

אלגברה ב2

© ארזים

7 ביוני 2017

1 הרחבות נעלות

נחזור על נקודה מהשיעור שעבר. תהי G חבורה סופית, L שדה שעליו G פועלת נאמנה (אז היה לנו $G = S_n$, $L = K(x_1, \dots, x_n)$, $\sigma(x_i) = x_{\sigma(i)}$, $\sigma|_K = \text{id}$). מהלמה של ארטין נקבל $[L : L^G] \leq |G|$. מהצד השני נקבל

$$|G| \leq |\text{Aut}(L/L^G)| \leq [L : L^G]$$

ולכן נקבל $\text{Aut}(L/L^G) = G$ וגם $|\text{Aut}(L/L^G)| = [L : L^G]$ בפרט, זו הרחבת גלואה. בעזרת כל זה, ראינו שאם $x_1, \dots, x_n$ בלתי תלויים אלגברית מעל K (משתנים), אז גם הפונקציות הסימטריות הבסיסיות

$$\begin{aligned} s_1 &= \sum x_i \\ s_2 &= \sum x_i x_j \\ &\vdots \\ s_n &= x_1 \cdots x_n \end{aligned}$$

הם בלתי תלויים אלגברית. כמו כן

$$K(x_1, \dots, x_n)^{S_n} = K(s_1, \dots, s_n)$$

הסקנו מכאן שלפולינום הגנרי $x^n - s_1 x^{n-1} + \dots + (-1)^n s_n$ יש חבורת גלואה S_n .

הגדרה 1.1 פולינום במשתנים $x_1, \dots, x_n$ ייקרא סימטרי אם לכל $\sigma \in S_n$ מתקיים

$$f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

מסקנה 1.2 כל פולינום סימטרי במשתנים $x_1, \dots, x_n$ הוא ניתן לכתיבה בעזרת $s_1, \dots, s_n$.

דוגמא

$$x_1^2 + x_2^2 = s_1^2 - 2s_2$$

2 מפורדות לינאריות של שדות

הגדרה 2.1 יהיו $K \subseteq L, E \subseteq \Omega$ שדות. נאמר כי L מפורד לינארית מהשדה E מעל K אם לכל $l_1, \dots, l_m \in L$ בלתי תלויים לינארית מעל K הם גם בלתי תלויים מעל E .

טענה 2.2 אם L מופרד לינארית מהשדה E מעל K , אז גם E מופרד לינארית מהשדה L מעל K .

הוכחה: יהיו $e_1, \dots, e_m \in E$ בלתי תלויים לינארית מעל K . נוכיח שהם בלתי תלויים לינארית מעל L . נניח כי

$$\sum_i l_i e_i = 0$$

כאשר $l_i \in L$. נבחר בסיס של $\text{span}\{l_1, \dots, l_m\}$, נאמר $y_1, \dots, y_r$. אז נוכל לקחת $c_{ij} \in K$ עם

$$l_i = \sum_j c_{ij} y_j$$

נציב בחזרה ונקבל

$$0 = \sum_i l_i e_i = \sum_i e_i \sum_j c_{ij} y_j = \sum_j y_j \sum_i e_i c_{ij}$$

לקחנו את $y_1, \dots, y_r$ בלתי תלויים לינארית מעל K , והנחנו כי L מופרד לינארית מהשדה E מעל K - לכן y_j בלתי תלויים לינארית גם מעל E . ברור שמתקיים $\sum_i e_i c_{ij} \in E$, ולכן נובע שלכל j מתקיים

$$\sum_i e_i c_{ij} = 0$$

לקחנו את $e_1, \dots, e_m$ בלתי תלויים לינארית מעל K , ולכן נובע כעת $c_{ij} = 0$ לכל i, j .
■

הרווחנו את הזכות לכתוב מעתה: L, E מופרדים לינארית מעל K .

דוגמה ניקח $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. כדי להראות שאלה מופרדים לינארית, די להראות כי $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$. זה כמובן אכן קורה.

