บทที่ 2

ความรู้พื้นฐาน

ในบทนี้จะกล่าวถึงความรู้พื้นฐานเฉพาะที่จำเป็น เพื่อนำไปใช้ในบทที่ 3 และบทที่ 4 โดยจะกล่าวถึงนิยาม ทฤษฎีและตัวอย่างพอสังเขป สำหรับทฤษฎีและตัวอย่างบางตัวอย่างที่กล่าวถึงจะไม่แสดงวิธีการพิสูจน์ไว้ แต่จะระบุหนังสืออ้างอิงและหน้าของหนังสือที่มีบทพิสูจน์นั้น เพื่อให้ผู้ที่สนใจได้ค้นคว้าต่อไป

ความรู้พื้นฐานเกี่ยวกับนิยามของคำศัพท์บางคำ เช่น ความสัมพันธ์ (relation) ฟังก์ชัน (function) ฟังก์ชัน 1-1 (1-1 function) ฟังก์ชันไปบน (onto function) ฯลฯ ผู้เขียนไม่ได้ให้รายละเอียดไว้ แต่ผู้สนใจสามารถค้นคว้าได้จากตำราคณิตศาสตร์ทั่วไป สำหรับในบทนี้จะศึกษาตามหัวข้อต่อไปนี้

2.1 นิยามและคุณสมบัติบางประการของกรุป (group) ริง (ring) ฟิลด์ (field) และฟิลด์ขยาย (extension field)

2.2 เมตริกซ์ (matrix)

2.3 โพลิโนเมียล (polynomial) และจำนวนเชิงพีชคณิต (algebraic number)

สัญลักษณ์	ความหมาย
$\in$, $\notin$	เป็นสมาชิกของ, ไม่เป็นสมาชิกของ
$\subset$	สับเซต
$=$	เท่ากับ
$>$	มากกว่า

สัญลักษณ์	ความหมาย
$\geq$	มากกว่าหรือเท่ากับ
$<$	น้อยกว่า
$\leq$	น้อยกว่าหรือเท่ากับ
Z^+	เซตของจำนวนเต็มบวก
Z	เซตของจำนวนเต็ม
Q	เซตของจำนวนตรรกยะ
R	เซตของจำนวนจริง
C	เซตของจำนวนเชิงซ้อน
$f : X \dashrightarrow Y$	f เป็นฟังก์ชันจาก X ไปยัง Y
$F[x]$	เซตของโพลิโนเมียลในอินดิเทอร์มิเนท x ที่มีสัมประสิทธิ์อยู่ใน F
$P(\pi)$	อิมเมจของฟังก์ชัน P ที่มีโดเมนเป็น S_n และ $\pi \in S_n$
$P(\pi)_{i,j}$	สมาชิกในตำแหน่งแถวที่ i และหลักที่ j ของเมตริกซ์ $P(\pi)$
$M_n(Z)$	เซตของเมตริกซ์จำนวนเต็มขนาด $n \times n$
$M_n(Q)$	เซตของเมตริกซ์จำนวนตรรกยะขนาด $n \times n$
$M_n(R)$	เซตของเมตริกซ์จำนวนจริงขนาด $n \times n$
$M_n(C)$	เซตของเมตริกซ์จำนวนเชิงซ้อนขนาด $n \times n$
$\mathrm{diag} \langle a_1, \ldots, a_n \rangle$	เมตริกซ์ทแยงที่มีสมาชิกในแนวทแยงมุมเป็น $a_1, a_2, \ldots, a_n$
$\det A$, $\lvert A \rvert$	ดีเทอร์มินันท์ของเมตริกซ์ A

สัญลักษณ์	ความหมาย
$T_n(Z)$	เซตของเมตริกซ์ซิงกูลาร์ขนาด nxn ที่เป็นเมตริกซ์ไอเดมโพเทน

2.1 นิยามและคุณสมบัติบางประการของกรุ๊ป (group) ริง (ring) ฟิลด์ (field) และฟิลด์ขยาย (extension field)

<u>นิยาม 2.1.1</u> กำหนดเซต $S \neq \emptyset$ และ $\cdot$ เป็นฟังก์ชันจาก $S \times S$ ไปยัง S เรียก $\cdot$ ว่าเป็นการดำเนินทวิภาค (binary operation) ในเซต S

<u>นิยาม 2.1.2</u> กำหนดเซต $G \neq \emptyset$ และให้ $\oplus$ เป็นการดำเนินทวิภาคใน G จะเรียก $(G , \oplus)$ ว่าเป็นกรุ๊ป (group) เมื่อคุณสมบัติต่อไปนี้เป็นจริง

1. $a \oplus b \in G \quad , \forall a, b \in G$
2. $(a \oplus b) \oplus c = a \oplus (b \oplus c) \quad , \forall a,b,c \in G$
3. มีสมาชิก $e \in G$ ที่ $e \oplus a = a \oplus e = a, \quad \forall a \in G$
   เรียก e ว่าสมาชิกเอกลักษณ์ภายใต้ $\oplus$ บน G
4. $\forall a, a \in G$ จะมี $a^{-1} \in G$ ที่
   $a \oplus a^{-1} = e = a^{-1} \oplus a$
   เรียก a^{-1} ว่าอินเวอร์สของ a ภายใต้ $\oplus$

<u>ข้อตกลง</u> ต่อไปจะเขียน $a + b$ แทน $a \oplus b$

<u>ทฤษฎี 2.1.1</u> ให้ $(G , +)$ เป็นกรุ๊ปจะได้ว่าแต่ละสมาชิกใน G จะมีอินเวอร์สได้เพียงสมาชิกเดียว

<u>พิสูจน์</u> ดู [1] หน้า 9

<u>นิยาม 2.1.3</u> ให้ $(G , +)$ เป็นกรุป จะเรียก $(G , +)$ ว่าเป็น<u>กรุปสลับที่</u> (abelian group) ก็ต่อเมื่อ $a + b = b + a , \forall a,b \in G$

<u>นิยาม 2.1.4</u> กำหนด $R \neq \emptyset$ และให้ $+$ และ $.$ เป็นการดำเนินทวิภาคใน R จะเรียก $(R, +, .)$ ว่าเป็น<u>ริง</u> (ring) เมื่อคุณสมบัติต่อไปนี้เป็นจริง

1. $(R, +)$ เป็นกรุปสลับที่
2. $a.b \in R, \forall a,b \in R$
3. $(a.b).c = a.(b.c), \forall a,b,c \in R$
4. $a.(b+c) = a.b + a.c$ และ
   $(b+c).a = b.a + c.a , \forall a,b,c \in R$

<u>ข้อตกลง</u> ต่อไปจะเขียน ab แทน $a.b$ และใช้ 0 แทนสมาชิกเอกลักษณ์ภายใต้ $+$ บน R

<u>นิยาม 2.1.5</u> ให้ $(R, +, .)$ เป็นริง จะเรียก $(R, +, .)$ ว่าเป็น<u>ริงที่มีเอกลักษณ์</u> (ring with identity) เมื่อมี $e' \in G$ ที่ $e'a = a = ae' , \forall a \in R$ และเรียก e' ว่าสมาชิกเอกลักษณ์ภายใต้ $.$ บน R

<u>นิยาม 2.1.6</u> ให้ $(R, +, .)$ เป็นริง จะเรียก $(R, +, .)$ ว่าเป็น<u>ริงสลับที่</u> (commutative ring) เมื่อ $ab = ba, \forall a,b \in R$

