אלגברה ב2

ארזים ©

16 במאי 2017

1 משפט הבסיס הנורמלי

אנחנו בדרך להוכיח את משפט הבסיס הנורמלי. ניזכר בניסוח.

משפט 1.1 אם N/K גלואה סופית עם $G = \operatorname{Gal}(N/K)$, אזי יש $\alpha \in N$ עבורו $\{\sigma(\alpha) \mid \sigma \in G\}$ בסיס.

התחלנו להוכיח בשביל זה למות. הראשונה הייתה הבאה.

למה 1.2 אם $0 \neq f \in K[x_1, \ldots, x_m]$ וגם $|K| = \infty$, אזי יש $a_1, \ldots, a_m$ עם $f(a_1, \ldots, a_m) \neq 0$.

כעת נמשיך.

למה 1.3 אם L/K פרידה, $\alpha_1, \ldots, \alpha_m$ בסיס של L/K, $\sigma_1, \ldots, \sigma_m$ כל שיכוני K לתוך סגור אלגברי $\overline{K}$, אזי המטריצה

$$A = (\sigma_j(\alpha_i))_{i,j=1}^{m} \in M_{m\times m}(\overline{K})$$

הפיכה.

הוכחה: נניח שיש $c_1, \ldots, c_m \in \overline{K}$ כך שמתקיים

$$A \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} = 0$$

נקבל שלכל i מתקיים

$$\sum_{j=1}^{m} \sigma_j(\alpha_i) c_j = 0$$

כלומר

$$\left(\sum_{j=1}^{m} c_j \sigma_j\right)(\alpha_i) = 0$$

על כן הפונקציה הפונקציה

$$\sum_{j=1}^{m} c_j \sigma_j$$

היא פונקציית האפס, וממשפט אי התלות של קרקטרים, נובע כי $c_j = 0$ לכל j. לכן A הפיכה. ■

למה 1.4 (מאלגברה לינארית) יהי V מרחב ווקטורי ממימד סופי מעל K, $T : V \to V$ העתקה לינארית כך שמתקיים $f_T = m_T$, כלומר הפולינום האופייני שווה לפולינום המינימלי.
אזי יש בסיס של V מהצורה

$$\left\{v, Tv, T^2 v, \ldots, T^{n-1} v\right\}$$

הוכחה: ניתן רעיון להוכחה. נרשום

$$f_T = m_T = p_1^{a_1} \cdots p_r^{a_r}$$

כאשר p_i אי פריקים שונים מעל $K[x]$. בשלב ראשון, מבצעים רדוקציה למקרה $r = 1$ בעזרת משפט הפירוק הפרימרי. בשלב השני, עבור חזקה של אי פריק, נראה שאפשר לקחת $v \in \ker p^a \setminus \ker p^{a-1}$.

הפרטים נשארים כתרגיל. ■

עתה, נוכיח את משפט הבסיס הנורמלי. **הוכחה:** ניתן שתי הוכחות - אחת עובדת כאשר K אינסופי, והשנייה עובדת כאשר החבורה G היא ציקלית. ראינו שבהרחבות של שדות סופיים החבורות תמיד מעגליות, ולכן זה יכסה שדות סופיים.

ראשית, נניח כי K אינסופי. נסמן $G = \{\sigma_1, \ldots, \sigma_m\}$, כאשר $\sigma_1 = 1$. נגדיר פעולה של G על השדה $K(x_1, \ldots, x_m)$ - פונקציות רציונאליות מעל K עם m משתנים - על ידי

$$\sigma(x_i) = x_j \iff \sigma \circ \sigma_i = \sigma_j$$

נגדיר כעת

$$\begin{aligned} B(x) &= \left(x_i^{\sigma_j}\right) \in M_{m \times m}(K[x_1, \ldots, x_m]) \\ h(x) &= \det B(x) \end{aligned}$$

נשים לב שאם נציב $x=(1,0,\ldots,0)$, נקבל מטריצת תמורה ־ כלומר בכל עמודה ובכל שורה יש בדיוק 1 יחיד, ושאר הכניסות הן 0. לכן הדטרמיננטה היא ±1. בפרט, קיבלנו $h(x)\not\equiv0$.

נחפש $\alpha\in N$ המקיים $h\left(\left(\sigma_i(\alpha)\right)_{i=1}^m\right)\neq0$. נניח שאין α כזה. נבחר בסיס $\alpha_1,\ldots,\alpha_m$ של N/K, ונגדיר

$$g(y_1,\ldots,y_k)=h\left(\left(\sum_{j=1}^m\sigma_i(\alpha_j)\,y_j\right)_{i=1}^m\right)$$

אם $g(a_1,\ldots,a_n)\neq0$, כאשר $a_i\in K$, אזי עבור $\alpha=\sum a_i\alpha_i$, מקבלים $h\left(\left(\sigma_i(\alpha)\right)_{i=1}^m\right)\neq0$ כמו שרצינו. אחרת, $g(\underline{a})=0$ לכל $\underline{a}\in K^m$, וכן K אינסופי, ולכן מהלמה הראשונה נקבל כי $g(\underline{y})=0$ כפולינום. אבל $g(\underline{y})=h(A\underline{y})$, כאשר $A=\left(\alpha_j^{\sigma_i}\right)_{i,j=1}^m$. A הפיכה, מלמה 2, ולכן נקבל כי $h(\underline{x})=g\left(A^{-1}\underline{x}\right)=0$, בסתירה.

לכן יש α עבורו $h\left(\left(\sigma_i(\alpha)\right)_{i=1}^m\right)\neq0$. אזי נקבל כי

$$0\neq h\left(\left(\sigma_i(\alpha)\right)_{i=1}^m\right)=\det B\left(\left(\sigma_i(\alpha)\right)_{i=1}^m\right)$$

כלומר B הזו הפיכה. נראה שהווקטורים $\sigma_i(\alpha)$ בלתי תלויים לינארית וינבע שהם בסיס. נניח כי

$$\sum_{i=1}^m a_i\sigma_i(\alpha)=0$$

נפעיל את σ_j ונקבל

$$\sum_{i=1}^m a_i\sigma_j\left(\sigma_i(\alpha)\right)=0$$

לכן נקבל

$$\left(\sigma_j\left(\sigma_i(\alpha)\right)\right)_{i,j}\begin{pmatrix}a_1\\ \vdots\\ a_m\end{pmatrix}=0$$

אבל המטריצה באגף שמאל היא בדיוק $B\left(\left(\sigma_i(\alpha)\right)_{i=1}^m\right)$, שהיא הפיכה ־ ולכן לכל j נקבל $a_j=0$, כלומר קיבלנו את מה שרצינו.

סיימנו את המקרה האינסופי. נניח כעת כי G מעגלית מסדר m. נסמן $G=\langle\tau\rangle$. נקח $f=f_\tau\in K[x]$ להיות הפולינום המינימלי של τ (כהעתקה לינארית על N מעל K).

$\tau^m=1$, ועל כן $f(x)\mid x^m-1$. בנוסף, מאי תלות של קרקטרים, $1,\tau,\ldots,\tau^{m-1}$ בלתי תלויים לינארים, ולכן $\deg f>m-1$. לכן נקבל $f_\tau(x)=x^m-1$. לכן, זהו גם הפולינום האופייני. מהלמה השלישית, יש $v\in N$ עבורו $\left\{v,\tau(v),\ldots,\tau^{m-1}(v)\right\}$ בסיס, וסיימנו. ■