นกลุ่มอุดมคติใหญ่สุดของ E

ข้อสังเกตุ ถ้า I เป็นกลุ่มอุดมคติใหญ่สุดของ R แล้ว R/I จะไม่มีกลุ่มอุดมคติแท้ เพราะกลุ่มอุดมคติแท้ J/I ใด ๆ ของ R/I จะนำไปสู่กลุ่มอุดมคติ J ของ R โดยที่ $I \subset J \subset R$ และ $I \neq J \neq R$ ซึ่งทำให้เกิดการขัดแย้งต่อคุณสมบัติการเป็นอุดมคติใหญ่สุดของ I และเมื่อไปเกี่ยวข้องกับสนามทำให้เราได้ทฤษฎีบทข้างล่างนี้

ทฤษฎี 5.2.1 ให้ R เป็นวงที่มี unity และสอดคล้องกฎการสลับที่ แล้ว I จะเป็นกลุ่มอุดมคติใหญ่สุดก็ต่อเมื่อ R/I เป็นสนาม

พิสูจน์

$\Rightarrow$ สมมติ I เป็นกลุ่มอุดมคติใหญ่สุดของ R

เนื่องจาก R เป็นวงที่มี unity และสอดคล้องกฎการสลับที่

ดังนั้น R/I เป็นวงที่ไม่มี unity และสอดคล้องกฎการสลับที่

และ R/I ไม่มีกลุ่มอุดมคติแท้

ดังนั้น โดยทฤษฎี 4.2.4

R/I เป็นสนาม

$\Leftarrow$ สมมติ R/I เป็นสนาม

โดยบทแทรกของทฤษฎี 4.1.1

R/I ไม่มีกลุ่มอุดมคติแท้ ....(*)

ถ้ามีกลุ่มอุดมคติ J ของ R ที่ $I \subset J \subset R$ และ $I \neq J \neq R$ แล้ว

J/I จะเป็นกลุ่มอุดมคติแท้ของ R/I

ซึ่งขัดแย้งกับ (*)

ดังนั้น จะต้องไม่มีกลุ่มอุดมคติ J ของ R ที่ $I \subset J \subset R$ และ $I \neq J \neq R$

$\therefore$ I เป็นกลุ่มอุดมคติใหญ่สุด #

เรื่องต่อมาเราจะมาดูแนวความคิดเกี่ยวกับกลุ่มอุดมคติจำนวนเฉพาะ (prime ideals) ซึ่งแนวความคิดนี้มีขึ้นจากการพิจารณากลุ่มอุดมคติของจำนวนเต็มที่ก่อกำเนิดโดยจำนวนเฉพาะ

· พิจารณา $<2> \subset Z$ และขอให้สังเกตว่า ถ้า $mn \in <2>$ แล้ว $mn = 2k$ ดังนั้น $2|mn$ แต่ 2 เป็นจำนวนเฉพาะ ดังนั้น $2|m$ หรือมิฉะนั้นก็ $2|n$ และด้วยเหตุนี้ m หรือมิฉะนั้นก็ n เป็นสมาชิกของ $<2>$

นิยาม ให้ I เป็นกลุ่มอุดมคติของวง R แล้ว จะกล่าวว่า I เป็นกลุ่มอุดมคติจำนวนเฉพาะ (prime ideal) ของ R เมื่อสำหรับ $r, s \in R \ni rs \in I$ แล้ว $r \in I$ หรือมิฉะนั้นก็ $s \in I$

ตัวอย่าง 5.2.3 พิจารณาวง Z กลุ่มอุดมคติ $\{0\}$, Z และ $<2>$ เป็นกลุ่มอุดมคติจำนวนเฉพาะ

ตัวอย่าง 5.2.4 กลุ่มอุดมคติ $<6>$ และ $<35>$ ไม่ใช่กลุ่มอุดมคติจำนวนเฉพาะของ Z

ตัวอย่าง 5.2.5 ให้ $E = \{2n | n \in Z\}$ กลุ่มอุดมคติ $<4>$ ไม่เป็นกลุ่มอุดมคติจำนวนเฉพาะของ E แต่กลุ่มอุดมคติ $<6>$ เป็นกลุ่มอุดมคติจำนวนเฉพาะของ E

ทฤษฎี 5.2.2 ให้ R เป็นวง และ I เป็นกลุ่มอุดมคติของ R แล้ว I เป็นกลุ่มอุดมคติจำนวนเฉพาะ ก็ต่อเมื่อ R/I ไม่มีตัวหารของศูนย์

