

לינארית 2א – אלי להר edition

שחר פרץ

19 בינואר 2026

איפה היינו ומה עשינו? סימנו ב- $\mathbb{F}[x]$ את קבוצת הפולינומים על מקסמים ב- \mathbb{F} , ואמרנו שאנחנו 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 ההצבה φ_A 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 הזו φ_A , שלוקחת פולינום ומסכפלת את מקדמיו עם ה- A^i -ים. כלומר $\varphi_A(p+q) = (p+q)(A) = p(A)+q(A) = \varphi_A(p)+\varphi_A(q)$.
תחומה קבוצת כל הפולינומים. נוכל על היותה לינארית, היא כפלית:

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

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

היא העתקה אלגברית, לא רק העתקה לינארית. יהיה מעניין להסתכל על הגרעין והתמונה שלה. יש לנו את $\varphi_A: \mathbb{F}[x] \rightarrow M_n(\mathbb{F})$. על התמונה אי אפשר להגיד כלום בינתיים. נסמן אותה ב- $\mathbb{F}[A]$. היא מרחב וקטורי שגם סגור לכפל. הראינו שלכל $B, C \in \mathbb{F}[A]$ המטריצות מתחלפות - $BC = CB$. גם ראינו ש- $V_{q(\lambda)}(B) \subseteq V_{q(\lambda)}(A)$ לכל $B = q(A)$. זה ראינו ביום חמישי.

עתה נדבר על הגרעין, שעליו לא ממש דיברנו. זו קבוצה שמכילה את הפולינומים שמאפסים את A . היא מ"ו שסגור לכפל (מודול או משהו כזה). אפשר להגיד קצת יותר - היא אידאל ב- $\mathbb{F}[x]$! אם $p \in \ker \varphi_A$ ו- $q \in \mathbb{F}[x]$ פולינום כלשהו אזי $pq \in \ker \varphi_A$. לפעמים מסמנים (סימן בלאטך שאני לא מכיר).

נגדיר פורמלית אידאל כי אלי לא עומד לעשות את זה. בהינתן R חוג, אם R' תת-חוג, הוא יקרא אידאל אם $\forall r \in R, c \in R': rc \in R'$. סגור לבליעה.

ברור ש- $\ker \varphi_A$ לא ריקה, כי 0 בפנים. ברור שיש פולינומים נוספים שהמטריצה מאפסת, וזה לא אידאל טריוויאלי - לכל $A \in M_n(\mathbb{F})$ קיים $p \neq 0$ כך ש- $p(A) = 0$. למה? עוד לפני קיילי המילטון, נוכל להסתכל על הסדרה:

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

זוהי סדרה של מטריצות ב- $M_n(\mathbb{F})$. ידוע $\dim M_n(\mathbb{F}) = n^2$. לכן אם הסדרה כוללת $n^2 + 1$ מטריצות, היא תלויה לינארית. מכאן שקיימים $a_0 \dots a_{n^2+1}$ שלאחר סכפול נותנים את מטריצת ה-0. אפשר להסתכל על זה גם כעל $\sum_{i=0}^{n^2+1} a_i A^i = 0$. למה זה מגניב? כי לא צריך לינארית 2 בשביל להגיד את זה. אפשר להגיד את זה משיקולים אפילו יותר מצחיקים - φ_A העתקה ממרחב $\mathbb{F}[x]$ שהוא מ"ו מממד אינסופי, אל תוך ממד סופי $M_n(\mathbb{F})$, ולכן הגרעין לא רק לא ריק, אלא אינסופי.

מכיוון שלמדנו לינארית 2, הפולינום האופייני נמצא בגרעין. ממשפט קיילי המילטון $p_A \in \ker \varphi_A$, שכן $p_A(A) = 0$. זה קצת יותר חזק ממה שקיבלנו בנימוקי לינארית 1 שלנו, שנתנו לנו פולינום ממעלה $n^2 + 1$, ולא ממעלה n .

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

הטענה המרכזית שנרצה לטעון היא:

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

בלשון של חוגים, אומרים ש- I הוא אידאל ראשי - הוא נוצר ע"י כפולות של איבר יחיד בחוג. גם קבוצת המספרים הזוגיים היא אידאל ראשי ב- \mathbb{Z} , שנוצרת ע"י 2. או -2 - כאן נבחין שהיוצר של האידאל הראשי (בתחום ראשי), קיים ויחיד עד לכדי חברות (כפל בהפוך).

טרמינולוגיה שאלי להר לא משתמש בה אבל אני כן: R' תת-חוג של R נוצר ע"י p אם $R' = \{rp \mid r \in R\}$ (או ב-*abuse of notion*, $R' = pR$). אפשר לדבר גם על אידאל ימני ושמאלי בחוגים לא קומטטיביים).

