บทที่ 15
สนามจำกัด
(Finite fields)

จุดประสงค์ของการศึกษาในบทนี้คือ การจะกำหนดโครงสร้างของสนามจำกัดทั้งหมด เราจะแสดงว่าสำหรับทุก ๆ จำนวนเฉพาะ p และจำนวนเต็มบวก n จะมีสนามจำกัดแน่นอนสนามหนึ่งของอันดับ p^n สนาม $GF(p^n)$ นี้ บ่อยครั้งที่เราเรียก "สนามกาลัวส์อันดับ p^n"

15.1 โครงสร้างของสนามจำกัด

(The structure of a finite field)

ทฤษฎี 15.1.1 ให้ E เป็นภาคยืดขยายจำกัดที่มีลำดับขั้น n เหนือสนามจำกัด F ถ้า F มีสมาชิก q ตัว แล้ว E มีสมาชิก q^n ตัว

พิสูจน์

ให้ $\{\alpha_1, \ldots, \alpha_n\}$ เป็นฐานของ E ซึ่งเป็นปริภูมิเวกเตอร์ F

แล้วทุก ๆ $\beta \in E$ สามารถเป็น uniquely เขียนได้ในรูป

$$\beta = b_1\alpha_1 + \ldots + b_n\alpha_n$$

สำหรับ $b_i \in F$

เนื่องจาก แต่ละ b_i อาจเป็นสมาชิก q ใด ๆ ของ F

จำนวนทั้งหมดของผลบวกเชิงเส้นที่แยกกันเด็ดขาดของ α_i คือ q^n #

บทแทรก ถ้า E เป็นสนามจำกัดที่มีลักษณะเฉพาะ p แล้ว E จะประกอบด้วยสมาชิกที่แน่นอน p^n ตัว สำหรับบางจำนวนเต็มบวก n

พิสูจน์

ทุก ๆ สนามจำกัด E เป็นภาคยืดขยายจำกัดของสนามจำนวนเฉพาะที่ถอดแบบกับสนาม Z_p โดยที่ p เป็นลักษณะเฉพาะของ E

โดยทฤษฎี 15.1.1 เราได้ข้อพิสูจน์โดยทันทีของบทแทรก

ทฤษฎี 15.1.2 สนามจำกัด E ที่มีสมาชิก p^n ตัว เป็นสนามแยกส่วนของ $x^{p^n} - x$ เหนือสนามย่อยจำนวนเฉพาะ Z_p

พิสูจน์

ให้ E เป็นสนามจำกัดที่มีสมาชิก p^n ตัว โดยที่ p เป็นลักษณะเฉพาะของ E

เซต E* เป็นเซตของสมาชิกที่ไม่ใช่ศูนย์ (nonzero) ของ E เป็นกลุ่มภายใต้การคูณที่มีอันดับ $p^n - 1$

สำหรับ $\alpha \in E^*$ อันดับของ α ในกลุ่มนี้หารอันดับ $p^n - 1$ ของกลุ่มได้ลงตัว

ดังนั้น สำหรับ $\alpha \in E^*$ เราได้

$$\alpha^{p^n-1} = 1$$

ดังนั้น $\alpha^{p^n} = \alpha$

ฉะนั้นสมาชิกทุกตัวใน E เป็นศูนย์ของ $x^{p^n} - x$

เนื่องจาก $x^{p^n} - x$ สามารถจะมีศูนย์ได้อย่างมากที่สุด p^n ตัว

เราจะเห็นว่า E เป็นสนามแยกส่วนของ $x^{p^n} - x$ เหนือ Z_p #

นิยาม สมาชิก α ของสนาม เป็นรากที่ n ของยูนิตี้ (n^{th} root of unity) ถ้า $\alpha^n = 1$, เป็นรากที่ n ปฐมฐานของยูนิตี้ (primitive n^{th} root of unity) ถ้า $\alpha^n = 1$ และ $\alpha^m \neq 1$ สำหรับ $0 < m < n$

ดังนั้น สมาชิกที่ไม่ใช้ศูนย์ (nonzero elements) ของสนามจำกัดที่มีสมาชิก p^n ตัว ล้วนเป็นรากที่ $(p^n - 1)$ ของยูนิตี้ทั้งหมด

