บทที่ 9
ฟีลด์และสมบัติเบื้องต้นของฟีลด์

ในบทนี้จะกล่าวถึงบทนิยามของโครงสร้างทางพีชคณิตที่ประกอบด้วยการดำเนินการทวิภาคสองการดำเนินการทวิภาคที่มีสมบัติมากที่สุด ประกอบด้วยหัวข้อต่าง ๆ 3 เรื่อง คือ บทนิยามและสมบัติเบื้องต้นของฟีลด์ ฟีลด์ของผลหาร และการแยกตัวประกอบของฟีลด์ ดังนี้

บทนิยามและสมบัติเบื้องต้นของฟีลด์

ถ้าเราพิจารณาริง R ที่มี 0 เป็นสมาชิกศูนย์ จะได้ว่า R เป็นเพียงกึ่งกรุปภายใต้การคูณเท่านั้น แต่ถ้า $R \setminus \{0\}$ จะเป็นอาบีเลียนกรุปภายใต้การคูณ แล้วเราจะเรียกริง R ดังบทนิยามต่อไปนี้

บทนิยาม 9.1 เรียกริง R ว่าฟีลด์ (field) ก็ต่อเมื่อ เป็นริงการหารและริงสลับที่

$(\mathbb{Q},+,\cdot),(\mathbb{R},+,\cdot)$ และ $(\mathbb{C},+,\cdot)$ เป็นตัวอย่างของระบบที่เป็นฟีลด์ แต่ระบบ $(\mathbb{Z},+,\cdot)$ ไม่เป็นฟีลด์

ทฤษฎีบท 9.2 ทุกฟีลด์เป็นอินทิกรัลโดเมน

การพิสูจน์ กำหนดให้ F เป็นฟีลด์
ดังนั้น F เป็นริงการหารและริงสลับที่
เนื่องจาก $F \setminus \{0\}$ กับการคูณเป็นกรุป
ทำให้ได้ว่า F เป็นริงที่มีสมาชิกเอกลักษณ์ 1
สำหรับ $a, b \in F$ ที่ซึ่ง $ab = 0$
จะได้ว่า ถ้า $a \neq 0$ แล้วจะมี $a' \in F$ ที่ทำให้ $a'a = 1$ ดังนั้น

$$b = 1b = (a'a)b = a'(ab) = a0 = 0$$

นั่นคือ F เป็นอินทิกรัลโดเมน

ทฤษฎีบท 9.3 อินทิกรัลโดเมนที่มีจำนวนสมาชิกจำกัดเป็นฟีลด์

การพิสูจน์ กำหนดให้ D เป็นอินทิกรัลโดเมนที่มีสมาชิกจำนวนจำกัด
ดังนั้น D เป็นริงสลับที่ที่ไม่มีตัวหารของศูนย์
จึงได้ว่า $D \setminus \{0\}$ มีสมบัติการปิด การสลับที่ และการเปลี่ยนหมู่ภายใต้การคูณ
ต่อไปจะแสดงว่า $D \setminus \{0\}$ กับการคูณเป็นกรุป

(1) จะแสดงว่า มี $1 \in D$ ที่ทำให้ $a1 = a$ สำหรับทุก $a \in D$
สมมติให้ $D = \{a_1, a_2, \ldots, a_n\}$ โดยที่ a_i แตกต่างกันหมด
และสมมติให้ $0 \neq a \in D$
พิจารณา $a_1a, a_2a, \ldots, a_na$
จะได้ว่า $a_ia \in D$ สำหรับทุก $i = 1, 2, \ldots, n$
ในกรณีที่ $i \neq j$ ถ้าให้ $a_ia = a_ja$ แล้ว $(a_i - a_j)a = 0$
แต่เนื่องจาก $a \neq 0$ จึงทำให้ $a_i - a_j = 0$
นั่นคือ $a_i = a_j$ เป็นผลให้ $i = j$
นั่นคือ ถ้า $i \neq j$ แล้ว $a_ia \neq a_ja$
เนื่องจาก D มีสมาชิก n ตัว จึงทำให้ $D = \{a_1a, a_2a, \ldots, a_na\}$
เพราะว่า $a \in D$ ดังนั้น จะมี $a_{i_o} \in D$ ที่ทำให้ $a = a_{i_o}a = aa_{i_o}$
ดังนั้น สำหรับแต่ละ $b \in D$ จะได้ว่า $b = a_ka$ สำหรับบาง $a_k \in D$ จึงได้ว่า

$$ba_{i_o} = (a_ka)a_{i_o} = a_k(aa_{i_o}) = a_ka = b$$

นั่นคือ $ba_{i_o} = b$ สำหรับทุก $b \in D$
เพราะฉะนั้น a_{i_o} เป็นสมาชิกเอกลักษณ์ของ D
นั่นคือ มี $1 = a_{i_o} \in D$ ที่ทำให้ $b1 = b$ สำหรับทุก $b \in D$

