# บทที่ 13
# สนามแยกส่วน
# (Splitting fields)

สิ่งสำคัญที่เรากำลังสนใจจะศึกษากันในหัวข้อนี้ คือ ฟังก์ชันถอดแบบร่วมกลุ่มของสนาม E มากกว่าฟังก์ชันถอดแบบของ E เราเห็นแล้วจากบทที่แล้วว่า เซตของฟังก์ชันถอดแบบร่วมกลุ่มของสนาม สามารถจะเป็นกลุ่มได้ เราสงสัยต่อไปว่าสำหรับบางสนามภาคยืดขยาย E ของสนาม F ทุก ๆ การส่งแบบถอดแบบ (isomorphic mapping) ของ E ไปใน $\bar{F}$ ซึ่งทิ้ง F คงที่ (leave F fixed) เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ E แน่นอนหรือไม่

สมมติ E เป็นสนามภาคยืดขยายพีชคณิตของสนาม F ถ้า $\alpha \in E$ และ $\beta \in \bar{F}$ เป็นสังยุคของ $\alpha$ เหนือ F แล้ว จะมีฟังก์ชันถอดแบบมูลฐาน

$$\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$$

โดยบทแทรกที่ 1 ของทฤษฎี 12.1.1, $\psi_{\alpha,\beta}$ สามารถจะขยายออกเป็นฟังก์ชันถอดแบบของ E ไปยัง $\bar{F}$ ในที่นี้ ถ้า $\beta \notin E$ ฟังก์ชันถอดแบบเช่นที่ว่านี้ของ E จะไม่สามารถเป็นฟังก์ชันถอดแบบร่วมกลุ่มของ E ดังนั้นถ้าสนามภาคยืดขยายพีชคณิต E ของสนาม F เป็นสนามชนิดที่ทุก ๆ ฟังก์ชันถอดแบบของมันที่ส่งไปยัง $\bar{F}$ ทิ้ง F คงที่ (leave F fixed) เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ E อย่างแน่นอน แล้วทุก ๆ $\alpha \in F$ สังยุคทั้งหมดของ $\alpha$ เหนือ F จะต้องอยู่ใน E ด้วย ข้อสังเกตนี้ดูเหมือนจะง่ายมาก เราชี้ให้เห็นว่า เราใช้การมีของฟังก์ชันถอดแบบร่วมกลุ่มมูลฐานและทฤษฎีการยืดขยายของฟังก์ชันถอดแบบ

แนวความคิดนี้นำเราไปสู่การสร้างนิยามต่อไปนี้

**นิยาม**

ให้ $F$ เป็นสนามที่ $\bar{F}$ เป็นสนามปิดพีชคณิต ให้ $\{f_i(x) | i \in I\}$ เป็นเซตของพหุนามใน $F[x]$, สนาม $E \leqslant \bar{F}$ จะเป็นสนามแยกส่วน (splitting field) ของ $\{f_i(x) | i \in I\}$ เหนือ $F$ ถ้า $E$ เป็นสนามย่อยที่เล็กที่สุดของ $\bar{F}$ ที่บรรจุ $F$ และศูนย์ทั้งหมด ใน $\bar{F}$ ของแต่ละ $f_i(x)$ สำหรับ $i \in I$, สนาม $K \leqslant \bar{F}$ เป็นสนามแยกส่วนเหนือ $F$ ถ้ามันเป็นสนามแยกส่วนของบางเซตของพหุนามใน $F[x]$

สำหรับพหุนาม (หนึ่งพหุนาม) $f(x) \in F[x]$ ที่เป็นสนามแยกส่วนของ $\{f(x)\}$ เหนือ $F$ เรานิยมเรียกบ่อย ๆ ว่า สนามแยกส่วนของ $f(x)$ เหนือ $F$ (splitting field of f(x) over F) และเป็นที่กระจ่างชัด (clear) ว่า สนามแยกส่วนของ $\{f_i(x) | i \in I\}$ เหนือ $F$ ใน $\bar{F}$ เป็นผลตัดของสนามย่อยทั้งหมดของ $\bar{F}$ ที่บรรจุ $F$ และศูนย์ทั้งหมดใน $\bar{F}$ ของแต่ละ $f_i(x)$ สำหรับ $i \in I$ ดังนั้นแน่ใจได้ว่าสนามแยกส่วนเช่นที่ว่านี้มีแน่นอน (does exist)

