**תזכורת**

 אם $p|a⋅b$, ו – $p$ אי פריק, אזי: $p|a$ או $p|b$.

**משפט**

לפולינומים במשתנה אחד מעל שדה, מתקיים פירוק יחיד. ז"א, אם:

$f=p\_{1}\cdots p\_{m}=q\_{1}\cdots q\_{n}$ כש - $p\_{1},\cdots ,p\_{m}$, $q\_{1},\cdots ,q\_{n}$ פולינומים אי פריקים, אזי $m=n$ ולכל $i$, $p\_{i}=q\_{i}$ (עד כדי כפל בקבוע ושינוי סדר של גורמים).

**הוכחה**

* בעזרת אינדוקציה, ניתן להוכיח שאם $p|a\_{1}\cdots a\_{n}$, $p$ אי פריק, אז $p\left|a\_{1} ∨\cdots ∨p\right|a\_{n}$.
* את טענת המשפט נוכיח בערת אינדוקציה על מספר הגורמים.

בסיס: טריוויאלי.

צעד: נניח נכונות הטענה עבור $m$ גורמים, כלומר פירוק יחיד של: $f=p\_{1}\cdots p\_{m}$.

נוכיח נכונות הטענה עבור $(m+1)$ גורמים, כלומר פירוק יחיד של:

 $f=p\_{1}\cdots p\_{m}⋅p\_{m+1}=q\_{1}\cdots q\_{n}⋅q\_{n+1}$.

נתבונן ב - $p\_{m+1}$. זהו פולינום אי פריק, $p\_{m+1}|f=q\_{1}\cdots q\_{n}⋅q\_{n+1}$. לכן, לפי הצעד הראשון של ההוכחה, $p\_{m+1}$ מחלק לפחות אחד מהפולינומים $q\_{j}$.

למשל, $p\_{m+1}|q\_{n+1}$. שניהם אי פריקים, לכן הם פרופורציונאליים, ז"א, עד כדי כפל בפולינום קבוע, מתקיים: $p\_{m+1}=q\_{n+1}$, לכן:

$f=p\_{1}\cdots p\_{m}⋅p\_{m+1}=q\_{1}\cdots q\_{n}⋅q\_{n+1}$.

אבל, בחוג $R=F[x]$, מתקיים חוק הצמום: אם $f⋅h=g⋅h,f, g,h\ne 0$, אזי

$f=g$ .

[נימוק: $f⋅h=g⋅h\rightarrow f⋅h-g⋅h=0\rightarrow \left(f-g\right)⋅h=0\rightarrow f-g=0\rightarrow f=g$].

לאחר הצמצום ב - $p\_{m+1}$, נקבל: $f=p\_{1}\cdots p\_{m}=q\_{1}\cdots q\_{n}$, ולפי הנחת האינדוקציה

$p\_{i}=q\_{j}$ עד כדי שינוי סדר של גורמים וכפל בקבוע.
 $∎ $

**הערה**

בעזרת פירוק יחיד, ניתן לנמק את הטענה הבאה: כל השורשים של הפולינום המינימלי של מטריצה $A$, הם הערכים העצמיים של $A$.

$m\_{A}\left(x\right)\left|p\_{A}\left(x\right)\right|\left[m\_{A}\left(x\right)\right]^{n}$. $p\_{A}\left(x\right)=\left(x-λ\_{1}\right)^{k\_{1}}\cdots \left(x-λ\_{s}\right)^{k\_{s}}$ (בהנחה שהפולינום האופייני מתפרק לגורמים לינאריים), ובשימוש בפירוק היחיד: $m\_{A}\left(x\right)=\left(x-λ\_{1}\right)^{d\_{1}}\cdots \left(x-λ\_{s}\right)^{d\_{s}}$.

**הערה**

אם $F=C$, אי הפולינומים האי פריקים הם פולינומים לינאריים בלבד.

**הערה**

אם $F=R$, אזי הפולינומים האי פריקים הם פולינומים לינאריים או פולינומים ריבועיים (ממעלה 2) בלבד.

**נימוק**

אם $f\in R[x]$ ואם $α\in C,α\notin R$ שורש של $f$, אזי גם $\tilde{α}$ הוא גם שורש של $f$.

**הערה**

אם $F=Q$ או $F$ שדה סופי, אזי קיימים אינסוף פולינומים אי פריקים, ויש פולינומים אי פריקים ממעלה כלשהי.

