บทที่ 6
วงพหุนาม
(Polynomial rings)

6.1 วงพหุนาม (Polynomial rings)

เชื่อว่านักศึกษาคงคุ้นเคยกับเรื่องของพหุนาม (polynomial) ไม่แต่เพียงตัวพหุนามอย่างเดียว แต่ยังรวมถึงการบวกและการคูณพหุนามด้วย ในบทนี้เราจะกำหนดพหุนามบนวง และกำหนดการบวกและการคูณ ในการนิยามวงพหุนามนี้ เราจะพยายามที่จะให้ครอบคลุมถึงความสัมพันธ์ที่เป็นจริงระหว่างคุณสมบัติของวง R และวงพหุนามบน R

ให้ R เป็นวง และ x เป็นสัญลักษณ์รูปแบบ (formal symbol) แล้วพหุนามใน x เหนือ R (Polynomial in x over R) เราหมายถึง สัญลักษณ์รูปแบบ $a_0 + a_1x + \ldots + a_nx^n$ โดยที่ $a_0, a_1, \ldots, a_n \in R$ และเรียก $a_0, a_1, \ldots, a_n$ ว่า สัมประสิทธิ์ของพหุนาม

เพื่อความสะดวกเรานิยมเขียนแทนพหุนามด้วย

$p(x) = \sum_{i=0}^{\infty} a_ix^i$ โดยที่เรายอมรับว่า $a_0x^0 = a_0$

และที่นอกเหนือจากบาง n ที่กำหนดสัมประสิทธิ์เป็นศูนย์หมด

ถ้า $p(x) = \sum_{i=0}^{\infty} a_ix^i$ เป็นพหุนามใน x เหนือ R แล้ว

เรานิยามระดับของ p(x) (degree of p(x)) ซึ่งจะเขียนแทนด้วย deg(p(x)) ว่า คือ ค่า n ตัวที่ใหญ่ที่สุด (largest *n*) ที่ $a_n \neq 0$

ดังนั้น พหนุนาม 0 ไม่มีระดับขั้น

เราเรียก พหุนาม 0 ว่า พหุนามศูนย์ (zero polynomial)

พหุนาม a_0 โดยที่ $a_0 \neq 0$ มีระดับขั้น 0

เราเรียก พหุนาม a_0 ว่า พหุนามค่าคงตัว (constant polynomial)

พหุนาม $a_0 + a_1x + \ldots + a_k x^k$ โดยที่ $a_k \neq 0$ มีระดับขั้น K

ถ้า $p(x) = \sum_{i=0}^{\infty} a_i x^i$ มีระดับชั้น k แล้ว $a_k \neq 0$ เรียก a_k ว่า สัมประสิทธิ์นำ (leading coefficient) ของ p(x)

ถ้า $p(x) = \sum_{i=1}^{\infty} a_i x^i$ แล้ว เรียก a_0 ว่า พจน์คงตัวของ p(x)

พหุนาม $p(x) = \sum_{i=1}^{\infty} a_i x^i$ และพหุนาม $q(x) = \sum_{i=1}^{\infty} b_i x^i$ จะเท่ากัน เขียนแทนด้วย $p(x) = q(x)$ ก็ต่อเมื่อ $a_i = b_i$ สำหรับแต่ละ i

เขียนแทนเซตของพหุนามใน x เหนือ R ทั้งหมดด้วย R[x]

นั่นคือ R[x] เป็นเซตของพหุนามทั้งหมดใน x เหนือ R

อย่างไรก็ตาม สำหรับ $r \in R$ พหุนาม $r = \sum_{i=0}^{\infty} a_i x^i \in R[x]$ โดยที่ ทุก ๆ $a_i = 0$ สำหรับ $i > 0$ และ $a_0 = r$

ดังนั้น เราจึงได้ว่า $R \subset R[x]$ และแน่นอนพหุนามคงตัวเป็นสมาชิกของ R

ขอให้สังเกตว่า ในขณะที่เพื่อความสะดวก เราจะเขียนแทนพหุนามด้วย $\sum_{i=1}^{\infty} a_i x^i$ แต่อันดับของพจน์ไม่สำคัญ

