บทที่ 11
ฟังก์ชันถอดแบบร่วมกลุ่มของสนาม
Automorphisms of fields

11.1 ฟังก์ชันถอดแบบมูลฐานของทฤษฎีสนามพีชคณิต

(The basic isomorphism of algebraic field theory)

ให้ F เป็นสนาม และให้ $\bar{F}$ เป็นสนามปิดเชิงพีชคณิตของ F นั่นคือ $\bar{F}$ เป็นสนามภาคยืดขยายเชิงพีชคณิตของ F ซึ่งปิดและเป็นพีชคณิต สนามเช่นสนาม $\bar{F}$ ที่มี (โดยทฤษฎี 10.2.3) การเลือก $\bar{F}$ ของเราไม่สำคัญสุดยอด เนื่องจาก สำหรับ algebraic closure ของ F ใด ๆ 2 สนามจะถอดแบบกัน ในหัวข้อนี้เราจะสมมติว่าสนามภาคยืดขยายพีชคณิตทั้งหมด และสมาชิกทั้งหมดเป็นพีชคณิตเหนือสนาม F ภายใต้การพิจารณา ซึ่งถูกบรรจุใน fixed algebraic closure $\bar{F}$ ของ E

คงจำได้ว่า เราได้ศึกษา ศูนย์ของพหุนามในบทที่ 7 และในบทที่ 10 ได้ศึกษาศูนย์ของพหุนามใน $F[x]$ ได้ศึกษาโครงสร้างของสนามภาคยืดขยายพีชคณิตของ F และสมาชิกซึ่งเป็นพีชคณิตเหนือ F เราสามารถจะแสดงได้ว่า ถ้า E เป็นภาคยืดขยายพีชคณิตของ F ที่ $\alpha, \beta \in E$ แล้ว α, β มีคุณสมบัติพีชคณิตเดียวกันก็ต่อเมื่อ $irr(\alpha, F) = irr(\beta, F)$ เราจะแสดงความจริงนี้ในเทอมของฟังก์ชัน เช่นที่เราเคยทำในทฤษฎีสนามทั้งหมด เราจะทำ (เพื่อบรรลุจุดประสงค์) โดยแสดงการมีของฟังก์ชันถอดแบบ $\psi_{\alpha,\beta}$ ของ $F(\alpha)$ ไปบน $F(\beta)$ ซึ่งส่งแต่ละสมาชิกของ F ไปบน F เอง และส่ง α ไปบน β ในกรณี $irr(\alpha, F) = irr(\beta, F)$ ทฤษฎีต่อไปจะแสดงฟังก์ชันถอดแบบ $\psi_{\alpha,\beta}$ นี้ ฟังก์ชันถอดแบบเหล่านี้จะกลายมาเป็นเครื่องมือพื้นฐานสำหรับศึกษาภาคยืดขยายพีชคณิต

นิยาม ให้ E เป็นภาคยืดขยายพีชคณิตของสนาม F สมาชิก 2 ตัว $\alpha, \beta \in E$ เป็นสังยุคเหนือ F (conjugate over F) เมื่อ irr (α, F) = irr (β, F) นั่นคือ เมื่อ α และ β เป็นศูนย์ของพหุนามลดทอนไม่ได้เดียวกันเหนือ F

ตัวอย่าง 11.1.1 แนวความคิดเรื่องสมาชิกสังยุคสามารถจะอธิบายได้ชัดเจน ในแนวเดียวกับสังยุคของจำนวนเชิงซ้อน ถ้าเราเข้าใจแล้วว่าสังยุคของจำนวนเชิงซ้อนเราหมายถึง จำนวนซึ่งเป็นสังยุคเหนือ R ถ้า $a, b \in R$ และ $b \neq 0$ สังยุคของจำนวนเชิงซ้อน $a + b_i$ และ $a - b_i$ คือ ศูนย์ของ $x^2 - 2ax + a^2 + b^2$ ซึ่งลดทอนไม่ได้ ใน $R[x]$

ทฤษฎี 11.1.1 (The Basic isomorphism of algebraic field theory)

ให้ F เป็นสนาม และให้ α และ β เป็นสมาชิกพีชคณิตเหนือ F
โดยที่ $\deg(\alpha, F) = n$ ฟังก์ชัน $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$
กำหนดโดย $\psi_{\alpha,\beta}\ (c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\beta + \ldots + c_{n-1}\beta^{n-1}$
สำหรับ $c_i \in F$ เป็นฟังก์ชันถอดแบบของ $F(\alpha)$ ไปบน $F(\beta)$ ก็ต่อเมื่อ α และ β เป็นสังยุคเหนือ F

