# บทที่ 10
# ฟีลด์ของผลหารและการแยกตัวประกอบของฟีลด์

## ฟีลด์ของผลหาร

พิจารณาเซตของจำนวนตรรกยะ $\mathbb{Q} = \left\{ \frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0 \right\}$ จะเห็นได้ว่าเซตของจำนวนตรรกยะเป็นฟีลด์ นั่นคือ เราสามารถสร้างฟีลด์ของจำนวนตรรกยะได้จากริงของจำนวนเต็ม โดยอาศัยแนวความคิดนี้ เราสามารถสร้างฟีลด์ของผลหารจากอินทิกรัลโดเมนใด ๆ ได้
ถ้าให้ $D$ เป็นอินทิกรัลโดเมน แล้วผลคูณคาร์ทีเซียนของ $D$ และ $D$ คือ

$$D \times D = \{(a, b) | a, b \in D\}$$

ซึ่ง ถ้าพิจารณาคู่อันดับ $(a, b) \in D \times D$ ในลักษณะผลหารรูปใน (formal quotiend) $\frac{a}{b}$ แล้วจะเห็นว่า ถ้า $D = \mathbb{Z}$ จะได้ว่า $(5, 9) \in D \times D$ ก็คือจำนวน $\frac{5}{9} \in \mathbb{Q}$ นั่นเอง แต่สำหรับ $(5, 0) \in D \times D$ นั้น ก็คือจำนวน $\frac{5}{0}$ ซึ่งไม่นิยาม เพราะฉะนั้นเราจึงมาพิจารณาเซตย่อยของ $D \times D$ แทน ซึ่งเซตย่อยดังกล่าวคือ

$$S(\{(a, b) | a, b(D \text{ และ } b)0\})$$

กรณีนี้ ถ้า $D = \mathbb{Z}$ ก็จะเห็นว่าคู่อันดับ $(5, 9)$ และ $(10, 18)$ นั้น ก็คือจำนวนตรรยะตัวเดียวกันจากข้อสังเกตดังกล่าวจึงกำหนดความสัมพันธ์ในเซต $S$ ดังบทนิยามต่อไปนี้

บทนิยาม 10.1 กำหนดให้ $D$ เป็นอินทิกรัลโดเมน และ $S = \{(a, b) | a, b \in D \text{ และ } b \neq 0\}$ กำหนดความสัมพันธ์ $\sim$ บน $S$ ดังนี้ สำหรับทุก $(a, b, ), (c, d) \in S$

$$(a, b) \sim (c, d) \text{ ก็ต่อเมื่อ } ad = bc$$

จากบทนิยาม 10.1 จะเห็นว่า ถ้า $D = \mathbb{Z}$ แล้วความสัมพันธ์ $\sim$ ก็คือการเท่ากัน $(=)$ นั่นเอง เช่น สำหรับ $(5, 9), (10, 18) \in S$ จะได้ว่า $\frac{5}{9} = \frac{10}{18}$ ทั้งนี้เพราะว่า $(5)(18) = (10)(9)$

ทฤษฎีบท 10.2 จากบทนิยาม 10.1 จะได้ว่า ความสัมพันธ์ $\sim$ บนเซต $S$ เป็นความสัมพันธ์สมมูล

การพิสูจน์ กำหนดให้ $(a_1, b_1), (a_2, b_3), (a_3, b_3) \in S$ ดังนั้น $a_1, a_2, a_3, b_1, b_2, b_3 \in D$ โดยที่ $b_1 \neq 0, b_2 \neq 0$ และ $b_3 \neq 0$

(1) เนื่องจาก $a_1b_1 = a_1b_1$ ดังนั้น $(a_1, b_1) \sim (a_1, b_1)$

(2) สมมติให้ $(a_1, b_1) \sim (a_2, b_2)$ จะได้ว่า $a_1b_2 = b_1a_2$ นั่นคือ $a_2b_1 = b_2a_1$ ทำให้ได้ว่า $(a_2, b_2) \sim (a_1, b_1)$