นั่นคือ $2 + 3x^2 + 4x \in Z[x]$ แล้ว

$$2 + 3x^2 + 4x = 2 + 4x + 3x^2 = 3x^2 + 4x + 2$$

นิยาม

ให้ R[x] เป็นเซตของพหุนามทั้งหมดของ x เหนือ R กำหนดการดำเนินการ + และ . บน R[x] โดย

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i)\, x^i$$

$$\left(\sum_{i=0}^{\infty} a_i x^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=0}^{\infty} c_k x^k$$

โดยที่ $c_k = \sum_{i=0}^{k} a_i b_{k-i}$

ทฤษฎี 6.1.1 ให้ R[x] เป็นเซตของพหุนามทั้งหมดใน x เหนือวง R แล้ว (R[x], +, .) เป็นวง

พิสูจน์

ให้ $\sum_{i=0}^{\infty} a_i x^i,\ \sum_{i=0}^{\infty} b_i x^i \in R[x]$

$$\because \sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i)\, x^i$$

$$= \sum_{i=0}^{\infty} c_i x^i$$

$\therefore$ การ + ปิดบนเซต R[x]

ให้ $\sum_{i=0}^{\infty} a_i x^i,\ \sum_{i=0}^{\infty} b_i x^i,\ \sum_{i=0}^{\infty} c_i x^i \in R[x]$

$$\therefore \left(\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i\right) + \sum_{i=0}^{\infty} c_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i + \sum_{i=0}^{\infty} c_i x^i$$

$$= \sum_{i=0}^{\infty} ((a_i + b_i) + c_i)x^i$$

$$= \sum_{i=0}^{\infty} (a_i + (b_i + c_i))x^i$$

$$= \sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} (b_i + c_i)x^i$$

$$= \sum_{i=0}^{\infty} a_i x^i + \left(\sum_{i=0}^{\infty} b_i x^i + \sum_{i=0}^{\infty} c_i x^i\right)$$

$\therefore$ การบวกบน $R[x]$ สอดคล้องกฎการเปลี่ยนกลุ่ม

ให้ $\sum_{i=0}^{\infty} a_i x^i \in R[x]$

$$\sum_{i=0}^{\infty} 0x^i + \sum_{i=0}^{\infty} a_i x^i = \sum_{i=0}^{\infty} (0 + a_i)x^i$$

$$= \sum_{i=0}^{\infty} a_i x^i$$

และ $\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} 0x^i = \sum_{i=0}^{\infty} (a_i + 0)x^i$

$$= \sum_{i=0}^{\infty} a_i x^i$$

$\therefore$ $\sum_{i=0}^{\infty} 0x^i$ เป็นเอกลักษณ์สำหรับการบวกของ $R[x]$

ให้ $\sum_{i=0}^{\infty} a_i x^i \in R[x]$

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} (-a_i)x^i = \sum_{i=0}^{\infty} (a_i + (-a_i))x^i$$

$$= \sum_{i=0}^{\infty}$$ [illegible]

และ $$\sum_{i=0}^{\infty}(-a_i)x^i + \sum_{i=0}^{\infty}a_ix^i = \sum_{i=0}^{\infty}(-a_i + a_i)x^i$$

$$= \sum_{i=0}^{\infty}0x^i$$

$\sum_{i=0}^{\infty}(-a_i)x^i$ เป็นตัวผกผันสำหรับการ + ของ $\sum_{i=0}^{\infty}a_ix^i$ บน $R[x]$

ให้ $\sum_{i=0}^{\infty}a_ix^i$, $\sum_{i=0}^{\infty}b_ix^i \in R[x]$

$\because$ $$\sum_{i=0}^{\infty}a_ix^i + \sum_{i=0}^{\infty}b_ix^i = \sum_{i=0}^{\infty}(a_i + b_i)x^i$$

$$= \sum_{i=0}^{\infty}(b_i + a_i)x^i$$

$$= \sum_{i=0}^{\infty}b_ix^i + \sum_{i=0}^{\infty}a_ix^i$$

$\therefore$ การ + บน $R[x]$ สอดคล้องกฎการสลับที่

$\therefore$ $(R[x], +)$ เป็นกลุ่มอาบีเลียน

ให้ $\sum_{i=0}^{\infty}a_ix^i$, $\sum_{i=0}^{\infty}b_jx^j$, $\sum_{i=0}^{\infty}c_kx^k \in R[x]$

