

אלגברה ב' 2 - הרצאה 18

2.5.11

K שדה המנות של תחום פריקות R . $f = x^n + a_1x^{n-1} + \dots + a_n \in R[x] \subseteq K[x]$.
 $G = \text{Gal}(f, K)$ רוצים לחשב את $\alpha_1, \dots, \alpha_n$ שורשים.

$$G_n = \prod_{\pi \in S_n} (x - t_{\pi(1)}u_1 - \dots - t_{\pi(n)}u_n) = P_n(s_1(\bar{t}), \dots, s_n(\bar{t}))$$

$$g(\bar{u}, x) = P_n(-a_1, \dots, (-1)^n a_n) \in R[\bar{u}, x]$$

$$g(\bar{u}, x) = g_1(\bar{u}, x) \dots g_r(\bar{u}, x)$$

פירוק לאי פריקים, הם שונים:

$$g_j(\bar{u}x) = \prod_{\pi \in V_j} (x - \alpha_{\pi(1)}u_1 - \dots - \alpha_{\pi(n)}u_n)$$

ראינו ש- $V_j = G\rho_j$.
 יהי $w \in S_k$ אז

$$\begin{aligned} g_j(u_{\omega(1)}, \dots, u_{\omega(n)}, x) &= \prod_{\pi \in G\rho_j} (x - \alpha_{\pi(1)}u_{\omega(1)} - \dots - \alpha_{\pi(n)}u_{\omega(n)}) = \\ &= \prod_{\pi \in G\rho_j} (x - \alpha_{\pi\omega^{-1}(1)}u_1 - \dots - \alpha_{\pi\omega^{-1}(n)}u_n) = \\ &= \prod_{\pi \in G\rho_j\omega^{-1}} (x - \alpha_{\pi(1)}u_1 - \dots - \alpha_{\pi(n)}u_n) = g_i(\bar{u}, x) \end{aligned}$$

עבור $1 \leq i \leq r$. זה מוכיח את 3.

$$\begin{aligned} \Leftrightarrow G\rho_j = G\rho_j\omega \Leftrightarrow G\rho_j\omega^{-1} = G\rho_j \Leftrightarrow g_1(u_1, \dots, u_n, x) &= g_j(u_{\omega(1)}, \dots, u_{\omega(n)}, x) \\ \omega \in \rho_j^{-1}G\rho_j = G^{\rho_j} \Leftrightarrow \rho_j\omega\rho_j^{-1} \in G & \end{aligned}$$

ומכאן נובע 4.

סיימנו את המשפט.

יהי $K = \mathbb{Q}$, $R = \mathbb{Z}$. ניקח ראשוני p . סימון: עבור $h \in \mathbb{Z}[x]$ נסמן ב- $\bar{h} \in F_p[x]$ את הפולינום שמקבל מ- h ע"י ההעתקה $\mathbb{Z} \rightarrow F_p = \mathbb{Z}/p\mathbb{Z}$ על מקדמיו.
 יהי $f(x) = x^n + a_1x^{n-1} + \dots + a_n \in \mathbb{Z}[x]$ כך ש- $\bar{f} \in F_p[x]$ פריד. יהי $P_n = g(-a_1, \dots, (-1)^n a_n) = g(\bar{u}, x) = g_1(\bar{u}, x) \dots g_r(\bar{u}, x)$ כמו קודם.

נסמן:

$$P_n(-\bar{a}_1, \dots, (-1)^n \bar{a}_n) = \bar{g}(\bar{u}, x) = \bar{g}_1(\bar{u}, x) \dots \bar{g}_r(\bar{u}, x)$$

הגורמים $\bar{g}_1, \dots, \bar{g}_n$ אינם בהכרח אי פריקים מעל $F_p(\bar{u})$. נפרק אותם לגורמים אי פריקים. למשל, $\bar{g}_1(\bar{u}, x) = \bar{g}_{11}(\bar{u}, x) \dots \bar{g}_{1s}(\bar{u}, x)$. יהי $\omega \in S_n$ כך ש- $\bar{g}_1 1(u_{\omega(1)}, \dots, u_{\omega(n)}, x) = \bar{g}_n(\bar{u}, x)$ לפי 3 יש $1 \leq i \leq r$ כך ש- $\bar{g}_1(u_{\omega(1)}, \dots, u_{\omega(n)}, x) = g_i(\bar{u}, x)$ נראה ש- $i = 1$.