(3) สมมติให้ $(a_1, b_1) \sim (a_2, b_2)$ และ $(a_2, b_2) \sim (a_3, b_3)$ ดังนั้น $a_1b_2 = b_1a_2$ และ $a_2b_3 = b_2a_3$ พิจารณา

$$a_1b_3b_2 = a_1b_2b_3 = b_1a_2b_3 = b_1b_2a_3 = b_1a_3b_2$$

จะได้ $(a_1b_3 - b_1a_3)b_2 = 0$ โดยที่ $b_2 \neq 0$
และเพราะว่า $D$ เป็นอินทิกรัลโดเมน จึงทำให้ $D$ ไม่มีตัวหารของศูนย์
ดังนั้น $a_1b_3 - b_1a_3 = 0$
ดังนั้น $a_1b_3 = b_1a_3$ นั่นคือ $(a_1, b_1) \sim (a_3, b_3)$
จาก $(1) - (3)$ จึงสรุปได้ว่า $\sim$ เป็นความสัมพันธ์สมมูลบน $S$

หมายเหตุ เนื่องจาก $\sim$ เป็นความสัมพันธ์สมมูลบน $S$ ดังนั้น สำหรับแต่ละ $(a, b) \in S$ ชั้นสมมูลของ $(a, b)$ หมายเหตุเซต

$$\begin{aligned}[(a,b)] &= \{(x,y) \in S | (x,y) \sim (a,b)\} \\ &= \{(x,y) \in S | xb = ya\}\end{aligned}$$

จะเห็นว่า ถ้า $b, d \in D$ โดยที่ $b \neq 0$ แล้ว

$$\begin{aligned}[(0,b)] &= \{(x,y) \in S | (x,y) \sim (0,b)\} \\ &= \{(x,y) \in S | xb = y0\} \\ &= \{(x,y) \in S | xb = 0\} \\ &= \{(x,y) \in S | x = 0\} \text{ (จาก } b \neq 0 \text{ และ } D \text{ ไม่มีตัวหารของศูนย์)} \\ &= \{(0,y) \in S | y \in D \text{ และ } y \neq 0\}\end{aligned}$$

ในทำนองเดียวกัน จะได้ว่า

$$\begin{aligned}[(0,b)] &= \{(x,y) \in S | x = 0\} \\ &= \{(0,y) \in S | y \in D \text{ และ } y \neq 0\}\end{aligned}$$

เช่นกัน ดังนั้น $[(0, b)] = [(0, d)]$

นอกจากนี้ ยังได้ว่า

$$\begin{aligned}[(b,b)] &= \{(x,y) \in S | (x,y) \sim (b,b)\} \\ &= \{(x,y) \in S | xb = yb\} \\ &= \{(x,y) \in S | xb - yb = 0 \in D\} \\ &= \{(x,y) \in S | (x-y)b = 0\} \\ &= \{(x,y) \in S | (x-y) = 0\}\end{aligned}$$

(จาก $b \neq 0$ และ $D$ ไม่มีตัวหารของศูนย์)

$$\begin{aligned}&= \{(x,y) \in S | (x = y\} \\ &= \{(y,y) \in S | y \in D \text{ และ } y \neq 0\}\end{aligned}$$

ในทำนองเดียวกัน จะได้ว่า

$$\begin{aligned}[(d,d)] &= \{(x,y) \in S | x = y\} \\ &= \{(y,y) \in S | y \in D \text{ และ } y \neq 0\}\end{aligned}$$

เช่นกัน ดังนั้น $[(b,b)] = [(d,d)]$

ต่อไปจะเป็นการสร้างฟีลด์ของผลหารโดยอาศัยความสัมพันธ์สมมูล $\sim$ บน $S$ ดังนี้

ทฤษฎีบท 10.3 กำหนดให้ $F$ เป็นเซตของชั้นสมมูลทั้งหมด ภายใต้ความสัมพันธ์สมมูลใน ทฤษฎีบท 10.2 ดังนั้น

$$\begin{aligned}F &= \{[(a,b)] | (a,b) \in S\} \\ &= \{[(a,b]) | a,b \in D \text{ (และ } b \neq 0)\}\end{aligned}$$