พิสูจน์

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

ให้ irr $(\alpha, F) = a_0 + a_1x + \ldots + a_nx^n$

$\therefore\ a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$

$$\psi_{\alpha,\beta}(a_0 + a_1\alpha + \ldots + a_n\alpha^n) = a_0 + a_1\beta + \ldots + a_n\beta^n$$
$$= 0$$

แสดงว่า irr (α, F) หาร irr (β, F) ลงตัว

อาร์กิวเมนต์เหมือนกันใช้ฟังก์ชันถอดแบบ $(\psi_{\alpha,\beta})^{-1} = \psi_{\alpha,\beta}$ แสดงว่า irr (α, F) หาร irr (β, F) ลงตัว

เนื่องจาก พหุนามทั้งสองเป็นโมนิก

irr (α, F) = irr (β, F)

ดังนั้น α และ β เป็นสังยุคเหนือ F

$\Leftarrow$ สมมติ irr (α, F) = irr (β, F) = $p(x)$

$\therefore$ ฟังก์ชันถ่ายแบบมูลฐาน $\phi_\alpha : F[x] \to F(\alpha)$ และ $\phi_\beta : F[x] \to F[\beta]$ มี ker $<p(x)>$ เดียวกัน

โดยทฤษฎี 5.1.7 จะต้องมี

ฟังก์ชันถอดแบบ $\psi_a : F[x]/<p(x)> \to \phi_\alpha[F[x]] = F(\alpha)$

และทำนองเดียวกัน จะต้องมี

ฟังก์ชันถอดแบบ $\psi_b : F[x]/<p(x)> \to \phi_\beta[F[x]] = F(\beta)$

ให้ $\psi = \psi_{\alpha,\beta} = \psi_\alpha^{-1}\psi_\beta$

การส่งสมาชิกของ ψ แสดงในรูปข้างล่างนี้

$\psi_{\alpha,\beta}$ เป็นฟังก์ชันถอดแบบและส่ง $F(\alpha)$ ไปบน $F(\beta)$

และสำหรับ $(c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}) \in F(\alpha)$ เราได้

$$\psi_{\alpha,\beta}(c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}) = (c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1})(\psi_\alpha^{-1}\psi_\beta)$$
$$= [(c_0 + c_1x + \ldots + c_{n-1}x^{n-1}) + <p(x)>]\psi_\beta$$
$$= c_0 + c_1\beta + \ldots + c_{n-1}\beta^{n-1}$$

$\therefore\ \psi_{\alpha,\beta}$ เป็นฟังก์ชันถอดแบบ #

$$\begin{tikzcd} & x \arrow[r, dash, dashed] & F[x] \arrow[dll, "\phi_\alpha"'] \arrow[d] \arrow[drr, "\phi_\beta"] & & \\ F(\alpha) \arrow[rr, dash, "\psi_\alpha"'] & & F[x]/<p(x)> \arrow[rr, "\psi_\beta"'] & & F(\beta) \\ a \arrow[u, dash, dashed] & & x + <p(x)> \arrow[u, dash, dashed] & & \beta \arrow[u, dash, dashed] \end{tikzcd}$$

บทแทรก 1 ถ้า α เป็นสมาชิกพีชคณิตเหนือสนาม F ทุก ๆ ฟังก์ชันถอดแบบ ψ จะส่ง $F(\alpha)$ ไปใน $\bar{F} \ni \psi(a) = a$ สำหรับ $a \in F$ ส่ง α ไปบนสังยุค β ของ α เหนือ F ในทางกลับกัน สำหรับแต่ละสังยุค β ของ α เหนือ F จะมีฟังก์ชันถอดแบบที่แน่นอน $\psi_{\alpha,\beta}$ ของ $F(\alpha)$ ไปใน $\bar{F}$ ส่ง α ไปบน β และส่งแต่ละ $a \in F$ ไปในตัวมันเอง

พิสูจน์

ให้ ψ เป็นฟังก์ชันถอดแบบจาก $F(\alpha)$ ไปใน $\bar{F} \ni \psi(a) = a;\ a \in F$

ให้ $\operatorname{irr}(\alpha, F) = a_0 + a_1x + \ldots + a_nx^n$ แล้ว

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$$

$$\psi(a_0 + a_1\alpha + + a_n\alpha^n) = 0$$

แต่ $\psi(a_0 + a_1\alpha + + a_n\alpha^n) = a_0 + a_1(\psi(\alpha)) + \ .\ .\ + a_n(\psi(\alpha))^n$

