תזכורת: רשימה של פולינומים אי פריקים (מעל $\mathbb{R}$)

א) לכל λ ממשי $x-\lambda$

ב) לכל מספר מרוכב לא ממשי $\{\mu,\bar{\mu}\}$

ג) $x^2+bx+c=(x-\mu)(x-\bar{\mu})$

כאשר $b=-(\mu+\bar{\mu}),\ c=|\mu|^2$ ואז $b^2-4ac<0$.

מקבלים שלכל $0\neq f(x)\in\mathbb{R}[x]$ יש פירוק מהצורה הבאה והפירוק הזה יחיד עד כדי סדר הגורמים:

$$f(x)=a_n(x-\lambda_1)^{n_1}\cdots(x-\lambda_k)^{n_k}(x^2+b_1x+c_1)^{l_1}\cdots(x^2+b_hx+c_h)^{l_h}$$

כאן $\lambda_1,\dots,\lambda_k$ הם השורשים הממשיים השונים (כי זה פירוק).

ואם נפרק $(x-\mu_j)(x-\bar{\mu}_j)=x^2+b_jx+c_j$ אז $\mu_1,\bar{\mu}_1,\dots,\mu_h,\bar{\mu}_h$ הם השורשים ב- $\mathbb{C}\setminus\mathbb{R}$ ומקבלים את הפירוק ב- $\mathbb{C}[x]$: $f(x)=a_n(x-\lambda_1)^{n_1}\cdots(x-\lambda_k)^{n_k}(x-\mu_1)^{l_1}(x-\bar{\mu}_1)^{l_1}\cdots$

וכל המקדמים בפירוק שונים זה מזה כי הפולינומים שונים ולכן גם השורשים שונים.

מסקנה: הריבוי של שורש מרוכב μ ב- $f(x)$ שווה לריבוי השורש המרוכב הצמוד לו ב- $f(x)$.

הערות לגבי אי פריקות ושורשים

(1) אם $p(x)\in\mathbb{F}[x]$ אי פריק ומדרגה גדולה מ-1 אז אין לו שורשים. אחרת היינו מקבלים פירוק מהצורה $p(x)=(x-\lambda)\underbrace{g(x)}_{\text{לא הפיך}}$.

(2) יתכן שפולינום חסר שורשים אך אינו אי-פריק. לדוגמא: x^4+1 לפי משפט הפירוק פולינום ממעלה 3 ומעלה תמיד פריק.

(3) אם $f(x)\in\mathbb{F}[x]$ מקיים $\deg f=2$ או $\deg f=3$ אז f אי פריק $\Leftrightarrow$ ל- f אין שורשים ב- $\mathbb{F}$. כי אם ל- f יש פירוק $f=f_1\cdot f_2$ אז המעלה של אחד הגורמים היא 1 (המעלה של אחד מהגורמים לפחות היא 1 ויש לו שורש) (הוא פירוק טריוויאלי, כלומר f_1,f_2 שניהם אינם הפיכים).

(4) יהי $f(x)\in\mathbb{F}[x]$ נסמן $\deg f=n$. נסמן ב- $\lambda_1,\dots,\lambda_k$ את השורשים השונים של f ב- $\mathbb{F}$. אז קיים פירוק יחיד מהצורה הבאה (עד כדי סדר):

$$f(x)=a_n(x-\lambda_1)^{n_1}\cdots(x-\lambda_k)^{n_k}p_1(x)^{m_1}\cdots p_h(x)^{m_h}$$

כאשר p_i פולינומים אי פריקים ממעלה גדולה מ-1.

מסקנות

(א) משפט: לפולינום ממעלה $n\geq 0$ $f(x)\in\mathbb{F}[x]$ יש לכל היותר n שורשים ב- $\mathbb{F}[x]$.

(ב) סכום הריבויים של כל שורשי f $=n_1+\dots+n_k\leq n$ (מעלת f) וקיים שוויון $\Leftrightarrow$ f מתפצל (מעל $\mathbb{F}$). (ישנו סכום התפצלות).