**צורת ז'ורדן**

**משפט (ז'ורדן)**

תהי $A\_{n×n}$ מטריצה ריבועית. נניח שהפולינום האופייני $p\_{A}(x)$ מתפרק למכפלה של גורמים לינאריים. אזי $A$ דומה למטריצה $J$ בצורה הבאה:

 $J=\left(\begin{matrix}J\_{n\_{1}}(λ\_{1})&0&\cdots &\cdots &0\\0&\ddots &\ddots &\ddots &\vdots \\\vdots &\ddots &\ddots &\ddots &\vdots \\\vdots &\ddots &\ddots &\ddots &0\\0&\cdots & \cdots &0&J\_{n\_{t}}\left(λ\_{t}\right)\end{matrix}\right)$. כשכל בלוק $J\_{n\_{i}}(λ\_{i})$ הוא תא ז'ורדן, כלומר:

$\left(\begin{matrix}λ\_{i}&1&0&\cdots &0\\0&\ddots &\ddots &\ddots &\vdots \\\vdots &\ddots &\ddots &\ddots &0\\\vdots &\ddots &\ddots &\ddots &1\\0&\cdots &\cdots &0&λ\_{i}\end{matrix}\right)\_{n\_{i}×n\_{i}}$ ($n\_{i}\geq 1$ , $λ\_{i}$ לא בהכרח שונים אחד מהשני).

בנוסף, המטריצה $J$ היא יחידה (עד כדי סדר של הבלוקים).

ל – $J$ קוראים צורת ז'ורדן של $A$.

**משפט**

אם $T:V\rightarrow V$ אופרטור לינארי כך ש - $p\_{T}(x)$ מתפרק למכפלה של גורמים לינאריים. אזי, קיים בסיס של $B$ כך שהמטריצה המייצגת $A=\left[T\right]\_{B}$ היא מטריצת ז'ורדן $J$. קוראים ל - $B$ בסיס מז'רדן. $J$ יחידה עד כדי שינוי סדר הבלוקים.

**מסקנה**

תהי $J$ צורת הז'ודרן של מטריצה $A$. נניח ש – $p\_{A}(x)$ מתפרק לגורמים לינאריים. נסמן $λ\_{1},\cdots ,λ\_{s}$ כל הערכים העצמיים השונים של $A$. אזי:

1. לכל $A\_{i}$, הריבוי האלגברי שלו $k\_{i}$ שווה לסכום הגדלים של כל הבלוקים המכילים את $λ\_{i}$.

$]$מזה נקבל: $[p\_{A}\left(x\right)=\left(x-λ\_{1}\right)^{k\_{1}}\cdots \left(x-λ\_{s}\right)^{k\_{s}}$.

1. לכל $A\_{i}$, הריבוי הגיאומטרי שלו $m\_{i}$ שווה למספר הבלוקים המכילים את $λ\_{i}$.
2. לפולינום המינימלי $m\_{A}(x)$ מתקיים: $m\_{A}\left(x\right)=\left(x-λ\_{1}\right)^{d\_{1}}\cdots \left(x-λ\_{s}\right)^{d\_{s}}$, כש - $d\_{i}$ הינו הגודל המקסימלי של הבלוק המכיל את $λ\_{i}$.

 **נימוק**

$m\_{A}\left(x\right)=m\_{J}\left(x\right)=l.c.m(m\_{n\_{1}}\left(x\right),\cdots ,m\_{n\_{t}}\left(x\right))$, ולכל בלוק ז'ורדן $m\_{J\_{n\_{i}}}\left(x\right)=\left(x-λ\_{i}\right)^{n\_{i}}$.

1. $A$ *לכסינה אם ורק אם* $m\_{A}\left(x\right)=\left(x-λ\_{1}\right)\cdots (x-λ\_{s})$*.*

**דוגמה**

נתבונן בשתי מטריצות $7×7$.

$$A=\left(\begin{matrix}λ&1&0|&0&0&0&0\\0&λ&1|&0&0&0&0\\0&0&λ|&0&0&0&0\\0&0&0&λ&1|&0&0\\0&0&0&0&λ|&0&0\\0&0&0&0&0&λ&1|\\0&0&0&0&0&0&λ|\end{matrix}\right)$$

$$A'=\left(\begin{matrix}λ&1&0|&0&0&0&0\\0&λ&1|&0&0&0&0\\0&0&λ|&0&0&0&0\\0&0&0&λ&1&0|&0\\0&0&0&0&λ&1|&0\\0&0&0&0&0&λ|&0\\0&0&0&0&0&0&λ|\end{matrix}\right)$$

$A≄ A'$, מיחידות צורת ז'ורדן. מתקיים:

1. $p\_{A}\left(x\right)=\left(x-λ\right)^{7}=p\_{A^{'}}(x)$
2. $m\_{A}\left(x\right)=\left(x-λ\right)^{3}=m\_{A^{'}}(x)$
3. $k\_{λ}=7$.
4. $m\_{λ}=3$.