

אלגברה ב' 2 - הרצאה 20

11.5.11

התסכלנו על $f_n = \text{irr}(\zeta_n, \mathbb{Q})$ וראינו $f_n(x) = \prod_{\zeta} (x - \zeta)$ כאשר ζ שורש יחידה n -י פרימיטיבי. ואז

$$\prod_{\zeta} (x - \zeta) = \prod_{\substack{0 \leq k < n \\ n \text{-זר } k}} (x - \zeta_n^k) = \prod_{\substack{\zeta \in \tilde{K}^* \\ \text{ord } \zeta = n}} (x - \zeta)$$

$$x^n - 1 = \prod_{\substack{\zeta \text{ שורש יחידה } n \\ \text{ord } \zeta | n}} (x - \zeta) = \prod_{d|n} \prod_{\substack{\zeta \in \tilde{K}^* \\ \text{ord } \zeta = d}} (x - \zeta) = \prod_{d|n} f_d(x)$$

ראינו שאם m, n זרים אז $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$ וכן $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

משפט. יהיו $n, a \in \mathbb{N}$ זרים. אז יש אינסוף ראשוניים p כך ש- $p \equiv a \pmod{n}$.

ללא הוכחה.

אנחנו נשתמש בגרסא קלה יותר עבור $a = 1$.

משפט. A חבורה אבלית סופית. אז יש $L/\mathbb{Q}$ גלואה כך ש- $\text{Gal}(L/\mathbb{Q}) = A$.

ראינו משפט כללי יותר אבל בלי הוכחה. את זה נוכיח:

הוכחה.

$$A \cong \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$$

לפי משפט דיריכלה יש ראשוניים שונים $p_1, \dots, p_r$ כך ש- $p_i \equiv 1 \pmod{n}$, $i = 1, \dots, r$. נסמן, $G_i = \text{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q})$ וראינו

$$G_i \cong (\mathbb{Z}/p_i\mathbb{Z})^* \cong \mathbb{Z}/(p_i - 1)\mathbb{Z}$$

$n_i | p_i - 1$ לכן יש תת חבורה $H_i \leq G_i$ כך ש- $(G_i : H_i) = n_i$. יהי L_i שדה השבת של H_i ב- $\mathbb{Q}(\zeta)$ ואז $\text{Gal}(L_i/\mathbb{Q}) = G_i/H_i \cong \mathbb{Z}/n_i\mathbb{Z}$.
כעת, די להוכיח: לכל $1 \leq k \leq r$ $L_1 L_2 \dots L_k / \mathbb{Q}$ גלואה ו-

$$\text{Gal}(L_1, \dots, L_k / \mathbb{Q}) \cong \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$$

ואכן, עבור $k = 1$ זה ברור. נניח נכונות עבור $k - 1$:

$$\text{Gal}(L_1, \dots, L_{k-1}/\mathbb{Q}) \cong \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_{k-1}\mathbb{Z}$$

ובאופן כללי: $\text{Gal}(L_i/\mathbb{Q}) \cong \mathbb{Z}/n_i\mathbb{Z}$.

$$(L_1 \cdots L_{k-1}) \cap L_k \subseteq \mathbb{Q}(\zeta_{p_1}) \cdots \mathbb{Q}(\zeta_{p_{k-1}}) \cap \mathbb{Q}(\zeta_{p_k}) = \mathbb{Q}(\zeta_{p_1 \cdots p_{k-1}}) \cap \mathbb{Q}(\zeta_{p_k}) = \mathbb{Q}$$

לכן, $L_1 \cdots L_{k-1}/\mathbb{Q}$ גלואה ו-

$$\begin{aligned} \text{Gal}(L_1 \cdots L_k/\mathbb{Q}) &= \text{Gal}(L_1 \cdots L_{k-1}/\mathbb{Q}) \times \text{Gal}(L_k/\mathbb{Q}) = \\ &= 1(\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_{k-1}\mathbb{Z}) \times \mathbb{Z}/n_k\mathbb{Z} = \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z} \end{aligned}$$

□

הערה. מצאנו $L \subseteq \mathbb{Q}(\zeta_m)$ עבור איזה $m \in \mathbb{N}$. אולי אפשר אחרת? לפי משפט Kronecker-Weker אם $L/\mathbb{Q}$ אבליט סופית אז $L \subseteq \mathbb{Q}(\zeta_m)$ עבור איזה m . לידע כללי, ללא הוכחה.