ขณะนี้เรากำลังจะแสดงว่าสนามแยกส่วนเหนือ $F$ คือ สนาม $E \leqslant \bar{F}$ มีคุณสมบัติว่าฟังก์ชันถอดแบบทั้งหมดของ $E$ ไปยัง $\bar{F}$ ที่ทิ้ง $F$ คงที่ เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ $E$

**ทฤษฎี 13.1**

สนาม $E$ ซึ่ง $F \leqslant E \leqslant \bar{F}$ เป็นสนามแยกส่วนเหนือ $F$ ก็ต่อเมื่อทุก ๆ ฟังก์ชันถอดแบบร่วมกลุ่มของ $\bar{F}$ ทิ้ง $F$ คงที่ ส่ง $E$ ไปบน $E$ เองอย่างทั่วถึง และเป็นเหตุให้ฟังก์ชันถอดแบบร่วมกลุ่มอันหนึ่งของ $E$ ทิ้ง $F$ คงที่

**พิสูจน์**

$\Rightarrow$ ให้ E เป็นสนามแยกส่วนเหนือ F ใน $\bar{F}$ ของ $\{f_i(x) | i \in I\}$

และให้ $\sigma$ เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ $\bar{F}$ ทิ้ง F คงที่

ให้ $\{\alpha_j | j \in J\}$ เป็นเซตของศูนย์ทั้งหมดใน $\bar{F}$ ของ $f_i(x)$ ทั้งหมดสำหรับ $i \in I$

ในขณะนี้ จากที่เคยทำมาแล้ว แสดงว่าสำหรับ $\alpha_i$ ที่เจาะจงคงที่ (a fixed $\alpha_j$), $F(\alpha_j)$ มีสมาชิกที่เขียนได้ในรูป

$$g(\alpha_j) = a_0 + a_1\alpha_j + \ldots + a_{n_j-1}\alpha_j^{n-1}$$

โดยที่ $n_j$ เป็นลำดับขั้นของ irr $(\alpha_j, F)$ และ $a_k \in F$

พิจารณาเซต S ของผลบวกจำกัดทั้งหมดของผลคูณจำกัดของสมาชิกของ $g(\alpha_j)$ สำหรับทุก ๆ $j \in J$

เซต S เป็นเซตย่อยของ E และเห็นได้ชัดว่า สอดคล้องกฎการปิดภายใต้การบวกและการ $\cdot$ และมี $0, 1 \in S$ และตัวผกผันสำหรับการบวกของสมาชิกแต่ละตัวของ S มีอยู่ใน S

เนื่องจาก แต่ละสมาชิกของ S จะต้องอยู่ในบาง $F(\alpha_{j_1}, \ldots, \alpha_{j_r}) \subseteq S$ เราจะเห็นว่า S จะมีตัวผกผันสำหรับการคูณ สำหรับสมาชิกแต่ละตัวที่ไม่ใช่ศูนย์ด้วย

ดังนั้น S เป็นสนามย่อยของ E ซึ่งบรรจุอยู่ $\alpha_j$ ทั้งหมดสำหรับ $j \in J$

โดนิยามของสนามแยกส่วน E ของ $\{f_i(x) | i \in I\}$ เราจะเห็นว่า เราจะต้องได้ $S = E$

สิ่งที่ทำมาทั้งหมดนี้ เพียงแต่แสดงว่า $\{\alpha_j | j \in J\}$ ก่อกำเนิด E เหนือ F ในแง่ที่ว่า ได้รับผลบวกจำกัดและผลคูณจำกัด

จากการทราบสิ่งเหล่านี้ทำให้เราเห็นต่อมาโดยทันทีว่า ค่าของ $\sigma$ บนสมาชิกใด ๆ ของ E ถูกกำหนดอย่างสมบูรณ์โดยค่า $\sigma(\alpha_j)$

แต่โดยบทแทรกที่ 1 ของทฤษฎี 11.1.1 $\sigma(\alpha_j)$ จะต้องเป็นศูนย์ของ irr $(\alpha_j, F)$

