พีชคณิตนามธรรม Abstract Algebra (ปลายภาค)

ผศ.ดร.ธนัชยศ จำปาหวาย

สาขาวิชาคณิตศาสตร์ คณะครุศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา

เนื้อหา Content

กลางภาค

- บทที่ 1 ความรู้พื้นฐาน
- บทที่ 2 กรุป
- บทที่ 3 กรุปย่อย
- บทที่ 4 กรุปย่อยปกติ

ปลายภาค

- บทที่ 5 สมสัณฐาน
- บทที่ 6 ริง
- บทที่ 7 โดเมนเชิงจำนวนเต็ม
- บทที่ 8 ริงพหุนาม

บทที่ 5 สมสัณฐาน

5.1 ฟังก์ชันสาทิสสัณฐาน

บทนิยาม

ให้ $(G,*)$ และ $(G',\circledast)$ เป็นกรุป

เรียกฟังก์ชัน $\varphi : G \to G'$ ว่า **ฟังก์ชันสาทิสสัณฐาน (homomorphism)** ถ้า

$$\varphi(x*y) = \varphi(x) \circledast \varphi(y) \qquad \text{ทุก ๆ } x,y \in G$$

และ **เคอร์เนล (kernel)** ของ φ เขียนแทนด้วย $\mathrm{Ker}(\varphi)$ นิยามโดย

$$\mathrm{Ker}(\varphi) = \{x \in G : \varphi(x) = e'\}$$

เมื่อ e' เป็นเอกลักษณ์ของ G'

เขียน $\varphi(xy) = \varphi(x)\varphi(y)$ แทนการเขียน $\varphi(x*y) = \varphi(x) \circledast \varphi(y)$

ตัวอย่าง

ให้ G และ G' เป็นกรุป เมื่อ e' เป็นเอกลักษณ์ของ G'

จงตรวจสอบว่า φ เป็นฟังก์ชันสาทิสสัณฐานหรือไม่

1. ให้ $\varphi : G \to G'$ นิยามโดย $\varphi(x) = e'$ เมื่อ $x \in G$
2. ให้ $\varphi : G \to G$ นิยามโดย $\varphi(x) = x^{-1}$ เมื่อ $x \in G$

ตัวอย่าง

จงตรวจสอบว่า φ เป็นฟังก์ชันสาทิสสัณฐานหรือไม่

1. ให้ $\varphi : (GL_2(\mathbb{R}), \cdot) \to (\mathbb{R}^*, \cdot)$ นิยามโดย $\varphi(A) = \det(A)$
2. ให้ $\varphi : (M_{nn}(\mathbb{R}), +) \to (\mathbb{R}, +)$ นิยามโดย $\varphi(A) = \det(A)$

ตัวอย่าง

จงตรวจสอบว่า φ เป็นฟังก์ชันสาทิสสัณฐานหรือไม่ และหา $\mathrm{Ker}(\varphi)$

1. ให้ $\varphi : (\mathbb{C}^*, \cdot) \to (\mathbb{R}^*, \cdot)$ นิยามโดย $\varphi(z) = |z|$ เมื่อ $z \in \mathbb{C}^*$
2. ให้ $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}_6, +)$ นิยามโดย $\varphi(x) = \bar{x}$ เมื่อ $x \in \mathbb{Z}$

ตัวอย่าง

ให้ $\varphi : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ นิยามโดย $\varphi(x) = \cos x + i \sin x$ เมื่อ $x \in \mathbb{R}$

จงแสดงว่า φ เป็นฟังก์ชันสาทิสสัณฐาน และหา $\mathrm{Ker}(\varphi)$

ตัวอย่าง

ให้ $\varphi : (\mathbb{R}^2, +) \to (\mathbb{R}, +)$ นิยามโดย $\varphi((x, y)) = x + y$ เมื่อ $x, y \in \mathbb{R}$

จงแสดงว่า φ เป็นฟังก์ชันสาทิสสัณฐาน และหา $\mathrm{Ker}(\varphi)$

ทฤษฎีบท

ให้ G เป็นกรุป และ $N \trianglelefteq G$ ให้ $\pi : G \to G/N$ นิยามโดย

$$\pi(g) = Ng \qquad \text{ทุก ๆ } g \in G$$

แล้ว π เป็นฟังก์ชันสาทิสสัณฐานแบบทั่วถึง

ซึ่งจะเรียกว่า ***ฟังก์ชันสาทิสสัณฐานธรรมชาติ (natural homomorphism)***

ทฤษฎีบท

ให้ G และ G' เป็นกรุป โดยที่ e และ e' เป็นเอกลักษณ์ของ G และ G' ตามลำดับ ให้ $\varphi : G \to G'$ เป็นฟังก์ชันสาทิสสัณฐาน และ $a \in G$ ซึ่งมีอันดับจำกัด และ $n \in \mathbb{Z}$ จะได้ว่า

1. $\varphi(e) = e'$
2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$
3. $\varphi(a^n) = (\varphi(a))^n$
4. $\circ(\varphi(a)) \mid \circ(a)$

ทฤษฎีบท

ให้ G และ G' เป็นกรุป โดยที่ $\varphi : G \to G'$ เป็นฟังก์ชันสาทิสสัณฐาน จะได้ว่า

1. $Ker(\varphi) \trianglelefteq G$
2. $Ran(\varphi) \leq G'$
3. *ถ้า G เป็นกรุปวัฏจักร แล้ว $Ran(\varphi)$ เป็นกรุปวัฏจักร*

ทฤษฎีบท

ให้ G และ G' เป็นกรุป โดยที่ $\varphi : G \to G'$ เป็นฟังก์ชันสาทิสสัณฐาน จะได้ว่า

$$\varphi \quad \text{เป็นฟังก์ชัน 1-1} \quad \text{ก็ต่อเมื่อ} \quad Ker(\varphi) = \{e\}$$

ตัวอย่าง

ให้ $\varphi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ นิยามโดย $\varphi(x) = e^x$

จะแสดงว่า $\varphi(x)$ เป็นฟังก์ชันสาทิสสัณฐานแบบหนึ่งต่อหนึ่ง

5.2 ฟังก์ชันสมสัณฐาน

บทนิยาม

ให้ G และ G' เป็นกรุป จะเรียกฟังก์ชัน $\varphi : G \to G'$ ว่าเป็น **ฟังก์ชันสมสัณฐาน (isomorphism)** ก็ต่อเมื่อ

$$\varphi \text{ เป็นฟังก์ชันสาทิสสัณฐานหนึ่งต่อหนึ่งทั่วถึง}$$

ถ้า φ เป็นฟังก์ชันสมสัณฐาน จะกล่าวว่า G **สมสัณฐาน (isomoephic)** กับ G' เขียนแทน $G \cong G'$

ข้อสังเกต

$G \cong G'$ ก็ต่อเมื่อ มีฟังก์ชัน $\varphi : G \to G'$ เป็นฟังก์ชันสมสัณฐาน

ตัวอย่าง

จงตรวจสอบว่าฟังก์ชันสาทิสสัณฐาน φ เป็นฟังก์ชันสมสัณฐานหรือไม่

1. $\varphi : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ นิยามโดย $\varphi(x) = 2^x$
2. $\varphi : (GL_2(\mathbb{R}), \cdot) \to (\mathbb{R}^*, \cdot)$ นิยามโดย $\varphi(A) = \det(A)$

ทฤษฎีบท

ให้ G และ G' เป็นกรุป และ $a \in G$ ถ้า $\varphi : G \to G'$ เป็นฟังก์ชันสมสัณฐาน แล้ว

1. *φ^{-1} เป็นฟังก์ชันสมสัณฐานจาก G' ไป G*
2. *ถ้า $\circ(a)$ เป็นอันดับจำกัด แล้ว $\circ(a) = \circ(\varphi(a))$*

ทฤษฎีบท

ให้ G_1 และ G_2 เป็นกรุป

$$\text{ถ้า} \quad G_1 \cong G_2 \quad \text{แล้ว} \quad G_2 \cong G_1$$

ทฤษฎีบท

ให้ G_1, G_2 *และ* G_3 *เป็นกรุป*

$$\text{ถ้า} \quad G_1 \cong G_2 \quad \text{และ} \quad G_2 \cong G_3 \quad \text{แล้ว} \quad G_1 \cong G_3$$

ทฤษฎีบท

ให้ G *เป็นกรุปวัฏจักร จะได้ว่า*

1. *ถ้า* G *เป็นกรุปอนันต์ แล้ว* $G \cong \mathbb{Z}$
2. *ถ้า* G *เป็นกรุปจำกัดที่มีอันดับเป็น* n *แล้ว* $G \cong \mathbb{Z}_n$

บทแทรก

ให้ G เป็นกรุป ซึ่ง $|G| = p$ เมื่อ p เป็นจำนวนเฉพาะ จะได้ว่า $G \cong \mathbb{Z}_p$

บทแทรก

ให้ $m, n \in \mathbb{N}$ ถ้า m และ n เป็นจำนวนเฉพาะสัมพัทธ์กันแล้ว $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$

ทฤษฎีบท

ให้ G และ G' เป็นกรุป ซึ่ง $G \cong G'$ จะได้ว่า

1. *G เป็นกรุปอาบีเลียน ก็ต่อเมื่อ G' เป็นกรุปอาบีเลียน*
2. *G เป็นกรุปวัฏจักร ก็ต่อเมื่อ G' เป็นกรุปวัฏจักร*
3. *G มีกรุปย่อยอันดับ n ก็ต่อเมื่อ G' มีกรุปย่อยอันดับ n*
4. *G มีสมาชิกอันดับ n ก็ต่อเมื่อ G' มีสมาชิกอันดับ n*
5. *ทุกสมาชิกของ G เป็นอันดับจำกัด ก็ต่อเมื่อ ทุกสมาชิกของ G' เป็นอันดับจำกัด*

ทฤษฎีบท

ให้ G_1, G_1' และ G_2, G_2' เป็นกรุป

$$\text{ถ้า} \quad G_1 \cong G_1' \quad \text{และ} \quad G_2 \cong G_2' \quad \text{แล้ว} \quad G_1 \times G_2 \cong G_1' \times G_2'$$

ทฤษฎีบทเคย์เลย์ (Cayley's Theorem)

บทตั้ง

ให้ G เป็นกรุป และ $a \in G$ กำหนดให้ $T_a : G \to G$ นิยามโดย

$$T_a(x) = ax \qquad \text{ทุก ๆ } x \in G$$

แล้ว T_a เป็นการเรียงสับเปลี่ยนของ G หรือ $T_a \in S_G$

ทฤษฎีบท

ทฤษฎีบทเคย์เลย์ (Cayley's Theorem)

ให้ G เป็นกรุป แล้ว

G สมสัณฐานกับกรุปย่อยของกรุปสมมาตรบนเซต G

บทแทรก

ให้ G เป็นกรุปจำกัดที่มีอันดับเท่ากับ n แล้วจะได้ว่ามี $H \leq S_n$ ซึ่ง $G \cong H$