ให้ F เป็นสนามใด ๆ และให้ U_n เป็นเซตของรากที่ n ทั้งหมดของยูนิตี้ใน F, ง่ายสำหรับเราที่จะดูว่า U_n เป็นกลุ่มภายใต้การคูณ ถ้า $a^n = 1$ และ $b^n = 1$ แล้ว

$$(ab)^n = a^n b^n = 1$$

ดังนั้น การคูณปิดบน U_n เราอ้าง U_n เป็นกลุ่มวัฏจักร

ทฤษฎี 15.1.3 ถ้า G เป็นกลุ่มย่อยจำกัดภายใต้การคูณของกลุ่ม $(F^*, .)$ ซึ่ง F^* เป็นเซตของสมาชิกที่ไม่ใช่ศูนย์ (nonzero) ของสนาม F แล้ว G เป็นกลุ่มวัฏจักร

พิสูจน์

$\because$ G เป็นกลุ่มอาบีเลียนที่มีสมาชิกจำกัด

$\therefore$ G ถอดแบบกับ direct product $Z_{m_1} \times Z_{m_2} \times \ldots \times Z_{m_r}$ ของกลุ่มวัฏจักร โดยที่ m_i หาร m_{i+1} ลงตัว

พิจารณาให้แต่ละสมาชิกของ Z_{m_i} เป็นกลุ่มวัฏจักรที่มีอันดับ m_i ภายใต้การคูณ

แล้วสำหรับ $a_i \in Z_{m_i}$, $a_i^{m_i} = 1$

ดังนั้น $a_i^{m_r} = 1$

เนื่องจาก m_i หาร m_r ได้ลงตัว

ดังนั้น สำหรับ $\forall \alpha \in G$ ทำให้ $\alpha^{m_r} = 1$

ฉะนั้น สมาชิกของ G ทุกตัวเป็นศูนย์ของ $x^{m_r} - 1$

แต่ G มีสมาชิก $\pi_{i=1}^{r} m_i$ ตัว ขณะที่ $x^{m_r} - 1$ สามารถจะมีศูนย์ในสนามได้อย่างมากที่สุด m_r ตัว

ดังนั้น เราจะต้องได้ $r = 1$

$\therefore$ G เป็นกลุ่มวัฏจักร #

บทแทรก 1 กลุ่มของสมาชิกที่ไม่ใช่ศูนย์ (nonzero) ทั้งหมดของสนามจำกัด ภายใต้การคูณเป็นกลุ่มวัฏจักร

พิสูจน์

ผลได้โดยทันทีจากทฤษฎี 15.1.3

บทแทรก 2 ภาคยืดขยายจำกัด E ของสนามจำกัด F เป็นภาคยืดขยายอย่างง่าย (simple extension) ของ F

พิสูจน์

ให้ α เป็นตัวก่อกำเนิดของกลุ่มวัฏจักร E^* ของสมาชิกที่ไม่ใช่ศูนย์ของ E แล้ว $E = F(\alpha)$

#

ตัวอย่าง 15.1.1 พิจารณาสนามจำกัด Z_{11}

โดยบทแทรกที่ 1 ของทฤษฎี 15.1.3

$(Z_{11}^*, .)$ เป็นกลุ่มวัฏจักร

เราลองมาหาตัวก่อกำหนดของ Z_{11}^* ดู

เราจะเริ่มต้นที่ 2

เนื่องจาก $|Z_{11}^*| = 10$

2 จะต้องเป็นสมาชิกของ Z_{11}^* ซึ่งอันดับหาร 10 ลงตัว

นั่นคือ 2, 5 หรือ 10

แต่ $2^2 = 4$, $2^4 = 4^2 = 5$ และ $2^5 = (2)(5) = 10 = -1$

ดังนั้น ไม่ใช่ทั้ง 2^2 และ 2^5 เป็น 1

แต่แน่นอน $2^{10} = 1$

ดังนั้น 2 เป็นตัวก่อกำเนิดของ Z_{11}^*

นั่นคือ 2 เป็นรากที่ 10 ปฐมฐานของ unity ใน Z_{11}

โดยทฤษฎีของกลุ่มวัฏจักร ตัวก่อกำเนิดทั้งหมดของ Z_{11}^* (ซึ่งคือ รากที่ 10 ปฐมฐานของ unity ใน Z_{11}) จะต้องอยู่ในรูป 2^n โดยที่ n เป็นจำนวนเฉพาะสัมพัทธ์กับ 10 สมาชิกเหล่านี้คือ

