אלגברה ב2

ארזים ©

25 באפריל 2017

תרגיל f פריד אם ורק אם $\gcd\left(f,f'\right)=1$.

טענה 0.1 (הקשר בין פולינומים לשדות) תהי L/K הרחבה סופית.

1. $\alpha\in L$ פריד מעל K אם ורק אם $\operatorname{irr}\left(\alpha,K\right)$ פריד (ההגדרה של איבר פריד היא שההרחבה $K(\alpha)/K$ פרידה).
2. L/K פרידה אם ורק אם כל $\alpha\in L$ הוא פריד מעל K.
3. L/K נורמלית אם ורק אם לכל $\alpha\in L$, הפולינום $\operatorname{irr}\left(\alpha,K\right)$ מתפצל מעליה.
4. אם L/K שדה פיצול של פולינום $f\in K\left[x\right]$ אזי L/K נורמלי.
5. אם L/K שדה פיצול של פולינום פריד אזי L/K גלואה.

הוכחה: הקדמה:
אם $\sigma\in\operatorname{Emb}_K\left(L,\overline{K}\right)$, ואם $f=\operatorname{irr}\left(\alpha,K\right)$ אזי נפעיל את σ על השוויון $f\left(\alpha\right)=0$:

$$\sigma\left(f\left(\alpha\right)\right)=0$$
$$f\left(\sigma\left(\alpha\right)\right)=0$$

לכן $\sigma\left(\alpha\right)$ שורש של f. אם $\beta\in\overline{K}$ הוא שורש של f, אזי ההעתקה $\sigma:K\left[\alpha\right]\to K\left[\beta\right]$ המוגדרת על ידי

$$\sigma\left(\sum_{i=1}^{n}a_i\alpha^i\right)=\sum_{i=1}^{n}\beta^i$$

היא הומומורפיזם של חוגים. זה משרה התאמה חד־חד־ערכית ועל

$$\operatorname{Emb}_K\left(K\left(\alpha\right),\overline{K}\right)\leftrightarrow\left\{\beta\mid f\left(\beta\right)=0\right\}$$

בפרט:

$$\left[K\left(\alpha\right):K\right]_S=\left|\left\{\beta\in\overline{K}\mid f\left(\beta\right)=0\right\}\right|$$

כעת נוכיח את הטענה.

1. $\alpha \in L$ אי פריד אם ורק אם

$$[K(\alpha):K]_s = [L:K]$$

כלומר, אם ורק אם

$$|\{\beta \mid \operatorname{irr}(\alpha,K)(\beta)=0\}| = \deg(\operatorname{irr}(\alpha,K))$$

כלומר אם ורק אם אין לפולינום $\operatorname{irr}(\alpha,K)$ שורשים כפולים, שזו הגדרת פרידות.

2. אם L/K פריד, ראינו כי כל הרחבת ביניים גם פרידה, ובפרט $K(\alpha)/K$ פריד לכל $\alpha \in L$. בכיוון השני, נניח כי כל $\alpha \in L$ פריד מעל K. L/K סופית, ולכן קיימים $\alpha_1,\ldots,\alpha_n$ עבורם:

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1,\alpha_2) \subseteq \cdots \subseteq K(\alpha_1,\ldots\alpha_n)$$

α_i פריד מעל K, ולכן פריד מעל $K(\alpha_1,\ldots,\alpha_{i-1})$ (ראינו). לכן, כל הרחבה עוקבת במגדל היא פרידה, ואז, לפי למה משעור קודם, נקבל כי L/K פרידה.

3. נניח כי L/K נורמלית. נקח $\alpha \in L$ ונראה כי כל השורשים של $f=\operatorname{irr}(\alpha,K)$ נמצאים בתוך L. יהי $\beta \in \overline{K}$ המקיים $f(\beta)=0$. יש $\sigma : K(\alpha) \to \overline{K}$ המקיים

$$\sigma(\alpha)=\beta$$

נרחיב אותו באופן כלשהו להעתקה

$$\sigma : L \to K$$

כיוון שההרחבה נורמלית נקבל $\sigma(L)=L$, ולכן $\beta \in \sigma(L)=L$ וסיימנו.
בכיוון השני, נניח כי L/K אינו נורמלי, כלומר יש $\sigma : L \to \overline{K}$ מהקיים $\sigma(L) \nsubseteq L$.
נקח $\beta \in \sigma(L)\setminus L$ ונסמן

$$\alpha = \sigma^{-1}(\beta) \in L$$

ואז $\operatorname{irr}(\alpha,K)$ אינו מתפצל, כי $\beta=\sigma(\alpha)$ הוא שורש שלו (לפי ההקדמה בתחילת ההוכחה).

4. נניח כי L/K שדה פיצול של פולינום $f \in K[x]$, כלומר

$$f = \prod_{I=1}^{n}(x-\alpha_i)$$
$$\alpha \in L$$
$$L = K(\alpha_1,\ldots,\alpha_n)$$

יהי $\sigma : L \to \overline{K}$ עם $\sigma \mid_K = \mathrm{id}$. אזי

$$\sigma\left(L\right)=\sigma\left(K\left(\alpha_1,\ldots,\alpha_n\right)\right)=K\left(\sigma\left(\alpha_1\right),\ldots\sigma\left(\alpha_n\right)\right)\subseteq L$$

כי $\sigma\left(\alpha_i\right)$ שורשים של f (שוב מההקדמה). לכן ${}^{L}/_{K}$ אכן נורמלית.

5. נניח כעת כי ${}^{L}/_{K}$ שדה פיצול של $f \in K\left[x\right]$ פריד. מצד אחד, ${}^{L}/_{K}$ נורמלית לפי 4. מצד שני, ${}^{L}/_{K}$ פריד, כי נוצר על ידי איברים פרידים. לכן ${}^{L}/_{K}$ גלואה.

■

דוגמאות $\mathbb{Q}\left(\sqrt{2}\right)$ גלואה. $\mathbb{Q}\left(\sqrt[3]{2}\right)$ לא גלואה. בנוסף, ${}^{\mathbb{F}_p\left(\sqrt[p]{u}\right)}/_{\mathbb{F}_p\left(u\right)}$ לא פרידה: נסמן $K=\mathbb{F}_p\left(u\right)$, שדה הפונקציות הרציונאלית במשתנה u מעל $\mathbb{F}_p$. אזי $\sqrt[p]{u}\notin\mathbb{F}_p\left(u\right)$, וכן

$$\mathrm{irr}\left(\sqrt[p]{u},K\right)=x^p-u$$

ברור שפולינום זה מתאפס על $\sqrt[p]{u}$, והוא אי פריק מאיזנשטיין (תרגיל). נשים לב כי

$$x^p-u=\left(x-\sqrt[p]{u}\right)^p$$

לכן $\mathbb{F}_p\left[\sqrt[p]{u}\right]$ לא פריד מעל $\mathbb{F}_p\left(u\right)$ (יש שורש יחיד בסגור האלגברי, כלומר שיכון יחיד, אבל מעלת ההרחבה היא $p\geq 2$). נעיר כי

$$\left(x^p-u\right)'=px^{p-1}=0$$
$$\gcd\left(x^p-u,0\right)=x^p-u\neq 1$$