אלגברה ב2

ⓒ ארזים

10 במאי 2017

1 משפטים

בשיעור שעבר הגדרנו דיסקרימיננטה, וראינו כמה נוסחאות שלה, כמה דוגמאות, והוכחנו שהיא תמיד שייכת לשדה שמעליו מוגדר הפולינום. הזכרנו גם שיש נוסחא במקדמים - נמשיך עם זה.

הגדרה 1.1 (מטריצת סילבסטר) בהינתן

$$f = \sum_{i=0}^{n} a_i x^{n-i}$$
$$g = \sum_{i=0}^{m} b_i x^{m-i}$$

נגדיר

$$\mathrm{Syl}(f,g)$$

את המטריצה הבאה: m השורות הראשונות יהיו סיבובים של $(a_0, a_1, \ldots, a_n, 0, \ldots, 0)$, שאורכו $n+m$. הסיבוב האחרון הוא $(0, \ldots, 0, a_0, a_1, \ldots, a_n)$. n השורות האחרונות מתקבלות באופן אנלוגי עם מקדמי g.

דוגמא

$$f = ax^2 + bx + c$$
$$g = f' = 2ax + b$$
$$\mathrm{Syl}(f,g) = \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix}$$

דוגמא

$$\begin{aligned} f &= ax^3 + bx^2 + cx + d \\ g &= f' \\ \mathrm{Syl}\left(f, f'\right) &= \begin{pmatrix} a & b & c & d & 0 \\ 0 & a & b & c & d \\ 3a & 2b & c & 0 & 0 \\ 0 & 3a & 2b & c & 0 \\ 0 & 0 & 3a & 2b & c \end{pmatrix} \end{aligned}$$

משפט 1.2 (שלא נוכיח)

$$\Delta\left(f\right) = \frac{\left(-1\right)^{\frac{n(n-1)}{2}}}{a_0} \underbrace{\det\left(\mathrm{Syl}\left(f, f'\right)\right)}_{:=\mathrm{Res}(f,f')}$$

למשל,

$$\begin{aligned} \Delta\left(ax^2 + bx + c\right) &= \frac{-1}{a}\left(4a^2c - b^2a\right) = b^2 - 4ac \\ \Delta\left(ax^3 + bx^2 + cx + d\right) &= b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd \end{aligned}$$

כעת, יש לנו חוב מהשיעור שעבר:

טענה 1.3 אם $f \in K\left[x\right]$, $\mathrm{char}K \neq 2$, עם $\Delta\left(f\right) \neq 0$, כלומר f פריד, ואם מזהים את $G = \mathrm{Gal}\left(f/K\right)$ כתת חבורה של S_n דרך הפעולה על $\alpha_1, \ldots, \alpha_n$ (שורשי f) אז $G \leq A_n$ אם ורק אם $\Delta\left(f\right) = x^2$ עבור $x \in K$ כלשהו.

הוכחה: נסמן

$$\delta\left(f\right) = \sqrt{\Delta\left(f\right)} = a_0^{n-1} \prod_{i<j} \left(\alpha_i - \alpha_j\right) \in N$$

אזי $\Delta\left(f\right)$ היא ריבוע אם ורק אם $\delta\left(f\right) \in K$. זה שקול לכך שלכל $\sigma \in G$, מתקיים $\sigma\left(\delta\left(f\right)\right) = \delta\left(f\right)$. נחשב:

$$\sigma\left(\delta\left(f\right)\right) = a_0^{n-1} \prod_{i<j} \left(\sigma\left(\alpha_i\right) - \sigma\left(\alpha_j\right)\right) = \mathrm{sgn}\left(\sigma\right)\delta\left(f\right)$$

וזה לפי ההגדרה של סימן של תמורה. על כן, $\sigma\left(\delta\left(f\right)\right) = \delta\left(f\right)$ אם ורק אם $\sigma \in A_n$. לכן, זה נכון לכל $\sigma \in G$ אם ורק אם $G \leq A_n$. ובסך הכל סיימנו. ■

1.1 משפט האיבר הפרימיטיבי

הגדרה 1.4 הרחבה סופית L/K נקראת <u>פשוטה</u> אם קיים $\alpha \in L$ כך שמתקיים $L = K(\alpha)$.