(2) จะแสดงว่า สำหรับแต่ละ $0 \neq a \in D$ จะมี $b \in D$ ที่ทำให้ $ab = 1$
เนื่องจาก $1 \in D$ จะได้ว่า

$$1 = a_ma = aa_m \text{ สำหรับบาง } a_m \in D$$

นั่นคือ สำหรับ $a \neq 0$ จะมี $a_m \in D$ ที่ทำให้ $aa_m = 1$
ดังนั้น $D \setminus \{0\}$ กับการคูณเป็นอาบีเลียนกรุป
จึงสรุปได้ว่า D เป็นฟีลด์

ผลพลอยได้จากทฤษฎีบท 9.3 คือ

บทแทรก 9.4 $\mathbb{Z}_n$ เป็นฟีลด์ ก็ต่อเมื่อ n เป็นจำนวนเฉพาะ

การพิสูจน์ สมมติให้ $\mathbb{Z}_n$ เป็นฟีลด์ และ a เป็นจำนวนเต็มบวกที่ซึ่ง $a|n$
จะได้ว่า $1 \leq a \leq n$ และ $n = aq$ สำหรับบาง $q \in N$ โดยที่ $1 \leq q \leq n$
ดังนั้น

$$[0] = [n] = [aq] = [a] \cdot_n [q]$$

โดยทฤษฎีบท 9.2 จะได้ว่า $\mathbb{Z}_n$ เป็นอินทิกรัลโดเมน
ดังนั้น $\mathbb{Z}_n$ ไม่มีตัวหารของศูนย์
จึงทำให้ $[a] = [0]$ หรือ $[q] = [0]$
ถ้า $[a] = [0]$ จะได้ว่า $[a] = [n]$ นั่นคือ $a = n$
แต่ถ้า $[q] = [0]$ แล้วจะได้ว่า $[q] = [n]$
นั่นคือ $q = n$ จึงทำให้ $a = 1$ นั่นคือ n เป็นจำนวนเฉพาะ
ในทางกลับกัน กำหนดให้ n เป็นจำนวนเฉพาะ
เห็นได้ชัดว่า $(\mathbb{Z}_n, +_n, \cdot_n)$ เป็นริงสลับที่ที่มีสมาชิกเอกลักษณ์
จะแสดงว่า $\mathbb{Z}_n$ เป็นอินทิกรัลโดเมน โดยให้ $[a], [b] \in \mathbb{Z}_n$ ที่ซึ่ง $[a] \cdot_n [b] = [0]$
ทำให้ได้ว่า $[ab] = [0]$ นั่นคือ $n|ab$
เนื่องจาก n เป็นจำนวนเฉพาะ จึงได้ว่า $n|a$ หรือ $n|b$
นั่นคือ $[a] = [0]$ หรือ $[b] = [0]$
นั่นคือ $\mathbb{Z}_n$ ไม่มีตัวหารของศูนย์
จึงสรุปได้ว่า $\mathbb{Z}_n$ เป็นอินทิกรัลโดเมนที่มีจำนวนสมาชิก n ตัว
โดยทฤษฎีบท 9.3 จะได้ว่า $\mathbb{Z}_n$ เป็นฟีลด์

ทฤษฎีบทต่อไปนี้จะให้ความสัมพันธ์ระหว่างไอดีลของริงกับความเป็นฟีลด์ของริงนั้น

ทฤษฎีบท 9.5 กำหนดให้ R เป็นริงสลับที่ที่มีสมาชิกเอกลักษณ์ ถ้าไอดีลของ R มีเพียงไอดีล-ทริเวียล ($\{0\}$ และ R) เท่านั้น แล้ว R เป็นฟีลด์

การพิสูจน์ กำหนดให้ R เป็นริงสลับที่ที่มีสมาชิกเอกลักษณ์ 1 และไอดีลของ R มีเพียง $\{0\}$ และ R เท่านั้น
จะแสดงว่า R เป็นฟีลด์ นั่นคือ จะแสดงว่าสำหรับแต่ละ $0 \neq a \in R$
จะมี $b \in R$ ที่ทำให้ $ab = 1$
สมมติให้ $0 \neq a \in R$ พิจารณา

$$Ra = \{ra | a \in R\} \subseteq R$$

สมมติให้ $r_1 a, r_2 a \in Ra$
จะเห็นว่า $r_1 a + r_2 a = (r_1 + r_2)a \in Ra$ และ $-(r_1) = (-r_1)a \in Ra$
ดังนั้น ra เป็นกรุปย่อยของ R ภายใต้การบวก
และถ้า $r \in R$ แล้ว $r(r_1) = (rr_1)a \in Ra$
เพราะฉะนั้น Ra เป็นไอดีลของ R
เนื่องจาก $a = 1a \in Ra$ โดยที่ $a \neq 0$ ทำให้ได้ว่า $Ra \neq \{0\}$
และจาก R มีเพียง $\{0\}$ และ R เป็นไอดีลของ R เท่านั้น
ดังนั้น $Ra = R$
เนื่องจาก $1 \in R$ จึงได้ว่า $1 \in Ra$ ดังนั้น $1 = ba$ สำหรับบาง $b \in R$
จึงสรุปได้ว่า $R - \{0\}$ เป็นอาบีเลียนกรุปภายใต้การคูณ นั่นคือ R เป็นฟีลด์