กำหนดการบวก และการคูณบน $F$ ดังนี้ สำหรับทุก $[(a,b)], [(c,d)] \in F$

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

และ $$[(a,b)][(c,d)] = [(ac, bd)]$$

จะได้ว่าการดำเนินการการบวก และกาารคูณบน $F$ เป็นการดำเนินการแจ่มชัด $(well-definedoperations)$ และเป็นการดำเนินการทวิภาคบน $F$

การพิสูจน์ กำหนดให้ $[(a,b)], [(c,d)] \in F$ ดังนั้น $(a,b), (c,d) \in S$
และได้ว่า $b \neq 0 d \neq 0$ เนื่องจาก $D$ เป็นอินทิกรัลโดเมน
จึงได้ว่า $bd \neq 0$
เพราะฉะนั้น $(ad+bc, bd) \in S$
นั่นคือ $[(ad+bc, bd)], [(ac, bd)] \in F$
สมมติให้ $[(a_1, b_1)] = [(a,b)]$
และ $[(c_1, d_1)] = [(c,d)]$ นั่นคือ $(a_1 b_1) \in [(a,b)]$ และ $(c_1, d_1) \in [(c,d)]$
ดังนั้น $(a_1, b_1) \sim (ab)$ และ $(c_1, d_1) \sim (cd)$

นั่นคือ $a_1b = b_1a$ และ $c_1d = d_1c$
จะได้ว่า $a_1bd_1d = b_1ad_1d$ และ $c_1db_1b = d_1cb_1b$
เพราะฉะนั้น

$$a_1bd_1d + c_1db_1b = b_1ad_1d + d_1cb_1b$$
$$(a_1b_1 + c_1b_1)bd = b_1d_1(ad + bc)$$

ดังนั้น $(a_1d_1 + c_1b_1, b_1d_1) \sim (ad + bc, bd)$
จึงได้ว่า $(a_1d_1 + b_1c_1, b_1d_1) \in [(ad + bc, bd)]$
นั่นคือ $[(a_1d_1 + b_1c_1, b_1d_1)] = [(ad + bc, bd)]$
หรือ $[(a_1, b_1)] + [(c_1, d_1)] = [(a, b)] + [(c,d)]$
และเนื่องจาก $a_1b = b_1a$ และ $c_1d = d_1c$
จะได้ว่า $a_1bc_1d = b_1ad_1c$
$a_1c_1bd = b_1d_1ac$ (เพราะว่า $D$ เป็นริงสลับที่)
ดังนั้น $(a_1c_1, b_1d_1) \sim (ac, bd)$
จึงได้ว่า $(a_1c_1, b_1d_1) \in [(ac, bd)]$
นั่นคือ $[(a_1c_1, b_1d_1)] = [(ac, bd)]$
หรือ $[(a_1, b_1)][(c_1, d_1)] = [(a, b)][(c, d)]$

ทฤษฎีบท 10.4 $F$ เป็นฟีลด์

การพิสูจน์ เนื่องจาก $D$ เป็นอินทิกรัลโดเมน
เพราะฉะนั้น $D$ เป็นริงสลับที่ที่ไม่มีตัวหารของศูนย์
สมมติให้ $[(a, b)], [(c, d)] \in F$
จะได้ว่า $[(a, b)] + [(c, d)] = [(ab + bc, bd)]$
และ $[(c, d)] + [(a, b)] = [(cb + da, db)]$
เนื่องจาก $ab + bc = cb + da$ และ $bd = db$
ดังนั้น $(ab + bc, bd) \sim (cb + da, db)$
นั่นคือ $[(ad + bc, bd)] = [(cb + da, db)]$
หรือ $[(a, b)] + [(c, d)] = [(c, d)] + [(a, b)]$
และจากบทนิยามการคูณบน $F$
จะได้ว่า $[(a, b)][(c, d)] = [(ac, bd)]$
และ $[(c, d)][(a, b)] = [(ca, db)]$ แต่เนื่องจาก $ac = ca$ และ $bd = db$
ดังนั้น $(ac, bd) \sim (ca, db)$
นั่นคือ $[(ac, bd)] = [(ca, db)]$ หรือ $[(a, b)][(c, d)] = [(c, d)][(a, b)]$
สรุปได้ว่า การบวกและการคูณใน $F$ มีสมบัติการสลับที่

