

אלגברה ב' 2 – הרצאה 17

27.4.11

אנחנו מדברים על חבורת גלואה של פולינום. $f \in L[x]$ פולינום מתוקן, פריד, $f = (x - \alpha_1) \dots (x - \alpha_n)$ בסגור האלגרי. ניקח $L = K(\alpha_1, \dots, \alpha_n)$ שדה פיצול. אז $\text{Gal}(f, K) \subseteq A = \{\alpha_1, \dots, \alpha_n\}$ כחבורת תמורות על $\text{Gal}(f, K) := \text{Gal}(L/K)$. $S(A) \cong S_n$.

הערה. (תרגיל)

אם נשנה את הסדר של $\alpha_1, \dots, \alpha_n$ נקבל במקום $\text{Gal}(f, K)$ חבורה צמודה לה ב- S_n , כלומר $\rho^{-1} \text{Gal}(f, K) \rho$ כאשר $\rho \in S_n$ אותה התמורה שהפעלנו על האיברים.

חבורת גלואה של פולינום ממעלה 3

יהי $f = x^3 + ax^2 + bx + c \in K[x]$ פולינום פריד ואז $f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$ שונים. $\alpha_1, \alpha_2, \alpha_3 \in \bar{K}$. $L = K(\alpha_1, \alpha_2, \alpha_3)$ שדה הפיצול הוא $[K(\alpha) : K] = 3$ ואז $[L : K] = 3$ לכל אופן, $K \subseteq K(\alpha_1) \subseteq L$ לכן אם f אי פריק אז $\text{Gal}(f, K) = S_3 \vee A_3$. איך לפי הפולינום נדע מי מהן?

תרגיל. יהי $D = (x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$ יהיו s_1, s_2, s_3 הפולינומים הסימטריים היסודיים במשתנים x_1, x_2, x_3 . מצא $g \in \mathbb{Z}[S_1, S_2, S_3]$ ממשקל ≥ 6 כך ש- $g(s_1, s_2, s_3) = D$.

פתרון. D סימטרי ממעלה 6 לכן זה אפשרי. יתר על כן, הוא הומוגני - כל המונומים שלו ממעלה 6. המונומים ממקשל 6 ב- g נותנים אחרי ההצבה של s_1, s_2, s_3 נותנים מונומים ממעלה 6 ב- x_1, x_2, x_3 ואילו מונומים ב- g ממקשל קטן יותר נותנים מונומים ממעלה קטנה מ-6 ב- x_1, x_2, x_3 . לכן, ב- g יש רק מונומים ממקשל 6, כלומר

$$(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2 = ks_1^6 + ls_1^4s_2 + ms_1^3s_3 + ns_1^2s_2^2 + ps_1s_2s_3 + qs_2^3 + rs_3^2$$

נותר רק למצוא את המקדמים: k, l, m, n, p, q, r . כיצד נעשה את זה? נציב ב- x_1, x_2, x_3 ונקבל 7 משוואות, ננסה גם להציב כך שיצאו בלתי תלויות ונקבל את המקדמים. למשל, $s_3 = 1, s_2 = 0, s_1 = 0$ כלומר x_1, x_2, x_3 הם שורשים של $x^3 - 1 = x^3 - 0x^2 + 0x - 1$. נציב: $x_3 = \omega^2, x_2 = \omega, x_1 = 1$

$$\begin{aligned} r &= (1 - \omega)^2(\omega - \omega^2)^2(\omega^2 - 1)^2 = ((1 - \omega)(1 - \omega)(1 - \omega))^2 = \\ &= (1 - \omega)^6 = ((1 - \omega)^2)^3(1 - 2\omega - \omega - 1)^3 = -27 \end{aligned}$$

בסופו של דבר:

$$g(s_1, s_2, s_3) = -4s_1^3s_3 + s_1^2s_2^2 + 18s_1s_2s_3 - 4s_2^3 - 27s_3^2$$

מה הקשר של התרגיל לנושא?
נסמן:

$$\delta := (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3) = \prod_{i < j} (\alpha_i - \alpha_j)$$

$$\Delta := \delta^2$$

זה נקרא הדיסקרימיננטה של f .
לפי התרגיל,

$$\Delta = g(-a, b, -c) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \in K$$

לכל $\sigma \in \text{Gal}(L/K)$ אז $\sigma(\delta) = \pm\delta$ ולמעשה זה נכון אפילו לכל תמורה $\sigma \in S_n$. לכן, $\sigma(\Delta) = \Delta$ כלומר $\Delta \in K$. זה כבר ידענו. אבל עכשיו:

• אם $\sigma|_A \in A_3$ אז $\sigma(\delta) = \delta$ אם $\sigma|_A \notin A_3$ אז $\sigma(\delta) = -\delta$.