$$\left[\left(\sum_{i=0}^{\infty}a_ix^i\right)\left(\sum_{i=0}^{\infty}b_ix^i\right)\right]\left(\sum_{i=0}^{\infty}c_kx^k\right) = \left[\sum_{n=0}^{\infty}\left(\sum_{i=0}^{n}a_ib_{n-i}\right)x^n\right]\sum_{k=0}^{\infty}c_kx^k$$

$$= \sum_{s=0}^{\infty}\left[\sum_{n=0}^{s}\left(\sum_{i=0}^{n}a_ib_{n-i}\right)c_{s-n}\right]x^s$$

$$= \sum_{s=0}^{\infty}\left(\sum_{i+j+k=s}a_ib_jc_k\right)x^s$$

$$= \sum_{s=0}^{\infty}\left[\sum_{m=0}^{s}a_{s-m}\left(\sum_{j=0}^{m}b_jc_{m-j}\right)\right]x^s$$

$$= \sum_{i=0}^{\infty} a_i x^i \Big[\sum_{m=0}^{\infty} \Big(\sum_{j=0}^{\infty} b_j c_{m-j} \Big) x^m \Big]$$

$$= \Big(\sum_{i=0}^{\infty} a_i x^i \Big) \Big[\Big(\sum_{j=0}^{\infty} b_j x^j \Big) \Big(\sum_{k=0}^{\infty} c_k x^k \Big) \Big]$$

$\therefore$ การคูณบน $R[x]$ สอดคล้องกฎการเปลี่ยนกลุ่ม

ให้ $\sum_{i=0}^{\infty} a_i x^i, \quad \sum_{j=0}^{\infty} b_j x^j, \quad \sum_{k=0}^{\infty} c_k x^k \in R[x]$

$$\because \quad \sum_{i=0}^{\infty} a_i x^i \Big[\Big(\sum_{j=0}^{\infty} b_j x^j \Big) + \Big(\sum_{k=0}^{\infty} c_k x^k \Big) \Big] = \sum_{i=0}^{\infty} a_i x^k \Big[\sum_{k=j=0}^{\infty} (b_j + x_k) x^k$$

$$= \sum_{i=0}^{\infty} a_i x^i \Big[\sum_{j=0}^{\infty} (b_j + x_j) x^j \Big]$$

$$= \sum_{n=0}^{\infty} \sigma_n x^n$$

โดยที่ $d_n = \sum_{i=j=0}^{n} a_i (b_{n-j} + c_{n-j})$

$$= \sum_{i=0}^{\infty} a_i (b_{n-i} + c_{n-i})$$

$$= \sum_{i=0}^{n} a_i b_{n-i} + \sum_{i=0}^{n} a_i c_{n-i}$$

$$= \sum_{i=j=0}^{n} a_i b_{n-j} + \sum_{i=k=0}^{n} a_i c_{n-k}$$

$$\therefore \quad \sum_{n=0}^{\infty} d_n x^n = \sum_{n=0}^{\infty} \Big(\sum_{i=j=0}^{n} a_i b_{n-j} + \Sigma a_i c_{n-k} \Big) x^n$$

$$= \sum_{n=0}^{\infty} \sum_{i=j=0}^{n} a_i b_{n-j} \, x^n + \sum_{n=0}^{\infty} \sum_{k=i}^{n} a_i c_{n-k} \, x^n$$

$$= \sum_{i=0}^{\infty} a_i x^i \sum_{j=0}^{\infty} b_j x^j + \sum_{i=0}^{\infty} a_i x^i \sum_{j=0}^{\infty} c_k x^k$$

$\therefore$ กฎการแจกแจงเป็นจริงใน $R[x]$

$\therefore$ $[R[x], +, .]$ เป็นวง #

นิยาม ให้ $R[x]$ เป็นเซตของพหุนามทั้งหมดใน x เหนือวง R แล้ว $(R[x], +, .)$ เป็นวงเรียกว่า วงพหุนาม (polynomial ring)