ในทำนองเดียวกัน จะได้ว่าการบวก และการคูณใน $F$ มีสมบัติการเปลี่ยนหมู่ด้วย นอกจากนี้ยังได้ว่า $[(0,b)]$ เป็นสมาชิกเอกลักษณ์การบวกเมื่อ $b \in D$ และ $b \neq 0$ และสำหรับ $[(a,b)] \in F$ จะได้ว่า $[(-a,b)] \in F$ เป็นตัวผกผันการบวกของ $[(a,b)]$ นั่นคือ $F$ เป็นอาบีเลียนกรุป ภายใต้การบวก

สำหรับการคูณนั้น จะได้ว่า $F - \{[0,b]|b \in D$ และ $b \neq 0\}$
มีสมบัติการปิด ทั้งนี้ เพราะว่า $D$ ไม่มีตัวหารของศูนย์ และมี $[a,a]$ เป็นสมาชิกเอกลักษณ์การคูณ เมื่อ $a \in D$ และ $a \neq 0$

สำหรับ $[(c,d)] \in F - \{[(0,b)]|b \in D$ และ $b \neq 0$ }
จะได้ว่า ถ้า $c = 0$ แล้ว $cb = 0d = 0$ และ $d0 = 0$
ดังนั้น $cd = d0$ นั่นคือ $(c,d) \sim (0,b)$
จึงได้ว่า $[(c,d)] = [(0,b)]$ แต่ $[(0,b)]$ เป็นสมาชิกเอกลักษณ์การบวกของ $F$ จึงเกิดข้อขัดแย้ง
เพราะฉะนั้น $c \neq 0$ เป็นผลให้ $[(d,c)] \in F - \{[(0,b)]|b \in D$
และ $b \neq 0\}$ จะเห็นว่า $[(c,d)][(d,c)] = [(cd,dc)]$
เนื่องจาก $D$ เป็นริงสลับที่ ดังนั้น $cd = dc$ ทำให้ได้ว่า $(cd)a = (dc)a$
นั่นคือ $(cd,dc) \sim (a,a)$ ดังนั้น $[(c,d)][(d,c)] = [(a,a)]$ โดยที่ $[(a,a)]$ เป็นสมาชิกเอกลักษณ์การคูณของ $F$
ฉะนั้น $[(d,c)]$ เป็นตัวผกผันการคูณของ $[(c,d)]$
จึงสรุปได้ว่า $F - \{[(0,b)]|b \in D$ และ $b \neq 0\}$ เป็นอาบีเลียนกรุปภายใต้การคูณ
ต่อไปสมมติให้ $[(p,q)], [(s,t)], [(u,v)] \in F$ เมื่อพิจารณา

$$\begin{aligned}
[(p,q)]([(s,t)] + [(u,v)]) &= [(p,q)][(sv+tu,tv)] \\
&= [(p(sv+tu),qtv)] \\
&= [(psv+ptu,qtv)] \\
&= [(psv+ptu,qtv)][(q,q)] \\
&= [((psv+pyu)q,(qtvq)] \\
&= [psvq+qtpu,qtqv] \\
&= [(ps)(qv)+(qt)(pu),(qt)(qv)] \\
&= [ps,qt]+[pu,qv] \\
&= [(p,q)][(s,t)]+[(p,q)][(u,v)]
\end{aligned}$$

จึงได้ว่า $F$ มีสมบัติการแจกแจง สรุปได้ว่า $F$ เป็นฟีลด์

หมายเหตุ เรียกฟีลด์ $F$ ในทฤษฎีบท 10.4 ว่าฟีลด์ของผลหาร (field of quotients) ของอินทิกรัลโดเมน $D$

ทฤษฎีบทต่อไปนี้จะให้ความสัมพันธ์ระหว่างอินทิกรัลโดเมนกับฟีลด์ของผลหารของอินทิกรัลนั้น

บทนิยาม 10.5 กำหนดให้ $R$ และ $R'$ เป็นริง จะกล่าวว่า $R$ สามารถฝังใน $R'$ (can beimbedded in $R'$) ก็ต่อเมื่อ มีโมโนมอร์ฟิซึม (monomorphism) จาก $R$ ไปยัง $R'$