$a_0 + a_1(\psi(\alpha)) + \ldots + a_n(\psi(\alpha))^n = 0$

และ $\beta = \psi(\alpha)$ เป็นสังยุคของ α

ในทางกลับกัน

สำหรับแต่ละสังยุค β ของ α เหนือ F

ฟังก์ชันถอดแบบ $\psi_{\alpha,\beta}$ ตามทฤษฎี 11.1.1 เป็นฟังก์ชันถอดแบบที่มีคุณสมบัติที่ต้องการคือ

$\psi_{\alpha,\beta}$ เป็นเพียงฟังก์ชันถอดแบบจากการที่ $F(\alpha)$ ถูกกำหนดโดยค่าของมันบนสมาชิกของ F และโดยค่าของมันบน α #

บทแทรก 2 ให้ $f(x) \in R[x]$ ถ้า $f(a + b_i) = 0$ สำหรับ $(a + b_i) \in C$ โดยที่ $a, b \in R$ แล้ว $f(a - b_i) = 0$ ด้วย

พิสูจน์

เราพบแล้วว่า $C = R(i)$

และแน่นอน $C = R(-i)$ ด้วย

$\therefore \operatorname{irr}(i, R) = \operatorname{irr}(-i, R) = x^2 + 1$

ดังนั้น i และ $-i$ เป็นสังยุคเหนือ R

โดยทฤษฎี 11.1.1 ฟังก์ชัน

$\psi_{i,-i} : C \to C$ กำหนดโดย $\psi_{i,-i}(a + b_i) = a - b_i$ เป็นฟังก์ชันถอดแบบ

ดังนั้น ถ้าสำหรับ $a_i \in R$

$f(a + b_i) = a_0 + a_1(a + b_i) + \ldots + a_n(a + b_i)^n = 0$ แล้ว

$$0 = \psi_{i,-i}(f(a + b_i)) = a_0 + a_1(a - b_i) + \ldots + a_n(a - b_i)^n$$
$$= f(a - b_i)$$

นั่นคือ $f(a - b_i) = 0$ ด้วย #

ตัวอย่าง 11.1.2 พิจารณา $Q(\sqrt{2})$ เหนือ Q

ศูนย์ของ $\mathrm{irr}(\sqrt{2}, Q) = x^2 - 2$ คือ $\sqrt{2}$ และ $-\sqrt{2}$

ดังนั้น $\sqrt{2}$ และ $-\sqrt{2}$ เป็นสังยุคเหนือ Q

$\therefore$ ตามทฤษฎี 11.1.1 ฟังก์ชัน $\psi_{\sqrt{2}, -\sqrt{2}} : Q(\sqrt{2}) \to Q\sqrt{2}$ กำหนดโดย $\psi_{\sqrt{2}, -\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$ เป็นฟังก์ชันถ่ายแบบของ $Q\sqrt{2}$ ไปบนตัวมันเอง #

11.2 ฟังก์ชันถอดแบบร่วมกลุ่ม และสนามคงที่

(Automorphism and fixed fields)

นิยาม ให้ F เป็นสนาม, $\psi : F \to F$ เป็นฟังก์ชันถอดแบบ เรียก ψ ว่า ฟังก์ชันถอดแบบร่วมกลุ่มของสนาม (automorphism of the field F)

นิยาม ถ้า σ เป็นฟังก์ชันถอดแบบของสนาม E ไปในบางสนาม แล้วสมาชิก a ของ E จะเรียกว่า leave fixed โดย σ ถ้า $\sigma(a) = a$ เซต S ของฟังก์ชันถอดแบบของ E leave fixed subfield F ของ E ถ้าแต่ละ $a \in F$ เป็น leave fixed โดยทุก ๆ $\sigma \in S$ ถ้า $\{\sigma\}$ leave fixed F แล้ว σ leave fixed F

