אלגברה ב׳

עידן איזנר

לפי רשימות הקורס של פרופ׳ אנה מלניקוב

תוכן העניינים

תוכן העניינים

פרק 1

אופרטורים לינאריים

1.1 העתקות ליניאריות ודמיון מטריצות

1.1.1 העתקות ומטריצה מייצגת

בהינתן מרחב וקטורי V מעל שדה F, ההעתקה $f: V \to V$ נקראת העתקה ליניארית אם:

1. לכל $v \in V$ ולכל $\alpha \in F$ מתקיים $f(\alpha v) = \alpha f(v)$.
2. לכל $v, w \in V$ מתקיים $f(v+w) = f(v) + f(w)$.

קריטריון מקוצר: $f(\alpha v + \beta w) = \alpha f(v) + \beta f(w)$.

הגדרה 1.1.1. האוסף של כל ההעתקות הליניאריות ממרחב וקטורי V לעצמו נקרא אלגברת האנדומורפיזמים של V ומסומן $\text{End}(V)$.

הערה 1.1.2. המילה "אלגברה" מציינת כי ניתן לבצע פעולות אלגבריות על ההעתקות הליניאריות הללו.

הפעולות האלגבריות האפשריות הן:

1. אם $f, g \in \text{End}(V)$, נגדיר: $(f+g)(v) = f(v) + g(v)$; אזי $f + g \in \text{End}(V)$.
2. אם $f \in \text{End}(V)$ וגם $\alpha \in F$, נגדיר: $(\alpha f)(v) = \alpha f(v)$; אזי $\alpha f \in \text{End}(V)$.
3. אם $f, g \in \text{End}(V)$, נגדיר: $(f \circ g)(v) = f(g(v))$; אזי $f \circ g \in \text{End}(V)$.

יהי V מרחב וקטורי סוף מימדי מעל שדה F, יהי $B = \{v_1, v_2, \ldots, v_n\}$ בסיס של V ויהי $f \in \text{End}(V)$ אופרטור ליניארי, אזי

$$f(v_j) = \sum_{i=1}^{n} \alpha_{ij} v_i$$

לכל $1 \leq j \leq n$.

במילים אחרות: $[f(v_j)]_B = \begin{pmatrix} \alpha_{1j} \\ \vdots \\ \alpha_{nj} \end{pmatrix}$.

הגדרה 1.1.3. המטריצה

$$[M_f]_B = \begin{bmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{bmatrix}$$

נקראת המטריצה המייצגת של f לפי בסיס B.

$$w \in V \Longrightarrow w = \sum_{j=1}^{n} \beta_j v_j \Longleftrightarrow [w]_B = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

אפשר לכתוב

$$f(w)=f\left(\sum_{j=1}^{n}\beta_jv_j\right)=\sum_{j=1}^{n}\beta_jf(v_j)=\sum_{j=1}^{n}\beta_j\sum_{i=1}^{n}\alpha_{ij}v_i$$
$$=\sum_{j=1}^{n}\sum_{i=1}^{n}\beta_j\alpha_{ij}v_i=\sum_{i=1}^{n}\left(\sum_{j=1}^{n}\beta_j\alpha_{ij}\right)v_i$$

ומכאן נקבל כי:

$$.\,[f(w)]_B=\begin{pmatrix}\sum_{j=1}^{n}\beta_j\alpha_{1j}\\ \vdots\\ \sum_{j=1}^{n}\beta_j\alpha_{nj}\end{pmatrix}$$

כלומר

$$.\,[M_f]_B\,[w]_B=\begin{pmatrix}\alpha_{11}&\cdots&\alpha_{1n}\\ \vdots&\ddots&\vdots\\ \alpha_{n1}&\cdots&\alpha_{nn}\end{pmatrix}\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix}=\begin{pmatrix}\sum_{j=1}^{n}\beta_j\alpha_{1j}\\ \vdots\\ \sum_{j=1}^{n}\beta_j\alpha_{nj}\end{pmatrix}=[f(w)]_B$$

מסקנה 1.1.4. יהי V מרחב וקטורי n- מימדי מעל שדה F, אזי $\mathrm{End}(V)\cong M_n(F)$ לאחר קביעת בסיס כלשהו, כלומר:

$$[M_{f+g}]_B=[M_f]_B+[M_g]_B$$
$$[M_{f\circ g}]_B=[M_f]_B\cdot[M_g]_B$$
$$[M_{\alpha f}]_B=\alpha[M_f]_B$$

1.1.2 מטריצות מעבר ומטריצות דומות

הגדרה 1.1.5. יהי V מרחב וקטורי n- מימדי מעל שדה F, ויהיו $B_1=\{v_1,v_2,\dots,v_n\}$ ו- $B_2=\{w_1,w_2,\dots,w_n\}$ שני בסיסים.

$$w_j=\sum_{i=1}^{n}\alpha_{ij}v_i\Longleftrightarrow[w_j]_{B_1}=\begin{pmatrix}\alpha_{1j}\\ \vdots\\ \alpha_{nj}\end{pmatrix}$$

מטריצת המעבר מ- B_1 ל- B_2 היא

$$.P_{B_1}^{B_2}=\begin{pmatrix}\alpha_{11}&\cdots&\alpha_{1n}\\ \vdots&\ddots&\vdots\\ \alpha_{n1}&\cdots&\alpha_{nn}\end{pmatrix}$$

זו מטריצה שבעמודות שלה מופיעים וקטורי הקואורדינטות של איברי הבסיס B_2 לפי הבסיס B_1.

$$w=\sum_{j=1}^{n}\beta_jv_j\Longrightarrow[w]_{B_1}=\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix}$$

ידוע ש- $P_{B_2}^{B_1} = \left(P_{B_1}^{B_2}\right)^{-1}$,
ולכן $[w]_{B_2} = P_{B_2}^{B_1} \cdot [w]_{B_1} = \left(P_{B_1}^{B_2}\right)^{-1} \cdot [w]_{B_1}$.
תזכורת: נתונה $A \in M_n(F)$ כאשר $V = F^n$,

$$A = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & \ddots & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{pmatrix}$$

ניקח

$$w_1 = \begin{pmatrix} \alpha_{11} \\ \vdots \\ \alpha_{n1} \end{pmatrix}, w_2 = \begin{pmatrix} \alpha_{12} \\ \vdots \\ \alpha_{n2} \end{pmatrix}, \ldots, w_n = \begin{pmatrix} \alpha_{1n} \\ \vdots \\ \alpha_{nn} \end{pmatrix}$$

מתקיים כי $\{w_1, w_2, \ldots, w_n\}$ בסיס $\Longleftrightarrow$ המטריצה A הפיכה.
לכן מטריצת המעבר $P_{B_1}^{B_2}$ היא הפיכה וכל מטריצה הפיכה מהווה מטריצת מעבר מהבסיס הנתון לבסיס חדש כלשהו.

בעיה 1.1.6. נתונים מ"ו n-מימדי מעל שדה F ואופרטור $f \in \mathrm{End}(V)$. נתונים שני בסיסים $B_1 = \{v_1, v_2, \ldots, v_n\}$ ו- $B_2 = \{w_1, w_2, \ldots, w_n\}$, עם מטריצת מעבר $P_{B_1}^{B_2}$, וידועה המטריצה $[M_f]_{B_1}$ (המטריצה המייצגת של f בבסיס B_1).
איך נראית המטריצה $[M_f]_{B_2}$?

פתרון 1.1.7. באופן כללי ניקח $w \in V$, ידוע כי $[M_f]_{B_2} \cdot [w]_{B_2} = [f(w)]_{B_2}$.
שלב 1: $[w]_{B_1} = P_{B_1}^{B_2} \cdot [w]_{B_2}$
שלב 2: $[M_f]_{B_1} \cdot [w]_{B_1} = [f(w)]_{B_1}$
שלב 3: $[f(w)]_{B_2} = \left(P_{B_1}^{B_2}\right)^{-1} \cdot [f(w)]_{B_1}$
ומכאן נקבל: $[M_f]_{B_2} = \left(P_{B_1}^{B_2}\right)^{-1} \cdot [M_f]_{B_1} \cdot P_{B_1}^{B_2}$.

הגדרה 1.1.8. מטריצות $A, B \in M_n(F)$ נקראות **דומות** אם קיימת מטריצה הפיכה $P \in M_n(F)$ כך ש- $B = P^{-1}AP$.

טענה 1.1.9. דמיון של מטריצות הוא יחס שקילות על $M_n(F)$.

הוכחה. נראה כי מתקיימות שלוש התכונות:
רפלקסיביות - ניקח $P = I_n$, אז $A = I_n^{-1}AI_n$ ולכן $A \sim A$ (כלומר A דומה לעצמה).
סימטריה - $B = P^{-1}AP$. ניקח $Q = P^{-1}$ ונקבל $A = Q^{-1}BQ$ זאת אומרת $A \sim B \longrightarrow B \sim A$.
טרנזיטיביות - אם $B = P^{-1}AP$ ו- $C = Q^{-1}BQ$ אז

$$C = Q^{-1}\left(P^{-1}AP\right)Q = (PQ)^{-1}A(PQ)$$

כלומר $A \sim B, B \sim C \longrightarrow A \sim C$. □

מסקנה 1.1.10. מטריצות הן דומות אם ורק אם הן מייצגות את אותה העתקה ליניארית לפי בסיסים שונים.

תזכורת מאלגברה לינארית א': נתונות מטריצות $A \in M_n(F)$ ו- $B \in M_n(F)$ הפיכה, אז

$$\mathrm{rank}(AB) = \mathrm{rank}(BA) = \mathrm{rank}(A).$$

מסקנה 1.1.11. למטריצות דומות יש אותה דרגה (rank).

הוכחה. אם $B = P^{-1}AP$ אז

$$\operatorname{Rank}(B) = \operatorname{rank}(P^{-1}AP) = \operatorname{rank}(AP) = \operatorname{rank}(A).$$

□

תזכורת מאלגברה ליניארית א': תכונות של דטרמיננטה:

1. $\det(AB) = \det(A) \cdot \det(B)$.
2. $\det(B^{-1}) = (\det(B))^{-1}$.

מסקנה 1.1.12. למטריצות דומות יש אותה דטרמיננטה.

הוכחה.

$$\begin{aligned}\det(B) &= \det(P^{-1}AP) = \det(P^{-1})\det(A)\det(P) \\ &= (\det(P))^{-1}\det(A)\det(P) = \det(A)\end{aligned}$$

□

1.2 ערכים עצמיים ווקטורים עצמיים של מטריצות, מטריצות לכסינות

1.2.1 הגדרות

הגדרה 1.2.1. תהי $A \in M_n(F)$. אם קיים $\alpha \in F$ ו- $\overrightarrow{0} \neq v \in F^n$ כך ש- $Av = \alpha v$ אז α נקרא **ערך עצמי** של A ו- v נקרא **וקטור עצמי** של A (המתאים ל- α).

דוגמא 1.2.2.
1. אם A מטריצה אלכסונית $A = \operatorname{diag}(\alpha_1, \ldots, \alpha_n)$ אז לכל i הוקטור $e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ הוא וקטור עצמי וכל α_i הוא ערך עצמי כי $Ae_i = \alpha_i e_i$ לכל $1 \leq i \leq n$.
2. $A = I$, אז כל $\overrightarrow{0} \neq v \in F^n$ הוא וקטור עצמי ו- $\alpha = 1$ הוא ערך עצמי.
3. $A \in M_2(\mathbb{R})$ מטריצת סיבוב $A = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$.
אם $\alpha \neq 0, \pi$ אז אין ל- A ערכים עצמיים.
אם $\alpha = 0$ נקבל $A = I_2$ (דוגמא קודמת).
אם $\alpha = \pi$ נקבל $A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, לכן כל $\overrightarrow{0} \neq v$ הוא וקטור עצמי של A עם ערך עצמי -1.

טענה 1.2.3. תהיינה $A, B \in M_n(F)$ מטריצות דומות, ויהי α ערך עצמי של A. אז α הוא גם ערך עצמי של B.

במילים אחרות: למטריצות דומות יש אותם ערכים עצמיים.

הוכחה. נתון $A \sim B$, לכן קיימת P הפיכה כך ש- $B = P^{-1}AP$.
יהי α ערך עצמי של A, אז קיים $\overrightarrow{0} \neq v \in F^n$ כך ש- $Av = \alpha v$.
נגדיר $w = P^{-1}v$ אז $w \neq 0$ (למה $w \neq 0$?) אז מקבלים:

$$\begin{aligned} Bw &= P^{-1}AP \cdot P^{-1}v = P^{-1}A \cdot (PP^{-1})v \\ &= P^{-1}Av = P^{-1}\alpha v = \alpha P^{-1}v = \alpha w \end{aligned}$$

קיבלנו $Bw = \alpha w$, כלומר α הוא ערך עצמי של B עם וקטור עצמי w. $\square$

הערה 1.2.4. אפשר להראות עכשיו שמטריצות דומות אינן בהכרח שקולות שורה, ושמטריצות שקולות שורה אינן בהכרח דומות.

למשל, נתונות המטריצות שקולות השורה $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \ B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

למטריצה B יש ערך עצמי 1 כי $B \cdot e_2 = e_2$, אבל 1 הוא לא ערך עצמי של A, כי $A^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,
ואילו היה קיים $\overrightarrow{0} \neq v \in F^n$ כך ש- $Av = 1 \cdot v$ היינו מקבלים

$$A^2 v = A(Av) = Av = v \neq \overrightarrow{0},$$

וזה סותר את $A^2 = 0$.

לכן $A^2u = \overrightarrow{0}$ לכל $u \in F^2$, ומכאן, לפי טענה 1.2.3 המטריצות A, B אינן דומות.

נתבונן כעת במטריצות $C = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

הן **אינן** שקולות שורה.

בדיקה ישירה מראה שהן דומות: אם ניקח $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, אז קל לבדוק ש- $P^{-1} = P$ ומתקיים

$$\begin{aligned} P^{-1}BP &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = C \end{aligned}$$

טענה 1.2.5. תהי $A \in M_n(F)$ ויהי α ערך עצמי של A עם וקטור עצמי מתאים $v \neq 0$. אז לכל $\beta \neq 0$ מתקיים ש- $w = \beta v$ הוא וקטור עצמי המתאים לערך α.

הוכחה. $Aw = A(\beta v) = \beta(Av) = \beta(\alpha v) = \alpha(\beta v) = \alpha w$. □

הגדרה 1.2.6. מטריצה $A \in M_n(F) = (\alpha_{ij})_{i,j=1}^n$ נקראת **אלכסונית** אם לכל $i \neq j$ מתקיים $\alpha_{ij} = 0$.

$$A = \begin{pmatrix} \alpha_{11} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \alpha_{nn} \end{pmatrix} = \operatorname{diag}(\alpha_{11}, \alpha_{22}, \ldots, \alpha_{nn}) = \operatorname{diag}(\beta_1, \beta_2, \ldots, \beta_n)$$

כאשר $\beta_i = \alpha_{ii}$ לכל $1 \leq i \leq n$.

אם $A = \operatorname{diag}(\beta_1, \beta_2, \ldots, \beta_n)$ אז $Ae_i = \beta_i e_i$ ולכן כל e_i הוא וקטור עצמי של A.

1.2.2 מטריצות לכסינות

הגדרה 1.2.7. מטריצה $A \in M_n(F)$ נקראת **לכסינה** אם היא דומה למטריצה אלכסונית.

טענה 1.2.8. יהיו $A, B \in M_n(F)$ מטריצות דומות, אז לכל $k \in \mathbb{N}$ מתקיים $A^k \sim B^k$. יתר על כן, A הפיכה אם ורק אם B הפיכה, ובמקרה זה לכל $k \in \mathbb{N}$ מתקיים $A^{-k} \sim B^{-k}$.

הוכחה. $B = P^{-1}AP$, לכן לכל $k \in \mathbb{N}$ נקבל:

.1

$$\begin{aligned} B^k &= \underbrace{\left(P^{-1}AP\right)\left(P^{-1}AP\right)\cdots\left(P^{-1}AP\right)}_{\text{פעמים } k} \\ &= \underbrace{P^{-1}A(PP^{-1})A(PP^{-1})\cdot\cdots\cdot P^{-1}AP}_{\text{פעמים } k} = P^{-1}A^kP \end{aligned}$$

.2 $B^{-1} = \left(P^{-1}AP\right)^{-1} = P^{-1}A^{-1}P$.

ומ- 1 ו- 2 מקבלים $B^{-k} = P^{-1}A^{-k}P$. □

הערה 1.2.9. מההוכחה אפשר לראות שמלבד העובדה שהחזקות של המטריצות דומות, מתקיים שמטריצת המעבר מ- A ל- B היא גם מטריצת מעבר מ- A^k ל- B^k.

הגדרה 1.2.10. לכל מטריצה $A \in M_n(F)$ נגדיר $A^0 = I_n$.

(זה מתאים לכך ש- $A^{n+m} = A^n \cdot A^m$ ולכן עבור $m = 0$ מקבלים $A^n = A^{n+0} = A^n \cdot A^0$).

הגדרה 1.2.11. נתונה מטריצה $A \in M_n(F)$ ו- $p(x) \in F[x]$ (פולינום במשתנה x עם מקדמים מ- F).
נכתוב $p(x) = a_k x^k + \cdots + a_0 x^0$ ו- $a_k \neq 0$ (כאשר k היא הדרגה של $p(x)$).
נגדיר

$$p(A) = a_k A^k + a_{k-1}A^{k-1} + \cdots + a_1 A + a_0 I_n.$$

מסקנה 1.2.12. תהיינה $A, B \in M_n(F)$ מטריצות דומות, אז לכל $p(x) \in F[x]$ מתקיים $p(A) \sim p(B)$.

הוכחה. נכתוב $B = Q^{-1}AQ$, ואז

$$\begin{aligned} p(B) &= a_k B^k + a_{k-1}B^{k-1} + \cdots + a_1 B + a_0 I_n \\ &= a_k Q^{-1}A^k Q + a_{k-1}Q^{-1}A^{k-1}Q + \cdots + a_1 Q^{-1}AQ + a_0 Q^{-1}I_n Q \\ &= Q^{-1}\left(a_k A^k + a_{k-1}A^{k-1} + \cdots + a_1 A + a_0 I_n\right)Q = Q^{-1}p(A)Q \end{aligned}$$

□

הערה 1.2.13. $p(A) \sim p(B) \not\Rightarrow A \sim B$.
למשל: $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.
ברור ש- $B \nsim A$ כי יש להן ערכים עצמיים שונים, אבל $A^2 = B^2 = I_2$,
לכן $A^2 \sim B^2$. אבל $A \nsim B$.
דוגמא נוספת: $A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\ B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.
גם כאן $B \nsim A$ כי A מטריצה סקלרית (ומטריצות סקלריות דומות רק לעצמן), אבל $A^2 = B^2 = 0$.
לכן $A^2 \sim B^2$. אבל $A \nsim B$.

כלומר – דמיון פולינומים (או חזקות) של מטריצות **לא גורר** דמיון של המטריצות.

מסקנה 1.2.14. אם מטריצה $A \in M_n(F)$ דומה למטריצה אלכסונית $B = \operatorname{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ אז $\alpha_1, \alpha_2, \ldots, \alpha_n$ הם ערכים עצמיים של A.

הוכחה. לפי טענה 1.2.3 - ל- A ול- B יש אותם ערכים עצמיים, ולפי ההגדרה של $B = \operatorname{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, כל α_i הוא ערך עצמי של B עם וקטור עצמי e_i. □

משפט 1.2.15. המטריצה $A \in M_n(F)$ לכסינה אם ורק אם ל- A יש קבוצה של n וקטורים עצמיים בת"ל.

הוכחה. נניח ש- A לכסינה, אז קיימת $P \in M_n(F)$ כך ש- $A = P^{-1}\operatorname{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)P$ ולפי מסקנה 1.2.14 וההוכחה של טענה 1.2.3 מתקיים שהוקטורים

$$v_1 = P^{-1} \cdot e_1, v_2 = P^{-1} \cdot e_2, \ldots, v_n = P^{-1} \cdot e_n$$

הם וקטורים עצמיים של A,
והם בת"ל כי הם תמונה של הקבוצה $\{e_1, e_2, \ldots, e_n\}$ שהיא קבוצה בת"ל.

בכיוון ההפוך: נניח ש- $v_1, v_2, \ldots, v_n$ הם וקטורים עצמיים של A והם בת"ל.
זאת אומרת שקיימים $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ כך ש- $Av_i = \alpha_i v_i$ לכל $1 \leq i \leq n$. נגדיר $P = [v_1 v_2 \cdots v_n]$ (מטריצה שהעמודות שלה הן הוקטורים v_i).
זו מטריצה הפיכה כי העמודות שלה בת"ל. נראה ש- $P^{-1}AP = \text{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)$:
מספיק להראות שלכל e_i מתקיים $\left(P^{-1}AP\right) e_i = \alpha_i e_i$ (כי מכפלה של מטריצה בוקטור עמודה e_i היא בעצם העמודה ה- i של המטריצה). נבדוק:

$$\left(P^{-1}AP\right) e_i = P^{-1}Av_i = P^{-1}\alpha_i v_i = \alpha_i P^{-1} v_i = \alpha_i e_i \ .$$

$\square$

מסקנה 1.2.16. תהי $A \in M_n(F)$ מטריצה לכסינה ויהיו $v_1, v_2, \ldots, v_n$ וקטורים עצמיים שלה עם ערכים עצמיים מתאימים $\alpha_1, \alpha_2, \ldots, \alpha_n$ כלומר $Av_i = \alpha_i v_i$.
אז $A \sim \text{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

מסקנה 1.2.17. תהי $A \in M_n(F)$ מטריצה לכסינה ויהיו $v_1, v_2, \ldots, v_n$ וקטורים עצמיים שלה עם ערכים עצמיים מתאימים $\alpha_1, \alpha_2, \ldots, \alpha_n$.
אז

$$\det(A) = \prod_{i=1}^{n} \alpha_i \ .$$

הוכחה. זה נובע מיידית מדטרמיננטה של מטריצה אלכסונית ומהעובדה שלמטריצות דומות יש אותה דטרמיננטה. $\square$

מסקנה 1.2.18. אם $A = \text{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ ו- $B = \text{diag}(\beta_1, \beta_2, \ldots, \beta_n)$ אז
$A \sim B$ (המטריצות A ו- B דומות) $\iff$ $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \{\beta_1, \beta_2, \ldots, \beta_n\}$.
ז"א יש להן את אותם ערכים עצמיים עם אותם ריבויים.

הוכחה. אם $A \sim B$ אז לפי טענה 1.2.3 וההוכחה שלה יש להן אותם ע"ע עם אותם ריבויים, ז"א $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \{\beta_1, \beta_2, \ldots, \beta_n\}$.
בכיוון ההפוך: אם $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \{\beta_1, \beta_2, \ldots, \beta_n\}$ אז $\alpha_1 = \beta_{i_1}, \alpha_2 = \beta_{i_2}, \ldots, \alpha_n = \beta_{i_n}$.
ניקח בסיס $B_1 = e_{i_1}, e_{i_2}, \ldots, e_{i_n}$ ונכתוב $P = [e_{i_1}, e_{i_2}, \ldots e_{i_n}]$ (מטריצה שעמודותיה הן וקטורי הבסיס B_1).
אז $P^{-1}BP = A$ ולכן $B \sim A$. $\square$

1.3 הפולינום האופייני של מטריצה ריבועית

1.3.1 פולינום אופייני

הגדרה 1.3.1. תהי $A \in M_n(F)$ מטריצה ריבועית. נגדיר $xI_n - A$ (כאשר x הוא משתנה) - זוהי המטריצה האופיינית של A.

איך נראית המטריצה האופיינית? תהי

$$.A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{bmatrix}$$

כעת $xI_n = \text{diag}(x, x, \ldots, x)$, כלומר זו מטריצה אלכסונית מהצורה

$$\begin{bmatrix} x & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & x \end{bmatrix},$$

ולכן

$$.xI - A = \begin{bmatrix} x-\alpha_{11} & -\alpha_{12} & \cdots & -\alpha_{1n} \\ -\alpha_{21} & x-\alpha_{22} & \cdots & -\alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -\alpha_{n1} & -\alpha_{n2} & \cdots & x-\alpha_{nn} \end{bmatrix}$$

הגדרה 1.3.2. תהי $A \in M_n(F)$. הפולינום האופייני של A הוא

$$\Delta_A(x) = \det(xI_n - A) = \begin{vmatrix} x-\alpha_{11} & -\alpha_{12} & \cdots & -\alpha_{1n} \\ -\alpha_{21} & x-\alpha_{22} & \cdots & -\alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -\alpha_{n1} & -\alpha_{n2} & \cdots & x-\alpha_{nn} \end{vmatrix}$$

במילים אחרות, הפולינום האופייני של A הוא הדטרמיננטה של המטריצה האופיינית של A.

הגדרה 1.3.3. (תזכורת:) תהי $A \in M_n(F)$. העקבה של A מוגדרת:

$$.\text{trace}(A) = \sum_{i=1}^{n} a_{ii} = a_{11} + a_{22} + \cdots + a_{nn}$$

מסקנה 1.3.4. תהי $A \in M_n(F)$. אז הפולינום האופייני של A שמסומן $\Delta_A(x)$ הוא

1. פולינום מדרגה n $\Delta_A(x) = \beta_n x^n + \cdots + \beta_1 x + \beta_0$, שמקיים:
2. $\beta_n = 1$ (פולינום כזה מכונה פולינום מתוקן).
3. $.\beta_{n-1} = -\text{trace}(A)$

4. $\beta_0 = (-1)^n \det(A)$.

הוכחה.

$$\Delta_A(x) = \begin{vmatrix} x-\alpha_{11} & -\alpha_{12} & \cdots & -\alpha_{1n} \\ -\alpha_{21} & x-\alpha_{22} & \cdots & -\alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -\alpha_{n1} & -\alpha_{n2} & \cdots & x-\alpha_{nn} \end{vmatrix}.$$

נזכיר את הגדרת הדטרמיננטה: למטריצה $B = (\beta_{ij})$ הדטרמיננטה

$$\det(B) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \cdot \beta_{1\sigma(1)} \cdot \cdots \cdot \beta_{n\sigma(n)} \tag{1.1}$$

כאשר $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ תמורה.

נזכיר כי התמורה היחידה שמעבירה כל איבר לעצמו היא $e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$.

בכל תמורה אחרת לפחות שני איברים לא עוברים לעצמם (כי עבור $1 \le i,j \le n$, אם $\sigma(i) = j \ne i$ אז $\sigma(j) \ne j$).
לכן בכל איבר מהסכום (1.1) מלבד האיבר $\beta_{11} \cdot \beta_{22} \cdot \cdots \cdot \beta_{nn}$ יש לכל היותר $n-2$ מאיברי האלכסון הראשי.
נחזור למטריצה האופיינית ונזכיר כי המשתנה x מופיע בה רק על האלכסון הראשי. לכן מקבלים

$$\begin{aligned} \Delta_A(x) &= (x-\alpha_{11})(x-\alpha_{22}) \cdot \cdots \cdot (x-\alpha_{nn}) \\ &+ \sum_{e \ne \sigma \in S_n} \text{מחוברים עם לכל היותר } n-2 \text{ איברים מהאלכסון הראשי} \end{aligned}$$

לכן החלק של הפולינום שמופיע בסכום הוא מדרגה קטנה או שווה ל- $n-2$. כעת, החזקה ה- n של הפולינום מתקבלת כמכפלה של x-ים בכל הסוגריים, והחזקה ה- $n-1$ מתקבלת כסכום של מכפלות כל הסוגריים פרט לסוגריים מספר i, שמהם מוציאים $-\alpha_{ii}$.

זה נותן:

$$\Delta_A(x) = x^n + (-\alpha_{11} - \alpha_{22} - \cdots - \alpha_{nn})\, x^{n-1} + \text{דרגות נמוכות יותר}$$

לכן $\Delta_A(x)$ הוא פולינום מתוקן מדרגה n, והמקדם של x^{n-1} הוא $-\operatorname{trace}(A)$, כך שהוכחנו את 1,2,3.

כדי לקבל את המקדם החופשי בפולינום, צריך להציב $x = 0$:

$$\begin{aligned} \beta_0 = \Delta_A(0) &= \begin{vmatrix} -\alpha_{11} & -\alpha_{12} & \cdots & -\alpha_{1n} \\ -\alpha_{21} & -\alpha_{22} & \cdots & -\alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -\alpha_{n1} & -\alpha_{n2} & \cdots & -\alpha_{nn} \end{vmatrix} = \det(-A) \\ &= \det(-I_n) \cdot \det(A) = (-1)^n \det(A) \end{aligned}$$

כלומר

$$\beta_0 = (-1)^n \det(A).$$

□

1.3.2 ערכים עצמיים והפולינום האופייני

נזכיר כי α ערך עצמי של A ו- $v \neq 0$ וקטור עצמי של A אם מתקיים $Av = \alpha v$.
כשמעבירים אגפים מקבלים $\alpha v - Av = 0$. נציב $\alpha v = \alpha I \cdot v$ ונקבל $(\alpha I - A)\, v = 0$.
$\Longleftrightarrow$ למערכת הלינארית $(\alpha I - A)\, x = 0$ יש פתרון לא טריוויאלי $x = v$.
$|\alpha I - A| = 0 \Longleftrightarrow$
$\Delta_A(\alpha) = 0 \Longleftrightarrow$
α הוא שורש של $\Delta_A(x) \quad \Longleftrightarrow$

מסקנה 1.3.5. תהי $A \in M_n(F)$. אז α הוא ערך עצמי של $A \Longleftrightarrow \alpha$ הוא שורש של $\Delta_A(x)$.

מסקנה 1.3.6. תהי $A \in M_n(F)$. אז 0 הוא ערך עצמי של $A \Longleftrightarrow A$ לא הפיכה.

משפט 1.3.7 (המשפט היסודי של האלגברה)**.** לכל פולינום מעל $\mathbb{C}$ מדרגה ≤ 1 קיים שורש.

הערה 1.3.8. נשים לב כי מגדירים את הדרגה של פולינום האפס $\deg(0) = -\infty$, כדי שגם מכפלה בפולינום האפס תעמוד בכלל שאומר שדרגה של מכפלת פולינומים היא סכום הדרגות שלהם.

מסקנה 1.3.9. תהי $A \in M_n(\mathbb{C})$ (מטריצה מעל המרוכבים) אז ל- A קיים לפחות ערך עצמי אחד ולפחות וקטור עצמי בת"ל אחד.

הערה 1.3.10. ללא תלות ב- n, קיימות מטריצות שיש להן בדיוק ע"ע אחד וו"ע בת"ל אחד.
למשל למטריצה

$$A = \begin{bmatrix} 0 & 1 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & \cdots & 0 \end{bmatrix}$$

נקבל כי 0 הוא ע"ע יחיד של A ו- $\text{rank}(A) = n - 1$. לכן

$$\dim\left(\ker(A)\right) = n - \text{rank}(A) = 1$$

ולכן יש ל- A ו"ע בת"ל אחד.

משפט 1.3.11. למטריצות דומות יש אותו פולינום אופייני.
במילים אחרות - תהי $A \in M_n(F)$ ותהי $P \in M_n(F)$ הפיכה, אז $\Delta_A(x) = \Delta_{P^{-1}AP}(x)$.

הוכחה. $\Delta_A(x) = \det(xI_n - A)$.

לכן

$$\begin{aligned} \Delta_{P^{-1}AP}(x) &= \det(xI_n - P^{-1}AP) = \det\left(xP^{-1}IP - P^{-1}AP\right) \\ &= \det\left(P^{-1}\left(xI - A\right)P\right) = \det\left(P^{-1}\right)\det\left(xI - A\right)\det\left(P\right) \\ &= \frac{1}{\det(P)} \cdot \det\left(P\right) \cdot \det\left(xI - A\right) = \det\left(xI - A\right) \end{aligned}$$

□

הערה 1.3.12. המשפט אומר שהפולינום האופייני הוא שמורה של מטריצות דומות.

תזכורת: ביחס שקילות, "שמורה" היא תכונה זהה לכל האיברים באותה מחלקת שקילות.

הערה 1.3.13. נשים לב כי $\Delta_A(x) = \Delta_B(x) \nRightarrow A \sim B$.

למשל: $A = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

ואז $A \nsim B$, אבל $\Delta_A(x) = \Delta_B(x) = (x-1)^2$ (בדקו!)

מסקנה 1.3.14. למטריצות דומות יש אותן דטרמיננטות ואותן עקבות.

הוכחה. המקדם של x^{n-1} ב- $\Delta_A(x)$ הוא $-\operatorname{trace}(A)$ והמקדם של x^0 הוא $(-1)^n \det(A)$ (הוכחנו). □

משפט 1.3.15. תהי $A \in M_n(F)$ ו- $\alpha_1, \alpha_2, \ldots, \alpha_k$ ערכים עצמיים שונים זה מזה עם וקטורים עצמיים מתאימים $v_1, v_2, \ldots, v_k$ (כלומר $Av_i = \alpha_i v_i$) אז הקבוצה $\{v_1, v_2, \ldots, v_k\}$ היא בת"ל.

הוכחה. נניח בשלילה ש- $\{v_1, v_2, \ldots, v_k\}$ ת"ל.
מכיוון שבקבוצה זו $v_i \neq 0$ לכל i (כל הוקטורים העצמיים שונים מאפס), קיים i כך שהקבוצה $\{v_1, v_2, \ldots, v_{i-1}\}$היא בת"ל והוקטור v_i הוא צ"ל שלה,
כלומר קיימים $\beta_1, \ldots, \beta_{i-1}$ שלא כולם אפסים כך ש- $v_i = \sum_{j=1}^{i-1} \beta_j v_j$. אז מצד אחד

$$Av_i = \alpha_i v_i = \alpha_i \sum_{j=1}^{i-1} \beta_j v_j = \sum_{j=1}^{i-1} \alpha_i \beta_j v_j ,$$

ומצד שני

$$Av_i = A\left(\sum_{j=1}^{i-1} \beta_j v_j\right) = \sum_{j=1}^{i-1} A\left(\beta_j v_j\right) = \sum_{j=1}^{i-1} \alpha_j \beta_j v_j .$$

מחסרים את השוויונים ומקבלים

$$Av_i - Av_i = \sum_{j=1}^{i-1} \alpha_i \beta_j v_j - \sum_{j=1}^{i-1} \alpha_j \beta_j v_j = \sum_{j=1}^{i-1} \left(\alpha_i - \alpha_j\right) \beta_j v_j = 0$$

נזכיר ש- $\alpha_i - \alpha_j \neq 0$ לכל $1 \leq j \leq i-1$ וגם ש- $\beta_j \neq 0$ עבור j כלשהו כי $v_i \neq 0$,
לכן קיבלנו צירוף לינארי לא טריוויאלי שנותן 0, בסתירה להנחה ש- $\{v_1, v_2, \ldots, v_{i-1}\}$ בת"ל.

□

הערה 1.3.16. נשים לב כי שני וקטורים עצמיים שמתאימים לאותו ערך עצמי יכולים להיות ת"ל.
למשל אם $v \neq 0$ מקיים $Av = \alpha v$ אז לכל $\beta \neq 0$ מתקיים $A\beta v = \alpha\left(\beta v\right)$
ואז $\{v, \beta v\}$ היא קבוצה של ו"ע ת"ל.

משפט 1.3.17. תהי $A \in M_n(F)$. אם ל- A יש n ערכים עצמיים שונים, אז A לכסינה.

הוכחה. יהיו $\alpha_1, \alpha_2, \ldots, \alpha_n$ ערכים עצמיים שונים זה מזה עם וקטורים עצמיים מתאימים $v_1, v_2, \ldots, v_n$.
אז לפי משפט 1.3.15 הקבוצה $\{v_1, v_2, \ldots, v_n\}$בת"ל, וע"פ משפט משיעור קודם, המטריצה A לכסינה אם ורק אם קיימת קבוצה של n וקטורים עצמיים בת"ל. □

מסקנה 1.3.18. אם ל- $A \in M_n(F)$ יש n ערכים עצמיים שונים $\alpha_1, \alpha_2, \ldots, \alpha_n$, אז $A \sim \operatorname{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

ההיפך ממסקנה זו לא נכון: אם למטריצה $A \in M_n(F)$ יש פחות מ- n ערכים עצמיים שונים זה לא אומר שהיא לא לכסינה.
למשל למטריצה $A = \alpha I_n$ יש ערך עצמי יחיד α, אבל A אלכסונית ולכן לכסינה (דומה לעצמה).

מסקנה 1.3.19. תהי $M_n(F) \ni A = (\alpha_{ij})_{i,j=1}^{n}$ מטריצה משולשית (עליונה/תחתונה) כך ש- $\alpha_{ii} \neq \alpha_{jj}$ לכל $1 \leq i \neq j \leq n$. אז A לכסינה ודומה ל- $\text{diag}(\alpha_{11}, \alpha_{22}, \ldots, \alpha_{nn})$.

הוכחה. אם $A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ 0 & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha_{nn} \end{bmatrix}$, אז

$$\Delta_A(x) = \begin{vmatrix} x-\alpha_{11} & -\alpha_{12} & \cdots & -\alpha_{1n} \\ 0 & x-\alpha_{22} & \cdots & -\alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & x-\alpha_{nn} \end{vmatrix} = (x-\alpha_{11})(x-\alpha_{22})\cdots(x-\alpha_{nn})$$

ולכן השורשים של $\Delta_A(x)$ הם $\alpha_{11}, \alpha_{22}, \ldots, \alpha_{nn}$.
כלומר $\alpha_{11}, \alpha_{22}, \ldots, \alpha_{nn}$ הם ערכים עצמיים של A ולפי התנאי כולם שונים, לכן לפי מסקנה 1.3.18 המטריצה A לכסינה ודומה ל- $\text{diag}(\alpha_{11}, \alpha_{22}, \ldots, \alpha_{nn})$. □

הגדרה 1.3.20. תהי $A \in M_n(F)$ ועבור $\alpha \in F$ נכתוב $V_{A,\alpha} = \ker(\alpha I - A)$ (כאשר $\alpha I - A$ הוא אופרטור ליניארי).
אם α הוא ערך עצמי של A אז $V_{A,\alpha}$ נקרא המרחב העצמי של A המתאים לערך העצמי α.

הערה 1.3.21

1. $V_{A,\alpha}$ הוא תת מרחב של F^n לכל $\alpha \in F$.

2. אם α הוא ערך עצמי של A אז המרחב העצמי הוא $\ker(\alpha I - A)$.
זה מרחב הפתרונות של $(\alpha I = A)\,x = 0$, ז"א כל הוקטורים v שמקיימים $\alpha I v - Av = 0$.
המשוואה האחרונה שקולה ל- $Av = \alpha v$. לכן $V_{A,\alpha}$ הוא אוסף כל הוקטורים העצמיים המתאימים לערך העצמי α בתוספת וקטור האפס - $\vec{0}$.

3. $\dim(V_{A,\alpha}) > 0 \iff \alpha$ הוא ערך עצמי של A.

דוגמא 1.3.22. נתבונן במטריצה $A = \begin{bmatrix} 1 & 2 \\ 0 & 3 \end{bmatrix}$.
הערכים העצמיים של A הם $1, 3$ ומתקיים:

1. עבור $\alpha = 1$: $I - A = \begin{bmatrix} 0 & -2 \\ 0 & -2 \end{bmatrix}$ ואז $V_{A,1} = \text{span}\{e_1\}$.

2. עבור $\alpha = 3$: $3I - A = \begin{bmatrix} 2 & -2 \\ 0 & 0 \end{bmatrix}$ ואז $V_{A,3} = \text{span}\{e_1 + e_2\}$.

3. עבור $\alpha \neq 1, 3$: $\alpha I - A = \begin{bmatrix} \alpha - 1 \neq 0 & -2 \\ 0 & \alpha - 3 \neq 0 \end{bmatrix}$ מטריצה הפיכה, ולכן $V_{A,\alpha} = \left\{\vec{0}\right\}$.

