

אלגברה ב2

© ארזים

13 ביוני 2017

טענה 0.1 יהי $K \subseteq L \subseteq N$ מגדל של הרחבות גלואה סופיות של K . נסמן

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

$$\overline{G} = \text{Gal}(L/K)$$

$$H = \text{Gal}(N/L)$$

אזי $G \cong H \rtimes \overline{G}$ (כלומר קיימת $\overline{G} \cong \hat{G} \leq G$ עם $G = H \rtimes \hat{G}$ כמכפלה פנימית) אם ורק אם קיים $K \subseteq E \subseteq N$ שמקיים $E \cap L = K, EL = N$.

הוכחה: נניח כי $G \cong H \rtimes \overline{G}$ וניקח את $\hat{G}$ כפי שתיארנו. נגדיר $E = N^{\hat{G}}$. מהאמת גלואה,

$$E \cap L = K \iff \langle \hat{G}, H \rangle = G$$

$$EL = N \iff \hat{G} \cap H = 1$$

ושני התנאים בימין מתקיימים בגלל ההנחת של המכפלה החצי ישרה. בכיוון השני, ניקח E כזה ונגדיר $\hat{G} = \text{Gal}(N/E)$. אזי משתי השורות שכתבנו למעלה מתקיים $\hat{G}H = G$ (כי הרי $\hat{G}$ נורמית כחבורת גלואה של תת הרחבת גלואה) וכן $\hat{G} \cap H = 1$. לכן $G = H \rtimes \hat{G}$. בנוסף, נתבונן בהעתקת הצמצום $\text{res} : G \twoheadrightarrow \overline{G}$, שגרעינה H . כעת,

$$\text{res}(\hat{G}) \cong \hat{G}H/H = G/H \cong \overline{G}$$

כעת $\hat{G} \cap H = 1$ כי ראינו כבר, ולכן $\text{res}|_{\hat{G}}$ היא חד-חד-ערכית ועל $\overline{G}$, ולכן $\hat{G} \cong \overline{G}$. ■

1 הרחבות אי-פרידות טהורות (Purely Inseparable)

תזכורת הרחבה סופית L/K נקראת פרידה אם $[L : K]_s = [L : K]$. אם $[L : K]_s < [L : K]$ נאמר כי L/K אי-פרידה. $\dim_K L$.

הגדרה 1.1 אם $[L : K]_s = 1$ נאמר כי L/K היא אי-פרידה טהורה.

הערה 1.2 הרחבה L/K פרידה וגם אי-פרידה טהורה בהכרח מקיימת $L = K$.

טענה 1.3 תהי L/K הרחבה סופית.

1. אם $\text{char} K = 0$ אזי L/K פרידה.

2. אם $p = \text{char} K > 0$ אז קיים $\mu \geq 0$ המקיים $[L : K]_s = p^\mu$, ויתר על כן, ההרחבה L^{p^μ}/K פרידה, באשר $L^{p^\mu} = \{x^{p^\mu} \mid x \in L\}$ (וזה שדה).

הוכחה:

1. ראינו בעבר - אפשר להניח בלי הגבלת הכלליות כי $L = K(\alpha)$, ואז לוקחים $f = \text{irr}(\alpha, K)$, מתקיים $f' \neq 0$ ולכן $\gcd(f, f') = 1$, כלומר f פריד.

2. נזכר שההתעקה $\varphi(x) = x^p$ היא הומומורפיזם ותמונתו L^p . נתבונן במגדל

$$K \subseteq KL^{p^\mu} \subseteq \dots \subseteq KL^{p^2} \subseteq KL^p \subseteq L$$

ראשית, נראה כי $[L : KL^p] = p^r$ עבור r כלשהו - אכן, אם $L = K(\alpha_1, \dots, \alpha_n)$ אזי $\beta_i = \alpha_i^p \in KL^p$ ולכן הפולינום המינימלי של α_i מעל KL^p מחלק את

$$f_i = x_i^p - \beta_i$$

השורשים שלו בתוך L הם בדיוק α_i , כי $x_i^p - \beta_i = x_i^p - \alpha_i^p = (x_i - \alpha_i)^p$. לכן הפולינום הזה פריק או מתפצל. לכן בכל צעד שבו מוסיפים את α_i או שהמעלה תהיה 1 או שהיא תהיה p (חייבת לחלק את דרגת f_i). באופן דומה מראים שגם $[KL^{p^i} : KL^{p^{i+1}}]$ הוא חזקת p , ואז נקבל שלכל μ שנבחר, $[L : KL^{p^\mu}]$ היא חזקת p . שנית, אם $\alpha \in L$, $f = \text{irr}(\alpha, K)$, ואם $v \geq 0$ מקסימלי עם $f(x) = g(x^{p^v})$ עבור $g \in K[x]$ כלשהו, אזי $g(x)$ אי פריק, ולכן $g = \text{irr}(\alpha^{p^v}, K)$, וכמו כן $g' \neq 0$. אכן, אם

$$g(x) = h(x) \cdot \tilde{h}(x)$$

אזי

$$f(x) = h(x^{p^v}) \tilde{h}(x^{p^v})$$

ואז $h(x^{p^v})$ קבוע או $\tilde{h}(x^{p^v})$ קבוע, ולכן h או $\tilde{h}$ קבוע. כמו כן, אם נרשום

$$g(x) = \sum_{i=0}^r a_i x^i$$

אם $g' = 0$ אזי $ia_i = 0$ לכל i . לכל i מתקיים $a_i = 0$. לכן,

$$g(x) = \sum_{j=0}^{\frac{r}{p}} a_{pj} (x^p)^j = h(x^p)$$

ולכן $f(x) = h(x^{p^{v+1}})$ בסתירה למקסימליות. לסיכום, קיבלנו שלכל $\alpha \in L$ יש איזשהו $v \leq \deg_{\text{irr}}(\alpha, K) \leq [L : K]$ כך שהפולינום האי פריק של α^{p^v} הוא בעל נגזרת שאינה אפס, ולכן α^{p^v} פריד. אז יש פירוק

$$K \subseteq E = KL^{p^{[L:K]}} \subseteq L$$

כך שמתקיים $[L : E] = p^r$. כל האיברים בתוך E פרידים מעל K ולכן E/K פריד ולכן $[E : K] = [E : K]_s$. נקבל שמתקיים

$$[L : K] = [L : E] [E : K] = p^r [E : K]_s$$

כעת

$$[E : K]_s = \frac{[L : K]_s}{[L : E]_s}$$

ולכן

$$[L : K] = p^{r'} [L : K]_s$$

■