ตัวอย่างที่ 10.1 พิจารณาริงของเซตของจำนวนเต็ม $\mathbb{Z}$ และฟีลด์ของเซตของจำนวนตรรกยะ $\mathbb{Q}$ ถ้าให้ $\theta : \mathbb{Z} \to \mathbb{Q}$ เป็นฟังก์ชันที่กำหนดโดย $\theta(z) = \frac{z}{1}$ สำหรับทุก $z \in \mathbb{Z}$

สมมติให้ $z_1, z_2 \in \mathbb{Z}$
เนื่องจาก $\theta(z_1 + z_2) = \frac{z_1+z_2}{1} = \frac{z_1}{1} + \frac{z_2}{1} = \theta(z_1) + \theta(z_2)$
และ $\theta(z_1 z_2) = \frac{z_1 z_2}{1} = \frac{z_1}{1} \cdot \frac{z_2}{1} = \theta(z_1)\theta(z_2)$
จะได้ว่า $\theta$ เป็นโฮโมมอร์ฟิซึมจาก $\mathbb{Z}$ ไปยัง $\mathbb{Q}$
และถ้าให้ $\theta(z_1)\theta(z_2)$ แล้ว $\frac{z_1}{1} = \frac{z_2}{1}$ นั่นคือ $z_1 = z_2$
ดังนั้น $\theta$ เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก $\mathbb{Z}$ ไปยัง $\mathbb{Q}$
เพราะฉะนั้น $\theta$ เป็นโมโนมอร์ฟิซึมจาก $\mathbb{Z}$ ไปยัง $\mathbb{Z}$
จึงสรุปได้ว่า ริงของเซตของจำนวนเต็ม $\mathbb{Q}$ สามารถฝังในฟีลด์ของเซตของจำนวนตรรกยะ $\mathbb{Q}$

**ทฤษฎีบท 10.6** ทุกอินทิกรัลโดเมนสามารถฝังในฟีลด์

การพิสูจน์ กำหนดให้ $D$ เป็นอินทิกรัลโดเมน และ $F$ เป็นฟีลด์ของผลหารของ $D$
พิจารณา $\theta : D \to F$ ที่กำหนดโดย

$$\theta(a) = [(ax, x)] \text{ สำหรับทุก } a \in D \text{ เมื่อ } x \in D - \{0\}$$

เห็นได้ชัดว่า $\theta$ เป็นฟังก์ชันจาก $D$ ไปยัง $F$
ต่อไปจะแสดงว่า $\theta$ เป็นฟังก์ชันหนึ่งต่อหนึ่ง
โดยสมมติให้ $\theta(a) = \theta(b)$ เมื่อ $a, b \in D$ ดังนั้น $[(ax, x)] = [(bx, x)]$
ฉะนั้น $(ax, x) \sim (bx, x)$ นั่นคือ $ax^2 = bx^2$
ทำให้ได้ว่า $ax^2 - bx^2 = (a - b)x^2 = 0$
เนื่องจาก $D$ ไม่มีตัวหารของศูนย์ ดังนั้น $x^2 \neq 0$ จึงทำให้ได้ว่า $a - b = 0$
ฉะนั้น $a = b$
นั่นคือ $\theta$ เป็นฟังก์ชันหนึ่งต่อหนึ่งจาก $D$ ไปยัง $F$ และสำหรับ $c, d \in D$

จะได้ว่า

$$\begin{aligned}\theta(c+d) &= [((c+d)x, x)] \\ &= [(cx+dx, x)] \\ &= [(cx+dx, x)][(x, x)] \\ &= [((cx+dx)x, xx)] \\ &= [(cx^2+dx^2, x^2)] \\ &= [(cx, x)] + [(dx, x)] \\ &= \theta(c) + \theta(d)\end{aligned}$$

และได้อีกว่า

$$\begin{aligned}\theta(cd) &= [(cdx, x)] \\ &= [(cdx, x)][(x, x)] \\ &= [(cxdx^2)] \\ &= [(cx, x)][(dx, x)] \\ &= \theta(c)\theta(d)\end{aligned}$$