ทฤษฎีบท 9.6 ถ้า F เป็นฟีลด์ แล้วไอดีลของ F มีเพียงไอดีลทริเวียล ($\{0\}$ และ F) เท่านั้น

การพิสูจน์ กำหนดให้ F เป็นฟีลด์ และสมมติว่า I เป็นไอดีลของ F โดยที่ $I \neq \{0\}$
จะได้ว่ามี $a \in I$ ที่ซึ่ง $a \neq 0$
เนื่องจาก F เป็นฟีลด์ ดังนั้น $F - \{0\}$ เป็นอาบีเลียนกรุปภายใต้การคูณ
นั่นคือ จะมี $a^{-1} \in F$ ที่ทำให้ $aa^{-1} = 1$
แต่เนื่องจาก I เป็นไอดีลของ F
จึงได้ว่า $aa^{-1} \in I$ นั่นคือ $1 \in I$
เพราะฉะนั้น $b = 1b \in I$ สำหรับทุก $b \in F$ นั่นคือ $F \subseteq I$
เพราะฉะนั้น $I = F$
จึงสรุปได้ว่า F มีเพียงไอดีลทริเวียล ($\{0\}$ และ F) เท่านั้น

จากทฤษฎีบท 9.5 จะได้ว่าเงื่อนไขที่จำเป็น และเพียงพอที่จะทำให้ริงผลหาร R/M เป็นฟีลด์ ก็คือ M จะต้องเป็นไอดีลใหญ่สุด ดังบทนิยามต่อไปนี้

ทฤษฎีบท 9.7 กำหนดให้ R เป็นริงสลับที่ที่มีสมาชิกเอกลักษณ์ และ M เป็นไอดีลของ R จะได้ว่า M เป็นไอดีลใหญ่สุดของ R ก็ต่อเมื่อ R/M เป็นฟิลด์

การพิสูจน์ กำหนดให้ R เป็นริงสลับที่ที่มีสมาชิกเอกลักษณ์ 1 และ M เป็นไอดีลของ R และให้ M เป็นไอดีลใหญ่สุดของ R เนื่องจาก R เป็นริงสลับที่ที่มีสมาชิกเอกลักษณ์ 1 จึงทำให้ R/M เป็นริงสลับที่ที่มีสมาชิกเอกลักษณ์ $1+M$
สมมติให้ I^* เป็นไอดีลของ R/M โดยที่ $I^* \neq \{M\}$
จะเห็นว่า ถ้า $a \in M$ แล้ว $a+M = M$
ดังนั้น จะมี $a \notin M$ ที่ซึ่ง $a+M \in I^*$ พิจารณา

$$I = M \cup \{a \in R | a+M \in I^*\}$$

จะได้ว่า I เป็นไอดีลของ R โดยที่ $M \subseteq I$ และ $M \neq I$
เนื่องจาก M เป็นไอดีลใหญ่สุดของ R
ดังนั้น จึงได้ว่า $I = R$
และเพราะว่า I^* เป็นกรุปย่อยของ R/M ภายใต้การบวก
ดังนั้น $M = 0 + M \in I^*$ และเนื่องจาก $1 \in R$
จึงได้ว่า $1 \in I$
กรณีที่ $1 \in M$
จะได้ว่า $1 + M = M \in I^*$
แต่ถ้า $1 \in \{a \in R | a + M \in I^*\}$ แล้ว $1 + m \in I^*$
จึงสรุปได้ว่า $1 + M \in I^*$
สำหรับแต่ละ $r + M \in R/M$
จะได้ว่า $(r + M)(1 + M) \in I^*\}$ ทั้งนี้เพราะว่า I^* เป็นไอดีลของ R/M
แต่เนื่องจาก

$$(r + M)(1 + M) = (r1) + M = r + M$$

ดังนั้น จึงได้ $r + M \in I^*$ นั่นคือ $I^* = R/M$
เพราะฉะนั้น R/M มีเพียงทริเวียลไอดีล ($\{m\}$ และ R/M) เท่านั้น
โดยทฤษฎีบท 3.7 จะได้ว่า R/M เป็นฟิลด์

ในทางกลับกัน สมมติให้ R/M เป็นฟีลด์ และ J เป็นไอดีลของ R
โดยที่ $M \subseteq J$ และ $M \neq J$
จะได้ว่ามี $a \in J - M$ และ $a + M \neq M$
เนื่องจาก R/M เป็นฟีลด์
จะได้ว่ามี $b + M \in R/M$
ที่ทำให้ $(a + M)(b + M) = (ab) + M = 1 + M$
นั่นคือ $M = (1 - ab) + M$
จึงได้ว่า $1 - ab \in M \subseteq J$ โดยที่ $ab \in J$
ดังนั้น $1 = (1 - ab) + ab \in J$
ดังนั้น $r = 1r \in J$ สำหรับทุก $r \in R$
นั่นคือ $R \subseteq J$ จึงได้ว่า $J = R$
เพราะฉะนั้น M เป็นไอดีลใหญ่สุดของ R

สรุปท้ายบท

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