דוגמא $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ פשוטה, כי $\sqrt{2}+\sqrt{3}$ יוצר אותה. הדוגמא הקטנה ביותר להרחבה לא פשוטה היא

$$\mathbb{F}_p\left(\sqrt[p]{x},\sqrt[p]{y}\right)/\mathbb{F}_p(x,y)$$

זו הרחבה לא פרידה, כי הפולינום $x^p - x = (x - \sqrt[p]{x})^p$ הוא $\sqrt[p]{x}$, שאינו פריד - בעל שורש אחד.

משפט 1.5 (משפט האיבר הפרימיטיבי) כל הרחבה סופית פרידה היא פשוטה.

הוכחה: אם K סופי, אזי K סופי, ולכן L^* ציקלי. היוצר שלו יוצר את ההרחבה, וסיימנו.
כעת נניח כי K אינסופי. מסופיות, $L = K(\alpha_1,\ldots,\alpha_n)$. באינדוקציה, די להוכיח עבור $n = 2$. כלומר, מניחים $L = K(\alpha_1,\alpha_2)$. נרצה למצוא $\alpha \in L$ המקיים $L = K(\alpha)$.
נבחר N/K גלואה המכילה את L. נסמן

$$G = \mathrm{Gal}(N/K), H = \mathrm{Gal}(N/L)$$

נקח $u \in K$ ונסמן $\alpha = \alpha_1 + u\alpha_2 \in L$. די להראות שאם $\sigma \notin H$ אזי $\sigma \notin \mathrm{Gal}(N/K(\alpha))$, כי אז $H = \mathrm{Gal}(N/K(\alpha))$, ולפי התאמת גלואה נקבל $L = K(\alpha)$. כלומר, ניקח $\sigma \notin H$ ונראה כי

$$\sigma(\alpha) \neq \alpha$$

נזכור שעוד יש לנו הרשות לבחור את u.

$$\sigma(\alpha) - \alpha = \sigma(\alpha_1) - \alpha_1 + u(\sigma(\alpha_2) - \alpha_2)$$

לכן $\sigma(\alpha) = \alpha$ אם ורק אם

$$\sigma(\alpha_1) - \alpha_1 = u(\alpha_2 - \sigma(\alpha_2))$$

כעת, $\sigma \notin H$, ולכן היא לא מקבעת את $L = K(\alpha_1,\alpha_2)$, כלומר

$$(\sigma(\alpha_1) - \alpha, \sigma(\alpha_2) - \alpha_2) \neq (0,0)$$

לכן המשוואה הקודמת שקיבלנו היא משוואה על u, שיש לה לכל היותר פתרון אחד:

$$u = \frac{\sigma(\alpha_1) - \alpha_1}{\alpha_2 - \sigma(\alpha_2)}$$

כיוון שהשדה K אינסופי, בעוד $H \leq G$ סופית, יש u שאינו מצורה זו לאף $\sigma \notin H$, וכן שהמכנה בו לא מתאפס, ואז, אם $\sigma \notin H$, אז

$$\sigma(\alpha) \neq \alpha$$

וסיימנו. ■

1.2 המשפט היסודי של האלגברה

משפט 1.6 (המשפט היסודי של האלגברה) $\mathbb{C}$ סגור אלגברית.

יש למשפט הזה המון הוכחות, אבל אין הוכחה אלגברית. ההוכחה הכי אלגברית (שהמרצה מכיר) היא זו שניתן: **הוכחה:** לכל מספר חיובי ממשי יש שורש ריבועי, ולכן גם עבור $z = re^{i\theta}$ יש:

$$z = \sqrt{r}e^{i\frac{\theta}{2}}$$

כדי להוכיח סגירות אלגברית של $\mathbb{C} = \mathbb{R}(i)$ די להראות שכל $f \in \mathbb{R}[x]$ מתפצל מעל $\mathbb{C}$ (כי אם $g \in \mathbb{C}[x]$ אזי $g \cdot \overline{g} \in \mathbb{R}[x]$, וכן שורשי f בתוך $\mathbb{C}$, לכן גם יש שורשים של g). בלי הגבלת הכלליות ניתן להניח כי f אי פריק, $f \neq x^2+1$.נסמן N את שדה הפיצול של $f(x)\left(x^2+1\right)$ הרחבת גלואה. די להוכיח כי $N = \mathbb{C}$. כעת, נסמן $G = \mathrm{Gal}(N/\mathbb{R})$, ובתור H את תת חבורת סילוב 2 של G. אזי H חבורת 2, $[G:H]$ אי זוגי. אזי

