บทที่ 3
สนามของผลหารของโดเมนเชิงจำนวนเต็ม
(The field of quotients of an integral domain)

ถ้าสมาชิกทุกตัว (ยกเว้นสมาชิก 0) ของโดเมนเชิงจำนวนเต็มมีตัวผกผันสำหรับการคูณ แล้วโดเมนเชิงจำนวนเต็มนั้นก็จะเป็นสนาม แต่อย่างไรก็ตาม มีโดเมนเชิงจำนวนเต็มหลายอัน เช่น-(Z, +, .) ไม่เป็นสนาม ในบทนี้เราจะแสดงให้เห็นว่า ทุก ๆ โดเมนเชิงจำนวนเต็มสามารถจะไปบรรจุในสนามได้ เรียกสนามของผลหารของโดเมนเชิงจำนวนเต็ม (a field of quotients of the integral domain) สนามนี้จะเป็นสนามที่เล็กที่สุดที่บรรจุโดเมนเชิงจำนวนเต็มที่เราจะสามารถบรรยายได้ ตัวอย่างเช่น จำนวนเต็มบรรจุอยู่ในสนาม Q ซึ่งสมาชิกของ Q สามารถเขียนได้ในรูปผลหารของจำนวนเต็ม การสร้างสนามของผลหารของโดเมนเชิงจำนวนเต็มก็จะทำเช่นเดียวกับการสร้างจำนวนเศษส่วนจากจำนวนเต็ม

3.1 การสร้างสนามของผลหารของโดเมนเชิงจำนวนเต็ม (The Construction)

ให้ D เป็นโดเมนเชิงจำนวนเต็ม ซึ่งเราต้องการจะขยายให้เป็นสนามของผลหาร (F) เค้าโครงของขั้นตอนที่เราจะสร้างจะเป็นดังนี้

1. นิยามว่า สมาชิกของ F คืออะไร
2. นิยามการดำเนินการทวิภาค (Binary operation) + และ . บน F
3. ตรวจสอบคุณสมบัติของสนามเพื่อแสดงว่า F เป็นสนามภายใต้การ + และ . ตามนิยามข้อ 2
4. แสดงให้เห็นว่า F สามารถจะบรรจุ D เป็นโดเมนเชิงจำนวนเต็มอยู่ใน F ได้

ขั้นตอนที่ 1 ให้ D เป็นโดเมนเชิงจำนวนเต็ม

และสร้างผลคูณคาร์ทีเซียน

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

และให้คู่อันดับ (a, b) แทนเศษส่วน $\frac{a}{b}$

นั่นคือ ถ้า $D = Z =$ เซตของจำนวนเต็มแล้ว

คู่อันดับ (2, 3) จะแทนเศษส่วน $\frac{2}{3}$

คู่อันดับ (2, 0) จะไม่แทนสมาชิกตัวไหน ใน Q เลย

ดังนั้น เพื่อตัดกรณีหลังนี้ทิ้งเราจึงตัดเซต $D \times D$ ลงนิดหน่อย เป็น

$\{(a, b) | a, b \in D$ และ $b \neq 0\}$ ให้ชื่อเซตนี้ว่า S

$\therefore\ S = \{(a, b) | a, b \in D$ และ $b \neq 0\}$

มาถึงตรงนี้ S ก็ยังไม่สามารถจะนำมาสร้างสนามได้ เพราะว่าเมื่อ $D = Z$ จะพบว่ามีคู่อันดับต่าง ๆ กันหลายคู่ที่จะแทนเศษส่วนจำนวนเดียวกัน เช่น (2, 3), (4, 6) แทน $\frac{2}{3}$

ดังนั้น เราจึงต้องมากำหนดกันเสียก่อนว่า เมื่อไรสมาชิกของ S จึงจะแทนสมาชิกของ F จำนวนเดียวกัน

นิยาม 3.1.1

สมาชิก (a, b) และ $(c, d) \in S$ จะสมมูลกันก็ต่อเมื่อ $ad = bc$ เขียนแทนด้วยสัญลักษณ์ $(a, b) \sim (c, d)$

