

אלגברה ב' 2 - הרצאה 21

16.5.11

הרחבות מעגליות

דיברנו עבר על הרחבות מעגליות מסדר n כאשר n זר לאפיון. נרצה לדבר על מקרה פרטי "הפוך" כאשר ההרחבות ממעלה $\text{chr } K = p$.

משפט. (משפט הילברט 90 - גרסה חיבורית)
 L/K הרחבה מעגלית סופית בעלת חבורה $\langle \sigma \rangle = G$. יהי $\beta \in L$. אז $T_{L/K}(\beta) = 0$ אם ורק אם $\alpha \in L$ כך ש- $\alpha - G(\alpha) = \beta$.
 הוכחה. $\Rightarrow$

$$\begin{aligned} T_{L/K}(\beta) &= \sum_{\tau \in G} \tau(\beta) = \sum_{\tau \in G} \tau(\alpha - \sigma(\alpha)) = \sum_{\tau \in G} \tau(\alpha) - \sum_{\tau \in G} \tau(\sigma(\alpha)) = \\ &= T_{L/K}(\alpha) - T_{L/K}(\alpha) = 0 \end{aligned}$$

$\Leftarrow$: כאן צריך טריק. $n = |G|$, $G = \{1, \sigma, \dots, \sigma^{n-1}\}$. $1, \sigma, \dots, \sigma^{n-1} : L^x \rightarrow L^x$. כרקטרים שונים ולפי משפט ארטיין הם בת"ל מעל L ולכן $1 + \sigma + \dots + \sigma^{n-1} \neq 0$. כלומר יש $z \in L$ כך ש- $T_{L/K}(z) \neq 0$.

$$\begin{aligned} \alpha' &:= \beta\sigma(z) + (\beta + \sigma(\beta))\sigma^2(z) + (\beta + \sigma(\beta) + \sigma^2(\beta))\sigma^3(z) + \dots \\ &\quad \dots + (\beta + \sigma(\beta) + \dots + \sigma^{n-2}(\beta))\sigma^{n-1}(z) \end{aligned}$$

$$\begin{aligned} \sigma(\alpha') &= \sigma(\beta)\sigma(z) + (\sigma(\beta) + \sigma^2(\beta))\sigma^3(z) + \dots \\ &\quad \dots + \underbrace{(\sigma(\beta) + \sigma^2(\beta) + \dots + \sigma^{n-1}(\beta))}_{=T_{L/K}(\beta) - \beta = -\beta} \underbrace{\sigma^n(z)}_{=z} \end{aligned}$$

$$\alpha' - \sigma(\alpha') = \beta z + \beta\sigma(z) + \beta\sigma^2(z) + \beta\sigma^3(z) + \dots + \beta\sigma^{n-1}(z) = \beta T_{L/K}(z)$$

□ אז $\alpha - \sigma(\alpha) = \beta$ או $\alpha = \frac{1}{T_{L/K}(z)}\alpha'$ נגדיר אם נגדיר $0 \neq T_{L/K} \in K$.

משפט. (Artin - Schreier) יהי K שדה $\text{chr } K = p > 0$ אז:

1. תהי L/K מעגלית ממעלה p אז יש $\alpha \in L$ כך ש- $L = K(\alpha)$ ו- α שורש של $x^p - x - a$ עבור איזה $a \in K$.

2. יהי $a \in K$ ויהי $\alpha \in F$ שורש של $f = x^p - x - a$. אז $K(\alpha)/K$ מעגלית ממעלה 1 או p . במקרה הראשון כל שורשי f בתוך K . במקרה השני f אי פריק.

הוכחה.

$$1. \text{ יהי } b \in K. \text{ אז } [L : K]b = p^b = 0 \text{ ולכן } \sum_{\tau \in \text{Gal}(L/K)} \tau(b) = b$$

בפרט, $T_{L/K}(-1) = 0$. לפי משפט 90 יש $\alpha \in L$ כך ש- $\alpha - \sigma(\alpha) = -1$, כלומר $\sigma(\alpha) = \alpha + 1$.

באינדוקציה $\sigma^i(\alpha) = \alpha + i$ לכל $i \geq 0$. לכן, $\alpha, \alpha + 1, \dots, \alpha + (p-1)$ הם שורשים של $\text{irr}(\alpha, K)$. הם שונים זה מזה. לכן $\deg \text{irr}(\alpha, K) \geq p$. $[K(\alpha) : K] = \deg \text{irr}(\alpha, K) \geq p$.

מצד שני $K \subseteq K(\alpha) \subseteq L$, $[L : K] = p$, לכן $K(\alpha) = L$. עבור $i = 0, 1, \dots, p-1$.

$$\begin{aligned} \sigma^i(\alpha^p - \alpha) &= \sigma^i(\alpha^p) - \sigma^i(\alpha) = (\sigma^i(\alpha))^p - \sigma(\alpha) = \\ &= \alpha^p + i^p - \alpha - i = \alpha^p - \alpha + i^p - i = \alpha^p - \alpha \end{aligned}$$

כל $i \in F_p$ שורש של $x^p - x$.

לכן $a := \alpha^p - \alpha \in L^{\text{Gal}(L/K)} = K$. מכאן α שורש של $x^p - x - a \in K[x]$.

2. $\alpha, \alpha + 1, \dots, \alpha + p - 1 \in K(\alpha)$ הם שורשים של f : אכן,

$$f(\alpha + i) = (\alpha + i)^p - (\alpha + i) - a = f(\alpha) + i^p - i = 0$$

הם שונים זה מזה לכן הם כל השורשים של f . בפרט f פריד. לכן $K(\alpha)$ הוא שדה הפיצול של f שהינו פריד ולכן $K(\alpha)/K$ גלואה. נסמן $L = K(\alpha)$, $G = \text{Gal}(L/K)$. אם $\sigma \in G$ אז גם $\sigma(\alpha)$ שורש של f . לכן,

$$(\sigma(\alpha) - \alpha)^p = \sigma(\alpha)^p - \alpha^p = (\sigma(\alpha) + a)^p - (\alpha + a) = \sigma(\alpha) - \alpha$$

לכן $\omega(\alpha) := \sigma(\alpha) - \alpha \in F_p$. כלומר $\sigma(\alpha) = \alpha + \omega(\sigma)$. אם $\sigma, \tau \in G$ אז עבור $\alpha \neq 0$:

$$\alpha + \omega(\sigma\tau) = \sigma(\tau(\alpha)) = \sigma(\alpha + \omega(\tau)) = \sigma(\alpha) + \omega(\tau) = \alpha + \omega(\sigma) + \omega(\tau)$$

$$\omega(\sigma\tau) = \omega(\sigma) + \omega(\tau) \text{ כלומר}$$

לכן, $\omega : G \rightarrow F_p$ הומומורפיזם של חבורות. גרעינו $\{\sigma \in G : \sigma(\alpha) = \alpha\} = \{1\}$. לכן ω שייכון. לכן G מסדר d , $d|p$ לכן $d = 1$ או $d = p$.

במקרה הראשון $\alpha \in K$ ולכן כל שורשי f שהם מהצורה $\alpha + i$ גם ב- K . במקרה השני $[K(\alpha) : K] = p = \deg f$ לכן f אי פריק.

□