טענה 2.3 אם L/K סופית וכן E/K כלשהו, אזי E, L מופרדים לינארית מעל K אם ורק אם

$$[L : K] = [LE : E]$$

הוכחה: ראשית נניח כי L, E מופרדים לינארית. נקח בסיס של L/K , נניח $x_1, \dots, x_m$. אז הם פורשים את LE מעל E והם בלתי תלויים לינארית מההנחה, ולכן הם בסיס - כנדרש. בכיוון השני, נקח $x_1, \dots, x_r \in L$ בלתי תלויים מעל K . נשלים אותם לבסיס $x_1, \dots, x_m$. עכשיו כמו קודם, הם פורשים את EL מעל E , ומההנחה על המימדים הם בסיס, ובפרט בלתי תלויים. ■

דוגמא ניקח $\mathbb{Q}(\sqrt[4]{3}), \mathbb{Q}(e^{\frac{2\pi i}{3}}) \subseteq \mathbb{Q}$. נשים לב שמתקיים $\mathbb{Q}(e^{\frac{2\pi i}{3}}) = \mathbb{Q}\left(\frac{1}{2} + \frac{\sqrt{-3}}{2}\right) = \mathbb{Q}(\sqrt{-3})$. $\mathbb{Q}(\sqrt{-3})$ בלתי תלויים מעל $\mathbb{Q}$, אבל לא מעל $\mathbb{Q}(\sqrt[4]{3})$.

טענה 2.4 L, E מופרדים לינארית מעל K אזי $L \cap E = K$.

הוכחה: נניח כי $L \cap E \neq K$. נקח $x \in L \cap E \setminus K$ ואז $x \in L$ ו- $1, x$ בלתי תלויים לינארית מעל K . אבל $1 \cdot x - x = 0$, וכן $x \in E$, אז הם תלויים מעל E . ■

דוגמא שמראה שהכיוון ההפוך לא נכון. $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}e^{\frac{2\pi i}{3}})$ הם שדות שהחיתוך שלהם הוא $\mathbb{Q}$, אבל הצירוף שלהם הוא ממעלה 2 מעל כל אחד מהם. בפרט

$$\left[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\right] = 3 \neq 2 = \left[\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2}e^{\frac{2\pi i}{3}})\right]$$

ולכן הם בהכרח לא מופרדים לינארית, למרות שהחיתוך שלהם הוא $\mathbb{Q}$.

משפט 2.5 (למת המגדל) בהנתן התרשים הבא של שדות:

$$\begin{array}{ccccc} E & \text{---} & EL & \text{---} & EM \\ | & & | & & | \\ K & \text{---} & L & \text{---} & M \end{array}$$

אזי M, E מופרדים לינארית מעל K אם ורק אם L, E מופרדים לינארית מעל K וגם M, EL מופרדים לינארית מעל L .

הוכחה: ראשית, כמה הכנות.

אם יש חוג $R \subseteq L$ כך שאיברי L הם מנות של איברים מתוך R , אז כדי להוכיח שהשדות L, E מופרדים לינארית מעל K , מספיק לקחת איברים מתוך R (כלומר אם כל $x_1, \dots, x_m \in R$ בלתי תלויים לינארית מעל K הם בלתי תלויים מעל E , אז L, E מופרדים לינארית). נראה זאת. נקח $y_1, \dots, y_m \in L$ בלתי תלויים לינארית מעל K . לפי ההנחה $\sum e_i x_i \left(\prod_{j \neq i} z_j\right) = 0$ מתקיים גם $\sum e_i y_i = 0$ אם $x_i, z_i \in R$. עבור $y = \frac{x_i}{z_i}$ עבור $x_i, z_i \in R$ אז $e_j = 0$ כולם, וסיימנו.

נחזור להוכחה. נניח כי L, E מופרדים לינארית מעל K וגם M, EL מופרדים לינארית מעל L . אם $x_1, \dots, x_m \in E$ בלתי תלויים לינארית מעל K , לפי ההנחה הם בלתי תלויים לינארית גם מעל L (ושאיכס כמובן אל EL). לפי ההנחה, EL, M מופרדים לינארית מעל K , ולכן $x_1, \dots, x_m$ בלתי תלויים לינארית מעל M כנדרש. בכיוון השני, נניח כי M, E מופרדות לינארית מעל K . ברור כי L, E מופרדים לינארית מעל K . כמו כן, EL הוא מנות של סכומים של מכפלות של איברים מתוך E, L , משמע

$$EL = \left\{ \sum e_i l_i \mid e_i, e_j \in E, l_i, l_j \in L \right\}$$

ניקח $y_1, \dots, y_m \in M$ בלתי תלויים לינארית מעל L , ונרצה להוכיח שהם בלתי תלויים מעל EL . אם יש צירוף לינארי לא טריוויאלי $\sum \frac{u_i}{v_i} y_i = 0$ כאשר