นั่นคือ $\theta$ เป็นโฮโมมอร์ฟิซึม จึงสรุปได้ว่า $\theta$ เป็นโมโนมอร์ฟิซึมจาก $D$ ไปยัง $F$

## การแยกตัวประกอบของฟีลด์

ในกรณีศึกษาสมบัติของจำนวนเต็ม เราได้ว่าสำหรับจำนวนเต็ม $a$ และ $b$ โดยที่ $b \neq 0$ จะมีจำนวนเต็ม $q$ และ $r$ เพียงคู่เดียวเท่านั้นที่ทำให้ $a = bq + r$ โดยที่ $0 \leq r < |b|$ ในเซตของพหุนามบนฟีลด์ ก็มีสมบัติเช่นเดียวกันนี้ ดังจะกล่าวในหัวข้อการแยกตัวประกอบของพหุนามบนฟีลด์ (factorization of polynomials over a field) นี้

ทฤษฎีบท 10.7 ขั้นตอนวิธีการหาร (Division Algorithm)
กำหนดให้ $F$ เป็นฟีลด์ สำหรับพหุนาม$f(x)$ และ $g(x)$ ใน $F[x]$ โดยที่ $g(x) \neq 0$ จะได้ว่ามีพหุนาม $t(x)$ และ $r(x)$ ใน $F[x]$ เพียงคู่เดียวเท่านั้นที่ทำให้ $f(x) = g(x)t(x) + r(x)$ โดยที่ $r(x) = 0$ deg$r(x) <$ deg$(x)$

การพิสูจน์ กำหนดให้ $F$ เป็นฟีลด์ และสมมติให้ $f(x)$ และ $g(x)$ เป็นพหุนามใน $F[x]$ โดยที่ $g(x) \neq 0$

กรณีที่ deg$(x) <$ deg$(x)$ :

ให้ $t(x) = 0$ และ $r(x) = f(x)$

จะได้ว่า$f(x) = g(x)t(x) + r(x)$ โดยที่ deg$r(x) <$ deg$g(x)$

กรณี deg$f(x) \geq$ deg$g(x)$ :

ถ้า deg$f(x) = 0$

จะได้ว่า deg$= 0$ นั่นคือ $f(x) = a$ และ $g(x) = b$ โดยที่ $a, b \in F - \{0\}$

จะเห็นว่า $t(x) = ab^{-}1$ และ $r(x) = 0$

แล้วจะได้ว่า $f(x) = g(x)t(x) + r(x)$ โดยที่ $r(x) = 0$

ถ้า deg$f(x) \geq 1$ แล้วจะพิสูจน์โดยอาศัยหลักการอุปนัยเชิงคณิตศาสตร์บนดีกรีของ $f(x)$ โดยเริ่มพิจารณาเมื่อ deg$f(x) = 1$

จะได้ว่า $f(x) = a_0 + a_1x$ เมื่อ $a_0, a_1 \in F$ และ $a_1 \neq 0$

เนื่องจาก deg$(x) \geq$ deg$g(x)$ ดังนั้น deg$g(x) = 0$ หรือ deg$g(x)1$

ในกรณี deg$g(x) = 0$

ทำให้ได้ว่า $g(x) = b_0$ เมื่อ $b_0 \in F - \{0\}$

ดังนั้น จะมี $t(x) = a_0b_0^{-}1 + a_1b_0^{-}1x \in F[x]$ และ $r(x) = 0$

ที่ทำให้ $f(x) = g(x)t(x) + r(x)$

ในกรณีที่ deg$g(x) = 1$

จะได้ว่า $g(x) = c_0 + c_1x$ เมื่อ $c_0, c_1 \in F$ และ $c_1 \neq 0$

ฉะนั้น จะได้ว่ามี $t(x) = a_1c_1^{-}1 \in F[x]$ และ $r(x) = a_0 - a_1c_0c_1^{-}1$

ที่ทำให้ $f(x) = g(x)t(x) + r(x)$ โดยที่ deg$r(x) = 0 <$ deg$g(x)$

จึงสรุปได้ว่า ถ้า deg$f(x) = 1$ แล้วทฤษฎีบทเป็นจริง

ต่อไปสมมติว่าทฤษฎีบทเป็นจริงสำหรับพหุนามที่มีระดับขั้นพหุนามหรือดีกรีน้อยกว่า $m$