ตัวอย่าง

จงหากรุปการเรียงสับเปลี่ยนที่สมสัณฐานกับ $\mathbb{Z}_3$ และเป็นกรุปย่อยของ S_3

5.3 ทฤษฎีบทสมสัณฐาน

ทฤษฎีบท

ทฤษฎีบทฟังก์ชันสมสัณฐานบทที่หนึ่ง (First Isomorphism Theorem)

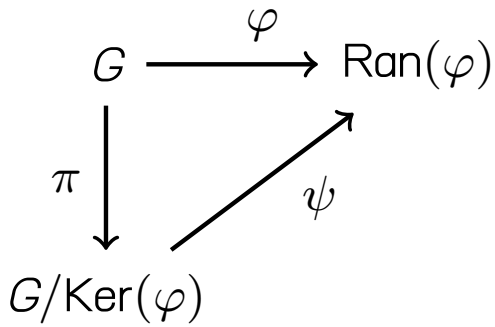
ให้ G และ G' เป็นกรุป โดยที่ $\varphi : G \to G'$ เป็นฟังก์ชันสาทิสสัณฐาน จะได้ว่า

$$G/Ker(\varphi) \cong Ran(\varphi)$$

ข้อสังเกต

ให้ G และ G' เป็นกรุป

1. ถ้า $\varphi : G \to G'$ เป็นฟังก์ชันสาทิสสัณฐานแบบทั่วถึง แล้ว $G/\mathrm{Ker}(\varphi) \cong G'$
2. $\psi \circ \pi = \varphi$ เมื่อ π เป็นฟังก์ชันสาทิสสัณฐานธรรมชาติ



ทฤษฎีบท

ให้ $n \in \mathbb{N}$ *แล้ว* $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

ตัวอย่าง

ให้ $\varphi : (\mathbb{R}, +) \to (\mathbb{C}^*, \cdot)$ นิยามโดย $\varphi(x) = \cos x + i \sin x$ เมื่อ $x \in \mathbb{R}$

จงแสดงว่า $\mathbb{R}/\langle 2\pi \rangle \cong \{\cos x + i \sin x : x \in \mathbb{R}\}$

ตัวอย่าง

ให้ $\varphi : (\mathbb{R}^2, +) \to (\mathbb{R}, +)$ นิยามโดย $\varphi((x, y)) = x + y$ เมื่อ $x, y \in \mathbb{R}$

จงแสดงว่า $\mathbb{R}^2/\{(x, -x) : x \in \mathbb{R}\} \cong \mathbb{R}$

ทฤษฎีบท

ให้ G เป็นกรุป และ $K \trianglelefteq G$ แล้วจะได้ว่า

$$\text{มีกรุป } G' \text{ และ } f : G \to G' \text{ เป็นฟังก์ชันสาทิสสัณฐาน ซึ่ง } Ker(f) = K$$

ทฤษฎีบทฟังก์ชันสมสัณฐานบทที่สอง (Second Isomorphism Theorem)

ทฤษฎีบท

ให้ G เป็นกรุป โดยที่ $H \leq G$ และ $K \trianglelefteq G$ จะได้ว่า

$$H/H \cap K \cong HK/K$$

ทฤษฎีบทฟังก์ชันสมสัณฐานบทที่สาม (Third Isomorphism Theorem)

ทฤษฎีบท

ให้ G เป็นกรุป โดยที่ $H \trianglelefteq G$, $K \trianglelefteq G$ และ $K \subseteq H$ จะได้ว่า

$$H/K \trianglelefteq G/K \qquad \text{และ} \qquad (G/K)/(H/K) \cong G/H$$

5.4 ฟังก์ชันอัตสัณฐาน

บทนิยาม

ให้ G เป็นกรุป ถ้า $\varphi : G \to G$ เป็นฟังก์ชันสมสัณฐาน

จะเรียก φ ว่าเป็น **ฟังก์ชันอัตสัณฐาน (automorphism)** ของ G เซตของฟังก์ชันอัตสัณฐานของ G เขียนแทนด้วย $\mathrm{Aut}(G)$ นั่นคือ

$$\mathrm{Aut}(G) = \{\varphi : G \to G : \varphi \text{ เป็นฟังก์ชันสมสัณฐาน } \}$$

เห็นได้ชัดว่าฟังก์ชันเอกลักษณ์ i_G เป็นฟังก์ชันหนึ่งต่อหนึ่งทั่วถึง และสำหรับ $x, y \in G$ จะได้ว่า

$$i_G(xy) = xy = i_G(x)i_G(y)$$

ดังนั้น i_G เป็นฟังก์ชันอัตสัณฐานของ G

ตัวอย่าง

ให้ G เป็นกรุปอาบีเลียน และ

$$\varphi : G \to G \quad \text{นิยามโดย} \quad \varphi(x) = x^{-1}$$

จงแสดงว่า φ ฟังก์ชันอัตสัณฐานของ G

ทฤษฎีบท

ให้ G เป็นกรุปวัฏจักร โดยที่ a และ b เป็นตัวก่อกำเนิดของ G กำหนดให้

$$\varphi : G \to G \quad \textit{นิยามโดย} \quad \varphi(a^k) = b^k \quad \textit{เมื่อ } k \in \mathbb{Z}$$

แล้ว φ เป็นฟังก์ชันอัตสัณฐานของ G

ทฤษฎีบท

ให้ G เป็นกรุป แล้ว $(Aut(G), \circ)$ เป็นกรุป

ทฤษฎีบท

ให้ G เป็นกรุป และ $a \in G$ กำหนดให้

$$f_a : G \to G \quad \text{นิยามโดย} \quad f_a(x) = a^{-1}xa$$

แล้ว f_a เป็นฟังก์ชันอัตสัณฐานของ G

บทนิยาม

ให้ G เป็นกรุป และ $a \in G$ จะเรียก f_a ในทฤษฎีบท 0.39 ว่า **ฟังก์ชันอัตสัณฐานภายใน (inner automorphism)** ของ G ซึ่งสมนัยกับ a และเซตของฟังก์ชันอัตสัณฐานภายในของ G เขียนแทนด้วย $\mathrm{Inn}(G)$ นั่นคือ

$$\mathrm{Inn}(G) = \{f_a \in \mathrm{Aut}(G) \,:\, a \in G\}$$

ข้อสังเกต

ถ้า G เป็นกรุปอาบีเลียน จะได้ว่า f_a คือ i_G สำหรับทุก ๆ $a \in G$

ตัวอย่าง

จงหา $f_a(x) \in \mathrm{Inn}(S_3)$ เมื่อ $a = (1\,2)$

ทฤษฎีบท

ให้ G เป็นกรุป จะได้ว่า

$$G/Z(G) \cong Inn(G) \qquad \text{และ} \qquad Inn(G) \trianglelefteq Aut(G)$$

เมื่อ $Z(G) = \{a \in G : ax = xa \ \text{ทุก ๆ } x \in G\}$

บทที่ 6 ริง

6.1 ริงและฟิลด์

บทนิยาม

ให้ R เป็นเซตที่ไม่ใช่เซตว่าง โดยที่ $+$ และ $\cdot$ เป็นการดำเนินการทวิภาคใน R จะเรียกว่า **ริง (ring)** เขียนแทนด้วย $(R,+,\cdot)$ ถ้าสอดคล้อง 3 ข้อต่อไปนี้

(ก) $(R,+)$ เป็นกรุปอาบีเลียน

(ข) $(R,\cdot)$ เป็นกึ่งกรุป

(ค) สำหรับ $a,b,c \in R$ จะได้ว่า

$$a\cdot(b+c) = a\cdot b + a\cdot c \qquad \text{และ} \qquad (b+c)\cdot a = b\cdot a + c\cdot a$$

เรียกว่า **สมบัติการแจกแจง (distributive law)** ใน R

เขียน R แทนริง $(R,+,\cdot)$ และ $a\cdot b$ เขียนแทนด้วย ab

ถ้า $(R+,\cdot)$ เป็นริง แล้ว

1. เอกลักษณ์ใน $(R,+)$ เขียนแทนด้วย 0 เรียกว่า **ศูนย์ (zero element)** และสำหรับ $a \in R$ เขียนตัวผกผันของ a ด้วย $-a$
2. ถ้ากึ่งกรุป $(R,\cdot)$ มีเอกลักษณ์ เขียนแทนด้วย 1 เรียกว่า **ยูนิตี (unity)** และเรียก $(R,+,\cdot)$ ว่า **ริงซึ่งมียูนิตี (ring with unity)**
3. ถ้ากึ่งกรุป $(R,\cdot)$ มีสมบัติการสลับที่ เรียก $(R,+,\cdot)$ ว่า **ริงสลับที่ (commutative ring)**

ข้อสังเกต

ถ้าริง $(R,+,\cdot)$ มีสมาชิกเพียงตัวเดียว จะได้ว่า $R=\{0\}$ และศูนย์ทำหน้าที่เป็นยูนิตี นั่นคือ $0=1$ โดยเรียก $(\{0\},+,\cdot)$ ว่า **ริงชัด (trivial ring)**

จากความรู้เรื่องกรุปถ้า $+$ เป็นการบวก และ $\cdot$ เป็นการคูณ จะได้ว่า

1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ และ $(\mathbb{C}, +, \cdot)$ เป็นริงสลับที่ซึ่งมียูนิตีคือ 1
2. สำหรับ $n \in \mathbb{N}$ จะได้ว่า $(\mathbb{Z}_n, +, \cdot)$ เป็นริงสลับที่ซึ่งมียูนิตีคือ $\bar{1}$
3. สำหรับ $n \in \mathbb{N}$ จะได้ว่า $(M_{nn}(\mathbb{R}), +, \cdot)$ เป็นริงที่ไม่สลับที่ซึ่งมียูนิตีคือ I

ตัวอย่าง

กำหนดให้

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}$$

จงแสดงว่า $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ เป็นริงสลับที่ซึ่งมียูนิตี

ตัวอย่าง

ให้ $a, b \in \mathbb{R}$ นิยามโดย

$$a \oplus b = a + b + 1$$

$$a \odot b = a + b + ab$$

จงแสดงว่า $(\mathbb{R}, \oplus, \odot)$ เป็นริงสลับที่ซึ่งมียูนิตี

ตัวอย่าง

ให้ $a, b, c, d \in \mathbb{R}$ นิยามโดย

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

$$(a, b) \odot (c, d) = (a \cdot c, b \cdot d)$$

จงแสดงว่า $(\mathbb{R}^2, \oplus, \odot)$ เป็นริงสลับที่ซึ่งมียูนิตี

ทฤษฎีบท

ให้ R และ S เป็นริง จะได้ว่า $R \times S$ เป็นริง เมื่อนิยาม $+$ และ $\cdot$ ดังสมการ (??) และ (??) ตามลำดับ และเรียกริง $R \times S$ ว่า ***ผลคูณตรงของริง (direct product of ring)***