<u>ตัวอย่าง 2.1.1</u> ให้ Z เป็นเซตของจำนวนเต็ม จะได้ว่า $(Z, +, .)$ เป็นริงสลับที่ที่มีเอกลักษณ์

<u>นิยาม 2.1.7</u> ให้ $F \neq \emptyset$ และ $+, .$ เป็นการดำเนินทวิภาคใน F จะเรียก $(F, +, .)$ ว่าเป็น<u>ฟิลด์</u> (field) เมื่อคุณสมบัติต่อไปนี้เป็นจริง

1. $(F, +)$ เป็นกรุปสลับที่
2. $(F - \{0\}, .)$ เป็นกรุปสลับที่

3. $a(b+c) = ab + ac$ และ

$(b+c)a = ba + ca, \quad \forall a,b,c \in F$

<u>ตัวอย่าง 2.1.2</u> ให้ R เป็นเซตของจำนวนจริง จะได้ว่า $(R, +, .)$ เป็นฟิลด์

<u>ตัวอย่าง 2.1.3</u> ให้ C เป็นเซตของจำนวนเชิงซ้อน จะได้ว่า $(C, +, .)$ เป็นฟิลด์

<u>ตัวอย่าง 2.1.4</u> ให้ Q เป็นเซตของจำนวนตรรกยะ จะได้ว่า $(Q, +, .)$ เป็นฟิลด์

<u>นิยาม 2.1.8</u> ให้ $X \neq \emptyset$ การจัดลำดับบน X (permutaion of X) คือ ฟังก์ชัน 1-1 จาก X ไปบน X
ดังนั้น π เป็นการจัดลำดับบน X ก็ต่อเมื่อ $\pi : X \rightarrow X$ เป็นฟังก์ชัน 1-1 และไปบน และเขียนแทนด้วยสัญลักษณ์

$$\pi = \begin{pmatrix} \ldots & x & \ldots \\ \ldots & \pi(x) & \ldots \end{pmatrix}$$

<u>นิยาม 2.1.9</u> ให้ $X = \{1,2,3,\ldots,n\}$ จะเรียกเซตของการจัดลำดับทั้งหมดบนเซต X กับการคอมโพสิต ว่า<u>กรุปสมมาตรที่มีขนาด</u> n (symmetric group of degree n) และ ใช้แทนด้วยสัญลักษณ์ $(S_n, \circ)$

<u>นิยาม 2.1.10</u> ให้ π เป็นการจัดลำดับบนเซต $X = \{1,2,\ldots,n\}$ จะเรียก π ว่าเป็น <u>ไซเคิล</u> (cycle) ความยาว k ก็ต่อเมื่อ $\pi(a_1) = a_2$, $\pi(a_2) = a_3, \ldots, \pi(a_{k-1}) = a_k$, $\pi(a_k) = a_1$
โดยที่ $a_r \in X$, $r = 1,2,\ldots,k$ และ $a_i \neq a_j$, $i \neq j$
และ $\pi(x) = x$, $x \in X$ และ $x \notin \{a_1,a_2,\ldots,a_k\}$
เขียนแทนไซเคิลความยาว k ด้วย $\pi = (a_1\ a_2\ \ldots\ a_k)$

จากนิยาม 2.1.10 จะเห็นว่า

$$a_2 = \pi(a_1)$$

$$a_3 = \pi(a_2) = \pi(\pi(a_1)) = (\pi o \pi)(a_1) = \pi^2(a_1)$$

$$a_4 = \pi(a_3) = \pi(\pi^2(a_1)) = (\pi o \pi^2)(a_1) = \pi^3(a_1)$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$a_n = \pi(a_{k-1}) = \pi(\pi^{k-2}(a_1)) = (\pi o \pi^{k-2})(a_1) = \pi^{k-1}(a_1)$$

$$a_1 = \pi(a_k) = \pi(\pi^{k-1}(a_1)) = (\pi o \pi^{k-1})(a_1) = \pi^k(a_1)$$

เนื่องจาก $a_i \neq a_j, \forall i,j = 1,2,\ldots,k$

ทำให้ $\pi(a_i) \neq \pi(a_j), \forall i \neq j$ และ $a_i \neq \pi(a_i), \forall i = 1,\ldots,k$

ในทำนองเดียวกัน $a_i \neq a_{\pi^k(i)}, \forall k = 1,\ldots,r, \forall i = 1,\ldots,k$

<u>นิยาม 2.1.11</u> ให้ F เป็นฟิลด์ จะเรียก E ว่าเป็น<u>ฟิลด์ขยาย</u> (extension field) ของ F ถ้า $F \subset E$ และ E เป็นฟิลด์

เรียกฟิลด์ขยาย E ว่าเป็น <u>ฟิลด์ขยายแท้</u> (proper **extension field**) ของ F ถ้า $F \neq E$