לא בכל חוג כל אידאל הוא אידאל ראשי. אפשר להסתכל על הקבוצה $\mathbb{R}[x, y]$ שכוללת את הקבוצה של $\{1, 2x - y^2, 3 - xy + y^3, -5x^2y\}$ וכו', שקוראים לה חוג הפולינומים בשני משתנים. אפשר לחשוב עליה כעל קבוצת הטנזורים בשני משתנים או משהו כזה. נבחין שבהינתן הפולינום x והפולינום y , והאידאל הנוצר על ידם $R' = xR + yR$, אינו 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 $I \triangleleft \mathbb{Z}$ הוא ראשי

הוכחה. אם $I = \{0\}$ אז הוא נוצר ע"י 0 וסיימנו. אם $I \neq \{0\}$ אז יש בו... מספרים. בפרט, יש בו מספרים חיוביים (למה? כי אפשר לכפול ב-1). יש לי נורמה אוקלידית, אהמהמהמה סדר טוב, ולכן אני אוכל לקחת $0 < a$ החיובי הקטן ביותר שנמצא ב- I , ונסמן $I = a\mathbb{Z}$ (עכשיו גם אלי להר התחיל להשתמש בסימון הזה), או בעברית, קבוצת הכפולות של a . הכיוון $a\mathbb{Z} \subseteq I$ טריויאלי מהגדרת I כאידאל (מבטיח לכם שאלי להר אמר "זה ברור" ואני לא מתעצל להעתיק). עתה נוכיח $I \subseteq a\mathbb{Z}$. יהי $b \in I$. נחלק את b ב- a עם שארית. נסמן $b : a = c \ (r)$ כאשר $0 \leq r < a$, או $b = sa + r$ עבור s כלשהו. ידוע ש- $b \in I$, $a \in I$ ולכן $sa \in I$. סה"כ $r = b - sa \in I$. האידאל סגור לחיסור ולכן $r \in I$. משום ש- $0 \leq r < a$ ו- a החיובי הכי קטן באידאל, $r = 0$. וסיימנו! $b = sa$, כלומר $b \in a\mathbb{Z}$. ■

ראנט שלי שלא קשור להרצאה. קצת משגע אותי שאלי להר לא מדבר על כל הקונספט של חברות בתורת החוגים. זה ממש מגניב וממש מועיל כדי לא לפרק למאנלואפלים מקרים. ואפשר ככה לסחוט קצת משפטי יחידות, לא רק קיום. הרעיון הוא - מספרים כמו $1, -1$ ב- \mathbb{Z} , או שורשי היחידה ב- \mathbb{C} , הוא הפולינומים הקבועים ב- $\mathbb{F}[x]$, כפל בהם "לא באמת משנה לי", וקוראים להם הפיכים. אומרים ששני מספרים הם "חברים" אם הם נבדלים בכפל בהפיך (ואז לדוגמה ב- \mathbb{Z} מתקיים ש- $4 \sim -4$ ביחס החברות, וב- $\mathbb{F}[x]$ מתקיים $2(x-1) \sim (x-1)$). והיחידות של היוצר של החוג, היא יחידות עד לכדי חברות, כלומר גם 2 וגם 2 יוצרים את \mathbb{N}_{even} , ובאופן דומה לשאר החוגים. עתה נחזור להוכיח את המשפט שאומר שכל אידאל ב- $\mathbb{F}[x]$ הוא ראשי. זו תהיה ממש אותה ההוכחה כמו ב- \mathbb{Z} , רק שה"דבר שמודד גודל" (נורמה אוקלידית קוראים לזה) יהיה \deg במקום ערך מוחלט.

הוכחה. אם $I = \{0\}$ אז I היא קבוצת כל הכפולות של פולינום האפס, והיא נוצרת על-ידו. אם $I \neq \{0\}$ יהי $m \in I$ ממעלה מינימלית. נראה $I = m(x)\mathbb{F}[x]$. "איזה כיוון הוא טריויאלי? זה ש- $m(x)\mathbb{F}[x] \subseteq I$ טריויאלי כי $m \in I$ ו- I אידאל וסגור לכפל בחוג (בליעה)". מצד שני צריך להראות $I \subseteq m(x)\mathbb{F}[x]$. יהי $p \in I$. נחלק את p ב- m ונקבל $p(x) = s(x)m(x) + r(x)$ כאשר r שארית ממעלה $\deg r < \deg m$. ואז מסגירות לחיבור $r(x) \in p(x) - s(x)m(x) \in I$ והוא אידאל. ומאותם הנימוקים $r(x) = 0$ כי m ממעלה חיובית מינימלית. ■

למי שרוצה את הגרסה הכי כללית של ההוכחה - תחפשו בויקיפדיה את ההוכחה שכל תחום אוקלידי הוא תחום ראשי. יאי אלי אמר עד כדי חברות. אני עכשיו שמח. אבל הוא לא הסביר מה זה. אני אסביר. m המינימלי הזה, יחיד עד לכדי כפל בסקלר - למה? כי הפולינומים הקבועים הם האיברים הפיכים שלי. כאן אלי טוען משהו שהוא לא יכול לטעון כי הוא לא הראה יחידות עד כדי חברות, אבל $m(x)$ הוא הפולינום.

