

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 $G = \text{Gal}(N/K)$, 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 $f \in K[x_1, \dots, x_m]$ וגם $0 \neq f$ וגם $|K| = \infty$, אזי יש $a_1, \dots, a_m$ עם $f(a_1, \dots, a_m) \neq 0$.

כעת נמשיך.

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

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

הפיכה.

הוכחה: נניח שיש $c_1, \dots, c_m \in \bar{K}$ 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 , $T : V \rightarrow V$ העתקה לינארית כך שמתקיים $f_T = m_T$, כלומר הפולינום האופייני שווה לפולינום המינימלי. אזי יש בסיס של V מהצורה

$$\{v, Tv, T^2v, \dots, T^{n-1}v\}$$

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

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

נגדיר כעת

$$B(x) = (x_i^{\sigma_j}) \in M_{m \times m}(K[x_1, \dots, x_m])$$

$$h(x) = \det B(x)$$

נשים לב שאם נציב $x = (1, 0, \dots, 0)$, נקבל מטריצת תמורה - כלומר בכל עמודה ובכל שורה יש בדיוק 1 יחיד, ושאר הכניסות הן 0. לכן הדטרמיננטה היא ± 1 . בפרט, קיבלנו $h(x) \neq 0$.
נחפש $\alpha \in N$ המקיים $h((\sigma_i(\alpha))_{i=1}^m) \neq 0$. נניח שאין α כזה. נבחר בסיס $\alpha_1, \dots, \alpha_m$ של N/K , ונגדיר

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

אם $g(a_1, \dots, a_n) \neq 0$, כאשר $a_i \in K$, אזי עבור $\alpha = \sum a_i \alpha_i$, מקבלים $h((\sigma_i(\alpha))_{i=1}^m) \neq 0$ 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 $g(\underline{y}) = h(\underline{Ay})$ כאשר $A = (\alpha_j^{\sigma_i})_{i,j=1}^m$. הפיכה, מלמה 2, ולכן נקבל כי $h(\underline{x}) = g(A^{-1}\underline{x}) = 0$ בסתירה. לכן יש α עבורו $h((\sigma_i(\alpha))_{i=1}^m) \neq 0$ אזי נקבל כי

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

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

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

לכן נקבל

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

אבל המטריצה באגף שמאל היא בדיוק $B((\sigma_i(\alpha))_{i=1}^m)$, 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 $x^m - 1 \mid f(x)$. בנוסף, מאי תלות של קרקטרים, $1, \tau, \dots, \tau^{m-1}$ 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 $\{v, \tau(v), \dots, \tau^{m-1}(v)\}$ בסיס, וסיימנו. ■