

lienarit גז - אלי להר edition

שר פַּרְצָן

19 בינואר 2026

איפה הינו ומה עשו? סימנו ב- $[x]$ את קבועות על הפולינומים על מקסימים ב- \mathbb{F} , ואמרנו שאחננו יכולים להציב בפולינום מטריצה, כלומר לכל $A \in M_n(\mathbb{F})$, בהינתן p עם מקדמים $a_0 \dots a_n$, יש לנו את העתקת החבזה φ שמסכפלת את הפולינום כך:

$$\begin{pmatrix} a_0 \\ \vdots \\ a_n \\ 0 \\ \vdots \end{pmatrix}^T \cdot \begin{pmatrix} I \\ A \\ A^2 \\ \vdots \end{pmatrix}$$

הפונקציה זו φ_A , שŁוקחת פולינום ומסכפלת את מקדמיו עם $-A^{-i}$. כלומר: $\varphi_A(p+q) = p(A) + q(A) = \varphi_A(p) + \varphi_A(q)$. כלומר: תחומר קבוצת כל הפולינומים. וכך על היותה לינארית, היא כפלייה:

$$\varphi_A(tp) = (tp)(A) = t \cdot p(A) = t \cdot \varphi_A()$$

$$\varphi_A(pq) = (pq)(A) = p(A)q(A) = \varphi_A(p)\varphi_A(q)$$

עתה נדבר על הגרעין, שעליו לא ממש דיברנו. זו קבוצה שמכילה את הפולינומים שמאפסים את A . היא מ"ו שסגור לכפּל (מודול או משוה זהה). אפשר להגיד יותר – היא אידאל ב- $\mathbb{F}[x]$! אם $\varphi_A \in \ker \varphi_A$ ו- $[q] \in \mathbb{F}[x] p \in \ker \varphi_A$ אז $\varphi_A(pq) = \varphi_A(p)\varphi_A(q) = 0$. לעיתים מסמנים (סימן בלאטן שאין לא מכיר).

ברור ש- φ_A לא ריקה, כי 0 בפנים. ברור שיש פולינומיים נספים שהמטריצה מאפסת, וזה לא אידאל טרוויאלי – לכל $A \in M_n(\mathbb{F})$ קיים $p \neq 0$ כך ש- $p(A) = 0$. למה? עוד לפני המילוטון, יוכל להסתכל על הסדרה:

$$(I, A, A^2, A^3 \dots A^{n^2})$$

זהו סדרה של מטריצות ב- $M_n(\mathbb{F})$. ידוע $\dim M_n(\mathbb{F}) = n^2$. לכן אם הסדרה כוללת $1 + n^2$ מטריצות, היא תלויות ליניארית. מכאן שקיימים a_0, \dots, a_{n^2+1} שלאחר סכול נוטנים את מטריצת ה-0. אפשר להסתכל על זה גם כעל $\sum_{i=0}^{1+n^2} a_i A^i = 0$. למה זה מוגןיב? כי לא ניתן φ_A העתקה מרובבת $[x] \mapsto \mathbb{F}[x]$ שהוא מיפוי אינסופי.

מכיוון שלמדו לנו אריתריה 2, הפולינום האופייני נמצא בגרען. מושפט כיילו המילטון $p_A(A)$, שכן $0 \in \ker \varphi_A$. זה קצת יותר חזק ממנו שקיבלו לנו בignumיקי ליניארייה 1 שלנו, שנותנו לנו פולינום ממעלה 1 $+ n^2$, ולא ממעלה n .

אבל אף אחד לא אמר שזו המעלה הקטנה ביותר של a . מכאן גם ש- $\{A^n\}$ ת"ל.

הטענה המרכזית שנרצה לטעון היא:

משפט 1. אם $I \triangleleft \mathbb{F}[X]$ אידאל בחוג הפולינומיים מעל \mathbb{F} , אז קיים $m \in \mathbb{F}$ כך ש- I נוצר על ידי m .