ข้อสังเกต

1. ถ้า R เป็นวงที่มี unity 1 แล้ว $R[x]$ เป็นวงที่มี unity 1
2. ถ้า R เป็นวงที่สอดคล้องกฎการสลับที่ แล้ว $R[x]$ เป็นวงที่สอดคล้องกฎการสลับที่
3. วง R เป็นวงย่อยของวง $R[x]$

ทฤษฎี 6.1.2 ถ้า R เป็นวงที่ไม่มีตัวหารของศูนย์ แล้ว $R[x]$ เป็นวงที่ไม่มีตัวหารของศูนย์

พิสูจน์

ให้ $p(x) = \sum_{i=0}^{\infty} a_i x^i$ และ $q(x) = \sum_{i=0}^{\infty} b_i x^i \in R[x] \ni p(x) \neq 0$ และ $q(x) \neq 0$

ให้ a_k และ b_n เป็นสัมประสิทธิ์นำ (leading coefficient) ของ $p(x)$ และ $q(x)$ ตามลำดับ เราจะพิสูจน์ว่า $p(x)\, q(x) \neq 0$ โดยการแสดงว่า สัมประสิทธิ์ของ x^{k+n} ไม่ใช่ 0

พิจารณา $p(x)\, q(x) = \sum_{i=0}^{\infty} c_i x^i$ โดยที่

$$c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

ดังนั้น $c_{k+n} = \sum_{j=0}^{k+n} a_j b_{k+n-j}$

สำหรับ $j > k$ เราได้ $a_j = 0$

สำหรับ $j < k$ เราได้ $(k + n) - j > (k + n) - k = n$ เราได้

$$b_{(k+n)-j} = 0$$

ดังนั้น $c_{k+n} = a_n b_n \neq 0$ (เพราะ R ไม่มีตัวหารของศูนย์)

ด้วยเหตุนี้ $p(x)\,q(x)$ ไม่ใช่พหุนามศูนย์ #

บทแทรก 1 ถ้า R เป็นโดเมนเชิงจำนวนเต็ม แล้ว $R[x]$ เป็นโดเมนเชิงจำนวนเต็ม

บทแทรก 2 ถ้า R เป็นสนามแล้ว $R[x]$ เป็นโดเมนเชิงจำนวนเต็ม

ทฤษฎี 6.1.3 ถ้า R เป็นวงที่ไม่มีตัวหารของศูนย์ และ $p(x)$ และ $q(x)$ เป็นสมาชิกที่ไม่ใช่ศูนย์ของ $R[x]$ แล้ว

$$\deg(p(x)\ q(x)) = \deg(p(x)) + \deg(q(x))$$

พิสูจน์

จากข้อพิสูจน์ของทฤษฎี 6.1.2 ทำให้เราได้ว่า

$$\deg(p(x)) = k$$

$$\deg(q(x)) = n$$

และเราพิสูจน์แล้วจากทฤษฎี 6.1.2 ว่า $c_{k+n} = a_k b_n \neq 0$

ดังนั้น ข้อพิสูจน์ของทฤษฎี 6.1.3 นี้ จะสมบูรณ์ถ้าเราสามารถพิสูจน์ได้ว่า $c_m = 0$

สำหรับทุก ๆ $m > k + n$

ให้ $m > k + n$

พิจารณา $c_m = \sum_{j=0}^{m} a_j b_{m-j}$

ถ้า $j > k$ แล้ว $a_j = 0$

ถ้า $j \leqslant k$ แล้ว $m - j \geqslant m - k > k + n - k = n$

ดังนั้น $b_{m-j} = 0$

ด้วยเหตุนี้ $c_m = 0$

ตัวอย่าง 6.1.1 พิจารณา $2 + 3x, 1 + 2x + 2x^3 \in Z_6[x]$

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

จะเห็นว่าลำดับขั้นของผลคูณ $\neq$ ผลบวกของลำดับขั้น

(เพราะ $Z_6[x]$ มีตัวหารของศูนย์)

ทฤษฎี 6.1.4 ขั้นตอนวิธีการหาร (Division Algorithm)

