אלגברה לינארית 2א

ⓒ ארזים

29 במרץ 2013

1 פולינום מינימלי

תרגיל: תהי

$$A=\begin{pmatrix}1 & 7 & 13\\ 0 & 2 & 109\\ 0 & 0 & 3\end{pmatrix}$$

הציגו את A^4 כצירוף לינארי של I,A,A^2.

טענה 1.1 אם $p\in F[x]$, $p(A)\in\operatorname{span}\left\{I,A,A^2,\dots\right\}$. נכתוב

$$p(x)=q(x)\cdot m_A(x)+r(x)$$

עם $\deg r(x)\leq\deg(m_A(x))$. כעת,

$$p(A)=r(A)$$

הטענה נכונה שכן $m_A(A)=0$.

פתרון התרגיל:

$$m_A(x)=x^3-6x^2+11x-6$$

כעת, נחלק את x^4 בפולינום המינימלי עם שארית:

$$\begin{aligned}x^4 &= (x+6)\left(x^3-6x^2+11x-6\right)+\left(25x^2-60x+36\right)=\\ &= (x+6)\left(x^3-6x^2+11x-6\right)+(5x-6)^2\end{aligned}$$

לכן מתקיים

$$A^4=25A^2-60A+36I=(5A-6I)^2$$

באותו אופן ניתן לומר

$$\begin{aligned} m_A(A) &= 0 = A^3 - 6A^2 + 11x - 6 \\ A^3 &= 6A^2 - 11A + 6I \\ A^4 &= 6A^3 - 11A^2 + 6A = 6\left(6A^2 - 11A + 6I\right) - 11A^2 + 6A = \\ &= 25A^2 - 60A + 36I = (5A - 6I)^2 \end{aligned}$$

תרגיל: תהי $A \in M_n(\mathbb{R})$, ונתון כי $\lambda \in \mathbb{C}$ ערך עצמי של A. הראו כי גם $\overline{\lambda}$ ערך עצמי של A. **הוכחה:** נוכיח בשתי דרכים.

1. יהי $v \in \mathbb{C}^n$ וקטור עצמי המתאים לערך העצמי λ. אזי $Av = \lambda v$ ולכן

$$A \cdot \overline{v} = \overline{A} \cdot \overline{v} = \overline{Av} = \overline{\lambda v} = \overline{\lambda} \cdot \overline{v}$$

כמו כן, $v \neq 0$ ולכן גם $\overline{v} \neq 0$, והוא ווקטור עצמי שמתאים לערך העצמי $\overline{\lambda}$.

2. נניח כי $\lambda \notin \mathbb{R}$ (אחרת טריוויאלי). מתבונן בפולינום

$$m_\lambda(x) = (x - \lambda)\left(x - \overline{\lambda}\right) = x^2 - \left(\lambda + \overline{\lambda}\right)x + \lambda\overline{\lambda} \in \mathbb{R}[x]$$

בנוסף, זהו פולינום אי־פריק מעל $\mathbb{R}$. לכן מתקיים (נסמן בתור p את הפולינום המינימלי או האופייני ־ אין הבדל)

$$m_\lambda \mid p$$

שכן λ מאפס את שני הפולינומים, ולכן $(x - \lambda)$ מחלק אותם, ולכן עבור $h(x) = \gcd(p, m_\lambda)$ הוא ממעלה חיובית. כמו כן, $h(x) \in \mathbb{R}$. לכן $h(x) = m_\lambda(x)$, שכן $m_\lambda(x)$ אי־פריק מעל $\mathbb{R}$. בפרט, $h(x) \mid p(x)$, ולכן $\overline{\lambda}$ הוא שורש של $p(x)$.

■

טענה 1.2 אם $p(x) \in F[x]$ אי־פריק, $q(x) \in F[x]$ כלשהו ומתקיים

$$\gcd(p(x), q(x)) \neq 1$$

אזי $p(x) \mid q(x)$.

תרגיל: נתונה $A \in M_n(\mathbb{Q})$, ונתון כי $\sqrt[3]{2}$ ערך עצמי של A. מה הערך המינימלי האפשרי של n?

פתרון: 3. נתבונן בפולינום $p(x) = x^3 - 2$, שהוא אי־פריק מעל הרציונאליים. לכן מהטענה הקודמת נובע כי $p(x) \mid m_A, f_A$. בפרט $n = \deg f \geq \deg p(x) = 3$. מצד שני, עבור

$$A = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

שהיא הטריצה המלווה של $p(x)$, מתקיים $f_A(x)=p(x)$, וכעת $\sqrt[3]{2}$ ערך עצמי של A, ולכן המינימום הוא 3.

מסקנה 1.3 אם $\sqrt[3]{2}$ הוא ערך עצמי של $A\in M_n(\mathbb{Q})$, אזי גם $\sqrt[3]{2}\cdot\omega, \sqrt[3]{2}\cdot\omega^2$ עבור שורש יחידה מסדר שלישי - $\omega=\frac{-1+\sqrt{-3}}{2}$. זאת משום שאלה השורשים של x^3-2, שמחלק את הפולינום האופייני. יותר מכך, יש להם את אותם ריבויים אלגבריים בפולינום אופייני ובפולינום המינימלי, והם שווים לריבויים של x^3-2 בפירוק מעל $\mathbb{Q}$. בנוסף, גם הריבויים הגיאומטריים שלהם זהים.