<u>ตัวอย่าง 2.1.5</u> ให้ R เป็นเซตจำนวนจริง และ Q เป็นเซตของจำนวนตรรกยะ

โดยตัวอย่าง 2.1.2 จะได้ว่า (R, +, .) เป็นฟิลด์

และโดยตัวอย่าง 2.1.4 จะได้ว่า (Q, +, .) เป็นฟิลด์

ดังนั้นโดยนิยาม 2.1.11 จะได้ว่า

R เป็นฟิลด์ขยายของ Q

<u>ตัวอย่าง 2.1.6</u> ให้ $Q(\sqrt{2}) = \{ x+y\sqrt{2} \mid x,y \in Q \}$

และให้ $a,b \in Q(\sqrt{2})$ โดยที่ $a = p+q\sqrt{2}$, $b = s+t\sqrt{2}$,

$p,q,s,t \in Q$ นิยามการบวกและคูณใน $Q(\sqrt{2})$ ดังนี้

$$a+b = (p+q\sqrt{2}) + (s+t\sqrt{2}) = (p+s) + (q+t)\sqrt{2}$$

$$a\,b = (p+q\sqrt{2})(s+t\sqrt{2})$$

$$= ps+2qt + (qs+pt)\sqrt{2}$$

<u>(i) จะแสดงว่า $(Q(\sqrt{2}), +)$ เป็นกรุปสลับที่</u>

ให้ $a,b,c \in Q(\sqrt{2})$ โดยที่

$$a = p+q\sqrt{2},\ b = s+t\sqrt{2},\ c = u+v\sqrt{2}$$

เมื่อ $p,q,s,t,u,v \in Q$

1. พิจารณา $a + b$ โดยนิยามจะได้ว่า

$$a + b = (p+s) + (q+t)\sqrt{2}$$

จาก $p,q,s,t \in Q$ ดังนั้น $p+s, q+t \in Q$

จะได้ว่า $a + b \in Q(\sqrt{2})$

2. พิจารณา $(a+b)+c = ((p+q\sqrt{2}) + (s+t\sqrt{2}))$

$$+ (u+v\sqrt{2})$$

$$= ((p+s) + (q+t)\sqrt{2})$$

$$+ (u+v\sqrt{2})$$

$$= ((p+s) + u)$$

$$+ ((q+t) + v)\sqrt{2}$$

$$= (p+(s+u)) + (q+(t+v))\sqrt{2}$$

$$= (p+q\sqrt{2}) + ((s+u) + (t+v)\sqrt{2})$$

$(a+b)+c = (p+q\sqrt{2})$

$+((s+t\sqrt{2})+(u+v\sqrt{2}))$

$= a+(b+c)$

3. จาก $0 = 0 + 0\sqrt{2}$ ดังนั้นจะได้ว่า $0 \in Q(\sqrt{2})$

พิจารณา $a + 0 = (p+q\sqrt{2}) + (0+0\sqrt{2})$

จะได้ว่า $a + 0 = p+q\sqrt{2} = a$

และ $0 + a = p+q\sqrt{2} = a$

ดังนั้นจะได้ว่า $a + 0 = a = 0 + a$

แสดงว่า 0 เป็นสมาชิกเอกลักษณ์ภายใต้ + บน $Q(\sqrt{2})$

4. จาก $a = p+q\sqrt{2} \in Q(\sqrt{2})$

ดังนั้น $-a = -(p+q\sqrt{2}) = -p-q\sqrt{2}$

จะเห็นว่า $-p, -q \in Q$ $\therefore -a = -p-q\sqrt{2} \in Q(\sqrt{2})$

พิจารณา $a+(-a) = (p+q\sqrt{2}) + (-p-q\sqrt{2})$

ดังนั้น $a+(-a) = (p+(-p)) + (q+(-q))\sqrt{2} = 0$

และ $(-a) + a = (-p-q\sqrt{2}) + (p+q\sqrt{2})$

ดังนั้น $(-a) + a = ((-p) + p) + ((-q) + q)\sqrt{2} = 0$

ดังนั้นจะได้ว่าสำหรับ $a \in Q(\sqrt{2})$ จะมี $-a \in Q(\sqrt{2})$

ที่ $a + (-a) = 0 = (-a) + a$

5. พิจารณา $a+b = (p+q\sqrt{2}) + (s+t\sqrt{2})$

$= (p+s) + (q+t)\sqrt{2}$

$= (s+p) + (t+q)\sqrt{2}$

$= (s+t\sqrt{2}) + (p+q\sqrt{2})$

ดังนั้น $a+b = b+a$

จาก 1-5 จะได้ว่า $(Q(\sqrt{2}), +)$ เป็นกรุปสลับที่

(ii) จะแสดงว่า $(Q(\sqrt{2})-\{0\}, \cdot)$ เป็นกรุปสลับที่

ให้ $a,b,c \in Q(\sqrt{2}) - \{0\}$ โดยที่

$a = p+q\sqrt{2}$, $b = s+t\sqrt{2}$, $c = u+v\sqrt{2}$

เมื่อ $p,q,s,t,u,v \in Q$

1. พิจารณา $ab = (p+q\sqrt{2})(s+t\sqrt{2})$

$= ps+2qt + (pt+qs)\sqrt{2}$

จาก $p,q,s,t \in Q$ ดังนั้น $ps+2qt, pt+qs \in Q$

จะได้ว่า $ab \in Q(\sqrt{2})$

2. พิจารณา $a(bc) = (p+q\sqrt{2})((s+t\sqrt{2})(u+v\sqrt{2}))$

$= (p+q\sqrt{2})(su+2tv + (tu + sv)\sqrt{2})$

$= p(su + 2tv) + 2q(tu + sv)$

$+ (q(su+ 2tv) + p(tu + sv))\sqrt{2}$

$a(bc) = psu + 2ptv + 2qtu + 2qsv$

$+ (qsu + 2qtv + ptu + psv)\sqrt{2}$ (1)

และ $(ab)c = ((p+q\sqrt{2})(s+t\sqrt{2}))(u+v\sqrt{2})$

$= ((ps + 2qt) + (qs + pt)\sqrt{2})(u+v\sqrt{2})$

$= (ps + 2qt)u + (qs + pt)2v$

$+ ((qs + pt)u + (ps + 2qt)v)\sqrt{2}$

ดังนั้น $(ab)c = psu + 2qtu + 2qsv + 2ptv$

$+ (qsu + ptu + psv + 2qtv)\sqrt{2}$ (2)

จาก (1) และ (2) จะได้ว่า $a(bc) = (ab)c$

3. จาก $1 = 1 + 0\sqrt{2}$ ดังนั้น $1 \in Q(\sqrt{2}) - \{0\}$

พิจารณา $a1 = (p+q\sqrt{2})(1 + 0\sqrt{2})$

จะได้ว่า $a1 = p+q\sqrt{2} = a$

และ $1a = p+q\sqrt{2} = a$

ดังนั้นจะได้ว่า $a1 = a = 1a$

แสดงว่า 1 เป็นสมาชิกเอกลักษณ์ภายใต้ . บน $Q(\sqrt{2})$

4. จาก $a = p+q\sqrt{2} \in Q(\sqrt{2}) - \{0\}$

ดังนั้น $\frac{1}{a} = \frac{1}{p+q\sqrt{2}}$, $p+q\sqrt{2} \neq 0$

จาก $p+q\sqrt{2} \neq 0$ ทำให้ได้ว่า $p \neq 0$ หรือ $q \neq 0$

และจะได้ว่า $p-q\sqrt{2} \neq 0$

พิจารณา $\frac{1}{a} = (\frac{1}{p+q\sqrt{2}})(\frac{p-q\sqrt{2}}{p-q\sqrt{2}})$, $p-q\sqrt{2} \neq 0$

เนื่องจาก $p+q\sqrt{2} \neq 0$ และ $p-q\sqrt{2} \neq 0$ ทำให้

$(p+q\sqrt{2})(p-q\sqrt{2}) \neq 0$ นั่นคือ $p^2-2q^2 \neq 0$

ดังนั้น $\frac{1}{a} = \frac{p-q\sqrt{2}}{p^2-2q^2} = \frac{p}{p^2-2q^2} + \left(\frac{-q}{p^2-2q^2}\right)\sqrt{2}$

เนื่องจาก $\frac{p}{p^2-2q^2}$, $\frac{-q}{p^2-2q^2} \varepsilon Q$ ดังนั้น

$$\frac{1}{a} = \frac{p}{p^2-2q^2} + \left(\frac{-q}{p^2-2q^2}\right)\sqrt{2} \;\varepsilon\; Q(\sqrt{2})-\{0\}$$

จะเห็นว่า $a(\frac{1}{a}) = (p+q\sqrt{2})\frac{(p-q\sqrt{2})}{p^2-2q^2} = 1$

และ $(\frac{1}{a})a = \left(\frac{p-q\sqrt{2}}{p^2-2q^2}\right)(p+q\sqrt{2}) = 1$

แสดงว่า $a(\frac{1}{a}) = 1 = (\frac{1}{a})a$

ดังนั้น สำหรับ $a \;\varepsilon\; Q(\sqrt{2})-\{0\}$

จะมี $\frac{1}{a} \;\varepsilon\; Q(\sqrt{2})-\{0\}$

ที่ $a(\frac{1}{a}) = 1 = (\frac{1}{a})a$

5. พิจารณา $ab = (p+q\sqrt{2})(s+t\sqrt{2})$

$= (ps+2qt) + (qs+pt)\sqrt{2}$

$= (sp+2tq) + (sq+tp)\sqrt{2}$

$= (s+t\sqrt{2})(p+q\sqrt{2})$

ดังนั้น $ab = ba$

จาก 1-5 จะได้ว่า $(Q(\sqrt{2}) - \{0\}, \cdot)$ เป็นกรุปสลับที่

(iii) ให้ $a, b, c \in Q(\sqrt{2})$ โดยที่

$a = p+q\sqrt{2}$, $b = s+t\sqrt{2}$, $c = u+v\sqrt{2}$,

เมื่อ $p, q, s, t, u, v \in Q$

พิจารณา $a(b+c) = (p+q\sqrt{2})((s+t\sqrt{2}) + (u+v\sqrt{2}))$

$= (p+q\sqrt{2})((s+u) + (t+v)\sqrt{2})$

$= (p(s+u) + 2q(t+v))$

$+ (q(s+u) + p(t+v))\sqrt{2}$

ดังนั้น $a(b+c) = ps+pu + 2qt+2qv$

$+ (qs+qu + pt + pv)\sqrt{2}$ (1)