אי תלות לינארית של כרקטרים

הגדרה. תהי G חבורה, K שדה. כרקטר הוא הומומורפיזם של חבורות $\chi: G \rightarrow K^*$.

משפט. Artin

כרקטרים שונים $\chi_1, \dots, \chi_n: G \rightarrow K^*$ ב"ת לינארית מעל K . מה הכוונה? (נסתכל הכרקטרים כפונקציות מ- G לתוך K . כל הפונקציות האלה מהוות מרחב וקטורי) אם $a_1, \dots, a_n \in K$ כך ש- $a_1\chi_1 + \dots + a_n\chi_n = 0$ (1) (הכוונה לפונקציית האפס) אז $a_1 = \dots = a_n = 0$.

הוכחה. באינדוקציה על n . $n = 1$ ברור כי $\chi_1 \neq 0$. נניח נכונות (1) עבור $n - 1$ כרקטרים. $\chi_n \neq \chi_1$ לכן יש $g_0 \in G$ כך ש- $\chi_1(g_0) \neq \chi_n(g_0)$. נכפיל את (1) ב- $\chi_n(g_0)$.

$$(2) \quad a_n\chi_n(g_0) + \dots + a_{n-1}\chi_{n-1}(g_0)\chi_n(g_0) + \dots + a_1\chi_1(g_0)\chi_n(g_0) = 0$$

מצד שני לכל $g \in G$:

$$a_1\chi_1(g) + \dots + a_n\chi_n(g) = 0$$

בפרט עבור g_0g :

$$a_1\chi_1(g_0g) + \dots + a_n\chi_n(g_0g) = 0$$

אבל χ הומומורפיזם לכן:

$$a_1\chi_1(g_0)\chi_1(g) + \dots + a_n\chi_n(g_0)\chi_n(g) = 0$$

כלומר אם נחשוב על זה כפונקציה ב- g מדובר בפונקציית האפס ולכן:

$$(3) \quad a_1 \chi_1(g_0) + \dots + a_n \chi_n(g_0) = 0$$

נכתוב (2) – (3):

$$a_1(\chi_n(g_0) - \chi_1(g_0))\chi_1 + \dots + a_{n-1}(\chi_n(g_0) - \chi_{n-1}(g_0)) = 0$$

לפי הנחת האינדוקציה $a_1(\chi_n(g_0) - \chi_1(g_0)) = 0$ מכאן $a_1 = 0$. נציב $a_1 = 0$ ב-(1) ונקבל $a_2 \chi_2 + \dots + a_n \chi_n = 0$ ואז לפי הנחת האינדוקציה $a_2 = \dots = a_n = 0$. $\square$

הגדרה. תהי L/K הרחבת גלואה סופית.

1. נגדיר $T_{L/K} : L \rightarrow K$ ע"י $T_{L/K}(\alpha) = \sum_{\sigma \in \text{Gal}(L/K)} \sigma(\alpha)$. זה נקרא העקבה מ- L לתוך K .

2. נגדיר $N_{L/K} : L \rightarrow K$ ע"י $N_{L/K}(\alpha) = \prod_{\sigma \in \text{Gal}(L/K)} \sigma(\alpha)$. זה נקרא הנורמה מ- L לתוך K .