נושא - שורשים של פולינום עם מקדמים **שלמים**

נניח $f(x)=a_nx^n+\dots+a_1x+a_0$ ו- a_i שלמים. אם $x=\frac{r}{s}$ שורש (רציונלי)

(ב.ה.כ) $f(\frac{r}{s})=0$ אז ע"י הכפלה נקבל $a_nr^n+a_{n-1}r^{n-1}s+\dots+a_1rs^{n-1}+a_0s^n=0$

אז מכאן של r ו- s אין גורמים משותפים אז s מחלק את a_n (בפרט אם $a_n=1$ השורש הוא שלם) וכן r מחלק את a_0.

אידאלים

בחוג, אידאל הוא מושג מקביל למושג תת-מרחב [illegible] - אם כופלים באיבר, יוצא מכפלה שנמצאת באידאל.

הגדרה - קבוצה $\emptyset\neq I\subset\mathbb{F}[x]$ נקראת אידאל אם מקיימת התנאי הבא:

$$g_1,\dots,g_n\in I,\ f_1,f_2,\dots,f_n\in\mathbb{F}[x]\Rightarrow f_1g_1+\dots+f_ng_n\in I.$$

וזה כקומבינציה לינארית של פולינומים, אך המקדמים לא נלקחים מהשדה אלא מהחוג.

באופן שקול ניתן לבדוק את 2 התנאים הבאים:

① $g_1,g_2\in I\Rightarrow g_1+g_2\in I$

② $p\in\mathbb{F}[x],\ g\in I\Rightarrow p\cdot g\in I$

מסקנה- יהי $I \subset \mathbb{F}[x]$ אידאל אז $g=gcd(I)$ מתוקן יחיד כך ש g המתוקן היחיד כך: $I = g\cdot\mathbb{F}[x] = (g) = \{f(x)g(x) \mid f\in\mathbb{F}[x]\} = \{\text{אוסף כל הפולינומים שמתחלקים ב } g\}$
(2 סימונים)

במקרה של פולינומים אידאל הוא די מקוצר! gcd, נקרא לו gcd, אבל כן יש הבדל.

<u>הוכחה</u>: <u>יחידות</u> - נובע מתכונת ההתחלקות ⇐ אם g_1 פולינום מתוקן המקיים הנדרש אז g מחלק את g_1 ו g_1 מחלק את g ושניהם מתוקנים אז $g=g_1$.

נסמן $g=gcd(I)$ אז ברור ש g מתוקן. מתכונת האידאל I ומתכונת gcd נראה $g\in I$ כי $g=f_1q_1+\dots+f_nq_n$ ושגם g אידאל אז $g_i\cdot f_i\in I$ מתכונת האידאל. ומן כל פולינום $p\in\mathbb{F}[x]$ מקיים $g\cdot p\in I$ ולכן נקבל $g\cdot\mathbb{F}[x]\subset I$. מצד שני מאחר ש $g=gcd(I)$ נקבל ש g מחלק את כל איברי I ולכן $I\subset g\cdot\mathbb{F}[x]$. מכאן נקבל $I=g\cdot\mathbb{F}[x]$

מינוח- g נקרא פולינום היוצר המתוקן של I.

הערה- מאור הסוגה $\mathbb{F}[x]$ נקרא <u>בתחום בקורס PID = Principle ideal domain</u>.

<u>פולינומים ויישומים של אידאלים</u>

(1) <u>פולינום שמאפס (מינימלי) של המטריצה</u> -

משפט- תהי $A\in M_n(\mathbb{F})$ אז קיים פולינום מתוקן יחיד $M_A(x)=M_A\in\mathbb{F}[x]$ בעל התכונה $q(A)=0 \Leftrightarrow q(x)$ מתחלק ב-$M_A(x)$ $\forall(q\in\mathbb{F}[x])$. ובנוסף $\deg M_A\geq 1$
ברור ש $M_A(A)=0$ כי הוא מחלק את עצמו. לכן הפולינום הזה מאפס את המטריצה אם ורק אם הוא נכפלה שלו.