เป็นความตั้งใจของเราที่จะศึกษาโครงสร้างของภาคยืดขยายพีชคณิต E ของสนาม F โดยศึกษาฟังก์ชันถอดแบบร่วมกลุ่มของ E ซึ่ง leave fixed แต่ละสมาชิกของ F เราจะแสดงว่าฟังก์ชันถอดแบบร่วมกลุ่มเหล่านี้เป็นกลุ่มได้ เราจะประยุกต์โดยใช้โครงสร้างของกลุ่มเพื่อให้ได้ข้อมูลเกี่ยวกับโครงสร้างของสนามภาคยืดขยาย ดังนั้นเราจะต้องนำหลายสิ่งมาร่วมกันเพื่อเป็นฐานนำไปสู่สิ่งที่ต้องการศึกษา ทฤษฎีสามทฤษฎีต่อไปนี้จะให้แนวความคิดรูปแบบพื้นฐานสำหรับสิ่งที่จะตามมา ทฤษฎีเหล่านี้สำคัญสำหรับเรามาก เพราะจะเป็นกุญแจไปสู่การหาคำตอบของจุดมุ่งหมายสุดท้าย (final goal) ของหนังสือเล่มนี้

ทฤษฎี 11.0.1 ให้ $\{\sigma_i | i \in I\}$ เป็นเซตของฟังก์ชันถอดแบบร่วมกลุ่มของสนาม E แล้ว เซต $E_{\{\sigma_i\}}$ ของ a ทั้งหมดที่อยู่ใน E leave fixed โดยทุก ๆ σ_i สำหรับ $i \in I$ จะเป็นสนามย่อยของสนาม E

พิสูจน์

ถ้า $\sigma_i(a) = a$ และ $\sigma_i(b) = b$ สำหรับทุก ๆ $i \in I$ แล้ว

$$\begin{aligned} \sigma_i(a \pm b) &= \sigma_i(a) \pm \sigma_i(b) \\ &= a \pm b \end{aligned}$$

และ
$$\begin{aligned} \sigma_i(ab) &= \sigma(a)\ \sigma_i(b) \\ &= ab \end{aligned}$$

สำหรับทุก ๆ $i \in I$ และเช่นเดียวกัน

ถ้า $b \neq 0$ แล้ว

$$\begin{aligned} \sigma_i(a/b) &= \sigma_i(a)/\sigma_i(b) \\ &= a/b \qquad \forall i \in I \end{aligned}$$

เนื่องจาก σ_i เป็นฟังก์ชันถอดแบบร่วมกลุ่ม

$$\sigma_i(0) = 0 \text{ และ } \sigma_i(1) = 1 \qquad \forall i \in I$$

$\therefore\ 0, 1 \in E_{\{\sigma_i\}}$

ดังนั้น $E_{\{\sigma_i\}}$ เป็นสนามย่อยของสนาม E #

นิยาม

สนาม $E_{\{\sigma_i\}}$ ตามทฤษฎี 11.2.1 เป็นสนามคงที่ (fixed field) ของ $\{\sigma_i \mid i \in I\}$ สำหรับฟังก์ชันถอดแบบร่วมกลุ่มอันเดียว σ เราจะเรียก $E_{\{\sigma_i\}}$ ว่าเป็นสนามคงที่ของ σ

ตัวอย่าง 11.2.1 พิจารณาฟังก์ชันถอดแบบร่วมกลุ่ม $\psi_{\sqrt{2}, -\sqrt{2}}$ ของ $Q(\sqrt{2})$

ตามตัวอย่าง 11.1.2 สำหรับ a, b $\in$ Q เรามี

$$\psi_{\sqrt{2}, -\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$$

และ $a - b\sqrt{2} = a + b\sqrt{2}$ ก็ต่อเมื่อ $b = 0$

ดังนั้น สนามคงที่ของ $\psi_{\sqrt{2}, -\sqrt{2}}$ คือ Q #

ขอให้สังเกตว่า ฟังก์ชันถอดแบบร่วมกลุ่มของสนาม E เป็นฟังก์ชัน (เฉพาะ) หนึ่งต่อหนึ่งแบบทั่วถึงส่งสมาชิกของ E ไปบนสมาชิกของ E นั่นคือ เป็นเพอร์มิวเตชันของ E ถ้า σ และ τ เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ E แล้ว เพอร์มิวเตชัน $\sigma\tau$ ก็เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ E ด้วย เนื่องจากโดยทั่ว ๆ ไป ผลคูณของฟังก์ชันถ่ายแบบยังคงเป็นฟังก์ชันถ่ายแบบ

ทฤษฎี 11.2.2

เซตของฟังก์ชันถอดแบบร่วมกลุ่มทั้งหมดของสนาม E เป็นกลุ่มภายใต้การดำเนินการคูณฟังก์ชัน