นั่นคือ $(a, b) \sim (c, d)$ ก็ต่อเมื่อ $ad = bc$

ขอให้สังเกตว่า นิยามนี้มีเหตุมีผล เพราะเกณฑ์ที่ $(a, b) \sim (c, d)$

คือ สมการ $ad = bc$ เกี่ยวพันกับสมาชิกใน D

นิยาม 3.1.2 สำหรับ $(a, b) \in S$ ให้

$$[(a, b)] = \{(x, y) \in S \mid (x, y) \sim (a, b)\}$$

เรียกเซต $[a, b]$ ว่า กลุ่มสมมูลของ (a, b)

ตัวอย่าง 3.1.1

$$\begin{aligned}[(2, 3)] &= \{(x, y) \in S \mid (x, y) \sim (a, b)\} \\ &= \{(2, 3), (4, 6), (6, 9), \ldots\}\end{aligned}$$

กลุ่มสมมูลเหล่านี้แหละที่จะมาเป็นสมาชิกของ F

ทฤษฎี 3.1.1 คู่อันดับ $(a, b) \in S$ อยู่ใน $[(a, b)]$ และสำหรับสองคู่อันดับ (a, b) และ (c, d) ใน S $[(a, b)] = [(c, d)]$ หรือมิฉะนั้นก็ $[(a, b)] \cap [(c, d)] = \phi$

พิสูจน์

ให้ $(a, b) \in S$

แสดงว่า (a, b) อยู่ใน $[(a, b)]$ จะต้องแสดงว่า $(a, b) \sim (a, b)$

$\because$ D เป็นโดเมนเชิงจำนวนเต็ม ดังนั้น D จึงเป็นวงที่สอดคล้องกฎการสลับที่

$\therefore$ $ab = ba$ ใน D

$\therefore$ $(a, b) \sim (a, b)$

$\therefore$ $(a, b) \in [(a, b)]$

ต่อไปจะแสดงสำหรับ $(a, b), (c, d) \in S$ จะได้ว่า

$$[(a, b)] = [(c, d)] \text{ หรือมิฉะนั้นก็ } [(a, b)] \cap [(c, d)] = \phi$$

ซึ่งเราจะทำโดยสมมติว่า $[(a, b)] \cap [(c, d)] \neq \phi$ จะต้องหาได้ว่า

$$[(a, b)] = [(c, d)]$$

สมมติ $[(a, b)] \cap [(c, d)] \neq \phi$

$$\exists (h, k) \in [(a, b)] \cap [(c, d)]$$

$\therefore$ $(h, k) \in |(a, b)|$ และ $(h, k) \in |(c, d)|$

$hb = ka$ และ $hd = kc$

ให้ $(x, y) \in |(a, b)|$

$\therefore$ $xb = ya$

$$
\begin{aligned}
(xb)dk &= (ya)dk \\
&= yd(ak) \\
&= yd(hb) \\
&= yb(hd) \\
&= yb(kc)
\end{aligned}
$$

ดังนั้น $(xd)bk = (yc)bk$

ถ้า $b \neq 0$, $k \neq 0$ และ D ไม่มีตัวหารของศูนย์ แล้ว

$$xd = yc$$

$$(x, y) \sim (c, d)$$

$\therefore$ $(x, y) \in |(c, d)|$

$\therefore$ $|(a, b)| \subseteq |(c, d)|$.(1)

ในทำนองเดียวกัน เราจะหาได้ว่า

$|(c, d)| \subseteq |(a, b)|$.(2)

จาก (1) และ (2) ได้ว่า

$|(a, b)| = |(c, d)|$ #

นิยาม 3.1.3 ให้ F เป็นเซตของกลุ่มสมมูล $|(a, b)|$ ทั้งหมดสำหรับ $(a, b) \in S$

จบขั้นตอนที่หนึ่ง

ขั้นตอนที่ 2 ทฤษฎีต่อมานี้จะใช้สำหรับนิยาม การบวก และการคูณ ใน F

ทฤษฎี 3.1.2

สำหรับ $[(a, b)]$ และ $[(c, d)]$ ใน F
$[(a, b)] + [(c, d)] = [(ad + bc), bd]$
และ $[(a, b)][(c, d)] = [(ac, bc)]$