โดยทฤษฎี 8.3.1 irr $(\alpha_j, F)$ หาร $f_i(x)$ ลงตัว สำหรับ $f_i(\alpha_j) = 0$

ดังนั้น $\sigma(\alpha_i) \in E$ ด้วย

ดังนั้น $\sigma$ ส่ง E ไปใน E ชนิดถอดแบบ (isomorphically)

อย่างไรก็ตาม จะเป็นจริงสำหรับฟังก์ชันถอดแบบร่วมกลุ่ม $\sigma^{-1}$ ของ $\bar{F}$ ด้วยเช่นกัน

เนื่องจาก สำหรับ $\beta \in F, \beta = (\sigma^{-1}(\beta))\sigma$ เราจะเห็นว่า $\sigma$ ส่ง E ไปบน E (อย่างทั่วถึง) จึงได้ฟังก์ชันถอดแบบร่วมกลุ่มของ E

$\Leftarrow$ ถ้าทุก ๆ ฟังก์ชันถอดแบบร่วมกลุ่มของ $\bar{F}$ ทิ้ง F คงที่เป็นเหตุให้ได้ฟังก์ชันถอดแบบร่วมกลุ่มของ E

ให้ g(x) เป็นพหุนามลดทอนไม่ได้ใน F[x] มี $\alpha$ เป็นศูนย์ใน E

ถ้า $\beta$ เป็นศูนย์ใด ๆ ของ g(x) ใน $\bar{F}$ แล้ว โดยทฤษฎีจะมีฟังก์ชันถอดแบบมูลฐาน $\psi_{\alpha,\beta}$

ของ $F(\alpha)$ ไปบน $F(\beta)$ (อย่างทั่วถึง) ทิ้ง F คงที่

โดยทฤษฎี 12.1.1, $\psi_{\alpha,\beta}$ สามารถจะขยายออกไปเป็นฟังก์ชันถอดแบบ $\tau$ ของ $\bar{F}$ ไปใน $\bar{F}$ แล้ว

$\tau^{-1} : \tau(\bar{F}) \to \bar{F}$ สามารถจะขยายออกไปเป็นฟังก์ชันถอดแบบส่ง $\bar{F}$ ไปใน $\bar{F}$

เนื่องจาก ภาพ (image) ของ $\tau^{-1}$ อยู่ใน $\bar{F}$ ทั้งหมดแล้ว

เราจะเห็นว่า $\tau$ จะต้องเป็นฟังก์ชันทั่วถึงบน $\bar{F}$

ดังนั้น $\tau$ เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ $\bar{F}$ ทิ้ง F คงที่

แล้วโดยสมมติฐาน $\tau$ เป็นเหตุให้ได้ฟังก์ชันถอดแบบร่วมกลุ่มอันหนึ่งของ E

ดังนั้น $\tau(\alpha) = \beta$ อยู่ใน E

เราได้แสดงแล้วว่า ศูนย์ทั้งหมดของ g(x) ใน $\bar{F}$ อยู่ใน E

ด้วยเหตุนี้ ถ้า $\{g_k(x)\}$ เป็นเซตของพหุนามลดทอนไม่ได้ทั้งหมดใน F[x] ที่มีศูนย์ใน E แล้ว E เป็นสนามแยกส่วนของ $\{q_k(x)\}$ #

**นิยาม**

| ให้ $E$ เป็นสนามภาคยืดขยายของสนาม $F$, พหุนาม $f(x) \in F[x]$ แยกส่วนใน $E$ (splits in $E$) ถ้า $f(x)$ แยกตัวประกอบออกเป็นผลคูณของตัวประกอบที่มีลำดับขั้น 1 (linear factors) ใน $E[x]$ |
|---|

**บทแทรก**

| ถ้า $E \leqslant \bar{F}$ เป็นสนามแยกส่วนเหนือ $F$ แล้วทุก ๆ พหุนามลดทอนไม่ได้ใน $F[x]$ ที่มีศูนย์ใน $E$ แยกส่วนใน $E$ |
|---|

**พิสูจน์**

ถ้า $E$ เป็นสนามแยกส่วนเหนือ $F$ ใน $\bar{F}$ แล้ว

ทุก ๆ ฟังก์ชันถอดแบบร่วมกลุ่มของ $\bar{F}$ เป็นเหตุให้ได้ฟังก์ชันถอดแบบร่วมกลุ่มของ $E$