พิสูจน์

การดำเนินการคูณฟังก์ชันถอดแบบร่วมกลุ่มของ E กำหนดโดยการทำฟังก์ชันประกอบ

ดังนั้น การคูณฟังก์ชันนี้จึงสอดคล้องกฎการเปลี่ยนกลุ่ม (เพราะมันเป็นการคูณ permutation)

และแน่นอน เอกลักษณ์ของ permutation คือ $i : E \to E$ ซึ่งกำหนดโดย $i(\alpha) = \alpha$ สำหรับทุก ๆ $\alpha \in E$ คือ เอกลักษณ์ของฟังก์ชันถอดแบบร่วมกลุ่มของ E

ถ้า σ เป็นฟังก์ชันถอดแบบร่วมกลุ่มแล้ว permutation σ^{-1} ก็เป็นฟังก์ชันถอดแบบร่วมกลุ่มด้วย

ดังนั้น เซตของฟังก์ชันถอดแบบร่วมกลุ่มทั้งหมดของสนาม E เป็นกลุ่มย่อยของกลุ่ม S_E ซึ่งเป็นกลุ่มของ permutation ทั้งหมดของ E #

ทฤษฎี 11.2.3 ให้ E เป็นสนาม F เป็นสนามย่อยของ E แล้วเซต G(E/F) ของฟังก์ชันถอดแบบร่วมกลุ่มทั้งหมดของ E leave F fixed เป็นกลุ่มย่อยของกลุ่มของฟังก์ชันถอดแบบร่วมกลุ่มของ E ยิ่งกว่านั้น $F \leqslant E_{G(E/F)}$

พิสูจน์

สำหรับ $\sigma, \tau \in G(E/F)$ และ $a \in F$ เราได้

$$(\tau\sigma)(a) = \tau(\sigma(a)) = \tau(a) = a$$

ดังนั้น $\tau\sigma \in G(E/F)$

และเป็นที่แน่ชัดว่า เอกลักษณ์ (ซึ่งเป็นฟังก์ชันถอดแบบร่วมกลุ่ม) i อยู่ใน G(E/F) ด้วย

ถ้า $\sigma(a) = a$ สำหรับ $a \in F$ แล้ว $\sigma^{-1}(a) = a$

ดังนั้น ถ้า $\sigma \in G(E/F)$ แล้ว $\sigma^{-1} \in G(E/F)$

$\therefore$ G(E/F) เป็นกลุ่มย่อยของกลุ่มของฟังก์ชันถอดแบบร่วมกลุ่มทั้งหมดของ E

เนื่องจากสมาชิกทุก ๆ ตัวของ F เป็น leave fixed โดยทุกสมาชิกของ G(E/F)

ดังนั้น จึงได้ทันทีว่า สนาม $E_{G(E/F)}$ ของสมาชิกทั้งหมดของ E ต้อง leave fixed โดย G(E/F) ซึ่งบรรจุ F อยู่ #

นิยาม

กลุ่ม G(E/F) ของตามทฤษฎี 11.2.3 เป็นกลุ่มของฟังก์ชันถอดแบบร่วมกลุ่มของ E ซึ่งทิ้ง F คงที่ (leave F fixed), (group of automorphisms of E leaving fixed) หรือเรียกสั้น ๆ ว่า กลุ่มของ E เหนือ F (group of E over F)

(สัญลักษณ์ E/F ไม่ได้หมายความว่าผลหารของปริภูมิ แต่เราหมายถึงว่า E เป็นสนามภาคขยายของสนาม F)

ตัวอย่าง 11.2.2 พิจารณาสนาม $Q(\sqrt{2}, \sqrt{3})$

ถ้าเราพิจารณา $Q(\sqrt{2}, \sqrt{3})$ เป็น $(Q(\sqrt{3}))(\sqrt{2})$

ฟังก์ชันถอดแบบมูลฐาน $\psi_{\sqrt{2}, -\sqrt{2}}$ กำหนดโดย

$\psi_{\sqrt{2}, -\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$ สำหรับ $a,b \in Q\sqrt{3})$ เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ $Q(\sqrt{2}, \sqrt{3})$ โดยมี $Q(\sqrt{3})$ เป็นสนามคงที่

ทำนองเดียวกัน เรามีฟังก์ชันถอดแบบร่วมกลุ่ม $\psi_{\sqrt{3}, -\sqrt{3}}$ ของ $Q(\sqrt{2}, \sqrt{3})$ โดยมี $Q(\sqrt{2})$ เป็นสนามคงที่