• אם $\text{chr } K \neq 2$ אז: $\sigma(\delta) = \delta \Leftrightarrow \sigma \in A_3$.

$\delta \neq 0$ כי השורשים שונים.
אם האפיון $\text{chr } K \neq 2$ אז: לכן $\text{Gal}(f, K) \subseteq A_3$ $\Leftrightarrow \sigma(\delta) = \delta$ לכל $\sigma \in \text{Gal}(L/K)$
 $\Leftrightarrow \delta \in K \Leftrightarrow \Delta$ הוא ריבוע ב- K .

דוגמא. $f = x^3 - 3x + 1 \in K[x]$ אז $f' = 3x^2 - 3 = 3(x-1)(x+1)$

1. הפולינום פריד אם זר לנגזרת. מתי ± 1 שורש של הפולינום? אם $\text{chr } K = 3$ אז $f = x^3 + 1 = (x+1)^3$ מתפצל מעל K , כלומר $L = K$ (זה שדה הפיצול).

2. אם $\text{chr } K \neq 3$ אז f, f' זרים (כי $f(\pm 1) \neq 0$) לכן f פריד. $\Delta = -4(-3)^4 - 26 = -26 \in K^2$. לכן אם $\text{chr } K \neq 2, 3$ אז $\text{Gal}(f, K) \leq A_3$. כלומר $\text{Gal}(f, K) = A_3$.
ואז $[L : K] = 3$ או $\text{Gal}(f, K) = \{1\}$ ואז $L = K$. כיצד מבדילים?

אם f אי פריק מעל K אז $\text{Gal}(f, K) = A_3$ ואם f פריק אז $g = (x - \alpha)g$ ממעלה 2 ואז L הוא שדה הפיצול של g , כי $\alpha \in K$. לכן $[L : K] \leq 2! = 2$ לכן לא ייתכן שזה 3 ולכן $\text{Gal}(f, K) = \{1\}$ ולכן $L = K$.

מה אם $\text{chr } K = 2$ אז:

$x^3 + x + 1 \in f \in F_2[x]$ הוא אי פריק מעל F_2 . מדוע? כי אם היה פריק היה צריך להיות שורש 0 או 1 אינם שורשים. לכן יוצר הרחבה ממעלה 3 של F_2 . יש רק הרחבה אחת ממעלה 3 ולכן היא F_{2^3} והיא גלואה מעל F_2 . ולכן F_{2^3} הוא שדה הפיצול של f מעל F_2 . לכן $L = K/F_{2^3}$ ומכאן נקבל $\text{Gal}(L/K) = \text{Gal}(F_{2^3}/K \cap F_{2^3})$ ו- L נוצר ע"י שורש של f מעל K . כעת נקבל את המסקנה מאותם הנימוקים כמו קודם.

אלגוריתם לחישוב $\text{Gal}(f, K)$

(אם יודעים לפרק פולינום). $t_1, \dots, t_n, u_1, \dots, u_n, Y_1, \dots, Y_n, X$ משתנים בלתי תלויים מעל K . נסמן $\bar{Y} = (Y_1, \dots, Y_n)$, $\bar{t} = (t_1, \dots, t_n)$, $\bar{u} = (u_1, \dots, u_n)$:
נגדיר לכל n :

S_n פועלת על $\mathbb{Z}[\bar{u}, x][\bar{t}]$ כתמורה על $t_1, \dots, t_n$. יהי $\sigma \in S_n$ אזי $\sigma(G_n) = \prod_{\pi \in S_n} (x - \text{אזי } \sigma \in S_n)$. לכן קיים סימטרי. G_n כלומר $(\sigma S_n = S_n)$ כי $t_{\sigma\pi(1)}u_1 - \dots - t_{\sigma\pi(n)}u_n = G_n$. $p_n(Y_1, \dots, Y_n) \in \mathbb{Z}[\bar{u}, x][\bar{Y}]$ יחיד המקיים $G_n = P_n(S_1(\bar{t}), \dots, S_n(\bar{t}))$. p_n זה נקרא פולינום קרונקר (Kronecker) ה- n -י.

למרות שהוא נראה מאוד אבסטרקטי מיתן לחשב אותו. נראה דוגמא:

לכן,

$\mathbb{Z} \rightarrow F \leq K$ כאשר F שדה ראשוני נותן פירוש של p_n ו- G_n כפולינומים מעל שדה כלשהו K .

