ליניארית 9 $\sim$ מבוא לצורת ג'ורדן, פולינום מינימלי

שחר פרץ

7 במאי 2025

רשימת פולינומים חמודים:

- הפולינום האופייני $f_A = f_T = \det(Ix - A)$
- בהינתו מטריצה, המטריצה המצורפת A_f

משפט 1. תהי $A \in M_n(\mathbb{F})$, נביט בקבוצה $I_A = \{p \in \mathbb{F}[[x]: p(A) = 0]\}$, אז $I_A \subseteq \mathbb{F}[x]$ אידיאל, קיים ויחיד ב־I_A פולינום מתוקן בעל דרגה מינימלית.

הגדרה 1. I_A לעיל

הוכחה. נבחין כי $0 \in I_A$. סגירות לחיבור – ברור. תכונת הבליעה – גם ברור. סה"כ אידיאל. $\mathbb{F}[x]$ תחום שלמות ולכן נוצר ע"י פולינום יחיד $I_A = (p)$. אם $I_A = (p) = (p')$ אז $p \sim p'$. אם נקבע אותו להיות מתוקן אז הוא יחיד. לפולינום הנ"ל נקרא הפולינום המינימלי של A הוא m_A. באותו האופן, עבור $T\colon V \to V$ ט"ל ניתן להגדיר את M_T. ■

הערה 1. אם $A \in M_n(\mathbb{F})$ ו־$p \in \mathbb{F}[x]$ כך ש־$p(A) = 0$, אז $p \in I_A$ ומתקיים $m_A \mid p$.

הערה 2. אנו יודעים ש־$f_a \mid m_a$ ממספט קיילי המילטון.

דוגמאות. עבור $A = I_n$ אז $f_A = (x-1)^n$ ו־$m_a = (x-1)$. לא בהכרח $m_a = f_a$, אל לפעמים כן – לדוגמה בעבור $D\colon \mathbb{F}[x] \to \mathbb{F}[x]$ אופרטור הגזירה מתקיים $f_D = x^{n+1}$ וכן $m_D = x^{n+1}$ כי יש פולינומים שנדרש לגזור n פעמים ע"מ לקבל 0, לדוגמה x^n.

משפט 2. (תזכורת) תהא $A = A_f$ המטריצה המצורפת ל־A. אז $f_A = m_A$.

משפט 3. אם A מייצגת את $T\colon V \to V$ אז $m_A = m_T$.

הוכחה. נבחר בסיס ל־V, B. יהי $p \in \mathbb{F}[x]$. אז $[p(T)]_B = p([T]_B)$. שני האגפים מתאפסים ביחד, ולכן $I_A = I_T$. ■

מסקנה 1. נניח ש־A לכסינה והע"ע השונים הם $\lambda_1 \dots \lambda_k$ (כלומר $f_A = \prod_{i=1}^k (x-\lambda_i)^{r^i}$) אז $m_a = \prod_{i=1}^k (x - \lambda_i)$.

הוכחה. בה"כ A אלכסונית, $A = \operatorname{diag}(\lambda_1 \dots \lambda_k)$ עם חזרות. נבחין ש־$\prod_{i=1}^k (x - \lambda_i I) = 0$ (הסברים בהמשך). A מייצגת העתקה $T\colon V \to V$ ול־V יש בסיס של ו"עים $B = (v_1 \dots v_n)$. אז $\left(\prod_{i=1}^k (T - \lambda_i)\right)(v_j) = 0$ כי v_j מתאים ל־λ_i כלשהו וכך זה מתאפס. ידוע $m_a \mid \prod_{i=1}^k (x - \lambda_i)$. אם נוריד את אחד המכופלים אז ה"ע שירד לא יתאפס/לא יפאס הז הוקטור העצמי המצאים. ■

איפיון דרגת הפולינום המינימלי

למעשה, d הנ"ל הוא המינימלי שעבורו ניתן לבטא את A^d כצ"ל של חזקות נמוכות יותר.

הערה 3. אם $A \in M_n(\mathbb{F})$, ו־$\mathbb{F} \subseteq \mathbb{K}$, אז ניתן לחשוב על $A \in M_n(\mathbb{K})$ ו־m_A לא משתנה ללא תלות בשדה.

משפט 4. אם $g, h \in \mathbb{F}[x]$ ו־$T\colon V \to V$ ט"ל אז $g(T), h(T)$ מתחלפות.

הוכחה.

$$\big(g(T) \circ h(T)\big)(v) = (g \cdot h)(T)(v) = (h \cdot g)(T)(v) = \big(h(T) \cdot g(T)\big)(v)$$

■

למה 1. (למה המחלק של פולינום מינימלי). יהי m_T הפולינום המינימלי של ט"ל $T\colon V \to V$. אם $f(x) \mid m_T(x)$ וגם $\deg f > 0$ אז $f(T)$ אינו הפיך.

