

אלגברה ב2

© ארזים

3 במאי 2017

נדון בשאלה הבאה: האם יש פולינום $f \in \mathbb{Z}[x]$ אי פריק, שפריק מודולו כל ראשוני? התשובה היא כן.

דוגמא נגדיר $\alpha = \sqrt{2} + \sqrt{3}$. ניוכח כי α מאפס את $f(x) = x^4 - 10x^2 + 1$. נשתכנע שזהו הפולינום האי פריק של α : ברור כי

$$\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt{3}\right):\mathbb{Q}\right]=2$$

וכמובן $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, ולכן

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$$

$$\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right): \mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right): \mathbb{Q}\left(\sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}\right): \mathbb{Q}\right]=4$$

מצד שני,

$$\alpha = \sqrt{2} + \sqrt{3}$$

$$\sqrt{6}\alpha = 2\sqrt{3} + 3\sqrt{2}$$

כאשר $\alpha^2 = 5 + 2\sqrt{6}$ ולכן יש את $\sqrt{6}$ בתוך $\mathbb{Q}(\alpha)$. מתוך שתי המשוואות הבלתי תלויות הללו נקבל כי $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha)$ ולכן

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

אם כן, f אי פריק. נסתכל כעת על f מודולו ראשוני p . נשים לב שמתקיים $\mathbb{F}_p \subseteq \mathbb{F}_{p^2}$.
 $\mathbb{F}_p(\sqrt{2}), \mathbb{F}_p(\sqrt{3}) \subseteq \mathbb{F}_{p^2}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{F}_{p^2}$, ועל כן, המעלה של הפולינום האי פריק של $\sqrt{2} + \sqrt{3}$ מעל $\mathbb{F}_p$ היא לכל היותר 2. לכן $f(x)$ פריק מודולו p .

הערה 0.1 מהי $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$? אפשר להעביר את $\sqrt{2}$ לעצמו או מינוס עצמו, וכך גם את $\sqrt{3}$, והם בלתי תלויים - לכן החבורה היא למעשה $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

1 מסקנות מהמשפט היסודי של תורת גלואה

טענה 1.1 תהיינה E, L שתי הרחבות של שדה K , המוכלות בשדה משותף, כך שהרחבה L/K היא גלואה וסופית. אזי EL/E גלואה, וכן העתקת צמצום האוטומורפיזמים: $\text{res}_{EL,L} : \text{Gal}(EL/E) \rightarrow \text{Gal}(L/K)$ היא חד-חד-ערכית, ותמונתה היא $\text{Gal}(L/E \cap L)$. בפרט מתקיים

$$\text{Gal}(L^E/E) \cong \text{Gal}(L/E \cap L)$$

הוכחה: L/K סופית, ולכן נסמן $L = K[\alpha_1, \dots, \alpha_n]$. יהיו $f_i = \text{irr}(\alpha_i, K)$. נובע כי f_i פרידים ומתפצלים מעל L . לכן

$$EL = E[\alpha_1, \dots, \alpha_n]$$

נסיק כי $f_i \mid \text{irr}(\alpha_i, E)$, כלומר פריד, וכל שורשיו בתוך EL . לכן EL/E הרחבת גלואה. העתקת הצמצום מוגדרת היטב, $\sigma \mapsto \sigma|_L$. התמונה H משביתה את $E \cap L$, ולכן $H \leq \text{Gal}(L/E \cap L)$. נחשב את שדה השבת של H : נניח כי $x \in L$ מושבת על ידי H . בפרט, $x \in E$ (אם $x \notin E$ אזי $x \in EL$), ולפי תורת גלואה יהיה $\sigma \in \text{Gal}(EL/E) \setminus \text{Gal}(EL/E(x))$ שאינו משבית את x . לכן, $L^H \subseteq E \cap L$. מכאן נקבל

$$\text{Gal}(L/E \cap L) \leq H$$

וזהו הכיוון השני. נשאר להראות שהצמצום חד-חד-ערכי. נקח $\sigma \in \text{Gal}(EL/E)$, כלומר $\sigma|_E = \text{id}$. נניח כי $\sigma|_L = \text{id}$. אזי $\sigma = \text{id}|_{EL}$, ולכן הצמצום אכן חד-חד-ערכי. אם כן, סיימנו. ■

תזכורת ראינו שאם L/K סופית אזי L מוכת בהרחבה נורמלית N/K , כאשר

$$N = \prod_{\sigma \in \text{Emb}_K(L, \bar{K})} L^\sigma$$

אם L/K פרידה, אז גם L^σ/K פרידה, ולכן N/K פרידה. מכאן, N/K גלואה.