พิจารณา $f(x)$ ซึ่งเป็นพหุนามดีกรี $m$ และ $g(x)$ ซึ่งเป็นพหุนามดีกรี $n$

จะได้ว่า $f(x) = a_0 + a_1x + \cdots + a_mx^m$

และ $g(x) = b_0 + b_1x + \cdots + b_nx^n$

ดังนั้น $a_m \neq 0, b_n0$ และ $m \geq n$

พิจารณา $f_1(x) = f(x)$ - $\left(\frac{a_m}{b_n}x^{m-n}\right)$ $g(x)$
จะพบว่า deg$f_1(x) \leq m-1$
โดยสมมติฐาน จะได้ว่า $f_1(x) = g(x)t_1(x) + r(x)$
สำหรับบาง $t_1(x), r(x) \in f[x]$ โดยที่ $r(x) = 0$ หรือ deg$r(x) <$ deg$g(x)$
นั่นคือ $f(x) = f_1(x)$ + $\left(\frac{a_m}{b_n}x^{m-n}\right)$ $g(x)$
$= g(x)$ $t_1(x)$ + $r(x)$ + $\left(\frac{a_m}{b_n}x^{m-n}\right)$ $g(x)$
$= g(x)$ - $\left(g(x)\frac{a_m}{b_n}x^{m-n}\right)$ + $r(x)$
ดังนั้น ถ้าให้ $t(x) = t_1(x) + \frac{a_m}{b_n}x^{m-n}$
แล้วจะได้ว่า $f(x) = g(x)t(x) + r(x)$ โดยที่ $r(x) = 0$
หรือ deg$r(x) <$ deg$g(x)$ ตามต้องการ
ต่อไปสมมติว่ามี $t^{'}(x), r^{'} \in F[x]$ อีกคู่หนึ่ง
ที่ทำให้ $f(x) = g(x)t^{'}(x) + r^{'}(x)$ โดยที่ $r^{'}(x) = 0$
หรือ deg$r^{'}(x) <$ deg$g(x)$
ดังนั้น $g(x)t(x) + r(x) = g(x)t^{'}(x) + r^{'}(x)$
นั่นคือ $g(x)(t(x) - t^{'}(x)) = r(x) - r^{'}(x)$
ถ้า $r^{'} = 0 = r(x)$
จะได้ว่า $g(x)(t(x) - t^{'}(x)) = 0$
จึงทำให้ได้ว่า $t(x) - t^{'}(x) = 0$ ทั้งนี้เพราะ $g(x) \neq 0$
นั่นคือ $t^{'}(x) = t(x)$
แต่ $r^{'}(x) \neq 0$ หรือ $r(x) \neq 0$
แล้วจะได้ว่า deg$r^{'}(x) <$ deg$g(x)$ หรือ deg$r(x) <$ deg$g(x)$
พิจารณา $r^{'}(x) - r(x)$
สมมติว่า $r^{'} - r(x) \neq 0$
ดังนั้น deg$(r^{'}(x) - r(x)) <$ deg$g(x)$
เนื่องจาก $g(x)(t(x) - t^{'}(x))$
ดังนั้น deg$g(x) \leq$ deg$g(x)$+ deg$(t(x) - t^{'}(x))$
$=$ deg$(r^{'}(x) - r(x))$
$<$ deg$g(x)$
ซึ่งเป็นไปไม่ได้

เพราะฉะนั้น $r^{'}(x) = r(x)$ และเป็นผลให้ $t^{'}(x) = t(x)$ จึงสรุปได้ว่ามีพหุนาม $t(x)$ และ $r(x)$ เพียงคู่เดียวเท่านั้น
ที่ทำให้ $f(x) = g(x)t(x) + r(x)$ โดยที่ $r(x) = 0$ หรือ deg$r(x) <$ deg$t(x)$