הוכחה. בכלל ש־$m_T \mid f$ אז קיים $g \in \mathbb{F}[x]$ כך ש־$f \cdot g = m_T$. נניח בשלילה ש־$f(T)$ הפיכה. אז:

$$f(T) \circ g(T) = m_T(T) = 0,\ 0 = f(T)^{-1} \circ (0) = g(T)$$

ידוע:

$$\deg m_T = \underbrace{\deg f}_{>0} + \deg g \implies \deg g < \deg m_T$$

בה"כ g מתוקן וקיבלנו סתירה למינימליות של m_T, אלא אם כן $g(x)$ פולינום ה־0 אבל $m_T = 0$ בסתירה להגדרתו של פולינום מינימלי. ■

הוכחה זהה עבור מחלק של m_A, עבור A מטריצה.

משפט 5. אם λ ע"ע של T אז $m_T(\lambda) = 0$.

הוכחה. נשתמש בטענת עזר: אם $p \in \mathbb{F}[x]$ פולינום המקיים $p(T) = 0$, ו־λ ע"ע של T, אז $p(\lambda) = 0$. [טענת עזר זו יותר חזקה מהמשפט]. קיים $v \neq 0$ שעבורו $0 = p(T)(v) = p(\lambda\mathrm{Id})(v) = p(\lambda)v$ (הסיבה לשוויון האחרון – תפתחו את $p(\lambda\mathrm{Id})$ וזה יהיה די ברור, אבל הנה נימוק קצר)

$$p(x) = \sum_{i=0}^{n} a_i x^i,\ \ p(T)(v) = \left(\sum_{i=0}^{n} a_i T^i\right)(v) = \sum_{i=0}^{n} a_i T^i(v) = \left(\sum_{i=0}^{n} a_i \lambda^i\right) v = p(\lambda)v$$

■

"זה טבעוני, זה טבעוני וזה ממשש טבעוני". "מה זה אומר שזה לא טבעוני? יש בזה קצת ביצה".

משפט 6. λ ע"ע של T אמ"מ $m_T(\lambda) = 0$

הוכחה. כיוון אחד הוכח. מהכיוון השני, ידוע $m_T(\lambda) = 0$. לפי משפט בזו $(x-\lambda) \mid m_T(x)$. ידוע $f_T \mid m_T$ וסה"כ $(x-\lambda) \mid f_T$ וסה"כ λ ע"ע של T. ■

משפט 7. $m_A(x) \mid f_A(x) \mid (m_A(x))^n$

הוכחה. נותר להוכיח $f_A(x) \mid (m_A(x))^n$. ידוע שפולינום מינימלי/אופייני נשארים זהים מעל כל שדה שמכיל את $\mathbb{F}$. לכן, ניתן להניח שהוא מתפרק לגורמים לינאריים. ראינו שאם $f, g \in \mathbb{F}[x]$, $\mathbb{F} \subseteq \mathbb{K}$ ומתקיים $g \mid f$ מעל $\mathbb{K}$, אז $g \mid f$ מעל $\mathbb{F}$. אז:

$$(\sum n_i = n) \qquad f_A = \prod_{i=1}^{k} (x-\lambda_i)^{n_i},\ \ m_A(x) = \prod_{i=1}^{k} (x-\lambda_i)^{m_i} \quad (1 \le m_i \le n_i),\ \ (m_a(x))^n = \prod_{i=1}^{k} (x-\lambda_i)^{n|m_i}$$

בגלל ש־$n \le m_i \cdot n \impliedby 1 \le m_i$ אז מצאנו $f_A \mid m_A^n$. ■

הוכחה זהה עבור $T\colon V \to V$ עם $\dim V = n$.

מסקנה (שימושית!). נניח ש־$f_A \mid g$. נניח ש־g אי פריק. אז $g \mid m_A$.

הוכחה.

$$g \mid f_A \mid (m_A)^n$$

ידוע g אי פריק, ולכן ראשוני (כי $\mathbb{F}[x]$ תחום ראשי) ולכן $g \mid m_A$. ■

משפט 8. נניח ש־A בלוקים עם בלוקים על האלכסון, $A = \mathrm{diag}(A_1 \dots A_k)$ כך ש־$\sum n_i = n$, $\forall i \in [k]\colon A_i \in M_{n_i}(\mathbb{F})$, אז מתקיים $m_a = \ell\mathrm{cm}(m_{A_1} \dots m_{A_k})$.

הגדרה 2. R תחום שלמות, $a_1 \dots a_n \in R$ ו־$\ell = \ell\mathrm{cm}(a_1 \dots a_n)$ אמ"מ:

1. $\forall i \in [n]\colon a_i \mid \ell$
2. $\forall b \in R\colon \forall i \in [n]\colon a_i \mid b \longrightarrow \ell \mid b$

דוגמה. $R = \mathbb{Z},\ \ell\mathrm{cm}(2,6,5) = 30$. במקרה שלנו, ה־$\ell\mathrm{cm}$ הנ"ל הוא הפולינום בעל הדרגה המינימלית שמתחלק בכל ה־$m_A(x)$. באופן כללי, $\ell\mathrm{cm}(a_1 \dots a_n)$ מתקבל כיוצר של אידיאל החיתוך בתחום הראשי. כלומר:

$$I = (\ell) = \bigcap_{i=1}^{n} Ra_i$$

(הבהרת הסימון: $Ra = (a) = \langle a \rangle$).