1.4 ערך עצמי ומרחב עצמי של העתקה לינארית

1.4.1 ערכים עצמיים של אופרטור לינארי

הגדרה 1.4.1. יהי V מרחב וקטורי n-מימדי מעל שדה F ו- $T \in \text{End}(V)$. הפולינום האופייני של T שיסומן $\Delta_T(x)$, הוא הפולינום $\Delta_{M_T}(x)$, כאשר M_T היא מטריצה מייצגת של T לפי בסיס כלשהו.

הערה 1.4.2. מאחר ולמטריצות דומות יש אותו פולינום אופייני, ומטריצות מייצגות לפי בסיסים שונים הן דומות, נובע כי $\Delta_T(x)$ לא תלוי בבחירת בסיס ומטריצה מייצגת.

הגדרה 1.4.3. יהי V מרחב וקטורי n-מימדי מעל שדה F ו- $T \in \text{End}(V)$. אומרים ש- T לכסינה אם מטריצה מייצגת שלה M_T היא לכסינה.

הגדרה 1.4.4. יהי V מרחב וקטורי n-מימדי מעל שדה F ו- $T \in \text{End}(V)$. אז $\alpha \in F$ נקרא ערך עצמי של T ו- $0 \neq v \in V$ נקרא וקטור עצמי של T המתאים לערך α, אם מתקיים $T(v) = \alpha v$.
בהתאם: $V_{T,\alpha} = \{v \in V | T(v) = \alpha v\}$ נקרא המרחב העצמי של T המתאים ל- α.

הערה 1.4.5. לפי משפט 15 מהשיעור על וקטורים עצמיים וערכים עצמיים, ההעתקה T לכסינה $\Longleftrightarrow$ קיימת קבוצה של n וקטורים עצמיים בת"ל.

הגדרה 1.4.6. תת מרחב $W \subset V$ נקרא T-שמור אם לכל $w \in W$ מתקיים $T(w) \in W$.

דוגמא 1.4.7. במרחב $V = \text{span}\{e_1, e_2\}$ נתונה ההעתקה T ע"י $T(e_1) = 5e_1$ ו- $T(e_2) = 5e_1 + e_2$.
אז $W = \text{span}\{e_1\}$ הוא T-שמור, אבל תת המרחב $U = \text{span}\{e_2\}$ הוא לא T-שמור כי $T(e_2) = 5e_1 + e_2 \notin U$.

הערה 1.4.8

1. מרחב האפס $\left\{\vec{0}\right\}$ והמרחב V כולו הם תמיד T-שמורים. אלה שני תתי מרחב T-שמורים טריוויאליים.

2. יהי $W \subset V$ תת מרחב ו- $w_1, \ldots, w_k$ בסיס של W. כדי לבדוק האם W הוא T שמור מספיק לבדוק אם לכל $1 \leq i \leq k$ מתקיים $T(w_i) \in W$ (תרגיל: מדוע זה מספיק?)

דוגמא 1.4.9

1. יהי $T \in \text{End}(V)$, α ערך עצמי של T ו- $v \in V_{T,\alpha}$ עבורו $T(v) = \alpha v$. אז $V_{T,\alpha}$ הוא תת מרחב T-שמור.

2. יהי $0 \neq v \in V$ ו- $W = \text{span}\left\{v, T(v), T^2(v), \ldots, T^{n-1}(v)\right\}$ (n וקטורים).
נראה קודם כי $T^{n+j}(v) \in \text{span}\left\{v, T(v), T^2(V), \ldots, T^{n-1}(V)\right\}$ לכל $j \geq 0$:
אם $\left\{v, T(v), T^2(V), \ldots, T^{n-1}(V)\right\}$ בת"ל אז זהו בסיס של V, ובפרט $T^{n+j}(v) \in W = V$.
אם $\left\{v, T(v), T^2(V), \ldots, T^{n-1}(V)\right\}$ ת"ל אז קיים $0 \leq k \leq n-2$ כך ש-
$\left\{v, T(v), T^2(V), \ldots, T^k(V)\right\}$ בת"ל ו- $\left\{v, T(v), T^2(V), \ldots, T^{k+1}(V)\right\}$ ת"ל,
כי $v \neq 0$ כך שהקבוצה $\{v\}$ בת"ל, ומתחילים להוסיף וקטורים עד שבשלב $k+1$ מקבלים קבוצה תלויה לינארית.
זאת אומרת שהוקטור האחרון הוא צ"ל של קודמיו –

$$T^{k+1}(v) = \sum_{i=0}^{k} \alpha_i T^i(v)$$

כל וקטור בקבוצה מתקבל ע"י פעולה של T על קודמו – $T\left(T^i(v)\right) = T^{i+1}(v)$ לכן

$$\begin{aligned} T : \text{span}\left\{v, T(v), T^2(v), \ldots, T^k(v)\right\} &\to \text{span}\left\{T(v), T^2(v), \ldots, T^{k+1}(v)\right\} \\ &\subseteq \text{span}\left\{v, T(v), T^2(v), \ldots, T^k(v)\right\} \end{aligned}$$

ז"א $\operatorname{span}\left\{v, T(v), T^2(v), \ldots, T^k(v)\right\}$ הוא T-שמור ולכן גם T^j-שמור לכל $j \geq 1$.
בפרט נקבל ש-

$$T^{k+j}(v) \in \operatorname{span}\left\{v, T(v), T^2(v), \ldots, T^k(v)\right\}$$

לכל $j \geq 1$.

כדי לקבל את המקדמים נחשב, למשל עבור $T^{k+2}(v)$ ונקבל:

$$\begin{aligned}
T^{k+2}(v) &= T\left(T^{k+1}(v)\right) = T\left(\sum_{i=0}^{k} \alpha_i T^i(v)\right) = \sum_{i=0}^{k} \alpha_i T^{i+1}(v) \\
&= \sum_{i=0}^{k-1} \alpha_i T^{i+1}(v) + T^{k+1}(v) \\
&= \sum_{i=0}^{k-1} \alpha_i T^{i+1}(v) + \alpha_k \sum_{i=0}^{k} \alpha_i T^i(v) = \sum_{i=0}^{k} \beta_i T^i(v)
\end{aligned}$$

כאשר $\beta_0 = \alpha_0 \alpha_k$ ו- $\beta_i = \alpha_i \alpha_k + \alpha_{i-1}$ לכל $1 \leq i \leq k$.
בפרט מקבלים כי

$$T^n(v) \in \operatorname{span}\left\{v, T(v), T^2(v), \ldots, T^k(v)\right\} = \operatorname{span}\left\{v, T(v), T^2(V), \ldots, T^{n-1}(V)\right\}.$$

הגדרה 1.4.10. יהיו $T \in \operatorname{End}(V)$ ו- $0 \neq v \in V$. תת המרחב $\left\{v, T(v), T^2(V), \ldots, T^{n-1}(V)\right\}$ span נקרא תת מרחב מסלולי של T הנוצר ע"י v.

הערה 1.4.11 1. השם **תת מרחב מסלולי** כי הוא נפרש ע"י מסלול של T: $v \xrightarrow{T} T(v) \xrightarrow{T} T^2(v) \xrightarrow{T} \cdots$.

2. תת מרחב מסלולי הוא חד מימדי $\Longleftrightarrow$ v הוא וקטור עצמי של T.

הסבר (ל- 2.): אם תת מרחב מסלולי הוא חד מימדי אז $\{0 \neq v, T(v)\}$ ת"ל, כלומר $T(v) = \alpha v$ ולכן v הוא וקטור עצמי של T.

1.4.2 סכום ישר

הגדרה 1.4.12. 1. יהי V מרחב וקטורי ו- $U, W \subseteq V$ תתי מרחב.
אומרים ש= $V = U + W$ אם לכל $v \in V$ קיימים $u \in U$ ו- $w \in W$ כך ש- $v = u + w$.
(במקרה זה אומרים גם שלכל $v \in V$ יש פירוק לסכום של וקטור ב- U ווקטור ב- W).

2. אומרים ש- $V = U \oplus W$ סכום ישר אם מתקיימים:

(א) לכל $v \in V$ קיימים $u \in U$ ו- $w \in W$ כך ש- $v = u + w$.

(ב) הפירוק הזה יחיד.

אם $V = U \oplus W$ אומרים גם ש- W משלים את U עד V.

דוגמא 1.4.13. נתונים $W = \left\{\overrightarrow{0}\right\}$, $U = V$, אז $V = U \oplus W$, ז"א כל מרחב הוא סכום ישר של תתי המרחבים הטריוויאליים שלו.

דוגמא 1.4.14. יהי V מרחב וקטורי n-מימדי מעל שדה F ותהי $\{v_1, \ldots, v_k\}$ קבוצה בת"ל.
נגדיר $U = \operatorname{span}\{v_1, \ldots, v_k\}$ ונשלים את $\{v_1, \ldots, v_k\}$ לבסיס $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$ של V. כעת נגדיר

$W=\text{span}\left\{v_{k+1},\ldots,v_n\right\}$.
אז $V=U\oplus W$. (תרגיל – למה?)

משפט 1.4.15. יהי מרחב וקטורי סוף מימדי מעל שדה F, ו- $U,W\subseteq V$ תתי מרחב כך ש- $V=U+W$. אז

$$\dim V=\dim U+\dim W-\dim U\cap W\,.$$

הוכחה. ניקח בסיס $\left\{v_1,\ldots,v_i\right\}$ של $U\cap W$ ונשלים אותו לבסיסים $\left\{v_1,\ldots,v_i,u_1,\ldots u_m\right\}$ של U ו- $\left\{v_1,\ldots,v_i,w_1,\ldots,w_k\right\}$ של W.
אז הקבוצה $\left\{v_1,\ldots,v_i,u_1,\ldots u_m,w_1,\ldots w_k\right\}$ פורשת את V כי כל וקטור ב- V הוא סכום של וקטור ב- U (שנפרש ע"י $\left\{v_1,\ldots,v_i,u_1,\ldots u_m\right\}$) ושל וקטור ב- W (שנפרש ע"י $\left\{v_1,\ldots,v_i,w_1,\ldots,w_k\right\}$).
נראה ש- $\left\{v_1,\ldots,v_i,u_1,\ldots u_m,w_1,\ldots w_k\right\}$ בת"ל, ואז נקבל שהיא בסיס של V:
נניח בשלילה שהקבוצה $\left\{v_1,\ldots,v_i,u_1,\ldots u_m,w_1,\ldots w_k\right\}$ היא ת"ל.
הקבוצה $\left\{v_1,\ldots,v_i,u_1,\ldots u_m\right\}$ היא בת"ל כבסיס של U, ולכן קיים $j\geq 1$ כך ש- $\left\{v_1,\ldots,v_i,u_1,\ldots u_m,w_1,\ldots,w_{j-1}\right\}$ בת"ל ו-

$$w_j=\sum_{s=1}^{i}\alpha_s v_s+\sum_{t=1}^{m}\beta_t u_t+\sum_{q=1}^{j-1}\gamma_q w_q$$

הוא צירוף לינארי של קודמיו.
אז

$$W\ni w_j-\sum_{q=1}^{j-1}\gamma_q w_q=\sum_{s=1}^{i}\alpha_s v_s+\sum_{t=1}^{m}\beta_t u_t\in U$$

ולכן

$$\sum_{s=1}^{i}\alpha_s v_s+\sum_{t=1}^{m}\beta_t u_t\in U\cap W$$

ומכאן ש- $\beta_t=0$ לכל $1\leq t\leq m$ כך ש-

$$w_j-\sum_{q=1}^{j-1}\gamma_q w_q=\sum_{s=1}^{i}\alpha_s v_s$$

או במילים אחרות

$$w_j-\sum_{q=1}^{j-1}\gamma_q w_q-\sum_{s=1}^{i}\alpha_s v_s=\overrightarrow{0}$$

וזה צירוף לא טריוויאלי, בסתירה לאי תלות של $\left\{v_1,\ldots,v_i,w_1,\ldots,w_k\right\}$.
מכאן נקבל כי

$$\dim V=i+m+k=(i+m)+(i+k)-i=\dim U+\dim W-\dim U\cap W$$

□

משפט 1.4.16. יהי V מרחב וקטורי מעל שדה F עם תתי מרחב $U,W\subseteq V$. אז $V=U\oplus W$ אם ורק אם מתקיימים שני התנאים:

1. $V=U+W$.

ג. $U \cap W = \left\{ \overrightarrow{0} \right\}$.

הוכחה. $\Longleftarrow$: נניח ש- $V = U \oplus W$, אז תנאי 1. נובע מיידית.
צריך לבדוק ש- $U \cap W = \left\{ \overrightarrow{0} \right\}$.
יהי $v \in U \cap W$ אז $v = v + \overrightarrow{0}$ (כאשר $v \in U,\ \overrightarrow{0} \in W$),
ובאותו אופן $v = \overrightarrow{0} + v$ (כאשר $\overrightarrow{0} \in U,\ v \in W$).
מיחידות ההצגה נקבל $v + \overrightarrow{0} = \overrightarrow{0} + v \Longrightarrow v = \overrightarrow{0}$,
כלומר $U \cap W = \left\{ \overrightarrow{0} \right\}$.

$\Longrightarrow$: נניח שמתקיימים תנאים 1. ו- 2. ונבדוק שזהו סכום ישר:

לפי 1. קיימת הצגה של כל $v \in V$ כסכום של וקטורים מ- U ומ- W. נבדוק שזו הצגה יחידה.
נניח שקיימות שתי הצגות $v = u_1 + w_1 = u_2 + w_2$.
זה אומר ש- $u_1 - u_2 = w_2 - w_1$ כאשר $u_1 - u_2 \in U$ ו- $w_1 - w_2 \in W$.
לכן $u_1 - u_2 \in U \cap W$ וזה אומר ש- $u_1 - u_2 = \overrightarrow{0}$, כלומר $u_1 = u_2$.
שיקול דומה מראה ש- $w_1 = w_2$, ולכן ההצגה היא יחידה, ז"א $V = U \oplus W$. $\square$

מסקנה 1.4.17. יהי V מרחב וקטורי סוף מימדי מעל שדה F עם תתי מרחב $U, W \subseteq V$. יהיו $\{u_1, \ldots, u_m\}$ בסיס של U ו- $\{w_1, \ldots, w_k\}$ בסיס של W.
אז

$$V = U \oplus W \Longleftrightarrow \{u_1, \ldots, u_m, w_1, \ldots, w_k\} \text{ בסיס של } V.$$

הוכחה. 1. אם $V = U \oplus W$ אז $V = U + W$ ו- $U \cap W = \left\{ \overrightarrow{0} \right\}$ לפי משפט 1.4.16
אז לפי משפט 1.4.15 $\{u_1, \ldots u_m, w_1, \ldots, w_k\}$ הוא בסיס של V.

2. נניח ש- $\{u_1, \ldots u_m, w_1, \ldots, w_k\}$ בסיס של V, אז $V = U + W$. נראה כי $U \cap W = \left\{ \overrightarrow{0} \right\}$:
אם $v \in U \cap W$ אז

$$v = \sum_{i=1}^{m} \alpha_i u_i = \sum_{j=1}^{k} \beta_j w_j$$

כך ש-

$$\sum_{i=1}^{m} \alpha_i u_i - \sum_{j=1}^{k} \beta_j w_j = \overrightarrow{0}.$$

נזכיר ש- $\{u_1, \ldots u_m, w_1, \ldots, w_k\}$ בת"ל, ולכן $\alpha_i = \beta_j = 0$ לכל $1 \leq i \leq m,\ 1 \leq j \leq k$, ז"א $v = \overrightarrow{0}$,
ולכן ע"פ משפט 1.4.16 מקבלים $V = U \oplus W$.

$\square$

ניתן להכליל את ההגדרה לסכום ישר של k תתי מרחב:

הגדרה 1.4.18. יהי V מרחב וקטורי מעל שדה F עם תתי מרחב $U_1, U_2, \ldots, U_k \subseteq V$. אומרים ש-

1. $V = U_1 + U_2 + \cdots + U_k$ סכום אם לכל $v \in V$ קיימת הצגה $v = u_1 + \cdots + u_k$ כאשר $u_i \in U_i$ לכל $1 \leq i \leq k$.

2. $V = U_1 \oplus U_2 \oplus \cdots \oplus U_k$ סכום ישר אם לכל $v \in V$ קיימת **הצגה יחידה** $v = u_1 + \cdots + u_k$ כאשר $u_i \in U_i$ לכל $1 \leq i \leq k$.

משפט 1.4.19. יהי V מרחב וקטורי מעל שדה F עם תתי מרחב $U_1, U_2, \ldots, U_k \subseteq V$. אז $V = U_1 \oplus U_2 \oplus \cdots \oplus U_k$ אם ורק אם מתקיימים שני התנאים הבאים:

1. $V = U_1 + U_2 + \cdots + U_k$.
2. לכל $1 \le i \le k$ מתקיים $U_i \cap \sum_{j \neq i} U_j = \left\{ \overrightarrow{0} \right\}$.

לפני שנוכיח את המשפט נראה שהתנאי $U_i \cap U_j = \left\{ \overrightarrow{0} \right\}$ לכל $1 \le i \neq j \le k$
(זו דרישה חלשה יותר מ- 2) לא מספיק:
ניקח כדוגמא $V = F^2$ ושלושה תתי מרחב

$$U_1 = \text{span}\left\{ e_1 \right\}, \; U_2 = \text{span}\left\{ e_2 \right\}, \; U_3 = \text{span}\left\{ e_1 + e_2 \right\}$$

אז מתקיימים

1. $V = U_1 + U_2 + U_3$.
2. $U_1 \cap U_2 = U_1 \cap U_3 = U_2 \cap U_3 = \left\{ \overrightarrow{0} \right\}$.

אבל $V \neq U_1 \oplus U_2 \oplus U_3$ כי ההצגה **אינה** יחידה.
למשל:

$$v = \alpha e_1 + \beta e_2 + \overrightarrow{0} = (\alpha - \beta)\, e_1 + \overrightarrow{0} + \beta(e_1 + e_2).$$

הוכחה. 1. נניח ש- $V = U_1 \oplus U_2 \oplus \cdots \oplus U_k$. אז תנאי 1 מתקיים מיידית.
זאת אומרת שלכל v קיימת הצגה $v = u_1 + \cdots + u_k$ כאשר $u_i \in U_i$ לכל $1 \le i \le k$. צריך לבדוק שתנאי 2 מתקיים.
נסמן $W_i = \sum_{i \neq j} U_j$ אז לפי ההגדרה נקבל $V = U_i \oplus W_i$ כי לכל $v \in V$ יש הצגה יחידה $v = u_i + (u_1 + \cdots + u_{i-1} + u_{i+1} + \cdots + u_k)$ כלומר כסכום של הוקטורים $u_i \in U_i$ ו-$u_1 + \cdots + u_{i-1} + u_{i+1} + \cdots + u_k \in W_i$.
מכאן לפי משפט 1.4.16: $U_i \cap W_i = \left\{ \overrightarrow{0} \right\}$, כלומר $U_i \cap \sum_{j \neq i} U_j = \left\{ \overrightarrow{0} \right\}$, וזה מתקיים לכל $1 \le i \le k$.

2. נניח שהתנאים 1 ו- 2 מתקיימים ונראה ש- $V = U_1 \oplus U_2 \oplus \cdots \oplus U_k$:
לפי תנאי 1 לכל $v \in V$ יש הצגה $v = u_1 + \cdots + u_k$ כאשר $u_i \in U_i$. צריך להראות שהצגה זו היא יחידה.
נניח שיש הצגה נוספת $v = u_1 + \cdots + u_k = w_1 + \cdots + w_k$ כאשר $u_i, w_i \in U_i$ לכל $1 \le i \le k$.
אז נעביר אגפים:

$$u_i - w_i = w_1 + \cdots + w_{i-1} + w_{i+1} + \cdots + w_k - (u_1 + \cdots + u_{i-1} + u_{i+1} + \cdots + u_k)$$

ונשים לב ש- $u_i - w_i \in U_i$ ו- $w_1 + \cdots + w_{i-1} + w_{i+1} + \cdots + w_k \in W_i$, וגם $u_1 + \cdots + u_{i-1} + u_{i+1} + \cdots + u_k \in W_i$.
מכאן

$$u_i - w_i = w_1 + \cdots + w_{i-1} + w_{i+1} + \cdots + w_k - (u_1 + \cdots + u_{i-1} + u_{i+1} + \cdots + u_k) \in W_i$$

כלומר $u_i - w_i \in U_i \cap W_i$ ולפי תנאי 2, $u_i - w_i = \overrightarrow{0}$,
או במילים אחרות $u_i = w_i$ לכל i.
זה אומר שההצגה היא יחידה ומכאן ש- $V = U_1 \oplus \cdots \oplus U_k$. □

תרגיל 1.4.20 יהי V מרחב וקטורי סוף מימדי מעל שדה F, ו- $U_1, U_2, \ldots, U_k \subset V$ תתי מרחב עם בסיסים $B_i = \left\{ u_1^{(i)}, \ldots u_{k_i}^{(i)} \right\}$ בהתאם.

1. להראות כי $V = U_1 \oplus \cdots \oplus U_k$ אם ורק אם $B_1 \sqcup B_2 \sqcup \cdots \sqcup B_k$ הוא בסיס של V (כאשר הסימן $\sqcup$ מסמן איחוד זר).

2. להראות כי אם V הוא סכום של תתי המרחב $U_1, U_2, \ldots, U_k$ אז $V = U_1 \oplus \cdots \oplus U_k$ אם ורק אם $\dim V = \sum_{i=1}^{k} \dim U_i$.

תזכורת: $T \in \mathrm{End}(V)$ ו- α ערך עצמי של T.
המרחב העצמי של T שמתאים ל- α הוא

$$V_{T,\alpha} = \{v \in V : T(v) = \alpha v\} = \ker(\alpha I - T).$$

משפט 1.4.21. יהי V מרחב וקטורי סוף מימדי מעל שדה F ויהי $T \in \mathrm{End}(V)$ עם $\alpha_1, \ldots, \alpha_k \in F$ ערכים עצמיים שונים של T. נסמן $W = \sum_{i=1}^{k} V_{T,\alpha_i}$. אז

$$W = V_{T,\alpha_1} \oplus \cdots \oplus V_{T,\alpha_k}.$$

הוכחה. לפי ההגדרה $W = \sum_{i=1}^{k} V_{T,\alpha_i}$, לכן צריך רק לבדוק שמתקיים תנאי 2 ממשפט 1.4.19.
נתבונן ב-

$$v \in V_{T,\alpha_i} \cap \sum_{\substack{j=1 \\ j \neq i}}^{k} V_{T,\alpha_j}.$$

נניח ש- $v \neq 0$, אז קיימים $j_1, \ldots, j_s \in \{1, \ldots, i-1, i+1, \ldots, k\}$
כך ש- $v = v_{j_1} + \cdots + v_{j_s}$, כאשר $v_{j_t} \in V_{T,\alpha_t}$ ו- $v_{j_t} \neq 0$.
נקבל מצד אחד

$$V_{T,\alpha_i} \ni T(v) = \alpha_i v = \alpha_i \left(v_{j_1} + \cdots + v_{j_s}\right) = \sum_{t=1}^{s} \alpha_i v_{j_t}$$

ומצד שני

$$\begin{aligned} T(v) &= T(v_{j_1} + \cdots + v_{j_s}) = T(v_{j_1}) + \cdots + T(v_{j_s}) \\ &= \alpha_{j_1} v_{j_1} + \cdots + \alpha_{j_s} v_{j_s} = \sum_{t=1}^{s} \alpha_{j_t} v_{j_t} \end{aligned}$$

ואז

$$0 = T(v) - T(v) = \sum_{t=1}^{s} \alpha_i v_{j_t} - \sum_{t=1}^{s} \alpha_{j_t} v_{j_t} = \sum_{t=1}^{s} \left(\alpha_i - \alpha_{j_t}\right) v_{j_t}$$

נשים לב ש- $\alpha_i - \alpha_{j_t} \neq 0$ וגם $v_{j_t} \neq 0$.
זה אומר שהקבוצה $\{v_{j_t}\}$ תלויה לינארית, בסתירה למשפט שאומר שקבוצה של וקטורים עצמיים ששייכים לערכים עצמיים שונים היא בת"ל.

לכן לכל i מתקיים

$$V_{T,\alpha_i} \cap \sum_{\substack{j=1 \\ j \neq i}}^{k} V_{T,\alpha_j} = \left\{\overrightarrow{0}\right\}$$

ולפי משפט 1.4.19 מקבלים

$$\sum_{j=1}^{k} V_{T,\alpha_j} = V_{T,\alpha_1} \oplus \cdots \oplus V_{T,\alpha_k}$$

וזה סכום ישר. $\square$

כמסקנה נקבל תנאי ללכסינות של אופרטור:

משפט 1.4.22. יהי V מרחב וקטורי סוף מימדי מעל שדה F ו- $T \in \mathrm{End}(V)$.
נסמן ב- $\alpha_1, \ldots, \alpha_k$ את קבוצת כל הערכים העצמיים השונים של T.
אז T לכסין אם ורק אם

$$V = \bigoplus_{i=1}^{k} V_{T,\alpha_i} = V_{T,\alpha_1} \oplus \cdots \oplus V_{T,\alpha_k}.$$

הוכחה. כיוון ראשון: נניח ש- T לכסין, ו- $\alpha_1, \ldots, \alpha_k$ ערכים עצמיים שונים שלו.
יהיו $V_{T,\alpha_1} \ldots, V_{T,\alpha_k}$ מרחבים עצמיים בהתאם.
T לכסין $\Longleftarrow$ קיים בסיס $\{v_1, \ldots, v_n\}$ שכל וקטור בו הוא וקטור עצמי.
זאת אומרת לכל v_i כאשר $1 \le i \le n$ קיים α_{s_i} כך ש-

$$v_i \in V_{T,\alpha_{s_i}} \iff Tv_i = \alpha_{s_i} v_i.$$

קיבלנו שלכל j מתקיים $v_j \in \sum_{i=1}^{k} V_{T,\alpha_i}$, כלומר $V \subseteq \sum_{i=1}^{k} V_{T,\alpha_i}$.
מצד שני, כל $V_{T,\alpha_i} \subseteq V$ (אלה תתי מרחב), לכן $\sum_{i=1}^{k} V_{T,\alpha_i} \subseteq V$.
מכאן נקבל ש-

$$V = \sum_{i=1}^{k} V_{T,\alpha_i} = \bigoplus_{i=1}^{k} V_{T,\alpha_i}$$

(השוויון השני מתקבל ממשפט 1.4.21).

כיוון שני: נניח ש- $V = \bigoplus_{i=1}^{k} V_{T,\alpha_i}$.
ניקח קבוצה שהיא איחוד של בסיסים של $V_{T,\alpha_1} \ldots, V_{T,\alpha_k}$.
הקבוצה הזו מהווה בסיס של V כי היא פורשת את V והיא בת"ל. (תרגיל: למה היא פורשת את V? למה היא בת"ל?)
נקבל בסיס של V שבו כל וקטור הוא וקטור עצמי של T, לכן T לכסין. $\square$

1.4.3 ריבוי של ערכים עצמיים

הגדרה 1.4.23. יהי V מרחב וקטורי סוף מימדי מעל שדה F, $T \in \mathrm{End}(V)$, ו- α ערך עצמי של T.
אז

1. הריבוי של α כשורש של הפולינום האופייני של T נקרא ריבוי אלגברי של α.

2. $\dim V_{T,\alpha}$ נקרא ריבוי גיאומטרי של α.

הסבר (ל- 1.): אם α הוא שורש של הפולינום $\Delta_T(x)$ אז אפשר לכתוב $\Delta_T(x) = (x-\alpha)^m \cdot p(x)$ כאשר $p(\alpha) \neq 0$.
אז m הוא הריבוי האלגברי של α.

משפט 1.4.24. יהי V מרחב וקטורי סוף מימדי מעל שדה F, $T \in \mathrm{End}(V)$, ו- $\alpha \in F$ ערך עצמי של T.
אז הריבוי הגיאומטרי של α קטן או שווה לריבוי האלגברי שלו.

הוכחה. נתבונן ב- $V_{T,\alpha} \subseteq V$. יהי $\{v_1, \dots, v_i\}$ בסיס של $V_{T,\alpha}$.
נשלים את הבסיס $\{v_1, \dots, v_i\}$ לבסיס של V:

$$B = \{v_1, \dots, v_i, v_{i+1}, \dots v_n\}$$

ונתבונן באופרטור לפי הבסיס B –

$$[M_T]_B = \begin{bmatrix} \alpha & 0 & & \beta_{1,i+1} & \cdots & \beta_{1n} \\ 0 & \ddots & 0 & \vdots & \vdots & \vdots \\ 0 & 0 & \alpha & \vdots & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & \beta_{n,i+1} & \cdots & \beta_{nn} \end{bmatrix}$$

ב- i העמודות הראשונות מופיע α פעם אחת בכל עמודה בדיוק על האלכסון.
אז

$$\Delta_T(x) = \begin{vmatrix} x-\alpha & 0 & & -\beta_{1,i+1} & \cdots & -\beta_{1n} \\ 0 & \ddots & 0 & \vdots & \vdots & \vdots \\ 0 & 0 & x-\alpha & \vdots & & \\ & & & x-\beta_{i+1,i+1} & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & -\beta_{n,i+1} & \cdots & x-\beta_{nn} \end{vmatrix}$$
$$= (x-\alpha)^i \begin{vmatrix} x-\beta_{i+1,i+1} & -\beta_{i+1,i+2} & \cdots & -\beta_{i+1,n} \\ \vdots & \vdots & \vdots & \vdots \\ -\beta_{n,i+1} & \cdots & \cdots & x-\beta_{nn} \end{vmatrix}$$

והדטרמיננטה הזו היא פולינום מדרגה $n-i$.
לכן $\Delta_T(x) = (x-\alpha)^i p(x)$, ו- i הוא הריבוי הגיאומטרי.

- אם α הוא שורש של $p(x)$ אז הריבוי האלגברי של α גדול מ- i.
- אם α לא שורש של $p(x)$ אז הריבוי האלגברי של α שווה ל- i.

קיבלנו אם כך שהריבוי האלגברי גדול או שווה לריבוי הגיאומטרי. □

נראה כי הריבוי האלגברי יכול להיות גדול כרצוננו מהריבוי הגיאומטרי:
נתבונן ב-

$$A = \begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \ddots & \ddots & 0 \\ 0 & 0 & \alpha & 1 \\ 0 & 0 & 0 & \alpha \end{pmatrix}$$

כלומר α על האלכסון הראשי ו- 1 באלכסון שמעליו.
זו מטריצה משולשת עליונה ולכן ניתן למצוא בקלות כי $\Delta_A(x) = (x-\alpha)^n$.
נשים לב ש- α הוא הערך העצמי היחיד, והריבוי האלגברי שלו הוא n.
מצד שני, הריבוי הגיאומטרי הוא המימד של מרחב הפתרונות של

$$(A-\alpha I)x = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & \ddots & \ddots & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} x = 0$$

והדרגה היא $\operatorname{rank}(A-\alpha I) = n-1$.
לכן הריבוי הגיאומטרי של α הוא

$$\dim\ker(A-\alpha I) = n - \operatorname{rank}(A-\alpha I) = 1 .$$

מסקנה 1.4.25. יהי V מרחב וקטורי ממימד n מעל שדה F ו- $T \in \operatorname{End}(V)$, ויהי α ערך עצמי של T.
אם הריבוי האלגברי של α הוא 1 אז גם הריבוי הגיאומטרי שלו הוא 1.

הוכחה. ראינו ש- $1 \leq$הריבוי הגיאומטרי $\leq$הריבוי האלגברי $= 1$, ומכאן נובע שהריבוי הגיאומטרי $= 1$. $\square$

מסקנה 1.4.26. יהי V מרחב וקטורי ממימד n מעל שדה F ו- $T \in \operatorname{End}(V)$. אז T לכסין אם ורק אם מתקיימים שני התנאים הבאים:

1. כל ערך עצמי שייך ל- F.
   זה שקול לכך שקיימים $\alpha_1, \ldots, \alpha_k$ כך ש- $\Delta(x) = \prod_{i=1}^{k}(x-\alpha_i)^{m_i}$, כאשר $m_1 + m_2 + \cdots + m_k = n$.
2. לכל ערך עצמי יש ריבוי גיאומטרי שווה לריבוי האלגברי.

הוכחה. תנאי 1 ברור.
נניח ש- T לכסין, אז לפי משפט 1.4.22: $V = \bigoplus_{i=1}^{k} V_{T,\alpha_i}$ ולכן

$$n = \dim(V) = \sum_{i=1}^{k} \dim\left(V_{T,\alpha_i}\right)$$

כלומר n הוא סכום של ריבויים גיאומטריים.
מצד שני, n הוא סכום של ריבויים אלגבריים.

$$n = m_1 + m_2 + \cdots + m_k = \text{ריבויים אלגבריים}$$
$$n = s_1 + s_2 + \cdots + s_k = \text{ריבויים גיאומטריים}$$

לפי משפט $1.4.24$ נובע ש- $s_i \leq m_i$ לכל $i = 1, \ldots, k$.
לכן גם $s_1 + s_2 + \cdots + s_k \leq m_1 + m_2 + \cdots + m_k$ ומקבלים שוויון אם ורק אם $s_i = m_i$ לכל $i = 1, \ldots, k$.
זאת אומרת שהריבוי האלגברי שווה לריבוי הגיאומטרי לכל α_i.
בכיוון השני:
נניח שהריבוי האלגברי שווה לריבוי הגיאומטרי לכל α_i.

לכן סכום הריבויים הגיאומטריים הוא n, ומכאן ש-

$$\dim\left(\bigoplus_{i=1}^{k} V_{T,\alpha_i}\right) = n ,$$

כלומר $V = \bigoplus_{i=1}^{k} V_{T,\alpha_i}$, ולפי משפט 1.4.22 מקבלים ש- T לכסין. $\square$

1.5 משפט קיילי – המילטון

1.5.1 מטריצה נלווית

כפי שלמדנו, הפולינום האופייני של מטריצה $A \in M_n(F)$ הוא פולינום מתוקן מדרגה n עם מקדמים מ- F.

נסמן את אוסף כל הפולינומים עם מקדמים מ- F על-ידי $F[x]$.

שאלה 1.5.1. נתון פולינום מתוקן מדרגה n ב- $F[x]$:

$$p(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$$

האם קיימת מטריצה $A \in M_n(F)$ כזאת ש- $\Delta_A(x) = p(x)$?

התשובה לשאלה מהעמוד הקודם היא חיובית. נציג מטריצה כזאת.

הגדרה 1.5.2. נתון פולינום מתוקן $p(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0 \in F[x]$.
מגדירים מטריצה $A \in M_n(F)$ על-ידי

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -\alpha_0 \\ 1 & 0 & \cdots & 0 & -\alpha_1 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & -\alpha_{n-2} \\ 0 & 0 & \cdots & 1 & -\alpha_{n-1} \end{pmatrix}.$$

במילים אחרות

$$(A)_{ij} = \begin{cases} 1, & j = i-1 \\ -\alpha_{i-1} & j = n \\ 0 & \text{אחרת} \end{cases}.$$

אז A נקראת מטריצה נלווית של $p(x)$.

טענה 1.5.3. יהי $p(x) \in F[x]$ פולינום מתוקן ותהי $A \in M_n(F)$ מטריצה נלווית שלו. אז $\Delta_A(x) = p(x)$.

הוכחה. נוכיח את הטענה באינדוקציה על n.
יהי $n = 2$, אז $p(x) = x^2 + \alpha x + \beta$ ו- $A = \begin{pmatrix} 0 & -\beta \\ 1 & -\alpha \end{pmatrix}$.
מקבלים

$$\Delta_A(x) = \begin{vmatrix} x & \beta \\ -1 & x+\alpha \end{vmatrix} = x(x+\alpha) + \beta = p(x).$$

עכשיו נניח שזה נכון ל- $n-1$ ונראה ל- n.

יהי $p(x)=x^n+\alpha_{n-1}x^{n-1}+\cdots+\alpha_1x+\alpha_0$, אז

$$.A=\begin{pmatrix}0&0&\cdots&0&-\alpha_0\\1&0&\cdots&0&-\alpha_1\\\vdots&\ddots&\ddots&\vdots&\vdots\\\vdots&\vdots&\ddots&0&-\alpha_{n-2}\\0&0&\cdots&1&-\alpha_{n-1}\end{pmatrix}$$

ובהתאם, בשימוש בפרוק לפי השורה הראשונה והנחת האינדוקציה מקבלים:

$$\begin{aligned}\Delta_A(x)&=\begin{vmatrix}x&0&\cdots&0&\alpha_0\\-1&x&\cdots&0&\alpha_1\\\vdots&\ddots&\ddots&\vdots&\vdots\\\vdots&\vdots&\ddots&x&\alpha_{n-2}\\0&0&\cdots&-1&x+\alpha_{n-1}\end{vmatrix}\\&=x\begin{vmatrix}x&\cdots&0&\alpha_1\\-1&\ddots&\vdots&\vdots\\\vdots&\ddots&x&\alpha_{n-2}\\0&\cdots&-1&x+\alpha_{n-1}\end{vmatrix}+(-1)^{n+1}\alpha_0\begin{vmatrix}-1&x&\cdots&0\\0&-1&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&-1\end{vmatrix}\\&=x\left(x^{n-1}+\alpha_{n-1}x^{n-2}+\cdots+\alpha_1\right)+(-1)^{n+1}\alpha_0(-1)^{n-1}=p(x)\end{aligned}$$

□

יהי $T\in\text{End}\,V$ ויהי $v\in V$.

- נזכיר שאנחנו יכולים לבנות תת-מרחב מסלולי $W=\text{span}\left\{v,Tv,\ldots,T^{k-1}v\right\}$ כאשר $\left\{v,Tv,\ldots,T^{k-1}v\right\}$ הוא בסיס של W ו- $T^kv=\alpha_0v+\alpha_1Tv+\cdots+\alpha_{k-1}T^{k-1}v$.
- בגלל שלפי הבניה W הוא T-שמור אנחנו מקבלים $T:W\to W$ כך שאפשר להתבונן על T כמו על אופרטור ליניארי של W.
- נסמן אותו ב- $T|_W\in\text{End}\,W$. הסימן $|_W$ נקרא "צמצום ל- W" ואנחנו צריכים אותו כדי לא לשכוח ש- T פועל כעקרון גם על מרחב וקטורי יותר "גדול" V, ש- W הוא תת-מרחב שלו.

מהו $[T|_W]_{\{v,Tv,\ldots,T^{k-1}v\}}$?
בגלל ש-

$$T\left(T^iv\right)=\begin{cases}T^{i+1}v&0\le i\le k-2\\\sum_{i=0}^{k-1}\alpha_iT^iv&i=k-1\end{cases}$$

מקבלים

$$[T|_W]_{\{v,Tv,\dots,T^{k-1}v\}} = \begin{pmatrix} 0 & 0 & \cdots & 0 & \alpha_0 \\ 1 & 0 & \cdots & 0 & \alpha_1 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & \alpha_{k-2} \\ 0 & 0 & \cdots & 1 & \alpha_{k-1} \end{pmatrix}.$$

ולפי טענה **1.5.3**, $\Delta_{T|_W}(x) = x^k - \alpha_{k-1}x^{k-1} - \cdots - \alpha_0$.

נזכיר כי בהינתן פולינום $p(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0 \in F[x]$ ומטריצה $A \in M_k(F)$, אפשר להגדיר מטריצה $p(A)$.

הגדרה 1.5.4. יהי $p(x) \in F[x]$. אומרים שהמטריצה $A \in M_k(F)$ מאפסת את $p(x)$ אם $p(A) = 0$.

הערה 1.5.5. כפי שראינו, אם מטריצות דומות גם פולינומים של המטריצות הם מטריצות דומות.
לכן אם $p(A) = 0$ אזי $p(B) = 0$ לכל B שדומה ל- A.
לכן נגדיר גם: אופרטור ליניארי $T \in \operatorname{End} V$ מאפס את הפולינום $p(x)$, אם $p(M_T) = 0$ לאיזושהי מטריצה מייצגת M_T של T.

שאלות:

- האם לכל מטריצה A יש פולינום ש- A מאפסת אותו?
- האם לכל פולינום יש מטריצה שמאפסת אותו?

התשובה לשתי השאלות היא חיובית.

