ליניארית 2א 4

שחר פרץ

2 באפריל 2025

מרצה: בן בסקין

1 על ההבדל בין פולינום לפולינום

נבחין ש־$\mathbb{F}[x]$ הוא מ"ו מעל $\mathbb{F}$. וכן $\mathbb{F}[x]$ הוא חוג חילופי עם יחידה. בחוג כפל לא חייב להיות קומטטיבי (נאמר, חוג המטריצות הריבועיות). אומנם קיימת יחידה (פולינום קבוע ב־1) אך אין הופכיים לשום דבר חוץ מלפונ' הקבועות. שזה מאוד חבל כי זה כמעט שדה.

לכן, נגדיר את $\mathbb{F}(x)$ – אוסף הפונקציות הרציונליות:

$$\mathbb{F}(x) = \left\{\frac{f(x)}{g(x)} \mid g(x) \neq 0\right\}$$

זהו שדה. אם נתבונן במטריצות דומות, יש הבדל בין להגיד $f_A(x) \in \mathbb{F}[x]$, אך אפשר לטעון $f_A(x) = |B|$ כש־$B \in M_n(\mathbb{F}(x))$. למה? כי $xI - A \in M_n(\mathbb{F}(x))$ (זה קצת מנוון כי איברי המטריצה הם או פולינומים קבועיים או ממעלה 1). משום שדטרמיננטה שולחת איבר לשדה, אז $|B| \in \mathbb{F}(x)$. כך למעשה נגיע לכך שפולינומים אופייניים שווים כשני איברים בתוך השדה, ולא רק באיך שהם מתנהגים ביחס לקבועיים.

דוגמה:

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{F}_2),\ f(x) = x^3,\ g(x) = x,\ f, g \in \mathbb{F}_2 \to \mathbb{F}_2 \implies f = g$$

אך:

$$f(A) = A^3 = 0,\ g(A) = A \neq 0$$

זה לא רצוי. נבחין בשני שוויונות שונים – שוויון פונקציות, בהם $f = g$ מעל $\mathbb{F}_2$, ושוויון בשדה – בו $f - g \neq 0$ (כי $-x^2$ לא פולינום האפס, ואף מעל $\mathbb{F}_2$) ולכן ב־$\mathbb{F}_2(x)$ מתקיים $f \neq g$.

2 על הקשר בין ריבוי גיאומטרי ואלגברי

הערה/טענה: נניח שפ"א של T או A:

$$f_T(x) = \prod_{i=1}^{k} (x - \lambda_i)^{n_i}$$

אז $d_{\lambda_i} = n_i$ הריבוי האלגברי. על כן, נבחין כי $n_i \leq d_{\lambda_i}$.

הוכחה. הוכחה:

$$(x - \lambda_i)^{n_i} \mid f_T(x) \implies f_T(x) = (x - \lambda_i)^{n_i} \prod_{\substack{j \in [k] \\ j \neq i}} (x - \lambda_j)^{n_j}$$

נניח בשלילה $d_{\lambda_i} \geq n + 1$. אז:

$$f_T(x) = \cdots = (x - \lambda_i) q(x)$$

נעביר אגפים מהשוויונות השונים ונוציא גורם משותף:

$$(x - \lambda_i)^n \left(\overbrace{\prod_{\substack{j \in [k] \\ j \neq i}} (x - \lambda_j)^{n_j} - (x - \lambda_i) q(x)}^{:= P(x)} \right) = 0$$

נדע כי $P(x)$ אינו פולינום האפס כי:

$$P(\lambda_i)=\prod_{\substack{j\in[k]\\ j\neq i}}(\lambda_i-\lambda_j)^{n_j}$$

שוויון בשדה $\mathbb{F}(x)$. וברור כי $(x-\lambda_i)^n$ אינו פולינום האפס. אך אחד מהם הוא אפס משום שכפל שני איברי שדה שווה לאפס אמ"מ אחד מהם הוא אפס, וסתירה. ■

הערה. בדוגמה שבטענה ראינו שמתקיים $\sum d_i=\sum n_i=n$ כאשר n דרגת הפולינום. זה לא תמיד המצב. דוגמה למצב בו זה לא קורה: $x^2(x^2+1)\in\mathbb{R}[x]$. סכום הריבויים האלגבריים הוא 2, אבל דרגת הפולינום היא 4. זה נכון מעל שדות סגורים אלגברית.