และ $ab+ac = (p+q\sqrt{2})(s+t\sqrt{2}) + (p+q\sqrt{2})(u+v\sqrt{2})$

$= ps+2qt + (qs+pt)\sqrt{2}$

$+ pu+2qv + (qu+pv)\sqrt{2}$ (2)

จะเห็นว่า (1) = (2) ดังนั้น $a(b+c) = ab+ac$

ในทำนองเดียวกันจะได้ว่า $(b+c)a = ba+ca$

จาก (i),(ii),(iii) และนิยาม 2.1.7 จะได้ว่า

$(Q(\sqrt{2}), +, \cdot)$ เป็นฟิลด์ (*)

และจากตัวอย่าง 2.1.4 ได้ว่า $(Q, +, \cdot)$ เป็นฟิลด์ (**)

ให้ $x \in Q$

เนื่องจาก $x = x + 0\sqrt{2}$

และ $x + 0\sqrt{2} \in Q(\sqrt{2})$

เพราะฉะนั้น $x \in Q(\sqrt{2})$

แสดงว่า $Q \subset Q(\sqrt{2})$ (***)

ดังนั้นจาก (*),(**),(***) และนิยาม 2.1.11 จะได้

$Q(\sqrt{2})$ เป็นฟิลด์ขยายของ Q

2.2 เมตริกซ์ (matrix)

นิยาม 2.2.1 เมตริกซ์คือกลุ่มของจำนวน ซึ่งเขียนเรียงกันตามแนวนอนและแนวตั้งอย่างเป็นระเบียบ ในรูปสี่เหลี่ยมมุมฉากภายใต้เครื่องหมาย [ ] หรือ ( )

รูปทั่วไปของเมตริกซ์ คือ

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}_{m \times n}$$

เรียกเมตริกซ์ที่มี m แถวและ n หลักว่า<u>เมตริกซ์ขนาด mxn</u> (m by n matrix)

เรียก a_{ij} ว่า<u>สมาชิก</u> (entry) ของเมตริกซ์ ซึ่งอยู่ในแถวที่ i และหลักที่ j

เพื่อความสะดวกเขียนสัญลักษณ์แทนเมตริกซ์ A ได้ดังนี้

$$A = \left[a_{ij}\right]_{mxn}$$

<u>นิยาม 2.2.2</u> ถ้า $A = \left[a_{ij}\right]_{mxn}$ และ $B = \left[b_{ij}\right]_{mxn}$ แล้ว $A = B$ ก็ต่อเมื่อ $a_{ij} = b_{ij}$, $\forall i = 1,2,\ldots,m$ และ $j = 1,2,\ldots,n$

<u>นิยาม 2.2.3</u> ถ้า $A = \left[a_{ij}\right]_{mxn}$ และ $B = \left[b_{ij}\right]_{mxn}$ <u>เมตริกซ์ A + B</u> คือเมตริกซ์ $C = \left[c_{ij}\right]_{mxn}$ ซึ่ง $c_{ij} = a_{ij} + b_{ij}$ โดยที่ $i = 1,2,\ldots, m$ และ $j = 1,2,\ldots, n$

<u>นิยาม 2.3.4</u> ถ้า $A = \left[a_{ij}\right]_{mxn}$ และ $r \in R$ แล้ว <u>ผลคูณสเกลาร์ของ A โดย r</u> เขียนแทนด้วย rA คือ เมตริกซ์ $C = \left[c_{ij}\right]_{mxn}$ ซึ่ง $c_{ij} = ra_{ij}$ โดยที่ $i = 1,2,\ldots, m$ และ $j = 1,2,\ldots, n$

<u>ทฤษฎี 2.2.1</u> ถ้า $A = \left[a_{ij}\right]_{mxn}$, $B = \left[b_{ij}\right]_{mxn}$ และ $r,s \in R$ แล้ว

1. $(r+s)A = rA + sA$
2. $r(A+B) = rA + rB$

พิสูจน์ ดู [7] หน้า 23

ทฤษฎี 2.2.2 ถ้า $A = [a_{ij}]_{m \times n}$, $B = [b_{ij}]_{m \times n}$ และ $C = [c_{ij}]_{m \times n}$ แล้ว

1. $A + B = B + A$
2. $(A+B)+C = A+(B+C)$

พิสูจน์ ดู [7] หน้า 18

นิยาม 2.2.5 ถ้า $A = [a_{ij}]_{m \times n}$ และ $B = [b_{ij}]_{n \times p}$ แล้ว ผลคูณของเมตริกซ์ A และ B จะมีขนาด $m \times p$ และเขียนแทนด้วย AB โดยที่

$$AB = C = [c_{ij}]_{m \times p} \text{ ซึ่ง } c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$$

โดยที่ $i = 1,2,\ldots,m$, $j = 1,2,\ldots,p$.

ทฤษฎี 2.2.3 ถ้า $A = [a_{ij}]_{m \times n}$, $B = [b_{ij}]_{n \times p}$, $C = [c_{ij}]_{p \times q}$ และ $r \in R$ แล้ว

1. $r(AB) = A(rB)$
2. $A(BC) = (AB)C$
3. $A(B+C) = AB+AC$
4. $(B+C)A = BA+CA$

พิสูจน์ ดู [7] หน้า 19, 20 และ 22

<u>นิยาม 2.2.6</u> ถ้า $A = \left[a_{ij}\right]_{m \times n}$ จะเรียก A ว่าเป็น<u>เมตริกซ์ศูนย์</u> (zero matrix) ก็ต่อเมื่อ $a_{ij} = 0$

โดยที่ $i = 1, 2, \ldots, m$ และ $j = 1, 2, \ldots, n$

แทนเมตริกซ์ศูนย์ด้วย $0 = \left[0_{ij}\right]_{m \times n}$ หรือ $[0]$

<u>นิยาม 2.2.7</u> จะเรียกเมตริกซ์ A ว่าเป็น<u>เมตริกซ์จัตุรัส</u> (square matrix) ที่มีขนาด n ก็ต่อเมื่อเมตริกซ์ A มี n แถวและ n หลัก

<u>นิยาม 2.2.8</u> ให้ $I_n = \left[e_{ij}\right]_{n \times n}$ โดยที่ $e_{ij} = \begin{cases} 1 & \text{เมื่อ } i = j \\ 0 & \text{เมื่อ } i \neq j \end{cases}$

จะเรียก I_n ว่า<u>เมตริกซ์เอกลักษณ์</u> (identity matrix)