1.5.2 משפט קיילי – המילטון

משפט 1.5.6 (קיילי – המילטון)**.** תהי $A \in M_n(F)$ אזי $\Delta_A(A) = 0$.

במילים אחרות – כל מטריצה ריבועית מאפסת את הפולינום האופייני שלה.
לפני הוכחת המשפט אנחנו צריכים להגדיר מטריצת בלוקים משולשת.
מטריצה $A \in M_{m\times n}(F)$ היא טבלה, לכן אפשר לחלק אותה לתת-מטריצות על ידי חלוקה של השורות ל- p קבוצות:

$$\{1,\dots,i_1\}, \{i_1+1,\dots,i_1+i_2\}, \dots \left\{\sum_{s=1}^{p-1} i_s + 1, \dots m\right\}$$

וחלוקה של העמודות ל- r קבוצות:

$$\{1,\dots,j_1\}, \{j_1+1,\dots,j_1+j_2\}, \dots \left\{\sum_{s=1}^{r-1} j_s + 1, \dots n\right\}.$$

נסמן את הבלוק הבנוי מקבוצה s של שורות $\left\{\sum_{\ell=1}^{s-1} i_\ell, \dots, \sum_{\ell=1}^{s} i_\ell\right\}$ וקבוצה t של עמודות $\left\{\sum_{\ell=1}^{t-1} j_\ell, \dots, \sum_{\ell=1}^{t} j_\ell\right\}$ על-ידי $A^{(s,t)}$.
שמים את האינדקסים בסוגריים למעלה כדי לא לבלבל עם המטריצה $A_{i,j}$ המתקבלת מ- A על-ידי מחיקה של שורה i ועמודה j.

במקרה הזה $A^{(s,t)} \in M_{i_s \times j_t}(F)$ ו-

$$.A = \begin{pmatrix} A^{(1,1)} & \dots & A^{(1,r)} \\ \vdots & \ddots & \vdots \\ A^{(p,1)} & \dots & A^{(p,r)} \end{pmatrix}$$

החלוקה הזאת היא טכנית לגמרי, ולפעמים היא מאד נוחה.
בפרט ניקח $A \in M_{n\times n}(F)$ ונחלק את n ל- p קבוצות:

$$\{1,\dots,i_1\},\{i_1+1,\dots,i_1+i_2\},\dots\left\{\sum_{s=1}^{p-1} i_s+1,\dots n\right\}$$

גם לפי שורות וגם לפי עמודות.
מקבלים מטריצת בלוקים שבה כל בלוק $A^{(s,s)} \in M_{i_s \times i_s}(F)$ הוא ריבועי.

הגדרה 1.5.7. מטריצת בלוקים $A = \left(A^{(s,t)}\right)_{1\le s,t\le p} \in M_n(F)$ כאשר $A^{(s,t)} \in M_{i_s \times i_t}(F)$ ו- $i_1+\dots+i_p = n$ נקראת:

1. מטריצת בלוקים משולשת עליונה, אם $A^{(s,t)} = 0$ לכל $s > t$.
2. מטריצת בלוקים משולשת תחתונה, אם $A^{(s,t)} = 0$ לכל $s < t$.
3. מטריצת בלוקים אלכסונית, אם $A^{(s,t)} = 0$ לכל $s \ne t$.

למה 1.5.8. תהי $A = \left(A^{(s,t)}\right)_{1\le s,t\le p} \in M_n(F)$ מטריצת בלוקים משולשת (עליונה או תחתונה) אז

א. $\det A = \prod_{i=1}^{p} \det A^{(i,i)}$.

ב. $\Delta_A(x) = \prod_{i=1}^{p} \Delta_{A^{(i,i)}}(x)$.

הוכחה. מספיק להוכיח כי $\det A = \prod_{i=1}^{p} \det A^{(i,i)}$, כי הפולינום האופייני הוא דטרמיננטה של המטריצה האופיינית, וגם היא מטריצת בלוקים משולשת.
כמו כן מספיק להוכיח את זה למטריצת בלוקים משולשת עליונה ול- 2 בלוקים אלכסוניים, ז"א $M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ כאשר

$$\begin{aligned} &M \in M_{n+m}(F) \\ &A = (\alpha_{i,j}) \in M_n(F) \\ &B = (\beta_{i,j}) \in M_{n\times m}(F) \\ &C \in M_m(F) \end{aligned}$$

ו- 0 היא מטריצת האפס ב- $M_{m\times n}$.
(תרגיל – למה מספיק להוכיח רק למטריצה כזאת?).
נוכיח באינדוקציה על n – הגודל של המטריצה A.
אם $n = 1$ אזי $\det M = \alpha_{1,1} \det C$ (פירוק לפי העמודה הראשונה).

נניח שזה נכון ל $n-1$ ונראה ל- n:

$$\det M=\sum_{i=1}^{n}(-1)^{1+i}\alpha_{1,i}M_{1,i}+\sum_{j=1}^{m}(-1)^{1+n+j}\beta_{1,j}M_{1,n+j}$$

כעת מספיק לשים לב כי לפי בניה של מינור והנחת האינדוקציה $M_{1,i}=A_{1,i}\det C$ לכל $1\leq i\leq n$ ולכל $1\leq j\leq m$.

מקבלים כי המטריצה המתקבלת ממחיקה של שורה 1 ועמודה $n+j$ היא מטריצת בלוקים עם חלוקה $(n-1,m)$ כאשר העמודה הראשונה של הבלוק האלכסוני מגודל m היא עמודת אפסים, כך שלפי הנחת האינדוקציה $M_{1,n+j}=0$.

לכן מקבלים:

$$\det M=\sum_{i=1}^{n}(-1)^{1+i}\alpha_{1,i}M_{1,i}=\sum_{i=1}^{n}(-1)^{1+i}\alpha_{1,i}A_{1,i}\det C$$
$$=\det C\sum_{i=1}^{n}(-1)^{1+i}\alpha_{1,i}A_{1,i}=\det A\det C$$

$\square$

למה 1.5.9. 1. תהיינה $A=\begin{pmatrix}A^{(1,1)} & A^{(1,2)}\\ 0 & A^{(2,2)}\end{pmatrix},\ B=\begin{pmatrix}B^{(1,1)} & B^{(1,2)}\\ 0 & B^{(2,2)}\end{pmatrix}\in M_{k+m}$ מטריצות בלוקים משולשות עליונות עם אותה חלוקה (k,m). אזי

$$AB=\begin{pmatrix}A^{(1,1)}B^{(1,1)} & A^{(1,1)}B^{(1,2)}+A^{(1,2)}B^{(2,2)}\\ 0 & A^{(2,2)}B^{(2,2)}\end{pmatrix}.$$

2. תהי $A=\left(A^{(s,t)}\right)_{1\leq s,t\leq p}\in M_n(F)$ משולשת (עליונה או תחתונה) אזי לכל $n\in\mathbb{N}$ המטריצה A^n היא מטריצה עם אותה חלוקה של בלוקים ולכל $1\leq s\leq p$ מתקיים $(A^n)^{(s,s)}=\left(A^{(s,s)}\right)^n$.
לכן גם לכל פולינום $p(x)$ מתקיים $(p(A))^{(s,s)}=p\left(A^{(s,s)}\right)$.

הוכחה. בדיקה מיידית. $\square$

למה 1.5.10. יהי $p(x)=p_1(x)\cdot p_2(x)\in F[x]$ ותהי $A\in M_n(F)$. אזי

$$p(A)=p_1(A)\cdot p_2(A)=p_2(A)\cdot p_1(A).$$

הוכחה. הוכחה: בגלל שפולינומים של A הם מטריצות מתחלפות אזי $p_1(A)\cdot p_2(A)=p_2(A)\cdot p_1(A)$ וברור שזה שווה ל- $p(A)$. $\square$

עכשיו אנחנו מוכנים להוכיח את משפט קיילי – המילטון:

הוכחה. נוכיח את המשפט בשני שלבים: בשלב הראשון נראה שזה נכון לתת-מרחב מסלולי של T.
יהי $T\in\operatorname{End}V$ ויהי $v\in V$. נזכיר שאנחנו יכולים לבנות תת-מרחב מסלולי

$$W=\operatorname{span}\left\{v,Tv,\ldots,T^{k-1}v\right\}$$

כאשר $\{v, Tv, \ldots, T^{k-1}v\}$ בסיס של W ו- $T^k v = \alpha_0 v + \alpha_1 Tv + \cdots + \alpha_{k-1}T^{k-1}v$.
אז

$$[T|_W]_{\{v,Tv,\ldots,T^{k-1}v\}} = \begin{pmatrix} 0 & 0 & \cdots & 0 & \alpha_0 \\ 1 & 0 & \cdots & 0 & \alpha_1 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 & \alpha_{k-2} \\ 0 & 0 & \cdots & 1 & \alpha_{k-1} \end{pmatrix}$$

ו- $\Delta_{T|_W}(x) = x^k - \alpha_{k-1}x^{k-1} - \cdots - \alpha_0$.

כעת

$$\Delta_{T|_W}(T)v = T^k v - \alpha_{k-1}T^{k-1}v - \cdots - \alpha_0 Iv.$$
$$= \big(\alpha_0 v + \alpha_1 Tv + \cdots + \alpha_{k-1}T^{k-1}v\big) - \big(\alpha_0 v + \alpha_1 Tv + \cdots + \alpha_{k-1}T^{k-1}v\big) = \overrightarrow{0}$$

לכל $T^i v$ מקבלים לפי למה 1.5.10

$$\Delta_{T|_W}(T)T^i v = T^i \Delta_{T|_W}(T)v = \overrightarrow{0}$$

כך ש- $\Delta_{T|_W}(T)w = \overrightarrow{0}$ לכל w בבסיס של W וזאת אומרת $\Delta_{T|_W}(T) = 0$.

בשלב השני נוכיח את הטענה באינדוקציה על המימד של V:
יהיו $\dim V = 2$ ו- $T \in \mathrm{End}\, V$. אזי או ש- T הוא אופרטור סקלרי, ז"א $T = \alpha I_2$ לאיזשהו $\alpha \in F$ או שהוא לא סקלרי.
אם T לא סקלרי אזי קיים $v (\neq \overrightarrow{0})$ כך שהוא לא ווקטור עצמי, ולכן הקבוצה $\{v, Tv\}$ בת"ל.
זאת אומרת V הוא מרחב מסלולי הנוצר על-ידי v כך שלפי השלב הקודם $\Delta_T(T) = 0$.
אם $T = \alpha I_2$ אזי

$$\Delta_T(T) = (T - \alpha I_2)^2 = (\alpha I_2 - \alpha I_2)^2 = 0$$

וקיבלנו שהטענה נכונה ל $n = 2$.

עכשיו נניח כי הטענה נכונה ל- V ממימד קטן מ- n ונוכיח ל- n:
ניקח $\overrightarrow{0} \neq v \in V$ ונבנה תת-מרחב מסלולי W. אם $W = V$ אז סיימנו לפי החלק הראשון.
אם קבוצה מקסימאלית בת"ל $E = \{v, Tv, \ldots, T^{k-1}v\}$ מקיימת $k < n$ אז נשלים אותה לבסיס של V:

$$B = \{v, Tv, \ldots, T^{k-1}v, w_1, \ldots, w_{n-k}\}.$$

המטריצה המייצגת של T לפי הבסיס הזה היא מטריצת בלוקים משולשת עליונה:

$$[T]_B = \begin{pmatrix} [T|_W]_E & A \\ 0 & B \end{pmatrix}$$

כאשר $B \in M_{n-k}(F)$.

לפי למה 1.5.8 $\Delta_T(x) = \Delta_{T|_W}(x)\Delta_B(x)$. לפי הנחת האינדוקציה וטענה על מרחב מסלולי $\Delta_B(B) = 0$ ו- $\Delta_{T|_W}(T|_W) = 0$.

לפי למה 1.5.10 $\Delta_T([T]_B)=\Delta_{T|_W}([T]_B)\cdot\Delta_B([T]_B)$ ולפי למה 1.5.9 מקבלים:

$$\begin{aligned}\Delta_{T|_W}([T]_B)\cdot\Delta_B([T]_B)&=\begin{pmatrix}0 & C\\ 0 & \Delta_{T|_W}(B)\end{pmatrix}\cdot\begin{pmatrix}\Delta_B([T|_W]_E) & D\\ 0 & 0\end{pmatrix}\\&=\begin{pmatrix}0\Delta_B([T|_W]_E) & 0D+C0\\ 0 & \Delta_{T|_W}(B)0\end{pmatrix}=0\end{aligned}$$

□

שימוש מיידי במשפט קיילי – המילטון:

תהי $A\in M_n(F)$ מטריצה ריבועית.

בהינתן פולינום $p(x)=\alpha_kx^k+\alpha_{k-1}x^{k-1}+\cdots+\alpha_1x+\alpha_0$, אם $k>n$ נוכל לכתוב את הפולינום לפי חלוקה עם שארית כ- $p(x)=f(x)\cdot\Delta_A(x)+r(x)$ כאשר $\deg(r(x))\leq n-1$ או $r(x)=0$.

נזכור כי $\Delta_A(A)=0$ ולכן נקבל:

$$p(A)=f(A)\cdot\Delta_A(A)+r(A)=0+r(A)=r(A).$$

כלומר $p(A)=r(A)$ ולכן אין צורך לחשב דרגות של A הגבוהות מ- $n-1$.

דוגמא 1.5.11. תהי

$$A=\begin{pmatrix}1 & 0 & 0\\ 0 & \cos\frac{\pi}{3} & \sin\frac{\pi}{3}\\ 0 & -\sin\frac{\pi}{3} & \cos\frac{\pi}{3}\end{pmatrix}.$$

מצאו את A^5-A^2.

פתרון 1.5.12.

$$\begin{aligned}\Delta_A(x)&=\begin{vmatrix}x-1 & 0 & 0\\ 0 & x-\cos\frac{\pi}{3} & -\sin\frac{\pi}{3}\\ 0 & \sin\frac{\pi}{3} & x-\cos\frac{\pi}{3}\end{vmatrix}=(x-1)\left(x-0.5\right)^2+0.75\\&=(x-1)(x^2-x+1)=x^3-2x^2+2x+1\end{aligned}$$

כדי לקבל פתרון צריך למצוא שארית של חלוקה של x^5-x^2 ב- $\Delta_A(x)$.

מקבלים

$$x^5-x^2=\left(x^2+2x+2\right)\left(x^3-2x^2+2x-1\right)+(-2x+2).$$

לכן לפי משפט קיילי – המילטון

$$A^5-A^2=-2A+2I_3=-2\begin{pmatrix}1 & 0 & 0\\ 0 & \cos\frac{\pi}{3} & \sin\frac{\pi}{3}\\ 0 & -\sin\frac{\pi}{3} & \cos\frac{\pi}{3}\end{pmatrix}+2I_3=\begin{pmatrix}0 & 0 & 0\\ 0 & 1 & -\sqrt{3}\\ 0 & \sqrt{3} & 1\end{pmatrix}.$$

1.6 הפולינום המינימלי

1.6.1 פולינום מינימלי ותכונותיו

הגדרה 1.6.1. תהי $A\in M_n(F)$. הפולינום המינימלי של A הוא פולינום $m_A(x)\in F[x]$ מתוקן מהדרגה הקטנה ביותר כך שמתקיים $m_A(A)=0$.

אומרים שהפולינום $f(x)$ מתחלק בפולינום $p(x)$ (ללא שארית) אם קיים פולינום $q(x)$ כך ש- $f(x)=q(x)\cdot p(x)$.
מסמנים זאת: $p(x)\mid f(x)$ ואומרים " $f(x)$ מתחלק ב- $p(x)$" או לחילופין " $p(x)$ מחלק את $f(x)$".

הערה 1.6.2. אפשר להוכיח שאם $\deg p(x)\le\deg f(x)$ אז תמיד ניתן לכתוב $f(x)=q(x)\cdot p(x)+r(x)$ כאשר $\deg r(x)<\deg p(x)$.

משפט 1.6.3. תהי $A\in M_n(F)$ ו- $m_A(x)$ הפולינום המינימלי של A. אם $f(x)\in F[x]$ פולינום כך ש- $f(A)=0$ אזי $m_A(x)\mid f(x)$.

הוכחה. לפי חלוקת פולינומים עם שארית מקבלים כי $f(x)=p(x)\cdot m_A(x)+r(x)$ כאשר $r(x)=0$ או $\deg r(x)<\deg m_A(x)$.
כלומר קיימות שתי אפשרויות:

1. $r(x)=0$ ואז $m_A(x)\mid f(x)$.
2. $r(x)\neq 0$. נציב A ונקבל:

$$f(A)=p(A)\cdot m_A(A)+r(A).$$

לפי הנתון $f(A)=0$ ומכיוון ש- $m_A(x)$ הוא הפולינום המינימלי של A אז $m_A(A)=0$.
לכן נקבל

$$0=f(A)=p(A)\cdot 0+r(A)\implies r(A)=0$$

כלומר אם $r(x)\neq 0$ נתקן אותו ונקבל סתירה להגדרה ש- $m_A(x)$ הוא פולינום מינימלי, כי קיבלנו פולינום מתוקן מדרגה יותר קטנה ש- A מאפסת אותו.

לכן מקרה 2. בלתי אפשרי, ולכן: $m_A(x)\mid f(x)$.

□

מסקנה 1.6.4. הפולינום המינימלי הוא יחיד.

הוכחה. יהיו $m_A(x)$ ו- $\tilde{m}_A(x)$ פולינומים מינימליים.
אז לפי משפט 1.6.3 – $m_A(x)\mid\tilde{m}_A(x)$ כך ש- $m_A(x)=f(x)\tilde{m}_A(x)$, ובדומה גם $\tilde{m}_A(x)\mid m_A(x)$ כך ש- $\tilde{m}_A(x)=g(x)m_A(x)$.
אזי

$$m_A(x)=f(x)\tilde{m}_A(x)=f(x)g(x)m_A(x),$$

וזה אומר ש- $f(x)g(x)=1$.
זה אפשרי אם ורק אם $f(x)=\alpha$ וגם $g(x)=\frac{1}{\alpha}$ כך ש- $m_A(x)=\alpha\tilde{m}_A(x)$.
מכיוון שהפולינום $m_A(x)$ הוא מתוקן, כלומר אם המעלה הגבוהה ביותר בו היא k אז המקדם של x^k הוא בהכרח 1, ולכן נובע כי $\alpha=1$ כי אחרת בפולינום $\tilde{m}_A(x)$ שגם הוא פולינום מתוקן המקדם של x^k היה שווה ל- α בסתירה לכך שהוא מתוקן.
לכן $m_A(x)=\tilde{m}_A(x)$, כלומר הפולינום המינימלי הוא יחיד. □

מסקנה 1.6.5. למטריצות דומות יש את אותו פולינום מינימלי.

הוכחה. תהיינה $A \sim B$ דומות, ויהי $m_A(x)$ פולינום מינימלי של A ו- $m_B(x)$ פולינום מינימלי של B.
אז $m_A(A) = 0$ ו- $m_A(B) \sim m_A(A) = 0$, זאת אומרת ש- $m_A(B) = 0$.
כך שלפי משפט 1.6.3 $m_B(x) \mid m_A(x)$.
בדיוק באותו אופן מקבלים ש- $m_A(x) \mid m_B(x)$.
מכאן בדיוק כמו בהוכחה של מסקנה 1.6.4 מקבלים ש- $m_A(x) = m_B(x)$. □

הערה 1.6.6. לפי מסקנה 1.6.4, $m_A(x)$ הוא שמורה של יחס הדמיון של מטריצות.
אבל מכך ש- $m_A(x) = m_B(x)$ לא נובע כי $A \sim B$.

דוגמא 1.6.7. נתבונן במטריצות:

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

הערך העצמי היחיד של A ושל B הוא 0, לכן $m_A(x) = x^s$ כאשר $1 \le s \le 4$.
בדיוק באותו אופן $m_B(x) = x^t$ כאשר $1 \le t \le 4$.
נשים לב כי $A^2 = 0$ ולכן $m_A(x) = x^2$, ובדומה גם $B^2 = 0$ ולכן $m_B(x) = x^2$, כלומר $m_A(x) = m_B(x)$.
אבל הדרגות שלהן שונות: $\operatorname{rank} A = 1$ ו- $\operatorname{rank} B = 2$, ולכן $A \nsim B$.

הגדרה 1.6.8. יהי V מרחב וקטורי סוף מימדי מעל שדה F ויהי $T \in \operatorname{End} V$.
הפולינום המינימלי של T מוגדר כ- $m_T := m_{M_T}(x)$ כאשר M_T היא מטריצה מייצגת כלשהי של T.

הערה 1.6.9. לפי מסקנה 1.6.4 הפולינום המינימלי של אופרטור לינארי מוגדר היטב ולא תלוי בבחירה של המטריצה המייצגת שלו.

מסקנה 1.6.10. תהי $A \in M_n(F)$ אז $m_A(x) \mid \Delta_A(x)$.

הוכחה. לפי משפט קיילי – המילטון $\Delta_A(A) = 0$, אז לפי משפט 1.6.3 $m_A(x) \mid \Delta_A(x)$. □

מסקנה 1.6.11. הדרגה של הפולינום המינימלי היא לכל היותר n.
כלומר, $\deg m_A(x) \le \deg \Delta_A(x)$.

מסקנה 1.6.12. כל שורש של $m_A(x)$ הוא ערך עצמי של A.

הוכחה. יהי $\alpha \in F$ שורש של הפולינום המינימלי $m_A(x)$, כלומר $m_A(\alpha) = 0$.
לפי מסקנה 1.6.10, $\Delta_A(x) = f(x) \cdot m_A(x)$ ולכן כשמציבים $x = \alpha$ מקבלים $\Delta_A(\alpha) = f(\alpha) \cdot m_A(\alpha) = 0$.
זאת אומרת ש- α הוא שורש של $\Delta_A(x)$, וזה אומר ש- α הוא ערך עצמי של A. □

משפט 1.6.13. ל- $\Delta_A(x)$ ול- $m_A(x)$ יש את אותם שורשים.

הוכחה. לפי מסקנה 1.6.12 נובע כי כל שורש של $m_A(x)$ הוא שורש של $\Delta_A(x)$.
נשאר להראות כי כל שורש של $\Delta_A(x)$ הוא שורש של $m_A(x)$:

יהי $\alpha \in F$ שורש של $\Delta_A(x) \iff \alpha$ הוא ערך עצמי של A, ויהי $v \neq 0$ וקטור עצמי מתאים, כלומר $Av = \alpha v$.
יהי $m_A(x) = x^k + \beta_{k-1}x^{k-1} + \cdots + \beta_0$. לפי ההגדרה $m_A(A) = 0$ ולכן מקבלים:

$$\begin{aligned}
\overrightarrow{0} &= 0 \cdot v = m_A(A)v = \left(A^k + \beta_{k-1}A^{k-1} + \cdots + \beta_0 I\right) \cdot v \\
&= A^k v + \beta_{k-1}A^{k-1}v + \cdots + \beta_0 v = \alpha^k v + \beta_{k-1}\alpha^{k-1}v + \cdots + \beta_0 v \\
&= \left(\alpha^k + \beta_{k-1}\alpha^{k-1} + \cdots + \beta_0\right) v
\end{aligned}$$

כלומר קיבלנו ש- $\left(\alpha^k + \beta_{k-1}\alpha^{k-1} + \cdots + \beta_0\right) v = \overrightarrow{0}$.
מכיוון ש- $v \neq \overrightarrow{0}$ נובע כי $\alpha^k + \beta_{k-1}\alpha^{k-1} + \cdots + \beta_0 = 0$.
אבל זה בדיוק אומר ש- $m_A(\alpha) = 0$, ולכן α הוא שורש של הפולינום המינימלי $m_A(x)$. □

מסקנה מיידית מהעובדה שלפולינום אופייני ופולינום מינימלי יש אותם שורשים היא:

מסקנה 1.6.14. תהי $A \in M_n(F)$ אז הטענות הבאות שקולות:

1. A הפיכה.
2. 0 הוא לא ערך עצמי של A.
3. $\det A \neq 0$.
4. $m_A(0) \neq 0$, או במילים אחרות: הקבוע של m_A שונה מאפס.

1.6.2 מטריצה ניתנת לשילוש

כדי להבין יותר טוב בנייה של פולינומים של מטריצות, נגדיר מטריצה ניתנת לשילוש.

הגדרה 1.6.15. אומרים שמטריצה $A \in M_n(F)$ ניתנת לשילוש אם כל הערכים העצמיים של A שייכים לשדה F.

כלומר A ניתנת לשילוש אם $\Delta_A(x) = \prod_{i=1}^{k}(x-\alpha_i)^{m_i}$ כאשר $\alpha_1, \ldots, \alpha_k$ ערכים עצמיים שונים עם ריבויים אלגברים מתאימים $m_1, \ldots, m_k$ כך ש- $m_1 + m_2 + \cdots + m_k = n$.

מסקנה 1.6.16. מטריצה משולשת עליונה/תחתונה ניתנת לשילוש.

הוכחה. נכתוב

$$A = \begin{pmatrix} \alpha_{11} & \cdots & \cdots & \alpha_{1n} \\ 0 & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_{nn} \end{pmatrix}$$

אז הפולינום האופייני של A הוא $\Delta_A(x) = \prod_{i=1}^{n}(x-\alpha_{ii})$,
כלומר המטריצה המשולשת העליונה A ניתנת לשילוש.

□

נראה דוגמא למטריצה ממשית שלא ניתנת לשילוש מעל השדה $\mathbb{R}$:

דוגמא 1.6.17.

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

הפולינום האופייני של A הוא $\Delta_A(x) = x^2 + 1$.
כלומר אף אחד מהערכים העצמיים של A לא שייך לשדה $\mathbb{R}$.

מסקנה 1.6.18. אם מטריצה $A \in M_n(F)$ ניתנת לשילוש, אז $\det A$ היא מכפלת הערכים העצמיים שלה (כולל ריבויים אלגבריים) ו- $\operatorname{trace} A$ הוא סכום הערכים העצמיים שלה (כולל ריבויים אלגבריים).

הוכחה. אם A ניתנת לשילוש ו- $\alpha_1, \ldots, \alpha_n$ ערכים עצמיים שלה, אז

$$\begin{aligned} \Delta_A(x) &= (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \\ \Delta_A(0) &= (-1)^n \cdot \alpha_1 \cdot \alpha_2 \cdots \alpha_n = (-1)^n \det A \end{aligned}$$

כי הדטרמיננטה של A היא מכפלת כל הערכים העצמיים.
המקדם של x^{n-1} הוא $-(\alpha_1 + \cdots + \alpha_n)$. מצד שני ראינו שהמקדם של x^{n-1} הוא $-\operatorname{trace} A$.
מכאן ש- $\operatorname{trace} A = \alpha_1 + \cdots + \alpha_n$. □

הערה 1.6.19. מסקנה 1.6.18 נותנת עוד הסבר למה למטריצות דומות (ניתנות לשילוש) יש אותה דטרמיננטה ואותה עקבה.

שאלה: מדוע מטריצה שכל הערכים העצמיים שלה בשדה נקראת ניתנת לשילוש?
התשובה במשפט הבא:

משפט 1.6.20. $A \in M_n(F)$ ניתנת לשילוש אם ורק אם A דומה למטריצה משולשת.

טענה 1.6.21. מטריצה משולשת עליונה דומה למטריצה משולשת תחתונה.

הוכחה.

$$A = \begin{pmatrix} \alpha_{11} & \cdots & \cdots & \alpha_{1n} \\ 0 & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_{nn} \end{pmatrix}$$

נעשה הצמדה במטריצה D:

$$D = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 1 & \cdots & 0 & 0 \end{pmatrix}$$

כאשר $D^{-1} = D$.
לאחר כפל משמאל ומימין ב- D נקבל

$$DAD = \begin{pmatrix} 0 & 0 & 0 & \alpha_{nn} \\ 0 & \cdots & \alpha_{n-1,n-1} & \alpha_{n-1,n} \\ \vdots & \ddots & \vdots & \vdots \\ \alpha_{11} & \cdots & \alpha_{1,n-1} & \alpha_{1n} \end{pmatrix} D = \begin{pmatrix} \alpha_{nn} & 0 & \cdots & 0 \\ \alpha_{n-1,n} & \alpha_{n-1,n-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{1n} & \alpha_{1,n-1} & \cdots & \alpha_{11} \end{pmatrix}$$

כלומר המטריצה המשולשת העליונה A דומה למטריצה משולשת תחתונה $B = DAD$
(שימו לב ש- $B \neq A^T$). □

כעת אפשר להוכיח את משפט 1.6.20 (מטריצה A ניתנת לשילוש אם ורק אם היא דומה למטריצה משולשת):

הוכחה. 1. אם מטריצה דומה למטריצה משולשת אזי היא ניתנת לשילוש לפי מסקנה 1.6.16.

2. נניח כי מטריצה ניתנת לשילוש ונראה כי היא דומה למטריצה משולשת עליונה, באינדוקציה על n.
עבור $n=2$: המטריצה A ניתנת לשילוש $\Longleftarrow$ יש לה ערך עצמי α ויש לה וקטור עצמי v מתאים.
נשלים את $\{v\}$ לבסיס $B=\{v,w\}$.
Aw הוא צירוף לינארי של וקטורי בסיס, כך שקיימים $a,b\in F$ המקיימים $Aw=av+bw$, ואז

$$[A]_B=\begin{pmatrix}\alpha & a\\ 0 & b\end{pmatrix}$$

וזוהי מטריצה משולשת עליונה.

נניח את נכונות הטענה עבור $n-1$ ונוכיח את נכונתה עבור n:
יהי α ערך עצמי של A, ו- v_1 וקטור עצמי מתאים: $Av_1=\alpha v_1$.
נשלים אותו לבסיס $B=\{v_1,v_2,\dots,v_n\}$ של F^n.
לכל v_i מתקיים: $Av_i=\sum_{j=1}^{n}\beta_{ji}v_j$ (כאשר $2\le i\le n$) – צירוף לינארי של וקטורי בסיס.
לפיכך

$$[A]_B=\begin{pmatrix}\alpha & \beta_{12} & \cdots & \beta_{1n}\\ 0 & \beta_{22} & \cdots & \beta_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ 0 & \beta_{n2} & \cdots & \beta_{nn}\end{pmatrix}.$$

נגדיר

$$B=\begin{pmatrix}\beta_{22} & \cdots & \beta_{2n}\\ \vdots & \ddots & \vdots\\ \beta_{n2} & \cdots & \beta_{nn}\end{pmatrix}$$

נקבל $\Delta_A(x)=(x-\alpha)\Delta_B(x)$ ע"י פירוק לפי העמודה הראשונה של המטריצה האופיינית של A,
כך ש- $\Delta_B(x)=\frac{\Delta_A(x)}{x-\alpha}$, ולכן B מטריצה ניתנת לשילוש.
אז לפי הנחת האינדוקציה קיימת $P\in M_n(F)$ כך ש-

$$P^{-1}BP=\begin{pmatrix}\beta_1 & \star & \star\\ \vdots & \ddots & \star\\ 0 & \cdots & \beta_{n-1}\end{pmatrix}$$

כלומר זוהי מטריצה משולשת עליונה.
נתבונן ב-

$$\hat{P}=\begin{pmatrix}1 & 0 & \cdots & 0\\ 0 & & & \\ \vdots & & P & \\ 0 & & & \end{pmatrix}$$

וההפכית שלה

$$.\hat{P}^{-1}=\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & P^{-1} & \\ 0 & & & \end{pmatrix}$$

נחשב:

$$\begin{aligned}\hat{P}^{-1}[A]_B\hat{P} &= \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & P^{-1} & \\ 0 & & & \end{pmatrix}\begin{pmatrix} \alpha & \beta_{12} & \cdots & \beta_{1n} \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & P & \\ 0 & & & \end{pmatrix} \\ &= \begin{pmatrix} \alpha & \beta_{12} & \cdots & \beta_{1n} \\ 0 & & & \\ \vdots & & P^{-1}B & \\ 0 & & & \end{pmatrix}\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & P & \\ 0 & & & \end{pmatrix} \\ &= \begin{pmatrix} \alpha & \gamma_{12} & \cdots & \gamma_{1n} \\ 0 & & & \\ \vdots & & P^{-1}BP & \\ 0 & & & \end{pmatrix} = \begin{pmatrix} \alpha & \star & \cdots & \star \\ 0 & \beta_1 & \star & \star \\ 0 & 0 & \ddots & \star \\ 0 & 0 & 0 & \beta_{n-1} \end{pmatrix}\end{aligned}$$

וזוהי מטריצה משולשת עליונה כנדרש. $\square$

מסקנה 1.6.22. אם מטריצה $A \in M_n(F)$ ניתנת לשילוש אזי לכל $j \in \mathbb{N}$ המטריצה A^j ניתנת לשילוש, ואם $\{\alpha_1,\dots,\alpha_n\}$הם ערכים עצמיים של A אז $\left\{\alpha_1^j,\dots,\alpha_n^j\right\}$ הם ערכים עצמיים של A^j.
אם בנוסף A הפיכה אז A^{-1} ניתנת לשילוש אם ורק אם A^{-1} ניתנת לשילוש והערכים העצמיים של A^{-1} הם $\left\{\frac{1}{\alpha_1},\dots,\frac{1}{\alpha_n}\right\}$.

הוכחה. A ניתנת לשילוש אם ורק אם קיימת $P \in M_n(F)$ הפיכה כך ש-

$$P^{-1}AP=\begin{pmatrix} \alpha_1 & \star & \cdots & \star \\ 0 & \alpha_2 & \star & \star \\ \vdots & \vdots & \ddots & \star \\ 0 & \cdots & 0 & \alpha_n \end{pmatrix}$$

אז

$$P^{-1}A^jP=\left(P^{-1}AP\right)^j=\begin{pmatrix} \alpha_1^j & * & \cdots & * \\ 0 & \alpha_2^j & * & * \\ \vdots & \vdots & \ddots & * \\ 0 & \cdots & 0 & \alpha_n^j \end{pmatrix}$$

וזו מטריצה משולשת עליונה עם ערכים עצמיים: $\alpha_1^j,\dots,\alpha_n^j$.

בדומה,

$$\left(P^{-1}AP\right)^{-1}=P^{-1}A^{-1}P=\begin{pmatrix}\alpha_1 & \star & \cdots & \star\\ 0 & \alpha_2 & \star & \star\\ \vdots & \vdots & \ddots & \star\\ 0 & \cdots & 0 & \alpha_n\end{pmatrix}^{-1}=\begin{pmatrix}\frac{1}{\alpha_1} & \star & \cdots & \star\\ 0 & \frac{1}{\alpha_2} & \star & \star\\ \vdots & \vdots & \ddots & \star\\ 0 & \cdots & 0 & \frac{1}{\alpha_n}\end{pmatrix}$$

□

מסקנה 1.6.23. תהי $A\in M_n(F)$ מטריצה ניתנת לשילוש ו- $\alpha_1,\dots,\alpha_k$ ערכים עצמיים שונים של A.
נכתוב בהתאם $\Delta_A(x)=\prod_{i=1}^{k}(x-\alpha_i)^{s_i}$ כאשר s_i הוא הריבוי האלגברי של α_i לכל $1\le i\le k$.
נכתוב גם $m_A(x)=\prod_{i=1}^{k}(x-\alpha_i)^{r_i}$ כאשר r_i הוא הריבוי של α_i כשורש של $m_A(x)$ לכל $1\le i\le k$.
אז $1\le r_i\le s_i$ לכל $1\le i\le k$.

הוכחה. $1\le r_i$ כי לפולינום האופייני ולפולינום המינימלי של A יש את אותם שורשים.
בגלל ש- $m_A(x)\mid\Delta_A(x)$ מקבלים $r_i\le s_i$.

□

דוגמא 1.6.24. דוגמא למטריצה שהפולינום המינימלי שלה מתלכד עם הפולינום האופייני:

$$A=\begin{pmatrix}0 & 1 & 0 & 0\\ 0 & \ddots & \ddots & 0\\ 0 & 0 & \ddots & 1\\ 0 & 0 & 0 & 0\end{pmatrix}$$

כאן $\Delta_A(x)=x^n$ ולכן באופן כללי $m_A(x)=x^m$ כאשר $m\le n$.
בדוגמא זו מתקיימים $Ae_n=e_{n-1},\ Ae_{n-1}=e_{n-2}$,
ובאופן כללי $Ae_i=e_{i-1}$ לכל $2\le i\le n$, ו- $Ae_1=\overrightarrow{0}$.
לאחר $n-1$ "הזזות" נקבל

$$A^{n-1}(e_n)=A^{n-2}(e_{n-1})=e_1\neq\overrightarrow{0}$$

ומכאן ש- A לא מאפסת את x^{n-1}, כלומר הדרגה של $m_A(x)$ צריכה להיות בדיוק n.
זה אומר ש- $m_A(x)=x^n=\Delta_A(x)$.

הערה 1.6.25. ריבוי גיאומטרי של ערך עצמי לא קשור לריבוי שלו בפולינום המינימלי.
למשל, בדוגמא הקודמת הריבוי הגיאומטרי של 0 (שהוא הערך העצמי היחיד של A) הוא 1.

מסקנה 1.6.26. תהי A מטריצה ניתנת לשילוש ו- $\alpha_1,\alpha_2,\dots,\alpha_k$ ערכים עצמיים שונים שלה, אז

$$.\prod_{i=1}^{k}(x-\alpha_i)\mid m_A(x)$$

הוכחה. לפי מסקנה 1.6.23 מקבלים כי $m_A(x)=\prod_{i=1}^{k}(x-\alpha_i)^{r_i}$ כאשר $r_i\ge 1$.
אז ברור ש- $\prod_{i=1}^{k}(x-\alpha_i)\mid m_A(x)$.

□

נסיים במשפט חשוב שמסביר איך נראה פולינום מינימלי של מטריצה לכסינה:

משפט 1.6.27. תהי $A \in M_n(F)$ מטריצה ניתנת לשילוש, ויהיו $\alpha_1, \alpha_2, \dots, \alpha_k$ כל הערכים העצמיים השונים שלה. אז A לכסינה $\iff$ $m_A(x) = \prod_{i=1}^{k}(x-\alpha_i)$.

הוכחה. $\Longleftarrow$: אם A לכסינה אז קיים בסיס של F^n שכל וקטור בו הוא וקטור עצמי של A.
זאת אומרת $B = \{v_1, \dots, v_n\}$ ו- $Av_j = \alpha_{i_j} v_j$.
מכיוון שלפי מסקנה 1.6.26 מתקיים $\prod_{i=1}^{k}(x-\alpha_i) \mid m_A(x)$, מספיק לבדוק שלכל j מתקיים

$$\left(\prod_{i=1}^{k}(A-\alpha_i I)\right) v_j = \overrightarrow{0}\,.$$

נבדוק זאת:

$$\left(\prod_{i=1}^{k}(A-\alpha_i I)\right) v_j = \left(\prod_{\substack{i=1\\ i\neq i_j}}^{k}(A-\alpha_i I)\right)(A-\alpha_{i_j})v_j = \left(\prod_{\substack{i=1\\ i\neq i_j}}^{k}(A-\alpha_i I)\right)\left(Av_j-\alpha_{i_j}v_j\right)$$
$$= \left(\prod_{\substack{i=1\\ i\neq i_j}}^{k}(A-\alpha_i I)\right)\left(\alpha_{i_j}v_j-\alpha_{i_j}v_j\right) = \left(\prod_{\substack{i=1\\ i\neq i_j}}^{k}(A-\alpha_i I)\right)\overrightarrow{0} = \overrightarrow{0}$$

$\Longrightarrow$: נניח כי A לא לכסינה ונראה כי $\prod_{i=1}^{k}(A-\alpha_i I) \neq 0$ (זאת אומרת $m_A(x) \neq \prod_{i=1}^{k}(x-\alpha_i)$).
אם A לא לכסינה אז קיים α_i כך שהריבוי הגיאומטרי שלו קטן מהריבוי האלגברי שלו.
בה"כ ניתן להניח כי $\alpha_i = \alpha_1$. ניקח בסיס $v_1, \dots, v_s$ של V_{A,α_1} ונשלים אותו לבסיס של V שבו A תהיה מטריצה משולשת עליונה (ביחס לבסיס זה), וגם α_1 מופיע במקום ה- $(s+1, s+1)$.