1. נגדיר:

נפרק את $g(\bar{u}, x)$ לגורמים אי פריקים מתוקנים $g_1(\bar{u}, x), \dots, g_r(\bar{u}, x)$.
 (ניתן לעשות זאת כי R תחום פריקות, ולכן $R[\bar{u}]$ תחום פריקות), שדה המניות שלו
 ולפי ההלפה של גאוס $R[\bar{u}][x] \ni g_1(\bar{u}, x), \dots, g_r(\bar{u}, x)$ ואז $g_1(\bar{u}, x), \dots, g_r(\bar{u}, x)$
 שונים זה מזה.

$$g_j(u_{w(1)}, \dots, u_{w(n)}, x) = -\psi \quad 1 \leq i \leq r \quad \psi \quad w \in S_n \quad , 1 \leq j \leq r \quad .3$$

4. לכל $1 \leq j \leq r$ $\text{Gal}(f, K)$ צמודה לתת החבורה הזאה של S_n :

הוכחה. יהיו $\alpha_1, \dots, \alpha_n \in \tilde{K}$ השורשים של שדה פיצול. אזי L/K גלואה סופית. נסמן $a_i = (-1)^i s_i(\alpha_1, \dots, \alpha_n)$. $u_1, \dots, u_n$ משתנים בלתי תלויים מעל L (ולכן גם מעל K) ולכן $K(\bar{u}) \cap L = K$ (כי אחרת יש $\alpha \in K(\bar{u}), \alpha \in L/K$ ולכן $\alpha \in K(\bar{u})$ וכן $\alpha = \frac{p(\bar{u})}{q(\bar{u})}$ ולכן $0 \neq p(\bar{u}) - \alpha \cdot q(\bar{u})$ אגף שמאל הוא פולינום מעל L במשתנים $u_1, \dots, u_n$ (תתירה).

לכן $L(\bar{u})/K(\bar{u})$ גלואה סופית והצמצום $\text{Gal}(L(u)/K(u)) \rightarrow \text{Gal}(L/K)$ הוא איזומורפיזם.
לכל $\pi \in S_n$ נסמן:

$$\pi(\tilde{}) = \alpha_{\pi(1)}u_1 + \dots + \alpha_{\pi(n)}u_n \in L[\bar{u}]$$

$$\pi = \pi' \Leftrightarrow i \text{ לכל } \pi(i) = \pi'(i) \Leftrightarrow i \text{ לכל } \alpha_{\pi(i)} = \alpha_{\pi'(i)} \Leftrightarrow \pi(\theta) = \pi'(\theta)$$

$$\begin{aligned} g(\bar{u}, x) &= p_n(-a_1, \dots, (-1)^n a_n) = p_n(S_1(\alpha_1, \dots, \alpha_n), \dots, S_n(\alpha_1, \dots, \alpha_n)) = \\ &= G_n(\alpha_1, \dots, \alpha_n) = \prod_{\pi \in S_n} (x - \alpha_{\pi(1)}u_1 - \dots - \alpha_{\pi(n)}u_n) = \prod_{\pi \in S_n} (x - \pi(\theta)) \end{aligned}$$

ולכן $\{\pi(\theta)\}_{\pi \in S_n}$ כל השורשים השונים של $g(\bar{u}, x)$ לכן $g_j(\bar{u}, x) = \prod_{\pi \in V_j} (x - \pi(\theta))$ כאשר $V_j \subseteq S_n$ כך ש- $S_n = \bigsqcup_{j=1}^r V_j$ נבחר $\rho_j \in V_j$ לכל j .
טענה. $V_j = \text{Gal}(f, K)\rho_j$.

הוכחה. יהי $\pi \in S_n$.
 $\pi(\theta) \Leftrightarrow \pi \in V_j$ שורש של $g_j = \text{irr}(\rho_j(\theta), K(\bar{u}))$ יש $\Leftrightarrow \sigma \in \text{Gal}(L(\bar{u})/K(\bar{u}))$ כך שמתקיים $\sigma(\rho(\theta)) = \pi(\theta)$ כלומר

$$\sigma(\alpha_{\rho(1)}u_1 + \dots + \alpha_{\rho_j(n)}u_n) = \alpha_{\pi(1)}u_1 + \dots + \alpha_{\pi(n)}u_n$$

$$\Leftrightarrow \sigma \text{ כך ש- } \alpha_{\pi(i)} = \sigma(\alpha_{\rho_j(i)}) \Leftrightarrow i \text{ לכל } \sigma = \alpha_{\pi\rho_j^{-1}(k)} \text{ לכל } k \Leftrightarrow \sigma \in \text{Gal}(f, K)\rho_j \Leftrightarrow \pi\rho_j^{-1} \in \text{Gal}(f, K)$$

□

□