พิสูจน์

$\Rightarrow$ สมมติ I เป็นกลุ่มอุดมคติจำนวนเฉพาะ

และให้ $r + I, s + I \in R/I$ โดยที่ $(r + I)(s + I) = 0 + I$

$\because \quad (r + I)(s + I) = 0 + I$

$\therefore \quad rs + I = 0 + I$

$\therefore \quad rs - 0 \in I$

$\therefore \quad rs \in I$

แต่ I เป็นกลุ่มอุดมคติจำนวนเฉพาะ

$\therefore$ $r \in I$ หรือมิฉะนั้นก็ $s \in I$

$\therefore$ $r + I = 0 + I$ หรือมิฉะนั้นก็ $s + I = 0 +$

ดังนั้น R/I ไม่มีตัวหารของศูนย์

$\Leftarrow$ สมมติ R/I ไม่มีตัวหารของศูนย์

ให้ $r, s \in R$ โดยที่ $rs \in I$

$\because$ $rs \in I$

$\therefore$ $rs + I = I = 0 + I$

$(r + I)(s + I) = 0 + I$

แต่ R/I ไม่มีตัวหารของศูนย์

$r + I = 0 + I$ หรือมิฉะนั้นก็ $s + I = 0 + I$

ดังนั้น $r \in I$ หรือมิฉะนั้นก็ $s \in I$ #

บทแทรก | ให้ I เป็นกลุ่มอุดมคติของวงที่สอดคล้องกฎการสลับที่ R แล้ว R/I เป็นโดเมนเชิงจำนวนเต็มก็ต่อเมื่อ I เป็นกลุ่มอุดมคติจำนวนเฉพาะ

ทฤษฎี 5.2.3 | ถ้า R เป็นวงที่มี unity และสอดคล้องกฎการสลับที่แล้ว ทุก ๆ กลุ่มอุดมคติใหญ่สุดของ R เป็นกลุ่มอุดมคติจำนวนเฉพาะ

พิสูจน์

ให้ I เป็นกลุ่มอุดมคติใหญ่สุดของ R

$\therefore$ R/I เป็นสนาม

$\therefore$ R/I เป็นโดเมนเชิงจำนวนเต็ม

โดยบทแทรกของทฤษฎี 5.2.2

I ต้องเป็นกลุ่มอุดมคติจำนวนเฉพาะ #

5.3 **สนามจำนวนเฉพาะ** (Prime fields)

ให้ R เป็นวงที่มี unity 1 นักศึกษาคงยังจำได้ว่า

$n.1 = 1 + 1 + + 1$ ทั้งหมด n ตัว สำหรับ $n > 0$

$= -1 + (-1) + \dots + (-1)$ ทั้งหมด n ตัว สำหรับ $n < 0$

และ $n.1 = 0$ สำหรับ $n = 0$

ทฤษฎี 5.3.1 | ถ้า R เป็นวงที่มี unity 1 แล้ว การส่ง $\psi : Z \to R$ กำหนดโดย $\phi(n) = n.1$ สำหรับ $n \in Z$ เป็นฟังก์ชันถ่ายแบบ

พิสูจน์

ให้ $m,n \in Z$

$$\psi : (n + m) = (n + m) . 1$$
$$= (n . 1) + (m . 1)$$
$$= \psi(n) + \psi(m)$$

และเนื่องจากกฎการแจกแจงใน R เราได้

$$\underbrace{(1 + 1 + \ldots + 1)}_{n \text{ ตัว}}\underbrace{(1 + 1 + \ldots + 1)}_{m \text{ ตัว}} = \underbrace{(1 + 1 + \ldots + 1)}_{nm \text{ ตัว}}$$

ดังนั้น $(n . 1)(m . 1) = (nm) . 1$ สำหรับ $n, m > 0$

ในทำนองเดียวกันเนื่องจากกฎการแจกแจงเป็นจริงบน Z เราจึงได้

สำหรับทุก ๆ $n, m \in Z$

$$(n . 1)(m . 1) = (nm) . 1$$

ดังนั้น

$$\psi(nm) = (mn) . 1$$
$$= (n . 1)(m . 1)$$
$$= \psi(n)\, \psi(m)$$

$\therefore$ ψ เป็นฟังก์ชันถ่ายแบบ #

บทแทรก

ถ้า R เป็นวงที่มี unity และ Char (R) = n > 1
แล้ว R จะมีวงย่อย ซึ่งถอดแบบกันกับ Z_p
ถ้า Char (R) = 0 แล้ว R จะมีวงย่อยที่ถอดแบบกับ Z