נעשה את המעבר הזה בשני שלבים:
שלב ראשון: ניתן להשלים את $v_1, \dots, v_s$ עד לבסיס $B = \{v_1, \dots, v_s, w_{s+1}, \dots w_n\}$ ואז:

$$[A]_B = \begin{pmatrix} \alpha_1 & 0 & \cdots & 0 & \beta_{1,s+1} & \cdots & \beta_{1n} \\ \vdots & \alpha_1 & \cdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & \ddots & 0 & \vdots & & \\ 0 & \cdots & 0 & \alpha_1 & \beta_{s,s+1} & & \beta_{s,n} \\ 0 & \cdots & \cdots & 0 & \beta_{s+1,s+1} & \cdots & \beta_{s+1,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \beta_{n,s+1} & \cdots & \beta_{n,n} \end{pmatrix}$$

והמטריצה B ניתנת לשילוש (תרגיל: למה?), וגם α_1 הוא ע"ע שלה (תרגיל: למה?)
לכן קיימת $P \in M_{n-s}(F)$ הפיכה כך ש-

$$P^{-1}BP = \begin{pmatrix} \alpha_1 & \cdots & \star \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \star \end{pmatrix}$$

היא מטריצה משולשת עליונה.

שלב שני: נגדיר

$$\hat{P} = \begin{pmatrix} I_s & 0 \\ 0 & P \end{pmatrix}$$

ואפשר לבדוק ישירות ש-

$$\hat{P}^{-1} \begin{pmatrix} I_s & 0 \\ 0 & P^{-1} \end{pmatrix}$$

וגם

$$\hat{P}^{-1}[A]_B\hat{P} = \begin{pmatrix} \alpha_1 & 0 & \cdots & 0 & a_{1,s+1} & \cdots & \cdots & a_{1n} \\ \vdots & \alpha_1 & \cdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \ddots & 0 & \vdots & & & \\ 0 & \cdots & 0 & \alpha_1 & a_{s,s+1} & \cdots & \cdots & a_{s,n} \\ 0 & \cdots & \cdots & 0 & \alpha_1 & \cdots & \cdots & a_{s+1,n} \\ 0 & \cdots & \cdots & 0 & 0 & \star & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & & \star \end{pmatrix}$$

היא מטריצה משולשת עליונה,

וגם $a_{1,s+1},\dots,a_{s,s+1}$ לא כולם 0, כי הריבוי הגיאומטרי של α_1 הוא s.

יהי $B' = \{v_1,\dots,v_n\}$ בסיס המתקבל מ- B על-ידי מטריצת מעבר $\hat{P}$.

זאת אומרת $[A]_{B'} = \hat{P}^{-1}[A]_B\hat{P}$ כך ש-

$$[Av_{s+1}]_{B'} = \begin{pmatrix} a_{1,s+1} \\ \vdots \\ a_{s,s+1} \\ \alpha_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

או במילים אחרות: $Av_{s+1} = \alpha_1 v_{s+1} + \sum_{j=1}^{s} a_{j,s+1} v_j$.

נבצע חישוב:

$$
\begin{aligned}
\left(\prod_{i=1}^{k}(A-\alpha_i I)\right)v_{s+1} &= \left(\prod_{i=2}^{k}(A-\alpha_i I)\right)(A-\alpha_1 I)v_{s+1}\\
&= \left(\prod_{i=2}^{k}(A-\alpha_i I)\right)(Av_{s+1}-\alpha_1 v_{s+1})\\
&= \left(\prod_{i=2}^{k}(A-\alpha_i I)\right)\left(\alpha_1 v_{s+1}+\sum_{j=1}^{s}a_{j,s+1}v_j-\alpha_1 v_{S+1}\right)\\
&= \left(\prod_{i=2}^{k}(A-\alpha_i I)\right)\left(\sum_{j=1}^{s}a_{j,s+1}v_j\right)=\sum_{j=1}^{s}a_{j,s+1}\left(\prod_{i=2}^{k}(A-\alpha_i I)\,v_j\right)\\
&= \sum_{j=1}^{s}a_{j,s+1}\left(\prod_{i=2}^{k}(\alpha_1-\alpha_i)\right)v_j\neq\overrightarrow{0}
\end{aligned}
$$

קיבלנו ש-

$$
\sum_{j=1}^{s}a_{j,s+1}\left(\prod_{i=2}^{k}(\alpha_1-\alpha_i)\right)v_j\neq\overrightarrow{0}
$$

כי $\prod_{i=2}^{k}(\alpha_1-\alpha_i)\neq 0$ ו- $\sum_{j=1}^{s}a_{j,s+1}v_j\neq\overrightarrow{0}$.

מכאן ש- $\prod_{i=1}^{k}(A-\alpha_i I)\neq 0$. $\square$

1.7 משפט הפירוק הספקטרלי של אופרטור לינארי לכסין

1.7.1 היטלים

הגדרה 1.7.1. הספקטרום של מטריצה הוא אוסף כל הערכים העצמיים שלה.

הגדרה 1.7.2. $E \in M_n(F)$ נקראת היטל אם $E^2 = E$.

דוגמא 1.7.3.
1. $I^2 = I$.
2. $0^2 = 0$.
3. $A = \text{diag}(\alpha_1, \alpha_2, \dots, \alpha_n)$ כאשר $\alpha_i \in \{0,1\}$, אז $A^2 = A$.

למה 1.7.4. אם $E \in M_n(F)$ היטל אז E מטריצה לכסינה, ואם $E \neq I, 0$ אז הערכים העצמיים שלה הם $0, 1$.

הוכחה. לפי ההגדרה $E^2 = E$ כלומר $E^2 - E = 0$.
ז"א ש- E מאפסת את הפולינום $p(x) = x^2 - x = x(x-1)$.
מכאן נקבל כי $m_E(x) \mid x(x-1)$. קיימות שלוש אפשרויות:

1. $m_E(x) = x$ ואז $E = 0$.
2. $m_E(x) = x - 1$ ואז $E - I = 0$, כלומר $E = I$.
3. $m_E(x) = x(x-1)$ ואז יש שני ערכים עצמיים: 0 ו- 1.

□

הגדרה 1.7.5. יהי V מרחב וקטורי סוף מימדי מעל F, יהי $W \subset V$ תת-מרחב ו- U תת-מרחב משלים של W, כלומר $V = W \oplus U$.
T נקרא היטל על W במקביל ל- U אם לכל $v \in V$ (כאשר $v = w + u$ הוא פירוק יחיד) מתקיים $T(v) = w$.

למה 1.7.6. היטל על W במקביל ל- U הוא אופרטור לינארי והיטל.

הוכחה. נבדוק לינאריות:

1. $T(\alpha v) = T(\alpha w + \alpha u) = \alpha w = \alpha T(v)$ לכל $v \in V$ ו- $\alpha \in F$.
2. $T(v_1 + v_2) = w_1 + w_2 = T(v_1) + T(v_2)$ לכל $v_1 = w_1 + u_1,\ v_2 = w_2 + u_2$.

נבדוק ש- $T^2 = T$:
אכן,
$$T^2(v) = T^2(w+u) = T(T(w+u)) = T(w) = T(w + \overrightarrow{0}) = w = T(v).$$

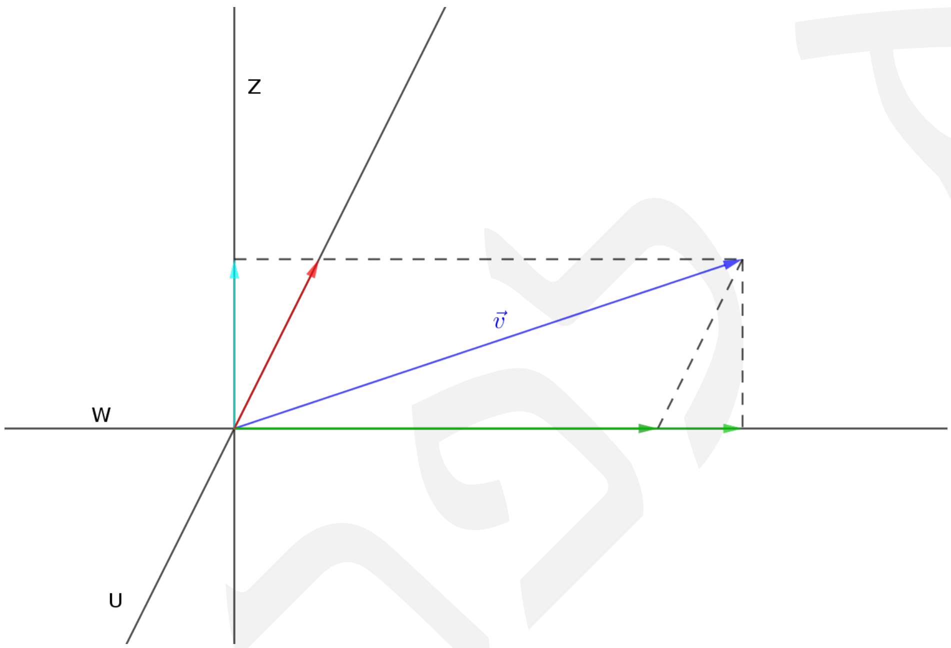
□

הערה 1.7.7. בהגדרה חשוב מאוד לציין לא רק על מה ההיטל אלא גם במקביל למה, כי לאותו תת-מרחב קיימות השלמות שונות והן נותנות היטלים שונים.

דוגמא 1.7.8. נתבונן ב- $V=\mathbb{R}^2$ וב- $U=\operatorname{span}\{e_1+2e_2\}\,,\ W=\operatorname{span}\{e_1\}$ ו- $W\oplus U=V$.
אז קיים היטל W על במקביל ל- U. נסמן אותו ב- pr_W^U.
נגדיר גם $Z=\operatorname{span}\{e_2\}$, אז $W\oplus Z=V$, ולכן קיים היטל על W במקביל ל- Z. נסמן אותו ב- pr_W^Z.
התמונה של שני ההיטלים היא W, אבל אלו שני אופרטורים שונים.
למשל נסתכל על $v=\begin{pmatrix}6\\2\end{pmatrix}$, אז $v=6e_1+2e_2=5e_1+(e_1+2e_2)$ כך ש-

$$\mathrm{pr}_W^U=5e_1,\quad \mathrm{pr}_W^Z=6e_1$$

והם שונים.



תרגיל 1.7.9. יהי W תת-מרחב של V ו- U,Z, שתי השלמות שונות של W.
מצאו תנאי הכרחי ומספיק על $v\in V$ כדי שיתקיים

$$\mathrm{pr}_W^U(v)=\mathrm{pr}_W^Z(v)\,.$$

טענה 1.7.10. יהיו $V_1,\ldots,V_k$ תתי-מרחבים של $V=F^n$ כך ש- $V=\bigoplus_{i=1}^k V_i$.
לכל V_i נגדיר $E_i:V\to V_i$ במקביל ל- $W_i=\bigoplus_{j\neq i}V_j$.
אז לכל $1\le i,j\le k$ מתקיים $E_i\cdot E_j=\delta_{ij}\cdot E_i$.

הסימן δ_{ij} מכונה הדלתא של קרוניקר ומוגדר

$$\delta_{ij}=\begin{cases}1, & i=j\\ 0, & \text{אחרת}\end{cases}.$$

הוכחה. יהי $v \in V$ אז $v = v_1 + \cdots + v_k$ כאשר $v_i \in V_i$ והפירוק הנ"ל יחיד.

$$E_iE_j(v) = E_i(v_j) = E_i(\overrightarrow{0} + \cdots + \overrightarrow{0} + v_j + \overrightarrow{0} + \cdots + \overrightarrow{0}) = \begin{cases} v_j & i = j \\ \overrightarrow{0} & \text{אחרת} \end{cases}$$

וזה בדיוק אומר ש- $E_i \cdot E_j = \delta_{ij} \cdot E_i$. □

1.7.2 פולינומי לגרנז'

בעיה 1.7.11. נתונות נקודות שונות $a_1, \dots, a_n \in \mathbb{R}$.
רוצים לבנות פונקציה רציפה f כך ש- $f(a_i) = b_i$ ובנוסף ש- f תהיה חלקה (למשל ש- f תהיה פולינום).
בכל פעם שמקבלים קבוצה חדשה של נקודות $b_1, \dots, b_n$ עלינו לבנות f חדשה.

פתרון כללי שמאפשר לבנות f כצירוף ליניארי של n פולינומים בסיסיים:
נבנה n פולינומים $\ell_1(x), \dots, \ell_n(x)$ המקיימים $\ell_i(a_j) = \delta_{ij}$.
לפי הדרישה לכל $\ell_j(x)$ צריכים להיות לפחות $n-1$ שורשים ולכן הוא צריך להיות פולינום מדרגה $n-1$ לכל הפחות.
יתר על כן אם נבנה את הפולינום $\ell_j(x)$ מדרגה $n-1$ אז $a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n$ יהיו כל השורשים שלו.
אם בנינו פולינומים כאלה, אז הפונקציה $f(x) = \sum_{j=1}^{n} b_j\ell_j(x)$ מקיימת $f(a_i) = \sum_{j=1}^{n} b_j\ell_j(a_i) = \sum_{j=1}^{n} b_j\delta_{ij} = b_i$, וזוהי בדיוק הפונקציה הנדרשת.

הגדרה 1.7.12. נתונים n מספרים שונים $a_1, \dots, a_n$ בשדה F.
קבוצת הפולינומים $\{\ell_1(x), \dots, \ell_n(x)\}$ מדרגה $n-1$ כאשר הפולינום ה- i מוגדר על-ידי

$$\ell_i(x) = \prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{x - a_j}{a_i - a_j}$$

נקראת פולינומי לגרנז' של הקבוצה $\{a_1, \dots, a_n\}$.

פולינומי לגרנז' מקיימים את התנאים $\ell_i(a_j) = \delta_{ij}$ וגם $\ell_i(x) \neq 0$ לכל $x \notin \{a_1, \dots, a_n\}$.

1.7.3 המשפט הספקטרלי

משפט 1.7.13 (המשפט הספקטרלי). יהי V מרחב וקטורי n מימדי מעל שדה F, ויהי $T \in \operatorname{End} V$ אופרטור לכסין, כאשר $\alpha_1, \dots, \alpha_k$ ערכים עצמיים שונים של T.
נכתוב $V_i = V_{T,\alpha_i}$ (המרחב העצמי של T המתאים לערך העצמי α_i), ויהי $W_i = \bigoplus_{\substack{j=1 \\ j \neq i}}^{k} V_j$. נסמן ב- E_i את ההיטל על V_i במקביל ל- W_i. אז:

1. $V = \bigoplus_{i=1}^{k} V_i$.
2. $\operatorname{Id} = \sum_{i=1}^{k} E_i$ (כאשר $\operatorname{Id}(v) = v$).
3. $T = \sum_{i=1}^{k} \alpha_i E_i$.
4. לכל פולינום $f(x)$ מתקיים $f(T) = \sum_{i=1}^{k} f(\alpha_i)E_i$.
5. $\ell_i(T) = E_i$ כאשר $\ell_1(x), \dots, \ell_k(x)$ הם פולינומי לגרנז' על הקבוצה $\{\alpha_1, \dots, \alpha_k\}$.

6. הפירוק $T=\sum_{i=1}^k \alpha_i E_i$ הוא יחיד.

הוכחה. 1. הוכחנו כבר ש- T לכסין $\iff$ $V=\bigoplus_{i=1}^k V_i$.

2. לכל $v\in V$ מתקיים $v=v_1+\cdots+v_k$ כאשר $v_i\in V_i$.
אז

$$\left(\sum_{i=1}^k E_i\right)(v)=\sum_{i=1}^k E_i(v)=\sum_{i=1}^k v_i=v\ .$$

מכאן כי לכל v מתקיים $\left(\sum_{i=1}^k E_i\right)(v)=v$, ולכן זהו בעצם אופרטור הזהות $\mathrm{Id}=\sum_{i=1}^k E_i$.

3. לכל $v\in V$ מתקיים $v=v_1+\cdots+v_k$ כאשר $v_i\in V_i$.
מכאן ש- $T(v_i)=\alpha_i v_i$ (כי V_i הוא המרחב העצמי המתאים ל- α_i).
נשווה את $T(v)$ ואת $\left(\sum_{i=1}^k \alpha_i E_i\right)(v)$:

- $T(v)=T(v_1+\cdots+v_k)=T(v_1)+\cdots+T(v_k)$
ולפי ההגדרה נקבל $T(v_1)+\cdots+T(v_k)=\alpha_1v_1+\cdots+\alpha_kv_k=\sum_{i=1}^k\alpha_iv_i$.

- מתקיים

$$\left(\sum_{i=1}^k \alpha_i E_i\right)(v)=\sum_{i=1}^k \alpha_i E_i(v)=\sum_{i=1}^k \alpha_i v_i\ .$$

ולכן לכל v מתקיים

$$T(v)=\left(\sum_{i=1}^k \alpha_i E_i\right)(v).$$

4. נוכיח קודם את הטענה לכל חזקה. נראה תחילה כי $T^2=\sum_{i=1}^k\alpha_i^2E_i$:
לפי 3 מקבלים

$$\left(\sum_{i=1}^k \alpha_i E_i\right)\left(\sum_{i=1}^k \alpha_i E_i\right)=\sum_{i=1}^k\alpha_i\left(E_i\sum_{j=1}^k\alpha_jE_j\right)=\sum_{i=1}^k\alpha_i\left(\sum_{j=1}^k\alpha_jE_iE_j\right)$$

נזכור שע"פ טענה 1.7.10 מתקיים $E_i\cdot E_j=\delta_{ij}\cdot E_i$ ולכן נקבל

$$\sum_{i=1}^k\alpha_i\left(\sum_{j=1}^k\alpha_jE_iE_j\right)=\sum_{i=1}^k\alpha_i\left(\sum_{j=1}^k\alpha_j\delta_{ij}E_i\right)=\sum_{i=1}^k\alpha_i\alpha_iE_i=\sum_{i=1}^k\alpha_i^2E_i\ .$$

נניח באינדוקציה כי הטענה נכונה עבור $s-1$ ונראה את נכונותה עבור s.

רוצים להראות ש- $T^s = \sum_{i=1}^k \alpha_i^s E_i$:

$$\begin{aligned}
T^s = T^{s-1}\cdot T &= \left(\sum_{i=1}^k \alpha_i^{s-1}E_i\right)\left(\sum_{j=1}^k \alpha_j E_j\right)\\
&= \left(\sum_{i=1}^k \alpha_i^{s-1}\right)\left(E_i\sum_{j=1}^k \alpha_j E_j\right) = \sum_{i=1}^k \alpha_i^{s-1}\left(\sum_{j=1}^k \alpha_j E_i E_j\right)\\
&= \sum_{i=1}^k \alpha_i^{s-1}\left(\sum_{j=1}^k \alpha_j \delta_{ij} E_i\right) = \sum_{i=1}^k \alpha_i^{s-1}\alpha_i E_i = \sum_{i=1}^k \alpha_i^s E_i
\end{aligned}$$

עכשיו נעבור לפולינומים.

נתבונן בפולינום $f(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$. לפי ההגדרה:

$$\begin{aligned}
f(T) &= b_m T^m + b_{m-1}T^{m-1} + \cdots + b_0 I\\
&= b_m\sum_{i=1}^k \alpha_i^m E_i + b_{m-1}\sum_{i=1}^k \alpha_i^{m-1}E_i + \cdots + b_0\sum_{i=1}^k E_i\\
&= \sum_{i=1}^k \left(b_m\alpha_i^m + \cdots + b_0\right)E_i
\end{aligned}$$

נשים לב כי $f(\alpha_i) = b_m\alpha_i^m + \cdots + b_0$, ולכן

$$\sum_{i=1}^k \left(b_m\alpha_i^m + \cdots + b_0\right)E_i = \sum_{i=1}^k f(\alpha_i)E_i .$$

5.

$$\ell_i(x) = \prod_{\substack{s=1\\ s\neq i}}^n \frac{x-\alpha_s}{\alpha_i-\alpha_s}$$

לפי 4 נקבל

$$\ell_i(T) = \sum_{j=1}^k \ell_i(\alpha_j)E_j = \sum_{j=1}^k\left(\prod_{\substack{s=1\\ s\neq i}}^k \frac{\alpha_j-\alpha_s}{\alpha_i-\alpha_s}E_j\right).$$

כאשר $j \neq i$ נקבל $\prod_{\substack{s=1\\ s\neq i}}^k \frac{\alpha_j-\alpha_s}{\alpha_i-\alpha_s} = 0$,

וכאשר $j = i$ נקבל $\prod_{\substack{s=1\\ s\neq i}}^k \frac{\alpha_j-\alpha_s}{\alpha_i-\alpha_s} = 1$.

לכן

$$\ell_i(T) = \sum_{j=1}^k\left(\prod_{\substack{s=1\\ s\neq i}}^k \frac{\alpha_j-\alpha_s}{\alpha_i-\alpha_s}E_j\right) = E_i$$

כלומר $\ell_i(T) = E_i$.

6. נובע מיידית מ- 5 כי כל E_i מוגדר כפולינום יחיד של T ולכן הוא מוגדר באופן יחיד.

$\square$

פרק 2

מרחבי מכפלה פנימית

2.1 מרחבי מכפלה פנימית

2.1.1 מכפלה פנימית

הערה 2.1.1. בפרק זה נעסוק בתאוריה מעל השדות $\mathbb{R}, \mathbb{C}$.

הגדרה 2.1.2. יהי V מרחב ווקטורי מעל $\mathbb{F}$.
אומרים ש- V הוא מרחב מכפלה פנימית, אם קיימת $\langle\ ,\ \rangle : V \times V \to \mathbb{F}$
(ז"א לכל זוג סדור $(u,v) \in V \times V$ מגדירים את המספר $\langle u,v\rangle \in \mathbb{F}$),
עם האקסיומות הבאות:

1. לכל $u,v,w \in V$ מתקיים $\langle u+v,w\rangle = \langle u,w\rangle + \langle v,w\rangle$.
2. לכל $u,v \in V$ ולכל $\alpha \in \mathbb{F}$ מתקיים $\langle \alpha u,v\rangle = \alpha\langle u,v\rangle$.
3. לכל $u,v \in V$ מתקיים $\langle u,v\rangle = \overline{\langle v,u\rangle}$.
4. לכל $0 \neq v \in V$ מתקיים $\langle v,v\rangle > 0$ (כלומר $\langle v,v\rangle$ הוא מספר חיובי ממשי).

הגדרה 2.1.3.
- מרחב בעל מכפלה פנימית (ממ"פ) מעל $\mathbb{R}$ נקרא מרחב אוקלידי.
- מרחב בעל מכפלה פנימית (ממ"פ) מעל $\mathbb{C}$ נקרא מרחב אוניטרי.

הערה 2.1.4. שימו לב שבמרחב אוקלידי אקסיומה 3 הופכת ל- $\langle u,v\rangle = \langle v,u\rangle$.

הגדרה 2.1.5. העתקה מ- $\langle\ ,\ \rangle : V \times V \to F$ נקראת

- תבנית לינארית לפי המשתנה הראשון אם מתקיים $\langle \alpha u+\beta v,w\rangle = \alpha\langle u,w\rangle + \beta\langle v,w\rangle$;
- תבנית לינארית לפי המשתנה השני אם מתקיים $\langle u,\alpha v+\beta w\rangle = \alpha\langle u,v\rangle + \beta\langle u,w\rangle$;
- תבנית בילינארית אם היא לינארית לפי שני המשתנים.

הערה 2.1.6. המילה תבנית מציינת שזוהי העתקה שהטווח שלה הוא שדה.

מסקנה 2.1.7. מכפלה פנימית במרחב אוקלידי היא תבנית בילינארית.

הוכחה. היא לינארית לפי המשתנה הראשון לפי אקסיומות 1 ו- 2.
לגבי המשתנה השני:

$$\begin{aligned}\langle u,\alpha v+\beta w\rangle &\underset{\text{לפי אקסיומה 3.}}{=} \overline{\langle \alpha v+\beta w,u\rangle}\\ &\underset{\text{לפי אקסיומות 1., 2.}}{=} \overline{\alpha\langle v,u\rangle} + \overline{\beta\langle w,u\rangle}\\ &\underset{\text{לפי אקסיומה 3.}}{=} \alpha\langle u,v\rangle + \beta\langle u,w\rangle\end{aligned}$$

□

כעת אפשר להבין את חשיבות הצמוד באקסיומה 3:
נסתכל למשל על מכפלה פנימית של הוקטור v עם עצמו, ללא דרישת ההצמדה:

$$\langle iv,iv\rangle = i\langle v,iv\rangle = i\langle iv,v\rangle = i^2\langle v,v\rangle = -\langle v,v\rangle$$

זאת אומרת שתבנית בילינארית כזו במרחב אוניטרי לא יכולה לקיים את אקסיומה 4.

מסקנה 2.1.8. יהי V מרחב אוניטרי, אז המכפלה הפנימית היא לינארית לפי המשתנה הראשון.
לגבי המשתנה השני מקבלים

$$\langle u, \alpha v + \beta w \rangle = \overline{\alpha} \langle u, v \rangle + \overline{\beta} \langle u, w \rangle \tag{2.1}$$

הוכחה. לינאריות במשתנה הראשון שקולה לצירוף של אקסיומות 1 ו- 2.

$$\begin{aligned}\langle u, \alpha v + \beta w \rangle &\underset{\text{לפי אקסיומה 3.}}{=} \overline{\langle \alpha v + \beta w, u \rangle} = \overline{\alpha \langle v, u \rangle + \beta \langle w, u \rangle} \\ &= \overline{\alpha} \overline{\langle v, u \rangle} + \overline{\beta} \overline{\langle w, u \rangle} = \overline{\alpha} \langle u, v \rangle + \overline{\beta} \langle u, w \rangle\end{aligned}$$

□

מסקנה 2.1.9. יהי V מרחב אוניטרי, יהיו $v_1, \dots v_k \in V$, $w_1, \dots w_m \in V$ ו- $\alpha_1, \dots \alpha_k \in F$, $\beta_1, \dots \beta_m \in F$. אז

$$\left\langle \sum_{i=1}^{k} \alpha_i v_i, \sum_{j=1}^{m} \beta_j w_j \right\rangle = \sum_{i=1}^{k} \sum_{j=1}^{m} \alpha_i \overline{\beta}_j \langle v_i, w_j \rangle$$

הוכחה.

$$\begin{aligned}\left\langle \sum_{i=1}^{k} \alpha_i v_i, \sum_{j=1}^{m} \beta_j w_j \right\rangle &= \sum_{i=1}^{k} \alpha_i \left\langle v_i, \sum_{j=1}^{m} \beta_j w_j \right\rangle \\ &\underset{\text{לפי אקסיומה 3.}}{=} \sum_{i=1}^{k} \alpha_i \overline{\left\langle \sum_{j=1}^{m} \beta_j w_j, v_i \right\rangle} = \sum_{i=1}^{k} \alpha_i \overline{\sum_{j=1}^{m} \beta_j \langle w_j, v_i \rangle} \\ &= \sum_{i=1}^{k} \alpha_i \sum_{j=1}^{m} \overline{\beta}_j \overline{\langle w_j, v_i \rangle} = \sum_{i=1}^{k} \alpha_i \sum_{j=1}^{m} \overline{\beta}_j \langle v_i, w_j \rangle \\ &= \sum_{i=1}^{k} \sum_{j=1}^{m} \alpha_i \overline{\beta}_j \langle v_i, w_j \rangle\end{aligned}$$

□

משפט 2.1.10. יהי V מרחב וקטורי n- מימדי מעל שדה $\mathbb{F}$, אז ניתן "לצייד" אותו במכפלה פנימית באופן הבא:
ניקח בסיס $\{e_1, \dots, e_n\}$ ונגדיר $\langle e_i, e_j \rangle = \delta_{ij}$.
אז אפשר להגדיר מכפלה פנימית על V בצורה הבאה:
לכל $v, w \in V$ כאשר $v = \sum_{i=1}^{n} \alpha_i e_i,\ w = \sum_{i=1}^{n} \beta_i e_i$ נכתוב

$$\langle v, w \rangle := \sum_{i=1}^{n} \alpha_i \overline{\beta}_i \,.$$

הוכחה. צריך לבדוק כי מתקיימות האקסיומות של מכפלה פנימית:

1. יהי $u=\sum_{i=1}^{n}\gamma_i e_i$, אז $u+v=\sum_{i=1}^{n}\left(\gamma_i+\alpha_i\right)e_i$ ולכן

$$\begin{aligned}\langle u+v,w\rangle &= \left\langle \sum_{i=1}^{n}\left(\gamma_i+\alpha_i\right)e_i, \sum_{j=1}^{n}\beta_j e_j\right\rangle \\ &= \sum_{i=1}^{n}\left(\gamma_i+\alpha_i\right)\overline{\beta}_i = \sum_{i=1}^{n}\gamma_i\overline{\beta}_i+\sum_{i=1}^{n}\alpha_i\overline{\beta}_i \\ &= \langle u,w\rangle+\langle v,w\rangle\end{aligned}$$

2.

$$\begin{aligned}\langle \gamma v,w\rangle &= \left\langle \gamma\sum_{i=1}^{n}\alpha_i e_i, \sum_{j=1}^{n}\beta_j e_j\right\rangle \\ &= \left\langle \sum_{i=1}^{n}\gamma\alpha_i e_i, \sum_{j=1}^{n}\beta_j e_j\right\rangle = \sum_{i=1}^{n}\gamma\alpha_i\overline{\beta}_i \\ &= \gamma\sum_{i=1}^{n}\alpha_i\overline{\beta}_i = \gamma\langle v,w\rangle\end{aligned}$$

3.

$$\begin{aligned}\overline{\langle w,v\rangle} &= \overline{\left\langle \sum_{j=1}^{n}\beta_j e_j, \sum_{i=1}^{n}\alpha_i e_i\right\rangle} = \overline{\sum_{j=1}^{n}\beta_j\overline{\alpha}_j} \\ &= \sum_{j=1}^{n}\overline{\beta}_j\overline{\overline{\alpha_j}} = \sum_{j=1}^{n}\alpha_j\overline{\beta}_j = \langle v,w\rangle\end{aligned}$$

4. אם $v\neq 0$ אז $\alpha_i\neq 0$ לפחות לאיזשהו i, לכן

$$\langle v,v\rangle = \left\langle \sum_{i=1}^{n}\alpha_i e_i, \sum_{i=1}^{n}\alpha_i e_i\right\rangle = \sum_{i=1}^{n}\alpha_i\overline{\alpha}_i = \sum_{i=1}^{n}\left|\alpha_i\right|^2 > 0 .$$

כלומר הראינו כי $\langle v,v\rangle>0$ אם $v\neq\overrightarrow{0}$.

□

2.1.2 נורמה ומרחק

הגדרה 2.1.11. יהי V מרחב מכפלה פנימית. לכל $v\in V$ נגדיר נורמה

$$\|v\| := \sqrt{\langle v,v\rangle} .$$

למה 2.1.12. יהי $v\in V$ ו- $\alpha\in F$, אז

$$\|\alpha v\| = |\alpha|\cdot\|v\| .$$

הוכחה.

$$\|\alpha v\| = \sqrt{\langle \alpha v, \alpha v\rangle} = \sqrt{\alpha\overline{\alpha}\,\langle v, v\rangle} = \sqrt{|\alpha|^2}\sqrt{\langle v, v\rangle} = |\alpha| \cdot \|v\| .$$

□

הגדרה 2.1.13. יהי V מרחב אוקלידי (או אוניטרי). $v \in V$ נקרא וקטור יחידה או וקטור נורמלי אם $\|v\| = 1$.

משפט 2.1.14 (אי שוויון קושי – שוורץ)**.** יהי V מרחב מכפלה פנימית ו- $v, w \in V$. אז מתקיים

$$|\langle v, w\rangle| \le \|v\| \cdot \|w\| ,$$

והשוויון מתקיים אם ורק אם v ו- w תלויים לינארית.

הוכחה. נסתכל בוקטור $v - tw$ כאשר $t \in F$ סקלר כלשהו. אז

$$0 \le \|v - tw\|^2 = \langle v - tw, v - tw\rangle \ge 0$$

וגם $\langle v - tw, v - tw\rangle = 0$ אם ורק אם $v = tw$.
אז מקבלים

$$\begin{aligned} 0 &\le \langle v - tw, v - tw\rangle = \langle v, v - tw\rangle - t\,\langle w, v - tw\rangle \\ &= \langle v, v\rangle - \bar{t}\,\langle v, w\rangle - t\,\langle w, v\rangle + |t|^2\,\langle w, w\rangle \\ &= \|v\|^2 - (\bar{t}\,\langle v, w\rangle + t\overline{\langle v, w\rangle}) + |t|^2\,\|w\|^2 \end{aligned}$$

נפריד למקרים:
אם $w = \overrightarrow{0}$ אז $\|v\| \cdot \|w\| = 0$ וגם $\langle v, w\rangle = \left\langle v, \overrightarrow{0}\right\rangle = 0$, כך שמקבלים שוויון.
אם $w \neq \overrightarrow{0}$ ניקח $t = \frac{\langle v,w\rangle}{\|w\|^2}$ ואז נקבל:

$$\begin{aligned} 0 &\le \|v\|^2 - \frac{1}{\|w\|^2}\left(\overline{\langle v, w\rangle}\langle v, w\rangle + \langle v, w\rangle\overline{\langle v, w\rangle}\right) + \frac{|\langle v, w\rangle|^2}{\|w\|^4}\|w\|^2 \\ &= \|v\|^2 - 2\frac{|\langle v, w\rangle|^2}{\|w\|^2} + \frac{|\langle v, w\rangle|^2}{\|w\|^2} = \|v\|^2 - \frac{|\langle v, w\rangle|^2}{\|w\|^2} \end{aligned}$$

נכפיל את שני האגפים ב- $\|w\|^2$ ונקבל

$$\begin{aligned} &0 \le \|w\|^2\|v\|^2 - |\langle v, w\rangle|^2 \\ \Longrightarrow\ &|\langle v, w\rangle|^2 \le \|w\|^2\|v\|^2 \\ \Longrightarrow\ &|\langle v, w\rangle| \le \|w\| \cdot \|v\| \end{aligned}$$

נזכיר שאם v, w בלתי תלויים לינארית, אז $\langle v - tw, v - tw\rangle > 0$ ומקבלים אי שוויון חזק.
אם v, w תלויים לינארית, אז או ש- $w = \overrightarrow{0}$ (וכבר ראינו שבמקרה זה מתקיים שוויון), או ש- $v = \alpha w$ עבור $\alpha \in F$.
במקרה זה נקבל מצד אחד

$$\langle v, w\rangle = \langle \alpha w, w\rangle = \alpha\langle w, w\rangle = \alpha\|w\|^2$$

כלומר $|\langle v,w\rangle| = |\alpha|\|w\|^2$
ומצד שני $\sqrt{\langle v,v\rangle} = \|v\|$, כך ש- $\|v\|\cdot\|w\| = |\alpha|\cdot\|w\|^2 = |\langle v,w\rangle|$. □

תזכורת 2.1.15. מסמנים ב- $\mathbb{R}^+$ את קבוצת הממשיים האי-שליליים.

מסקנה 2.1.16 (אי שוויון המשולש). יהי V מרחב מכפלה פנימית ו- $v,w\in V$. אז

$$\|v+w\| \le \|v\| + \|w\|$$

והשוויון מתקבל אם ורק אם $w=0$ או $v=\alpha w$ כאשר $0\le\alpha\in\mathbb{R}$.

הוכחה.

$$\begin{aligned}\|v+w\|^2 &= \langle v+w, v+w\rangle = \langle v,v\rangle + \langle v,w\rangle + \langle w,v\rangle + \langle w,w\rangle\\ &= \|v\|^2 + \|w\|^2 + \left(\langle v,w\rangle + \overline{\langle v,w\rangle}\right) \underset{(*)}{\le} \|v\|^2 + \|w\|^2 + 2\left|\langle v,w\rangle\right|\\ &\underset{(**)}{\le} \|v\|^2 + \|w\|^2 + 2\|v\|\cdot\|w\| = (\|v\|+\|w\|)^2\end{aligned}$$

כלומר בסה"כ קיבלנו

$$\|v+w\|^2 \le (\|v\|+\|w\|)^2$$

ולכן

$$\|v+w\| \le \|v\| + \|w\|.$$

השוויון מתקבל ב- $(*)$ אם $\langle v,w\rangle = |\langle v,w\rangle|$,
והשוויון מתקבל ב- $(**)$ אם ורק אם $|\langle v,w\rangle| = \|v\|\cdot\|w\|$,
ולפי משפט קושי – שוורץ מתקיים שוויון אם ורק אם $w=\overrightarrow{0}$ או $v=\alpha w$.
המקרה $w=\overrightarrow{0}$ טריוויאלי.
אם $v=\alpha w$ אז

$$\mathrm{Re}\,\langle v,w\rangle = \mathrm{Re}\,\alpha\langle w,w\rangle = \mathrm{Re}\left(\alpha\|w\|^2\right) = (\mathrm{Re}\,\alpha)\|w\|^2$$

ולפי חישובים בהוכחה של משפט קושי שוורץ במקרה הזה מתקיים $\|v\|\cdot\|w\| = |\alpha|\,\|w\|^2$, ולכן תנאי הכרחי ומספיק הוא $\mathrm{Re}\,\alpha = |\alpha|$, וזה שקול ל- $\alpha\in\mathbb{R}^+$. □

הגדרה 2.1.17. יהי V מרחב וקטורי מעל $\mathbb{R}$. הפונקציה $\rho: V\times V\to\mathbb{R}^+$ נקראת פונקצית מרחק אם היא מקיימת את שלוש האקסיומות:

1. $\rho(v,w)=0 \iff v=w$.
2. $\rho(v,w)=\rho(w,v)$.
3. לכל $u,v,w\in V$ מתקיים $\rho(v,w)\le\rho(v,u)+\rho(u,w)$.

הערה 2.1.18. על אותו מרחב וקטורי V ניתן להגדיר פונקציות מרחק שונות.

דוגמא 2.1.19. נסתכל ב- $V=\mathbb{R}^2$ כאשר $v=\begin{pmatrix}v_1\\v_2\end{pmatrix},\ w=\begin{pmatrix}w_1\\w_2\end{pmatrix}$:

1. נגדיר

$$\rho(v,w)=\max\left(|v_1-w_1|,|v_2-w_2|\right)$$

ברור כי

$$\begin{aligned}\rho(v,w)&=\max\left(|v_1-w_1|,|v_2-w_2|\right)\\&=\max\left(|w_1-v_1|,|w_2-v_2|\right)=\rho(w,v)\end{aligned}$$

2. בנוסף מתקיים אי-שוויון המשולש כי

$$\begin{aligned}\rho(u,w)&=\max\left(|u_1-w_1|,|u_2-w_2|\right)\\\rho(v,u)&=\max\left(|v_1-u_1|,|v_2-u_2|\right)\end{aligned}$$

ולפי תכונות הערך המוחלט:

$$\begin{aligned}|v_1-w_1|&\leq|v_1-u_1|+|u_1-w_1|\\|v_2-w_2|&\leq|v_2-u_2|+|u_2-w_2|\end{aligned}$$

מכאן נקבל כי:

$$\begin{aligned}\max\left(|v_1-w_1|,|v_2-w_2|\right)&\leq\max\left(|v_1-u_1|+|u_1-w_1|,|v_2-u_2|+|u_2-w_2|\right)\\&\leq\max\left(|v_1-u_1|,|v_2-u_2|\right)+\max\left(|u_1-w_1|,|u_2-w_2|\right)\end{aligned}$$

כלומר $\rho(v,w)\leq\rho(v,u)+\rho(u,w)$.