טענה 1.2 תהיינה L_1, L_2 הרחבות גלואה של שדה K המוכלות בשדה משותף. אזי $L_1 L_2$, $L_1 \cap L_2$ שתיהן גלואה מעל K .

הוכחה: נקח N גלואה מהכילה את $L_1 L_2$. יהיו

$$G = \text{Gal}(N/K), H_1 = \text{Gal}(N/L_1), H_2 = \text{Gal}(N/L_2)$$

אזי $H_1, H_2 \triangleleft G$, ואז

$$\text{Gal}(N/L_1 L_2) = H_1 \cap H_2 \triangleleft G$$

$$\text{Gal}(N/L_1 \cap L_2) = \langle H_1, H_2 \rangle \triangleleft G$$

ועל כן $L_1 L_2, L_1 \cap L_2$ גלואה מעל K . ■

הגדרה 1.3 תהיינה G_1, G_2 חבורות, ויהיו $\alpha_i : G_i \rightarrow H$ הומומורפיזמים. נגדיר את מכפלת הסיב להיות:

$$G_1 \times_H G_2 = \{(g_1, g_2) \in G_1 \times G_2 \mid \alpha_1(g_1) = \alpha_2(g_2)\}$$

למשל, כאשר $G_1, G_2 \leq G$ וניקח את השיכון, נקבל $G_1 \times_G G_2 \cong G_1 \cap G_2$. אצלנו α_1, α_2 תמיד יהיו על. כעת, יש העתקות הטלה:

$$pr_i : G_1 \times_H G_2 \rightarrow G_i$$

נסכם בדיאגרמה קומוטטיבית:

$$\begin{array}{ccc} G_1 \times_H G_2 & \xrightarrow{pr_2} & G_2 \\ pr_1 \downarrow & & \downarrow \alpha_2 \\ G_1 & \xrightarrow{\alpha_1} & H \end{array}$$

הערה 1.4 אם α_1, α_2 על, G_1, G_2 סופיות, אזי

$$|G_1 \times_H G_2| = \sum_{\alpha(g_1)=\alpha(g_2)} 1 = \sum_{h \in H} \sum_{\alpha(g_1)=\alpha(g_2)=h} 1 = \sum_{h \in H} \frac{|G_1|}{|H|} \frac{|G_2|}{|H|} = \frac{|G_1| |G_2|}{|H|}$$

למה 1.5 (מכפלת הסיב מקיימת תכונה אוניברסלית) תהיינה G_1, G_2, H כמו בהגדרה. נניח שיש חבורה G ושני הומומורפיזמים $\pi_i : G \rightarrow G_i$ כך שמתקיים

$$\alpha_1 \circ \pi_1 = \alpha_2 \circ \pi_2$$

אזי יש הומומורפיזם יחיד $\pi : G \rightarrow G_1 \times_H G_2$ המקיים

$$\pi_2 = pr_2 \circ \pi$$

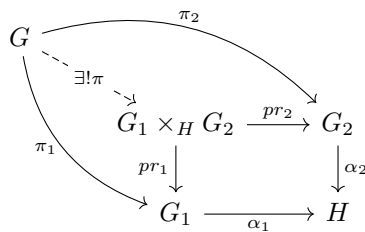
$$\pi_1 = pr_1 \circ \pi$$

הוכחה: מגדירים

$$\pi(g) = (\pi_1(g), \pi_2(g))$$

■

ואפשר בקלות להיווכח שהדיאגרמה הבאה קומוטטיבית:



טענה 1.6 תהיינה L_1, L_2 הרחבות גלואה של K . אזי העתקות הצמצום $r_i : \text{Gal}(L_1 L_2 / K) \rightarrow \text{Gal}(L_i / K)$ משורות איזומורפיזם

$$r : \text{Gal}(L_1 L_2 / K) \rightarrow \text{Gal}(L_1 / K) \times_{\text{Gal}(L_1 \cap L_2 / K)} \text{Gal}(L_2 / K)$$

כאשר כאן מכפלת הסיב היא לפי הצמצומים.