ส่วนที่ 2 ของบทพิสูจน์ทฤษฎี 13.1 แสดงแล้วว่า $E$ เป็นสนามแยกส่วนเหนือ $F$ ของเซต $\{g_k(x)\}$ ของพหุนามลดทอนไม่ได้ทั้งหมดใน $F[x]$ ที่มีศูนย์ใน $E$ ด้วยเหมือนกัน

ดังนั้น พหุนามลดทอนไม่ได้ $f(x) \in F[x]$ ที่มีศูนย์ใน $E$ ซึ่งมีศูนย์ทั้งหมดของมันใน $\bar{F}$ ใน $E$

ด้วยเหตุนี้ การแยกตัวประกอบของมันถึงแยกออกเป็นผลคูณของ linear factor ใน $\bar{F}[x]$ โดยทฤษฎี 10.2.2 แทนที่ด้วย $E[x]$ แล้ว

$f(x)$ แยกส่วนใน $E$ #

**บทแทรก 2** ถ้า $E \leqslant \bar{F}$ เป็นสนามแยกส่วนเหนือ F แล้วทุก ๆ ฟังก์ชันถอดแบบของ E ไปใน $\bar{F}$ ทิ้ง F คงที่เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ E แน่นอน ในกรณีเฉพาะ ถ้า E เป็นสนามแยกส่วนที่มีลำดับขั้นจำกัดเหนือ F แล้ว $\{E : F\} = |G(E/F)|$

**พิสูจน์**

ทุก ๆ ฟังก์ชันถอดแบบ $\sigma$ ส่ง E ไปใน $\bar{F}$ ทิ้ง F คงที่ สามารถจะขยายออกไปเป็นฟังก์ชันถอดแบบร่วมกลุ่ม $\tau$ ของ $\bar{F}$ โดยทฤษฎี 12.1.1 ร่วมกับส่วนที่ 2 ของบทพิสูจน์ทฤษฎี 13.1

ถ้า E เป็นสนามแยกส่วนเหนือ F แล้ว โดยทฤษฎี 12.1.1 $\tau$ จำกัดยัง (restrict to) E, นั่นคือ $\sigma$, เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ E

สำหรับสนามแยกส่วน E เหนือ F, ทุก ๆ ฟังก์ชันถอดแบบของ E ไปยัง $\bar{F}$ ซึ่งทิ้ง F คงที่ เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ E

สมการ $\{E : F\} = |G(E/F)|$ ตามมาโดยทันทีสำหรับสนามแยกส่วน E ที่มีลำดับขั้นจำกัดเหนือ F, เนื่องจาก $\{E : F\}$ ถูกกำหนดให้เป็นจำนวนของฟังก์ชันถอดแบบต่าง ๆ กันของ E ไปยัง $\bar{F}$ ทิ้ง F คงที่ #

**ตัวอย่าง 13.1** แจ้งชัดว่า $Q(\sqrt{2}, \sqrt{3})$ เป็นสนามแยกส่วนของ $\{x^2 - 2, x^2 - 3\}$ เหนือ Q ตัวอย่าง 11.2.2 แสดงแล้วว่า ฟังก์ชัน $i, \sigma_1, \sigma_2$ และ $\sigma_3$ ทั้งหมดเป็นฟังก์ชันถอดแบบร่วมกลุ่มของ $Q(\sqrt{2}, \sqrt{3})$ ทิ้ง Q คงที่

แน่นอน, เนื่องจากทุก ๆ ฟังก์ชันถอดแบบร่วมกลุ่มของสนามจะต้องทิ้งสนามย่อยจำนวนเฉพาะคงที่ (leave the prime subfield fixed)

เราจะเห็นว่า จะมีฟังก์ชันถอดแบบร่วมกลุ่มของ $Q(\sqrt{2}, \sqrt{3})$ เท่านั้น

แล้ว $[Q(\sqrt{2}, \sqrt{3}) : Q] = |G(Q(\sqrt{2}, \sqrt{3})/Q)| = 4$ #

เราอยากจะกำหนดเงื่อนไข ซึ่ง

$$|G(E/F)| = \{E : F\} = [E : F]$$

สำหรับสนามยืดขยายจำกัด E ของ F นี่คือ สิ่งที่เราสนใจต่อไป เราจะแสดงในบทต่อไปว่า สมการข้างบนนี้เป็นจริงได้เมื่อ E เป็นสนามแยกส่วนเหนือสนาม F ที่มีลักษณะเฉพาะ (characteristic) 0 หรือเมื่อ F เป็นสนามจำกัด สมการนี้ไม่จำเป็นจะต้องจริงเมื่อ F เป็นสนามอนันต์ (infinite field) ที่มีลักษณะเฉพาะ $p \neq 0$