אפשר להגדיר פונקצית מרחק שונה לאותו מרחב, למשל

$$\tilde{\rho}(v,u)=|v_1-u_1|+|v_2-u_2|.$$

ברור כי $\tilde{\rho}$ מקיים את אקסיומות (1) ו- (2).
לגבי אקסיומת אי-שוויון משולש:
מתקיים

$$\begin{aligned}\tilde{\rho}(w,u)&=|w_1-u_1|+|w_2-u_2|\\\tilde{\rho}(v,w)&=|v_1-w_1|+|v_2-w_2|\end{aligned}$$

וסכומם

$$\underbrace{\left(|v_1-w_1|+|w_1-u_1|\right)}_{\geq|v_1-u_1|}+\underbrace{\left(|v_2-w_2|+|w_2-u_2|\right)}_{\geq|v_2-u_2|}$$

כלומר $\tilde{\rho}(v,u)\leq\tilde{\rho}(v,w)+\tilde{\rho}(w,u)$.

דוגמא 2.1.20. פונקצית המרחק המוכרת

$$d(u,v)=\sqrt{(u_1-v_1)^2+(u_2-v_2)^2}=\|u-v\|.$$

הגדרה 2.1.21. אם V מרחב וקטורי עם פונקצית מרחק אז V נקרא מרחב מטרי.

הערה 2.1.22. אפשר להגדיר פונקצית מרחק על מרחבים מעל $\mathbb{Z}_2$.
פונקציה שימושית כזו היא מרחק Hamming שמודד עד כמה שני וקטורים של אותיות או 0 ו- 1 שונים זה מזה.
המרחק בין שני וקטורים (או בין שתי מילים) מוגדר להיות מספר המקומות השונים זה מזה
לא קשה לראות שהפונקציה הזו מקיימת את האקסיומות.

מסקנה 2.1.23. יהי V מרחב מכפלה פנימית. נגדיר $\rho(u,v) = \|u-v\|$, אז זו פונקצית מרחק.

בפרט כל מרחב אוקלידי אפשר להפוך למרחב מטרי ע"י הגדרת פונקצית מרחק באופן כזה.

הוכחה. הוכחה: נראה את קיומן של שלוש האקסיומות:

1. $u=v \iff u-v=\overrightarrow{0} \iff \|u-v\|=0$.
2. $\|u-v\| = \|(-1)(v-u)\| = |-1|\cdot\|v-u\| = \|v-u\|$.
3. $\|u-v\| = \|(u-w)+(w-v)\| \le \|u-w\|+\|w-v\|$.

□

בפרט כל מרחב אוקלידי אפשר להפוך למרחב מטרי ע"י הגדרת פונקצית מרחק באופן כזה.

הגדרה 2.1.24. יהי V מרחב אוקלידי. אזי עבור $v,w\neq 0$ מתקיים

$$-1 \le \frac{\langle v,w\rangle}{\|v\|\cdot\|w\|} \le 1 \iff |\langle v,w\rangle| \le \|v\|\cdot\|w\| \,.$$

אז במרחב אוקלידי אפשר להגדיר את φ להיות הזוית בין שני הוקטורים v,w ע"י:

$$\cos\varphi = \frac{\langle v,w\rangle}{\|v\|\cdot\|w\|}$$

(φ מוגדרת היטב כי $|\cos\varphi| \le 1$).

ומכאן ש- $\langle v,w\rangle = \|v\|\cdot\|w\|\cdot\cos\varphi$.

דוגמא 2.1.25. 1. עבור $v=w$ נקבל $\cos\varphi = 1$ ומכאן $\varphi = 0$.

2. עבור $w=-v$ נקבל $\cos\varphi=-1$ ומכאן $\varphi=\pi$.

הערה 2.1.26. למה אי אפשר להגדיר מכפלה פנימית מעל שדה $\mathbb{Z}_p$?
בגלל ששם לא מוגדר סדר על המספרים. לכן למשל אקסיומה (4) של ההגדרה של מכפלה פנימית לא יכולה להתקיים.

2.2 אורתוגונליות ובסיס אורתונורמלי

הגדרה 2.2.1. יהי V מרחב מכפלה פנימית. וקטורים $u,v \in V$ נקראים אורתוגונלים או ניצבים אם $\langle u,v\rangle = 0$.
במקרה כזה מסמנים $u \perp v$.

הערה 2.2.2. הוקטור היחיד שהוא אורתוגונלי לכל הוקטורים במרחב הוא וקטור האפס
(כי כל ווקטור השונה מ- $\overrightarrow{0}$ אינו אורתוגונלי לעצמו).

הגדרה 2.2.3. יהי V מרחב מכפלה פנימית. קבוצה $\{v_1,\dots,v_k\}$ נקראת אורתוגונלית אם לכל $1 \leq i \neq j \leq k$ מתקיים
$v_i \perp v_j$.

משפט 2.2.4. יהי V מרחב מכפלה פנימית ו- $\{v_1,\dots,v_k\}$ קבוצה אורתוגונלית ב- V. אם $\overrightarrow{0} \notin \{v_1,\dots,v_k\}$ אז
הקבוצה $\{v_1,\dots,v_k\}$ היא בלתי תלויה לינארית.

הוכחה. יהיו $\alpha_1,\dots,\alpha_k$ כך ש- $\sum_{i=1}^{k}\alpha_i v_i = 0$.
אז לכל j המקיים $1 \leq j \leq k$ מתקיים

$$0 = \left\langle \sum_{i=1}^{k}\alpha_i v_i, v_j \right\rangle = \sum_{i=1}^{k}\alpha_i \langle v_i, v_j\rangle = \alpha_j \underbrace{\langle v_j, v_j\rangle}_{\neq 0}$$

ומכאן ש- $\alpha_j = 0$ לכל $1 \leq j \leq k$, ולכן הקבוצה $\{v_1,\dots,v_k\}$ בלתי תלויה לינארית. $\square$

מסקנה 2.2.5. יהי V מרחב מכפלה פנימית n-מימדי ו- $\{v_1,\dots,v_k\}$ קבוצה אורתוגונלית כך ש- $\overrightarrow{0} \notin \{v_1,\dots,v_k\}$.
אז $k \leq n$.

הגדרה 2.2.6. בסיס $\{v_1,\dots,v_n\}$ של מרחב מכפלה פנימית V נקרא אורתוגונלי אם הקבוצה $\{v_1,\dots,v_n\}$ אורתוגונלית,
ונקרא אורתונורמלי אם בנוסף כל v_i נורמלי, כלומר $\|v_i\| = 1$ לכל $1 \leq i \leq n$.

הערה 2.2.7. קבוצה אורתונורמלית היא תמיד בלתי תלויה לינארית.

משפט 2.2.8 (גרם – שמידט).[1] יהי V מרחב מכפלה פנימית ויהי $\{v_1,\dots,v_n\}$ בסיס של V.
אז קיים בסיס אורתונורמלי $\{u_1,\dots,u_n\}$ המקיים

$$\text{span}\{v_1,\dots,v_i\} = \text{span}\{u_1,\dots,u_i\}$$

לכל $1 \leq i \leq n$.

הערה 2.2.9. המשפט נכון גם עבור מרחבי מכפלה פנימית בעלי מימד אינסופי.

הוכחה. שלב ראשון: נגדיר $u_1 = \frac{1}{\|v_1\|}\cdot v_1$ ואז $\|u_1\| = 1$ וברור ש- $\text{span}\{u_1\} = \text{span}\{v_1\}$.
שלב שני: נגדיר $w_2 = v_2 - \langle v_2, u_1\rangle u_1$.
נבדוק אורתוגונליות:

$$\begin{aligned}\langle w_2, u_1\rangle &= \langle v_2 - \langle v_2,u_1\rangle u_1, u_1\rangle \\ &= \langle v_2,u_1\rangle - \langle v_2,u_1\rangle\langle u_1,u_1\rangle \\ &= \langle v_2,u_1\rangle - \langle v_2,u_1\rangle\cdot 1 = 0\end{aligned}$$

[1] J□rgen Pedersen Gram 1850 – 1916
Erhard Schmidt 1876 1959–

כלומר $u_1 \perp w_2$.
כעת ננרמל: נגדיר $u_2 = \frac{1}{\|w_2\|} \cdot w_2$.
ברור ש- $u_1, u_2 \in \text{span}\{v_1, v_2\}$, וגם לפי משפט 2.2.4 הקבוצה $\{u_1, u_2\}$ בת"ל,
כך ש- $\text{span}\{u_1, u_2\} \subseteq \text{span}\{v_1, v_2\}$ וגם $\dim \text{span}\{v_1, v_2\} = \dim \text{span}\{u_1, u_2\} = 2$,
לכן $\text{span}\{v_1, v_2\} = \text{span}\{u_1, u_2\}$.

שלב שלישי: נניח שבנינו קבוצה $\{u_1, \ldots, u_j\}$ אורתונורמלית ו- $\text{span}\{v_1, \ldots, v_j\} = \text{span}\{u_1, \ldots, u_j\}$.
נגדיר

$$w_{j+1} = v_{j+1} - \sum_{i=1}^{j} \langle v_{j+1}, u_i \rangle u_i .$$

ראשית נשים לב ש- $w_{j+1} \neq 0$ כי $w_{j+1} \notin \text{span}\{v_1, \ldots, v_j\} = \text{span}\{u_1, \ldots, u_j\}$.
כעת נבדוק ש- $u_i \perp w_{j+1}$ לכל $1 \leq i \leq j$:

$$\begin{aligned}
\langle w_{j+1}, u_i \rangle &= \left\langle v_{j+1} - \sum_{s=1}^{j} \langle v_{j+1}, u_s \rangle u_s, u_i \right\rangle \\
&= \langle v_{j+1}, u_i \rangle - \sum_{s=1}^{j} \langle v_{j+1}, u_s \rangle \langle u_s, u_i \rangle \\
&= \langle v_{j+1}, u_i \rangle - \langle v_{j+1}, u_i \rangle = 0
\end{aligned}$$

וזה אומר ש- $u_i \perp w_{j+1}$ לכל $1 \leq i \leq j$.

ננרמל את w_{j+1} ע"י שנגדיר

$$u_{j+1} = \frac{1}{\|w_{j+1}\|} \cdot w_{j+1} .$$

לכל u_i כאשר $1 \leq i \leq j$ מתקיים $u_i \in \text{span}\{v_1, \ldots, v_j\}$ ולכן $u_i \in \text{span}\{v_1, \ldots, v_{j+1}\}$.
אז $u_{j+1} \in \text{span}\{u_1, \ldots, u_j, v_{j+1}\} = \text{span}\{v_1, \ldots, v_{j+1}\}$,
ומכאן

$$\text{span} \underbrace{\{u_1, \ldots, u_{j+1}\}}_{\text{קבוצה אורתונורמלית בלתי תלויה לינארית}} \subseteq \text{span}\{v_1, \ldots, v_{j+1}\} .$$

כמו כן מתקיים

$$j + 1 = \dim \text{span}\{u_1, \ldots, u_{j+1}\} = \dim \text{span}\{v_1, \ldots, v_{j+1}\}$$

ומכאן מקבלים

$$\text{span}\{u_1, \ldots, u_{j+1}\} = \text{span}\{v_1, \ldots, v_{j+1}\} .$$

□

הגדרה 2.2.10. תהליך הבנייה של בסיס אורתונורמלי $\{u_1, \ldots, u_n\}$ מבסיס $\{v_1, \ldots, v_n\}$ במרחב מכפלה פנימית, כך שלכל i מתקיים $\text{span}\{u_1, \ldots, u_i\} = \text{span}\{v_1, \ldots, v_i\}$ נקרא תהליך גרם – שמידט.

מסקנה 2.2.11. יהי V מרחב מכפלה פנימית ממימד n אז:

1. יש ל- V בסיס אורתונורמלי.
2. כל קבוצה אורתונורמלית ב- V אפשר להשלים לבסיס אורתונורמלי.

משפט 2.2.12 (פיתגורס). [2] יהי V מרחב מכפלה פנימית ו- $\{v_1,\dots,v_k\}$ קבוצה של וקטורים אורתוגונלים ב- V.
אז

$$\left\|\sum_{i=1}^{k} v_i\right\|^2=\sum_{i=1}^{k}\|v_i\|^2 .$$

הוכחה.

$$\left\|\sum_{i=1}^{k} v_i\right\|^2=\left\langle\sum_{i=1}^{k} v_i,\sum_{i=1}^{k} v_i\right\rangle=\sum_{i=1}^{k}\sum_{j=1}^{k}\underbrace{\langle v_i,v_j\rangle}_{\delta_{ij}\langle v_i,v_j\rangle}=\sum_{i=1}^{k}\|v_i\|^2 .$$

□

הערה 2.2.13. משפט 2.2.12 הוא הכללה של משפט פיתגורס המוכר בגיאומטריה תיכונית.

משפט 2.2.14. יהי V מרחב מכפלה פנימית ו- $\{v_1,\dots,v_n\}$ בסיס אורתונורמלי.
אז לכל $v\in V$ מתקיים $v=\sum_{i=1}^{n}\langle v,v_i\rangle v_i$.

הוכחה. יהי $\{v_1,\dots,v_n\}$ בסיס אורתונורמלי ו- $v\in V$ וקטור כלשהו, אז $v=\sum_{i=1}^{n}\alpha_i v_i$.
נמצא את המקדמים α_i:

$$\langle v,v_j\rangle=\left\langle\sum_{i=1}^{n}\alpha_i v_i,v_j\right\rangle=\sum_{i=1}^{n}\alpha_i\underbrace{\langle v_i,v_j\rangle}_{\delta_{ij}}=\alpha_j .$$

□

משפט 2.2.15. יהי V מרחב מכפלה פנימית ו- $B=\{v_1,\dots,v_n\}$ בסיס של V, אז B הוא בסיס אורתונורמלי אם ורק אם לכל $v,w\in V$ כאשר $v=\sum_{i=1}^{n}\alpha_i v_i$ ו- $w=\sum_{i=1}^{n}\beta_i v_i$ מתקיים

$$\langle v,w\rangle=\sum_{i=1}^{n}\alpha_i\overline{\beta}_i . \tag{2.2}$$

הוכחה. כיוון ראשון: נניח כי (2.2) מתקיים, אז בפרט $v_i=1\cdot v_i$ ו- $v_j=1\cdot v_j$ ומכאן

$$\langle v_i,v_j\rangle=\begin{cases}1, & i=j\\ 0, & \text{אחרת}\end{cases}$$

אז $B=\{v_1,\dots,v_n\}$ הוא בסיס אורתונורמלי.

כיוון שני: נניח כי $B=\{v_1,\dots,v_n\}$ קבוצה אורתונורמלית, אז

$$\begin{aligned}\langle v,w\rangle&=\left\langle\sum_{i=1}^{n}\alpha_i v_i,\sum_{j=1}^{n}\beta_j v_j\right\rangle=\sum_{i=1}^{n}\alpha_i\left\langle v_i,\sum_{j=1}^{n}\beta_j v_j\right\rangle\\&=\sum_{i=1}^{n}\alpha_i\sum_{j=1}^{n}\overline{\beta}_j\underbrace{\langle v_i,v_j\rangle}_{\delta_{ij}}=\sum_{i=1}^{n}\alpha_i\overline{\beta}_i\cdot 1=\sum_{i=1}^{n}\alpha_i\overline{\beta}_i\end{aligned}$$

□

[2] Pythagoras 570 BC – 495 BC

הערה 2.2.16. כאשר הוכחנו (בפרק הקודם) שכל מרחב וקטורי ממימד סופי מעל הממשיים אפשר לצייד במכפלה פנימית, בעצם לקחנו בסיס והגדרנו מכפלה פנימית כזו שהבסיס הנבחר הוא אורתונורמאלי ביחס אליה.

הגדרה 2.2.17. יהי V מרחב מכפלה פנימית ו- $\{v_1,\dots,v_k\}$ קבוצה אורתונורמלית ב- V.
יהי $v\in V$, אז $\alpha_j=\langle v,v_j\rangle$ (כאשר $1\le j\le k$) נקרא מקדם פורייה[3] ה- j של v לפי הקבוצה $\{v_1,\dots,v_k\}$.

משפט 2.2.18 (אי-שוויון בסל). [4] יהי V מרחב מכפלה פנימית ו- $\{v_1,\dots,v_k\}$ קבוצה אורתונורמלית ב- V. יהי $v\in V$ וקטור כלשהו עם מקדמי פורייה $\{\alpha_1,\dots,\alpha_k\}$.
אז

$$\|v\|^2\ge|\alpha_1|^2+\cdots+|\alpha_k|^2.$$

הוכחה. נשלים את $\{v_1,\dots,v_k\}$ עד לבסיס אורתונורמלי $\{v_1,\dots,v_k,w_{k+1},\dots,w_n\}$.
אז לפי משפט 2.2.14:

$$v=\sum_{i=1}^k\underbrace{\langle v,v_i\rangle}_{\alpha_i}v_i+\sum_{j=k+1}^n\underbrace{\langle v,w_j\rangle}_{\beta_j}w_j$$

כלומר $v=\sum_{i=1}^k\alpha_iv_i+\sum_{j=k+1}^n\beta_jw_j$.
לפי ההגדרה:

$$\|v\|^2=\langle v,v\rangle=\left\langle\sum_{i=1}^k\alpha_iv_i+\sum_{j=k+1}^n\beta_jw_j,\sum_{i=1}^k\alpha_iv_i+\sum_{j=k+1}^n\beta_jw_j\right\rangle$$

ולפי משפט פיתגורס נקבל:

$$\|v\|^2=\sum_{i=1}^k\underbrace{\langle\alpha_iv_i,\alpha_iv_i\rangle}_{|\alpha_i|^2}+\sum_{j=k+1}^n\underbrace{\langle\beta_jw_j,\beta_jw_j\rangle}_{|\beta_j|^2}=\sum_{i=1}^k|\alpha_i|^2+\sum_{j=k+1}^n|\beta_j|^2\ge\sum_{i=1}^k|\alpha_i|^2.$$

□

מסקנה 2.2.19 (שוויון פרסבל). [5] יהי V מרחב מכפלה פנימית ו- $\{v_1,\dots,v_k\}$ בסיס אורתונורמלי של V. יהי $v\in V$ ונכתוב $\alpha_i=\langle v,v_i\rangle$.
אז

$$\|v\|^2=\sum_{i=1}^k|\alpha_i|^2.$$

משפט 2.2.20. יהי V מרחב מכפלה פנימית ו- $\{v_1,\dots,v_k\}$ קבוצה אורתונורמלית ב- V. יהי $v\in V$ וקטור כלשהו עם מקדמי פורייה $\{\alpha_1,\dots,\alpha_k\}$.
אז לכל $\beta_1,\dots,\beta_k\in F$ מתקיים

$$\left\|v-\sum_{i=1}^k\alpha_iv_i\right\|\le\left\|v-\sum_{i=1}^k\beta_iv_i\right\|,$$

והשוויון מתקבל אם ורק אם $\beta_i=\alpha_i$ לכל $1\le i\le k$.

---

[3] Joseph Fourier 1768 – 1830
[4] Friedrich Wilhelm Bessel 1784 – 1846
[5] Marc-Antoine Parseval 1755 – 1836

הוכחה. נבדוק כי $v-\sum_{i=1}^{k}\alpha_i v_i \perp \sum_{j=1}^{k}\gamma_j v_j$:

$$\begin{aligned}\left\langle v-\sum_{i=1}^{k}\alpha_i v_i, \sum_{j=1}^{k}\gamma_j v_j\right\rangle &= \left\langle v, \sum_{j=1}^{k}\gamma_j v_j\right\rangle - \sum_{i=1}^{k}\alpha_i\left\langle v_i, \sum_{j=1}^{k}\gamma_j v_j\right\rangle \\ &= \sum_{j=1}^{k}\overline{\gamma}_j\left\langle v, v_j\right\rangle - \sum_{i=1}^{k}\alpha_i\sum_{j=1}^{k}\overline{\gamma}_j\left\langle v_i, v_j\right\rangle \\ &= \sum_{j=1}^{k}\overline{\gamma}_j\alpha_j - \sum_{i=1}^{k}\overline{\gamma}_i\alpha_i = 0\end{aligned}$$

כעת

$$\left\|\underbrace{v-\sum_{i=1}^{k}\beta_i v_i}_{z}\right\| = \left\|\underbrace{v-\sum_{i=1}^{k}\alpha_i v_i}_{w}+\underbrace{\sum_{i=1}^{k}\left(\alpha_i-\beta_i\right)v_i}_{u}\right\|$$

והראינו ש- $u\perp w$. לכן לפי משפט פיתגורס נקבל

$$\begin{aligned}\|z\|^2 = \|w+u\|^2 = \|w\|^2+\|u\|^2 &= \left\|v-\sum_{i=1}^{k}\alpha_i v_i\right\|^2 + \left\|\underbrace{\sum_{i=1}^{k}(\alpha_i-\beta_i)v_i}_{\sum_{i=1}^{k}|\alpha_i-\beta_i|^2\|v_i\|^2}\right\|^2 \\ &= \left\|v-\sum_{i=1}^{k}\alpha_i v_i\right\|^2 + \underbrace{\sum_{i=1}^{k}\left|\alpha_i-\beta_i\right|^2}_{\geq 0} \geq \left\|v-\sum_{i=1}^{k}\alpha_i v_i\right\|^2\end{aligned}$$

כלומר בסה"כ קיבלנו $\left\|v-\sum_{i=1}^{k}\beta_i v_i\right\|^2 \geq \left\|v-\sum_{i=1}^{k}\alpha_i v_i\right\|^2$,
והשוויון מתקבל אם ורק אם $\sum_{i=1}^{k}\left|\alpha_i-\beta_i\right|^2=0$, כלומר $\alpha_i=\beta_i$ לכל $1\leq i\leq k$.
אם נוציא שורש ריבועי משני אגפי אי-השוויון הנ"ל נקבל $\left\|v-\sum_{i=1}^{k}\beta_i v_i\right\| \geq \left\|v-\sum_{i=1}^{k}\alpha_i v_i\right\|$,
והשוויון מתקבל אם ורק אם $\alpha_i=\beta_i$ לכל $1\leq i\leq k$. □

הערה 2.2.21. תהי $\{v_1,\ldots,v_k\}$ קבוצה אורתונורמלית במרחב מכפלה פנימית, ונסמן $U=\operatorname{span}\{v_1,\ldots,v_k\}$.
נגדיר פונקצית מרחק על V ע"י $\rho(u,v)=\|u-v\|$.
תהי $W\subseteq V$ קבוצה כלשהי ב- V ו- $v\in V$, ונגדיר $\rho(v,W)=\inf\{\rho(v,w)|w\in W\}$.
אז $\rho(v,U)=\min\{\rho(v,u)|u\in U\}$ מוגדר היטב ומתקיים $\rho(v,U)=\rho(v,w)$ כאשר $w=\sum_{i=1}^{k}\langle v,v_i\rangle v_i$.

2.3 משלים אורתוגונלי

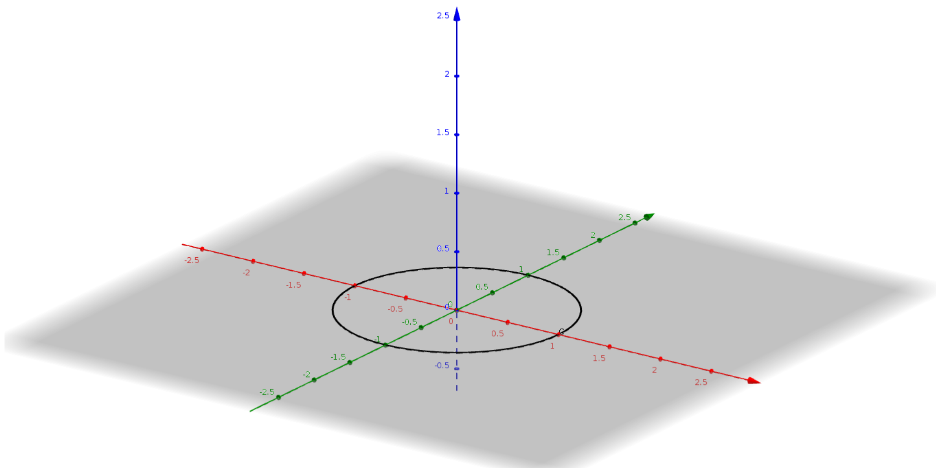
2.3.1 תתי מרחב אורתוגונליים

הגדרה 2.3.1 יהי V מרחב מכפלה פנימית ותהיינה $U, W \subseteq V$ קבוצות לא ריקות ב- V.

אומרים ש- $U \perp W$ (W ניצב ל- U) אם לכל $w \in W$ ולכל $u \in U$ מתקיים $w \perp u$.

טענה 2.3.2 יהי V מרחב מכפלה פנימית, ותהיינה $U, W \subseteq V$ קבוצות לא ריקות.
אם $U \perp W$ אז $U \cap W \subseteq \left\{ \overrightarrow{0} \right\}$ (ז"א או $\left\{ \overrightarrow{0} \right\}$ או קבוצה ריקה).

דוגמא 2.3.3 ב- $\mathbb{R}^3$ החיתוך בין ציר ה- z לבין מעגל היחידה במישור xy הוא $\emptyset$:



הוכחה. נניח כי $v \in W \cap U$, אז $v \perp v$ ומכאן ש- $v = \overrightarrow{0}$. □

מסקנה 2.3.4 יהי V מרחב מכפלה פנימית ו- $U, W \subset V$ תתי-מרחב כך ש- $U \perp W$. אז $U + W = U \oplus W$.

טענה 2.3.5 יהי V מרחב מכפלה פנימית ו- $U_1, \ldots, U_k \subset V$ תתי-מרחב כך ש- $V = \bigoplus_{i=1}^k U_i$ ונניח ש- $U_i \perp U_j$ לכל $1 \le i \ne j \le k$.
יהיו $u, v \in V$ שני וקטורים שניתנים לכתיבה $u = u_1 + \cdots + u_k$ ו- $v = v_1 + \cdots + v_k$ כאשר $u_i, v_i \in U_i$.
אז

$$\langle u, v \rangle = \sum_{i=1}^k \langle u_i, v_i \rangle .$$

הוכחה.

$$\langle u, v \rangle = \left\langle \sum_{i=1}^k u_i, \sum_{j=1}^k v_j \right\rangle = \sum_{i=1}^k \sum_{j=1}^k \langle u_i, v_j \rangle \underset{u_i \perp v_j,\ i \ne j}{=} \sum_{i=1}^k \langle u_i, v_i \rangle .$$

□

הגדרה 2.3.6 יהי V מרחב מכפלה פנימית ותהי $\emptyset \ne W \subset V$ קבוצה כלשהי.
משלים אורתוגונלי של W הוא הקבוצה

$$W^{\perp} = \{ v \in V | \langle v, w \rangle = 0,\ \forall w \in W \}.$$

משפט 2.3.7. יהי V מרחב מכפלה פנימית ו- $\emptyset \neq W \subset V$ אז $W^{\perp}$ הוא תת-מרחב.

הוכחה.
1. $W^{\perp} \neq \emptyset$ כי $\overrightarrow{0} \in W^{\perp}$.
2. אם $v \in W^{\perp}$ אז לכל $\alpha \in F$ ולכל $w \in W$ מתקיים $\langle \alpha v, w\rangle = \alpha \langle v, w\rangle = 0$,
זאת אומרת ש- $\alpha v \in W^{\perp}$.
3. לכל $u, v \in W^{\perp}$ ולכל $w \in W$ מתקיים $\langle u+v, w\rangle = \langle u, w\rangle + \langle v, w\rangle = 0$,
לכן $u + v \in W^{\perp}$.

$\square$

משפט 2.3.8. יהי V מרחב מכפלה פנימית n-מימדי, ויהי $W \subseteq V$ תת-מרחב. אז $V = W \oplus W^{\perp}$.

הוכחה. $W + W^{\perp} = W \oplus W^{\perp}$ לפי מסקנה 2.3.4 (כי לפי ההגדרה $W \perp W^{\perp}$).
צריך להוכיח כי $W \oplus W^{\perp} = V$.
יהי $\{w_1, \dots, w_k\}$ בסיס אורתונורמלי של W, ויהי $\{u_1, \dots, u_m\}$ בסיס אורתונורמלי של $W^{\perp}$.
אז $\{w_1, \dots, w_k, u_1, \dots, u_m\}$ היא קבוצה אורתונורמלית.
אם היא לא בסיס של V, אז ניתן להשלים אותה לבסיס אורתונורמלי של V: $\{w_1, \dots, w_k, u_1, \dots, u_m, v_1, \dots, v_s\}$.
אבל לפי ההגדרה $w_i \perp v_j$ לכל $1 \leq i \leq k$, ולכן $v_j \perp W$ ומכאן כי $v_j \in W^{\perp}$, וזו סתירה.
מכאן מקבלים ש- $W \oplus W^{\perp} = V$. $\square$

מסקנה 2.3.9. יהי V מרחב מכפלה פנימית ו- $\emptyset \neq W \subset V$. אז $W \subseteq \left(W^{\perp}\right)^{\perp}$.
בפרט אם W תת-מרחב ו- V ממימד סופי אז $W = \left(W^{\perp}\right)^{\perp}$.

הוכחה. לכל $w \in W$ ולכל $u \in W^{\perp}$ מתקיים $u \perp w$, לכן $W \subseteq \left(W^{\perp}\right)^{\perp}$.
אם W הוא תת-מרחב אז $V = W \oplus W^{\perp}$ לפי משפט 2.3.8, וגם $V = W^{\perp} \oplus \left(W^{\perp}\right)^{\perp}$.
בנוסף מקבלים כי $\dim W = \dim V - \dim W^{\perp}$ סופי, וגם $\dim \left(W^{\perp}\right)^{\perp} = \dim V - \dim W^{\perp}$.
לכן $\dim \left(W^{\perp}\right)^{\perp} = \dim W$.
לפי משפט מאלגברה לינארית א': תת-מרחב של מרחב סוף מימדי שהמימד שלו שווה למימד של המרחב הוא המרחב כולו, ז"א $W = \left(W^{\perp}\right)^{\perp}$. $\square$

מסקנה 2.3.10. המשלים האורתוגונלי הוא יחיד.

2.3.2 היטל אורתוגונלי

הגדרה 2.3.11. יהי V מרחב מכפלה פנימית ויהי $U \subseteq V$ תת-מרחב.
$V = U \oplus U^{\perp}$ ולכן לכל $v \in V$ קיימים $u \in U$ ו- $w \in U^{\perp}$ יחידים כך ש- $v = u + w$.
ההיטל על U במקביל ל- $U^{\perp}$ המסומן $\mathrm{pr}_U^{\perp} = \mathrm{pr}_U^{U^{\perp}} : V \to U$ המקיים $\mathrm{pr}_U^{\perp} v = u$ נקרא היטל אורתוגונלי על U.

מסקנה 2.3.12. יהי V מרחב מכפלה פנימית ויהי $U \subseteq V$ תת-מרחב ו- $v \in V$.
יהי $u = \mathrm{pr}_U^{\perp} v$, אז

$$\min_{w \in U} \|v - w\| = \|v - u\|$$

ו-

$$\|v - w\| = \|v - u\| \iff w = u.$$

הוכחה.

$$\|v-w\|^2=\left\|\underbrace{(v-u)}_{u^\perp\in U^\perp}+(u-w)\right\|^2$$

לכן $\underbrace{(u-w)}_{\in U}\perp\underbrace{(v-u)}_{\in U^\perp}$, ואז לפי משפט פיתגורס

$$\|v-w\|^2=\|v-u\|^2+\underbrace{\|u-w\|^2}_{\geq 0}\geq\|v-u\|^2$$

והשוויון מתקבל אם ורק אם $\|u-w\|=0$ כלומר כאשר $u=w$.
לפי מונוטוניות של ריבוע על אי-שליליים מקבלים $\|v-w\|\geq\|v-u\|$, והשוויון מתקבל אם ורק אם $u=w$. ☐

מסקנה 2.3.13. יהי V מרחב מכפלה פנימית, $U\subseteq V$ תת-מרחב, ו- $\{v_1,\ldots,v_k\}$ בסיס אורתונורמלי של U.
אז

$$\mathrm{pr}_U^\perp v=\sum_{i=1}^k\alpha_i v_i$$

כאשר $\alpha_i=\langle v,v_i\rangle$ הם מקדמי פוריה.

הוכחה. לפי משפט 20 מהפרק הקודם מתקיים

$$\left\|v-\sum_{i=1}^k\alpha_i v_i\right\|\leq\|v-w\|$$

לכל $w\in U$, והשוויון מתקבל אם ורק אם $w=\sum_{i=1}^k\alpha_i v_i$.
לפי מסקנה 2.3.12 מתקיים $\|v-u\|\leq\|v-w\|$ והשוויון מתקבל אם ורק אם $w=u$.
מכאן מקבלים

$$u=\sum_{i=1}^k\alpha_i v_i.$$

☐

2.4 מכפלה פנימית כללית ב- $\mathbb{C}^n$

2.4.1 תבניות ומטריצות

הגדרה 2.4.1. תהי $A \in M_{n\times m}(\mathbb{F})$ כאשר $\mathbb{F}=\mathbb{R},\mathbb{C}$.
נגדיר $A^* = \overline{A^t}$.

המטריצה A^* נקראת הצמודה ההרמיטית של המטריצה A.
אם $\mathbb{F}=\mathbb{R}$ נקבל $A^* = A^t$.
אם $\mathbb{F}=\mathbb{C}$ אז עבור $A = \left((\alpha_{ij})_{i=1}^n\right)_{j=1}^m$ נקבל $A^* = \left((\overline{\alpha}_{ji})_{i=1}^n\right)_{j=1}^m$ ז"א $(A^*)_{ij} = \overline{\alpha}_{ji}$.

למה 2.4.2. תהיינה $A \in M_{n\times m}(\mathbb{F}), B \in M_{m\times k}(\mathbb{F})$ כאשר $\mathbb{F}=\mathbb{R},\mathbb{C}$.
אז

$$(AB)^* = B^*A^*.$$

הוכחה.

$$(AB)^* = \overline{(AB)^t} = \overline{B^tA^t} = \overline{B^t}\cdot\overline{A^t} = B^*A^*.$$

□

הערה 2.4.3. נסתכל על וקטור עמודה כמטריצה $n\times 1$

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in M_{n\times 1}(\mathbb{C})$$

אז $v^* = (\overline{v_1},\dots\overline{v_n}) \in M_{1\times n}(\mathbb{C})$.

הגדרה 2.4.4. תבנית $f:\mathbb{C}^n\times\mathbb{C}^n\to\mathbb{C}$ נקראת תבנית בילינארית אם היא לינארית לפי שני הגורמים, ז"א:

1. לכל $u,v,w\in\mathbb{C}^n$ מתקיים $f(u+v,w) = f(u,w)+f(v,w)$ וגם $f(u,v+w) = f(u,v)+f(u,w)$.
2. לכל $v,w\in\mathbb{C}^n$ ו- $\alpha\in\mathbb{C}$ מתקיים $f(\alpha v,w) = \alpha f(v,w) = f(v,\alpha w)$.

דוגמא 2.4.5 1. לכל $\mathbb{C}^n$ אפשר להגדיר $f(v,w)=0$ (תבנית לא מעניינת).

2. כל מכפלה פנימית היא תבנית בילינארית במרחב אוקלידי (מעל הממשיים).
במרחב אוניטרי (מעל המרוכבים) היא לינארית במשתנה הראשון, אבל לא במשתנה השני (בגלל ההצמדה)

הערה 2.4.6. לתבנית שהיא לינארית במשתנה הראשון ולינארית עם הצמדה במשתנה השני (כמו מכפלה פנימית מרוכבת) קוראים גם "תבנית $1\frac{1}{2}$ לינארית".

יהי $\{v_1,\dots,v_n\}$ בסיס של $\mathbb{F}^n$, ויהיו $v=\sum_{i=1}^n \alpha_i v_i$ ו- $w=\sum_{j=1}^n \beta_j v_j$ שני וקטורים.
תהי $f:\mathbb{C}^n\times\mathbb{C}^n\to\mathbb{C}$ תבנית בילינארית (או $1\frac{1}{2}$ לינארית).

אז לפי הגדרה 2.4.4 נקבל

$$f(v,w) = f\left(\sum_{i=1}^{n}\alpha_i v_i, \sum_{j=1}^{n}\beta_j v_j\right) = \sum_{i=1}^{n}\alpha_i f\left(v_i, \sum_{j=1}^{n}\beta_j v_j\right) \tag{2.3}$$

$$= \sum_{i=1}^{n}\alpha_i \sum_{j=1}^{n}\overline{\beta}_j f(v_i,v_j) = \sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i\overline{\beta}_j f(v_i,v_j) \tag{2.4}$$

מסקנה 2.4.7. תהי $f:\mathbb{F}^n\times\mathbb{F}^n\to\mathbb{F}$ תבנית בילינאארית ויהי $\{v_1,\dots,v_n\}$ בסיס של $\mathbb{F}^n$. אם יודעים מהם $f(v_i,v_j)$ לכל i,j אז יודעים מהם $f(v,w)$ לכל v,w לפי הנוסחה (2.3).

בהינתן $\{v_1,\dots,v_n\}$ בסיס של $\mathbb{C}^n$, נגדיר מטריצה של תבנית בילינארית (או אחת וחצי לינארית) $A_f = [A_f]_{\{v_1,\dots,v_n\}}$ (ביחס לבסיס זה) ע"י $a_{ij}=f(v_j,v_i)$ לכל $1\le i,j\le n$.
נקבל

$$A_f = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn}\end{pmatrix}.$$

הערה 2.4.8. שימו לב שהאינדקסים מחליפים מקומות: $a_{ij}=f(v_j,v_i)$.

טענה 2.4.9. יהי $V=\mathbb{F}^n$ ו- $\{v_1,\dots,v_n\}$ בסיס של $\mathbb{F}^n$. תהי $f:\mathbb{F}^n\times\mathbb{F}^n\to\mathbb{F}$ תבנית בילינארית (או אחת וחצי לינארית) ו- $(A_f)_{ij}=f(v_j,v_i)$ מטריצה של התבנית f.
אז לכל $v,w\in\mathbb{F}^n$ כך ש- $v=\sum_{i=1}^n\alpha_i v_i$ ו- $w=\sum_{j=1}^n\beta_j v_j$ נקבל

$$f(v,w)=w^*A_f v.$$

הוכחה. מצד אחד

$$f(v,w)=\sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i\overline{\beta}_j f(v_i,v_j)=\sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i\overline{\beta}_j a_{ji},$$

מצד שני

$$w^*A_f v = (\overline{\beta}_1,\dots,\overline{\beta}_n)\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn}\end{pmatrix}\begin{pmatrix}\alpha_1\\ \vdots \\ \alpha_n\end{pmatrix} = (\overline{\beta}_1,\dots,\overline{\beta}_n)\begin{pmatrix}\sum_{i=1}^n a_{1i}\alpha_i \\ \sum_{i=1}^n a_{2i}\alpha_i \\ \vdots \\ \sum_{i=1}^n a_{ni}\alpha_i\end{pmatrix}$$

$$= \sum_{j=1}^{n}\overline{\beta}_j\sum_{i=1}^{n}a_{ji}\alpha_i = \sum_{j=1}^{n}\sum_{i=1}^{n}\alpha_i\overline{\beta}_j a_{ji}$$

□

הגדרה 2.4.10. תהי $A=(a_{i,j})_{i,j=1}^n$ מטריצה ב- $M_n(\mathbb{F})$ ויהיו $v,w\in\mathbb{F}^n$ כאשר

$$v=\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix},\ w=\begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix}$$

לפי בסיס סטנדרטי.

נגדיר את התבנית

$$.f_A(v,w)=w^*Av$$

מסקנה 2.4.11. f_A היא תבנית בילינארית (או אחת וחצי לינארית) המתאימה לתבנית המקיימת $f(e_i,e_j)=a_{ji}$.

מסקנה 2.4.12. יש העתקה חד-חד ערכית ועל בין תבניות בילינאריות על $\mathbb{F}^n$ ו- $M_n(\mathbb{F})$ דרך $f_A(v,w)=w^*Av$ ו- $.f(e_i,e_j)=a_{ji}$

-

הוכחה. לפי הבנייה שעשינו ברור כי קיימת העתקה מתבניות למטריצות ריבועיות והיא על.