ให้ F เป็นสนาม และ $p(x), q(x) \in F[x]$ โดยที่ $q(x) \neq 0$ แล้วจะมี $s(x), r(x) \in F[x]$ ซึ่ง $p(x) = q(x)\,s(x) + r(x)$ โดยที่ $r(x) = 0$ หรือมิฉะนั้นก็ $\deg(r(x)) < \deg(q(x))$

พิสูจน์

ถ้า $p(x) = 0$ หรือ $\deg(p(x)) < \deg(q(x))$ แล้ว

$$p(x) = 0q(x) + p(x)$$

สมมติว่า $\deg(p(x)) \geqslant \deg(q(x))$

ถ้า $\deg(p(x)) = 0$ แล้ว

$p(x)$ เป็นพหุนามค่าคงตัว

ดังนั้น $p(x) = a$

เนื่องจาก $\deg(p(x)) \geqslant \deg(q(x))$ และ $q(x) \neq 0$

เราทราบว่า $q(x)$ เป็นพหุนามค่าคงตัว

$\therefore\ q(x) = b$

$\therefore\ a = b(ab^{-1}) + 0$ สอดคล้องทฤษฎี

สมมติทฤษฎีเป็นจริงสำหรับทุก ๆ พหุนาม $p(x)$ ที่มีลำดับขั้นน้อยกว่า k และทุก ๆ พหุนาม $q(x)$

ให้ $p(x)$ เป็นพหุนามที่มีลำดับขั้น k

ถ้า $\deg(p(x)) < \deg q(x))$ ข้อพิสูจน์จะสมบูรณ์

ด้วยเหตุนี้เราสมมติ $\deg(p(x)) = k \geqslant \deg(q(x)) = n$

ให้ a_k และ b_n เป็นสัมประสิทธิ์นำของ $p(x)$ และ $q(x)$ ตามลำดับ

ขอให้สังเกตว่า $p(x) - (a_k b_n^{-1} x^{k-n})\, q(x)$ เป็นพหุนามที่มีลำดับขั้นน้อยกว่า k

ดังนั้น จะมีพหุนาม $s(x)$ และ $r(x)$ ซึ่ง

$$p(x) - (a_k b_n^{-1} x^{k-n})\, q(x) = s(x)\, q(x) + r(x)$$

โดยที่ $r(x) = 0$ หรือ $\deg(r(x)) < \deg(q(x))$

ดังนั้น $p(x) = /s(x) + a_k b_n^{-1} x^{k-n}]\, q(x) + r(x)$ #

ทฤษฎี 6.1.5 ถ้า F เป็นสนามแล้วทุก ๆ กลุ่มอุดมคติของ $R[x]$ เป็นกลุ่มอุดมคติหลัก (principal)

พิสูจน์

ให้ I เป็นกลุ่มอุดมคติของ $R[x]$

ถ้า $I = \{0\}$ แล้ว I เป็นกลุ่มอุดมคติหลัก

ถ้า $I \neq \{0\}$ แล้ว โดยคุณสมบัติจำนวนเต็มที่ว่าทุก ๆ เซตย่อยของเซตจำนวนเต็มจะต้องมีสมาชิกตัวที่เล็กที่สุด จึงได้ว่า

จะมี $p(x) \in I \ni p(x) \neq 0$ และ $\deg(p(x)) < \deg(q(x))$

สำหรับทุก ๆ $0 \neq q(x) \in I$

ให้ $q(x) \in I$

โดยขั้นตอนวิธีการหาร (Division Algorithm)

จะมีพหุนาม $s(x), r(x) \in F[x] \ni q(x) = p(x)\,s(x) + r(x)$ /

โดยที่ $r(x) = 0$ หรือมิฉะนั้นก็ $\deg(r(x)) < \deg(p(x))$

แต่ $p(x) \in I$

$\therefore\ p(x)\,s(x) \in I$

และเนื่องจาก $q(x) \in I$

$\therefore\ r(x) = q(x) - p(x)\,s(x) \in I$

ถ้า $r(x) \neq 0$ แล้ว $r(x) \in I$ โดยที่

$$\deg(r(x)) < \deg(p(x))$$

ซึ่งขัดแย้งกับการเลือก $p(x)$ ($\because$ $p(x)$ เป็นสมาชิกตัวที่เล็กที่สุดของ I)