טענה 1.4 אם $2\leq\deg p(x)\leq 3$ אזי $p(x)$ אי פריק בחוג $F[x]$ אם ורק אם אין לו שורשים בשדה F.

טענה 1.5 אם לפולינום

$$f(x)=\sum_{i=0}^{n}a_ix^i\in\mathbb{Z}[x]$$

יש שורש רציונאלי $\frac{p}{q}$ (מצומצם), אזי $p\mid a_0$, $q\mid a_n$.

הוכחה: נציב ונקבל

$$\begin{aligned}0&=\sum_{i=0}^{n}a_i\left(\frac{p}{q}\right)^i\\0&=\sum_{i=0}^{n}a_ip^iq^{n-i}\end{aligned}$$

ומכאן נקבל

$$\begin{aligned}p&\mid a_0\cdot q^n\\q&\mid a_n\cdot p^n\end{aligned}$$

ומשום שהתחלנו משבר מצומצם, $\gcd(p,q)=1$, ולכן

$$\begin{aligned}p&\mid a_0\\q&\mid a_n\end{aligned}$$

■

דוגמה: x^3-2: שורשים חשודים - $\frac{p}{q}$, $p\mid 2, q\mid 1$, כלומר השורשים האפשריים הם $\pm1,\pm2$.
אבל:

$$\begin{aligned}p(-1)&=-3\\p(1)&=-1\\p(-2)&=-10\\p(2)&=6\end{aligned}$$

לכן אין שורשים רציונאליים, והפולינום אי פריק.

טענה 1.6 (קריטריון אייזנשטיין) אם

$$f\left(x\right)=x^{n}+\sum_{i=0}^{n-1}a_{i}x^{i}\in\mathbb{Z}\left[x\right]$$

וקיים p ראשוני כך שמתקיים

$$p\mid a_{0},\dots,a_{n-1}$$

אבל גם p^{2} אינו מחלק את a_{0}, אזי $f\left(x\right)$ אי פריק מעל $\mathbb{Q}$.

תרגיל: נתונה מטריצה $A\in M_{9}\left(\mathbb{Q}\right)$ ונתון כי $m_{A}\left(x\right)=x^{3}-6x^{2}+4x-2$. מצאו את $f_{A}\left(x\right)$.

פתרון: נשים לב כי לפי קריטריון אייזנשטיין עם $p=2$, m_{A} אי פריק. כמו כן, $m_{A}\mid f_{A}\mid m_{A}^{9}$, ולכן f_{A} הוא חזקה של m_{A}. כעת ידוע כי $\deg f_{A}=9$, ולכן $f_{A}=m_{A}^{3}$.

וריאציה: נתונה $A\in M_{8}\left(\mathbb{Q}\right)$ עם $m_{A}=\left(x^{2}-3\right)\left(x^{2}-2\right)$. מצאו את כל האפשרויות עבור f_{A}.

פתרון: שוב, $m_{A}\mid f_{A}\mid m_{A}^{8}$, ולכן

$$f_{A}=\left(x^{2}-2\right)^{d_{2}}\left(x^{2}-3\right)^{d_{3}}$$

כאשר $1\le d_{2},d_{3}\le8$ וכן $\deg f_{A}=8=2d_{2}+2d_{3}$, כלומר $4=d_{2}+d_{3}$, ולכן

$$\left(d_{2},d_{3}\right)\in\left\{ \left(1,3\right),\left(2,2\right),\left(3,1\right)\right\}$$

נראה שכל האפשרויות הללו אפשריות. זאת עושים על ידי בלוקים:

$$\begin{aligned}A_{2} & = & \begin{pmatrix}0 & 2\\1 & 0\end{pmatrix}\\A_{3} & = & \begin{pmatrix}0 & 3\\1 & 0\end{pmatrix}\end{aligned}$$

הפולינומים המינימליים של הבלוקים הללו הם $x^{2}-2,x^{2}-3$ בהתאמה (כי אלה המטריצות המלוות של הפולינום). לכן בחירת d_{2} בלוקים של A_{2} ובחירת d_{3} בלוקים של A_{3}, נקבל את האפשרויות שרצינו.

1.1 קונספט

יהיו $F\subseteq K$ שדות.

1. $v_{1},\dots,v_{m}\in F^{n}\subseteq K^{n}$ בלתי תלויים מעל F אם ורק אם הם בלתי תלויים מעל K.

2. אם $K^n \subseteq F^n \in v_1,\ldots,v_m$, אזי $v \in \operatorname{span}_F\{v_1,\ldots,v_m\}$ אם ורק אם $v \in \operatorname{span}\{v_1,\ldots,v_m\}$.

3. לכל $f,g \in F[x]$, אזי $f \mid g$ בחוג $F[x]$ אם ורק אם $f \mid g$ בחוג $K[x]$.

4. אם $h,f,g \in F[x]$ אזי $h = \gcd(f,g)$ מעל F אם ורק אם $h = \gcd(f,g)$ מעל K.

כל הטענות הללו הן טענות על דברים שניתן לבדוק אלגוריתמית - דירוג מטריצה, חילוק עם שארית. באלגוריתמים אלה מפעילים רק חיבור וכפל עם סקלרים בשדות.