พิสูจน์

ให้ $\psi : Z \rightarrow R$ กำหนดโดย $\psi(m) = m . 1$ สำหรับ $\forall m \in Z$

โดยทฤษฎี 5.3.1 ψ เป็นฟังก์ชันถ่ายแบบ

ker (ψ) ต้องเป็นกลุ่มอุดมคติของ Z

กลุ่มอุดมคติของ Z ทุกกลุ่มจะต้องอยู่ในรูป sZ สำหรับบาง $s \in Z$

โดยทฤษฎี 2.3.1 ทำให้ได้ว่า

ถ้า Char (R) $= n > 0$ แล้ว

$$\ker(\psi) = nZ$$

แล้ว ภาพ (image) $\psi(Z) \leqslant R$

และ $\psi(Z) \cong Z/nZ \cong Z_p$

ถ้า Char (R) $= 0$ แล้ว

$m \cdot 1 \neq 0$ สำหรับทุก ๆ $m \neq 0$

ดังนั้น $\ker(\psi) = \{0\}$

$\therefore \psi(Z) \cong Z$ #

ทฤษฎี 5.3.2 ให้ F เป็นสนาม แล้ว Char (F) $= p$ ($p =$ จำนวนเฉพาะ) และมีสนามย่อยของ F ซึ่งถอดแบบกันกับ Z_p หรือมิฉะนั้นก็ Char (F) $= 0$ และมีสนามย่อยของ F ซึ่งถอดแบบกันกับ Q

พิสูจน์

ถ้า Char (F) $= n \neq 0$

โดยบทแทรกข้างต้น

F มีสนามย่อย ซึ่งถอดแบบกันกับ Z_p

ดังนั้น n จะต้องเป็นจำนวนเฉพาะ หรือ F จะต้องมีตัวหารของศูนย์

ถ้า Char (F) $= 0$ แล้ว

F จะต้องมีสนามย่อย ซึ่งถอดแบบกันกับ Z
ในกรณีนี้ โดยบทแทรกของทฤษฎี 3.2.1 แสดงว่า
F จะต้องมีสนามของผลหารของวงย่อยนี้
และสนามของผลหารนี้จะต้องถอดแบบกับ Q #

ดังนั้น ทุก ๆ สนาม มีสนามย่อยซึ่งถอดแบบกับ Z_p สำหรับบาง p ที่เป็นจำนวนเฉพาะ หรือมิฉะนั้นก็สนามย่อยถอดแบบกับ Q

นิยาม สนาม Z_p และ Q ตามทฤษฎี 5.3.2 เรียกสนามจำนวนเฉพาะ (prime fields)

นิยาม ถ้า F เป็นสนาม และ K เป็นสนามย่อยของ F โดยที่ K อยู่ในทุก ๆ สนามย่อยของ F (K เป็นสนามย่อยที่ "เล็กที่สุด" ของ F) แล้วเรียก K ว่า สนามย่อยจำนวนเฉพาะ (prime subfield) ของ F

แบบฝึกหัดที่ 5

1) จงพิจารณาข้อความแต่ละข้อต่อไปนี้เป็นจริงหรือเป็นเท็จ

..............ก) ฟังก์ชันถ่ายแบบของวง คือ ฟังก์ชันถอดแบบของกลุ่ม

..............ข) ฟังก์ชันถ่ายแบบของวงจะเป็นฟังก์ชันหนึ่งต่อหนึ่ง ก็ต่อเมื่อส่วนกลางคือ 0

..............ค) ส่วนกลางของฟังก์ชันถ่ายแบบของวง เป็นกลุ่มอุดมคติของวงนั้น

..............ง) ทุก ๆ กลุ่มอุดมคติจำนวนเฉพาะของทุก ๆ วงที่มี unity และสอดคล้องกฎการสลับที่เป็นกลุ่มอุดมคติใหญ่สุด

..............จ) ทุก ๆ กลุ่มอุดมคติใหญ่สุดของทุก ๆ วงที่มี unity และสอดคล้องกฎการสลับที่เป็นกลุ่มอุดมคติจำนวนเฉพาะ

..............ฉ) Q เป็นสนามย่อยจำนวนเฉพาะของตัวเอง

..............ช) สนามย่อยจำนวนเฉพาะของ C คือ R

..............ซ) ทุก ๆ สนามบรรจุสนามจำนวนเฉพาะเป็นสนามย่อยของมัน

2) จงบอกฟังก์ชันถ่ายแบบทั้งหมดของวง Z ไปยังวง Z

3) จงบอกฟังก์ชันถ่ายแบบทั้งหมดของวง $Z + Z$ ไปยังวง Z

4) จงหากลุ่มอุดมคติจำนวนเฉพาะทั้งหมด และกลุ่มอุดมคติใหญ่สุดทั้งหมดของ Z_{12}

5) จงหากลุ่มอุดมคติใหญ่สุดของ $Z + Z$

6) จงหากลุ่มอุดมคติจำนวนเฉพาะของ $Z + Z$ ซึ่งไม่ใช่กลุ่มอุดมคติใหญ่สุด

7) จงหากลุ่มอุดมคติแท้ของ $Z + Z$ ซึ่งไม่ใช่กลุ่มอุดมคติจำนวนเฉพาะ

8) จงบอกฟังก์ชันถ่ายแบบทั้งหมดของวง $Z + Z$ ไปยัง $Z + Z$