בשונן של חוגים, אומרים ש-*I* הוא אידאל ראשי – והוא נוצר ע"י כפולות של איבר יחיד בחוג. גם קבוצת המספרים הזוגיים היא אידאל ראשי ב-*Z*, שנוצרת ע"י 2. או-*2* – כאן נבחון שהיוצר של האידאל הראשי (בתחום ראשי), קיים ויחד עד לכדי חברות (כפל בהיפך).

טרמינולוגיה שאלינו להר לא משתמש בה אבל אני כן: $R' = \{rp \mid r \in R\}$ או ב- R' נוצר ע"י p תחתוג של R . אפשר לדבר גם על אידאל ימני ושמאלי בחוגים לא קומוטטיביים.

לא בכל חוג כל אידאל הוא אידאל ראשי. אפשר להסתכל על הקבוצה $[y][x]$ שכוללת את הקבוצה של $\{1, 2x - y^2, 3 - xy + y^3, -5x^2y\}$ וכן, שוכרים לה חוג הפולינומים בשני משתנים. אפשר לחשב עלייה כעל קבוצת הטנורים בשני משתנים או משהו צזה. נבחן שהינתן הפולינום x והפולינום y , והאידאל הנוצר על ידי $xR + yR' = xR + yR'$, אכן ראשי.

תחום ראשי הוא תחום שבו כל אידאל הוא אידאל ראשי. לדוגמה, חוג המספרים השלמים הוא אידאל ראשי. נתחיל מלהוכיח את שם את זה.

משפט 2. כל אידאל $\triangleleft I$ הוא ראשי

הוכחה. אם $\{0\} = I$ אז הוא נוצר ע"י 0 וסימנו. אם $0 \neq I$ אז יש בו... מספרים. בפרט, יש בו מספרים חיוביים (למה? כי אפשר לכפול $b - 1$). יש-li נורמה אוקלידית, אההמהמה סדר טוב, ולכן אני אוכל ל选取 $a < 0$ החובי הקטן ביותר שמנצ'א ב- I , ונסמן $I = a\mathbb{Z}$ (עכשו $I = a\mathbb{Z}$ גם אליו להר התחל להשתמש בסימון הזה), או בעברית, קבוצת הכפולות של a . הכיוון I טרויאלי מהגדרת I כאידאל (mbitach לכטם שאלי להר אמר "זה ברור" ואני לא מתנצל להעתיק). עתה נוכח $a\mathbb{Z} \subseteq I$. יהי $I \in a\mathbb{Z}$. נחקק את b ב- a עם שארית. נסמן (r) כאשר אמר "זה ברור" ואני לא מתנצל להעתיק). עתה נוכח $b = sa + r$, $s \in I$, $a \in I$, $r \in a\mathbb{Z}$. האידאל סגור לחישור $b = sa + r \leq r$, או $r = b - sa \in I$. $r = b - sa \in I$. האידאל סגור לחישור $b \in a\mathbb{Z}$ ונסמן $a - r < 0$, ו- a החובי הקטן באידאל, 0 . וסימנו $sa = b$, כלומר $b \in a\mathbb{Z}$.

ראנט שליל שלא קשור להרצאה. קצת משגע אותי שאליך להר על כל הקונספט של חברות בתורת החוגים. זה ממש מגניב ומשמעותי כדי לא לפרק למאנלטאפלים מקרים. ואפשר ככה לשחוט קצת משפטים ייחודיים, לא רק קיומיים. הרעיון הוא – מספרים כמו $-1, 1, -\mathbb{Z}$, או שורשי היחידה ב- \mathbb{C} , הוא הפולינומיים הקבועים ב- $\mathbb{F}[x]$, כפלו בהם "לא באמת משנה לי", וקוראים להם היפיכים. אומרים שניים מספרים הם "חברים" אם הם נבדלים בכפוף בהיפיך (ואז לדוגמה ב- \mathbb{Z} מתקיים $-4 \sim 4$ ביחס החבורות, וב- $\mathbb{F}[x]$ מתקיים $x \sim 2(x-1)$). והיחידות של היוצר של החוג, היא ייחידות עד לכדי חברות, כלומר גם 2 יוצרים את \mathbb{N}_{even} , ובאופן דומה לשאר החוגים. עתה נחזור להוכיח את המשפט שאומר שכל אידאל ב- \mathbb{F} הוא ראשי. זו תהיה ממש אותה ההוכחה כמו ב- \mathbb{Z} , רק שה"דבר שמודד גודל" (נורמה אוקלידית קוראים לויה) יהיה \deg במקומותUrף מוחלט.