נשאר להראות כי אם $f\neq\tilde{f}$ תבניות בילינאריות, אז $A_f\neq A_{\tilde{f}}$, וזה שקול ל- $f=\tilde{f}\implies A_f=A_{\tilde{f}}$.

אם $f\neq\tilde{f}$ אז קיימים i,j כך ש- $.f(e_i,e_j)\neq\tilde{f}(e_i,e_j)$

לכן $\left(A_{\tilde{f}}\right)_{ji}\neq(A_f)_{ji}$ וזה אומר ש- $.A_f\neq A_{\tilde{f}}$ □

כעת אנו יודעים כי כל מכפלה פנימית היא תבנית בי-לינארית.

2.4.2 מטריצה של מכפלה פנימית

שאלה 2.4.13. מהם התנאים הנדרשים ממטריצה A כדי שהיא תהיה מטריצה של מכפלה פנימית?

נזכיר כי תכונות נוספת של מכפלה פנימית הן:

1. $.\langle v,w\rangle=\overline{\langle w,v\rangle}$
2. $\langle v,v\rangle>0$ לכל $.v\neq\overrightarrow{0}$

תהי A מטריצה של מכפלה פנימית, אז $\langle v,w\rangle=w^*Av$ ו- $.\langle w,v\rangle=v^*Aw$

לפי התכונה הראשונה נקבל $\langle v,w\rangle=\overline{\langle w,v\rangle}$ ולכן $.w^*Av=\overline{v^*Aw}=(v^*Aw)^*=w^*A^*v$

בפרט זה נכון לכל $v=e_i$ ו- $.w=e_j$

לפי הגדרה $\langle e_i,e_j\rangle=a_{ji}=e_j^*Ae_i$ ולכן נקבל $.e_j^*A^*e_i=(A^*)_{ji}=\overline{a_{ij}}$

כלומר קיבלנו כי לכל i,j מתקיים ש- $a_{ji}=\overline{a_{ij}}$, ובמילים אחרות $.A^*=A$

הגדרה 2.4.14.
1. מטריצה $A\in M_n(\mathbb{R})$ המקיימת $A^t=A$ נקראת מטריצה סימטרית.
2. מטריצה $A\in M_n(\mathbb{C})$ המקיימת $A^*=A$ נקראת מטריצה הרמיטית.

הערה 2.4.15. מטריצה הרמיטית ממשית היא מטריצה סימטרית.

לכן מטריצה של מכפלה פנימית במרחב אוניטרי היא מטריצה הרמיטית, ומטריצה של מכפלה פנימית במרחב אוקלידי היא מטריצה סימטרית.

התנאי השני הוא ש- $\langle v,v\rangle > 0$ לכל $v \neq 0$.
ז"א A צריכה לקיים $v^*Av > 0$ לכל $v \neq 0$.

הגדרה 2.4.16. 1. מטריצה $A \in M_n(\mathbb{C})$ הרמיטית המקיימת $v^*Av > 0$ לכל $0 \neq v \in \mathbb{C}^n$ נקראת מטריצה הרמיטית מוגדרת חיובית.

2. מטריצה $A \in M_n(\mathbb{R})$ סימטרית המקיימת $v^*Av > 0$ לכל $0 \neq v \in \mathbb{R}^n$ נקראת מטריצה סימטרית מוגדרת חיובית.

מסקנה 2.4.17. $A \in M_n(\mathbb{C})$ (או $A \in M_n(\mathbb{R})$) היא מטריצה של מכפלה פנימית אם ורק אם היא מטריצה הרמיטית (סימטרית) מוגדרת חיובית.

מסקנה 2.4.18. יהי $V = \mathbb{R}^n, \mathbb{C}^n$. כל מכפלה פנימית על V מוגדרת על ידי מטריצה הרמיטית מוגדרת חיובית A, כאשר $(A)_{ij} = \langle e_j, e_i\rangle$ לפי הבסיס הסטנדרטי $\{e_1,\dots,e_n\}$.

הערה 2.4.19. מכפלה פנימית סטנדרטית היא מכפלה שעבורה $A = I_n$.
נזכיר שהגדרנו

$$\langle u,v\rangle = \left\langle \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}, \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \right\rangle = \sum_{i=1}^n \alpha_i \overline{\beta}_i$$
$$= (\overline{\beta}_1,\dots,\overline{\beta}_n) \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

שאלה 2.4.20. מהן התכונות של מטריצה הרמיטית מוגדרת חיובית?

משפט 2.4.21. תהי $A \in M_n(\mathbb{C})$.

1. אם A הרמיטית אז כל הערכים העצמיים שלה הם ממשיים.

2. אם A הרמיטית מוגדרת חיובית, אז כל הערכים העצמיים שלה הם חיוביים.

הוכחה. תהי A הרמיטית, ויהי α ערך עצמי של A עם וקטור עצמי מתאים v. נקבל

$$v^*Av = v^*\alpha v = \alpha v^*v = \alpha\langle v,v\rangle$$

ואם נסתכל על הצמוד המרוכב

$$(v^*Av)^* = (\alpha\langle v,v\rangle)^* = \overline{\alpha}\overline{\langle v,v\rangle} = \overline{\alpha}\langle v,v\rangle$$

מצד שני,

$$(v^*Av)^* = v^*A^*v = v^*Av = \alpha\langle v,v\rangle$$

ולכן $\overline{\alpha}\langle v,v\rangle = \alpha\langle v,v\rangle$, ומכיוון ש- $\langle v,v\rangle \neq 0$ נקבל $\alpha = \overline{\alpha}$, או במילים אחרות, α ממשי.

נשאר להוכיח שאם A הרמיטית מוגדרת חיובית אז $\alpha > 0$:
נכתוב

$$0 < v^*Av = v^*\alpha v = \alpha v^*v = \alpha\langle v, v\rangle$$

ולכן $\alpha > 0$. $\square$

הערה 2.4.22. בהמשך נראה כי כל מטריצה הרמיטית היא לכסינה, ושמטריצה הרמיטית מוגדרת חיובית אם ורק אם כל הערכים העצמיים שלה הם חיוביים.

מסקנה 2.4.23. יהי $V = \mathbb{C}^n$. כל מכפלה פנימית על V מוגדרת ע"י A מטריצה הרמיטית מוגדרת חיובית לפי הבסיס הסטנדרטי $\{e_1, \ldots, e_n\}$ כאשר $(A)_{ij} = \langle e_j, e_i\rangle$.

הערה 2.4.24. מכפלה פנימית סטנדרטית היא המכפלה הפנימית שעבורה $A = I_n$.
אכן,

$$\begin{aligned}\langle v, w\rangle = \left\langle \begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}, \begin{pmatrix}\beta_1\\ \vdots\\ \beta_n\end{pmatrix}\right\rangle &= \sum_{i=1}^{n}\alpha_i\beta_i\\ &= (\beta_1, \ldots, \beta_n)\begin{pmatrix}1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & 1\end{pmatrix}\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}\end{aligned}$$

שאלה 2.4.25. תהי $f(v, w)$ תבנית בי-לינארית המוגדרת לפי בסיס $B_1 = \{v_1, \ldots v_n\}$ ע"י מטריצה A.
איך נראית מטריצה של אותה תבנית במעבר לבסיס $B_2 = \{w_1, \ldots, w_n\}$?

תשובה 2.4.26.
- נזכיר כי המטריצה $M_{B_1}^{B_2}$ מייצגת את הווקטורים של הבסיס B_2 לפי הבסיס B_1.
- מתקיים $M_{B_2}^{B_1}[v]_{B_1} = [v]_{B_2}$ (וזה שקול ל- $M_{B_1}^{B_2}[v]_{B_2} = [v]_{B_1}$).
- התבנית לפי הבסיס B_1 מיוצגת ע"י המטריצה A.
- רוצים למצוא את המטריצה מייצגת של אותה תבנית לפי הבסיס B_2.
- בהינתן $[v]_{B_2}$ ו- $[w]_{B_2}$, אנו רוצים להעביר את v ואת w ל- B_1.
- תחילה $[v]_{B_1} = M_{B_1}^{B_2}[v]_{B_2}$.
  מכאן נקבל

$$\begin{aligned}f\left([v]_{B_2}, [w]_{B_2}\right) &= \left(M_{B_1}^{B_2}[w]_{B_2}\right)^* \cdot A \cdot M_{B_1}^{B_2}[v]_{B_2}\\ &= \left([w]_{B_2}\right)^*\left(M_{B_1}^{B_2}\right)^* \cdot A \cdot M_{B_1}^{B_2} \cdot [v]_{B_2}\end{aligned}$$

ומכאן כי המטריצה המייצגת את התבנית לפי הבסיס B_2 היא:

$$B = \left(M_{B_1}^{B_2}\right)^* \cdot A \cdot M_{B_1}^{B_2}.$$

הגדרה 2.4.27. מטריצות $A, B \in M_n(\mathbb{C})$ נקראות חופפות, אם קיימת מטריצה $M \in M_n(\mathbb{C})$ הפיכה כך ש- $B = M^*AM$.

מסקנה 2.4.28. מטריצות חופפות מייצגות את אותה תבנית בילינארית לפי בסיסים שונים.

הערה 2.4.29. חפיפה הוא יחס שקילות, וזה יחס שקילות שונה מדמיון.
מטריצות דומות בדרך כלל לא חופפות, ומטריצות חופפות לא דומות.

דוגמא 2.4.30. תהי $A = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}$. אז $B = \begin{pmatrix} 1 & 2 \\ 0 & 4 \end{pmatrix}$ דומה ל- A, אבל היא לא חופפת לה.
הסבר: $(P^*AP)^* = P^*A^*P = P^*AP$, כלומר כל מטריצה חופפת ל- A היא הרמיטית, אבל B לא הרמיטית.
נראה כי $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ חופפת ל- A:

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0.5 \end{pmatrix}^* \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0.5 \end{pmatrix}$$

אבל היא לא דומה ל- A, כי הערכים העצמיים של A הם $1, 4$ ול- I_2 יש ערך עצמי יחיד 1.

מסקנה 2.4.31. תהי A מטריצה הרמיטית מוגדרת חיובית, כלומר מטריצה של מכפלה פנימית.
אזי לפי גרם-שמידט קיים למכפלה הפנימית הזו בסיס אורתונורמלי , ז"א קיימת מטריצה הפיכה כך ש-

$$I_n = M^*AM.$$

מסקנה 2.4.32. מטריצה A היא הרמיטית מוגדרת חיובית אם ורק אם קיימת מטריצה הפיכה P כך ש- $A = P^*P$.

הוכחה. כיוון ראשון: אם $A = P^*P$ כאשר P הפיכה, אזי A הרמיטית כי

$$A^* = (P^*P)^* = P^*P = A.$$

A גם מוגדרת חיובית כי

$$v^*Av = v^*P^*Pv = \langle Pv, Pv \rangle > 0$$

לכל $v \neq 0$ (כי $Pv \neq 0 \implies v \neq 0$).
כיוון שני: תהי A הרמיטית מוגדרת חיובית. אז לפי מסקנה 2.4.31 אפשר לכתוב $I_n = M^*AM$ ואז $A = (M^*)^{-1} M^{-1}$.
לפי הגדרה $I_n = M^* (M^*)^{-1}$ וגם $M^{-1}M = I_n$ כך ש-

$$\left(M^{-1}M\right)^* = M^* \left(M^{-1}\right)^* = (I_n)^* = I_n$$

לכן ברור כי $(M^*)^{-1} = \left(M^{-1}\right)^*$.
מכאן מקבלים $A = \left(M^{-1}\right)^* M^{-1}$ או במילים אחרות $A = P^*P$ כאשר $P = M^{-1}$. $\square$

הערה 2.4.33. ראינו שכל מכפלה פנימית מוגדרת על-ידי מטריצה הרמיטית מוגדרת חיובית שהיא $A = P^* I_n P$. כלומר מכפלה פנימית לא סטנדרטית היא אותו דבר כמו מכפלה פנימית סטנדרטית לפי בסיס לא סטנדרטי, לכן שינוי מכפלה פנימית שקול לשינוי בסיס עבור מכפלה סטנדרטית.

הגדרה 2.4.34. מטריצה $A \in M_n(\mathbb{C})$ נקראת אוניטרית אם $A^*A = I$,
או במילים אחרות $A^{-1} = A^*$.

הגדרה 2.4.35. מטריצה $A \in M_n(\mathbb{R})$ נקראת אורתוגונלית אם $A^tA = I$,
או במילים אחרות $A^{-1} = A^t$ (כלומר מטריצה אורתוגונלית היא מטריצה אוניטרית ממשית).

משפט 2.4.36. תהי $A \in M_n(\mathbb{C})$ (או $A \in M_n(\mathbb{R})$), ו- $A = \left(\underbrace{a_1, \ldots, a_n}_{\text{וקטורי עמודה}}\right)$.
אז A אוניטרית (אורתוגונלית) אם ורק אם הקבוצה $\{a_1, \ldots, a_n\}$ היא בסיס אורתונורמלי לפי המכפלה הפנימית הסטנדרטית.

הוכחה. A אוניטרית $\iff A^*A = I$.
נסמן $A = (a_1, \ldots, a_n)$ אז

$$A^*A = \begin{pmatrix} \overline{a}_1^t \\ \vdots \\ \overline{a}_n^t \end{pmatrix} (a_1, \ldots, a_n)$$

נשים לב ש- $\{a_1, \ldots, a_n\}$ הוא בסיס אורתונורמלי אם ורק אם

$$(A^*A)_{ij} = \overline{a}_i^t a_j = \langle a_j, a_i \rangle = \delta_{ij},$$

וזה שקול ל- $A^*A = I$. $\square$

הגדרה 2.4.37. מטריצה $A \in M_n(\mathbb{C})$ נקראת נורמלית אם $A^*A = AA^*$.

דוגמא 2.4.38.
1. אם A מטריצה הרמיטית $A^* = A$, אז $AA^* = A^2 = AA = (A^*)^2$ לכן $A^*A = AA^*$.
2. מטריצה אוניטרית $A^*A = I$ כלומר $A^* = A^{-1}$ ומכאן $AA^* = I$. זאת אומרת ש- $A^*A = AA^*$.
3. $A \in M_n(\mathbb{C})$ נקראת אנטי-הרמיטית אם $A^* = -A$.
זו מטריצה נורמלית כי אכן מתקיים $A^*A = -A^2$ וגם $AA^* = A(-A) = -A^2$,
ולכן $A^*A = AA^*$.

הגדרה 2.4.39. יהי V מרחב מכפלה פנימית מעל $\mathbb{F}$ (כאשר $\mathbb{F} = \mathbb{R}, \mathbb{C}$) ויהי $T \in \text{End}\, V$.
האופרטור $T^* \in \text{End}\, V$ הוא אופרטור המקיים

$$\langle Tv, w \rangle = \langle v, T^*w \rangle$$

לכל $v, w \in V$.

האופרטור T^* נקרא אופרטור צמוד ל- T.

אם $B=\{e_1,\dots,e_n\}$ הוא בסיס אורתונורמלי לפי מכפלה פנימית ו- A_T היא מטריצה מייצגת של T לפי הבסיס B, אז לכל $v,w\in V$ מתקיים

$$\begin{aligned}\langle Tv,w\rangle &= \langle A_T[v]_B,[w]_B\rangle = [w]_B^*A_T[v]_B\\ &= \left(A_T^*[w]_B\right)^*[v]_B = \langle [v]_B, A_T^*[w]_B\rangle\end{aligned}$$

זאת אומרת ש- A_T^* היא מטריצה מייצגת של T^* לפי אותו בסיס.

הגדרה 2.4.40. יהי V מרחב מכפלה פנימית. אופרטור $T\in\operatorname{End}V$ נקרא הרמיטי אם $T^*=T$ לפי המכפלה הפנימית. ז"א אם $\langle v,Tw\rangle=\langle Tv,w\rangle$ לכל $v,w\in V$.

תרגיל 2.4.41. להוכיח כי $w^*Av=w^*Bv$ לכל $w,v\in\mathbb{C}^n$ אם ורק אם $A=B$.

מסקנה 2.4.42. יהי V מרחב מכפלה פנימית סוף-מימדי. אופרטור $T\in\operatorname{End}V$ הוא הרמיטי אם ורק אם לפי איזשהו בסיס אורתונורמלי המטריצה המייצגת A_T היא הרמיטית.

הוכחה. יהי $B=\{e_1,\dots,e_n\}$ בסיס אורתונורמלי.
ראינו כי $\langle Tv,w\rangle=[w]_B^*A_T[v]_B$.
בדיוק באותו אופן $\langle v,Tw\rangle=(A_T[w]_B)^*[v]_B=[w]_B^*A_T^*[v]_B$.
אז $\langle Tv,w\rangle=\langle v,Tw\rangle$ לכל $v,w\in V$ אם ורק אם $[w]_B^*A_T[v]_B=[w]_B^*A_T^*[v]_B$ לכל $[v]_B,[w]_B\in\mathbb{C}^n$,
וזה שקול לפי תרגיל 2.4.41 ל- $A_T=A_T^*$, כלומר A_T הרמיטית. □

הערה 2.4.43. אם T הרמיטי זה לא אומר שהמטריצה המייצגת של T לפי בסיס כלשהו היא הרמיטית:
יהי B_1 בסיס אורתונורמלי לפי המכפלה הפנימית ו- B_2 בסיס לא אורתונורמלי.
תהיינה $[T]_{B_1}$ מטריצה מיצגת של T לפי הבסיס B_1 ו- $M=M_{B_1}^{B_2}$ מטריצת מעבר.
אז המטריצה המייצגת של T לפי בסיס B_2 היא $[T]_{B_2}=M^{-1}[T]_{B_1}M$ כך ש-

$$[T]_{B_2}{}^*=\left(M^{-1}[T]_{B_1}M\right)^*=M^*[T]_{B_1}(M^*)^{-1}$$

וזה לא שווה ל- $[T]_{B_2}$.

תרגיל 2.4.44. מהם התנאים על M כך ש- $[T]_{B_2}^*=[T]_{B_2}$?

2.5 דמיון אורתוגונאלי

הגדרה 2.5.1. 1. מטריצות $A,B\in M_n(\mathbb{C})$ נקראות דומות אוניטרית אם קיימת $M\in M_n(\mathbb{C})$ אוניטרית כך ש- $A=M^*BM$.

2. מטריצות $A,B\in M_n(\mathbb{R})$ נקראות דומות אורתוגונלית אם קיימת $M\in M_n(\mathbb{R})$ אורתוגונלית כך ש- $A=M^tBM$.

הערה 2.5.2. מטריצות דומות אורתוגונלית הן גם דומות וגם חופפות.

הערה 2.5.3. גם דמיון וגם חפיפה הם יחסי שקילות, אבל עבור מטריצה לא אוניטרית, נקבל תוצאות שונות לגמרי אם נשתמש בה לדמיון או לחפיפה.
זאת אומרת שבאופן כללי $M^{-1}AM\neq M^*AM$.

תרגיל 2.5.4. נסתכל במטריצה

$$A=\begin{pmatrix}0&1\\-1&0\end{pmatrix},$$

ותהי המטריצה $M=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ הפיכה, ז"א $D=ad-bc\neq 0$.

אז $M^{-1}=\frac{1}{D}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}$, ולכן מטריצה B שדומה ל- A היא מהצורה

$$\begin{aligned}B=M^{-1}AM&=\frac{1}{D}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}\\&=\frac{1}{D}\begin{pmatrix}ab+cd&b^2+d^2\\-\left(a^2+c^2\right)&-(ab+cd)\end{pmatrix}\end{aligned}$$

ומטריצה C שחופפת ל- A היא מהצורה

$$C=M^tAM=\begin{pmatrix}a&c\\b&d\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}0&D\\-D&0\end{pmatrix}.$$

1. מצאו תנאי הכרחי ומספיק על M כדי ש- B תהי חופפת ל A.
2. מצאו תנאי הכרחי ומספיק על M כדי ש- C תהי דומה ל A.
3. מהן כל המטריצות שדומות אורתוגונלית ל A?

משפט 2.5.5. אם $A,B\in M_n(\mathbb{C})$ מטריצות דומות אוניטרית, אז:

א. אם A נורמלית אז גם B נורמלית.

ב. אם A אוניטרית אז גם B אוניטרית.

ג. אם A הרמיטית אז גם B הרמיטית.

משפט 2.5.6. אם $A,B\in M_n(\mathbb{R})$ מטריצות דומות אורתוגונלית, אז:

א. אם A נורמלית אז גם B נורמלית.

2. אם A אורתוגונלית אז גם B אורתוגונלית.

3. אם A סימטרית אז גם B סימטרית.

הוכחה. ההוכחה זהה למקרה של דמיון אוניטרי ולמקרה של דמיון אורתוגונלי. לכן נוכיח רק עבור דמיון אוניטרי.

1. נתון ש- $A^*A = AA^*$, ו- $B = M^*AM$ (כאשר M אוניטרית).
אז

$$\begin{aligned} B^*B &= (M^*AM)^* M^*AM = M^*A^*MM^*AM = M^*A^*AM \\ &= M^*AA^*M = M^*AIA^*M = M^*AM(M^*A^*M) = BB^* \end{aligned}$$

2. נתון ש- $A^*A = I$. אז
$$B^*B = M^* \underbrace{A^*MM^*A}_{I} M = M^*M = I.$$

3. אם $A = A^*$ ו- $B = M^*AM$ אז

$$B^* = (M^*AM)^* = M^*A^*M = M^*AM = B.$$

□

טענה 2.5.7 1. מכפלה של מטריצה הרמיטית (שונה ממטריצת האפס) במספר היא מטריצה הרמיטית אם ורק אם המספר הוא ממשי.

2. סכום של מטריצות הרמיטיות הוא מטריצה הרמיטית.

3. מכפלה של מטריצות אוניטריות היא מטריצה אוניטרית.

הוכחה. 1. $\overline{\alpha} \cdot A = \overline{\alpha} \cdot A^* = \overline{\alpha}\overline{A}^t = \left(\overline{\alpha A^t}\right) = (\alpha A)^*$. ומכאן נקבל $(\alpha A)^* = \alpha A$ אם ורק אם $\alpha = \overline{\alpha}$, כלומר α ממשי.

2. $(A+B)^* = A^* + B^* = A + B$.

3. אם A, B אוניטריות, אז $(AB)^*AB = B^*A^*AB = I$.

□

משפט 2.5.8 (שור). [6]

1. כל מטריצה $A \in M_n(\mathbb{C})$ דומה אוניטרית למטריצה משולשית עליונה.

2. אם מטריצה $A \in M_n(\mathbb{R})$ ניתנת לשילוש אז היא דומה אורתוגונלית למטריצה משולשית עליונה.

[6] Issai Schur 1875 - 1941

הוכחה. לפי משפט על מטריצות ניתנות לשילוש, כל מטריצה $A \in M_n(\mathbb{C})$ ניתנת לשילוש דומה למטריצה משולשית עליונה.

ז"א שקיים בסיס $B = \{v_1, \dots, v_n\}$ כך שלכל v_i כאשר $1 \le i \le n$ מתקיים

$$[A]_B = \begin{pmatrix} a_{11} & a_{12} & \cdots & \star \\ 0 & a_{22} & \cdots & \vdots \\ \vdots & & \ddots & \star \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix} \iff Av_i = \sum_{j=1}^{i} a_{ji} v_j$$

לפי גרם-שמידט, קיים בסיס אורתונורמאלי $\{u_1, \dots, u_n\}$ כך שלכל i מתקיים $\text{span}\{u_1, \dots, u_i\} = \text{span}\{v_1, \dots, v_i\}$.

נשים לב ש- $Au_i \in \text{span}\{v_1, \dots, v_i\} = \text{span}\{u_1, \dots, u_i\}$, כי $u_i = a_1 v_1 + \cdots + a_i v_i$ ו- $Av_j \in \text{span}\{v_1, \dots, v_j\}$ לכל j.

ז"א שקיימים β_{ji} כאשר $j \le i$ כך ש- $Au_i = \sum_{j=1}^{i} \beta_{ji} u_j$, או בצורה מטריציאלית:

$$A_{\{u_1, \dots, u_n\}} = \begin{pmatrix} \beta_{11} & \beta_{12} & \cdots & \star \\ 0 & \beta_{22} & \cdots & \vdots \\ \vdots & & \ddots & \star \\ 0 & \cdots & 0 & \beta_{nn} \end{pmatrix}$$

וזו מטריצה משולשת עליונה.

אבל מעבר מבסיס לבסיס זה דימיון לפי מטריצה שהעמודות שלה הם וקטורים של הבסיס, כלומר:

$$[u_1, \dots, u_n]^{-1} A [u_1, \dots, u_n] = \begin{pmatrix} \beta_{11} & \beta_{12} & \cdots & \star \\ 0 & \beta_{22} & \cdots & \vdots \\ \vdots & & \ddots & \star \\ 0 & \cdots & 0 & \beta_{nn} \end{pmatrix}.$$

ראינו שהבסיס $\{u_1, \dots, u_n\}$ הוא אורתונורמלי אם ורק אם המטריצה $U = [u_1, \dots, u_n]$ אוניטרית.

מכאן ש-

$$U^* A U = \begin{pmatrix} \beta_{11} & \beta_{12} & \cdots & \star \\ 0 & \beta_{22} & \cdots & \vdots \\ \vdots & & \ddots & \star \\ 0 & \cdots & 0 & \beta_{nn} \end{pmatrix}$$

וזו מטריצה משולשית עליונה. □

שאלה 2.5.9. מהי צורה "קנונית" של מטריצה נורמלית לפי דימיון אוניטרי?

כלומר מהי מטריצה משולשית עליונה שדומה למטריצה נורמלית?

התשובה ניתנת במשפט הבא:

משפט 2.5.10. מטריצה $A \in M_n(\mathbb{C})$ היא נורמלית אם ורק אם היא דומה אוניטרית למטריצה אלכסונית.

הוכחה. כיוון ראשון: נניח ש- A דומה אוניטרית למטריצה אלכסונית, ז"א קיימת P אוניטרית כך ש- $P^*AP = \operatorname{diag}(\alpha_1, \dots, \alpha_n)$.
בגלל שמטריצה אלכסונית היא נורמלית, אז לפי משפט 2.5.5, A נורמלית.

כיוון שני: תהי A נורמלית. אז לפי משפט 2.5.8, A דומה אוניטרית למטריצה משולשית עליונה $B = \begin{pmatrix} \beta_{11} & \cdots & \beta_{1n} \\ & \ddots & \\ 0 & & \beta_{nn} \end{pmatrix}$.

אז לפי משפט 2.5.5 המטריצה B נורמלית, כלומר $BB^* = B^*B$.

נזכיר ש- $B^* = \begin{pmatrix} \overline{\beta}_{11} & \cdots & 0 \\ \vdots & \ddots & \\ \overline{\beta_{1n}} & & \overline{\beta}_{nn} \end{pmatrix}$.

נחשב $(B^*B)_{11} = \overline{\beta}_{11}\beta_{11} = |\beta_{11}|^2$ ו-
$(BB^*)_{11} = \beta_{11}\overline{\beta}_{11} + \beta_{12}\overline{\beta}_{12} + \cdots + \beta_{1n}\overline{\beta}_{1n} = |\beta_{11}|^2 + |\beta_{12}|^2 + \cdots + |\beta_{1n}|^2$.
מכיוון ש- $BB^* = B^*B$ וכל המספרים בסכום הזה הם לא שליליים, נובע ש- $\beta_{12} = \cdots = \beta_{1n} = 0$.

נמשיך באותו אופן: $(B^*B)_{22} = \overline{\beta}_{22}\beta_{22} = |\beta_{22}|^2$ ו-
$(BB^*)_{22} = \beta_{22}\overline{\beta}_{22} + \beta_{23}\overline{\beta}_{23} + \cdots + \beta_{2n}\overline{\beta}_{2n} = |\beta_{22}|^2 + |\beta_{23}|^2 + \cdots + |\beta_{2n}|^2$.
ושוב, מכיוון ש- $BB^* = B^*B$ וכל המספרים בסכום הם הם לא שליליים, נובע ש- $\beta_{23} = \cdots = \beta_{2n} = 0$.
באותו אופן מקבלים $\beta_{ij} = 0$ לכל $i < j$.
זאת אומרת ש- $B = \operatorname{diag}(\beta_{11}, \dots, \beta_{nn})$, וזו מטריצה אלכסונית. □

למה 2.5.11. אם A נורמלית, אז לכל $\alpha \in \mathbb{C}$ גם $A + \alpha I$ נורמלית.

הוכחה. נבדוק:

$$\begin{aligned}(A+\alpha I)(A+\alpha I)^* &= (A+\alpha I)(A^* + \overline{\alpha} I) \\ &= AA^* + \alpha A^* + \overline{\alpha}A + \alpha\overline{\alpha}I = (A+\alpha I)^*(A+\alpha I)\end{aligned}$$

□

למה 2.5.12. תהי A מטריצה נורמלית, α ערך עצמי שלה ו- v וקטור עצמי מתאים.
אז v הוא וקטור עצמי של A^* שמתאים לערך העצמי $\overline{\alpha}$.

הוכחה. נתון ש- $Av = \alpha v$, וזה שקול ל- $(A - \alpha I)v = 0$.
מכאן ש-

$$0 = \|(A-\alpha I)v\|^2 = \langle (A-\alpha I)v, (A-\alpha I)v \rangle$$

אבל לפי למה 2.5.11, המטריצה $B = A - \alpha I$ נורמלית, לכן

$$\begin{aligned}\langle Bv, Bv \rangle &= (Bv)^*(Bv) = v^*B^*Bv = v^*BB^*v \\ &= \langle (B^*v), (B^*v) \rangle = \|B^*v\|^2 \\ &= \|(A^* - \overline{\alpha}I)v\|^2\end{aligned}$$

וזה אומר ש- $(A^* - \overline{\alpha}I)v = 0$, כלומר v הוא וקטור עצמי של A^* עם ערך עצמי מתאים $\overline{\alpha}$. □

משפט 2.5.13. תהי A נורמלית, ו- α, β ערכים עצמיים שונים של A עם וקטורים עצמיים מתאימים u, v.
אז $u \perp v$.

הוכחה. נתון $\alpha \neq \beta$. נחשב:

$$\begin{aligned}\alpha \langle u, v\rangle &= \langle Au, v\rangle = v^* A u = \langle u, A^* v\rangle \\ &= \langle u, \overline{\beta} v\rangle = \beta \langle u, v\rangle\end{aligned}$$

כלומר $(\alpha-\beta)\langle u, v\rangle = 0$ ומכיוון ש- $\alpha \neq \beta$ מקבלים $\langle u, v\rangle = 0$, כלומר $v \perp u$ כנדרש. $\square$

מסקנה 2.5.14. תהי A מטריצה נורמלית ו- α, β ערכים עצמיים שונים של A עם וקטורים עצמיים מתאימים u, v, אז $V_{\alpha,A} \perp V_{\beta,A}$.

הגדרה 2.5.15. יהי V מרחב מכפלה פנימית ויהי $W \subset V$ תת מרחב.
היטל $E : V \to W$ נקרא היטל אורתוגונלי אם הוא במקביל למשלים האורתוגונלי של W.

משפט 2.5.16. יהי $V = \mathbb{C}^n$ (או $V = \mathbb{R}^n$) עם מכפלה פנימית סטנדרטית, יהי $W \subset V$ תת מרחב ו- $E : V \to W$ היטל אורתוגונלי.
אז E הוא אנדומורפיזם הרמיטי (סימטרי) והמטריצה המייצגת שלו לפי הבסיס הסטנדרטי, M_E היא מטריצה הרמיטית (סימטרית).

הוכחה. בשני המקרים ההוכחה זהה, לכן נוכיח כאשר $V = \mathbb{C}^n$.
יהי $\{v_1, \ldots, v_k\}$ בסיס אורתונורמלי של W. נשלים אותו לבסיס אורתונורמלי של V, כלומר $B = \{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$, כאשר $\{v_{k+1}, \ldots, v_n\}$ הוא בסיס של $W^\perp$.
נשים לב ש-

$$[E]_B = \operatorname{diag}(\underbrace{1, \ldots, 1}_{\text{פעמים } k}, \underbrace{0, \ldots, 0}_{\text{פעמים } n-k})$$

וזו מטריצה הרמיטית, לכן נובע ש- $E \in \operatorname{End}(V)$ הרמיטית.
נזכיר ש- $\{v_1, \ldots, v_n\}$ בסיס אורתונורמלי, כלומר המטריצה $[v_1, \ldots, v_n]$ (המטריצה שהעמודות שלה הן $v_1, \ldots, v_n$) היא מטריצה אוניטרית, ו-

$$[v_1, \ldots, v_n]^* M_E [v_1, \ldots, v_n] = [v_1, \ldots, v_n]^{-1} M_E [v_1, \ldots, v_n] = E_B$$

ולכן M_E היא מטריצה הרמיטית על פי משפט 2.5.5. $\square$

מסקנה 2.5.17. יהי $V = \mathbb{C}^n$ (או $V = \mathbb{R}^n$) עם מכפלה פנימית סטנדרטית, ויהי $E : V \to W$ היטל.
אז המטריצה המייצגת לפי הבסיס הסטנדרטי M_E היא הרמיטית אם ורק אם E הוא היטל אורתוגונלי. כלומר היטל אורתוגונלי הוא היטל הרמיטי.

הוכחה. אם E אורתוגונלי, אז M_E הרמיטית לפי משפט 2.5.16.
אם M_E הרמיטית אז היא דומה אוניטרית למטריצה אלכסונית שהיא

$$\operatorname{diag}(\underbrace{1, \ldots, 1}_{\text{פעמים } k}, \underbrace{0, \ldots, 0}_{\text{פעמים } n-k})$$

וזה בדיוק אומר שקיים בסיס אורתונורמלי $\{v_1, \ldots, v_n\}$ כך ש- $\{v_1, \ldots, v_k\}$ בסיס של W, ו- $\{v_{k+1}, \ldots, v_n\}$ הוא בסיס של משלים של W שלפיו מגדירים את ההיטל.
אז $W \perp \operatorname{span}\{v_{k+1}, \ldots, v_n\}$. $\square$

משפט 2.5.18 (פירוק ספקטרלי של מטריצות נורמליות). 1. תהי $A \in M_n(\mathbb{C})$ מטריצה נורמלית ו- $\alpha_1, \dots, \alpha_k$ ערכים עצמיים שונים שלה.
אז הפירוק הספקטרלי של A הוא $A = \sum_{i=1}^{k} \alpha_i E_i$ כאשר E_i הוא היטל הרמיטי לכל $1 \le i \le k$.
זאת אומרת שבמשפט הפירוק הספקטרלי הכללי צריך להוסיף לכל היטל את שם התואר "הרמיטי".

2. מטריצה לכסינה היא נורמלית אם ורק אם כל היטל בפירוק הוא הרמיטי.

הוכחה. 1. תהי A נורמלית, אז A לכסינה לפי משפט 2.5.10 ו- $V_{A,\alpha_i} \perp V_{A,\alpha_j}$ כאשר $i \neq j$, לפי מסקנה 2.5.14. לכן גם מתקיים

$$V_{A,\alpha_i} \perp \sum_{\substack{j=1 \\ j\neq i}}^{k} V_{A,\alpha_j}$$

כך ש- E_i הוא היטל על V_{A,α_i} במקביל ל- $\sum_{\substack{j=1 \\ j\neq i}}^{k} V_{A,\alpha_j}$ והוא הרמיטי על פי משפט 2.5.16.
קיבלנו ש- $A = \sum_{i=1}^{k} \alpha_i E_i$ כאשר E_i היא מטריצה הרמיטית לכל $1 \le i \le k$.
בגלל שהפירוק הספקטרלי הוא יחיד, מקבלים את כל התכונות האחרות של הפירוק לפי משפט הפירוק הספקטרלי.

2. תהי A לכסינה. אם A נורמלית, אז E_i הרמיטי לכל i לפי החלק הקודם.
עכשיו נניח ש- $A = \sum_{i=1}^{k} \alpha_i E_i$ כאשר E_i היא מטריצה הרמיטית לכל i ונראה ש- A נורמלית:
נחשב

$$A^* = \left(\sum_{i=1}^{k} \alpha_i E_i\right)^* = \sum_{i=1}^{k} \overline{\alpha_i} E_i^* = \sum_{i=1}^{k} \overline{\alpha_i} E_i$$

אז מקבלים

$$\begin{aligned} AA^* &= \left(\sum_{i=1}^{k} \alpha_i E_i\right)\left(\sum_{j=1}^{k} \overline{\alpha_j} E_j\right) = \sum_{i=1}^{k} \alpha_i \overline{\alpha_i} E_i \\ &= \sum_{i=1}^{k} \overline{\alpha_i} \alpha_i E_i = \left(\sum_{j=1}^{k} \overline{\alpha_j} E_j\right)\left(\sum_{i=1}^{k} \alpha_i E_i\right) = A^*A \end{aligned}$$

כלומר A נורמלית.

□

מסקנה 2.5.19. תהי $A \in M_n(\mathbb{C})$ נורמלית, אז:

1. A הרמיטית אם ורק אם כל הערכים העצמיים שלה ממשיים.
2. A הרמיטית מוגדרת חיובית אם ורק אם כל הערכים העצמיים שלה חיוביים.
3. A אוניטרית אם ורק אם כל הערכים העצמיים שלה הם בעלי ערך מוחלט השווה ל- 1.
4. A היא אנטי-הרמיטית אם ורק אם כל הערכים העצמיים שלה השונים מ- 0 הם מדומים.
5. מטריצה נורמלית ממשית היא לכסינה מעל הממשיים אם ורק אם היא סימטרית.
6. מטריצה ממשית לכסינה מעל הממשיים היא נורמלית אם ורק אם היא סימטרית.
7. מטריצה סימטרית ממשית דומה אורתוגונלית למטריצה אלכסונית.

הוכחה. A נורמלית, אז לפי משפט 2.5.18: $A=\sum_{i=1}^k \alpha_i E_i$ כאשר E_i הרמיטי, ו- $A^*=\sum_{i=1}^k \overline{\alpha_i}E_i$.

1. $A=A^*$ אם ורק אם $\overline{\alpha_i}=\alpha_i$, או במילים אחרות α_i ממשי לכל i.
2. A הרמיטית מוגדרת חיובית אם ורק אם $v^*Av>0$ לכל $v\neq 0$.
ל- v יש פירוק יחיד $v=v_1+\cdots+v_k$ כאשר $v_i\in V_{A,\alpha_i}$ כך ש-

$$\begin{aligned}0<v^*Av&=(v_1^*+\cdots+v_k^*)\left(\sum_{i=1}^k \alpha_i E_i\right)(v_1+\cdots+v_k)\\&=(v_1^*+\cdots+v_k^*)(\alpha_1 v_1+\cdots+\alpha_k v_k)=\alpha_1\|v_1\|^2+\cdots+\alpha_k\|v_k\|^2\end{aligned}$$

אז A מוגדרת חיובית אם ורק אם $\alpha_i>0$ לכל i.

3. $A=\sum_{i=1}^k \alpha_i E_i$ אוניטרית אם ורק אם
$A^*A=\sum_{i=1}^k \alpha_i\overline{\alpha_i}E_i$

זאת אומרת אם ורק אם $\alpha_i\overline{\alpha_i}=1$, או במילים אחרות $|\alpha_i|=1$.

4. $A^*=\sum_{i=1}^k \overline{\alpha_i}E_i$, ו- $A^*=-A$ שקול ל- $\overline{\alpha_i}=-\alpha_i$, זאת אומרת ש- $\alpha_i=0$ או ש- α_i מדומה.
5. מטריצה נורמלית ממשית לכסינה מעל הממשיים אם ורק אם כל הערכים העצמיים שלה ממשיים, זאת אומרת לפי 1 אם ורק אם היא הרמיטית.
מטריצה הרמיטית ממשית היא סימטרית.
6. מטריצה לכסינה מעל הממשיים ונורמלית היא סימטרית לפי 5.
7. ניקח בסיסים אורתונורמליים של V_{A,α_i} ויהי B איחוד של הבסיסים האלה. אז B הוא בסיס אורתונורמלי, ו- $[A]_B$ היא מטריצה אלכסונית, זאת אומרת ש- A דומה אורתוגונלית למטריצה אלכסונית.