พิสูจน์

ก่อนอื่นขอให้สังเกตก่อนว่า ถ้า $[(a, b)]$ และ $[(c, d)] \in F$ แล้ว

(a, b) และ $(c, d) \in S$ ดังนั้น $b \neq 0$ และ $d \neq 0$

เพราะว่า D เป็นโดเมนเชิงจำนวนเต็ม

และ $bd \neq 0$

ดังนั้น $(ad + bc, bd) \in S$ และ $(ac, bd) \in S$

$\therefore$ $[(ad + bc), bd] \in F$ และ $[(ac, bd)] \in F$

จึงเหลือแต่เพียงแสดงว่า การดำเนินการบวก (+) และการคูณ . แจ่มชัด (well defined)

นั่นคือ จะต้องแสดงว่าสำหรับ $(a_1, b_1) \in [(a, b)]$ และ $(c_1, d_1) \in [(c, d)]$

$(a_1d_1 + b_1c_1, b_1d_1) \in [(ad + bc, bd]$

และ $(a_1c_1, b_1d_1) \in [(ac, bd)_1$

$\because$ $(a_1, b_1) \in [(a, b)]$

$\therefore$ $(a_1, b_1) \sim (a, b)$

$\therefore$ $a_1b = b_1a$.(1)

และ $(c_1, d_1) \in [(c, d)]$

$(c_1, d_1) \sim (c, d)$

$c_1d = d_1c$ .... (2)

$(1) \times d_1d$ $a_1bd_1d = b_1ad_1d$ .... (3)

$(2) \times b_1b$ $c_1db_1b = d_1cb_1b$ ....(4)

$$
\begin{aligned}
(3)+(4) \qquad a_1bd_1d + c_1db_1b &= b_1ad_1d + d_1cb_1b \\
(a_1d_1 + c_1b_1)bd &= b_1d_1(ad + cb) \\
(a_1d_1 + b_1c_1)bd &= b_1d_1(ad + bc) \\
(a_1d_1 + b_1c_1, b_1d_1) &\sim (ad + bc, bd) \\
(a_1d_1 + b_1c_1, b_1d_1) &\in [(ad + bc, bd)] \\
(1)\times(2) \qquad a_1bc_1d &= b_1ad_1c \\
a_1c_1bd &= b_1d_1ac \\
(a_1c_1, b_1d_1) &\sim (ac, bd) \\
(a_1c_1, b_1d_1) &\in [(ac, bd)]
\end{aligned}
$$

#

จบขั้นตอนที่ 2

ขั้นตอนที่ 3 จะต้องแสดงว่า F ภายใต้การ + และ . เป็นสนาม นั่นคือ จะต้องแสดงว่า

ก. การบวกใน F สอดคล้องกฎการสลับที่

ข. การบวกใน F สอดคล้องกฎการเปลี่ยนกลุ่ม

ค. $[(0, 1)]$ เป็นเอกลักษณ์สำหรับการบวกใน F

ง. $[(-a, b)]$ เป็นตัวผกผันสำหรับการบวกของ $[(a, b)] \in F$

จ. การคูณใน F สอดคล้องกฎการเปลี่ยนกลุ่ม

ฉ. การคูณใน F สอดคล้องกฎการสลับที่

ช. กฎการแจกแจงเป็นจริงใน F

ซ. (1, 1) เป็นเอกลักษณ์สำหรับการคูณใน F

ฌ. ถ้า $[(a, b)] \in F$ ไม่ใช่เอกลักษณ์สำหรับการบวก แล้ว $a \neq 0$ ใน D และ $[(b, a)]$ เป็นตัวผกผันสำหรับการคูณของ $[(a, b)]$

ในที่นี้จะพิสูจน์เฉพาะข้อ ก, ค และ ฌ นอกนั้นละไว้เป็นแบบฝึกหัด

พิสูจน์

ก. การบวกใน F สอดคล้องกฎการสลับที่

ให้ $[(a, b)], [(c, d)] \in F$

$$\because\ [(a, b)] + [(c, d)] = [(ad + bc, bd)]$$
$$= [(bc + ad, bd)]$$
$$= [(cb + da, bd)]$$
$$= [(c, d)] + [(a, b)]$$