טענה. תהי $T\colon V\to V$ ט"ל. אזי לכל ע"ע λ מתקיים $r_\lambda\le f_\lambda$.

הוכחה. יהי λ ע"ע. אז $V_\lambda=\{v\in V\mid Tv=\lambda v\}$. יהי $B_\lambda\subseteq V_\lambda$ בסיס עבור V_λ. נשלים אותו לבסיס B של V.

$$[T]_B=\begin{pmatrix}\lambda & & 0 & *\\ & \lambda & & \\ 0 & & \ddots & \\ * & & & C\end{pmatrix}$$

ואז:

$$f_T(x)=(x-\lambda)^{r_\lambda}C(x)\implies r_\lambda\le d_\lambda$$

■

משפט. תהי $T\colon V\to V$ ט"ל עם פ"א $f_T(x)$. אז T לכסינה אמ"מ:

- בעבור k הע"ע שונים, $f_T(x)=\prod_{i=1}^k(x-\lambda_i)^{n_i}$
- לכל λ ע"ע של T מתקיים $r_\lambda=d_\lambda$

(הבהרה: 1 לא גורר את 2. צריך את שניהם).

הוכחה.

$\Longleftarrow$ T לכסינה ראינו ש־1 מתקיים. במקרה שלכסינה ראינו ש־$n=\sum r_{\lambda_i}\le\sum d_{\lambda_i}=n$ ולכן אם לאחד מבין הערכים העצמיים מתקיים $r_\lambda\neq d_k$ אז מתקיים $r_k<d_k$ ונקבל סתירה לשוויונות לעיל.

$\Longrightarrow$

$$1\implies\sum d_{\lambda_i}=n$$
$$2\implies\sum r_{\lambda_i}=\sum d_{\lambda_i}=n$$

וסה"כ $\sum r_{\lambda_i}=n$ אמ"מ T לכסינה. ■

3 לכסון ושילוש

3.1 פיבונאצ'י במרחב סופי

סדרת פיבונאצ'י:

$$\begin{pmatrix}a_{n+1}\\ a_n\end{pmatrix}=\underbrace{\begin{pmatrix}1&1\\1&0\end{pmatrix}}_{=0}^{n}\begin{pmatrix}1\\0\end{pmatrix}$$

נניח שאנו מסתכלים מעל $\mathbb{F}_p$ כלשהו. אז הסדרה חייבת להיות מחזורית. **שאלה:** מתי מתקיים $A^m=I$־ש (בעבור m מינימלי)? במילים אחרות, מתי מתחילים מחזור.

היות שמספר הזוגות השונים עבור $\begin{pmatrix}a_{n+1}\\ a_n\end{pmatrix}$ הוא p^2, אז $m\le p^2$. עבור $p=7$: $0,1,1,2,3,4,5,1,6,0,6,6,5,4,2,6,1,0,1$ – כלומר עבור $p=7$ יש מחזור באורך $m=16$. (הערה: תירואטית עם המידע הנוכחי ייתכן ויהפוך למחזורי ולא יחזור להתחלה)

טענה. אם p ראשוני אז $p\equiv 1\pmod 5$ אז אורך המחזור חסום מלעיל ע"י $p-1$.

הוכחה. תנאי מספיק (אך לא הכרחי) לקבלת מחזור באורך k הוא $A^k = I$. אז:

$$f_A(x) = x^2 - x - 1$$

יש דבר שנקרא "הדדיות ריבועית" (חומר קריאה רשות במודל) שמבטיחה שורש לפולינום להלן עבור p כנ"ל. אכן יש לנו שני ע"ע שונים (אם קיים רק אחד אז סתירה מהיות הדיסקרימיננטה $5 = 0$ אך $p \not\equiv 1 \pmod 5$). לכן קיימת P הפיכה כך ש־:

$$P^{-1}AP = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

כך ש־$\lambda_1, \lambda_2 \neq 0$. משפט פרמה הקטן אומר ש־$\lambda_1^{p-1} = \lambda_2^{p-1} = 1$. ואז $A^{p-1} = I$. ■

3.2 מבוא למשפט קיילי־המילטון

הגדרה. $T \colon V \to V$ ט"ל ניתנת לשילוש אם קיים בסיס B ל־V כך ש־$[T]_B$ משולשית.