$$\bar{g}_1(u_{\omega(1)}, \dots, u_{\omega(n)}, x) = \bar{g}_i(\bar{u}, x)$$

$$\bar{g}_{11}(\bar{u}, x) | \bar{g}_1(\bar{u}, x), \bar{g}_i(\bar{u}, x)$$

מכאן $i = 1$ אחרת $g_{11}(\bar{u}, x)$ יופיע פעמיים בפירוק של $\bar{g}(u, x)$ שיש לו גורמים אי פריקים שונים.

$$g_1(u_{\omega(1)}, \dots, u_{\omega(n)}, x) = g_1(\bar{u}, x) \text{ ואז } \bar{g}_{11}(u_{\omega(1)}, \dots, u_{\omega(n)}, x) = \bar{g}_1 1(\bar{u}, x)$$

משפט. יהי $f \in \mathbb{Z}[x]$ מתקון פריד כך ש- $\bar{f} \in F_p[x]$ פריד. אז קיים שיכון $\text{Gal}(\bar{f}, F_p) \rightarrow \text{Gal}(f, \mathbb{Q})$ של חבורות תמורות. כלומר אם $\alpha_1, \dots, \alpha_n \in \mathbb{Q}$ השורשים של f אפשר לסדר את השורשים של $\bar{f}$ ב- $\bar{\alpha}_1, \dots, \bar{\alpha}_n$ כך ש- $\text{Gal}(f, F_p) \leq \text{Gal}(f, \mathbb{Q})$.

חישוב של $\text{Gal}(\bar{f}, F_p)$:

$\bar{f} \in F_p[x]$ מתוקן פריד. תהי A קבוצה השורשים שלו ב- $\bar{F}_p$. $\text{Gal}(\bar{f}, F_p) = \langle \sigma \rangle$. מעגלית כאשר $\varphi(x) = x^p$, $\sigma = \varphi|_A$. מהי σ כתמורה ב- S_n ? יהי $\bar{f} = \bar{f}_1 \dots \bar{f}_k$ פירוק של $\bar{f}$ לגורמים אי פריקים מעל F_p . $A = \bigsqcup A_i$ כאשר A_i קבוצת השורשים של $\bar{f}_i$. אז $\text{Gal}(\bar{f}, F_p)$ מעתיקה את איברי A_i לתוך A_i ופועלת באופן טרנזיטיבי על A_i לכל i .

$$A_i = \{\alpha_i, \varphi(\alpha_i), \varphi^2(\alpha_i), \dots, \varphi^{\deg \bar{f}_i - 1}(\alpha_i)\}$$

מכאן ש- σ הוא מכפלה של k חישוקים מאורכים $\deg \bar{f}_1, \dots, \deg \bar{f}_k$. למשל, אם ניקח $f = x^5 - x - 1 \in \mathbb{Z}[x]$. נסמן f_p את הצמצום של f מודולו p . אז $f_2 = (x^2 + x + 1)(x^3 + x + 1)$. פירוק לגורמים אי פריקים מעל F_2 . לכן חבורת גלואה $(1, 1) \in \text{Gal}(f_2, F_2)$ עד כדי הצמדה וכן $G = \text{Gal}(f, \mathbb{Q}) = (1, 2)(3, 4, 5)$ (עד כדי הצמדה). בה"כ נניח שבאמת מכילה $\pi := (1, 2)(3, 4, 5)$.

אם $p = 5$ f_5 אי פריק מעל F_5 לכן $\text{Gal}(f, \mathbb{Q})$ מכילה חישוק מאורך 5. לכן $(1, 2) = \pi^3 \in G$, $\rho \in G$, ρ חישוק מאורך 5. נחליף ρ בחזקה מתאימה ואז $\rho = (1, 2, \dots)$ בה"כ נניח $\rho = (1, 2, 3, 4, 5)$. קיבלנו ש- G מכילה את החבורה $S_5 = \langle (1, 2, 3, 4, 5), (1, 2) \rangle$.