เนื่องจาก ผลคูณของฟังก์ชันถอดแบบร่วมกลุ่มยังคงเป็นฟังก์ชันถอดแบบร่วมกลุ่ม

เราจึงสามารถจะพิจารณา $\psi_{\sqrt{2},-\sqrt{2}}\psi_{\sqrt{3},-\sqrt{3}}$ **ซึ่ง** move **ทั้ง** $\sqrt{2}$ **และ** $\sqrt{3}$ **นั่นคือไม่** leave fixed **จำนวนใด ๆ**

ให้ i = ฟังก์ชันถอดแบบร่วมกลุ่มเอกลักษณ์

$\sigma_1 = \psi_{\sqrt{2},-\sqrt{2}}$

$\sigma_2 = \psi_{\sqrt{3},-\sqrt{3}}$

$\sigma_3 = \psi_{\sqrt{2},-\sqrt{2}}\ \psi_{\sqrt{3},-\sqrt{3}}$

กลุ่มของฟังก์ชันถอดแบบร่วมกลุ่มทั้งหมดของ $Q(\sqrt{2}, \sqrt{3})$ มีสนามคงที่

สนามคงที่นี้จะต้องบรรจุ Q

เนื่องจากทุก ๆ ฟังก์ชันถอดแบบร่วมกลุ่มของสนาม leave 1 และด้วยเหตุนี้ สนามย่อยจำนวนเฉพาะคงที่

ฐานสำหรับ $Q(\sqrt{2}, \sqrt{3})$ เหนือ Q คือ $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$

เนื่องจาก $\sigma_1(\sqrt{2}) = -\sqrt{2}$

$\sigma_1(\sqrt{6}) = -\sqrt{6}$

และ $\sigma_2(\sqrt{3}) = -\sqrt{3}$

เราพบว่า Q เป็นสนามคงที่ของ $\{i, \sigma_1, \sigma_2, \sigma_3\}$

และจะเห็นได้ง่าย ๆ ว่า $G = \{i, \sigma_1, \sigma_2, \sigma_3\}$ เป็นกลุ่มภายใต้การคูณฟังก์ชันถอดแบบร่วมกลุ่ม

ตารางการดำเนินการบนกลุ่มของ G เป็นดังนี้

	i	σ_1	σ_2	σ_3
i	i	σ_1	σ_2	σ_3
σ_1	σ_1	i	σ_3	σ_2
σ_2	σ_2	σ_3	i	σ_1
σ_3	σ_3	σ_2	σ_1	i

ตัวอย่าง

$$\begin{aligned}\sigma_1\sigma_3 &= \psi_{\sqrt{2}, -\sqrt{2}}(\psi_{\sqrt{2}, -\sqrt{2}}\psi_{\sqrt{3}, -\sqrt{3}}) \\ &= \psi_{\sqrt{3}, -\sqrt{3}} \\ &= \sigma_2\end{aligned}$$

กลุ่ม G นี้ ถอดแบบกันกับ Klein 4-group

เราสามารถจะแสดงได้ว่า G เป็นกลุ่มเต็ม $G(Q(\sqrt{2}, \sqrt{3})/Q)$

สำหรับทุก ๆ ฟังก์ชันถอดแบบร่วมกลุ่ม τ ของ $Q(\sqrt{2}, \sqrt{3})$ ส่ง $\sqrt{2}$ ไปบน $+\sqrt{2}$ หรือมิฉะนั้นก็ $-\sqrt{2}$ โดยบทแทรกที่ 1 ของทฤษฎี 11.1.1

ทำนองเดียวกัน τ ส่ง $\sqrt{3}$ ไปบน $+\sqrt{3}$ หรือมิฉะนั้นก็ $-\sqrt{3}$

แต่เนื่องจาก $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$ เป็นฐานสำหรับ $Q(\sqrt{2}, \sqrt{3})$ เหนือ Q

ฟังก์ชันถอดแบบร่วมกลุ่มของ $Q(\sqrt{2}, \sqrt{3})$ leave fixed Q ถูกกำหนดโดยค่าของมันเองบน $\sqrt{2}$ และ $\sqrt{3}$

แน่ชัดว่า i, σ_1, σ_2 และ σ_3 ให้การจัดหมู่ (combination) ทั้งหมดที่อาจเป็นไปได้ของค่าบน $\sqrt{2}$ และ $\sqrt{3}$

และด้วยเหตุนี้ จึงได้ฟังก์ชันถอดแบบร่วมกลุ่มที่อาจเป็นไปได้ทั้งหมดของ $Q(\sqrt{2}, \sqrt{3})$