บทแทรก

ให้ R และ S เป็นริงซึ่งมียูนิตี จะได้ว่า $R \times S$ เป็นริงซึ่งมียูนิตี

ทฤษฎีบท

ให้ R เป็นริง และ $a, b \in R$ จะได้ว่า

1. $a0 = 0a = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$

บทแทรก

ให้ R เป็นริงซึ่งมียูนิตี และ $a \in R$ จะได้ว่า

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

บทแทรก

ถ้า R เป็นริงซึ่งมียูนิตี และ $R \neq \{0\}$ แล้ว $0 \neq 1$

บทนิยาม

ให้ $(R,+,\cdot)$ เป็นริง โดยที่ $x \in R$ และ $n \in \mathbb{N}$ กำหนดให้

1. $nx = x + (n-1)x$
2. $0x = 0$ เมื่อ 0 ทางขวามือเป็นเอกลักษณ์ใน $(R,+)$ และ 0 ทางซ้ายมือเป็นจำนวนเต็ม
3. $(-n)x = n(-x)$
4. $x^0 = 1$ เมื่อ $0 \in \mathbb{Z}$ และ 1 เป็นเอกลักษณ์ใน $(R,\cdot)$ โดยที่ x ไม่เป็นเอกลักษณ์ใน $(R,+)$
5. $x^n = xx^{n-1}$ เมื่อ x ไม่เป็นเอกลักษณ์ใน $(R,+)$

ทฤษฎีบท

ให้ $(R,+,\cdot)$ *เป็นริง โดยที่* $x,y\in R$ *และ* $n,m\in\mathbb{Z}$ *จะได้ว่า*

1. $-(nx)=n(-x)$
2. $nx+mx=(n+m)x$
3. $n(x+y)=nx+ny$
4. $n(xy)=(nx)y=x(ny)$
5. $(nx)(my)=(nm)xy$
6. $(xy)^n=x^ny^n$ *เมื่อ* xy *ไม่เป็นเอกลักษณ์ใน* $(R,+)$

บทนิยาม

ให้ R เป็นริง ถ้ามี $k \in \mathbb{N}$ ซึ่ง $ka = 0$ ทุก $a \in R$ และ

$$n = \min\{k \in \mathbb{N} : ka = 0 \text{ ทุก ๆ } a \in R\}$$

เรากล่าวว่า R มี **แคแรกเทอริสติก (characteristic)** เท่ากับ n เขียนแทนด้วย $\text{Char}(R)$

ถ้าไม่มี $k \in \mathbb{N}$ ซึ่ง $ka = 0$ ทุก $a \in R$ จะกล่าวว่า R มีแคแรกเทอริสติกเท่ากับ 0

ข้อสังเกต

จะได้ว่า $\text{Char}(R) > 0$ ก็ต่อเมื่อ $\min\{k \in \mathbb{N} : ka = 0 \text{ ทุก ๆ } a \in R\} \neq \varnothing$

ตัวอย่าง

จงหาแคแรกเทอริสติกของ $\mathbb{Z}_6$

ทฤษฎีบท

ให้ R เป็นริงซึ่งมียูนิตี และ $Char(R) = n$ จะได้ว่า

$$n > 0 \qquad \textit{ก็ต่อเมื่อ} \qquad \{k \in \mathbb{N} : k1 = 0\} \neq \varnothing$$

บทแทรก

ให้ R เป็นริงซึ่งมียูนิตี และ $\mathrm{Char}(R) > 0$ จะได้ว่า

$$\mathrm{Char}(R) = \{k \in \mathbb{N} : k1 = 0\}$$

บทนิยาม

ให้ R เป็นริงซึ่งมียูนิตี และ $a \in R$ จะเรียก a ว่า **หน่วย (unit)** ถ้า

$$\text{มี } b \in R \quad \text{ซึ่ง} \quad ab = 1 = ba$$

หรือกล่าวได้ว่า a เป็นหน่วย ก็ต่อเมื่อ a มีตัวผกผันในกึ่งกรุป $(R, \cdot)$

และเซตของหน่วยของ R เขียนแทนด้วย $\mathcal{U}(R)$ นั่นคือ

$$\mathcal{U}(R) = \{a \in R : \text{ มี } b \in R \text{ ซึ่ง } ab = 1 = ba\}$$

ตัวอย่าง

จงหา $\mathcal{U}(R)$ ของริงต่อไปนี้

1. $\mathbb{Z}_6$
2. $\mathbb{Z}_7$

ทฤษฎีบท

ให้ $a, b \in \mathbb{Z}$ *จะได้ว่า*

$$a + b\sqrt{2} \quad \text{เป็นหน่วยใน} \quad \mathbb{Z}[\sqrt{2}] \quad \text{ก็ต่อเมื่อ} \quad a^2 - 2b^2 = \pm 1$$

ทฤษฎีบท

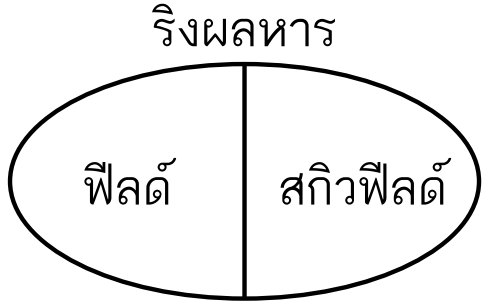
ให้ R *และ* S *เป็นริงซึ่งมียูนิตี ถ้า* R *และ* S *มีหน่วย แล้ว* $R \times S$ *มีหน่วย*

บทนิยาม

ให้ R เป็นริงซึ่งมียูนิตี โดยที่ $1 \neq 0$ แล้วเรียก R ว่า

1. **ริงผลหาร (division ring)** ถ้าทุกสมาชิกที่ไม่ใช่ศูนย์ใน R เป็นหน่วย
2. **ฟิลด์ (field)** ถ้า R เป็นริงผลหารสลับที่ (commutative division ring)
3. **สกิวฟิลด์ (skew field)** ถ้า R เป็นริงผลหารไม่สลับที่

จากบทนิยามข้างต้นแสดงความสัมพันธ์ได้ดังต่อไปนี้



6.2 ริงย่อย ไอดีล และริงผลการ

บทนิยาม

ให้ $(R,+,\cdot)$ เป็นริง และ $S \subseteq R$ ถ้า $(S,+,\cdot)$ เป็นริง จะเรียก S ว่า **ริงย่อย (subring)** ของ R

$(\mathbb{Z},+,\cdot)$ เป็นริงย่อยของ $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ และ $(\mathbb{C},+,\cdot)$

$(\mathbb{Q},+,\cdot)$ เป็นริงย่อยของ $(\mathbb{R},+,\cdot)$ และ $(\mathbb{C},+,\cdot)$

$(\mathbb{R},+,\cdot)$ เป็นริงย่อยของ $(\mathbb{C},+,\cdot)$

$(n\mathbb{Z},+,\cdot)$ เป็นริงย่อยของ $(\mathbb{Z},+,\cdot)$ เมื่อ $n \in \mathbb{N}$

ตัวอย่าง

จงหาริงย่อยทั้งหมดของ $(\mathbb{Z}_6,+,\cdot)$

เกณฑ์การพิจารณาริงย่อย (Subring Criterion

ทฤษฎีบท

ให้ $(R,+,\cdot)$ *เป็นริง และ* $S \subseteq R$ *โดยที่* $S \neq \varnothing$ *ข้อความต่อไปนี้สมมูลกัน*

1. $(S,+,\cdot)$ *เป็นริงย่อยของ* $(R,+,\cdot)$
2. $(S,+)$ *เป็นกรุปย่อยของ* $(R,+)$ *และ* $ab \in S \quad$ *ทุก ๆ* $a,b \in S$
3. $a-b \in S$ *และ* $ab \in S \quad$ *ทุก ๆ* $a,b \in S$

ตัวอย่าง

จงตรวจสอบว่าเซตต่อไปนี้เป็นริงย่อยของ $M_{22}(\mathbb{R})$ หรือไม่

1. $S = \left\{ \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} : x, y \in \mathbb{R} \right\}$
2. $T = \left\{ \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} : x \in \mathbb{R} \right\}$

ตัวอย่าง

จงตรวจสอบว่า S เป็นริงย่อยของ $\mathbb{Z} \times \mathbb{Z}$ หรือไม่

1. $S = \{(x, x) : x \in \mathbb{Z}\}$
2. $T = \{(x, 0) : x \in \mathbb{Z}\}$
3. $U = \{(x, 1) : x \in \mathbb{Z}\}$

ทฤษฎีบท

ให้ S_1 และ S_2 เป็นริงย่อยของ R จะได้ว่า $S_1 \cap S_2$ เป็นริงย่อยของ R

บทนิยาม

ให้ $(R, +, \cdot)$ เป็นริง และ $(I, +)$ เป็นกรุปย่อยของ $(R, +)$ แล้ว

1. เรียก I ว่า **ไอดีลซ้าย (left ideal)** ของ R ถ้า $RI \subseteq I$
2. เรียก I ว่า **ไอดีลขวา (right ideal)** ของ R ถ้า $IR \subseteq I$
3. เรียก I ว่า **ไอดีล (ideal)** ของ R ถ้า $RI \subseteq I$ และ $IR \subseteq I$

ข้อสังเกต

สำหรับริง R ใด ๆ จะได้ว่า $\{0\}$ และ R เป็นไอดีลของ R

ทฤษฎีบท

ไอดีลซ้าย ไอดีลขวา และไอดีล ของริง R ย่อมเป็นริงย่อยของ R

ทฤษฎีบท

ให้ R เป็นริงซึ่งมี 1 และ I เป็นไอดีลของ R จะได้ว่า

$$\text{ถ้า} \quad 1 \in I \quad \text{แล้ว} \quad I = R$$

ตัวอย่าง

จงหาไอดีลของ $\mathbb{Z}_6$

ตัวอย่าง

จงแสดงว่า $n\mathbb{Z}$ เป็นไอดีลของ $\mathbb{Z}$ เมื่อ $n \in \mathbb{N}$

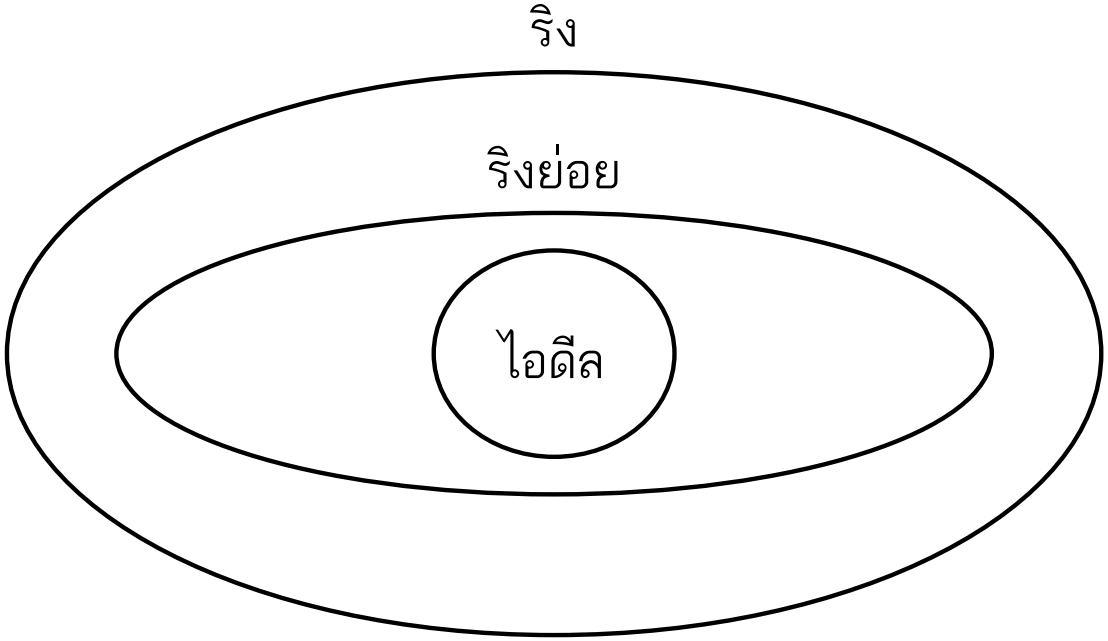
ข้อสังเกต

ให้ R เป็นริงสลับที่ จะได้ว่า

1. ถ้า I เป็นไอดีลซ้ายของ R แล้ว I เป็นไอดีลขวา และไอดีลของ R
2. ถ้า I เป็นไอดีลขวาของ R แล้ว I เป็นไอดีลซ้าย และไอดีลของ R