$$u_i, v_i \in \left\{ \sum e_k l_k \right\}$$

אז על ידי כפל במכנה משותף נקבל צירוף לינארי לא טריוויאלי

$$\sum u_i y_i = 0$$

כאשר $u_i \in \left\{ \sum e_k l_k \right\}$ נרשום

$$u_i = \sum_{j=1}^n l_{ij} e_j$$

עם $e_1, \dots, e_n \in E$ בלתי תלויים לינארית וכן $l_{ij} \in L$ אזי

$$0 = \sum_i u_i y_i = \sum_i \sum_j l_{ij} e_j y_i = \sum_j e_j \left(\sum_i l_{ij} y_i \right)$$

מכאן נקבל מהנחת המופרדות הלינאריות $\sum_j l_{ij} y_i = 0$ אבל $L \subseteq M$ ולקחנו $y_1, \dots, y_m$ בלתי תלויים, ולכן $l_{ij} = 0$ מכאן נקבל $u_i = 0$ ונסיים. ■

טענה 2.6 אם L/K גלואה וסופית אזי $L \cap E = K$ אם ורק אם L, E מופרדים לינארית.

הוכחה: ראינו בעבר כי במצב זה

$$\text{res} : \text{Gal}(L^E/E) \rightarrow \text{Gal}(L/L \cap E)$$

היא איזומורפיזם. לכן $[L : L \cap E] = [LE : E]$, ובפרט $[L : K] = [LE : E]$ אם ורק אם $E \cap L = K$ כנדרש. ■

טענה 2.7 יהי $f(x) = x^p - 2$ באשר p ראשוני, N שדה הפיצול של f . אזי $\text{Gal}(N/\mathbb{Q}) \cong C_p \rtimes C_{p-1}$.

תזכורת אם G חבורה, $H, M \leq G$ עם:

$$1. M \triangleleft G$$

$$2. H \cap M = 1$$

$$3. HM = G$$

אזי נאמר כי $G = M \rtimes H$. במצב זה H פועלת על M על ידי

$$(h, m) \mapsto h m h^{-1} \in M$$

דרך אחרת לראו תאית זה (חיצונית במקום פנימית) - ניקח H, M סתם חבורות, כאשר H פועלת על M . ניתן לבנות G כך שיתקיים $G = M \rtimes H$ והפעולה המושרתת תהיה הפעולה הנתונה. עושים את זה באופן הבא: נסמן את הפעולה על ידי $(h, m) \mapsto h \cdot m$ נגדיר את איברי G להיות איברי המכפלה הקרטזית $M \times H$, והכפל יתבצע על ידי

$$(m_1, h_1) (m_2, h_2) = (m_1 (h_1 \cdot m_2), h_1 h_2)$$

הוכחה: (של הטענה) ברור שבשדה הפיצול יש את $\sqrt[p]{2}$ וכן את המכפלה שלו בכל שורש יחידה מסדר p . לכן כל שורשי היחידה מסדר p נמצאים בתוך N . לכן $\mathbb{Q}(\sqrt[p]{2}), \mathbb{Q}(\mu_p) \subseteq N$. יש לנו

$$1 \mapsto M \mapsto G \mapsto \overline{G} \mapsto 1$$

ולכן

$$\text{Gal}(N/\mathbb{Q}(\mu_p)) = M = \ker(G \rightarrow \overline{G})$$

מאיזנסטיין נקבל f אי פריק מעל $\mathbb{Q}$. כמו כן, שני השדות $\mathbb{Q}(\sqrt[p]{2}), \mathbb{Q}(\mu_p)$ נחתכים רק בתוך $\mathbb{Q}$, כי המעלה מתחלקת במספרים $p, p-1$. כיוון שההרחבה $[\mathbb{Q}(\mu_p) : \mathbb{Q}]$ גלואה, הם מופרדים לינארית, ולכן $[N : \mathbb{Q}(\mu_p)] = p$ אבל $N = \mathbb{Q}(\mu_p, \sqrt[p]{2})$, ולכן לפי קומר נקבל כי

$$M = \text{Gal}(N/\mathbb{Q}(\mu_p)) \cong C_p$$

יתר על כן, $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) = C_{p-1}$ בגלל החיתוך. אפשר לראות ממש שהתכונות של מכפלה חצי ישרה מתקיימות. ■