ในบางครั้งอาจเขียนแทนด้วย I

<u>นิยาม 2.2.9</u> จะเรียกเมตริกซ์จัตุรัส A ว่า<u>อินเวอร์ทิเบิล</u> (invertible) หรือ<u>นอนซิงกูลาร์</u> (nonsingular) ก็ต่อเมื่อมีเมตริกซ์ B ซึ่งทำให้

$$AB = I = BA$$

ถ้า A เป็นเมตริกซ์นอนซิงกูลาร์แล้วจะเรียกเมตริกซ์ B ซึ่งทำให้ $AB = I = BA$ ว่า เป็น<u>อินเวอร์สของเมตริกซ์ A</u> (inverse of A) และเขียนแทนด้วยสัญลักษณ์ A^{-1}

<u>หมายเหตุ</u> อาจกล่าวได้ว่าเมตริกซ์นอนซิงกูลาร์คือเมตริกซ์ที่มีอินเวอร์ส และในกรณีที่เมตริกซ์จัตุรัส A ไม่มีอินเวอร์สจะเรียก A ว่าเป็น<u>เมตริกซ์ซิงกูลาร์</u> (singular matrix)

<u>ข้อตกลง</u> ถ้า $A = \left[a_{ij}\right]_{nxn}$ **แล้ว** กำหนดรูปยกกำลังของ A ดังนี้

$$A^2 = A.A\ ,\ A^3 = A^2.A\ ,\ \ldots,\ A^n = A^{n-1}.A$$

<u>ตัวอย่าง 2.2.1</u> ให้ $M_n(Z)$ เป็นเซตของเมตริกซ์จำนวนเต็มขนาด nxn จะได้ว่า $(M_n(Z),+,.)$ เป็นริงที่มีสมาชิกเอกลักษณ์

<u>ตัวอย่าง 2.2.2</u> ให้ $M_n(Q)$ เป็นเซตของเมตริกซ์จำนวนตรรกยะขนาด nxn จะได้ว่า $(M_n(Q),+,.)$ เป็นริงที่มีสมาชิกเอกลักษณ์

<u>ตัวอย่าง 2.2.3</u> ให้ $M_n(R)$ เป็นเซตของเมตริกซ์จำนวนจริงขนาด nxn จะได้ว่า $(M_n(R),+,.)$ เป็นริงที่มีสมาชิกเอกลักษณ์

<u>ตัวอย่าง 2.2.4</u> ให้ $M_n(C)$ เป็นเซตของเมตริกซ์จำนวนเชิงซ้อนขนาด nxn จะได้ว่า $(M_n(C),+,.)$ เป็นริงที่มีสมาชิกเอกลักษณ์

<u>ทฤษฎี 2.2.4</u> ถ้า $A = \left[a_{ij}\right]_{nxn}$ เป็นเมตริกซ์นอนซิงกูลาร์ $B = \left[b_{ij}\right]_{nxn}$, $C = \left[c_{ij}\right]_{nxn}$ และ $AB = AC$ แล้ว $B = C$

<u>พิสูจน์</u> ดู [6] หน้า 72

<u>ทฤษฎี 2.2.5</u> ถ้า $A = \left[a_{ij}\right]_{nxn}$ เป็นเมตริกซ์ที่มีสมาชิกอย่างน้อยแถว(หลัก)ใดแถว(หลัก)หนึ่งเป็นศูนย์ทั้งหมด แล้ว A เป็นเมตริกซ์ซิงกูลาร์

<u>พิสูจน์</u> ดู [5] หน้า 23

<u>นิยาม 2.2.10</u> จะเรียกเมตริกซ์จัตุรัส A ขนาด nxn ว่าเป็น<u>เมตริกซ์สเกลาร์</u> ก็ต่อเมื่อ $A = rI$ สำหรับบาง $r \in R$ และ I เป็นเมตริกซ์เอกลักษณ์ขนาด n

<u>นิยาม 2.2.11</u> จะเรียกเมตริกซ์จัตุรัส $A = [a_{ij}]_{n\times n}$ ว่าเป็น<u>เมตริกซ์ทแยง</u> (diagonal matrix) ก็ต่อเมื่อ $a_{ij} = 0$ สำหรับ $i \neq j$ เรียก $a_{11}, a_{22}, \ldots, a_{nn}$ ของ A ว่าสมาชิกในแนวทแยง ใช้สัญลักษณ์ $[a]$ แทนเมตริกซ์ทแยงใด ๆ และใช้สัญลักษณ์ $\text{diag}\langle a_1, \ldots, a_n\rangle$ แทนเมตริกซ์ทแยงที่

$a_i = a_{ii}$, $\forall i = 1,2,\ldots, n$

<u>ทฤษฎี 2.2.6</u> ให้ $A = \text{diag}\langle a_1, \ldots, a_n\rangle$ และ $B = \text{diag}\langle b_1, \ldots, b_n\rangle$ จะได้ว่า AB เป็นเมตริกซ์ทแยงขนาด $n\times n$ โดยที่

$AB = \text{diag}\langle a_1b_1, a_2b_2, \ldots, a_nb_n\rangle$

<u>พิสูจน์</u> ดู [8] หน้า 19

<u>นิยาม 2.2.12</u> จะเรียกเมตริกซ์ A ว่า<u>เมตริกซ์ไอเดมโพเทนท์</u> (idempotent matrix) ก็ต่อเมื่อ $A^2 = A$

<u>ข้อสังเกต 2.2.1</u> ให้ A เป็นเมตริกซ์ไอเดมโพเทนท์ขนาด $n\times n$ จะได้ว่า

$A^m = A, \ m \in Z^+$

<u>นิยาม 2.2.13</u> จะเรียกเมตริกซ์ A ว่า<u>เมตริกซ์อินโวลูทอรี</u> (involutory matrix) ก็ต่อเมื่อ $A^2 = I$

<u>นิยาม 2.2.14</u> ถ้า $A = [a_{ij}]_{m\times n}$ แล้ว<u>ทรานสโพส</u> (transpose) ของเมตริกซ์ A เขียนแทนด้วย $A^t = [a^t_{ij}]_{n\times m}$ หมายถึง เมตริกซ์ขนาด $n\times m$ ซึ่งกำหนดโดย $a^t_{ij} = a_{ji}$ สำหรับ $i = 1,2,\ldots, n$ และ $j = 1,2, \ldots, m$

<u>ทฤษฎี 2.2.7</u> ถ้า $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ เป็นเมตริกซ์ที่มีขนาด 2x2 เรียก A ว่าเป็นเมตริกซ์นอนซิงกูลาร์ ก็ต่อเมื่อ $ad - bc \neq 0$

<u>พิสูจน์</u> ดู [7] หน้า 115

<u>นิยาม 2.2.15</u> ให้ $A = [a_{ij}]_{mxn}$ เรียก A ว่า<u>เมตริกซ์พาร์ทิชัน</u> (partitioned matrix) ก็ต่อเมื่อ A ถูกแบ่งโดยเส้นตรงในแนวตั้งหรือแนวนอน โดยส่วนที่ถูกแบ่งแต่ละส่วนเป็นเมตริกซ์ย่อย (submatrix) ของ A