ตัวอย่าง

จงแสดงว่า $I = \{(x, 0) : x \in \mathbb{Z}\}$ เป็นไอดีลของ $\mathbb{Z} \times \mathbb{Z}$



ทฤษฎีบท

ให้ I และ J เป็นไอดีลซ้าย (ไอดีลขวา, ไอดีล) ของ R แล้ว

$$I \cap J \text{ เป็นไอดีลซ้าย (ไอดีลขวา, ไอดีล) ของ } R$$

ทฤษฎีบท

ให้ R เป็นริง และ $a \in R$ จะได้ว่า

$$Ra \text{ เป็นไอดีลซ้าย และ } aR \text{ เป็นไอดีลขวาของ } R$$

ทฤษฎีบท

ให้ R เป็นริงสลับที่และมียูนิตี และ $a \in R$ จะได้ว่า

$$Ra \text{ เป็นไอดีลที่มี } a \text{ เป็นสมาชิก}$$

บทนิยาม

ให้ R เป็นริงสลับที่และมียูนิตี และ $a \in R$ จะเรียก

$$Ra = \{ra : r \in R\}$$

ว่า **ไอดีลมุขสำคัญ (principal ideal)** เขียนแทนด้วย $\langle a \rangle$

ตัวอย่าง

จงแจกแจงสมาชิกของไอดีลมุขสำคัญใน $\mathbb{Z}_6$

1. $\langle \bar{1} \rangle$
2. $\langle \bar{2} \rangle$
3. $\langle \bar{3} \rangle$

ข้อสังเกต

ทุกไอดีลในริง $\mathbb{Z}$ และ $\mathbb{Z}_n$ เป็นไอดีลมุขสำคัญ เมื่อ $n \in \mathbb{N}$

ทฤษฎีบท

ให้ I และ J เป็นไอดีลซ้าย (ไอดีลขวา, ไอดีล) ของ R และ S ตามลำดับ แล้ว

$$I \times J \text{ เป็นไอดีลซ้าย (ไอดีลขวา, ไอดีล) ของ } R \times S$$

ตัวอย่าง

จงหาไอดีลทั้งหมดของ $\mathbb{Z}_2 \times \mathbb{Z}_6$

ทฤษฎีบท

ให้ R เป็นริงสลับที่ซึ่งมียูนิตี และ $R \neq \{0\}$ จะได้ว่า

$$R \text{ เป็นฟิลด์} \quad \text{ก็ต่อเมื่อ} \quad R \text{ มีเพียง 2 ไอดีลเท่านั้นคือ } R \text{ และ } \{0\}$$

ทฤษฎีบท

ให้ I เป็นไอดีลของริง R และ $R/I = \{I + a : a \in R\}$ กำหนดให้

$$(I + a) + (I + b) = I + (a + b)$$

$$(I + a) \cdot (I + b) = I + (ab)$$

แล้ว $(R/I, +, \cdot)$ เป็นริง และเรียกว่า ***ริงผลหาร (quotient ring)***

ข้อสังเกต

ถ้า R เป็นริงสลับที่ซึ่งมียูนิตี และ I เป็นไอดีลของ R จะได้ว่า R/I เป็นริงสลับที่ซึ่งมียูนิตี โดยที่

$$I \quad \text{เป็นศูนย์} \quad \text{และ} \quad I+1 \quad \text{เป็นยูนิตี ในริงผลหาร } R/I$$

ทฤษฎีบท

ให้ I, J เป็นไอดีลของริง R โดยที่ I เป็นเซตย่อยของ J จะได้ว่า

$$J/I = \{I\} \quad \textit{ก็ต่อเมื่อ} \quad J = I$$

ทฤษฎีบท

ให้ I, J, K เป็นไอดีลของริง R โดยที่ I เป็นเซตย่อยของ J และ K จะได้ว่า

$$K/I = J/I \quad \textit{ก็ต่อเมื่อ} \quad K = J$$

6.3 ฟังก์ชันสาทิสสัณฐานของริง

บทนิยาม

ให้ $(R, +, \cdot)$ และ $(S, \oplus, \odot)$ เป็นริง และ $\varphi : R \to S$

1. เรียก φ ว่า **ฟังก์ชันสาทิสสัณฐานของริง (ring homomorphism)** ถ้าทุก ๆ $a, b \in R$ สอดคล้อง 2 เงื่อนไขต่อไปนี้

$$\varphi(a + b) = \varphi(a) \oplus \varphi(b)$$
$$\varphi(a \cdot b) = \varphi(a) \odot \varphi(b)$$

2. เรียก φ ว่า **ฟังก์ชันสมสัณฐานของริง (ring isomorphism)** ถ้า φ เป็นฟังก์ชันสาทิสสัณฐานของริงซึ่งเป็นฟังก์ชันหนึ่งต่อหนึ่งทั่วถึง และกล่าวว่า R **สมสัณฐาน (isomorphic)** กับ S เขียนแทนด้วย $R \cong S$

3. **เคอร์เนล (Kernel)** ของ φ เขียนแทนด้วย $\text{Ker}(\varphi)$ นิยามโดย $\text{Ker}(\varphi) = \{x \in R : \varphi(x) = 0_S\}$ เมื่อ 0_S เป็นศูนย์ใน S

สำหรับริง $(R, +, \cdot)$ และ $(S, \oplus, \odot)$ ถ้า $\varphi : R \to S$ เป็นฟังก์ชันสาทิสสัณฐานของริง จะได้ว่า $\varphi : (R, +) \to (S, \oplus)$ เป็นฟังก์ชันสาทิสสัณฐาน เพราะว่า $(R, +)$ และ $(S, \oplus)$ เป็นกรุปอาบีเลียน จากสมบัติของฟังก์ชันสาทิสสัณฐาน ทำให้ได้ว่า

1. $\varphi(0_R) = 0_S$ เมื่อ 0_R และ 0_S เป็นศูนย์ใน R และ S ตามลำดับ
2. $\varphi(-x) = -\varphi(x)$ ทุก ๆ $x \in R$

ตัวอย่าง

จงแสดงว่า φ เป็นฟังก์ชันสาทิสสัณฐานของริง และหา $\mathrm{Ker}(\varphi)$

1. กำหนดให้ $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ นิยามโดย $\varphi(x) = \bar{x}$ เมื่อ $n \in \mathbb{N}$
2. กำหนดให้ $\varphi : \mathbb{C} \to \mathbb{C}$ นิยามโดย $\varphi(x + yi) = x - yi$ เมื่อ $x, y \in \mathbb{R}$

ตัวอย่าง

จงตรวจสอบว่า φ เป็นฟังก์ชันสาทิสสัณฐานของริงหรือไม่

1. กำหนดให้ $\varphi : \mathbb{Z} \to \mathbb{Z}_2$ นิยามโดย $\varphi(x) = (\bar{x})^2$
2. กำหนดให้ $\varphi : \mathbb{Z} \to \mathbb{Z}_3$ นิยามโดย $\varphi(x) = (\bar{x})^2$

ทฤษฎีบท

ให้ R และ S เป็นริง และ φ เป็นฟังก์ชันสมสัณฐานของริงจาก R ไป S จะได้ว่า

$$\varphi \text{ เป็นฟังก์ชัน 1-1} \quad \text{ก็ต่อเมื่อ} \quad Ker(\varphi) = \{0_R\}$$

ตัวอย่าง

ให้ $\varphi : \mathbb{R} \to M_{22}(\mathbb{R})$ นิยามโดย

$$\varphi(a) = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$$

จงแสดงว่า φ เป็นฟังก์ชันสาทิสสัณฐานของริงแบบ 1-1

ข้อสังเกต

ให้ R และ S เป็นริง และ φ เป็นฟังก์ชันสาทิสสัณฐานของริงจาก R ไป S

ถ้า φ เป็นฟังก์ชัน 1-1 แล้ว $R \cong Ran(\varphi)$

ตัวอย่าง

ให้ $S = \{(x, x) : x \in \mathbb{Z}\}$ เป็นริงย่อยของ $\mathbb{Z}$ จงแสดงว่า $S \cong \mathbb{Z}$

ทฤษฎีบท

ให้ R และ S เป็นริง และ φ เป็นฟังก์ชันสาทิสสัณฐานของริงจาก R ไป S จะได้ว่า

1. *$Ker(\varphi)$ เป็นริงย่อยของ R*
2. *$Ran(\varphi)$ เป็นริงย่อยของ S*
3. *$Ker(\varphi)$ เป็นไอดีลของ R*
4. *ถ้า R มียูนิตีคือ 1_R แล้ว $\varphi(1_R)$ เป็นยูนิตีใน $Ran(\varphi)$*

ทฤษฎีบท

ให้ I เป็นไอดีลของริง R กำหนดให้

$$\pi : R \to R/I \quad \text{นิยามโดย} \quad \pi(a) = I + a$$

ทฤษฎีบท

ทฤษฎีบทฟังก์ชันสมสัณฐานของริงบทที่หนึ่ง

ให้ R และ S เป็นริง โดยที่ $\varphi : R \to S$ เป็นฟังก์ชันสาทิสสัณฐานของริง จะได้ว่า

$$R/Ker(\varphi) \cong Ran(\varphi)$$

ข้อสังเกต

ให้ R และ S เป็นริง

1. ถ้า $\varphi : R \to S$ เป็นฟังก์ชันสาทิสสัณฐานของริงแบบทั่วถึง แล้ว $R/\mathrm{Ker}(\varphi) \cong S$
2. $\psi \circ \pi = \varphi$ เมื่อ π เป็นฟังก์ชันสาทิสสัณฐานของริงธรรมชาติ