הוכחה. אם $\{0\} = I$ היא קבוצת כל הכפולות של פולינום האפס, והוא נוצרת על-ידי. אם $\{0\} \neq I$ יהי $I \in m$ ממעלה מינימלית. נראת $I = m(x)\mathbb{F}[x]$. "אייה" כיוון הוא טרויאלי? זה $\subseteq m(x)\mathbb{F}[x] \subseteq m(x)$. בפרט, אם $I \in m$, אז I אידאל וסגור לכפוף בחוג (בליעה). מצד שני צריך להראות $m(x)\mathbb{F}[x] \subseteq m$. יהי $I \in m$, נחקק את p ב- m ונקבל $p(x) = s(x)m(x) + r(x)$ כאשר r שארית ממעלה מינימלית. ואז מסגרות לחיבור I והוא אידאל. ומאותם הנימוקים $0 \in p(x) - s(x)m(x) = r(x)$ כי m ממעלה חיובית מינימלית.

למי שורצ'ה את הגרסה הכי כללית של ההוכחה – תחפשו בוקיפדיה את ההוכחה שכל תחומי אוקלידיים הוא תחום ראשי. אי-לי אמר עד כדי חברות. אני עציו שמה. אבל הוא לא הסביר מה זה. אני אסביר. m המינימלי הזה, היחיד עד כדי כפוף בסקלר – מה? כי הפולינומיים הקבועים הם האיברים ההיפיכים שלו. אכן אליו טוען שהוא לא יכול לטען כי הוא לא הראה ייחידות עד כדי חברות, אבל m הוא הפולינום.

נסכם מה ראיינו לפני הפסקה: כל אידאל $\triangleleft I$ הוא ראשי (קבוצת כל הכפולות של פולינום $\mathbb{F}[x] \in m$, כאשר אם $0 \neq I$ אז $0 \neq m$ פולינום ממעלה מינימלית ב- I). נבחר את m , "הפולינום המינימלי", להיות הפולינום המתוקן המינימלי. לכל $A \in M_n(\mathbb{F})$, ראיינו $I_0(A)$ היא אידאל, וכך קיימים פולינומים מותוקן יחיד $m_A(x) = \ker \varphi_A$ והוא ממעלה מינימלית שיש לו התכונה הזו,

$$\forall q \in \mathbb{F}[x]: q(A) = 0 \implies m_A \mid q.$$

למעשה א' וב' שקולים.

למעשה, ראיינו איך מוצאים את m_A . אם גירדנו את A , ראיינו ש- $m_A = \prod_{i=1}^k (x - \lambda_i)^{k_i}$ גודל בלוק היג'ורדן הגדל ביוטר שמתאים לע"ע $\lambda_1, \dots, \lambda_k$, ו- λ_n לע"ע. בפרט, אם λ לע"ע של A , אז $\lambda \mid m_A$.

מה עושים עם הפולינום המינימלי בחיים? "לא הרבה, [...] אבל אפשר לעשות את הדברים הבאים" **משפט 3.** בהינתן $0 \neq a_0, a_1, \dots, a_n$, יהי $q(A) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$. אם $q(x) = 0$, אפשר להסיק ש- A הפיכה, ונitin לכתוב את ההופכית שלה כפולינום $(A - r)$ אשר r פולינום כלשהו.

הוכחה. בשיעורי הבית (אבל בשלבים)

נעשה דוגמה. נבחר:

$$q(x) = 2x^3 - 5x^2 + 7x - 9$$

ידוע $q(A) = 0$. מכאן:

$$2A^3 - 5A^2 + 7A = 9I \implies A \cdot \frac{1}{9} (2A^2 - 5A - 7I) = I$$

מפה אפשר לנתח את ההוכחה.