הוכחה (למשפט לעיל). לכל $g \in \mathbb{F}[x]$ מתקיים:

$$g(A) = \begin{pmatrix} g(A_1) & & \\ & \ddots & \\ & & g(A_k) \end{pmatrix}$$

מתקיים $g(A) = 0$ אמ"מ $g(A_i) = 0 \quad \forall i \in [k]$. לכן $g \mid m_{A_i} \quad \forall i \in [k]$. מהגדרת ה־$\ell\mathrm{cm}$ סיימנו. ■

משפט 9. נניח ש־$T, S\colon V \to V$ ט"ל מתחלפות. אז:

1. $\operatorname{Im} S,\ \ker S$ הם T־אינווריאנטים (ולהפך).
2. אם $S \subseteq W$ תמ"ו הוא T־אינווו' אז גם $S(W)$ הוא T־איני'!
3. אם $W_1, W_2 \subseteq V$ הם T־איני' אז גם $W_1 \cap W_2,\ W_1 + W_2$ הם T־איני'!
4. אם $f \in \mathbb{F}[x]$ ו־$W \subseteq V$ תמ"ו T־איני', אז W גם $f(T)$־איני'!

הוכחה. 1. יהא $v \in \operatorname{Im} S$, אז קיים $u \in V$ כך ש־$S(u) = v$:

$$Tv = T(S(u)) = (T \circ S)(u) = (S \circ T)(u) = S(T(u)) \in \operatorname{Im} S$$

ועבור $v \in \ker S$:

$$S(T(v)) = \cdots = T(S(v)) = T(0) = 0 \implies T(v) \in \ker S$$

2. יהי $v \in S(W)$. קיים $w \in W$ כך ש־$v = S(w)$

$$T(v) = T(S(w)) = S(T(w)) \in S(W)$$

כי $T(w) \in W$.

3. ראינו בתרגול הקודם

4. יהי $w \in W$.

$$f = \sum_{i=1}^{n} a_i x^i,\ \ f(T)w(= \left(\sum_{i=0}^{n} a_i T^i\right)(w) = \sum_{i=0}^{n} a_i T^i(w)$$

באינדוקציה $T^i(w) \in W$. W תמ"ו ולכן סגור וצ"ל וסיימנו. [בסיכום כתוב הוכחה: קל]

■

(הערה: 3, 4 לא תלויים בהיות הטרנספורמציות מתחלפות)

משפט 10. ("מאוד חשוב") יהי V מ"ו מעל $\mathbb{F}$. נניח $T\colon V \to V$ ט"ל. נניח $f(T) = 0$. נניח ש־$f = g \cdot h$ עבור $\gcd(g,h) = 1$. אז:

$$V = \ker g(T) \oplus \ker h(T)$$

ואם $f = M_T$, אז g, h הם הפולינומים המינימליים לצמצום T על תת־המרחבים לעיל בהתאמה.

הבהרת הכוונה ב"פולינום המינימלי לצמצום T על תתי המרחבים": בהינתן $T = U \oplus W$, $T_u = T_{|_U}\colon U \to U$ ובאופן דומה T_w, אז $m_T = m_{T_U} \cdot m_{T_W}$.

הוכחה. מכך ש־$(g,h) = 1$ קיימים $a, b \in \mathbb{F}[x]$ כך ש־$ag + bh = 1$. בפרט, קיימים $a, b \in \mathbb{F}[x]$ כך ש־$ag + bh = 1$. אזי:

$$a(T) \circ g(T) + b(T) \circ h(T) = \mathrm{Id}$$

אזי:

$$(a(T) \circ g(T))(v) + (b(T) \circ h(T))(v) = v$$

טענת עזר. $(a(T) \circ g(T))(v) \in \ker h(T)$. זאת כי:

$$(h(T) \circ a(T) \circ g(T))(v) = a(T) \circ (h \cdot g)(T) = a(T)(0) = 0$$

באופן זהה $(b(T) \circ h(T))(v) \in \ker g(T)$. סה"כ הצגנו כל וקטור כסכום של וקטור מ־$\ker g(T)$ ווקטור מ־$\ker h(T)$, ולכן $\ker h(T) + \ker g(T) = V$. עתה נראה שהסכום הוא ישר. יהא $v \in \ker g(T) \cap \ker h(T)$. נבחין ש־:

$$0 + 0 = (a(T) \circ g(T))(v) + (b(T) \circ h(T))(v) = v$$

■

שחר פרץ, 2025

GitHub.com/shpe/cs-tau-shpe