ตัวอย่าง

จงแสดงว่า $\mathbb{Z}/\langle n\rangle \cong \mathbb{Z}_n$

ทฤษฎีบท

ทฤษฎีบทฟังก์ชันสมสัณฐานของริงบทที่สอง

ให้ A เป็นริงย่อยของ R และ B เป็นไอดีลของ R แล้ว $A+B=\{a+b : a\in A \text{ และ } b\in B\}$ เป็นริงย่อยของ R และ $A\cap B$ เป็นไอดีลของ A และ

$$(A+B)/B \cong A/(A\cap B)$$

บทที่ 7 อินทิกรัลโดเมน

7.1 ตัวหารศูนย์และอินทิกรัลโดเมน

บทนิยาม

ให้ R เป็นริงสลับที่ และ a เป็นสมาชิกที่ไม่ใช่ศูนย์ใน R แล้ว

เรียก a ว่า **ตัวหารศูนย์ (zero divisor)** ถ้ามี b ซึ่งเป็น สมาชิกที่ไม่ใช่ศูนย์ใน R ที่ทำให้ $ab = 0$

ข้อสังเกต

ถ้า R เป็นริงสลับที่ซึ่งไม่มีตัวหารศูนย์ แล้วทุก ๆ ริงย่อยของ R ไม่มีตัวหารศูนย์

สำหรับ $a, b \in \mathbb{C}$ โดยสมบัติของจำนวนเชิงซ้อนจะได้ว่า

$$a \neq 0 \quad \text{และ} \quad b \neq 0 \quad \text{ก็ต่อเมื่อ} \quad ab \neq 0$$

ตัวอย่าง

จงหาตัวหารศูนย์ทั้งหมดของ $\mathbb{Z}_6$

ทฤษฎีบท

ให้ $a \in \{1, 2, 3, ..., n-1\}$ *เมื่อ* $n \in \mathbb{N}$ *จะได้ว่า*

$$\bar{a} \text{ เป็นตัวหารศูนย์ใน } \mathbb{Z}_n \qquad \text{ก็ต่อเมื่อ} \qquad gcd(a, n) \neq 1$$

ตัวอย่าง

จงหาตัวหารศูนย์ทั้งหมดของริงต่อไปนี้

1. $\mathbb{Z}_{12}$
2. $\mathbb{Z}_{18}$
3. $\mathbb{Z}_{20}$

บทแทรก

จำนวนตัวหารศูนย์ของ $\mathbb{Z}_n$ เท่ากับ $(n-1)-\phi(n)$ เมื่อ $n \in \mathbb{N}$ ซึ่ง $n > 1$

ตัวอย่าง

จงหาจำนวนตัวหารศูนย์ทั้งหมดของริงต่อไปนี้

1. $\mathbb{Z}_{15}$
2. $\mathbb{Z}_{23}$
3. $\mathbb{Z}_{36}$
4. $\mathbb{Z}_{100}$

บทแทรก

ถ้า p เป็นจำนวนเฉพาะ แล้ว $\mathbb{Z}_p$ ไม่มีตัวหารศูนย์

ทฤษฎีบท

ให้ R และ S เป็นริงสลับที่ จะได้ว่า

ถ้า a หรือ b เป็นตัวหารศูนย์ของ R และ S ตามลำดับ แล้ว (a,b) เป็นตัวหารศูนย์ของ $R \times S$

ทฤษฎีบท

ให้ R และ S เป็นริงสลับที่ ให้ $a \in R - \{0\}$ และ $b \in S - \{0\}$ จะได้ว่า

ถ้า (a,b) เป็นตัวหารศูนย์ของ $R \times S$ แล้ว a หรือ b เป็นตัวหารศูนย์ของ R และ S ตามลำดับ

ตัวอย่าง

จงหาตัวหารศูนย์ของ $\mathbb{Z}_3 \times \mathbb{Z}_4$

อินทิกรัลโดเมน (integral domain

บทนิยาม

จะเรียกริงสลับที่ซึ่งไม่มีตัวหารศูนย์ว่า **อินทิกรัลโดเมน (integral domain)**

จากบทนิยามข้างต้น ให้ R เป็นริงสลับที่จะได้ว่า

$$R \text{ เป็นอินทิกรัลโดเมน} \quad \text{ก็ต่อเมื่อ} \quad ab \neq 0 \text{ ทุก ๆ } a, b \in R - \{0\}$$

หรือกล่าวอีกนัยได้ว่า R เป็นอินทิกรัลโดเมน ก็ต่อเมื่อ ทุก ๆ $a, b \in R$

$$\text{ถ้า} \quad ab = 0 \quad \text{แล้ว} \quad a = 0 \quad \text{หรือ} \quad b = 0$$

หรือกล่าวได้ว่า R เป็นอินทิกรัลโดเมน ก็ต่อเมื่อ ทุก ๆ $a, b \in R$

$$\text{ถ้า} \quad a \neq 0 \quad \text{และ} \quad b \neq 0 \quad \text{แล้ว} \quad ab \neq 0$$

เนื่องจาก $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ และ $\mathbb{C}$ ไม่มีตัวหารศูนย์ ดังนั้นริงดังกล่าวเป็นอินทิกรัลโดเมน

ตัวอย่าง

จงตรวจสอบว่าริงต่อไปนี้เป็นอินทิกรัลโดเมนหรือไม่

1. $\mathbb{Z}_5$
2. $\mathbb{Z}_6$
3. $\mathbb{Z}_7$
4. $\mathbb{Z}_8$

ทฤษฎีบท

$\mathbb{Z}_n$ เป็นอินทิกรัลโดเมน ก็ต่อเมื่อ n เป็นจำนวนเฉพาะ

ทฤษฎีบท

ให้ R เป็นริงสลับที่ จะได้ว่า

R เป็นอินทิกรัลโดเมน ก็ต่อเมื่อ R สอดคล้องเงื่อนไขการตัดออกภายใต้การคูณ

ทฤษฎีบท

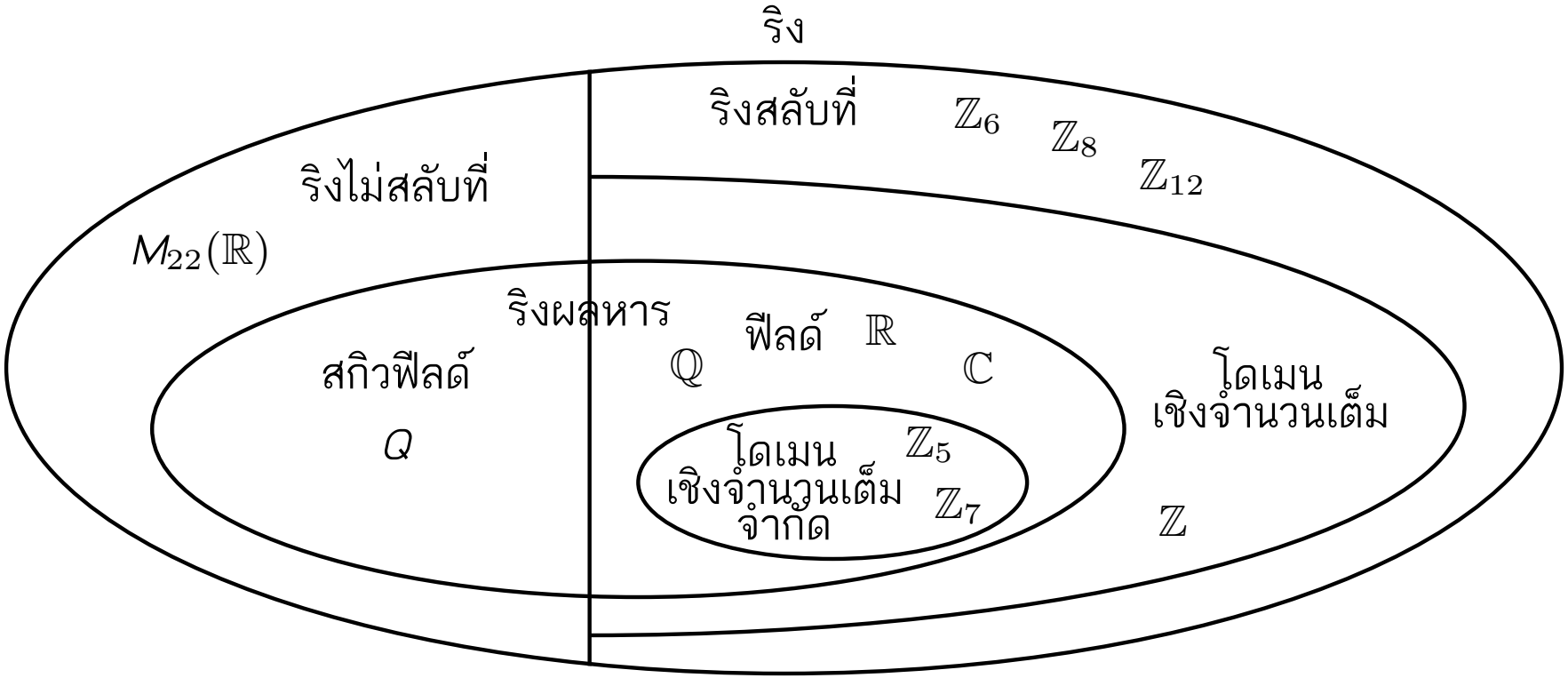
ฟิลด์เป็นอินทิกรัลโดเมน

ทฤษฎีบท

อินทิกรัลโดเมนที่มีสมาชิกจำกัดเป็นฟิลด์

บทแทรก

$\mathbb{Z}_n$ เป็นฟิลด์ ก็ต่อเมื่อ n เป็นจำนวนเฉพาะ


ริง
ริงสลับที่
$\mathbb{Z}_6$
$\mathbb{Z}_8$
$\mathbb{Z}_{12}$
ริงไม่สลับที่
$M_{22}(\mathbb{R})$
ริงผลหาร
ฟิลด์
$\mathbb{R}$
$\mathbb{Q}$
$\mathbb{C}$
สกิวฟิลด์
Q
โดเมน
เชิงจำนวนเต็ม
โดเมน
เชิงจำนวนเต็ม
จำกัด
$\mathbb{Z}_5$
$\mathbb{Z}_7$
$\mathbb{Z}$

7.2 ไอดีลใหญ่สุดและไอดีลเฉพาะ

บทนิยาม

ให้ M เป็นไอดีลของริง R โดยที่ $M \neq R$ จะกล่าวว่า M เป็น **ไอดีลใหญ่สุด (maximal ideal)** ของ R ก็ต่อเมื่อ

$$\text{ทุก ๆ ไอดีล } I \text{ ของ } R \text{ ถ้า } \quad M \subseteq I \subseteq R \quad \text{แล้ว} \quad I = M \quad \text{หรือ} \quad I = R$$

ตัวอย่าง

จงหาไอดีลใหญ่สุดของริงต่อไปนี้

1. $\mathbb{Z}_6$
2. $\mathbb{Z}_8$
3. $\mathbb{Z}_{12}$

ตัวอย่าง

จงตรวจสอบว่า $\langle 4 \rangle$ และ $\langle 5 \rangle$ เป็นไอดีลใหญ่สุดของ $\mathbb{Z}$ หรือไม่

ทฤษฎีบท

ให้ $p \in \mathbb{N}$ *จะได้ว่า*

$$\langle p \rangle \text{ เป็นไอดีลใหญ่สุดของ } \mathbb{Z} \quad \text{ก็ต่อเมื่อ} \quad p \text{ เป็นจำนวนเฉพาะ}$$