พิสูจน์

ค. $[(0, 1)]$ เป็นเอกลักษณ์สำหรับการ $+$ ใน F

ให้ $[(a, b)] \in F$

$$\because\ [(a, b)] + [(0, 1)] = [(a \,.\, 1 + b \,.\, 0, b \,.\, 1)]$$
$$= [(a, b)]$$

และ $[(0, 1)] + [(a, b)] = [(0 \,.\, b + 1 \,.\, a, 1 \,.\, b)]$

$$= [(a, b)]$$

แสดงว่า $[(0, 1)]$ เป็นเอกลักษณ์สำหรับการ $+$ ใน F

พิสูจน์

ฌ. ถ้า $[(a, b)] \in F$ ไม่ใช่เอกลักษณ์สำหรับการบวก แล้ว $a \neq 0$ และ $[(b, a)]$ เป็นตัวผกผันสำหรับการคูณของ $[(a, b)]$

ให้ $[(a, b)] \in F$

ถ้า $a = 0$

$$a \,.\, 1 = b \,.\, 0 = 0$$

แต่ $a \,.\, 1 = b \,.\, 0 \Rightarrow (a, b) \sim (0, 1)$

นั่นคือ $[(a, b)] = [(0, 1)]$

แต่จาก ค. เราได้ว่า $[(0, 1)]$ เป็นเอกลักษณ์สำหรับการ $+$

ดังนั้น ถ้า $[(a, b)]$ ไม่ใช่เอกลักษณ์สำหรับการบวกใน F

แล้ว $a \neq 0$

และเนื่องจาก $[(a, b)][(b, a)] = [(ab, ba)]$

แต่ใน D เรามี $ab = ba$

หรือ $(ab)1 = (ba)1$

ดังนั้น $(ab, ba) \sim (1, 1)$

$[(a, b)][(b, a)] = [(1, 1)]$

ดังนั้น $[(b, a)]$ เป็นตัวผกผันสำหรับการคูณ

จบขั้นตอนที่ 3

ขั้นตอนที่ 4 ในขั้นตอนนี้จะต้องแสดงให้เห็นว่า F สามารถจะบรรจุ D เป็นโดเมนเชิงจำนวนเต็มอยู่ใน F ได้ ซึ่งเราจะทำโดยแสดงว่ามีฟังก์ชัน monomorphism ψ จาก D ไปยัง F

ทฤษฎี 3.1.3 ให้ $\psi : D \to F$ เป็นฟังก์ชันกำหนดโดย $\psi(a) = [(a, 1)]$ แล้ว ψ เป็น monomorphism

พิสูจน์

ให้ $a, b \in D$

$\because \quad \psi(a + b) = [(a + b, 1)]$

และ $\quad \psi(a) + \psi(b) = [(a, 1)] + [(b, 1)]$

$= [(a\ 1 + 1\ b,\ 1)]$

$= [(a + b,\ 1)]$

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

$\because \quad \psi(a \,.\, b) = [(ab, 1)]$

และ $\quad \psi(a)\,\psi(b) = [(a, 1)][(b, 1)]$

$= [(ab, 1)]$

ดังนั้น $\quad \psi(ab) = \psi(a)\,\psi(b)$

ต่อไปจะแสดงว่า ψ เป็นฟังก์ชันชนิดหนึ่งต่อหนึ่ง

ให้ $a, b \in D \ni \psi(a) = \psi(b)$

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

$\therefore \quad [(a, 1)] = [(b, 1)]$

$(a, 1) \sim (b, 1)$

$a \,.\, 1 = 1 \,.\, b$

$a = b$

$\therefore$ ψ เป็น monomorphism

และ $\psi(D)$ เป็น subdomain ของ F #

จบขั้นตอนที่ 4

และจากการสร้างทั้งสี่ขั้นตอนทำให้เราได้ข้อพิสูจน์ของทฤษฎีข้างล่างนี้ (ทฤษฎี 3.1.4)

ทฤษฎี 3.1.4 โดเมนเชิงจำนวนเต็ม D ใด ๆ สามารถจะขยายขึ้นไปเป็นสนามโดยที่ทุก ๆ สมาชิกของ F สามารถจะเขียนได้ในรูปผลหารของสมาชิกของ D