מדוע לתוך K ? עבור $\tau \in \text{Gal}(L/K)$:

$$\tau(T_{L/K}(\alpha)) = \sum_{\sigma \in \text{Gal}(L/K)} \tau\sigma(\alpha) = T_{L/K}(\alpha)$$

$$\tau(N_{L/K}(\alpha)) = \prod_{\sigma \in \text{Gal}(L/K)} \tau\sigma(\alpha) = N_{L/K}(\alpha)$$

לכן $T_{L/K}(\alpha) \in L^{\text{Gal}(L/K)} = K$, לכן $N_{L/K}(\alpha) \in L^{\text{Gal}(L/K)} = K$.

הערה. עבור העתקה לינארית $x \mapsto \alpha x$ העקבה של ההעתקה הזאת היא העקבה של המטריצה והנורמה היא בדיוק הדטרמיננטה.

הרחבות מעגליות

משפט. משפט ה-90 של הילברט

תהי L/K הרחבה מעגלית סופית עם חבורת גלואה $G = \langle \sigma \rangle$. יהי $\beta \in L^x$ אזי $\beta = \frac{\alpha}{\sigma(\alpha)} \Leftrightarrow N_{L/K}(\beta) = 1$.

הוכחה. $\Rightarrow$

$$N_{L/K}(\beta) = \prod_{\tau \in G} \tau\left(\frac{\alpha}{\sigma(\alpha)}\right) = \prod_{\tau \in G} \frac{\tau(\alpha)}{\tau\sigma(\alpha)} = \frac{\prod_{\tau \in G} \tau(\alpha)}{\prod_{\tau \in G} \tau \circ \sigma(\alpha)} = \frac{\prod_{\tau \in G} \tau(\alpha)}{\prod_{\tau \in G} \varphi(\alpha)} = 1$$

$\Leftarrow$: נניח $N_{L/K}(\beta) = 1$ נסמן $n = |G| = [L : K]$. $1, \sigma, \sigma^2, \dots, \sigma^{n-1} : L^x \rightarrow L^x$. שונים. לפי משפט ארטין הם ב"ת מעל L : נסתכל על הצירוף

$$1 \cdot 1_L + \beta\sigma + \beta\sigma(\beta)\sigma^2 + \dots + \beta\sigma(\beta) \dots \sigma^{n-2}(\beta)\sigma^{k-1} \neq 0$$

לכן קיים $z \in L^x$ המקיים:

$$\alpha := 1 \cdot z + \beta\sigma(z) + \beta\sigma(\beta)\sigma^2(z) + \dots + \beta\sigma(\beta) \dots \sigma^{n-2}(\beta)\sigma^{n-1}(z) \neq 0$$

נפעיל את σ ונכפיל ב- β . נקבל:

$$\beta\sigma(\alpha) = \beta \cdot \sigma(z) + \dots + \beta\sigma(\beta) \dots \sigma^{n-2}(\beta)\sigma^{n-1}(z) + \beta \dots \sigma^{n-1}(\beta) \cdot \sigma^n(z)$$

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

$$\beta\sigma(\alpha) = \beta \cdot \sigma(z) + \dots + \beta\sigma(\beta) \dots \sigma^{n-2}(\beta)\sigma^{n-1}(z) + z$$

$$\beta\sigma(\alpha) = \sigma$$

ולבסוף:

$$\beta = \frac{\alpha}{\sigma(\alpha)}$$

□

משפט. Kummer

יהי K שדה, $n \in \mathbb{N}$ כך ש- $\text{chr } K \nmid n$: נניח $r_n \in K$ שורש פרימיטיבי.

1. תהי L/K מעגלית ממעלה n . אז יש $\alpha \in L$ כך ש- $L = K(\alpha)$, $\alpha^n \in K$.

2. יהי $a \in K$, ויהי $\alpha \in \tilde{K}$ שורש של $x^n - a$. אז $K(\alpha)/K$ מעגלית ממעלה d כאשר $d|n$ וכן $\alpha^n \in L$ ולכן $\alpha^n = (\alpha^d)^{n/d} \in K$.