$$\left[N^H : \mathbb{R}\right] = [G:H]$$

אי זוגי. אם היה $x \in N^H \backslash \mathbb{R}$, אזי $\deg \mathrm{irr}(x, \mathbb{R}) = 2k+1$, כלומר היה לו שורש בתוך $\mathbb{R}$, בסתירה. לכן $N^H = \mathbb{R}$. לכן $G = H$, ומעתה נניח כי G חבורת 2.
אזי גם $\tilde{G} = \mathrm{Gal}(N/\mathbb{C}) \leq G$ חבורת 2. לכן, יש סדרה

$$1 \leq G_\nu \leq \cdots \leq G_2 \leq G_1 \leq \tilde{G} = G_0$$

כאשר $[G_i : G_{i+1}] = 2$. לפי המשפט היסודי של תורת גלואה, אם נסמן $K_i = N^{G_i}$, נקבל

$$\mathbb{C} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_\nu = N$$

וכל ההרחבות מסדר 2. אם $\tilde{G}$ אינה טריוויאלית, $K_1/\mathbb{C}$ היא הרחבה ריבועית, שנוצרת על ידי שורש של x^2+ax+b. שורש זה הוא שורש של $\left(x+\frac{a}{2}\right)^2 - \left(\frac{a^2-4b}{4}\right)$. לכן השורש הזה יוצר את אותו שדה כמו $\sqrt{a^2-4b}$ - אבל זה מספר מרוכב, כי אמרנו שיש שורש ריבועי! לכן $K_1 = \mathbb{C}$, בסתירה. אם כן, $\tilde{G}$ טריוויאלית. ■

1.3 משפט הבסיס הנורמלי

תהי N/K הרחבת גלואה סופית, ונסמן $G = \mathrm{Gal}\left(N/K\right)$. ההרחבה סופית, ולכן יש בסיס $\alpha_1, \ldots, \alpha_n$. היא פרידה, ולכן יש בסיס $1, \alpha, \ldots, \alpha^{n-1}$ (ממשפט האיבר הפרימיטיבי). אנחנו רוצים בסיס שקשור לחבורה.

דוגמא ניקח $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\right) \cong \mathbb{Z}/2\mathbb{Z}$ עם יוצר $\sigma\left(\sqrt{2}\right) = -\sqrt{2}$. האם $\sqrt{2}, \sigma\left(\sqrt{2}\right)$ בסיס?
לא, כי הם תלויים לינארית. אם נגדיר $\alpha = 1 + \sqrt{2}$, אז $\sigma, \sigma\left(\alpha\right)$ בסיס. קיבלנו בסיס, שעליו G פועלת.

משפט 1.7 (משפט הבסיס הנורמלי) אם N/K גלואה עם חבורה $G = \mathrm{Gal}\left(N/K\right)$ אז יש $\alpha \in N$ כך שהקבוצה $\{\sigma\left(\alpha\right)\}_{\sigma \in G}$ היא בסיס של N.
כדי להוכיח אותו נצטרך כמה למות.

למה 1.8 יהי K שדה אינסופי, ויהי $f \in K\left[x_1, \ldots, x_m\right]$ פולינום עם m משתנים. אם לכל $\underline{a} \in K^m$ מתקיים $f\left(\underline{a}\right) = 0$, אזי $f = 0$ כפולינום.

הוכחה: באינדוקציה על m.
$m = 1$: לפולינום שאינו 0 במשתנה יחיד יש לכל היותר $\deg f$ פתרונות, ולכן יש $\alpha \in K$ עבורו $f\left(\alpha\right) \neq K$. לכן אם הפולינום מתאפס בכל נקודה, הוא 0.
$m > 1$: $f\left(\underline{x}\right) \in K\left[x_1, \ldots, x_n\right]$. נרשום

$$f\left(\underline{x}\right) = \sum_{i=0}^{k} c_i\left(x_1, \ldots, x_{m-1}\right) x_m^i$$

מניחים כי $f\left(\underline{a}\right) = 0$ לכל $\underline{a} \in K^m$. נבחר $a_1, \ldots, a_{m-1} \in K$ ונסתכל על

$$g\left(x_m\right) = f\left(a_1, \ldots, a_{m-1}, x_m\right)$$

לפי בסיס האינדוקציה, $g\left(a\right) = 0$ לכל $a \in K$, ולכן $g \equiv 0$. לכן לכל i, $c_i\left(x_1, \ldots, x_{m-1}\right)$ מתאפס על כל K^{m-1}, ובאינדוקציה נסיים. ■