ขอให้สังเกตว่า $G(Q(\sqrt{2}, \sqrt{3})/Q)$ มีอันดับ (order) 4 และ $|(Q(\sqrt{2}, \sqrt{3}) : Q| = 4$ #

11.3 ฟังก์ชันถอดแบบร่วมกลุ่มโฟรเบนิอุส

(The Frobenius automorphism)

ให้ F เป็นสนามจำกัด เราสามารถจะแสดงภายหลังได้ว่า กลุ่มของฟังก์ชันถอดแบบร่วมกลุ่มของ F เป็นวัฏจักร (cyclic) กลุ่มวัฏจักร (cyclic group) โดยนิยามเป็นกลุ่มที่มีตัวก่อกำเนิดและอาจมีตัวก่อกำเนิดได้หลายตัว ไม่มีหนทางใดจะมาวัดได้ว่าตัวก่อกำเนิดใดสำคัญกว่ากันอย่างไรก็ตามสำหรับกลุ่มวัฏจักรของฟังก์ชันถอดแบบร่วมกลุ่มทั้งหมดของสนามจำกัด จะมี

ตัวก่อกำเนิดธรรมชาติ (natural generator หรือ canonical generator) เรียกว่า ฟังก์ชันถอดแบบร่วมกลุ่มโฟรเบนิอุส

ทฤษฎี 11.3.1 ให้ F เป็นสนามจำกัดของลักษณะเฉพาะ (characteristic) p แล้วฟังก์ชัน $\sigma_p : F \to F$ กำหนดโดย $\sigma_p(a) = a^p$ สำหรับ $a \in F$ เป็นฟังก์ชันถอดแบบร่วมกลุ่ม เรียกว่า ฟังก์ชันถอดแบบร่วมกลุ่มโฟรเบนิอุส ของ F และ $F_{\{\sigma_p\}} = Z_p$

พิสูจน์

ให้ $a, b \in F$

โดยทฤษฎีการกระจายทวินาม $(a + b)^p$ เราจะได้ว่า

$$
\begin{aligned}
(a + b)^p &= a^p + (p \cdot 1)a^{p-1}b + \left(\frac{p(p-1)}{2} \cdot 1\right)a^{p-2}b^2 + \dots + (p \cdot 1)ab^{p-1} + b^p \\
&= a^p + 0a^{p-1}b + 0a^{p-2}b^2 + \dots + 0ab^{p-1} + b^p \\
&= a^p + b^p
\end{aligned}
$$

ดังนั้น

$$
\begin{aligned}
\sigma_p(a + b) &= (a + b)^p \\
&= a^p + b^p \\
&= \sigma_p(a) + \sigma_p(b)
\end{aligned}
$$

และ

$$
\begin{aligned}
\sigma_p(ab) &= (ab)^p \\
&= a^p b^p \\
&= \sigma_p(a)\,\sigma_p(b)
\end{aligned}
$$

$\therefore$ σ_p เป็นฟังก์ชันถ่ายแบบ

ถ้า $\sigma_p(a) = 0$ แล้ว $a^p = 0$

$\therefore$ $a = 0$

$\therefore$ $\ker(\sigma_p) = \{0\}$

เนื่องจาก F เป็นเซตจำกัด

และสำหรับ a^p ซึ่ง $a \in F$ จะได้ว่า $\sigma_p(a) = a^p$

$\therefore$ σ_p เป็นฟังก์ชันหนึ่งต่อหนึ่งแบบทั่วถึง

$\therefore$ σ_p เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ F

สนามจำนวนเฉพาะ Z_p จะต้องบรรจุอยู่ใน F เนื่องจาก F มีลักษณะเฉพาะ p

สำหรับ $c \in Z_p$

$\sigma_p(c) = c^p = c$

ดังนั้น พหุนาม $x^p - x$ มีศูนย์ p ตัวใน F เรียกสมาชิกของ Z_p

โดยทฤษฎี 7.1.2 กล่าวว่า พหุนามที่มีลำดับขั้น n จะมีศูนย์ได้อย่างมากที่สุด n ตัวในสนาม

เนื่องจากสมาชิกเหล่านี้คงที่ภายใต้ σ_p เป็นศูนย์ใน F ของ $x^p - x$

$\therefore$ $Z_p = F_{\{\sigma_p\}}$ #

แบบฝึกหัดที่ 11

1) จงพิจารณาข้อความแต่ละข้อต่อไปนี้เป็นจริงหรือเท็จ

...............ก) สำหรับแต่ละ $\alpha, \beta \in E$ จะมีฟังก์ชันถอดแบบร่วมกลุ่มของ E ส่ง α ไปบน β เสมอ