□

תרגיל 2.5.20. הוכיחו את הטענות הבאות:

1. אם A מטריצה נורמלית אז כל חזקה טבעית שלה היא מטריצה נורמלית.
2. אם A מטריצה הרמיטית אז כל חזקה טבעית שלה היא מטריצה הרמיטית.
3. אם A הפיכה ונורמלית אז כל חזקה שלמה שלה היא נורמלית.
4. אם A הפיכה והרמיטית אז כל חזקה שלמה שלה היא הרמיטית.

הערה 2.5.21. מכפלה של מטריצות סימטריות לא חייבת להיות סימטרית.
יתרה מזו, אם A,B מטריצות סימטריות אז AB סימטרית אם ורק אם A ו- B מתחלפות.
אכן,

$$(AB)^t=B^tA^t=BA$$

ולכן $AB=(AB)^t$ אם ורק אם $AB=BA$.

למה 2.5.22. תהי $A\in M_n(\mathbb{R})$ סימטרית. אז

1. כל מטריצה חופפת ל- A היא סימטרית.

2. אם A סימטרית מוגדרת חיובית, אז כל מטריצה חופפת לה היא גם מוגדרת חיובית.

הוכחה. 1. $B = P^tAP$, אז

$$B^t = (P^tAP)^t = P^tA^tP = P^tAP = B.$$

2. A מוגדרת חיובית אם ורק אם לכל $0 \neq v \in \mathbb{R}^n$ מתקיים $v^tAv > 0$.
אז

$$v^tBv = v^tP^tAPv = (Pv)^tA(Pv) > 0$$

זאת אומרת ש- B מוגדרת חיובית.

□

נסיים במשפט המתאר צורה קנונית במחלקות שקילות של מטריצות סימטריות ממשיות חופפות.

משפט 2.5.23 (משפט התמדה של סילבסטר).[7] תהי $A \in M_n(\mathbb{R})$ מטריצה סימטרית. אז היא חופפת למטריצה יחידה מהצורה $\mathrm{diag}(I_k, -I_\ell, 0_m)$ כאשר $k + \ell + m = n$.
בפרט מטריצות סימטריות ממשיות הן חופפות אם ורק אם יש להן אותו מספר של ע"ע חיוביים ואותו מספר של ע"ע שליליים.

הוכחה. כל הערכים העצמיים של A הם ממשיים.
יהיו $\alpha_1, \dots, \alpha_k$ ערכים עצמיים חיוביים שלה (עם חזרות), ויהיו $\beta_1, \dots, \beta_\ell$ ערכים עצמיים שליליים שלה (עם חזרות).
אז 0 הוא ערך עצמי של A אם ורק אם $k + \ell < n$, ובמקרה הזה הריבוי של 0 הוא $n - (k + \ell)$.
לפי מסקנה 2.5.19 (חלק 7), המטריצה A דומה אורתוגונלית למטריצה אלכסונית

$$B = \mathrm{diag}(\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_\ell, \underbrace{0, \dots, 0}_{n-k-\ell \text{ פעמים}})$$

אז A גם חופפת ל- B.
ניקח

$$P = \mathrm{diag}\left(\frac{1}{\sqrt{\alpha_1}}, \dots, \frac{1}{\sqrt{\alpha_k}}, \frac{1}{\sqrt{-\beta_1}}, \dots, \frac{1}{\sqrt{-\beta_l}}, 1, \dots, 1\right)$$

ונקבל

$$\begin{aligned} P^tBP &= P^t\,\mathrm{diag}(\alpha_1, \dots \alpha_k, \beta_1, \dots, \beta_l, 0, \dots, 0)P \\ &= P(\alpha_1, \dots \alpha_k, \beta_1, \dots, \beta_l, 0, \dots, 0)P \\ &= \mathrm{diag}(\underbrace{1, \dots, 1}_{k \text{ פעמים}}, \underbrace{-1, \dots, -1}_{\ell \text{ פעמים}}, \underbrace{0, \dots, 0}_{n-k-\ell \text{ פעמים}}) \\ &= \mathrm{diag}(I_k, -I_\ell, 0_m) \end{aligned}$$

כלומר A חופפת למטריצה $\mathrm{diag}(I_k, -I_\ell, 0_m)$.

[7] James Joseph Sylvester 1814 – 1897

כדי להראות שהיא יחידה נזכיר כי מטריצות חופפות מייצגות אותן תבניות בילינאריות לפי בסיסים שונים.
בפרט, צמצום של A לתת מרחב שהוא סכום של מרחבים עצמיים ששייכים לערכים עצמיים חיוביים, היא מטריצה סימטרית מוגדרת חיובית, וצמצום של כל מטריצה חופפת ל- A לאותו תת מרחב היא גם מטריצה מוגדרת חיובית לפי למה 2.5.22 (חלק 2.)
לכן מספר הערכים החיוביים על האלכסון של מטריצה אלכסונית חופפת ל- A הוא $k' \geq k$.
בדיוק באותו אופן, צמצום של A לתת מרחב שהוא סכום של מרחבים עצמיים ששייכים לערכים עצמיים שליליים היא מטריצה סימטרית מוגדרת שלילית (כלומר מכפלה של מטריצה סימטרית מוגדרת חיובית ב- -1), וכל מטריצה חופפת למטריצה הזו היא מוגדרת שלילית.
לכן מספר הערכים השליליים על האלכסון של מטריצה אלכסונית חופפת ל- A הוא $\ell' \geq \ell$.

לבסוף נזכיר שדרגות של מטריצות חופפות הן שוות, לכן $k' + \ell' = k + \ell$, ומכאן נובע ש- $k' = k$ וגם $\ell' = \ell$, כלומר מספר הערכים העצמיים החיוביים ומספר הערכים העצמיים השליליים הם קבועים לכל מטריצות סימטריות חופפות, כך ש- $\operatorname{diag}(I_k, -I_\ell, 0_m)$ היא יחידה. ☐

הגדרה 2.5.24. תהי $A \in M_n(\mathbb{R})$ מטריצה סימטרית. ההפרש בין מספר הערכים העצמיים החיוביים של A למספר הערכים העצמיים השליליים שלה (ז"א $k - \ell$ במשפט 2.5.23) נקרא סיגנטורה או חותמת של A.
$\operatorname{sign}\ A = k - \ell$.

הערה 2.5.25. לפעמים המושג חותמת משמש לציון הזוג (k, ℓ) של מספר הערכים העצמיים החיוביים ומספר הערכים העצמיים השליליים.

מסקנה 2.5.26. מטריצות סימטריות $A, B \in M_n(\mathbb{R})$ הן חופפות אם ורק אם $\operatorname{rank} A = \operatorname{rank} B$ וגם $\operatorname{sign}\ A = \operatorname{sign}\ B$.

הוכחה. תרגיל. ☐

2.6 מטריצות מוגדרות חיובית ומוגדרות אי-שלילית

2.6.1 שורש של מטריצה

הגדרה 2.6.1. מטריצה $A \in M_n(\mathbb{C})$ הרמיטית נקראת:

1. מוגדרת חיובית אם לכל $0 \neq v \in \mathbb{C}^n$ מתקיים $v^*Av > 0$.
2. מוגדרת אי-שלילית אם לכל $0 \neq v \in \mathbb{C}^n$ מתקיים $v^*Av \geq 0$.

משפט 2.6.2. תהי A מטריצה הרמיטית (או סימטרית ממשית), אזי התנאים הבאים שקולים:

1. A מוגדרת אי-שלילית (חיובית).
2. כל הע"ע של A אי-שליליים (חיוביים).
3. קיימת מטריצה הרמיטית C (הרמיטית הפיכה) כך ש- $A = C^2$.
4. קיימת B (הפיכה) כך ש- $A = B^*B$.

הוכחה. הוכחה: נוכיח $1. \implies 2. \implies 3. \implies 4. \implies 1.$

$1. \implies 2$:

נתון $v^*Av \geq 0$ ($v^*Av > 0$) לכל $0 \neq v \in \mathbb{C}^n$.

בפרט לערך עצמי α עם וקטור עצמי v

$$0 \leq v^*Av = v^*\alpha v = \alpha \underbrace{\langle v, v \rangle}_{>0}$$

ולכן $\alpha \geq 0$ (ואם מחליפים את הסימן $\geq$ ב- $>$ זה גם נכון).

$2. \implies 3$:

לפי המשפט הספקטרלי, $A = \alpha_1 E_1 + \cdots + \alpha_k E_k$ כאשר $\alpha_1, \ldots, \alpha_k \geq 0$ (או $\alpha_1, \ldots, \alpha_k > 0$) ו- $E_1, \ldots, E_k$ הרמיטיים.

נגדיר $C = \sum_{i=1}^k \sqrt{\alpha_i} E_i$, ואז לפי טענה מהפרק הקודם נובע ש- C הרמיטית.

אז

$$C^2 = \left(\sum_{i=1}^k \sqrt{\alpha_i} E_i \right)^2 = \sum_{i=1}^k \sum_{j=1}^k \sqrt{\alpha_i} \sqrt{\alpha_j} \underbrace{E_i E_j}_{\delta_{ij} E_i} = \sum_{i=1}^k \alpha_i E_i = A.$$

$3. \implies 4$:

ניקח $B = C$. מכיוון ש- C הרמיטית, מתקיים $B^* = C^* = C = B$,

ולכן $A = C^2 = B^*B$.

$4. \implies 1$:

נתון $A = B^*B$ אז $A^* = (B^*B)^* = B^*B = A$ הרמיטית.

לכל $v \in \mathbb{C}^n$ מתקיים

$$v^*Av = v^*B^*Bv = \langle Bv, Bv \rangle \geq 0.$$

(בהתאם, אם B הפיכה אז לכל $v \neq 0$ גם $Bv \neq 0$ ואז $\langle Bv, Bv \rangle > 0$). □

מסקנה 2.6.3. לכל מטריצה A הרמיטית (סימטרית ממשית) מוגדרת אי-שלילית (חיובית) קיימת C הרמיטית (סימטרית ממשית) מוגדרת אי-שלילית (חיובית) כך ש- $A = C^2$.

הוכחה. זאת בדיוק C מההוכחה של משפט 2.6.2.

$\square$

הגדרה 2.6.4. תהי A מטריצה הרמיטית (סימטרית ממשית) מוגדרת אי-שלילית (חיובית). למטריצה היחידה C שהיא הרמיטית (סימטרית ממשית) מוגדרת אי-שלילית (חיובית) המקיימת $A = C^2$ קוראים שורש של A.

הערה 2.6.5. 1. לכל $A \in M_n(\mathbb{C})$ לכסינה קיימת $B \in M_n(\mathbb{C})$ כך ש- $A = B^2$.
(תרגיל: למה זה נכון?)

2. לכל $A \in M_n(\mathbb{C})$ הפיכה קיימת $B \in M_n(\mathbb{C})$ כך ש- $A = B^2$.

משפט 2.6.6. המטריצה $A = (\alpha_{ij})_{i,j=1}^n$ היא הרמיטית (סימטרית ממשית) מוגדרת אי-שלילית (חיובית) אם ורק אם קיימים וקטורים $\{v_1, \ldots, v_n\}$ (בלתי תלויים לינארית) כך ש- $\alpha_{ij} = \langle v_j, v_i \rangle$.

הוכחה. אם A הרמיטית (סימטרית ממשית) מוגדרת אי-שלילית (חיובית), אז קיימת B כך ש- $A = B^*B$.
יהי $B = [v_1, \ldots, v_n]$, אז

$$A = \begin{bmatrix} v_1^* \\ \vdots \\ v_n^* \end{bmatrix} \begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix},$$

ז"א $(A_{ij}) = v_i^* v_j = \langle v_j, v_i \rangle$.
יתרה מכך, A מוגדרת חיובית אם ורק אם B הפיכה, ז"א $\{v_1, \ldots, v_n\}$ בלתי תלויים לינארית. $\square$

2.7 פירוקים של מטריצה, ערכים סינגולריים ומשפט SVD

לפעמים מבחינה טכנית נוח להציג מטריצה כמכפלה של כמה מטריצות עם תכונות מיוחדות.
למשל ראינו כבר פירוק של מטריצה הפיכה כמכפלה של מטריצות אלמנטריות.
בפרק הזה נלמד כמה פירוקים חשובים.

2.7.1 פירוקים של מטריצה

משפט 2.7.1. 1. תהי $A \in M_n(\mathbb{C})$ מטריצה הפיכה, אז A ניתנת לפירוק יחיד $A = UH$ כאשר H הרמיטית מוגדרת חיובית ו- U אוניטרית.

2. תהי $A \in M_n(\mathbb{R})$ מטריצה הפיכה, אז A ניתנת לפירוק יחיד $A = US$ כאשר S סימטרית מוגדרת חיובית ו- U אורתוגונלית.

הוכחה. הוכחת המשפט היא על ידי בניה של מטריצות הפירוק.
נוכיח רק את 1. ההוכחה של 2. זהה, רק מחליפים את המטריצה המרוכבת במטריצה ממשית.
נגדיר H כשורש של A^*A, אז H מוגדרת חיובית.
נגדיר $U = AH^{-1}$, ואז ברור ש- $A = UH$.
נשאר להראות ש- U אוניטרית:

$$\begin{aligned} U^*U &= \left(AH^{-1}\right)^* \left(AH^{-1}\right) = \left(H^{-1}\right)^* \underbrace{A^*A}_{H^2} H^{-1} \\ &= H^{-1}H^2H^{-1} = I \end{aligned}$$

נראה שהפירוק הנ"ל הוא יחיד:
אם $A = UH$ אז

$$A^*A = (UH)^*(UH) = HU^*UH = H^2$$

והשורש של מטריצה הרמיטית מוגדרת חיובית הוא יחיד.
לכן H מוגדרת באופן יחיד, וגם $U = AH^{-1}$ מוגדרת באופן יחיד. □

למה 2.7.2. $\ker(A) = \ker(A^*A)$.

הוכחה. יהי $v \in \ker A$, אז $A^*Av = A^*0 = 0$ ולכן $\ker A \subseteq \ker A^*A$.
יהי $v \in \ker A^*A$ אז בפרט מתקיים $\langle A^*Av, v\rangle = 0$ וזה שקול ל-

$$0 = \langle A^*Av, v\rangle = v^*A^*Av = (Av)^*\,Av = \langle Av, Av\rangle,$$

וזה אומר ש- $Av = 0$, כך ש- $v \in \ker A$, והראינו $\ker A^*A \subseteq \ker A$.
ביחד זה נותן שוויון $\ker(A) = \ker(A^*A)$. □

משפט 2.7.3. 1. תהי $A \in M_n(\mathbb{C})$ מטריצה לא הפיכה, אז היא ניתנת לפירוק $A = UH$ כאשר H היא הרמיטית מוגדרת אי-שלילית והיא מוגדרת באופן יחיד, ו- U אוניטרית (אבל לא מוגדרת באופן יחיד).

2. תהי $A \in M_n(\mathbb{R})$ מטריצה לא הפיכה, אז היא ניתנת לפירוק $A = US$ כאשר S היא סימטרית ממשית מוגדרת אי-שלילית והיא מוגדרת באופן יחיד, ו- U אורתוגונלית (אבל לא מוגדרת באופן יחיד).

הוכחה. כמו בהוכחה הקודמת, מספיק להוכיח את החלק הראשון. כדי להוכיח את החלק השני צריך רק להחליף את המטריצה המרוכבת במטריצה ממשית.
תהי H שורש של A^*A.
יהיו $\alpha_1, \ldots, \alpha_n$ הערכים העצמיים של A^*A (עם ריבויים) מסודרים כך ש- $\alpha_i > 0$ לכל $1 \leq i \leq m$ ו- $\alpha_{m+1} = \cdots = \alpha_n = 0$.
תהי $\{z_1, \ldots, z_n\}$ קבוצה אורתונורמאלית של וקטורים עצמיים של A^*A בהתאם כך ש- $A^*Az_i = \alpha_i z_i$.
בהתאם מקבלים $Hz_i = \sqrt{\alpha_i} z_i$.
נגדיר $w_i = \frac{1}{\sqrt{\alpha_i}} Az_i$ לכל $1 \leq i \leq m$.
נראה כי $\{w_1, \ldots, w_m\}$ היא קבוצה אורתונורמלית:

$$\langle w_i, w_j \rangle = \left\langle \frac{1}{\sqrt{\alpha_i}} Az_i, \frac{1}{\sqrt{\alpha_j}} Az_j \right\rangle = \frac{1}{\sqrt{\alpha_i}} \cdot \frac{1}{\sqrt{\alpha_j}} \cdot \underbrace{z_j^* A^* A z_i}_{z_j^t \alpha_i z_i} = \delta_{ij} .$$

נשלים את $\{w_1, \ldots, w_m\}$ לבסיס אורתונורמלי $\{w_1, \ldots, w_n\}$.
נכתוב $U = [w_1 \cdots w_n] [z_1 \cdots z_n]^*$. ברור כי U אוניטרית כמכפלה של מטריצות אוניטריות, ומתקיים $U [z_1 \cdots z_n] = [w_1 \cdots w_n]$ או במילים אחרות $Uz_i = w_i$.
נבדוק כי לכל z_i מתקיים $UHz_i = Az_i$:

$$UHz_i = \begin{cases} U\left(\sqrt{\alpha_i} z_i\right), & i \leq m \\ \overrightarrow{0}, & i > m \end{cases} = \begin{cases} \sqrt{\alpha_i} w_i, & i \leq m \\ \overrightarrow{0}, & i > m \end{cases} .$$

מצד שני, לכל $i \leq m$ מקבלים $Az_i = \sqrt{\alpha_i} w_i$ לפי ההגדרה של w_i, ואם $i > m$ אז $Az_i = \overrightarrow{0}$ כי לפי למה 2.7.2, $\ker(A) = \ker(A^*A)$.
אז $Az_i = UHz_i$ לכל וקטור בסיס z_i, וזה שקול ל- $A = UH$.
H מוגדרת באופן יחיד כי נובע כי $A^*A = H^2$. □

הגדרה 2.7.4. תהי $A \in M_n(\mathbb{F})$ כאשר $\mathbb{F} = \mathbb{R}, \mathbb{C}$.
מספר ממשי חיובי $\alpha \in \mathbb{R}^+$ נקרא ערך סינגולרי של A אם קיימים $v, w \in \mathbb{F}^n$ כאשר $\|v\| = \|w\| = 1$ המקיימים

$$Av = \alpha w, \quad A^*w = \alpha v .$$

במקרה כזה הוקטור w נקרא וקטור סינגולרי שמאלי של A, ו- v נקרא וקטור סינגולרי ימני של A.

המשפט הבא מראה איך בונים ערכים סינגולריים ווקטורים סינגולריים למטריצה נתונה, ולכן הוא נקרא משפט הפירוק לערכים סינגולריים או SVD (Singular Value Decomposition).

משפט 2.7.5 (SVD). תהי $A \in M_n(\mathbb{F})$, כאשר $\mathbb{F} = \mathbb{R}, \mathbb{C}$.
אז קיימת מטריצה אלכסונית $D = \text{diag}(\alpha_1, \ldots, \alpha_n)$ כאשר $\alpha_1 \geq \cdots \geq \alpha_n$ יחידה, ומטריצות P, Q אוניטריות (אורתוגונליות במקרה ש- $\mathbb{F} = \mathbb{R}$) כך ש- $A = PDQ$.

בפירוק הזה $\alpha_1, \ldots, \alpha_n$ הם השורשים של הערכים העצמיים של A^*A כתובים בסדר לא עולה, ולכן D מוגדרת באופן יחיד. P היא מטריצת וקטורים סינגולריים שמאליים של A, ו- Q^* מטריצת וקטורים סינגולריים ימניים של A (לא מוגדרות באופן יחיד בדרך כלל).

הוכחה. כמו בהוכחות של משפטים 2.7.1 ו- 2.7.3, נוכיח למטריצה מרוכבת. המקרה הממשי דומה.
לפי משפטים 2.7.1 ו- 2.7.3 יש פירוק $A = UH$ כאשר $H = \sqrt{A^*A}$ הרמיטית מוגדרת אי-שלילית, ו- U אוניטרית.
A^*A היא הרמיטית, מוגדרת אי-שלילית ולכן היא דומה אוניטרית (אורתוגונלית) למטריצה אלכסונית, זאת אומרת $A^*A = V^* \operatorname{diag}(\alpha_1^2, \dots, \alpha_n^2)V$ כאשר V אוניטרית, ו- $\alpha_1^2, \dots, \alpha_n^2$ הם ע"ע של A^*A כתובים בסדר לא עולה.
אז $H = V^* \operatorname{diag}(\alpha_1, \dots, \alpha_n)V$ ו- $A = UH = UV^*DV = PDQ$ כאשר $Q = V$, $P =$, $D = \operatorname{diag}(\alpha_1, \dots, \alpha_n)$, UV^*, אוניטרית כמכפלה של מטריצות אוניטריות.
לפי השוויון הזה מקבלים $AQ^* = PD$.
תהיינה $P = [p_1, \dots, p_n]$ ו- $Q^* = [q_1, \dots, q_n]$, אז $AQ^*e_i = Aq_i = PDe_i = P\alpha_i e_i = \alpha_i p_i$.
כמו כן, $A^* = Q^*DP^* \iff A^*P = Q^*D$, כך ש- $A^*Pe_i = A^*p_i = Q^*De_i = Q^*\alpha_i e_i = \alpha_i q_i$.
לכן הוקטורים $q_1, \dots, q_n$ הם וקטורים סינגולרים ימניים של A, ו- $p_1, \dots, p_n$ הם וקטורים סינגולריים שמאליים של A בהתאם. □

הערה 2.7.6. מבחינה גיאומטרית, מעל הממשיים מטריצות אורתוגונליות הן מטריצות סיבוב ושיקוף. לכן משפט SVD אומר שפעולה של כל מטריצה על מרחב אוקלידי היא סיבוב ו/או שיקוף של מערכת אורתונורמלית בעזרת מטריצה Q, אחר כך מתיחה או כיווץ (תלוי אם המספר המתאים ב- D הוא גדול או קטן מ- 1) של כל קואורדינטה חדשה (פעולה של האלכסון האי-שלילי של D), ולבסוף עוד סיבוב ו/או שיקוף.

מסקנה 2.7.7. לכל $A \in M_n(\mathbb{F})$ מתקיים $AA^* \sim A^*A$ אוניטרית.
בפרט יש להם את אותם ערכים עצמיים עם אותם ריבויים.

הוכחה. $A = PDQ$, לכן $A^*A = (PDQ)^* (PDQ) = Q^*D^2Q$.
כמו כן $AA^* = (PDQ)(PDQ)^* = PD^2P^*$.
אז $D^2 = QA^*AQ^*$ ולכן

$$AA^* = PQA^*AQ^*P^* = (PQ)A^*A(PQ)^*$$

מכפלה של מטריצות אוניטריות היא מטריצה אוניטרית, ולכן קיבלנו ש- A^*A ו- AA^* דומות אוניטרית. □

הערה 2.7.8. בדרך כלל המטריצות AB ו- BA הן דומות (לא אוניטרית) אם לפחות אחת מהן הפיכה, ויכולות להיות לא דומות אם שתיהן לא הפיכות.
לפי מסקנה 2.7.7, יש דמיון אוניטרי $AA^* \sim A^*A$ לכל A.

הערה 2.7.9. לפי ההוכחה של מסקנה 2.7.7 מקבלים ש- Q היא מטריצת וקטורים עצמיים של A^*A, ו- P^* היא מטריצת וקטורים עצמיים של AA^*.
אז $A = PDQ$, כאשר:

1. המטריצה P היא "כוכב" של וקטורים עצמיים אורתונורמליים של AA^*.
2. D היא מטריצה אלכסונית של שורשים ריבועיים של הערכים העצמיים של A^*A, כתובים בסדר לא עולה.
3. Q היא מטריצה של וקטורים עצמיים אורתונורמליים של A^*A.

משפט 2.7.10 (SVD כללי). תהי $A \in M_{m\times n}(\mathbb{R})$ אז קיימות מטריצות אורתוגונליות $Q \in M_n(\mathbb{R})$ ו- $P \in M_m(\mathbb{R})$, ומטריצה אלכסונית $D \in M_{m\times n}(\mathbb{R})$ עם ערכים לא שליליים באלכסון שלה כך ש- $A = PDQ$.
כאן Q היא מטריצת וקטורים עצמיים של A^tA ו- P היא מטריצת וקטורים עצמיים של AA^t.

הערה 2.7.11. אם A מלבנית אזי ריבוי של 0 כערך עצמי של AA^t ושל A^tA הוא שונה.
לכל הערכים העצמיים האחרים הריבוי ב- AA^t שווה לריבוי ב- A^tA.

עוד פירוק שימושי של מטריצות ממשיות:

משפט 2.7.12. כל מטריצה $A \in M_n(\mathbb{F})$ הפיכה (כאשר $\mathbb{F} = \mathbb{C}, \mathbb{R}$) ניתנת לפירוק כ- $A = UD$,
כאשר U אוניטרית (אורתוגונלית אם A ממשית) ו- D משולשית עליונה.
הפירוק הזה יחיד עד כדי מכפלה של U במטריצה אלכסונית אוניטרית בצד ימין ומכפלה של D בהפכית שלה בצד שמאל.

הוכחה. ההוכחה היא פשוט "הבנת הנקרא" של תהליך גרם-שמידט:
יהיו

$$a_1 = \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, \ldots, a_n = \begin{pmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{pmatrix}$$

וקטורי עמודות של A.
אז A הפיכה אם ורק אם הקבוצה $\{a_1, \ldots, a_n\}$ היא בסיס של $\mathbb{F}^n$.
לפי משפט גרם – שמידט קיים בסיס אורתונורמאלי

$$\left\{ u_1 = \begin{pmatrix} \mu_{11} \\ \vdots \\ \mu_{n1} \end{pmatrix}, \ldots, u_n = \begin{pmatrix} \mu_{1n} \\ \vdots \\ \mu_{nn} \end{pmatrix} \right\}$$

מוגדר לפי תהליך גרם-שמידט המקיים לכל $\operatorname{span}\{a_1, \ldots, a_i\} = \operatorname{span}\{u_1, \ldots, u_i\}$ לכל $1 \le i \le n$.
הבסיס הזה מוגדר באופן יחיד עד כדי מכפלה של כל u_i ב- $\pm 1\ \alpha_i$.
לאחר בחירה של בסיס $\{u_1, \ldots, u_n\}$ קיימים $\{\beta_{ij}\}_{1 \le i \le j \le n}$ מוגדרים באופן יחיד, כך ש- $a_j = \sum_{i=1}^{j} \beta_{ij} u_i$,
וזה שקול ל-

$$\begin{pmatrix} \alpha_{1j} \\ \vdots \\ \alpha_{nj} \end{pmatrix} = \sum_{i=1}^{j} \beta_{ij} \begin{pmatrix} \mu_{1i} \\ \vdots \\ \mu_{ni} \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{j} \beta_{ij} \mu_{1i} \\ \vdots \\ \sum_{i=1}^{j} \beta_{ij} \mu_{ni} \end{pmatrix}$$

או במילים אחרות

$$\alpha_{sj} = \sum_{i=1}^{j} \beta_{ij} \mu_{si} = \sum_{i=1}^{j} \mu_{si} \beta_{ij}. \tag{2.5}$$

תהיינה $U = [u_1, \ldots, u_n]$ ו-

$$D = \begin{pmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1n} \\ 0 & \beta_{22} & \cdots & \beta_{2n} \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & \beta_{nn} \end{pmatrix}$$

מטריצה משולשית עליונה.
אז

$$(UD)_{sj} = \sum_{i=1}^{j} \mu_{si} \beta_{ij} = \alpha_{sj},$$

וכשמשווים את הביטוי הזה למה שקיבלנו ב- (2.5) ומקבלים $A = UD$.

נשים לב כי

$$UD = (U \cdot \mathrm{diag}(\alpha_1, \dots, \alpha_n)) \left(\mathrm{diag}(\alpha_1^{-1}, \dots, \alpha_n^{-1}) \cdot D\right)$$

ו- $\mathrm{diag}(\alpha_1, \dots, \alpha_n)$ היא גם אלכסונית וגם אורתוגונאלית. מכפלה של משולשית עליונה באלכסונית היא תמיד משולשית עליונה, ומכפלה של אורתוגונלית באורתוגונלית היא אורתוגונאלית.

שימו לב שמכפלה של מטריצה במטריצה אלכסונית משמאל היא בדיוק מכפלה של העמודה u_i בקבוע α_i. $\square$

הערה 2.7.13. אם $A \in M_{n\times n}(\mathbb{F})$ מטריצה לא הפיכה, היא גם ניתנת לפירוק כ- $A = UD$ כאשר U אורתוגונלית ו- D משולשית עליונה, אבל הפירוק הזה רחוק מלהיות יחיד עד מכפלה במטריצה אורתוגונלית אלכסונית.

יש עוד הרבה פירוקים שמשמשים ביישומים שונים.

בפרק הבא נראה שימושים של SVD.

2.8 שימושים של SVD ו- PCA

2.8.1 הקדמה

נראה כאן איך התיאוריה שלמדנו יכולה להיות שימושית לבעיות מעשיות.

נתחיל מלמות קטנות שנשתמש בהן בהמשך.

למה 2.8.1. תהי $U \in M_n(\mathbb{R})$ אורתוגונלית. אז לכל וקטור $v \in \mathbb{R}^n$ מתקיים $\|Uv\| = \|v\|$.

הוכחה.

$$\|Uv\|^2 = \langle Uv, Uv\rangle = v^t \underbrace{U^tU}_{I} v = v^t v = \langle v, v\rangle = \|v\|^2$$

ולכן $\|Uv\| = \|v\|$. $\square$

למה 2.8.2. תהי $A \in M_{n\times k}(\mathbb{R})$ מטריצה מדרגה k (ברור כי $k \leq n$), אז $A^tA \in M_k(\mathbb{R})$ היא מטריצה הפיכה.

הוכחה. למטריצה A נוסיף $n-k$ עמודות של 0 ונקבל

$$\hat{A} = \begin{pmatrix} \underbrace{A}_{k\text{עמודות}} & \underbrace{0}_{n-k\text{עמודות}} \end{pmatrix} \in M_n(\mathbb{R}).$$

זו מטריצה ריבועית מדרגה k כך ש $\dim\ker \hat{A} = n-k$.

נתבונן במטריצה $\hat{A}^t\hat{A}$: מצד אחד

$$\hat{A}^t\hat{A} = \begin{pmatrix} \underbrace{A^tA}_{k\times k} & \underbrace{0}_{k\times(n-k)} \\ \underbrace{0}_{(n-k)\times k} & \underbrace{0}_{(n-k)\times(n-k)} \end{pmatrix},$$

ומצד שני $\ker \hat{A}^t\hat{A} = \ker \hat{A}$, כך ש- $\operatorname{rank} \hat{A}^t\hat{A} = \operatorname{rank} \hat{A} = k$, וזה שקול לכך ש- A^tA הפיכה. $\square$

2.8.2 בעיית הריבועים הפחותים

נציג את בעיית הריבועים הפחותים – Least Square Problem – LSP:

בעיה 2.8.3. נתונים k וקטורים בת"ל $\{a_1, \ldots, a_k\}$ ב- $\mathbb{R}^n$ ועוד וקטור $b \in \mathbb{R}^n$.
רוצים למצוא $v \in \operatorname{span}\{a_1, \ldots, a_k\}$, כך ש- $\|v-b\| = \min \|u-b\|$
כאשר $u \in \operatorname{span}\{a_1, \ldots, a_k\}$.

אם נכתוב

$$a_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}, \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

אז לכל $u \in \operatorname{span}\{a_1, \ldots, a_k\}$ מתקיים $u = \sum_{j=1}^k \alpha_j a_j$, ו-

$$\|u-b\|^2 = \sum_{i=1}^n \left(\sum_{j=1}^k \alpha_j a_{ij} - b_i\right)^2 \tag{2.6}$$

ואנחנו מחפשים $\alpha_1,\dots,\alpha_k$ כך ש- (2.6) מינימלי, לכן הבעיה נקראת "בעיית הריבועים הפחותים" (באנגלית LSP).

התשובה כבר ידועה לנו: צריך למצוא v שהוא היטל אורתוגונלי של b על $\operatorname{span}\{a_1,\dots,a_k\}$.
v הוא היטל אורתוגונלי אם ורק אם $a_j \perp (v-b)$ לכל $1 \le j \le k$, וזה קורה אם ורק אם $a_j^t \cdot (v-b) = 0$ לכל j.

יהי $A=[a_1,\dots,a_k]$, אז $v=[a_1,\dots,a_k]\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}$, ומחפשים $x_1,\dots,x_k$ המקיימים

$$\begin{aligned} 0 &= A^t\left(A\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} - b\right) \\ \iff A^tA\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} - A^tb &= 0 \\ \iff \underbrace{A^tA}_{\text{הפיכה } k\times k}\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} &= A^tb \end{aligned}$$

ולכן תשובה תיאורטית שלמה היא

$$x=\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \left(A^tA\right)^{-1}A^tb$$

שימו לב: A היא מטריצה $n\times k$ כך שאת $\left(A^tA\right)^{-1}$ בשום פנים ואופן אי-אפשר לפתוח ל- $A^{-1}\left(A^t\right)^{-1}$!!!

תשובה תיאורטית זה טוב, אבל בחישובים הדיוק של A^tA כאשר $n,k \gg 0$ יכול להיות מאוד נמוך.
לכן משתמשים ב- SVD.

הערה 2.8.4. תיאורטית צריך לחשב את A^tA כדי לדעת מהו פירוק SVD של A, אבל בפועל יש דרכים אחרות לחשב אותו (בדיוק מאותה סיבה של איבוד הדיוק).

נתחיל בחישוב: נכתוב $A=U_{n\times n}D_{n\times k}V_{k\times k}$, ומחפשים $\|UDVx-b\|$ מינימלי.

$$\begin{aligned} \|UDVx-b\| &= \|UDVx-UU^tb\| \\ &= \|U(DVx-U^tb)\| = \|DVx-U^tb\| \end{aligned}$$

יהיו $c=U^tb=\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ ו- $Vx=y=\begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix}$, ואז צריך למצוא $\|Dy-c\|$ מינימלי.

נכתוב את D

$$D = \begin{pmatrix} \underbrace{\operatorname{diag}(d_1, \ldots, d_k)}_{k \times k} \\ \underbrace{0}_{(n-k) \times k} \end{pmatrix}$$

כאשר $d_1 \geq \cdots \geq d_k$.
אז

$$Dy = \begin{pmatrix} d_1 y_1 \\ \vdots \\ d_k y_k \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

ו-

$$\begin{pmatrix} d_1 y_1 \\ \vdots \\ d_k y_k \\ 0 \\ \vdots \\ 0 \end{pmatrix} - \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} d_1 y_1 - c_1 \\ \vdots \\ d_k y_k - c_k \\ -c_{k+1} \\ \vdots \\ -c_n \end{pmatrix} \tag{2.7}$$

והנורמה של (2.7) מינימלית אם $d_i y_i - c_i = 0$ כלומר $y_i = \frac{c_i}{d_i}$ לכל $1 \leq i \leq k$.
אנחנו גם רואים כי LS הוא $\sum_{j=k+1}^{n} c_j^2$.
נגדיר "קוואזי-הפכית" של D (ז"א הפכית של D בצמצום ל- k השורות הראשונות) :

$$\hat{D} = \begin{pmatrix} \operatorname{diag}\left(\frac{1}{d_1}, \ldots, \frac{1}{d_k}\right) & \underbrace{0}_{k \times (n-k)} \end{pmatrix}$$

אז התשובה היא $y = \hat{D}c$ ונזכיר ש- $c = U^t b$ ו- $y = Vx$, כלומר $Vx = \hat{D}U^t b$.
מכאן ש-

$$\boxed{x = V^t \hat{D} U^t b}$$

ו- $\|x - b\|^2 = \sum_{j=k+1}^{n} c_j^2$ כאשר $c = U^t b$.

2.8.3 דחיסת מידע ובניית פילטרים

- תהי $A = UDV$ כאשר $D = \operatorname{diag}(\alpha_1, \ldots, \alpha_n)$ ו- $\alpha_1 \geq \cdots \geq \alpha_n \geq 0$.
- כדי לדחוס מידע אפשר להחליף כל $\alpha_i < \delta$ ב- 0.
- מקבלים מטריצה הרבה יותר פשוטה אבל לא מאבדים דיוק (עד סדר δ).

על אותו עקרון בונים כל מיני פילטרים: בגלל "הרעש" 0 הופך לערך שונה מ- 0 אבל קטן מ- δ בערך מוחלט, ובעזרת

הפיכה בחזרה ל- 0 מקבלים את הדבר המקורי.

2.8.4 Principal Component Analysis (PCA)

- נתונים מספרים בצורה $A = \{a_1, \ldots, a_m\}$.
- $\mu_A = \frac{1}{m}\sum_{i=1}^m a_m$ הוא הממוצע של הקבוצה A, ו- $\text{Var}_A = \frac{1}{m}\sum_{i=1}^m (a_m - \mu_A)^2$ הוא השונות.
- השונות מודדת כמה (בממוצע) הנתונים שונים מהממוצע.
- אם יש שני נתונים מספריים על אותה אוכלוסייה (סידרת ניסיונות), למשל לקבוצה של m אנשים מודדים גובה ומשקל, אז יש נתונים $A = \{a_1, \ldots, a_m\}$ ו- $B = \{b_1, \ldots, b_m\}$ ומגדירים שונות משותפת (Covariance)

$$\text{Cov}(A, B) = \frac{1}{m}\sum_{i=1}^m (a_i - \mu_A)(b_i - \mu_B).$$

- השונות המשותפת היא חיובית אם הנתונים של A ו- B גדלים וקטנים ביחד, ושלילית אם כאשר אחד מהם גדל השני קטן.

הערה 2.8.5. לאחר נרמול של השונות המשותפת אפשר לקבל עד כמה A ו-B קשורים ליניארית אבל לא נכנס לזה. בפרט אם $\text{Cov}(A, B) = 0$ זה אומר שהמשתנים לא תלויים ליניארית.

נניח שיש לנו נתונים של מחקר סטטיסטי – n נסיונות ולכל נסיון יש k פרמטרים מספריים.

אנחנו יכולים לכתוב כל ניסוי כוקטור k-מימדי $x_i = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ki} \end{pmatrix}$.

אפשר לחשב ממוצע ושונות לכל אחד מהנתונים $A_j = \{a_{j1}, \ldots, a_{jn}\}$, ושונות משותפת לכל זוג (A_i, A_j).

נחשב וקטור ממוצע

$$\mu = \frac{1}{n}\begin{pmatrix} \sum_{i=1}^n a_{1i} \\ \vdots \\ \sum_{i=1}^n a_{ki} \end{pmatrix}$$

ונגדיר $y_i = x_i - \mu$.

מקבלים מטריצה $A = [y_1 \cdots y_n]$ של נתונים שהממוצע של כל אחד מהם הוא 0.

נגדיר מטריצה $S = \frac{1}{n}AA^t$.

זאת מטריצת שונות משותפת, ז"א

$$(S)_{ii} = \frac{1}{n}\sum_{i=1}^n (a_i - \mu_A)^2 = \text{Var}_{A_i}$$

וגם

$$(S)_{ij} = (S)_{ji} = \frac{1}{n}\sum_{l=1}^n (a_{il} - \mu_{A_i})(a_{jl} - \mu_{A_j}) = \text{Cov}(A_i, A_j)$$

ז"א על האלכסון במקום ה- i נמצא Var_{A_i} ובמקום ה- (i,j) (כאשר $i \neq j$) נמצא $\text{Cov}(A_i, A_j)$.

בפרט $\text{trace}\, S = \sum_{i=1}^k \text{Var}_{A_i}$ היא השונות הכוללת.

מהצד השני, בגלל ש- S סימטרית מוגדרת אי-שלילית, היא דומה אורתוגונלית למטריצה אלכסונית $P^tSP = \text{diag}(\lambda_1, \ldots, \lambda_k)$ כאשר $\lambda_1 \geq \cdots \geq \lambda_k \geq 0$ ו- $P = [p_1, \ldots, p_k]$ כאשר $\{p_1, \ldots, p_k\}$ הם וקטורים עצמיים

אורתונורמלים של S.