הוכחה-
<u>יחידות</u> נניח שקיימים פולינום מתוקן ע"י מתוקנים. התנאי והסימטריה שהוא מתוקן קובע את מחלקי הפולינום, לכן הוא יחיד. לפורמלי נניח ש $\tilde{M}$ עוד פולינום מתוקן כך ש $q(A)=0 \Leftrightarrow q(x)$ מתחלק ב- $\tilde{M}$ $\forall q\in\mathbb{F}[x]$. אז $M_A(A)=0$ כי M_A מחלק את עצמו ⟸ M_A מתחלק ב $\tilde{M}$ ובנוסף $\tilde{M}(A)=0$ כי $\tilde{M}$ מחלק את עצמו ⟸ $\tilde{M}$ מתחלק ב M_A. מכאן $\tilde{M}\sim M_A$ אך שניהם מתוקנים אז $M_A=\tilde{M}$

<u>קיום</u>: נסמן $I_A=\{q(x)\in\mathbb{F}[x] \mid q(A)=0\}$ מכיון ש $0\in I_A$ אז I_A קבוצה לא ריקה ברור ש I_A אידאל. יהי $M_A=gcd(I_A)$ היוצר המתוקן של האידאל I_A אז לכל פולינום $k(x)\in\mathbb{F}[x]$ מתקיים $k(A)=0 \Leftrightarrow k\in I_A=M_A(x)\cdot\mathbb{F}[x] \Leftrightarrow k$ מתחלק ב M_A
לכן הוא מאפס את המטריצה אם ורק אם הוא מחלק את היוצר המתוקן.
מהמשפט כאיוש בשיעור הראשון קיים פולינום $q(x)\neq 0$ כך ש $q(A)=0$ לכן $I_A\neq 0$ וזה אומר $M_A\neq 0$ מכיון $\deg M_A\geq 0$ (כי פולינום האפס).
אילו הוא היה קבוע ($\deg M_A=0$) אז (מתוקנות שונה מ-0) נקבל $M_A(A)=C(A)=CI$ בסתירה ל $M(A)=0$, לכן $\deg M_A\geq 1$ $[(\sum c_ix^i)(A)=\sum c_iA^i]$
למשל עבור מטריצת האפס הפולינום המינימלי הוא x וזה אומר המטריצה A היא מטריצת האפס אם הפולינום המינימלי שלה הוא x.

דוגמא: פולינום מינימלי של בלוק ז'ורדן

$$M_n(\mathbb{F})\ni J_n(\lambda)=\begin{pmatrix}\lambda & 1 & 0 & \dots & 0\\ 0 & \lambda & 1 & 0 & \dots\\ 0 & 0 & \lambda & 1 & \\ & & & \ddots & \\ 0 & \dots & & 0 & \lambda\end{pmatrix}=\lambda I+N \quad , \quad N=\underbrace{\begin{pmatrix}0 & 1 & 0 & \dots & 0\\ 0 & 0 & 1 & & \vdots\\ 0 & 0 & 0 & 1 & \\ & & & \ddots & 0\\ 0 & \dots & & & 1\\ 0 & \dots & & \dots & 0\end{pmatrix}}_{n\times n}$$

$$(x-\lambda)^n(J_n(\lambda))=(J_n(\lambda)-\lambda I)^n=N^n=0$$

לכן $M_{J_n(\lambda)}(x)$ מחלק את $(x-\lambda)^n$ לכן $M_{J_n(\lambda)}(x)=(x-\lambda)^k$ כאשר $1\leq k\leq n$
(מתוך הפולינום המינימלי לפחות 1)

כעת
$$(x-\lambda)^k(J_n(\lambda))=N^k=\begin{pmatrix}\overbrace{0 & \dots & 0}^{k\text{ אפסים}} & 1 & \dots & 0\\ 0 & \dots & & 0 & 1 & \\ \vdots & & & \ddots & & \\ & & & & & 0\\ 0 & \dots & & & & 0\end{pmatrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} k \text{ אפסים}$$