ดังนั้น $r(x) = 0$ และ

$$q(x) = s(x)\,p(x)$$

$\therefore\ I = \langle p(x) \rangle$ #

6.2 ฟังก์ชันถ่ายแบบมูลฐาน (Basic homomorphism)

ให้ R เป็นวง x และ y เป็นสัญลักษณ์รูปแบบ (formal symbol) แล้ว เราสามารถสร้างวงพหุนาม $(R[x])[y]$ ซึ่งเป็นวงพหุนามใน y โดยที่สัมประสิทธิ์ของ y เป็นพหุนามใน x เขียนแทนด้วยสัญลักษณ์ $R[x, y]$ เราอาจพิจารณาวง $R[x, y]$ ว่าเป็นวงของพหุนามใน x, y โดยที่สัมประสิทธิ์

ของ x, y **เป็นสมาชิกของ** R **ตัวอย่างเช่น พหุนาม** $2 + 3xy^2 + 3x^3y + 4xy + 4x^2y^2 + x^3y^2 + x^4y^2$ **เป็นพหุนามใน** x **และ** y โดยมีสัมประสิทธิ์จำนวนเต็ม หรือเราอาจเขียนเป็น $2 + (4x + 3x^3)y + (3x + 4x^2 + x^3 + x^4)y^2$ ซึ่งเป็นพหุนามใน y โดยมีสัมประสิทธิ์เป็นพหุนามจาก $Z[x]$

ในทำนองเดียวกัน $R[x_1, x_2, \ldots, x_n]$ ก็เป็นวงพหุนามของสัญลักษณ์รูปแบบ x_i $(i = 1, 2, \ldots, n)$ **โดยมีสัมประสิทธิ์ของ** x_i เป็นสมาชิกของ R

ทฤษฎี 6.2.1 ถ้า R เป็นวงที่ไม่มีตัวหารของศูนย์แล้ว $R[x_1, x_2, \ldots, x_n]$ เป็นวงที่ไม่มีตัวหารของศูนย์

(ข้อพิสูจน์ละไว้ให้ น.ศ. ทำเป็นแบบฝึกหัด)

(การพิสูจน์ใช้การอุปมาน จากความจริงที่ได้จากทฤษฎี 6.1.2)

บทแทรก ถ้า R เป็นโดเมนเชิงจำนวนเต็มแล้ว แล้ว $R[x_1, x_2, \ldots, x_n]$ เป็นโดเมนเชิงจำนวนเต็ม

ทฤษฎี 6.2.2 ทฤษฎีฟังก์ชันถ่ายแบบมูลฐานของสนาม

(The Basic homomorphism for field theory)

> ให้ F เป็นสนามย่อยของสนาม E, $\alpha \in E$ และ x เป็นสัญลักษณ์รูปแบบ, ฟังก์ชัน $\psi_\alpha : F[x] \to E$ กำหนดโดย $\psi_\alpha(a_0 + a_1x + \ldots + a_nx^n) = a_0 + a_1\alpha + \ldots + a_n\alpha^n$ สำหรับ $(a_0 + a_1x + \ldots + a_nx^n) \in F[x]$ แล้ว ψ_α เป็นฟังก์ชันถ่ายแบบของ F[x] ไปใน E
> และ $\psi_\alpha(x) = x$ ด้วย และ ψ_α ส่ง F ถอดแบบกันโดย identity map นั่นคือ $\psi_\alpha(a) = a$ สำหรับ $a \in F$

พิสูจน์

ถ้า $f(x) = a_0 + a_1x + \ldots + a_nx^n$

$g(x) = b_0 + b_1x + \ldots + b_mx^m$

และ $h(x) = f(x) + g(x)$

$= c_0 + c_1x + \ldots + c_rx^r$ แล้ว

$\psi_\alpha(f(x) + g(x)) = c_0 + c_1\alpha + \ldots + c_r\alpha^r$

และ $\psi_\alpha(f(x)) + \psi_\alpha(g(x)) = (a_0 + a_1\alpha + \ldots + a_n\alpha^n) + (b_0 + b_1\alpha + \ldots b_m\alpha^m)$