.............ข) สำหรับ α, β ที่เป็นพีชคณิตเหนือสนาม F จะมีฟังก์ชันถอดแบบของ $F(\alpha)$ ไปบน $F(\beta)$

.............ค) ถ้า α, β ที่เป็นพีชคณิตและสังยุคเหนือสมการ F จะมีฟังก์ชันถอดแบบของ $F(\alpha)$ ไปบน $F(\beta)$ เสมอ

.............ง) ทุก ๆ ฟังก์ชันถอดแบบร่วมกลุ่มของทุก ๆ สนาม E leave fixed ทุก ๆ สมาชิกของสนามย่อยจำนวนเฉพาะของ E

.............จ) ทุก ๆ ฟังก์ชันถอดแบบร่วมกลุ่มของทุก ๆ สนาม E leave fixed สมาชิกของ E เป็นจำนวนอนันต์

.............ฉ) ทุก ๆ ฟังก์ชันถอดแบบร่วมกลุ่มของทุก ๆ สนาม E leave fixed สมาชิกของ E อย่างน้อยที่สุด 2 ตัว

.............ช) ทุก ๆ ฟังก์ชันถอดแบบร่วมกลุ่มของทุก ๆ สนาม E ที่มีลักษณะเฉพาะ O leave fixed สมาชิกของ E เป็นจำนวนอนันต์

.............ซ) เซตของฟังก์ชันถอดแบบร่วมกลุ่มทั้งหมดของสนาม E เป็นกลุ่มภายใต้การคูณฟังก์ชัน

.............ฌ) สำหรับสนาม $F \leqslant E \leqslant K$, $G(K/E) \leqslant G(K/F)$

2) จงหาสังยุคทั้งหมดของแต่ละจำนวนที่กำหนดให้เหนือสนามที่กำหนดให้

ก) $\sqrt{2}$ เหนือ Q

ข) $\sqrt{2}$ เหนือ R

ค) $3 + \sqrt{2}$ เหนือ Q

ง) $\sqrt{2} - \sqrt{3}$ เหนือ Q

จ) $\sqrt{2} + i$ เหนือ Q

ฉ) $\sqrt{2} + i$ เหนือ R

ช) $\sqrt{1 + \sqrt{2}}$ เหนือ Q

ซ) $\sqrt{1 + \sqrt{2}}$ เหนือ $Q(\sqrt{2})$

3 พิจารณาสนาม $E = Q(\sqrt{2}, \sqrt{3}, \sqrt{5})$ เรามีฟังก์ชันถอดแบบมูลฐานต่อไปนี้ (ซึ่งในที่นี้เป็นฟังก์ชันถอดแบบร่วมกลุ่มของ E)

$\psi_{\sqrt{2}, -\sqrt{2}} : (Q(\sqrt{3}, \sqrt{5}))(\sqrt{2}) \to (Q(\sqrt{3}, \sqrt{5}))(-\sqrt{2})$

$\psi_{\sqrt{3}, -\sqrt{3}} : (Q(\sqrt{2}, \sqrt{5}))(\sqrt{3}) \to (Q(\sqrt{2}, \sqrt{5}))(-\sqrt{3})$

$\psi_{\sqrt{5}, -\sqrt{5}} : (Q(\sqrt{2}, \sqrt{3}))(\sqrt{5}) \to (Q(\sqrt{2}, \sqrt{3}))(-\sqrt{5})$

ถ้าให้ $\tau_2 = \psi_{\sqrt{2}, -\sqrt{2}}, \tau_3 = \psi_{\sqrt{3}, -\sqrt{3}}, \tau_5 = \psi_{\sqrt{5}, -\sqrt{5}}$

จงหาค่าต่อไปนี้

ก) $\tau_2(\sqrt{3})$

ข) $\tau_2(\sqrt{2} + \sqrt{5})$

ค) $\tau_2\tau_3(\sqrt{2} + 3\sqrt{5})$

ง) $\tau_3\tau_5\left(\dfrac{\sqrt{2} - 3\sqrt{5}}{2\sqrt{3} - \sqrt{2}}\right)$

4) สนาม $Q(\sqrt{2})$ และ $Q(3 + \sqrt{2})$ เหมือนกัน ให้ $\alpha = 3 + \sqrt{2}$ จงหาสังยุค $\beta \neq \alpha$ เหนือ Q