**ตัวอย่าง 13.2** ให้ $\sqrt[3]{2}$ เป็นรากที่สาม ซึ่งเป็นจำนวนจริงของ 2

$x^3 - 2$ ไม่แยกส่วนใน $Q(\sqrt[3]{2})$ สำหรับ $Q(\sqrt[3]{2}) < R$

และศูนย์ (ซึ่งมีเพียงตัวเดียว) ของ $x^3 - 2$ เป็นจำนวนจริง

ดังนั้น $x^3 - 2$ แยกตัวประกอบใน $(Q(\sqrt[3]{2}))[x]$ ออกเป็น $x - \sqrt[3]{2}$ ซึ่งเป็นตัวประกอบลำดับขั้น 1 และลดทอนไม่ได้

สนามแยกส่วน E ของ $x^3 - 2$ เหนือ Q จึงมีลำดับขั้น 2 เหนือ $Q(\sqrt[3]{2})$ แล้ว

$$[E : Q] = [E : Q(\sqrt[3]{2})][Q(\sqrt[3]{2}) : Q] = (2)(3) = 6$$

เราได้แสดงว่าสนามแยกส่วน Q ของ $x^3 - 2$ มีลำดับขั้น 6 เหนือ Q

นักศึกษาสามารถจะพิสูจน์ความจริงโดยยกกำลัง 2 ได้ว่า

$\sqrt[3]{2}\,\frac{-1 + i\sqrt{3}}{2}$ และ $\sqrt[3]{2}\,\frac{-1 - i\sqrt{3}}{2}$ เป็นศูนย์ (ตัวอื่น ๆ) ของ $x^3 - 2$ ใน C

ดังนั้น สนามแยกส่วน E ของ $x^3 - 2$ เหนือ Q คือ $Q(\sqrt[3]{2}, i\sqrt{3})$ #

## แบบฝึกหัดที่ 13

1) จงพิจารณาข้อความแต่ละข้อต่อไปนี้เป็นจริงหรือเท็จ

..............ก) R เป็นสนามแยกส่วนเหนือ Q

..............ข) R เป็นสนามแยกส่วนเหนือ R

..............ค) C เป็นสนามแยกส่วนเหนือ R

..............ง) Q(i) เป็นสนามแยกส่วนเหนือ Q

..............จ) $Q(\pi)$ เป็นสนามแยกส่วนเหนือ $Q(\pi^2)$

..............ฉ) สำหรับทุก ๆ สนามแยกส่วน E เหนือ F โดยที่ $E \leqslant \bar{F}$, ทุก ๆ ฟังก์ชันถอดแบบของ E เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ E

..............ช) สำหรับทุก ๆ สนามแยกส่วน E เหนือ F โดยที่ $E \leqslant \bar{F}$, ทุกฟังก์ชันถอดแบบจาก E ไปยัง $\bar{F}$ เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ E

..............ซ) สำหรับทุกสนามแยกส่วน E เหนือ F โดยที่ $E \leqslant \bar{F}$, ทุกฟังก์ชันถอดแบบจาก E ไปยัง $\bar{F}$ และทิ้ง F คงที่เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ E

..............ฌ) ทุก algebraic closure $\bar{F}$ ของสนาม F เป็นสนามแยกส่วนเหนือ F

2) สำหรับแต่ละพหุนามที่กำหนดให้ Q[x] จงหาลำดับขั้นเหนือ Q ของสนามแยกส่วนเหนือ Q ของพหุนาม

ก) $x^2 + 3$

ข) $x^4 - 1$

ค) $(x^2 - 2)(x^2 - 3)$

ง) $x^3 - 3$

จ) $x^3 - 1$

ฉ) $(x^2 - 2)(x^3 - 2)$

3) ให้ $\alpha$ เป็นศูนย์ของ $x^3 + x^2 + 1$ เหนือ $Z_2$ จงแสดงว่า $x^3 + x^2 + 1$ แยกส่วนใน $Z_2(\alpha)$