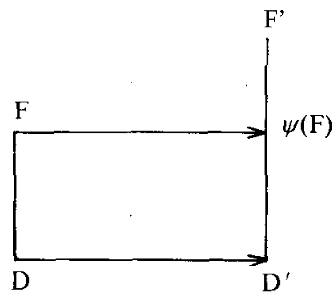
3.2 Uniqueness

ดังได้กล่าวไว้ในตอนต้นของหัวข้อ 3.1 แล้วว่า สนาม F เป็นตัวอย่างของสนามที่เล็กที่สุดที่บรรจุโดเมนเชิงจำนวนเต็มไว้ และเป็นที่เห็นเด่นชัดโดยปราศจากข้อสงสัยว่า เหตุเพราะทุก ๆ สนามที่ประกอบด้วยโดเมนเชิงจำนวนเต็ม D จะต้องประกอบด้วยสมาชิก $\frac{a}{b}$ ทั้งหมด สำหรับ

$a, b \in D$ โดยที่ $b \neq 0$ ทฤษฎีต่อมานี้จะให้แนวคิดที่กว้างขึ้นอีก

ทฤษฎี 3.2.1 ให้ D และ D' เป็นโดเมนเชิงจำนวนเต็มที่ถอดแบบ (isomorphic integral domains) และให้ $\phi : D \to D'$ เป็นฟังก์ชัน monomorphism ให้ F เป็นสนามของผลหารของ D และให้ F' เป็นสนามที่บรรจุ D' ไว้ แล้วจะมีฟังก์ชัน monomorphism ψ จาก F ไปยัง F' ซึ่ง $\psi(a) = \phi(a)$ สำหรับทุก ๆ $a \in D$ เรากล่าวว่า ϕ ขยายออกเป็นฟังก์ชัน monomorphism ψ ของทุกสมาชิกของ F

Proof



รูป 3.1

จากรูปจะช่วยให้เข้าใจทฤษฎีบทได้ดีขึ้น

ทุก ๆ $x \in F$ จะได้ว่า

$$x = \frac{a}{b} \quad \text{โดยที่ } a, b \in D \text{ และ } b \neq 0$$

กำหนด $\psi : F \to F'$ โดย $\psi\left(\frac{a}{b}\right) = \phi(a)/\phi(b)$

เราจะต้องแสดงก่อนว่า ψ ตามที่กำหนดนี้ มีเหตุผลเป็นไปได้ และแจ่มชัด

$\because$ ϕ เป็นฟังก์ชัน monomorphism

$\therefore$ สำหรับ $b \neq 0$ เรามี

$$\phi(b) \neq 0$$

ดังนั้น $\psi\left(\frac{a}{b}\right) = \frac{\phi(a)}{\phi(b)}$ มีเหตุผลเป็นไปได้

ถ้า $\frac{a}{b} = \frac{c}{d}$ ใน F แล้ว

$ad = bc$ ใน D

ดังนั้น $\phi(ad) = \phi(bc)$

แต่ ϕ เป็นฟังก์ชัน monomorphism

$\therefore\ \phi(ad) = \phi(a)\,\phi(d)$

และ $\phi(bc) = \phi(b)\,\phi(c)$

ดังนั้น $\frac{\phi(a)}{\phi(b)} = \frac{\phi(c)}{\phi(d)}$ ใน F'

ดังนั้น ψ แจ่มชัด (well defined)

สมการ $\psi(xy) = \psi(x)\,\psi(y)$

และ $\psi(x + y) = \psi(x) + \psi(y)$

จะเป็นผลตามมาจากนิยามของ ϕ และจากความจริงที่ว่า ϕ เป็นฟังก์ชัน monomorphism

ถ้า $\psi\left(\frac{a}{b}\right) = \psi\left(\frac{c}{d}\right)$ แล้ว

$$\frac{\phi(a)}{\phi(b)} = \frac{\phi(c)}{\phi(d)}$$

$$\phi(a)\,\phi(d) = \phi(b)\,\phi(c)$$

เนื่องจาก ϕ เป็นฟังก์ชัน monomorphism

$$\phi(a)\,\phi(d) = \phi(ad)$$

และ $\phi(b)\,\phi(c) = \phi(bc)$

$\therefore\ \phi(ad) = \phi(bc)$

ดังนั้น $ad = bc$

เพราะว่า ϕ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

ดังนั้น $\frac{a}{b} = \frac{c}{d}$

ดังนั้น ψ เป็นฟังก์ชันหนึ่งต่อหนึ่ง

สำหรับ $a \in D$

$$\psi(a) = \psi\left(\frac{a}{1}\right)$$

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

$$= \phi(a)$$

เนื่องจาก $\phi(1)$ เป็นเอกลักษณ์ของ D'