הבחנה. אם T ניתנת לשילוש אז הפולינום האופייני שלה מתפרק לגורמים ליניארים (האם איברי האלכסון של הגרסה המשולשית). יהיה מעניין לשאול אם הכיוון השני מתקיים.

משפט. $T \colon V \to V$ ט"ל. נניח ש־$f_T(x) = \prod_{i=1}^{n}(x - \lambda_i)$ (ניתנת לפירוק לגורמים ליניאריים) אז T ניתנת לשילוש.

הוכחה. בסיס. $n = 1$ היא כבר משולשית וסיימנו.
צעד. נניח שהטענה נכונה בעבור n טבעי כלשהו, ונראה נכונות עבור $n + 1$. אז f_T מתפרק לגורמים ליניאריים, לכן יש לו שורש. יהי λ ע"ע של T. בסיס B של V מקיים ש־$[T]_B$ משולשית עליונה (נסמן $B = (w_1 \ldots w_{n+1})$) $\iff$ אז $T(w_i) \in \operatorname{span}(w_1 \ldots w_i)$. נגדיר את w_1 להיות ו"ע של λ. נשלימו לבסיס B^1.

$$[T]_B = \begin{pmatrix} \lambda & & * & \\ 0 & & \vdots & \\ \vdots & \cdots & C & \cdots \\ 0 & & \vdots & \end{pmatrix}$$

אז ניתן לומר כי:

$$f_T(x) = (x - \lambda) f_C(x)$$

נסמן $w = \operatorname{span}(w_2 \ldots w_{n+1})$. קיימת העתקה ליניארית $S \colon W \to W$ כך ש־$f_S(x) = f_C(x)$. לפי ה"א קיים בסיס ל־W הוא B'' שעבורו S משולשית עליונה. נטען ש־$B = B'' \cup \{w_1\}$ ייתן את הדרוש.

$$\forall w \in B'' \colon (T - S)(w) = Tw - Sw = aw_1 + S(w) - S(w) = aw_1$$

(כלומר, השורה העליונה של $[T]_B$ "תרמה" את aw_1 בלבד) לכן:

$$(T - S)w \subseteq \operatorname{span}(w_1)$$

זה גורר שלכל $w \in W$ מליניאריות מתקיים ש־$(T - S)w \subseteq \operatorname{span}(w_1)$. סה"כ לכל $w \in B'' \cup \{w_1\}$ מתקיים $T(w_i) \in \operatorname{span}(w_1 \ldots)$. ■

בהוכחה הזו, בנינו בסיס כך ש־:

$$[T(w) - S(w)]_B = ae_1$$

3.2.1 עוד מבוא לקיילי־המילטון

הגדרה. יהי $f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{F}[x]$, V מ"ו מעל $\mathbb{F}$ נ"ס (נוצר סופית) וכן $T \colon V \to V$ ט"ל. נגדיר:

$$f(T) = \sum_{i=0}^{d} a_i T^i, \ T^0 = id, \ T^n = T \circ T^{n-1}$$

כנ"ל עם מטריצות (ראה תרגול)

טענה. אם $A = [T]_B$ ו־$f(x) \in \mathbb{F}[x]$, אז $[f(T)]_B = f(A)$. הוכחה נובעת מהתכונות $[TS]_B = AC, \ [T + S]_B = A + C, \ [\alpha T]_B = \alpha A, \ [S]_B = C < \ [T]_B = A$.

טענה. אם $f, g \in \mathbb{F}[x]$ ו־$T \colon V \to V$ ט"ל, אז $(f \cdot g)(T) = f(T) \cdot g(T)$. באופן דומה $(f + g)(T) = f(T) + g(T)$.
לכן קל לראות ש־$f(A) = 0 \iff f(T) = 0$.

מסקנה. אם A, C דומות אז $f(C) = 0 \iff f(A) = 0$.

4 משפט קיילי־המילטון

משפט קיילי־המילטון. לכל $T\colon V \to V$ ט"ל (V נוצר סופית) ולכל $A \in M_n(\mathbb{F})$ מתקיים:

$$f_T(T) = 0,\ \ f_A(A) = 0$$

דוגמה. (מנוונת) נתבונן ב־$D\colon \mathbb{F}_n[x] \to \mathbb{F}_n[x]$ אופרטור הגזירה. ראינו $f_D(x) = x^{n+1}$ (הפולינום האופייני). אז $f_D(D)(p) = p^{(n+1)} = 0 \implies f_D(D) = 0$