บทแทรก

สำหรับริง $\mathbb{Z}$ จะได้ว่า

$$\text{ถ้า} \quad M \text{ เป็นไอดีลใหญ่สุดของ } \mathbb{Z} \quad \text{แล้ว} \quad M = \langle p \rangle \quad \text{เมื่อ } p \text{ เป็นจำนวนเฉพาะ}$$

ตัวอย่าง

จงหา $n \in \mathbb{N}$ ซึ่ง $100 < n < 110$ ที่ทำให้ $\langle n \rangle$ เป็นไอดีลใหญ่สุดของ $\mathbb{Z}$

บทตั้ง

ให้ I เป็นไอดีลของริง R และ $I \subseteq J \subseteq R$ จะได้ว่า

$$J \text{ เป็นไอดีลของ } R \quad \text{ก็ต่อเมื่อ} \quad J/I \text{ เป็นไอดีลของ } R/I$$

ทฤษฎีบท

ให้ R เป็นริงสลับที่ซึ่งมียูนิตี และ M เป็นไอดีลของ R โดยที่ $M \neq R$

$$M \text{ เป็นไอดีลใหญ่สุดของ } R \quad \text{ก็ต่อเมื่อ} \quad R/M \text{ เป็นฟิลด์}$$

ตัวอย่าง

จงหาไอดีลใหญ่สุดทั้งหมดของ $\mathbb{Z}_8$ โดยใช้ทฤษฎีบท

บทแทรก

ให้ $n \in \mathbb{N}$ จะได้ว่า

$$\mathbb{Z}/\langle n \rangle \text{ เป็นฟิลด์} \quad \text{ก็ต่อเมื่อ} \quad n \text{ เป็นจำนวนเฉพาะ}$$

ข้อสังเกต

ไอดีลใหญ่สุดของ $\mathbb{Z}_{p^n}$ มีเพียง $\langle \bar{p} \rangle$ เท่านั้น เมื่อ p เป็นจำนวนเฉพาะ และ $n \in \mathbb{N}$

ตัวอย่าง

จงหาไอดีลใหญ่สุดทั้งหมดของริงต่อไปนี้

1. $\mathbb{Z}_{81}$
2. $\mathbb{Z}_{50}$
3. $\mathbb{Z}_{144}$
4. $\mathbb{Z}_{3575}$

ตัวอย่าง

จงหาไอดีลใหญ่สุดทั้งหมดของ $\mathbb{Z}_2 \times \mathbb{Z}_6$

บทนิยาม

ให้ P เป็นไอดีลของริงสลับที่ R และ $P \neq R$ จะกล่าวว่า P เป็น **ไอดีลเฉพาะ (prime ideal)** ก็ต่อเมื่อ

$$\text{ทุก ๆ } a, b \in R \quad \text{ถ้า} \quad ab \in P \quad \text{แล้ว} \quad a \in P \quad \text{หรือ} \quad b \in P$$

หรือกล่าวได้อีกอย่างคือ

$$\text{ทุก ๆ } a, b \in R \quad \text{ถ้า} \quad a \notin P \quad \text{และ} \quad b \notin P \quad \text{แล้ว} \quad ab \notin P$$

ข้อสังเกต

$\{0\}$ เป็นไอดีลเฉพาะของอินทิกรัลโดเมน D เนื่องจากทุก ๆ $a, b \in D$

$$\text{ถ้า} \quad ab = 0 \quad \text{แล้ว} \quad b = 0 \quad \text{หรือ} \quad b = 0$$

ทฤษฎีบท

ฟิลด์มีไอดีลเฉพาะเพียงตัวเดียวคือ $\{0\}$

ตัวอย่าง

จงหาไอดีลเฉพาะทั้งหมดของ $\mathbb{Z}_6$

ตัวอย่าง

จงตรวจสอบว่า $\langle 2 \rangle$ และ $\langle 10 \rangle$ เป็นไอดีลเฉพาะของ $\mathbb{Z}$ หรือไม่

บทแทรก

ให้ R เป็นริงสลับที่ซึ่งมียูนิตี

ถ้า M เป็นไอดีลใหญ่สุดของ R แล้ว M เป็นไอดีลเฉพาะ

ตัวอย่าง

จงแสดงว่า $\langle 4 \rangle$ เป็นไอดีลใหญ่สุดแต่ไม่เป็นไอดีลเฉพาะของ $\langle 2 \rangle$

ตัวอย่าง

จงแสดงว่า $\mathbb{Z} \times \{0\}$ เป็นไอดีลเฉพาะแต่ไม่เป็นไอดีลใหญ่สุดของ $\mathbb{Z} \times \mathbb{Z}$

บทแทรก

ให้ R เป็นริงจำกัดสลับที่ซึ่งมียูนิตี จะได้ว่า

M เป็นไอดีลใหญ่สุดของ R ก็ต่อเมื่อ M เป็นไอดีลเฉพาะ

บทแทรก

ให้ $p \in \mathbb{N}$ จะได้ว่า

1. $\langle p \rangle$ เป็นไอดีลเฉพาะของ $\mathbb{Z}$ ก็ต่อเมื่อ p เป็นจำนวนเฉพาะ
2. ถ้า P เป็นไอดีลเฉพาะของ $\mathbb{Z}$ แล้ว $P = \langle p \rangle$ เมื่อ p เป็นจำนวนเฉพาะ

7.3 โดเมนแยกตัวประกอบได้อย่างเดียว

บทนิยาม

ให้ R เป็นริงสลับที่ซึ่งมียูนิตี และ $a, b \in R$

จะกล่าวว่า ***a* หาร *b* ลงตัว** (***a* divides *b***) เขียนแทนด้วย $a \mid b$ ก็ต่อเมื่อ

$$\text{มี} \quad c \in R \quad \text{ซึ่ง} \quad b = ac$$

ข้อสังเกต

ให้ R เป็นริงสลับที่ซึ่งมียูนิตี และ $a, b \in R$ โดยที่ $a \neq 0$ จะได้ว่า

1. $a \mid 0$, $1 \mid a$ และ $a \mid a$ เนื่องจาก $0 = 0a$ และ $a = 1a$
2. $a \mid b$ ก็ต่อเมื่อ มี $k \in R$ ซึ่ง $b = ak$ ก็ต่อเมื่อ $b \in \langle a \rangle$

จากบทนิยามกล่าวว่า a เป็นหน่วยในริง R ซึ่งมียูนิตี ก็ต่อเมื่อ

ลดทอนไม่ได้ (irreducible)

บทนิยาม

ให้ D เป็นอินทิกรัลโดเมนซึ่งมียูนิตี ให้ $r \in D - \{0\}$ และ r ไม่เป็นหน่วย
จะกล่าวว่า r **ลดทอนไม่ได้ (irreducible)** ก็ต่อเมื่อ

$$\text{ถ้า} \quad r = ab \quad \text{แล้ว} \quad a \quad \text{หรือ} \quad b \quad \text{เป็นหน่วย}$$

ถ้าเป็นอย่างอื่นเรียก r ว่า **ลดทอนได้ (reducible)** นั่นคือ r ลดทอนได้ ก็ต่อเมื่อ

$$r = ab \quad \text{โดยที่} \quad a \quad \text{และ} \quad b \quad \text{ไม่เป็นหน่วย}$$

ข้อสังเกต

เนื่องจากสมาชิกทุกตัวที่ไม่ใช่ศูนย์ในฟิลด์เป็นหน่วย ดังนั้นจะไม่กล่าวถึงลดทอนได้หรือไม่ได้ของสมาชิกในฟิลด์

ทฤษฎีบท

ให้ $a, b \in \mathbb{Z}$ *และ* $K \in \mathbb{Z}$ *โดยที่* $K > 0$ *จะได้ว่า*

$$a + b\sqrt{-K} \quad \text{เป็นหน่วยใน} \quad \mathbb{Z}[\sqrt{-K}] \quad \text{ก็ต่อเมื่อ} \quad a^2 + Kb^2 = 1$$

ตัวอย่าง

จงแสดงว่า 2 และ 3 ลดทอนไม่ได้ใน $\mathbb{Z}[\sqrt{-5}]$

ตัวอย่าง

จงแสดงว่า $1+\sqrt{-5}$ ลดทอนไม่ได้ใน $\mathbb{Z}[\sqrt{-5}]$

สมาชิกเฉพาะ (prime element)

บทนิยาม

ให้ D เป็นอินทิกรัลโดเมนซึ่งมียูนิตี ให้ $p \in D - \{0\}$ และ p ไม่เป็นหน่วย

จะกล่าวว่า p เป็น **สมาชิกเฉพาะ (prime element)** ของ D ก็ต่อเมื่อ

$$\text{ถ้า} \quad p \mid ab \quad \text{แล้ว} \quad p \mid a \quad \text{หรือ} \quad p \mid b$$

ทฤษฎีบท

ให้ D เป็นอินทิกรัลโดเมนซึ่งมียูนิตี จะได้ว่า

$$\text{ถ้า} \quad p \text{ เป็นสมาชิกเฉพาะของ } D \quad \text{แล้ว} \quad p \text{ ลดทอนไม่ได้}$$

ตัวอย่าง

จงแสดงว่า 3 ลดทอนไม่ได้ใน $\mathbb{Z}[\sqrt{-5}]$ แต่ไม่เป็นสมาชิกเฉพาะ

บทนิยาม

ให้ D เป็นอินทิกรัลโดเมนซึ่งมียูนิต

จะกล่าวว่า D เป็น **โดเมนซึ่งแยกตัวประกอบได้อย่างเดียว (Unique Factorization Domain)** เขียนสั้น ๆ ว่า U.F.D. ก็ต่อเมื่อ สำหรับ $d \in D - \{0\}$ และ d ไม่เป็นหน่วย สอดคล้อง 2 เงื่อนไขดังนี้

1. มี $p_1, p_2, ..., p_n \in D$ ซึ่งลดทอนไม่ได้ และ $d = p_1 p_2 ... p_n$
2. ถ้า $d = p_1 p_2 ... p_n = q_1 q_2 ... q_m$ เมื่อ $q_1, q_2, ..., q_m \in D$

   แล้ว $n = m$ และสำหรับ i จะมี j ซึ่ง $p_i = uq_j$ โดยที่ u เป็นหน่วย

   เมื่อ $i, j \in \{1, 2, ..., n\}$

ตัวอย่าง

จงแสดงว่า $\mathbb{Z}[\sqrt{-5}]$ ไม่เป็น U.F.D.