כך ש $M_{J}(x)$ לא מחלק את $(x-\lambda)^{n-1}$ מסקנה- הפולינום המינימלי $M_{J_n(\lambda)}(x)=(x-\lambda)^n$

(2) כפולה משותפת מזערית $l.c.m$

הגדרה- תהי $\emptyset \neq S \subset \mathbb{F}[x]$

נסמן: $I_s = \{$ אוסף כל הפולינומים שמתחלקים בכל איברי S $\}$

אז $0 \in I_s$ (כי 0 מתחלק בכל דבר) לכן $I_s \neq \emptyset$ ונראה ש- I_s אידיאל לפי ההגדרה.

נגדיר $l(x) = l.c.m(S) = g.c.d(I_s)$

תכונות $l(x)$

א) $l(x)$ מתוקן

ב) לכל פולינום $q(x) \in \mathbb{F}[x]$ מתקיים: $q(x)$ מתחלק בכל איברי S $\iff$ $q(x)$ מתחלק ב- $l(x)$

(כי זה בדיוק $q(x) \in I_s \equiv$ מתחלק ב- $l(x)$)

ג) $l(x)$ הוא יחיד כי אם $l_1(x)$ מתחלק ב- $l_2(x)$ ולהיפך ושניהם מתוקנים אז $l_1(x) = l_2(x)$.

תכונות אלו מאפיינות את $l = l.c.m$ באופן יחיד ומספיק מתחלק בכל איברי S.

תיאור $g.cd$ ו- $l.cm$ בעזרת פירוק

א) דוגמא- נתונים פולינומים מתוקנים

$$f_1 = p_1^7 \cdot p_2^2 \cdot p_3^5 \cdot p_4^6$$
$$f_2 = p_2^8 \cdot p_3 \cdot p_4 \cdot p_5$$
$$f_3 = p_1^2 \cdot p_2^3 \cdot p_3^3 \cdot p_5^4$$

כאשר p_i פולינומים אי פריקים מתוקנים שונים זה מזה.

מקבל את כל הפולינומים המשותפים בחזקה המינימלית.
$$gcd(f_1, f_2, f_3) = p_2^2 \cdot p_3^3$$

כאן מקבלים את מקסימום הרכיבים בחזקה המקסימלית.
$$lcm(f_1, f_2, f_3) = p_1^7 \cdot p_2^8 \cdot p_3^5 \cdot p_4^6 \cdot p_5^4$$

ב) באופן כללי- יהיו $f_1, \dots, f_t \neq 0$ פולינומים ותהי $p_1, \dots, p_k$ רשימת הגורמים האי פריקים המופיעים בפירוק אחד או יותר מ- $f_1, \dots, f_t$ (ללא כפילויות) אז נוכל לרשום פירוקים (כאשר c_i מקדם ראשי של f_i)

$$f_i = c_i\, p_1^{n_{i1}} \cdots p_k^{n_{ik}}$$

(*כאשר p_j לא מופיע בפירוק $n_{ij} = 0$)

כאשר $0 \leq n_{ij}$, $n_{ij} = V(f_i, p_j)$ (הערכה) וכאשר $n_{ij} = 0$ = הפולינום אינו גורם של f_i.

$$gcd(f_1, \dots, f_t) = p_1^{\min\{n_{11}, \dots, n_{1k}\}} \cdots p_k^{\min\{n_{k1}, \dots, n_{kk}\}}$$
$$lcm(f_1, \dots, f_t) = p_1^{\max\{n_{11}, \dots, n_{1k}\}} \cdots p_k^{\max\{n_{k1}, \dots, n_{kk}\}}$$

וזהו תיאור תאורטי משום שמציאת פירוק זה קשה.

ג) מסקנה-
$$lcm(f_1, f_2) = \frac{f_1 \cdot f_2}{gcd(f_1, f_2)}$$

לכמה מספר פולינומים (נשתמש באינדוקציה):
$$lcm(f_1, \dots, f_t) = lcm(lcm(f_1, \dots, f_{t-1}), f_t)$$
וזה נובע מתכונות א', ב' (כמו ב- $g.c.d$).