ใช้สัญลักษณ์แทนเมตริกซ์ย่อยของ A ด้วย A_{ij}

<u>ทฤษฎี 2.2.8</u> ให้ $A = [a_{ij}]_{mxn}$ และ $B = [b_{ij}]_{nxp}$

และกำหนดเมตริกซ์พาร์ทิชันของ A และ B คือ

$$A = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1s} \\ A_{21} & A_{22} & \cdots & A_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ A_{r1} & A_{r2} & \cdots & A_{rs} \end{bmatrix} \quad B = \begin{bmatrix} B_{11} & B_{12} & \cdots & B_{1t} \\ B_{21} & B_{22} & \cdots & B_{2t} \\ \vdots & \vdots & \ddots & \vdots \\ B_{s1} & B_{s2} & \cdots & B_{st} \end{bmatrix}$$

โดยที่ $m = m_1+\ldots+m_r,\ n = n_1+\ldots+n_s,\ p = p_1+\ldots+p_t$

เมื่อ m_i = จำนวนแถวของ A_{ij}, $\forall i = 1,2,\ldots,r,\ \forall j = 1,2,\ldots,s,$

n_j = จำนวนหลักของ A_{ij} = จำนวนแถวของ B_{ij},

$\forall i,j = 1,2,\ldots,s$

p_j = จำนวนหลักของ B_{ij} , $\forall i = 1,2,\ldots,s,$

$\forall j = 1,\ldots, t$

จะได้ว่า 1. $\sum_{k=1}^{s} A_{ik}B_{kj}$ หาค่าได้และมีขนาดเท่ากับ $m_i x p_j$

สำหรับ $i = 1,2,\ldots, r$ และ $j = 1,2,\ldots,t$

2. ถ้า $C = [C_{ij}]_{mxp}$ โดยที่ C_{ij} เป็นเมตริกซ์ย่อย

ที่ $C_{ij} = \sum_{k=1}^{s} A_{ik}B_{kj}$ จะได้ว่า $C = AB$

<u>พิสูจน์</u> ดู [2] หน้า 50

<u>นิยาม 2.2.16</u> ให้ $C = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$ เป็นเมตริกซ์ขนาด 2x2

<u>ดีเทอร์มินันท์</u> (determinant) ของ C แทนด้วย det(C)

หรือ $|C|$ และ

$$\det(C) = c_{11}c_{22} - c_{21}c_{12}$$

<u>นิยาม 2.2.17</u> ให้ $A = [a_{ij}]_{nxn}$ เรียกเมตริกซ์ที่เกิดจากการตัดแถวที่ i

และหลักที่ j ของเมตริกซ์ A ว่า <u>ไมเนอร์</u> (minor)

ของสมาชิก a_{ij} ของ A เขียนสัญลักษณ์แทนด้วย M_{ij}

<u>นิยาม 2.2.19</u> ให้ $A = [a_{ij}]_{nxn}$ แล้ว det (A) กำหนดดังนี้

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det M_{ij} \ , \ i = 1,\ldots,n$$

<u>ทฤษฎี 2.2.9</u> ถ้า $A = [a_{ij}]_{nxn}$ จะได้ว่า A เป็นเมตริกซ์นอนซิงกูลาร์

ก็ต่อเมื่อ $\det A \neq 0$

<u>พิสูจน์</u> ดู [7] หน้า 137

<u>ทฤษฎี 2.2.10</u> ให้ $A = [a_{ij}]_{n\times n}$ ถ้า A มีสมาชิกแถว (หลัก) ใดแถว (หลัก) หนึ่งเป็นศูนย์ทั้งหมด แล้ว $\det A = 0$

<u>พิสูจน์</u> ดู [7] หน้า 125

2.3. <u>โพลิโนเมียล (polynomial) และจำนวนเชิงพีชคณิต (algebraic number)</u>

<u>นิยาม 2.3.1</u> ให้ F เป็นฟีลด์ (field) และให้นิพจน์ (expression)

$$a_0x^n + a_1x^{n-1} + \dots + a_n = \sum_{i=0}^{n} a_ix^{n-i} \qquad (1)$$

จะเรียก (1) ว่า <u>โพลิโนเมียล</u> (polynomial) ใน<u>อินดีเทอร์มิเนท</u> (indeterminate) x เมื่อ n เป็นจำนวนเต็มบวก

และ $a_i \in F, \ \forall i = 0, 1, \dots, n$

และนิยมเขียนแทนด้วย $f(x), g(x), p(x), \dots$

ดังนั้น (1) อาจเขียนได้เป็น $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$

จะเรียก (1) ว่า<u>โพลิโนเมียลศูนย์</u> (zero polynomial)

เมื่อ n เป็นจำนวนเต็มบวก $a_i \in F$ และ

$a_i = 0, \ \forall i = 0, \dots, n$

จะเรียก (1) ว่า <u>โพลิโนเมียลคงที่</u> (constant polynomail)

เมื่อ n เป็นจำนวนเต็มบวก, $a_i \in F, \forall i = 0, 1, \dots, n$

และ $a_i = 0, \ \forall i = 0, \dots, n-1$

<u>นิยาม 2.3.2</u> ถ้า $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ ไม่เป็นโพลิโนเมียลศูนย์ และ $a_0 \neq 0$ แล้ว จะเรียก n ว่าเป็น<u>อันดับ</u> (degree) ของ f(x) เขียนแทนด้วย $\deg f(x) = n$ ถ้า f(x) เป็นโพลิโนเมียลคงที่ที่ไม่เท่ากับศูนย์ จะเรียก 0 ว่าเป็น <u>อันดับ</u> (degree) ของ f(x) เขียนแทนด้วย $\deg f(x) = 0$

<u>นิยาม 2.3.3</u> ถ้า $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ จะเรียก f(x) ว่าเป็น <u>โมนิคโพลิโนเมียล</u> (monic polynomial) เมื่อ $a_0 = 1$

<u>นิยาม 2.3.4</u> ให้ F เป็นฟิลด์ และให้โพลิโนเมียล $f(x) = \sum_{i=0}^{n} a_i x^{n-i}$,

$a_i \in F, \quad \forall i = 0, 1, \ldots, n$

และกำหนดฟังก์ชัน $f : F \longrightarrow F$ โดยกำหนด

$$f(d) = \sum_{i=0}^{n} a_i d^{n-i}, \quad d \in F$$

จะเรียก f(d) ว่า<u>ฟังก์ชันโพลิโนเมียล</u> (polynomial function)

<u>นิยาม 2.3.5</u> ให้ f(x) เป็นโพลิโนเมียลอันดับที่ n, $n \in Z^+$ จะเรียก $f(x) = 0$ ว่า <u>สมการโพลิโนเมียลอันดับ n</u> (polynomial equation degree n) และ เรียก $d \in F$ ว่า <u>รากของสมการ</u> ถ้า $f(d) = 0$

<u>หมายเหตุ</u> 1. สมการโพลิโนเมียลอันดับ 2 มีชื่อเรียกว่าสมการควอดราติค (quadratic equation) เช่น

$$x^2 + 3x + 1 = 0 \;, \; x^2 + \sqrt{3} = 0$$

2. สมการโพลิโนเมียลอันดับ 3 มีชื่อว่าสมการคิวบิค (cubic equation) เช่น

$$x^3 + 10x^2 - \sqrt{3}x + 1 = 0, \quad x^3 - x^2 = 0, \quad x^3 + 3x - 4 = 0$$

<u>นิยาม 2.3.6</u> ให้ F เป็นฟิลด์ <u>เซตของโพลิโนเมียลในอินดิเทอร์มิเนท x ที่มีสัมประสิทธิ์อยู่ใน F</u> จะเขียนแทนด้วย $F[x]$

