אלגברה ב2

ארזים ©

13 ביוני 2017

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

$$G = \mathrm{Gal}\left(N/K\right)$$
$$\overline{G} = \mathrm{Gal}\left(L/K\right)$$
$$H = \mathrm{Gal}\left(N/L\right)$$

אזי $G \cong H \rtimes \overline{G}$ (כלומר קיימת $G \geq \hat{G} \cong \overline{G}$ 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 $E = N^{\hat{G}}$. מהאתמת גלואה,

$$E \cap L = K \iff \left\langle \hat{G}, H \right\rangle = G$$
$$EL = N \iff \hat{G} \cap H = 1$$

ושני התנאים בימין מתקיימים בגלל ההנחת של המכפלה החצי ישרה.

בכיוון השני, ניקח E כזה ונגדיר $\hat{G} = \mathrm{Gal}\left(N/E\right)$. 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 $\mathrm{res} : G \twoheadrightarrow \overline{G}$, שגרעינה H. כעת,

$$\mathrm{res}\left(\hat{G}\right) \cong \hat{G}H/H = G/H \cong \overline{G}$$

כעת $\hat{G} \cap H = 1$ כי ראינו כבר, ולכן $\mathrm{res}\mid_{\hat{G}}$ היא חד־חד־ערכית ועל $\overline{G}$, ולכן $\hat{G} \cong \overline{G}$, וסיימנו. ■

1 הרחבות אי־פרידות טהורות (Purely Inseparable)

תזכורת הרחבה סופית L/K נקראת פרידה אם $\left|\mathrm{Emb}_K\left(L, \overline{K}\right)\right| = [L:K]_s = [L:K] = \dim_K L$. אם $[L:K]_s < [L:K]$ נאמר כי L/K אי־פרידה.

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

הוכחה:

1. ראינו בעבר ־ אפשר להניח בלי הגבלת הכלליות כי $L=K(\alpha)$, ואז לוקחים $f=\mathrm{irr}(\alpha,K)$, 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

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

ראשית, נראה כי $[L:KL^p]=p^r$ עבור r כלשהו ־ אכן, אם $L=K(\alpha_1,\ldots,\alpha_n)$ 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 $(x-\alpha_i)^p=x^p-\alpha_i^p=x^p-\beta_i$. 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). באפן דומה מראים שגם $\left[KL^{p^i}:KL^{p^{i+1}}\right]$ הוא חזקת p, ואז נקבל שלכל μ שנבחר, $\left[L:KL^{p^{\mu}}\right]$ היא חזקת p. שנית, אם $\alpha\in L$, $f=\mathrm{irr}(\alpha,K)$, ואם $v\geq 0$ מקסימלי עם $f(x)=g\left(x^{p^v}\right)$ עבור $g\in K[x]$ כלשהו, אזי $g(x)$ אי פריק, ולכן $g=\mathrm{irr}\left(\alpha^{p^v},K\right)$, וכמו כן $g'\neq 0$. אכן, אם

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

אזי

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

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

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

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

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

ולכן $f(x) = h\left(x^{p^{v+1}}\right)$ בסתירה למקסימליות. לסיכום, קיבלנו שלכל $\alpha \in L$ יש איזשהו $v \leq \operatorname{degirr}(\alpha, K) \leq [L:K]$ 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

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

■