ดังนั้น $\phi(a) = \psi(a)$ สำหรับ $a \in D$

นั่นคือ ψ ขยาย ϕ (ψ extends ϕ) #

บทแทรก 1 ทุก ๆ สนาม F' ที่บรรจุโดเมนเชิงจำนวนเต็ม D บรรจุสนามของผลหารของ D

ข้อพิสูจน์ละไว้ให้ น.ศ. ทำ

บทแทรก 2 ทุก ๆ สองสนามของผลหารของโดเมนเชิงจำนวนเต็ม D ถอดแบบกัน (isomorphic)

พิสูจน์

จากทฤษฎี 3.2.1 ถ้า F' เป็นสนามของผลหารของ D' แล้ว สำหรับทุก ๆ $x' \in F'$ จะเขียนได้เป็น

$$x' = \frac{a'}{b'} \text{ สำหรับ } a', b' \in D'$$

เนื่องจาก ϕ เป็นฟังก์ชันทั่วถึงบน D' จึงได้ว่า

สำหรับ $a', b' \in D'$ จะมี $a, b \in D$ ซึ่ง

$$\phi(a) = a' \text{ และ } \phi(b) = b'$$

แล้ว $\psi\left(\frac{a}{b}\right) = \frac{a'}{b'}$

$\therefore$ ψ เป็นฟังก์ชันทั่วถึงไปบน F'

ให้ $D' = D$ และ ϕ เป็น identity map

เราจะได้ บทแทรกที่ 2

แบบฝึกหัดที่ 3

1) จงพิจารณาข้อความแต่ละข้อต่อไปนี้เป็นจริงหรือเป็นเท็จ

..............ก) Q เป็นสนามของผลหารของ Z

..............ข) R เป็นสนามของผลหารของ Z

..............ค) R เป็นสนามของผลหารของ R

..............ง) C เป็นสนามของผลหารของ R

..............จ) ถ้า D เป็นสนามแล้วสนามของผลหารใด ๆ ของ D ถอดแบบกับ D

..............ฉ) เป็นความจริงว่า D ที่ไม่มีตัวหารของศูนย์ถูกใช้หลายครั้งในการสร้างสนาม F ซึ่งเป็นสนามของผลหารของโดเมนเชิงจำนวนเต็ม D

..............ช) ทุก ๆ สมาชิกของโดเมนเชิงจำนวนเต็ม D เป็น unit ในสนาม F ซึ่งเป็นสนามของผลหารของ D

..............ซ) ทุก ๆ สมาชิกที่ไม่ใช่ 0 ของโดเมนเชิงจำนวนเต็ม D เป็น unit ในสนาม F ซึ่งเป็นสนามของผลหารของ D

..............ฌ) สนาม F' ซึ่งเป็นสนามของผลหารของโดเมนเชิงจำนวนเต็มย่อย D' ของโดเมนเชิงจำนวนเต็ม D สามารถจะเป็นสนามย่อยของบางสนามของผลหารของ D

2) จงบอกสมาชิกของสนาม F ซึ่งเป็นสนามของผลหารของโดเมนย่อยเชิงจำนวนเต็ม $D = \{(n + mi \mid m, n \in Z\}$ ของ C

3) จงบอกสมาชิกของสนาม F ซึ่งเป็นสนามของผลหารของโดเมนย่อยเชิงจำนวนเต็ม $D = \{n + m\sqrt{2} \mid m, n \in Z\}$ ของ R

4) จงแสดงโดยยกตัวอย่างสนาม F' ซึ่งเป็นสนามของผลหารของโดเมนย่อยแท้เชิงจำนวนเต็ม D' ของโดเมนเชิงจำนวนเต็ม D อาจเป็นสนามของผลหารของ D ด้วยเหมือนกัน

5) จงพิสูจน์ บทแทรกที่ 1 ของทฤษฎี 3.2.1