$2^1 = 2,\ 2^3 = 8$

$2^7 = 7,\ 2^9 = 6$

รากที่ 5 ปฐมฐานของ unity ใน Z_{11} จะอยู่ในรูป 2^m โดยที่ ห.ร.ม. ของ m และ 10 คือ 2 นั่นคือ

$2^2 = 4,\ 2^4 = 5$

$2^6 = 9,\ 2^8 = 3$

รากที่ 2 ปฐมฐานของ unity ใน Z_{11} คือ $2^5 = 10 = 1$ #

15.2 การมีของ $GF(p^n)$

(The existence of $GF(p^n)$)

เรากลับมาที่คำถามของการมีของสนามจำกัดของอันดับ p^r สำหรับทุก ๆ กำลังจำนวนเฉพาะ p^r; $r > 0$

ทฤษฎี 15.2.1 ถ้า F เป็นสนามจำกัด ที่มีลักษณะเฉพาะ p แล้ว $x^{p^n} - x$ มีศูนย์ที่แยกกันเด็ดขาด p^n ตัวในสนามแยกส่วน $K \leq \bar{F}$ ของ $x^{p^n} - x$ เหนือ F

พิสูจน์

ให้ F เป็นสนามจำกัดที่มีลักษณะเฉพาะ p

ให้ K เป็นสนามแยกส่วนใน $\bar{F}$ ของพหุนาม $x^{p^n} - x$ เหนือ F

เราจะต้องแสดงว่า $x^{p^n} - x$ มีศูนย์ (ที่แยกกันเด็ดขาด) ใน K ทั้งหมด p^n ตัว

เนื่องจาก 0 เป็นศูนย์ของ $x^{p^n} - x$ ของภาวะรากค่าซ้ำ 1

สมมติ $a \neq 0$ เป็นศูนย์ของ $x^{p^n} - x$ และในที่นี้เป็นศูนย์ของ $f(x) = x^{p^n-1} - 1$ แล้ว

$x - a$ เป็นตัวประกอบตัวหนึ่งของ $f(x) \in K[x]$

และโดยการหารยาว เราพบว่า

$$\frac{f(x)}{x - a} = g(x)$$

$$= x^{p^n-2} + \alpha x^{p^n-3} + \alpha^2 x^{p^n-4} + \ldots + \alpha^{p^n-3}x + \alpha^{p^n-2}$$

$\therefore$ g(x) มีผลบวก $p^n - 1$ เทอม

และใน $g(\alpha)$ แต่ละผลบวกคือ

$$\alpha^{p^n-2} = \frac{\alpha^{p^n-1}}{\alpha} = \frac{1}{\alpha}$$

ดังนั้น $g(\alpha) = [(p^n - 1) . 1] \frac{1}{\alpha}$

$$= -\frac{1}{\alpha}$$

เนื่องจาก สนามนี้มีลักษณะเฉพาะ p

ดังนั้น $g(\alpha) \neq 0$

ดังนั้น α เป็นศูนย์ f(x) ของภาวะรากค่าซ้ำ 1 #

ทฤษฎี 15.2.2 มีสนามจำกัด $GF(p^n)$ ที่มีสมาชิก p^n ตัว สำหรับทุก ๆ กำลังจำนวนเฉพาะ p^n

พิสูจน์

ให้ $K \leqslant \bar{Z}_p$ เป็นสนามแยกส่วนของ $x^{p^n} - x$ เหนือ Z_p

ให้ F เป็นเซตย่อยของ K ประกอบด้วยศูนย์ทั้งหมดของ $x^{p^n} - x$ ใน K

แล้วสำหรับ $\alpha, \beta \in F$,

$$(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta$$

และ $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$

แสดงว่า F สอดคล้องกฎการปิดภายใต้การบวก การลบ และการคูณ

$\therefore$ 0 และ 1 เป็นศูนย์ของ $x^{p^n} - x$

สำหรับ $\alpha \neq 0$, ถ้า $\alpha^{p^n} = \alpha$ แล้ว $(1/2)^{p^n} = \frac{1}{\alpha}$