נסכם מה ראינו לפני ההפסקה: כל אידאל $I \triangleleft \mathbb{F}[x]$ הוא ראשי (קבוצת כל הכפולות של פולינום $m \in \mathbb{F}[x]$, כאשר אם $I \neq \{0\}$ אז $m \neq 0$ פולינום ממעלה מינימלית ב- I). נבחר את m , "הפולינום המינימלי", להיות הפולינום המתוקן המינימלי. לכל $A \in M_n(\mathbb{F})$, ראינו ש- $I_0(A) = \ker \varphi_A$ היא אידאל, ולכן קיים פולינום מתוקן יחיד $m_A(x)$ המקיים:

א. $m_A(x) = 0$ 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, ראינו איך מוצאים את m_A . אם ג'ירדנו את A , ראינו ש- $m_A = \prod_{i=1}^k (x - \lambda_i)^{k_i}$ כאשר k_i גודל בלוק הג'ורדן הגודל ביותר שמתאים לע" λ_i , ו- $\lambda_1 \dots \lambda_k$ ע"עים. בפרט, אם λ ע"ע של A , אז $(x - \lambda) \mid m_A$.

מה עושים עם הפולינום המינימלי בחיים? "לא הרבה, [...] אבל אפשר לעשות את הדברים הבאים"

משפט 3. בהינתן $a_0 \neq 0$, יהי $q(x) = a_n x^n + \dots + a_1 x + a_0$. אם $q(A) = 0$, אפשר להסיק ש- A הפיכה, וניתן לכתוב את ההופכית שלה כפולינום $r(A)$ כאשר 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 לנסח את ההוכחה.

אפשר גם לנסח את הונקטוראפואסיטיב 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 אופייני מתפצל, כך ש- $p_A(x) = \prod_{i=1}^r (x - \lambda_i)^{k_i}$, ו- $\lambda_1 \dots \lambda_n$ ע"עים של A , אזי

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

(כאשר \mathcal{Z}_r זה \ker או \mathcal{N} אבל בסימוני אלי להר, ו- \mathcal{Z}_r^\times בהקשר הזה הוא מ"ו עצמי מוכלל). "משפט הפירוק הפרימרי הוא דבילי בהינתן צורת ג'ורדן" – אם $A \sim \text{diag}(J_3(5), J_2(5), J_2(5), J_7(-2), J_1(-2), J_4(0))$ כוללת 7 פעמים 5, 8 פעמים -2, ומטריצה יחידה מגודל 4 לע"ע 0, ואז הפולינום האופייני $(x-5)^7(x+2)^8(x^4)$. בכל "בלוק קטן" של מ"ו עצמי מוכלל, אחרי שנעלה בחזקה 3 פעמים, כבר נקבל 0. משפט הפירוק הפרימרי אומר שאפשר לעשות את זה 8 פעמים, זה יותר חלש.

אני מצטער אם זה לא ברור – אלי להר דיבר המון בעפ עכשיו, אבל מה שהוא אומר, להבנתי, הוא שמשפט הפירוק הפרימרי "די חלש" בגלל שאנחנו לא באמת צריכים להעלות בחזקת k_i כדי לקבל את המ"ו העצמי המוכלל, מספיק להעלות בחזקת גודל הבלוק הכי קטן, כי זה כבר יאפס את החלק הרלוונטי.

ביום חמישי נוכיח את משפט הפירוק הפרימרי מתכונות פולינומים.

לאן נעלמו ההעתקות הלינאריות?

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

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

עכשיו אלי להר מצייר את הדיאגרמה הקומטטיבית של לינארית 1א. זה קצת חזרה ואני גם לא יודע לצייר את זה בלאטך.

עכשיו הוא מראה איך מוצאים מטריצה לפי מטריצה מייצגת. זה די חומר של לינארית 1א, הדבר היחיד שחשוב לציין שמבחינתו הסימון $[T]_Q$ לא אומר הייצוג של T לפי הבסיס Q , אלא הייצוג של T לפי האיזומורפיזם $Q: V \rightarrow \mathbb{R}^n$, כאשר הוא תלוי בסיס ולמעשה שווה ל- $[\cdot]_B$ העתקת הייצוג לפי בסיס B כלשהו. בגלל ש- B ו- Q הם naturally isomorphic, זה סתם סימון.