הוכחה: נסמן $G_i = \text{Gal}(L_i / K)$, $H = \text{Gal}(L_1 \cap L_2 / K)$, $\alpha_i : G_i \rightarrow H$ העתקת הצמצום, $G = \text{Gal}(L_1 L_2 / K)$ וכן $\pi_i : G \rightarrow G_i$ העתקת הצמצום. ההעתקות מקיימות את תנאי הלמה הקודמת, כי הן העתקות צמצום - ברור שלצמצם כך או כך לא משנה. לכן יש הומומורפיזם יחיד $\pi : G \rightarrow G_1 \times_H G_2$ שמביא אותנו למצב של הדיאגרמה האחרונה. כדי להראות שהוא איזומורפיזם, מספיק להראות שהוא חד-חד-ערכי ולהראות שוויון גדלים, כלומר

$$|G| = \frac{|G_1| |G_2|}{|H|}$$

חד-חד-ערכיות: נקח $\sigma \in G$, ונניח כי $\pi(\sigma) = 1$. אזי

$$\sigma|_{L_i} = pr_i \circ \pi(\sigma) = pr_i(1) = 1$$

לכן נובע כי $\sigma|_{L_1 L_2} = 1$, כלומר $\sigma = 1$. לכן π אכן חד-חד-ערכי. כעת נעבור לחישוב הגדלים. מתקיים

$$|G| = [L_1 L_2 : K] = [L_1 L_2 : L_1] [L_1 : L_1 \cap L_2] [L_1 \cap L_2 : K]$$

ראינו כי $\text{Gal}(L_1 L_2 / L_1) \cong \text{Gal}(L_2 / L_1 \cap L_2)$ ולכן

$$\begin{aligned}
 |G| &= [L_2 : L_1 \cap L_2] [L_1 : L_1 \cap L_2] [L_1 \cap L_2 : K] = \\
 &= \frac{[L_1 : K]}{[L_1 \cap L_2 : K]} \frac{[L_2 : K]}{[L_1 \cap L_2 : K]} [L_1 \cap L_2 : K] = \\
 &= \frac{|G_1| |G_2|}{|H|}
 \end{aligned}$$

■

וסיימנו.

מסקנה 1.7 אם L_1, L_2 גלואה מעל K , $L_1 \cap L_2 = K$, אזי

$$\text{Gal}(L_1 L_2 / K) = \text{Gal}(L_1 / K) \times \text{Gal}(L_2 / K)$$

הוכחה: במקרה זה מתקיים $\text{Gal}(L_1 \cap L_2 / K) = 1$, וזה מספיק כי מקבלים

$$G_1 \times_H G_2 = G_1 \times G_2$$

■

דוגמא כמו קודם,

$$\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

2 שדות סופיים

משפט 2.1 מתקיים

$$\text{Gal}(\mathbb{F}_{q^n} / \mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$$

עם יוצר $\text{Frob}_q : x \mapsto x^q$.

הוכחה: נסמן

$$\text{Gal}(\mathbb{F}_{q^n} / \mathbb{F}_q) \geq H = \langle \text{Frob}_q \rangle$$

נחשב את שדה השבת:

$$\mathbb{F}_{q^n}^H = \{x \in \mathbb{F}_{q^n} \mid x^q = x\} = \mathbb{F}_q$$

■

ולכן קיבלנו $H = \text{Gal}(\mathbb{F}_{q^n} / \mathbb{F}_q)$.

3 חבורת גלואה של פולינום

אם N/K הרחבת גלואה אזי $\text{Gal}(N/K)$ היא חבורה סופית (לא יותר).
יהי $f \in K[x]$ פולינום פריד ממעלה חיובית. נסמן בתור N את שדה הפיצול של f . אזי N/K גלואה. עכשיו, $\text{Gal}(N/K)$ פועלת על שורשי f - כי אם $f(\alpha) = 0$ אז גם $f(\sigma(\alpha)) = 0$ לכל $\sigma \in \text{Gal}(N/K)$.
לכן, יש לנו הומומורפיזם

$$f : \text{Gal}(N/K) \rightarrow \text{Sym}(\text{Roots}(f))$$

הגדרה 3.1 מסמנים

$$\text{Gal}(f/K) = \text{Gal}(N/K)$$

והחבורה הזו באה עם שיכון

$$\rho : \text{Gal}(f/K) \rightarrow \text{Sym}(\text{Roots}(f))$$