โดเมนไอดีลมุขสำคัญ (Principal Ideal Domain)

ทฤษฎีบท

สมาชิกซึ่งลดทอนไม่ได้ของ U.F.D. จะเป็นสมาชิกเฉพาะ

บทนิยาม

ให้ D อินทิกรัลโดเมนซึ่งมียูนิตี

จะกล่าวว่า D เป็น **โดเมนไอดีลมุขสำคัญ (Principal Ideal Domain)** เขียนแทนด้วย P.I.D. ก็ต่อเมื่อ ทุกไอดีลของ D เป็นไอดีลมุขสำคัญ

ทฤษฎีบท

สมาชิกลดทอนไม่ได้ใน P.I.D. จะเป็นสมาชิกเฉพาะ

บทแทรก

ให้ D เป็น P.I.D. โดยที่ p ลดทอนไม่ได้ใน D และ $a_1, a_2, ..., a_n \in D$

$$\text{ถ้า} \quad p \mid (a_1 a_2 ... a_n) \quad \text{แล้ว} \quad \text{มี} \ i \in \{1, 2, ..., n\} \quad \text{ซึ่ง} \quad p \mid a_i$$

ทฤษฎีบท

ให้ D เป็น P.I.D. และ $p \in D - \{0\}$ ซึ่งไม่ใช่หน่วย แล้ว

$$\langle p \rangle \ \text{เป็นไอดีลใหญ่สุดของ } D \quad \text{ก็ต่อเมื่อ} \quad p \ \text{ลดทอนไม่ได้ใน } D$$

ทฤษฎีบท

P.I.D. เป็น U.F.D.

ริงแบบยุคลิด (Euclidean ring)

บทนิยาม

ให้ E เป็นอินทิกรัลโดเมนซึ่งมียูนิตี

จะกล่าวว่า E เป็น **ริงแบบยุคลิด (Euclidean ring)** ก็ต่อเมื่อ มีฟังก์ชัน $d : E - \{0\} \to \mathbb{N}_0$ ซึ่งสำหรับทุก $a, b \in E - \{0\}$ สอดคล้อง 2 เงื่อนไขต่อไปนี้

1. $d(b) \leq d(ab)$
2. มี $q, r \in E$ ซึ่ง $b = aq + r$ โดยที่ $r = 0$ หรือ $d(r) < d(a)$

ตัวอย่าง

จงแสดงว่า $\mathbb{Z}$ เป็นริงแบบยุคลิด

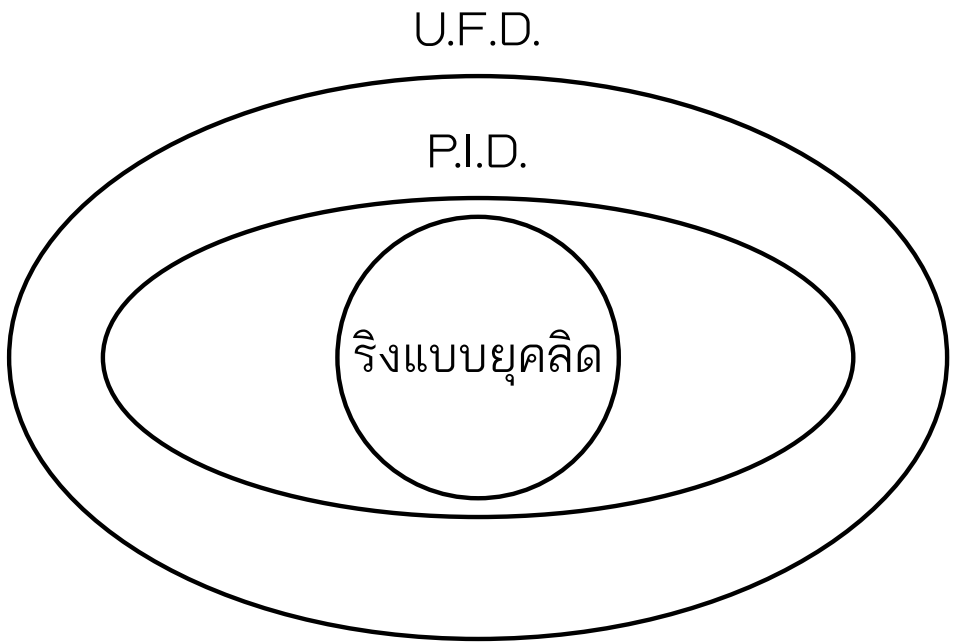
ทฤษฎีบท

ฟิลด์เป็นริงแบบยุคลิด

ทฤษฎีบท

ริงแบบยุคลิดเป็น P.I.D.

จากทฤษฎีบทที่ผ่านมาของ ริงยุคลิด P.I.D. และ U.F.D. อาจแสดงความสัมพันธ์ได้ดังนี้



บทที่ 8 ริงพหุนาม

8.1 พหุนาม

ให้ R เป็นริงสลับที่ซึ่งมียูนิตี กำหนดให้

$$R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \ : \ a_i \in R,\ n \in \mathbb{N}_0\}$$

เรียกสมาชิก $p(x)$ ใน $R[x]$ ว่า **พหุนาม (polynomial)** ซึ่งอยู่ในรูป

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

- $a_n, a_{n-1}, \ldots, a_1, a_0$ เรียกว่า **สัมประสิทธิ์ (coefficient)** ของ $x^n, x^{n-1}, \ldots, x, 1$ ตามลำดับ
- เรียก $a_n \neq 0$ ว่า **สัมประสิทธิ์ตัวนำ (leading coefficient)**
  ถ้า $a_i \neq 0$ เรียกแต่ละ $a_i x^i$ ว่า **พจน์ (term)** ของพหุนาม $p(x)$ หรือ **เอกนาม (monomial)**
- ถ้า $a_n \neq 0$ เรียก $p(x)$ ว่า **พหุนามระดับขั้น n (polynomial of degree n)**
  และเขียน n แทนด้วย $\deg p(x)$ นั่นคือ $\deg p(x) = n$
- ถ้า $a_n = 1$ เรียก $p(x)$ ว่า **พหุนามโมนิก (monic polynomial)**
- ถ้า $p(x) = a_0$ เรียก $p(x)$ ว่า **พหุนามคงตัว (constant polynomial)**
  ให้ $\deg p(x) = 0$ เมื่อ $a_0 \neq 0$
- กรณี $p(x) = 0$ เรียก **พหุนามศูนย์ (zero polynomaial)** และไม่นิยามระดับขั้น

ข้อสังเกต

ให้ R เป็นริงสลับที่ซึ่งมียูนิตี เห็นได้ชัดว่า $R \subseteq R[x]$

ตัวอย่าง

จงเขียนสมาชิกทั้งหมดของพหุนามระดับขั้น 2 ใน $\mathbb{Z}_2[x]$

บทนิยาม

ให้ R เป็นริงสลับที่ซึ่งมียูนิตี ให้ $p(x)$ และ $q(x)$ เป็นพหุนามที่ไม่ใช่พหุนามศูนย์ใน $R[x]$ จะได้ว่า $p(x) = q(x)$ ก็ต่อเมื่อ $\deg\ p(x) = \deg\ q(x)$ และอยู่ในรูป

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

$$q(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$$

เมื่อ $n \in \mathbb{N}_0$ และ $a_i = b_i$ ทุก ๆ $i \in \{1, 2, ..., n\}$

ตัวอย่าง

ให้ $p(x) = \bar{2}x^2 + x + \bar{1}$ และ $q(x) = ax^2 + bx + c$ เป็นพหุนามใน $\mathbb{Z}_2[x]$ ถ้า $p(x) = q(x)$ จงหา a, b และ c

ข้อสังเกต

ให้ R เป็นริงสลับที่ซึ่งมียูนิตี ถ้า $p(x)$ และ $q(x)$ เป็นพหุนามที่ไม่ใช่พหุนามศูนย์ใน $R[x]$ จะได้ว่า

1. $\deg\ (p(x) + q(x)) \leq \max\{\deg\ p(x), \deg\ q(x)\}$ หรือ $p(x) + q(x) = 0$
2. $\deg\ (p(x)q(x)) \leq \deg\ p(x) + \deg\ q(x)$ หรือ $p(x) \cdot q(x) = 0$

ตัวอย่าง

กำหนดให้ $p(x) = x^3 + x^2 - 3x + 1$ และ $q(x) = x^2 - 3$ เป็นพหุนามใน $\mathbb{Z}[x]$

จงหา $p(x) + q(x)$ และ $p(x)q(x)$

ตัวอย่าง

กำหนดให้

$$p(x) = Ax^3 + Bx^2 + Cx + D \text{ และ } q(x) = (x-2)(x+3)(x+1) + 5 \text{ เป็นพหุนามใน } \mathbb{Z}[x]$$

ถ้า $p(x) = q(x)$ จงหาค่าของ A, B, C และ D

ตัวอย่าง

ให้ $p(x) = x^2 + ax + b$ และ $q(x) = x^4 + x^3 + x + \bar{1}$ เป็นพหุนามใน $\mathbb{Z}_3[x]$

ถ้า $[p(x)]^2 = q(x)$ จงหา a และ b

ทฤษฎีบท

ให้ R เป็นริงสลับที่ซึ่งมียูนิตี แล้ว

$$R[x] \text{ ซึ่งนิยามการบวกและการคูณในบทนิยามข้างต้น เป็นริงสลับที่ซึ่งมียูนิตี}$$

และเรียก $R[x]$ ว่า ***ริงพหุนาม (polynomial ring)***

ถ้า R เป็นริงสลับที่ซึ่งมียูนิตี จะได้ว่า

- ศูนย์ใน $R[x]$ คือพหุนามศูนย์เขียนแทนด้วย 0
- ยูนิตีใน $R[x]$ คือพหุนามคงตัวยูนิตี เขียนแทนด้วย 1

นั่นคือริง $R[x]$ มีศูนย์และยูนิตีเป็นตัวเดียวกับ R

ตัวอย่าง

ให้ $p(x), q(x), r(x)$ เป็นพหุนามใน $\mathbb{Z}_4[x]$ โดยที่

$$p(x) = \bar{2}x^2 + x + \bar{2}, \quad q(x) = \bar{2}x^2 + \bar{2} \quad \text{และ} \quad r(x) = \bar{2}x^3 + \bar{1}$$

จงหา $p(x) + q(x)$, $q(x) + r(x)$, $[q(x)]^2$ และ $q(x)r(x)$

ทฤษฎีบท

ถ้า R เป็นอินทิกรัลโดเมนซึ่งมียูนิตี แล้ว

$$R[x] \text{ เป็นอินทิกรัลโดเมนซึ่งมียูนิตี}$$

ทฤษฎีบท

ให้ R เป็นอินทิกรัลโดเมนซึ่งมียูนิตี
ถ้า $p(x)$ และ $q(x)$ เป็นพหุนามที่ไม่ใช่พหุนามศูนย์ใน $R[x]$ แล้วจะได้ว่า

1. $deg\ (p(x)q(x)) = deg\ p(x) + deg\ q(x)$
2. $deg\ p(x) \leq deg\ (p(x)q(x))$

ทฤษฎีบท

ให้ R เป็นอินทิกรัลโดเมนซึ่งมียูนิตีจะได้ว่า

หน่วยใน R และ $R[x]$ คือตัวเดียวกัน

8.2 ริงพหุนามบนฟิลด์

ทฤษฎีบท

ขั้นตอนวิธีการหารสำหรับพหุนาม (Division Algorithm for Polynomial)
ให้ F เป็นฟิลด์ และ $a(x)$, $b(x)$ เป็นพหุนามใน $F[x]$ โดยที่ $a(x)$ ไม่เป็นพหุนามศูนย์ แล้วจะได้ว่ามีพหุนาม $q(x)$ และ $r(x)$ เพียงคู่เดียวเท่านั้นใน $F[x]$ ที่สอดคล้อง

$$b(x) = q(x)a(x) + r(x) \qquad \text{เมื่อ } r(x) = 0 \quad \text{หรือ} \quad \deg r(x) < \deg a(x)$$

*เรียก $r(x)$ ว่า **เศษเหลือ (remainder)** และ $q(x)$ ว่า **ผลหาร (quotient)** ของการหาร $b(x)$ ด้วย $a(x)$*
*ในกรณี $r(x) = 0$ โดยบทนิยาม 0.147 จะได้ว่า $a(x)$ หาร $b(x)$ ได้ หรือเขียนแทนด้วย $a(x) \mid b(x)$ โดยเรียก $a(x)$ ว่า **ตัวประกอบ (factor)** ของ $b(x)$ ใน $F[x]$*

ตัวอย่าง

จงหาผลหารและเศษเหลือที่เกิดจากการหาร

$$b(x) = x^3 + 1 \text{ ด้วย } a(x) = x^2 - 1 \text{ ใน } \mathbb{Z}[x]$$

ทฤษฎีบท

ถ้า F เป็นฟิลด์ แล้ว $F[x]$ เป็นริงแบบยุคลิด

บทแทรก

ถ้า F เป็นฟิลด์ แล้ว $F[x]$ เป็น P.I.D. และ U.F.D.