יישום של $l.c.m$ - חישוב הפולינום המינימלי של מטריצה בלוק אלכסונית

נניח $A_1, \dots, A_k$ מטריצות ריבועיות מעל $\mathbb{F}$ (לאו דווקא מאותו סדר)

נסמן כאשר A_i מטריצה.

$$A_1 \oplus \dots \oplus A_k = diag(A_1, \dots, A_k) = A = \begin{pmatrix} A_1 & 0 & 0 & \\ 0 & A_2 & 0 & \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & & A_k \end{pmatrix}$$

אזי ראינו ש- $q\in F[x]$. $q(A)=\begin{pmatrix} q(A_1) & & & 0 \\ 0 & q(A_2) & & \\ 0 & 0 & \ddots & 0 \\ 0 & & & q(A_k)\end{pmatrix}$

q מתאפס ב M_A $\longleftrightarrow$ $q(A)=0$ $\longleftrightarrow$ $\forall_{1\le i\le k}\, q(A_i)=0$ $\longleftrightarrow$ q מתאפס ע"י כל אחד מ $M_{A_1}\dots M_{A_k}$

מכאן שq מתאפס ב $lcm(M_{A_1},\dots,M_{A_k})$ (הכפולה המינימלית המשותפת).

<u>מסקנה:</u> $M_A = lcm(M_{A_1},\dots,M_{A_k})$

דוגמא- נמצא את M_J עבור

$$J=\begin{pmatrix} 2 & & & & & & & & \\ & 2 & 1 & & & & & & \\ & & 2 & & & & & & \\ & & & 2 & 1 & & & & \\ & & & & 2 & 1 & & & \\ & & & & & 2 & & & \\ & & & & & & 5 & 1 & \\ & & & & & & & 5 & \\ & & & & & & & & 7 \end{pmatrix}$$

$M_J = lcm(x-2,(x-2)^2,(x-2)^3,(x-5)^2,(x-7))$

$M_J = (x-2)^3(x-5)^2(x-7)$

והפולינום הזה לא חלק כי שורשיו כמה מהם יש מכל סוג של שורש זוגי.

<u>אפיון פולינומים זרים בזוגות ע"י משוואה</u>

<u>הגדרה:</u> $q_1,\dots,q_n\in F[x]$ $(n\ge 2)$ נקראים זרים בזוגות אם לכל $i\ne j$, p_i, p_j זרים כלומר אם $\forall i,j.\ gcd(p_i,p_j)=1$.

<u>משפט</u>- יהיו $q_1,\dots,q_n\in F[x]$ $(n\ge 2)$ אזי $q_1,\dots,q_n$ זרים בזוגות אם"ם קיימים פולינומים $f_1,\dots,f_n\in F[x]$ כך ש $\sum_{i=1}^{n} f_i\cdot q_1\cdots\hat{q}_i\cdots q_n$

<u>תזכורת:</u>
* $\hat{q}_i$ - הפולינום הזה מושמט מהמכפלה

<u>סימון</u>- $q_1\cdots\hat{q}_i\cdots q_n=\begin{cases} q_2q_3\cdots q_n & i=1\\ q_1\cdots q_{i-1}q_{i+1}\cdots q_n & 1<i<n\\ q_1\cdots q_{n-1} & i=n\end{cases}$

הוכחה- מספר שורש של פולינום $q_1,\dots,q_n$ שורשים. אי פריקים נותנים ש- $q_1,\dots,q_n$ זרים בזוגות $\longleftrightarrow$ כל פולינום אי פריק p מופיע לכל היותר <u>באחד</u> מבין $q_1\dots q_n$ $\longleftrightarrow$ הפולינומים $q_1\cdots\hat{q}_i\cdots q_n$ $i=(1,\dots,n)$ זרים $\longleftrightarrow$ קיימים $f_1,\dots,f_n$ המקיימים את התנאי שבצורה.

כלומר נתאר פולינומים זרים בזוגות ע"י צירוף של הכפל פולינומים.