ดังนั้น F เป็นสนามย่อยของ K บรรจุ Z_p ไว้

เนื่องจาก K เป็นภาคยืดขยายที่เล็กที่สุดของ Z_p ที่บรรจุศูนย์ของ $x^{p^n} - x$

เราจะเห็นว่าเราจะต้องมี $K = F$

ดังนั้น K เป็นสนามที่ต้องการสมาชิก p^n ตัว เนื่องจากโดยทฤษฎี 15.1.4 แสดงว่า $x^{p^n} - x$ มีศูนย์ (ที่แยกกันเด็ดขาด) p^n ตัวใน $\bar{Z}_p$ #

บทแทรก	ถ้า F เป็นสนามจำกัด แล้วทุก ๆ จำนวนเต็มบวก n มีพหุนามลดทอนไม่ได้ที่มีลำดับขั้น n ใน $F[x]$

พิสูจน์

ให้ F มีสมาชิก $q = p^r$ ตัว โดยที่ p เป็นลักษณะเฉพาะของ F

โดยทฤษฎี 15.1.5

มีสนาม $K \leqslant \bar{F}$ บรรจุ Z_p ได้ และประกอบด้วยศูนย์ของ $x^{p^{rn}} - x$

สมาชิกทุก ๆ ตัวของ F เป็นศูนย์ของ $x^{p^r} - x$

$\therefore\ p^{rs} = p^r p^{r(s-)}$ ....(*)

ใช้สมการ (*) ซ้ำ และใช้ความจริงที่ว่า สำหรับ $\alpha \in F$ เรามี $\alpha^{p^r} = \alpha$ เราพบว่า สำหรับ $\alpha \in F$

$$\alpha^{p^{rn}} = \alpha^{p^{r(n-1)}}$$

$$= \alpha^{p^{r(n-2)}} = \ldots = \alpha^{p^r} = \alpha$$

ดังนั้น $F \leqslant K$ แล้ว

ทฤษฎี 15.1.1 แสดงว่า เราจะต้องมี $|K : F| = n$

เราพบแล้วว่า K เป็นสนามอย่างง่ายเหนือ F ในบทแทรก 2 ของทฤษฎี 15.1.3

ดังนั้น $K = F(\beta)$ สำหรับบาง $\beta \in K$

ดังนั้น $\mathrm{irr}(\beta, F)$ จะต้องมีลำดับขั้น n #

แบบฝึกหัดที่ 15

1) จงพิจารณาข้อความแต่ละข้อต่อไปนี้เป็นจริงหรือเท็จ

..............ก) สมาชิกที่ไม่ใช่ 0 ของทุก ๆ สนามจำกัดเป็นกลุ่มวัฏจักรภายใต้การคูณ

..............ข) สมาชิกของทุก ๆ สนามจำกัดเป็นกลุ่มวัฏจักรภายใต้การบวก

..............ค) มีสนามจำกัดที่มีสมาชิก 60 ตัว

..............ง) มีสนามจำกัดที่มีสมาชิก 125 ตัว

..............จ) มีสนามจำกัดที่มีสมาชิก 36 ตัว

..............ฉ) จำนวนเชิงซ้อน i เป็นรากที่ 4 ปฐมฐานของ unity

..............ช) มีพหุนามลดทอนไม่ได้ที่มีลำดับขั้น 58 ใน $Z_{12}[x]$

..............ซ) สมาชิกที่ไม่ใช่ 0 ของ Q เป็นกลุ่มวัฏจักร Q* ภายใต้การคูณ

..............ฌ) ถ้า F เป็นสนามจำกัด แล้วทุก ๆ ฟังก์ชันถอดแบบส่ง F ไปยัง $\bar{F}$ ซึ่งเป็นสนามปิดพีชคณิตของ F เป็นฟังก์ชันถอดแบบร่วมกลุ่ม

2) จงหาตัวก่อกำเนิดของกลุ่มวัฏจักรต่อไปนี้

ก) $(Z_5^*, .)$

ข) $(Z_{17}^*, .)$

ค) $(Z_{23}^*, .)$

3) จงหาจำนวนรากที่ 8 ปฐมฐานของ unity ใน GF(9)

4) จงหาจำนวนรากที่ 15 ปฐมฐานของ unity ใน GF(31)

5) จงหาจำนวนรากที่ 18 ปฐมฐานของ unity ใน GF(19)