הוכחה.

1. $\text{ord } \sigma = n, \text{Gal}(L/K) = \langle \sigma \rangle$.

$$M_{L/K}(r_n^{-1}) = \prod_{i=0}^{n-1} r_n^{-1} = (r_n^n)^{-1} = 1$$

לפי משפט הילברט 90 יש $\alpha \in L$ כך ש- $r_n^{-1} = L/\sigma(L)$, כלומר $\sigma(\alpha) = \alpha r_n$. מכאן, $\sigma^2(\alpha) = \alpha r_n^2, \dots, \sigma^{(n-1)}(\alpha) = \alpha r_n^{n-1}$, אז $\alpha, \alpha r_n, \dots, \alpha r_n^{n-1}$ צמודים ל- α ע"י אוטומורפיזם של L מעל K , לכן הם השורשים של $\text{irr}(\alpha, K)$. הם שונים זה מזה לכן $[K(\alpha) : K] = \deg(\text{irr}(\alpha, K)) \geq n$.

מצד שני, $\alpha \in L$ ולכן $K(\alpha) \subseteq L$ ולכן $[K(\alpha) : K] \leq [L : K] = n$ ולכן עפ"י כלל שני השורטרים והשיכור $[K(\alpha) : K] = n$ ולכן $K(\alpha) = L$.

$$\sigma^i(\alpha^n) = (\sigma^i(\alpha))^n = (r_n^i \alpha)^n = r_n^{in} \alpha^n = \alpha^n$$

ולכן $\alpha^n \in L^G = K$.

2. $\alpha, r_n\alpha, r_n^{n-1}\alpha \in K(\alpha)$ הם שורשים של $x^n - a$ שונים זה מזה. לכן הם כל השורשים של $x^n - a$. לכן שדה הפיצול של $x^n - a$ מעל K הוא $K(\alpha, r_n\alpha, \dots, r_n^{n-1}\alpha) = K(\alpha)$. לכן $K(\alpha)/K$ נורמלית ופרידה ולכן גלואה. אם $\sigma \in \text{Gal}(L/K)$ אז גם $\sigma(\alpha)$ שורש של $x^n - a$ כלומר $(\sigma(\alpha))^n = a$, $\left(\frac{\sigma(\alpha)}{\alpha}\right)^n = \frac{a}{a} = 1$ לכן יש $w(\sigma) \in \langle r_n \rangle = r_n(\tilde{K}) \cong \mathbb{Z}/n\mathbb{Z}$ כך ש- $\sigma(\alpha) = w(\sigma)\alpha$. אם $\sigma, \tau \in \text{Gal}(L/K)$ אז

$$w(\sigma\tau)\alpha = \sigma\tau(\alpha) = \sigma(\tau(\alpha)) = \sigma(w(\tau), \alpha) = w(\tau)(\sigma(\alpha)) = w(\tau)w(\sigma)\alpha$$

כלומר $w(\sigma\tau) = w(\sigma)w(\tau)$ ולכן $w : \text{Gal}(L/K) \rightarrow \langle r_n \rangle \cong \mathbb{Z}/n\mathbb{Z}$ הומומורפיזם. גרעינו $\{1\} = \{\sigma | \sigma(\alpha) = \alpha\} = \{\sigma | w(\sigma) = 1\}$ לכן w שיכון ולכן $\text{Gal}(L/K)$ מעגלית (כי כל תת חבורה של $\mathbb{Z}/n\mathbb{Z}$ מעגלית) והסדר שלה מחלק את n .

אם $\sigma \in \text{Gal}(L/K)$ אז $\text{ord } w(\sigma) = \text{ord } \sigma | d$

$$\sigma(\alpha^d) = (\sigma(\alpha))^d = (w(\sigma)\alpha)^d = w(\sigma)^d \alpha^d = \alpha^d$$

ולכן $\alpha^d \in K$.

□