โดยนิยามของการบวกพหุนาม $c_i = a_i + b_i$

$\therefore \quad \psi_\alpha(f(x) + g(x)) = \psi_\alpha(f(x)) + \psi_\alpha(g(x))$

ถ้า $f(x)\,g(x) = d_0 + d_1x + \ldots + d_sx^s$

แล้ว $\psi_\alpha(f(x)\,g(x)) = d_0 + d_1\alpha + \ldots + d_s\alpha^s$

และ $[\psi_\alpha(f(x))][\psi_\alpha(g(x))] = (a_0 + a_1\alpha + \ldots + a_n\alpha^n)(b_0 + b_1\alpha + \ldots + b_m\alpha^m)$

โดยนิยามของการคูณพหุนาม

$$d_j = \sum_{i=0}^{j} a_ib_{j-i}$$

$\therefore \qquad \psi_\alpha[f(x)\,g(x)] \;=\; [\psi_\alpha(f(x)][\psi_\alpha(g(x))]$

ดังนั้น ψ_α เป็นฟังก์ชันถ่ายแบบ

จากข้อกำหนดของ ψ_α

สำหรับ พหุนามค่าคงตัว $a \in F[x]$ โดยที่ $a \in F$

เราได้ว่า $\psi_\alpha(a) = a$

ดังนั้น ψ_α ส่ง F ถอดแบบกัน โดย identity map

โดยข้อกำหนดของ ψ_α เราได้

$$\psi_\alpha(x) \;=\; \psi_\alpha(1x) = 1\alpha = \alpha \qquad \#$$

ตัวอย่าง 6.2.1 ให้ F เป็น Q (เซตจำนวนตรรกยะ)

E เป็น R (เซตจำนวนจริง)

พิจารณาฟังก์ชันถ่ายแบบมูลฐาน $\psi_0 : Q[x] \to R$ ในที่นี้

$$\begin{aligned}\psi_0(a_0 + a_1x + \ldots + a_nx^n) &= a_0 + a_1(0) + a_1(0)^2 + \quad + a_n(0)^n \\ &= a_0\end{aligned}$$

ดังนั้น ทุก ๆ พหุนามถูกส่งไปบนพจน์ค่าคงตัวของตัว

ตัวอย่าง 6.2.2 ให้ F เป็น Q (เซตจำนวนตรรกยะ)

E เป็น R (เซตจำนวนจริง)

พิจารณาฟังก์ชันถ่ายแบบมูลฐาน $\psi_2 : Q[x] \to R$

$$\psi_2(a_0 + a_1x + \ldots + a_nx^n) = a_0 + a_1(2) + \ldots + a_n(2)^n$$

ขอให้สังเกตว่า

$$\begin{aligned}\psi_2(x^2 + x - 6) &= 2^2 + 2 - 6 \\ &= 0\end{aligned}$$

ดังนั้น $(x^2 + x - 6) \in \ker \psi_2$

ตัวอย่าง 6.2.3 ให้ F เป็น Q (เซตจำนวนตรรกยะ)

E เป็น C (เซตจำนวนเชิงซ้อน)

พิจารณาฟังก์ชันถ่ายแบบมูลฐาน $\psi_i\, Q[x] \to C$

$$\psi_i(a_0 + a_1x + \dots + a_nx^n) = a_0 + a_1i + \dots + a_ni^n$$

และ $\psi_i(x) = i$

ขอให้สังเกตว่า

$$\psi_i(x^2 + 1) = i^2 + 1 = 0$$

ดังนั้น $x^2 + 1 \in \ker \psi_i$

นิยาม

> ให้ F เป็นสนามย่อยของสนาม E, $\alpha \in E$
>
> ให้ $f(x) = a_0 + a_1x + \dots + a_nx^n \in F[x]$
>
> ให้ $\psi_\alpha F[x] \to E$ เป็นฟังก์ชันถ่ายแบบมูลฐาน
>
> ให้ $f(\alpha)$ เขียนแทน
>
> $$\psi_\alpha(f(x)) = a_0 + a_1\alpha + \dots + a_n\alpha^n$$
>
> เรียก $f(\alpha)$ ว่า ศูนย์ของ f(x) (zero of f(x)) เมื่อ
>
> $$f(\alpha) = 0$$

