נכתב על ידי יהונתן רגב

הגדרה

מטריצה $\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A_s \end{pmatrix}$, כש - $A_1, A_2, \cdots, A_s$ מטריצות ריבועיות, נקראת **מטריצה אלכסונית בלוקים**.

משפט

תהי A מטריצה אלכסונית בלוקים. יהיו $p_1(x), p_2(x), \cdots, p_s(x)$ פולינומים אופייניים של$A_1, \cdots, A_s$ ו - $m_1(x), \cdots, m_s(x)$ פולינומים מינימליים שלהן.

אזי לפולינום האופייני $p_A(x)$ ולפולינום המינימלי $m_A(x)$ של A מתקיימים השוויונים הבאים:

1. $p_A(x) = p_1(x) \cdots p_s(x)$.
2. $m_A(x) = l.c.m(m_1(x), \cdots, m_s(x))$.

הוכחה

.1

$$p_A(x) = \det(x \cdot I - A) = \det \begin{pmatrix} x \cdot I - A_1 & 0 & \cdots & 0 \\ 0 & \mathrm{x \cdot I - A_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & x \cdot I - A_s \end{pmatrix}$$

$$p_A(x) = \det(x \cdot I - A_1) \cdots \det(x \cdot I - A_s) = p_1(x) \cdots p_s(x)$$

.2

$$g(x) = l.c.m(m_1(x), \cdots, m_s(x))$$

$g(x)$, לפי ההגדרה מקיים את התכונות הבאות:

- $m_i(x) | g(x)$ לכל $1 \le i \le s$.
- אם $h(x)$ פולינום אחר כך ש - $m_i(x) | h(x)$ לכל $1 \le i \le s$ אזי: $g(x) | h(x)$.
- $g(x)$ פולינום מתוקן.

נרצה להוכיח כי ש - $m_A(x) = g(x)$.

נוכיח שמתקיים: $m_A(x) | g(x)$ וגם $g(x) | m_A(x)$.

1. אם $f(x)$ פולינום כשלהו, אזי $f(x)$ מאפס למטריצה A אוי"א $f(x)$ מאפס לכל אחת מהמטריצות $A_1, \cdots, A_s$.
   הוכחה:

$$f(A) = \begin{pmatrix} f(A_1) & 0 & \cdots & 0 \\ 0 & f(A_2) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & f(A_s) \end{pmatrix}$$

נכתב על ידי יהונתן רגב

(דורש הוכחה, אך נובע מהעובדה שחישוב הפולינום $f(A)$ מהווה שילוב של פעולות כפל מטריצות, כפל מטריצה בסקלר וחיבור מטריצות, וכל אחת מהפעולות הנ"ל הולכת בלוק בלוק).

לכן: $f(A) = 0 \leftrightarrow f(A_i)$ לכל $1 \leq i \leq s$.

2. $g(A_i)$ לכל $1 \leq i \leq s$.

הוכחה: $m_i(x)|g(x)$ ז"א $g(x) = m_i(x) \cdot h(x)$, ולכן:

$$g(A_i) = m_i(A_i) \cdot h(A_i) = 0 \cdot h(A_i) = 0.$$

3. $g(A) = 0$.

הוכחה: נובע מסעיפים 1 ו – 2.

4. $m_A(x)|g(x)$.

הוכחה: נובע מסעיף 3 ומהמשפט שאומר שכל פולינום מאפס מתחלק בפולינום המינימלי.

5. $m_A(A_i) = 0$.

הוכחה: נובע מסעיף 1 ומההגדרה של הפולינום המינימלי.

6. $m_{A_i}(x)|m_A(x)$ לכל $1 \leq i \leq s$.

הוכחה: נובע מסעיף 5 ומהמשפט שאומר שכל פולינום מאפס מתחלק בפולינום המינימלי.

7. $g(x)|m_A(x)$.

הוכחה: עפ"י סעיף 6, $m_A(x)$ הינו כפולה משותפת של $m_1(x),\cdots,m_s(x)$. לפי ההגדרה של $l.c.m$, מתקיים: $g(x)|m_A(x)$.

8. $m_A(x) = g(x)$.

הוכחה: נובע מסעיפים 4 ו - 7.

בסה"כ: $m_A(x) = lcm(m_1(x), \cdots, m_s(x))$.

■

עובדות נוספות על פירוק פולינומים

חוג פולינומים

יהי $\mathbb{K}$ שדה ויהי $\mathcal{R} = \mathbb{K}[x]$ חוג פולינומים (נתבונן בשתי פעולות חיבור, $\oplus$, וכפל, $\otimes$) במשתנה אחד.

הערה

האיברים ההפיכים ב - $\mathcal{R}$ הינם פולינומים קבועים (שונים מאפס) (כלומר, חוג דומה לשדה, פרט לתכונה לפיה לכל איבר שונה מאפס קיים איבר הופכי).

הוכחה

אם f הפיך, אזי קיים פולינום g כך ש - $f \cdot g = 1$.

$$\deg(f \cdot g) = \deg(1) = 0$$

$$\deg(f \cdot g) = \deg(f) + \deg(g) = 0$$

$$\Downarrow$$

$$\deg(f) = 0$$

הערה

ב - $\mathcal{R} = \mathbb{K}[\mathrm{x}]$ אין מחלקי אפס (כלומר, אם $f \neq 0, g \neq 0$, אזי $f \cdot g = 0$).

הגדרה

יהי f פולינום לא הפיך.

אומרים ש $f -$ **פריק** אם קיימים g, h, שניהם לא הפיכים, כך ש - $f = g \cdot h$. אחרת, אומרים

ש $f -$ **פולינום אי פריק.**

עובדה

כל פולינום מתפרק למכפלה של פולינומים אי פריקים, והצגה זו יחידה, במובן הבא: לכל פולינום f קיימת הצגה בצורה $f = u \cdot g_1 \cdots g_n$, כך ש $u -$ פולינום הפיך (פולינום קבוע עפ"י ההערה לעיל) ו - $g_1, \cdots, g_n$, ואם $f = u' \cdot h_1 \cdots h_m$ הצגה נוספת (u' הפיך ו $h_1, \cdots, h_m -$ אי פריקים), אזי: $n = m$ ומתקיים $g_i = h_i$ (עד כדי שינוי סדר של גורמים).

הערה

קיימים חוגים שתכונה זו ("המשפט היסודי של האריתמטיקה"=פירוק יחיד לאי פריקים) אינו מתקיים.

נתבונן בחוג $\mathcal{S} = \{\mathrm{a} + \mathrm{b} \cdot \sqrt{-5} | a, b \in \mathbb{Z}\}$. ניתן להוכיח שב $\mathcal{S} -$ אין פירוק יחיד לאי פריקים.
דוגמה: $9 = 3 \cdot 3 = \left(2 + \sqrt{-5}\right) \cdot (2 - \sqrt{-5})$.