เรียกพหุนาม $f(x)$ และ $g(x)$ ในสมการ $f(x) = g(x)t(x) + r(x)$ ว่าตัวตั้ง และตัวหาร (divisor) ตามลำดับ และเรียก $r(x)$ ว่าเศษเหลือ (remainder) ของการหาร $f(x)$ ด้วย $g(x)$ ในกรณีที่ $r(x) = 0$ จะกล่าวว่า $g(x)$ หาร $f(x)$ ลงตัว ในบางครั้งจะพิจารณาพหุนาม $f(x)$ บนฟีลด์ $f$ เป็นฟังก์ชันที่มีโดเมน คือ $f$ ดังนั้น เรนจ์ของ $f(x)$ คือ เซตย่อยของ $F$ และเมื่อพหุนาม $f(x)$ เท่ากับพหุนาม $g(x)$ และ $a \in F$ จะได้ว่า $f(a)g(a)$ ในกรณีที่ $f(a) = 0$ จะเรียก $a$ ว่าราก (root) ของพหุนาม $f(x)$

ทฤษฎีบท 10.8 ทฤษฎีบทเศษเหลือ (Remainder Theorem)
กำหนดให้ $F$ เป็นฟีลด์ ถ้า $f(x)$ เป็นพหุนามใน $F[x]$ และ $a \in F$ แล้วเศษเหลือของการหาร $f(x)$ ด้วย $x - a$ คือ $f(a)$

การพิสูจน์ กำหนดให้ $F$ เป็นฟีลด์ ถ้า $f(x)$ เป็นพหุนามใน $F[x]$ และ $a \in F$ แล้ว
โดยทฤษฎีบท 10.7
จะได้ว่ามี $t(x)$ และ $r(x)$ ใน $F[x]$ ที่ทำให้ $f(x) = (x - a)t(x) + r(x)$
โดยที่ $r(x) = 0$ หรือ deg$r(x) <$ deg$(x - a) = 1$ เนื่องจาก $aF$
ดังนั้น $f(a) = (0)t(a)+r(a) = r(a)$ โดยที่ $r(a) = 0$ หรือ deg$r(a) = 0$
นั่นคือ $r(x) = f(a)$

บทแทรก 10.9 กำหนดให้ $F$ เป็นฟีลด์ ถ้า $f(x)$ เป็นพหุนามใน $F[x]$ และ $a \in F$ จะได้ว่า $x - a$ หาร $f(x)$ ลงตัว ก็ต่อเมื่อ $a$ เป็นรากของ $f(x)$

การพิสูจน์ กำหนดให้ $F$ เป็นฟีลด์
และสมมติให้ $f(x)$ เป็นพหุนามใน $F[x]$ และ $a \in F$ โดยทฤษฎีบท 10.7
จะได้ว่ามี $t(x)$ และ $r(x)$ ใน $f[x]$ ที่ทำให้ $f(x) = (x - a)t(x) + r(x)$
โดยที่ $r(x) = 0$ หรือ deg$r(x) <$ deg$(x - a) = 1$
ถ้า $x - a$ หาร $f(x)$ ลงตัว แล้ว $r(x) = 0$
โดยทฤษฎีบท 7.15
จะได้ว่า $r(x) = f(a)$ นั่นคือ $f(a) = 0$ นั่นคือ $a$ เป็นรากของ $f(x)$

ในทางกลับกัน ถ้าสมมติให้ $a$ เป็นรากของ $f(x)$ แล้ว $f(a) = 0$
โดยทฤษฎีบท 7.15
จะได้ว่า $r(x) = f(a)$ นั่นคือ $r(x) = 0$
เพราะฉะนั้น $x - a$ หาร $f(x)$ ลงตัว

## สรุปท้ายบท

ฟีลด์ เป็นเนื้อหาทางคณิตศาสตร์ที่สำคัญ เป็นระบบที่ถูกนำมาใช้หลากหลาย ทั้งทฤษฎีรหัสซึ่งเป็นพื้นฐานของระบบสารสนเทศพื้นฐานในปัจจุบัน ระบบจำนวนจริงกับการบวกการคูณ ระบบของจำนวนเชิงซ้อน จากเนื้อหาที่กล่าวมาทั้งหมดทุกบท จะเห็นว่า เนื้อหามีความซับซ้อนแต่สามารถนำมาใช้ให้เกิดประโยชน์อย่างมาก รวมถึงสามารถนำไปประยุกต์ใช้ในศาสตร์อื่น ๆ ได้