אפשר גם לנתח את הונקטראפושיטיב של הטענה: אם A אינה הפיכה, והיא מאפסת q כלשהו, האיבר החופשי של q הוא אפס. אפשר להוכיח את משפט הפירוק הפרימרי בעזרת פולינומים. תהי $A \in M_n(\mathbb{F})$ מטריצה עם פולינום אופיני מתפרק, כך ש- $= p_A(x) = \prod_{i=1}^r (x - \lambda_i)^{k_i}$

$$\mathcal{Z}_r^\times(A - \lambda_i I) = \mathcal{Z}_r((A - \lambda_i I)^{k_i}) \quad \mathbb{F}^n = \bigoplus \mathcal{Z}_r((A - \lambda_i I)^{k_i})$$

(כאשר $\ker \mathcal{Z}_r$ זה או \mathcal{N} אבל בסימוני אליו להר, ו- \mathcal{Z}_r^\times בקשר הזה הוא מ"ז עצמי מוכלל). "משפט הפירוק הפרימרי הוא דבילי בהינתן צורת ג'ירדן" – אם ($J_4(0)$ – אם $J_4(-2)$, $J_2(5)$, $J_2(5)$, $J_7(-2)$, $J_1(-2)$, $A \sim \text{diag}(J_3(5), J_2(5), J_2(5))$, 4 פעמים –, ומטריצה יחידה מגודל 4 לע"ע 0, ואז הפולינום האופייני (בכל "בלוק קטן" של מ"ז עצמי מוכלל, אחרי שנעה בחזקה 3 פעמים, כבר קיבל 0. משפט הפירוק הפרימרי אומר שאפשר לעשות את זה 8 פעמים, זה יותר חלש.

אני מצטער אם זה לא ברור – אליו לחר דבר המנו בעפ' עכשי, אבל מה שהוא אומר, להבנתי, הוא שמשפט הפירוק הפרימרי "די חלש" בגל שאנחנו לא באמת צריכים להעלות בחזקת k_i כדי לקבל את המ"ז העצמי המוכלל, מספיק להעלות בחזקת גודל הבלוק הכי קטן, כי זה כבר יאפס את החלק הרלוונטי. ביום חמישי נוכחים את משפט הפירוק הפרימרי מתכונות פולינומיים.

לאו נעלמו העתקות הלינאריות?

את כל הקורס עשינו על מטריצות. מה קורה עם העתקות לינאריות? בעיקר דיברנו על דברים כמו \mathbb{Z}_r (תמונה), $A\star$ (קרנל), $M_n(\mathbb{F})$, \mathbb{F}^n , משפט הממדים, ודברים כאלה. במקומות \mathbb{F}^n אפשר לדבר על מרחבים וקטורים כלליים. אנחנו בעצם התעסקנו בפונקציה הלינארית (האיזומורפיים) שעושה את זה:

$$V \mapsto \mathbb{F}^n \quad \text{Lin}(V \rightarrow V) \mapsto M_n(\mathbb{F}) \quad T(v) \mapsto Av \quad \ker T \mapsto \mathcal{Z}_r(A) \quad \text{Im } T \mapsto A\star$$

עכשו אליו לחר מציר את הדיאגרמה הקומוטטיבית של לינארית 1א. זה קצר חזרה ואני גם לא יודע לציר את זה בלאטך. עכשו הוא מראה איך מוצאים מטריצה לפי מטריצה מייצגת. זה די חומר של לינארית 1א, הדבר היחיד שחשוב לציין שambilינו הסימון $[T]_Q$ לא אומר הייצוג של T לפי הבסיס Q , אלא הייצוג של T לפי האיזומורפיים $\mathbb{R}^n \rightarrow \mathbb{R}^m$, כאשר הוא תלוי בסיס ולמעשה שווה ל- $[T]_{B'}[-]$. העתקת הייצוג לפי בסיס B כלהו. בכלל ש- B' ו- Q הם naturally isomorphic, זה סתם סימונו.