โดยนิยามนี้ทำให้เราสามารถจะหาผลเฉลย (solution) ของสมการพหุนาม $r^2 + r - 6 = 0$ โดยให้ F = Q และ E = R และหาทุก ๆ $\alpha \in R \ni \psi_\alpha(x^2 + x - 6) = 0$ นั่นคือ หาทุก ๆ ศูนย์ (zeros) ของ $x^2 + x - 6$ ใน R ซึ่งคือ

$$\{\alpha \in R \mid \psi_\alpha(x^2 + x - 6) = 0\} = \{2, -3\}$$

แบบฝึกหัดที่ 6

1) จงพิจารณาข้อความต่อไปนี้แต่ละข้อ เป็นจริงหรือเป็นเท็จ

..............ก) พหุนาม $(a_nx^n + \ldots + a_1x + a_0) \in R[x]$ เป็นศูนย์ก็ต่อเมื่อ $a_i = 0$ สำหรับ $i = 0, 1, 2, \ldots, n$

..............ข) ถ้า R เป็นวงที่สอดคล้องกฎการสลับที่แล้ว $R[x]$ เป็นวงที่สอดคล้องกฎการสลับที่

..............ค) ถ้า D เป็นโดเมนเชิงจำนวนเต็มแล้ว $D[x]$ เป็นโดเมนเชิงจำนวนเต็ม

..............ง) ถ้า R เป็นวงที่มีตัวหารของศูนย์แล้ว $R[x]$ มีตัวหารของศูนย์

..............จ) ถ้า R เป็นวง และ $f(x)$ และ $g(x)$ อยู่ใน $R[x]$ โดยที่มีลำดับขั้น 3 และ 4 ตามลำดับ แล้ว $f(x)\,g(x)$ อาจมีลำดับขั้น 8 ใน $R[x]$

..............ฉ) ถ้า R เป็นวง และ $f(x)$ และ $g(x)$ เป็นพหุนามที่มีลำดับขั้น 3 และ 4 ตามลำดับใน $R[x]$ แล้ว $f(x)\,g(x)$ จะต้องมีลำดับขั้น 7 เสมอ

..............ช) ถ้า F เป็นสนามย่อยของสนาม E และ $a \in E$ เป็นศูนย์ของ $f(x) \in F[x]$ แล้ว a เป็นศูนย์ของ $h(x) = f(x)\,g(x)$ สำหรับทุก ๆ $g(x) \in F[x]$

..............ซ) ถ้า F เป็นสนามย่อยของสนาม E และ $f(x) \in F[x]$ แล้วเซตของศูนย์ทั้งหมดของ $f(x)$ ใน E เป็นกลุ่มอุดมคติของ E

..............ฌ) ถ้า F เป็นสนามย่อยของสนาม E และ $\alpha \in E$ แล้วเซตของ $f(x)$ ทั้งหมดที่อยู่ใน $F[x]$ ซึ่ง $f(\alpha) = 0$ เป็นกลุ่มอุดมคติของ $F[x]$

2) จงหาผลบวกและผลคูณของพหุนาม $f(x) = 2x^3 + 4x^2 + 3x + 2$ และ $g(x) = 3x^4 + 2x + 4$ กำหนดให้ $f(x), g(x) \in Z_5[x]$

3) ให้ $F = E = Z_7$ จงหาค่าของแต่ละข้อต่อไปนี้สำหรับฟังก์ชันถ่ายแบบมูลฐาน

$\phi_2 : Z_7[x] \to Z_7$

ก) $Q_2(x^2 + 3)$

ข) $\phi_0(2x^3 - x^2 + 3x + 2)$

ค) $\phi_3[(x^4 + 2x)(x^3 - 3x^2 + 3)]$

ง) $\phi_5[(x^3 + 2)(4x^2 + 3)(x^7 + 3x^2 + 1)]$

4) พิจารณาฟังก์ชันถ่ายแบบมูลฐาน $\phi_5 : Q[x] \to R$ จงหาสมาชิก ๖ ตัวในส่วนกลางของ ϕ_5

5) จงหาศูนย์ทั้งหมดใน Z_5 ของพหุนาม $(x^5 + 3x^3 + x^2 + 2x) \in Z_5[x]$