<u>ตัวอย่าง 2.3.1</u> ให้ R เป็นเซตของจำนวนจริง จะได้ว่า

$p(x) = x^3 - \sqrt{3}x + 5 \in R[x]$ เมื่อ $R[x]$ เป็นเซตของโพลิโนเมียลในอินดิเทอร์มิเนท x ที่มีสัมประสิทธิ์อยู่ใน R

<u>นิยาม 2.3.7</u> เรียก $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n, \ a_0 \neq 0$

และ $g(x) = b_0x^n + b_1x^{n-1} + \ldots + b_n, \ b_0 \neq 0$

ว่าเป็น <u>เอกลักษณ์ต่อกัน</u> (identically polynomial)

เมื่อ $a_i = b_i, \ \forall i = 0, 1, \ldots, n$

และใช้สัญลักษณ์แทนด้วย $f(x) \equiv g(x)$

<u>นิยาม 2.3.8</u> ให้ $p(x) \in F[x]$ จะเรียก $p(x)$ ว่าเป็น<u>โพลิโนเมียลที่ลดทอนไม่ได้</u> (irreducible polynomial) บน F ถ้า

$p(x) = a(x) \cdot b(x)$ โดยที่ $a(x), b(x) \in F[x]$

แล้ว $a(x)$ หรือ $b(x)$ อันใดอันหนึ่งมีอันดับเท่ากับ 0 และ

เรียก $p(x)$ ว่า <u>โพลิโนเมียลที่ลดทอนได้</u> (reducible polynomial) บน F ถ้า

$p(x) = a(x) \cdot b(x)$ โดยที่ $a(x), b(x) \in F[x]$

แล้ว $a(x)$ และ $b(x)$ มีอันดับที่ไม่เท่ากับ 0 ทั้งคู่

<u>ตัวอย่าง 2.3.2</u> ให้ $p(x) \in R[x]$ โดยที่ $p(x) = x^2 - 2$

จะได้ว่า $p(x) = (x-\sqrt{2})(x+\sqrt{2})$

จะเห็นว่า $(x-\sqrt{2}),(x+\sqrt{2}) \in R[x]$ และมีอันดับเท่ากับ 1

ดังนั้นจะได้ว่า $p(x)$ ลดทอนได้

<u>ตัวอย่าง 2.3.3</u> ให้ $p(x) \in Q[x]$ โดยที่ $p(x) = x^2 + 2$

<u>จะแสดงว่า $p(x)$ ลดทอนไม่ได้</u>

นั่นคือจะต้องแสดงว่า

ถ้า $p(x) = a(x)b(x), a(x), b(x) \in Q[x]$

แล้ว $a(x)$ หรือ $b(x)$ อันใดอันหนึ่งมีอันดับเท่ากับ 0

<u>สมมุติให้ $a(x)$ และ $b(x)$ มีอันดับไม่เท่ากับ 0 ทั้งคู่</u>

แต่เนื่องจาก $p(x)$ มีอันดับเท่ากับ 2 และ

อันดับของ $p(x)$ = อันดับของ $a(x)$ + อันดับของ $b(x)$

ทำให้ได้ว่า $a(x)$ และ $b(x)$ มีอันดับเท่ากับ 1

เพราะฉะนั้นให้ $a(x) = x+c$, $b(x) = x+d$, $c,d \in Q$

จะได้ว่า
$$\begin{aligned} p(x) &= a(x)b(x) \\ &= (x+c)(x+d) \\ &= x^2 + (c+d)x + cd \end{aligned}$$

นั่นคือ $x^2 + 2 = x^2 + (c+d)x + cd$

โดยการเปรียบเทียบสัมประสิทธิ์ของโพลิโนเมียล จะได้ว่า

$$(c+d) = 0 \qquad (1)$$

$$cd = 2 \qquad (2)$$

จาก (1) จะได้ $c = -d$

แทนค่า c ใน (2) จะได้ว่า

$$-d^2 = 2$$

$$d^2 = -2$$

แต่เนื่องจาก $d \in Q$ ดังนั้น $d^2 \geq 0$

แสดงว่าขัดแย้ง

ดังนั้นจะได้ว่า $a(x)$ หรือ $b(x)$ อันใดอันหนึ่งมีอันดับเท่ากับ 0

ให้ $a(x)$ มีอันดับเท่ากับ 0 และ $a(x) = c$, $c \in Q$

เพราะฉะนั้นจะได้ว่า $b(x)$ มีอันดับเท่ากับ 2

ดังนั้น ให้ $b(x) = d_1x^2+d_2x+d_3$, $d_1,d_2,d_3 \in Q$

จาก $p(x) = a(x)b(x)$

ดังนั้น $x^2 + 2 = c(d_1x^2 + d_2x + d_3)$

$$= cd_1x^2 + cd_2x + cd_3$$

นั่นคือ $x^2 + 2 = cd_1x^2 + cd_2x + cd_3$

โดยการเทียบสัมประสิทธิ์ของ โพลิโนเมียล จะได้ว่า

$$cd_1 = 1 \quad (3)$$

$$cd_2 = 0 \quad (4)$$

$$cd_3 = 2 \quad (5)$$

จาก (4) จะได้ว่า $c = 0$ หรือ $d_2 = 0$

สมมุติให้ $c = 0$ จาก (3) จะได้ว่า $0(d_1) = 1$ ซึ่งขัดแย้ง

เพราะฉะนั้น $c \neq 0$ จะได้ว่า $d_2 = 0$

ถ้าให้ $c = 1$ แทนค่า c ใน (3) จะได้ $d_1 = 1$

และ แทนค่า c ใน (5) จะได้ $d_3 = 2$

ดังนั้น $a(x) = 1$, $b(x) = x^2+2$

เพราะฉะนั้น โดยนิยาม 2.3.8 จะได้ว่า $p(x)$ ลดทอนไม่ได้

<u>นิยาม 2.3.9</u> ให้ $p(x) = x^n+a_1x^{n-1}+\ldots+a_n \in Q[x]$

โดยที่ $a_i \in Q$ $\forall i = 1,\ldots,n$, และ $a \in C$

จะเรียก a ว่า <u>จำนวนเชิงพีชคณิตที่มีอันดับเท่ากับ</u> n

(algebraic number degree n) บน Q เมื่อ $p(a) = 0$

และ $p(x)$ เป็นโมนิคโพลิโนเมียลที่ลดทอนไม่ได้

ถ้า $a_i \in Z$, $\forall i = 1,\ldots,n$

จะเรียก a ว่า<u>จำนวนเต็มเชิงพีชคณิตที่มีอันดับเท่ากับ</u> n

(algebraic integer degree n) บน Q

<u>ทฤษฎี 2.3.1</u> สมการกำลังสองราศิค $ax^2 + bx + c = 0$, $a,b,c \in C$

จะมีรากของสมการคือ $\dfrac{-b+\sqrt{b^2-4ac}}{2a}$

และ $\dfrac{-b-\sqrt{b^2-4ac}}{2a}$

<u>พิสูจน์</u> ดู [4] หน้า 31

<u>นิยาม 2.3.10</u> กำหนดสมการคิวบิค $x^3+bx^2+cx+d = 0$

และให้ $x = y - \frac{b}{3}$ แทนค่า x ในสมการคิวบิคจะได้

$y^3+py+q = 0$ โดยที่ $p = c - \frac{b^2}{3}$, $q = d - \frac{bc}{3} + \frac{2b^3}{27}$