ทฤษฎีบท

ให้ F เป็นฟิลด์ และ $p(x)$ เป็นพหุนามที่ไม่ใช่พหุนามศูนย์ใน $F[x]$ แล้วข้อความต่อไปนี้สมมูลกัน

1. $p(x)$ *เป็นหน่วยใน* $F[x]$
2. $p(x)$ *เป็นพหุนามคงตัวที่ไม่ใช่พหุนามศูนย์ใน* $F[x]$
3. $\deg p(x) = 0$

ตัวอย่าง

จงแสดงว่า

1. $x^2 + 1$ ลดทอนไม่ได้ใน $\mathbb{R}[x]$ แต่ลดทอนได้ใน $\mathbb{C}[x]$
2. $x^2 + x + \bar{1}$ ลดทอนไม่ได้ใน $\mathbb{Z}_2[x]$

บทแทรก

ให้ F เป็นฟิลด์และ $p(x)$ เป็นพหุนามซึ่งไม่ใช่พหุนามศูนย์ใน $F[x]$ โดยที่ $f(x)$ และ $g(x)$ เป็นพหุนามใน $F[x]$ แล้วข้อความต่อไปนี้สมมูลกัน

1. $p(x)$ ลดทอนไม่ได้ใน $F[x]$
2. ถ้า $p(x) = f(x) \cdot g(x)$ แล้ว $\deg f(x) = 0$ หรือ $\deg g(x) = 0$

ทฤษฎีบท

ให้ F เป็นฟิลด์และ $p(x)$ เป็นพหุนามระดับขั้น 1 ใน $F[x]$ จะได้ว่า

$$p(x) \text{ ลดทอนไม่ได้ใน } F[x]$$

ทฤษฎีบท

ให้ F เป็นฟิลด์ และ $p(x)$ เป็นพหุนามใน $F[x]$ แล้วข้อความต่อไปนี้สมมูลกัน

1. $\langle p(x) \rangle$ *เป็นไอดีลใหญ่สุด*
2. $p(x)$ *ลดทอนไม่ได้ใน* $F[x]$
3. $F[x]/\langle p(x) \rangle$ *เป็นฟิลด์*

ตัวอย่าง

จงตรวจสอบว่า $\mathbb{Z}_3[x]/\langle x^2 + \bar{1} \rangle$ เป็นฟิลด์หรือไม่

ทฤษฎีบท

ให้ F เป็นฟิลด์ และ $p(x)$ ลดทอนไม่ได้ใน $F[x]$ โดยที่ $\deg p(x) = n$ จะได้ว่า

$$F[x]/\langle p(x)\rangle = \{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 + \langle p(x)\rangle \ : \ a_i \in F \text{ ทุก ๆ } i \in \{0, 1, ..., n-1\}\}$$

ตัวอย่าง

จงเขียนรูปแบบสมาชิกของฟิลด์ต่อไปนี้

1. $\mathbb{C}[x]/\langle x+1\rangle$
2. $\mathbb{R}[x]/\langle x^2+1\rangle$

ตัวอย่าง

จงแจกแจงสมาชิกของ $\mathbb{Z}_3[x]/\langle x^2+\bar{1}\rangle$

บทแทรก

ให้ p เป็นจำนวนเฉพาะ และ $g(x)$ ลดทอนไม่ได้ใน $\mathbb{Z}_p[x]$ ถ้า $\deg g(x) = n$ แล้ว

$$\mathbb{Z}_p[x]/\langle g(x)\rangle \text{ เป็นฟิลด์อันดับ } p^n$$

ตัวอย่าง

จงยกตัวอย่างฟิลด์อันดับ 25

ตัวอย่าง

จงสร้างตารางกรุปการคูณของ $\mathbb{Z}_2[x]/\langle x^2+x+\bar{1}\rangle$ พร้อมหาตัวผกผันการคูณของสมาชิก

ตัวอย่าง

จงหาตัวผกผันการคูณของ $x+1+\langle x^2+1\rangle$ ใน $\mathbb{R}[x]/\langle x^2+1\rangle$

8.3 ริงพหุนามบนฟิลด์ตรรกยะ

บทนิยาม

ให้ $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ เป็นพหุนามซึ่ง $a_i \in \mathbb{Z}$ ทุก $i \in \{0, 1, ..., n\}$ จะเรียก $f(x)$ ว่า **พหุนามปฐมฐาน (primitive polynomial)** ก็ต่อเมื่อ

$$\gcd(a_0, a_1, ..., a_n) = 1$$

ตัวอย่างเช่น $x^2 + x + 3$ และ $2x^3 - x^2 + 2x - 4$ เป็นพหุนามปฐมฐาน แต่ $2x^2 + 2x + 4$ และ $3x^3 + 3$ ไม่เป็นพหุนามปฐมฐาน

ข้อสังเกต

ให้ $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ เป็นพหุนามซึ่ง $a_i \in \mathbb{Z}$

ถ้า $f(x)$ ไม่เป็นพหุนามปฐมฐาน ก็ต่อเมื่อ $\gcd(a_0, a_1, ..., a_n) \neq 1$ หรือมี $a \in \mathbb{Z}$ โดยที่ $a \neq 1$ ซึ่ง

$$f(x) = ag(x) \quad \text{เมื่อ } g(x) \text{ เป็นพหุนามปฐมฐาน}$$

ตัวอย่างเช่น $a = \gcd(a_0, a_1, ..., a_n)$ ซึ่ง $a \neq 1$ และ $b_i = \dfrac{a_i}{a} \in \mathbb{Z}$ ทุก $i \in \{0, 1, ..., n\}$ จะได้ว่า

$$f(x) = ab_n x^n + ab_{n-1}x^{n-1} + \cdots + ab_1 x + ab_0 = ag(x)$$

เมื่อ $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$ จะได้ว่า

$$\gcd(b_0, b_1, ..., b_n) = \gcd\left(\frac{a_0}{a}, \frac{a_1}{a}, ..., \frac{a_n}{a}\right) = 1$$

นั่นคือ $g(x)$ เป็นพหุนามปฐมฐาน

ทฤษฎีบท

ให้ $f(x)$ และ $g(x)$ เป็นพหุนามปฐมฐาน แล้ว $f(x)g(x)$ เป็นพหุนามปฐมฐาน

บทตั้ง

บทตั้งของเกาส์ (Gauss' Lemma)

ให้ $f(x) \in \mathbb{Q}[x]$ โดยที่ $f(x)$ เป็นพหุนามปฐมฐาน ถ้า $f(x) = u(x)v(x)$ เมื่อ $u(x), v(x) \in \mathbb{Q}[x]$

$$\text{แล้วจะมี } g(x), h(x) \in \mathbb{Z}[x] \text{ ซึ่ง } f(x) = g(x)h(x)$$

จากบทตั้งของเกาส์สรุปได้ว่า สำหรับพหุนามปฐมฐาน $f(x)$ จะได้ว่า

$$f(x) \text{ ลดทอนไม่ได้ใน } \mathbb{Q}[x] \quad \text{ก็ต่อเมื่อ} \quad f(x) \text{ ลดทอนไม่ได้ } \mathbb{Z}[x]$$

ถ้า $f(x)$ ไม่เป็นพหุนามปฐมฐาน แล้วบทตั้งของเกาส์จะไม่จริงดังตัวอย่างต่อไปนี้

ตัวอย่าง

จงแสดงว่า $4x+2$ ลดทอนได้ใน $\mathbb{Z}[x]$ แต่ลดทอนไม่ได้ $\mathbb{Q}[x]$

บทแทรก

ให้ $f(x) \in \mathbb{Q}[x]$ โดยที่สัมประสิทธิ์ทุกตัวเป็นจำนวนเต็ม

ถ้า $f(x) = u(x)v(x)$ เมื่อ $u(x), v(x) \in \mathbb{Q}[x]$

$$\text{แล้วจะมี } g(x), h(x) \in \mathbb{Z}[x] \text{ ซึ่ง } f(x) = g(x)h(x)$$

บทแทรก

$\mathbb{Z}[x]$ เป็น U.F.D.

ทฤษฎีบท

เกณฑ์การพิจารณาไอเซนสไตน์ (Eisenstein's Criterion)

ให้ $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ *โดยที่* $a_i \in \mathbb{Z}$ *ทุก* $i \in \{0, 1, 2, ..., n\}$ *มีจำนวนเฉพาะ* p *ซึ่ง*

1. $p \mid a_i \quad$ *ทุก* $\quad i \in \{0, 1, ..., n-1\}$
2. $p \nmid a_n \quad$ *และ* $\quad p^2 \nmid a_0$

แล้ว $f(x)$ *ลดทอนไม่ได้ใน* $\mathbb{Q}[x]$

ตัวอย่าง

จงตรวจสอบว่าพหุนามต่อไปนี้ลดทอนได้หรือไม่ใน $\mathbb{Q}[x]$

1. $x^4 + 10x + 5$ ลดทอนไม่ได้ใน $\mathbb{Q}[x]$ เลือก $p = 5$
2. $3x^3 + 4x + 2$ ลดทอนไม่ได้ใน $\mathbb{Q}[x]$ เลือก $p = 2$
3. $x^2 - x - 12$ ลดทอนได้ใน $\mathbb{Q}[x]$ เนื่องจาก

   $x^2 - x - 12 = (x - 4)(x + 3)$
4. $5x^5 + 9x + 6$ ลดทอนไม่ได้ใน $\mathbb{Q}[x]$ เลือก $p = 3$
5. $x^7 + 7$ ลดทอนไม่ได้ใน $\mathbb{Q}[x]$ เลือก $p = 7$
6. $x^7 + 5^3$ ลดทอนไม่ได้ใน $\mathbb{Q}[x]$ เลือก $p = 5$
7. $(x + 1)^4 + 1$ พิจารณา

$$(x + 1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$$

ดังนั้น $(x + 1)^4 + 1$ ลดทอนไม่ได้ใน $\mathbb{Q}[x]$ เลือก $p = 2$