จะเรียก $y^3+py+q = 0$ ว่า<u>สมการคิวบิคลดรูป</u>

(reduced cubic equation)

<u>ทฤษฎี 2.3.2</u> ถ้า y_1, y_2, y_3 เป็นรากของสมการคิวบิค $y^3+py+q = 0$

จาก นิยาม 2.3.10 แล้ว

$$x_1 = y_1 - \frac{b}{3},\ x_2 = y_2 - \frac{b}{3},\ x_3 = y_3 - \frac{b}{3},$$

จะเป็นรากของสมการคิวบิค $x^3+bx^2+cx+d = 0$

<u>พิสูจน์</u> ดู [4] หน้า 35

<u>หมายเหตุ</u> จากนิยาม 2.3.11 และทฤษฎี 2.3.2

$$y_1 = \sqrt[3]{-\frac{q}{2}+\sqrt{H}} + \sqrt[3]{-\frac{q}{2}-\sqrt{H}}\ ,\ \text{เมื่อ}\ H = \left(\frac{p}{3}\right)^3+\left(\frac{q}{2}\right)^2$$

$$y_2 = w\sqrt[3]{-\frac{q}{2}+\sqrt{H}} + w^2\sqrt[3]{-\frac{q}{2}-\sqrt{H}}\ ,\ \text{เมื่อ}\ w = -\frac{1}{2}+\frac{\sqrt{3}}{2}i$$

$$y_3 = w^2\sqrt[3]{-\frac{q}{2}+\sqrt{H}} + w\sqrt[3]{-\frac{q}{2}-\sqrt{H}},$$

<u>ตัวอย่าง 2.3.4</u> ให้ $p(x) \in Q[x]$ โดยที่ $p(x) = x^2 + 2$

โดยทฤษฎี 2.3.1 จะได้ว่า

$$x = \frac{\pm\sqrt{-8}}{2} = \pm\sqrt{2}\, i \in C$$

จะเห็นว่า $p(\sqrt{2}i) = (\sqrt{2}\, i)^2 + 2 = 0$ (1)

เพราะว่า $p(x)$ มีสัมประสิทธิ์ของ x^2 เท่ากับ 1 และจาก ตัวอย่าง 2.3.3 จะได้ว่า $p(x)$ เป็นโมนิคโพลิโนเมียลที่ลดทอนไม่ได้ (2)

จาก (1) และ (2) และโดยนิยาม 2.3.10 จะได้ว่า

$\sqrt{2}\, i$ เป็นจำนวนเต็ม เชิงพีชคณิตที่มีอันดับเท่ากับ 2

<u>ตัวอย่าง 2.3.5</u> ให้ $p(x) = x^3 + 9 \in Q[x]$

<u>จะแสดงว่า $p(x)$ ลดทอนไม่ได้</u>

<u>สมมุติว่า $p(x)$ ลดทอนได้</u>

เพราะฉะนั้นจะได้ว่า $p(x) = a(x)b(x)$, $a(x), b(x) \in Q[x]$

โดยที่ $a(x)$ และ $b(x)$ มีอันดับไม่เท่ากับ 0 ทั้งคู่

แต่เนื่องจาก $p(x)$ มีอันดับเท่ากับ 3 และ

อันดับของ $p(x)$ = อันดับของ $a(x)$ + อันดับของ $b(x)$

ให้ $a(x)$ มีอันดับเท่ากับ 1 และ $b(x)$ มีอันดับเท่ากับ 2

ดังนั้น $a(x) = x+c$, $b(x) = x^2+dx+e$, $c, d, e \in Q$

จะได้ว่า
$$\begin{aligned} p(x) &= a(x)b(x) \\ &= (x+c)(x^2+dx+e) \\ &= x^3+(c+d)x^2+(cd+e)x+ce \end{aligned}$$

นั่นคือ $x^3 + 9 = x^3 + (c+d)x^2 + (cd+e)x + ce$

โดยการเทียบสัมประสิทธิ์ของโพลิโนเมียล จะได้ว่า

$$c+d = 0 \quad (1)$$

$$cd+e = 0 \quad (2)$$

$$ce = 9 \quad (3)$$

จาก (1) จะได้ $c = -d$

แทนค่า c ใน (2) จะได้

$$-d^2+e = 0$$

นั่นคือ $e = d^2$

แทนค่า c, e ใน (3) จะได้

$$-d^3 = 9$$

$$d = \sqrt[3]{-9} = -\sqrt[3]{9}$$

จะได้ว่า $c = \sqrt[3]{9}$ และ $e = 3\sqrt[3]{3}$

นั่นคือ $a(x) = x + \sqrt[3]{9}$, $b(x) = x^2 - \sqrt[3]{9}x + 3\sqrt[3]{3}$

จะเห็นว่า $a(x), b(x) \notin Q[x]$

ดังนั้น ขัดแย้งกับกำหนดให้

แสดงว่า $p(x)$ เป็นโพลิโนเมียลที่ลดทอนไม่ได้

และเนื่องจาก $p(x)$ มีสัมประสิทธิ์ของ x^2 เท่ากับ 1

ดังนั้น $p(x)$ เป็นโมนิคโพลิโนเมียลที่ลดทอนไม่ได้

นั่นคือ $a(x)$ หรือ $b(x)$ อันใดอันหนึ่งมีอันดับเท่ากับ 0

ให้ $a(x)$ มีอันดับเท่ากับ 0 และ $a(x) = c$, $c \in Q$

เพราะฉะนั้น $b(x)$ มีอันดับเท่ากับ 3

ดังนั้นให้ $b(x) = dx^3 + ex^2 + fx + g,\ d, e, f, g \in Q$

จาก $p(x) = a(x)b(x)$

เพราะฉะนั้น $x^3 + 9 = c(dx^3 + ex^2 + fx + g)$

$= cdx^3 + cex^2 + cfx + cg$

โดยการเทียบสัมประสิทธิ์ของโพลิโนเมียล จะได้ว่า

$$cd = 1 \quad (1)$$

$$ce = 0 \quad (2)$$

$$cf = 0 \quad (3)$$

$$cg = 9 \quad (4)$$

จาก (2) จะได้ว่า $c = 0$ หรือ $e = 0$

สมมุติให้ $c = 0$ จาก (1) จะได้ $0(d) = 1$ ซึ่งขัดแย้ง

เพราะฉะนั้น $c \neq 0$ จะได้ว่า $e = 0$

และจาก (3) จะได้ว่า $f = 0$ ด้วย

ถ้าให้ $c = 1$ แทนค่า c ใน (1) จะได้ $d = 1$

และแทนค่า c ใน (4) จะได้ $g = 9$

ดังนั้น $a(x) = 1,\ b(x) = x^3 + 9$

จะเห็นว่า $a(x), b(x) \in Q[x]$

โดยที่ $p(x) = 1(x^3 + 9)$

จาก $-\sqrt[3]{9} \in C$

และ $p(-\sqrt[3]{9}) = (-\sqrt[3]{9})^3 + 9 = -9 + 9 = 0$

ดังนั้นโดยนิยาม 2.3.10 จะได้ว่า

$-\sqrt[3]{9}$ เป็นจำนวนเต็มเชิงพีชคณิตที่มีอันดับเท่ากับ 3