מקבלים משתנים חדשים שהם בסיס אורתונורמלי ובקואורדינטות האלה הנתונים שלנו נמצאים סביב אליפסויד עם צירים $\pm\sqrt{\lambda_1}p_1, \dots, \pm\sqrt{\lambda_k}p_k$.

נזכיר כי $\text{trace}\, S = \lambda_1 + \cdots + \lambda_k$.

הנתונים שלנו משתנים לפי צירים $p_1, \dots, p_k$, כאשר השינויים הכי משמעותיים קורים לפי ציר p_1 שהוא עונה על חלק $\frac{\lambda_1}{\text{trace}\, S}$ של השונות הכוללת, לאחר מכן לפי ציר p_2 שעונה על החלק ה- $\frac{\lambda_2}{\text{trace}\, S}$ וכך הלאה.

הוקטורים $p_1, \dots, p_k$ נקראים רכיבים עיקריים (Principal Components) של הנתונים שלנו.

ברור כי p_1 הוא החשוב ביותר, p_2 הכי חשוב בין כל השאר וכו'.

השימושים ב- PCA הם רבים ומגוונים, אבל הרעיון הכללי הוא ירידה של הפרמטרים שצריך לחשב.

במקרים רבים יש לנו n פרמטרים לנתונים שלנו, אבל לאחר חישוב המטריצה D מתברר למשל ש- $\lambda_1 + \cdots + \lambda_i = 0.98\, \text{trace}\, S$.

ז"א שלאחר שינוי המשתנים רק $p_1, \dots, p_i$ אחראים על (כמעט) כל השונות של הנתונים ומספיק להתבונן רק בהם כדי לערוך אנליזה של הנתונים.

זה יכול להוריד משמעותית את מספר הפרמטרים בניתוח הנתונים.

נסתכל בתמונה שבאיור 2.1:

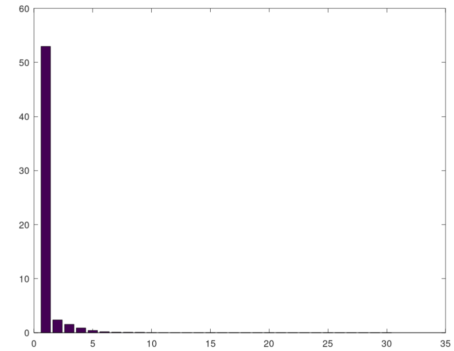
איור 2.1: תמונה של 512×512 פיקסלים

נסתכל על הערכים העצמיים הסינגולריים של המטריצה S:

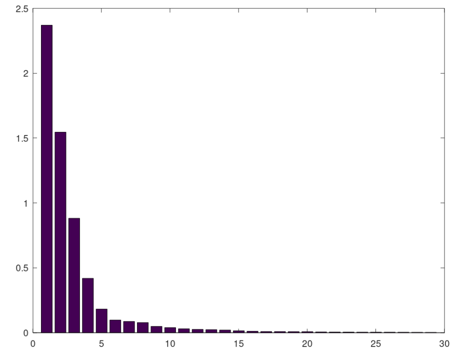
באיור 2.2 אפשר לראות שהערכים העצמיים יורדים מהר מאד, אבל לא ברור כמה מהם נחוצים כדי שהתמונה תהיה "דומה למקור".

התמונות באיור 2.3 מראות מספרים שונים של רכיבים עיקריים (PC) של התמונה הקודמת:

דוגמא אחרונה: זיהוי פנים.



(א) 30 הערכים העצמיים הראשונים



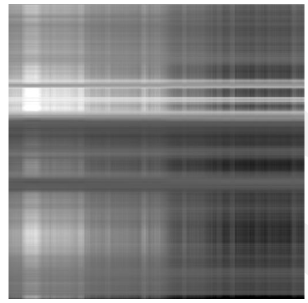
(ב) הערכים העצמיים 2 – 30

איור 2.2: ערכים עצמיים סינגולריים בסדר יורד

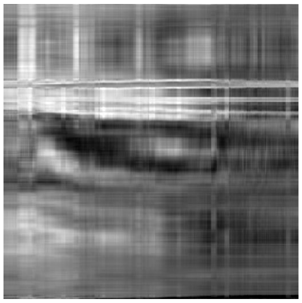
- כל צילום שחור-לבן הוא טבלה של פיקסלים שחורים ולבנים.
- ניתן לפיקסל שחור ערך 0.0, לפיקסל לבן ערך 1.0 וכל האפורים מקבלים ערכים בינהם.
- אז כל תמונה היא טבלה של מספרים בין 0 ל- 1 שאנחנו יכולים לכתוב כוקטור (עמודה לאחר עמודה) בעל אורך k (גדול מאד).
- נצלם מספר גדול של פנים ונקבל n וקטורים. נבנה מהם מטריצה, נקבל מטריצה S ונחשב מטריצה D בהתאם.
- מקבלים רכיבים עיקרים שמהם באופן מפתיע (או שלא) רק ה- 100 ראשונים עונים על רוב ההתפלגויות של שוני הפנים.
- אם יש אנשים $Q_1, \ldots, Q_m$ שאנחנו רוצים לזהות בכניסה, אז משאירים את 100 הרכיבים הראשונים של כל אחד מהקבוצה במערכת, ז"א הוקטורים

$$.Q_1 = (a_{11}, \ldots, a_{1,100}), \ldots, Q_m = (a_{m1}, \ldots, a_{m,100})$$

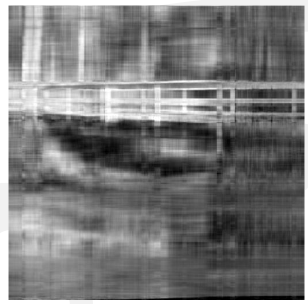
- לכל אדם שנכנס עושים צילום שחור-לבן, ולתמונה עושים שינוי קואורדינטות ל- $p_1, \ldots, p_k$ (יש לנו כבר מטריצת מעבר לקואורדינטות $p_1, \ldots, p_k$).
- משווים את 100 המקדמים הראשונים לכל אחד מ- $Q_1 \ldots, Q_m =$.
- אם מקבלים קואורדינטות שוות לאחד מהם (או קרובות, כי כל העבודה נעשית עם קרובים) – קיבלנו אחד מ"האורחים הרצויים".



(א) רכיב עיקרי אחד



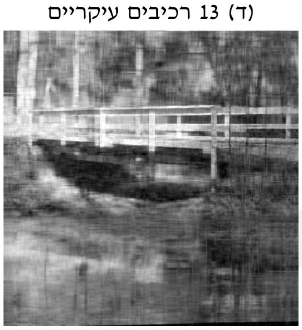
(ב) 5 רכיבים עיקריים



(ג) 9 רכיבים עיקריים

(ד) 13 רכיבים עיקריים

(ה) 17 רכיבים עיקריים



(ו) 21 רכיבים עיקריים

(ז) 25 רכיבים עיקריים

(ח) 29 רכיבים עיקריים

איור 2.3: השוואה בין מספרים שונים של רכיבים עיקריים בתמונה

2.9 נורמה של מטריצה ורדיוס ספקטראלי של מטריצה

הגדרה 2.9.1. תהי $A \in M_{n\times m}(\mathbb{R})$. הנורמה של A המושרית על ידי $\|.\|$ (הנורמה הסטנדרטית ב- $\mathbb{R}^n$) מוגדרת על-ידי

$$\|A\| = \sup_{\|v\|=1} \|Av\| = \sup_{v\neq 0} \frac{\|Av\|}{\|v\|}.$$

אפשר להסתכל על A כהעתקה ליניארית, והנורמה מראה לתוך כדור מאיזה רדיוס עובר כדור היחידה ב- $\mathbb{R}^n$. בגלל שכדור היחידה הוא קבוצה סגורה וחסומה, אז אפשר לכתוב $\|A\| = \max_{\|v\|=1} \|Av\|$.

למה 2.9.2. הנורמה שהגדרנו מקיימת את התכונות של נורמה:

1. לכל $A \in M_{n\times m}(\mathbb{R})$ ו- $\alpha \in \mathbb{R}$ מתקיים $\|\alpha A\| = |\alpha| \cdot \|A\|$;
2. לכל $A \in M_{n\times m}(\mathbb{R})$ מתקיים $\|A\| \geq 0$, ו- $\|A\| = 0$ אם ורק אם $A = 0$;
3. לכל $A, B \in M_{n\times m}(\mathbb{R})$ מתקיים $\|A+B\| \leq \|A\| + \|B\|$ (אי-שוויון המשולש);
4. לכל $A, B \in M_{n\times m}(\mathbb{R})$ מתקיים $\|AB\| \leq \|A\| \cdot \|B\|$.

הוכחה.
1. לכל $v \in \mathbb{R}^n$ מתקיים $(\alpha A)v = \alpha(Av)$ ולכן $\|\alpha Av\| = |\alpha| \cdot \|Av\|$.
מכאן לפי ההגדרה מקבלים
$$\|\alpha A\| = |\alpha| \cdot \|A\|.$$
2. תהי $A \neq 0$ אז קיים $v \in \mathbb{R}^n$ כך ש- $Av \neq 0$, וזה שקול לפי ההגדרה ל-$\|Av\| > 0$ ולכן $\|A\| > 0$.
3. לכל $v \in \mathbb{R}^n$ מתקיים
$$\|(A+B)v\| = \|Av + Bv\| \leq \|Av\| + \|Bv\|$$
לכן גם
$$\begin{aligned}\|A+B\| &= \max_{\|v\|=1} \|(A+B)v\| \leq \max_{\|v\|=1} (\|Av\| + \|Bv\|) \\ &\leq \max_{\|v\|=1} \|Av\| + \max_{\|v\|=1} \|Bv\| = \|A\| + \|B\|\end{aligned}$$
4. יהי $\|B\| = \beta$. אז לכל $v : \|v\| = 1$ מתקיים $Bv = \gamma w$ כאשר $0 \leq \gamma \leq \beta$ ו- $\|w\| = 1$.
אז
$$\begin{aligned}\|AB\| &= \max_{\|v\|=1} \|ABv\| = \max_{\|v\|=1} \|A(Bv)\| \\ &= \max_{\|v\|=1} \|A(\gamma w)\| = \max_{\|v\|=1} \|\gamma Aw\| \\ &\leq \max_{\|v\|=1} \gamma \|Aw\| \leq \beta \max_{\|w\|=1} \|Aw\| = \|A\| \cdot \|B\|\end{aligned}$$

□

הערה 2.9.3. תכונה 4 קשורה לעובדה ש- $M_{n\times m}(\mathbb{R})$ הוא אלגברה ולא רק מרחב וקטורי.

טענה 2.9.4 תהי $A \in M_n(\mathbb{R})$, ויהי $A = PDQ$ פרוק SVD של A כאשר $D = \text{diag}(\lambda_1, \dots, \lambda_n)$ ו- $\lambda_1 \geq \dots \geq \lambda_n$.
אז
$$\|A\| = \lambda_1.$$

הוכחה. יהי $v \in \mathbb{R}^n$ עם $\|v\| = 1$, אז לפי למה מהפרק הקודם $w = Qv$ מקיים $\|w\| = 1$, או במילים אחרות

$$w = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

כאשר $\sum_{i=1}^n a_i^2 = 1$.
נחשב:

$$\begin{aligned} \langle Av, Av \rangle &= v^t A^t A v = v^t (PDQ)^t PDQv = v^t Q^t D^2 Q v \\ &= (a_1, \dots, a_n) \begin{pmatrix} \lambda_1^2 a_1 \\ \vdots \\ \lambda_n^2 a_n \end{pmatrix} = \sum_{i=1}^n \lambda_i^2 a_i^2 \leq \lambda_1^2 \sum_{i=1}^n a_i^2 = \lambda_1^2 \end{aligned}$$

כך ש- $\|Av\| \leq \lambda_1$ לכל $\|v\| = 1 : v$.
לכן גם $\|A\| = \sup_{\|v\|=1} \|Av\| \leq \lambda_1$.
כעת נכתוב $w = Q^t e_1$, אז $\|w\| = \|Q^t e_1\| = \|e_1\| = 1$.
נחשב את $\|Aw\|$:
$$\|Aw\|^2 = w^t Q^t D^2 Q w = e_1^t D^2 e_1 = \lambda_1^2$$

כך ש- $\|Aw\| = \lambda_1$, ולכן $\|A\| \geq \lambda_1$.
ביחד זה נותן $\|A\| = \lambda_1$.
□

הגדרה 2.9.5 תהי $A \in M_n(\mathbb{R})$. יהיו $\alpha_1, \dots \alpha_k$ ערכים עצמיים של A (כמטריצה מרוכבת).
הרדיוס הספקטרלי של A הוא
$$\rho(A) = \max\{|\alpha_1|, \dots, |\alpha_k|\}.$$

בגלל שתמיד אפשר למצוא ווקטור עצמי נורמאלי (שהנורמה שלו שווה ל- 1), יהי v ווקטור עצמי מנורמל ששייך לערך עצמי עם ערך מוחלט מקסימלי.
אז נקבל $\|Av\|^2 = (\rho(A))^2$ כך ש- $\rho(A) \leq \|A\|$.
יתרה מזו, בדיוק באותו אופן נקבל

טענה 2.9.6 תהי $A \in M_n(\mathbb{R})$. אזי לכל $k \in \mathbb{N}$ מתקיים $\rho(A) \leq \left\|A^k\right\|^{1/k}$.

הוכחה. יהיו $\alpha_1, \dots, \alpha_m$ ערכים עצמיים של A ו- $v_1, \dots, v_m$ וקטורים עצמיים (מנורמלים) מתאימים.
אז $\alpha_1^k, \dots, \alpha_m^k$ הם ערכים עצמיים של A^k עם אותם וקטורים עצמיים.
בפרט $(\rho(A))^k = \rho(A^k) \leq \|A^k\|$, ומכאן נובע $\rho(A) \leq \|A^k\|^{1/k}$.
□

הרדיוס הספקטרלי יכול להיות הרבה יותר קטן מהנורמה.

דוגמא 2.9.7. נתבונן ב- $A = \begin{pmatrix} 0 & a \\ a^{-1} & 0 \end{pmatrix}$, כאשר $a > 1$.
מקבלים $\Delta_A(x) = x^2 - 1 = (x-1)(x+1)$, ולכן $\rho(A) = 1$.
כמו כן, $A \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} av_2 \\ a^{-1}v_1 \end{pmatrix}$, ולכן

$$\|A\| = \sup_{0 \le r \le 1} \sqrt{a^2 r + a^{-2}(1-r)} = a$$

כך ש- $\|A\|$ יכולה להיות הרבה יותר גדולה מ- $\rho(A)$.
לפי טענה 2.9.6 מקבלים

מסקנה 2.9.8. $\|A\| = \sqrt{\rho\left(A^t A\right)}$.

קשר יותר מעניין ניתן על ידי המשפט הבא:

משפט 2.9.9 (גלפנד)**.** תהי $A \in M_n(\mathbb{R})$. אז

$$\lim_{k \to \infty} \|A^k\|^{1/k} = \rho(A) \, .$$

הוכחת המשפט הקודם מבוססת על המשפט:

משפט 2.9.10. תהי $A \in M_n(\mathbb{R})$ עם רדיוס ספקטראלי $\rho(A)$. אז $\lim_{k\to\infty} A^k = 0$ אם ורק אם $\rho(A) < 1$.
אם $\rho(A) > 1$ אז $\lim_{k\to\infty} A^k = \infty$.

לא נוכיח כאן את המשפטים האלה, כי ההוכחות שלהם דורשות ידע של צורת ז'ורדן והגדרת טופולוגיה על המרחב $M_n(\mathbb{R})$.

בדוגמא הקודמת שראינו $A = \begin{pmatrix} 0 & a \\ a^{-1} & 0 \end{pmatrix}$ מקבלים $A^{2k} = I_2$ ו- $A^{2k+1} = A$.
כאן $\rho(A) = 1$ והגבול $\lim_{k\to\infty} A^k$ לא קיים.

פרק 3

מבוא לתורת החבורות

3.1 חבורות ותת חבורות

3.1.1 הגדרות ודוגמאות

הגדרה 3.1.1. קבוצה לא ריקה G יחד עם פעולת "מכפלה" $\cdot : G \times G \to G$ נקראת חבורה אם פעולת המכפלה מקיימת את האקסיומות הבאות:

1. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ לכל $a, b, c \in G$ (קיבוציות, או אסוציאטיביות).
2. קיים $e \in G$ שנקרא "יחידה" המקיים $ae = ea = a$ לכל $a \in G$ (קיום יחידה).
3. לכל $a \in G$ קיים $b \in G$ המקיים $ab = ba = e$ (קיום הפכי).

דוגמא 3.1.2.
1. $G = \{e\}$.
2. $G = \{1, -1\}$ עם פעולת הכפל.
3. $G = \mathbb{Z}$ עם פעולת החיבור.
4. חבורת קליין (כסימטריות של מלבן).
5. S_n עם הרכבות של תמורות

- תמורה היא העתקה חד-חד-ערכית ועל $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$.
- כותבים תמורה בצורה $\sigma = \begin{pmatrix} 1 & \cdots & n \\ a_1 & \cdots & a_n \end{pmatrix}$ או $\sigma = (a_1, \ldots, a_n)$ כאשר $\sigma(i) = a_i$.
- הרכבה של תמורות מוגדרת על ידי $\sigma\tau(i) = \sigma(\tau(i))$.
לדוגמא אם

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

אז $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ ו- $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

הגדרה 3.1.3. קבוצת כל התמורות על $\{1, \ldots, n\}$ עם פעולת ההרכבה נקראת החבורה הסימטרית מסדר n. מסמנים אותה ב- S_n.

הערה 3.1.4. בחבורה הסימטרית לא מתקיים חוק החילוף, כי כמו שראינו בדוגמא הקודמת $\sigma\tau \neq \tau\sigma$. כלומר S_n היא חבורה לא אבלית לכל $n \geq 3$.

הגדרה 3.1.5. תהי $(G, \cdot)$ חבורה. אם G סופית כקבוצה, אז $(G, \cdot)$ נקראת חבורה סופית. אחרת היא נקראת חבורה אינסופית.

הגדרה 3.1.6. מספר האיברים ב- G נקרא סדר החבורה ומסומן $o(G)$.

הגדרה 3.1.7. תהי $(G, \cdot)$ חבורה. אם לכל $a, b \in G$ מתקיים $a \cdot b = b \cdot a$ (חילופיות של המכפלה) אז G נקראת אבלית[8] או קומוטטיבית.

---

[8] Niels Henrik Abel 1802 – 1829

למה 3.1.8. תהי $(G,\cdot)$ חבורה. אז:

1. איבר היחידה הוא יחיד בחבורה.
2. לכל $a \in G$ ההפכי הוא יחיד. נסמן אותו ב- a^{-1}.
3. לכל $a,b,c \in G$ מתקיים $ab = ac \Leftarrow b = c$ וגם $ab = cb \Leftarrow a = c$.
4. אם $a,b \in G$ מקיימים $ab = e$ אז $b = a^{-1}$.
אם $a,b \in G$ מקיימים $ba = e$ אז $b = a^{-1}$.
ז.א. הפכי מצד אחד הוא ההפכי.
5. לכל $a,b \in G$ מתקיים $(ab)^{-1} = b^{-1}a^{-1}$.

הוכחה. 1. נניח שיש שני איברי יחידה e,g. אז $e = eg = g$.

2. נניח שלאיבר a יש שני הפכיים b ו- c. אז $b = be = bac = ec = c$.
3. כפל בהפכי של a (מימין או משמאל) נותן את המבוקש.
4. אם $ab = e$, נכפול ב- b משמאל ונקבל $bab = b = eb$. כעת ע"פ 3. מקבלים $ba = e$ ולכן $b = a^{-1}$. באותו אופן מראים שאם $ba = e$ אז $b = a^{-1}$.
5. קל לראות ש- $(ab)\left(b^{-1}a^{-1}\right) = abb^{-1}a^{-1} = e$ ומכאן (ע"פ 4.) מקבלים $(ab)^{-1} = b^{-1}a^{-1}$.

$\square$

הגדרה 3.1.9. יהיו $m,n \in \mathbb{N}$. אם n מתחלק ב- m נכתוב $m \mid n$.
אם n לא מתחלק ב- m נכתוב $m \nmid n$.

3.2 תת חבורות

הגדרה 3.2.1. תהי $(G,\cdot)$ חבורה.
$\emptyset \neq H \subseteq G$ נקראת תת חבורה של G אם $(H,\cdot)$ מהווה חבורה.
מסמנים $H < G$.

למה 3.2.2. תהי $(G,\cdot)$ חבורה ו- $\emptyset \neq H \subseteq G$. אז $H < G$ אם ורק אם H מקיימת שתי אקסיומות:

1. לכל $a \in H$ גם $a^{-1} \in H$.
2. לכל $a,b \in H$ גם $ab \in H$.

הוכחה. יהי $h \in H$ (יש כזה, כי H לא ריקה).
אז לפי 1. גם $h^{-1} \in H$ ולפי 2. גם $e = hh^{-1} \in H$.
מכאן שמתקיימים שלושת התנאים שבהגדרה 3.1.1 ולכן H היא תת חבורה.
מצד שני, ברור שאם H תת חבורה אז מתקיימים תנאים 1. ו- 2. $\square$

קריטריון נוסף לבדיקת תת חבורה:

למה 3.2.3. תהי $(G,\cdot)$ חבורה ו- $\emptyset \neq H \subseteq G$.
אז $H < G$ אם ורק אם לכל $a,b \in H$ מתקיים $ab^{-1} \in H$.

הוכחה. ברור שאם $H<G$ אז התנאי מתקיים.
בכיוון ההפוך: יהי $h\in H$ אז גם $e=hh^{-1}\in H$ ואז לכל $g\in H$ מתקיים $eg^{-1}=g^{-1}\in H$, והראינו קיום הפכי ב- H (תנאי 1. מלמה 3.2.2).
אם $a,b\in H$ אז גם $b^{-1}\in H$ ולכן

$$ab=a\left(b^{-1}\right)^{-1}\in H$$

וזה תנאי 2. של למה 3.2.2. לכן $H<G$. □

למה 3.2.4. תהי $(G,\cdot)$ חבורה ויהי $a\in G$.
נכתוב $\langle a\rangle:=\{a^n:n\in\mathbb{Z}\}$.
אז $\langle a\rangle<G$.

הוכחה. $a\in\langle a\rangle$ ולכן זו קבוצה לא ריקה.
לכל a^m ו- a^n מתקיים $a^m(a^n)^{-1}=a^ma^{-n}=a^{m-n}\in\langle a\rangle$, ולכן לפי למה 3.2.3. □

הגדרה 3.2.5. תהי $(G,\cdot)$ חבורה. $\langle a\rangle$ נקראת תת חבורה ציקלית של G.
אם קיים $a\in G$ כך ש- $G=\langle a\rangle$,
אז G נקראת חבורה ציקלית ו- a נקרא יוצר של G.

הגדרה 3.2.6. אם $\emptyset\neq S\subset G$ קבוצה לא ריקה של איברים של G, מסמנים ב- $\langle S\rangle$ את תת החבורה הנוצרת על ידי S.
זוהי תת החבורה הקטנה ביותר שמכילה את S.

דוגמא 3.2.7. בחבורה $G=(\mathbb{Z},+)$ נסתכל בתתי החבורות:

א. $\langle 1\rangle=G$

ב. $\langle 2,3\rangle=G$

ג. $\langle 4,6\rangle=\{\ldots,-4,-2,0,2,4,\ldots\}$

הגדרה 3.2.8. תהי $H\subseteq G$ תת קבוצה. מספר האיברים ב- H נקרא הסדר של H ומסומן $o(H)$.

למה 3.2.9. תהי $(G,\cdot)$ חבורה.

א. אם $H_1,H_2<G$ אז גם $H_1\cap H_2<G$.

ב. אם $\{H_\alpha:\alpha\in S\}$ הוא אוסף תתי חבורות של G אז $\bigcap_{\alpha\in S}H_\alpha$ היא תת חבורה של G.

הוכחה. 1. יהיו $g,h\in H_1\cap H_2$. אז גם $h^{-1}\in H_1$ (כי H חבורה), ובאותו אופן גם $h^{-1}\in H_2$, לכן $gh^{-1}\in H_1$ (כי H_1 היא חבורה), וגם $gh^{-1}\in H_2$. מכאן $gh^{-1}\in H_1\cap H_2$, ולפי למה 3.2.3 נובע ש- $H_1\cap H_2<G$.

2. זו הכללה ישירה של הסעיף הקודם.

□

הגדרה 3.2.10. תהי $(G,\cdot)$ חבורה ו- $H<G$ תת חבורה. יהיו $a,b\in G$. אומרים ש- a שקול ל- b מודולו H מימין אם $ab^{-1}\in H$.
נסמן את היחס הזה ב- $a\overset{r}{\equiv}b\pmod H$.

למה 3.2.11. תהי $(G,\cdot)$ חבורה ו- $H<G$. אז היחס $a\overset{r}{\equiv}b\pmod H$ הוא יחס שקילות.

הוכחה. 1. לכל $a \in G$ מתקיים $aa^{-1} = e \in H$ ולכן $a \overset{r}{\equiv} a \pmod H$, כלומר היחס רפלקסיבי.

2. אם $a \overset{r}{\equiv} b \pmod H$ אז $ab^{-1} \in H$ ומכאן $ba^{-1} = (ab^{-1})^{-1} \in H$ לכן $b \overset{r}{\equiv} a \pmod H$ והיחס סימטרי.

3. אם $a \overset{r}{\equiv} b \pmod H$ וגם $b \overset{r}{\equiv} c \pmod H$ אז $ab^{-1} \in H$ וגם $bc^{-1} \in H$ ומכאן ש- $ac^{-1} = ab^{-1}bc^{-1} \in H$
כלומר $a \overset{r}{\equiv} c \pmod H$ והיחס טרנזיטיבי.

□

הגדרה 3.2.12. תהי $(G, \cdot)$ חבורה, $H < G$ ויהי $a \in G$.
הקבוצה $Ha := \{ha : h \in H\}$ נקראת מחלקה ימנית של H ב- G.
כל איבר $b \in Ha$ נקרא נציג של Ha.

למה 3.2.13. תהי $(G, \cdot)$ חבורה ו- $H < G$.
אז לכל $a \in G$ מתקיים $Ha = \left\{x \in G : x \overset{r}{\equiv} a \pmod H\right\}$.
במילים אחרות, מחלקות ימניות הן מחלקות שקילות של היחס $a \overset{r}{\equiv} b \pmod H$.

מסקנה 3.2.14. תהי $(G, \cdot)$ חבורה ו- $H < G$. אז

1. לכל $a, b \in G$ מתקיים

$$Ha \cap Hb = \begin{cases} Ha & \text{if} b \in Ha, \\ \emptyset & \text{otherwise.} \end{cases}$$

2. לכל $a, b \in G$ הפונקציה $f : Ha \to Hb$ המוגדרת $f(ha) = hb$ היא חח"ע ועל.

3. אם $o(H) < \infty$, אז $o(Ha) = o(H)$ לכל $a \in G$.

משפט 3.2.15 (לגרנז').[9] תהי $(G, \cdot)$ חבורה סופית ו- $H < G$. אז $o(H) \mid o(G)$.

הוכחה. יהי k מספר המחלקות הימניות של H ב- G. הסדר $o(G)$ סופי, לכן גם k סופי.
יהיו $\{a_1, \ldots, a_k\}$ נציגים של מחלקות ימניות שונות ב- G. אז לכל $1 \leq i \neq j \leq k$ מתקיים $Ha_i \cap Ha_j = \emptyset$, כך ש-

$$G = \bigsqcup_{i=1}^{k} Ha_i$$

הוא איחוד זר.
כמו כן, $o(Ha_i) = o(H)$ לכל i (ע"פ מסקנה 3.2.14). לכן

$$.o(H) \mid o(G) \iff o(G) = k \cdot o(H)$$

□

הערה 3.2.16. יהי $o(G) = n$, ויהי m כך ש- $m \mid n$. זה <u>לא</u> גורר של- G יש תת חבורה מסדר m.
למשל, ניקח $G = A_4$ - זו החבורה של התמורות הזוגיות של S_4. אז $o(A_4) = 12$.

[9] Joseph-Louis Lagrange 1736 - 1813

בדיקה ישירה מראה שכל תתי החבורות של A_4 הן: $A_4, \{e\}$ ועוד חמש תת חבורות לא טריוויאליות:

$$\{(1,2,3),(1,3,2),e\}$$
$$\{(1,3,4),(1,4,3),e\}$$
$$\{(1,2,4),(1,4,2),e\}$$
$$\{(2,3,4),(2,4,3),e\}$$
$$\{(1,2)(3,4),(1,3)(2,4),(1,4)(2,3),e\}$$

כך של- A_4 אין תת חבורה מסדר 6.

הגדרה 3.2.17. תהי $(G,\cdot)$ חבורה, $H < G$. האינדקס של H ב- G שנסמן אותו $i_G(H)$ (לפעמים גם $[G:H]$) הוא מספר המחלקות הימניות של H ב- G.
אם זה לא מספר סופי, אומרים ש- H בעלת אינדקס אינסופי ב- G.

מסקנה 3.2.18. תהי $(G,\cdot)$ חבורה סופית ו- $H < G$. אז

$$[G:H] = \frac{o(G)}{o(H)}.$$

הגדרה 3.2.19. תהי $(G,\cdot)$ חבורה ויהי $a \in G$. הסדר של a ב- G שנסמן אותו $o(a)$ הוא $m \in \mathbb{N}$ הקטן ביותר כך ש- $a^m = e$.
אם אין m כזה אומרים ש- a בעל סדר אינסופי ב- G.

למה 3.2.20. תהי $(G,\cdot)$ חבורה ויהי $a \in G$. אז $o(a) = o(\langle a \rangle)$.
בפרט אם G סופית אז כל האיברים של G הם מסדר סופי.

מסקנה 3.2.21. תהי $(G,\cdot)$ חבורה סופית, אז לכל $a \in G$ מתקיים $o(a) \mid o(G)$.

הוכחה. ראינו ש- $o(a) = o(\langle a \rangle)$, וגם $\langle a \rangle < G$.
לפי משפט 3.2.15 $o(\langle a \rangle) \mid o(G)$. □

מסקנה 3.2.22. אם G חבורה סופית אז לכל $a \in G$ מתקיים $a^{o(G)} = e$.

טענה 3.2.23. יהי $1 \neq n \in \mathbb{N}$. נגדיר $P(n) = \{k < n : (k,n) = 1\}$ ונגדיר $\cdot : P(n) \times P(n) \to P(n)$ ע"י $(m,k) \mapsto mk \pmod n$.
אז $(P(n),\cdot)$ היא חבורה.

הגדרה 3.2.24. יהי $1 \neq n \in \mathbb{N}$. הפונקציה $\phi(n) = o(P(n))$ נקראת פונקצית אוילר (של n).

מסקנה 3.2.25 (משפט אוילר).[10] יהיו $a, n \in \mathbb{N}$ כך ש- $(a,n) = 1$.
אז $a^{\phi(n)} = 1 \pmod n$.

הוכחה. זו פשוט מסקנה 3.2.22 על החבורה $P(n)$. □

מסקנה 3.2.26 (המשפט הקטן של פרמה).[11] יהי $p \in \mathbb{N}$ ראשוני. אז לכל $a \in \mathbb{N}$ מתקיים $a^p = a \pmod p$.

---

[10] Leonhard Euler 1707 - 1783
[11] Pierre de Fermat 1607 - 1665

הוכחה. לפי משפט 3.3.3 לחבורה $P(p)$ מקבלים $a^{p-1}=1 \pmod p$, ומכאן ברור ש- $a^p=a \pmod p$. $\square$

מסקנה 3.2.27. אם $o(G)$ ראשוני אז G ציקלית.

הוכחה. תהי G חבורה עם $o(G)=p$ ראשוני, ויהי $a\in G$.
לפי מסקנה 3.2.21, $o(a) \mid p$, לכן אם $o(a)\neq 1$ (כלומר $a\neq e$) מקבלים $o(a)=p$ ואז $\langle a\rangle = G$. $\square$

מסקנה 3.2.28. אם $o(G)$ ראשוני ו- $e\neq a\in G$ אז $G=\langle a\rangle$.
במילים אחרות, כל איבר של G פרט ליחידה הוא יוצר של G.

הגדרה 3.2.29. תהי $(G,\cdot)$ חבורה, $H<G$ תת חבורה ויהיו $a,b\in G$. אומרים ש- a שקול ל- b מודולו H משמאל אם $b^{-1}a\in H$. נסמן את היחס הזה ב- $a \overset{\ell}{\equiv} b \pmod H$.

הערה 3.2.30. $a \overset{\ell}{\equiv} b \pmod H$ אם ורק אם $a^{-1} \overset{r}{\equiv} b^{-1} \pmod H$.

מסקנה 3.2.31. תהי $(G,\cdot)$ חבורה ו- $H<G$ אז $a \overset{\ell}{\equiv} b \pmod H$ הוא יחס שקילות.

הגדרה 3.2.32. תהי $(G,\cdot)$ חבורה, $H<G$ ו- $a\in G$. אז $aH := \{ah : h\in H\}$ נקראת מחלקה שמאלית של H.

מסקנה 3.2.33. מחלקות שמאליות הן מחלקות שקילות של היחס $a \overset{\ell}{\equiv} b \pmod H$. בפרט לכל $a,b\in H$ מתקיים $aH=bH$ אם ורק אם $a \overset{\ell}{\equiv} b \pmod H$. אחרת $aH\cap bH=\emptyset$.

מסקנה 3.2.34. תהי $(G,\cdot)$ חבורה ו- $H<G$. אז $f_H : aH \mapsto Ha^{-1}$ היא העתקה חח"ע ועל ממחלקות שמאליות למחלקות ימניות של H ב- G.

הערה 3.2.35. במעבר ממחלקות שמאליות לימניות חשוב מאד לעבור מ- a ל- a^{-1}, כי $aH\neq bH \not\Leftarrow Ha\neq Hb$.
לדוגמא: $G=S_4$ ו- $H=\langle(1,2,3)\rangle=\{(1,2,3),(1,3,2),e\}$.
ניקח $a=(1,2,3,4)$ ו- $b=(1,3,4,2)$.
אז $aH=\{(1,2,3,4),(1,3,2,4),(1,4)\}$ כך ש- $b\notin aH$ ולכן $aH\neq bH$.
אבל $Ha=\{(1,2,3,4),(1,3,4,2),(3,4)\}$ כך ש- $b\in Ha$ ולכן $Ha=Hb$.

הגדרה 3.2.36. תהי $(G,\cdot)$ חבורה ו- $\emptyset\neq H,K\subseteq G$. נגדיר $HK := \{hk : h\in H, k\in K\}$.

למה 3.2.37. תהי $(G,\cdot)$ חבורה עם $H,K<G$. אז $HK<G$ אם ורק אם $HK=KH$.

הוכחה. ניקח שני איברים $h_1k_1, h_2k_2\in HK$ (כאשר $h_1,h_2\in H$ ו- $k_1,k_2\in K$).
אם $HK=KH$ אז קיימים $h_3\in H, k_3\in K$ כך ש- $k_1k_2^{-1}h_2^{-1}=h_3k_3$, ואז

$$h_1k_1\left(h_2k_2\right)^{-1}=h_1k_1k_2^{-1}h_2^{-1}=h_1h_3k_3\in HK$$

ולכן $HK<G$.
בכיוון ההפוך, אם $HK<G$ אז $h=he\in HK$ לכל $h\in H$ ובדומה $k=ek\in HK$ לכל $k\in K$.
לכן לכל $kh\in KH$ מתקיים $kh\in HK$ כי זו מכפלה של שני איברים בחבורה HK ומכאן $KH\subseteq HK$.
כעת, כל איבר $hk\in HK$ הוא הפכי של איזשהו איבר בחבורה $hk=\left(\bar h\bar k\right)^{-1}=\bar k^{-1}\bar h^{-1}\in KH$, ולכן $HK\subseteq KH$,
והראינו ש- $HK=KH$. $\square$

מסקנה 3.2.38. אם $(G,\cdot)$ חבורה אבלית ו- $H,K<G$ אז $HK<G$.

3.3 שימושים בתורת המספרים והצפנת RSA

3.3.1 הצפנת RSA

נזכיר כמה עובדות ותוצאות מתורת המספרים:

1. מספרים $m,n \in \mathbb{N}$ נקראים זרים אם המחלק המשותף הגדול ביותר שלהם $GCD(m,n)$ הוא 1.
   כותבים $GCD(m,n)=1$ ולפעמים פשוט $(m,n)=1$.

2. $GCD(m,n)=1$ אם ורק אם קיימים שלמים $s,t \in \mathbb{Z}$ כך ש- $ms+nt=1$.
   (לפי האלגוריתם של אוקלידס למציאת המחלק המשותף הגדול ביותר).

3. אם $m,n \in \mathbb{N}$ זרים אז לכל $1 \le a \le m$ ולכל $1 \le b \le n$ קיים $1 \le x \le mn$ יחיד כך ש-

$$\begin{cases} x = a \pmod m \\ x = b \pmod n \end{cases}$$

(משפט השאריות הסיני).

הגדרה 3.3.1. יהי $n \in \mathbb{N} \setminus \{1\}$. נגדיר $E(n) = \{k < n : (k,n) = 1\}$.
הקבוצה $E(n)$ עם פעולת הכפל מודולו n נקראת חבורת אוילר.
הפונקציה $\phi(n) := |E(n)|$ נקראת פונקציית אוילר.

תרגיל 3.3.2 1. הוכיחו ש- $(E(n), \cdot \pmod n)$ היא חבורה.

2. יהי $n = p^k$ כאשר p ראשוני ו- $k \in \mathbb{N}$. הוכיחו ש- $\phi(n) = p^k - p^{k-1}$.

3. יהיו $m,n \in \mathbb{N}$ זרים. הוכיחו ש- $\phi(mn) = \phi(m) \cdot \phi(n)$.

4. ידוע שלכל $n \in \mathbb{N} \setminus \{1\}$ יש פירוק יחיד $n = p_1^{k_1} \cdots p_m^{k_m}$ כאשר $p_1, \ldots, p_m$ ראשוניים.
   מצאו נוסחה כללית ל- $\phi(n)$.

מסקנה 3.3.3 (משפט אוילר).[12] יהיו $a,n \in \mathbb{N}$ כך ש- $(a,n)=1$.
אז $a^{\phi(n)} = 1(\mod n)$.

הוכחה. לפי מסקנה ממשפט לגרנז', איבר בחזקת סדר החבורה שווה ליחידה.
לכן לפי חלק 1 של תרגיל 3.3.2 מקבלים את המשפט. □

מסקנה 3.3.4 (משפט פרמה).[13] יהי $p \in \mathbb{N}$ ראשוני. אז לכל $a \in \mathbb{N}$ מתקיים $a^p = a(\mod p)$.

הוכחה. לפי משפט 3.3.3 לחבורה $E(p)$ מקבלים $a^{p-1} = 1(\mod p)$, ומכאן ברור ש- $a^p = a(\mod p)$. □

המשפטים האלה שימושיים מאד בקריפטוגרפיה ובפרט באלגוריתם RSA.[14]

- הרעיון המרכזי הוא שהקידוד והפיענוח אינם סימטריים.
- זה אומר שלפי אלגוריתם ההצפנה לא ניתן לדעת איך לפענח את הקוד.

---

[12] Leonhard Euler 1707 - 1783

[13] Pierre de Fermat 1607 - 1665

◦ אפשר לפרסם בפומבי את הוראות ההצפנה, לכן לפעמים קוראים לשיטה "הצפנה פומבית".

1. נבחר שני מספרים ראשוניים גדולים p, q.
נסמן $n = pq$. אז לפי סעיפים 2 ו- 3 של תרגיל 3.3.2 מקבלים

$$\phi(n) = (p-1)(q-1).$$

2. נבחר a כך ש- $1 < a < \phi(n)$. נוודא ש- $a \neq p, q$ (המספרים p, q הם הסוד הגדול), כך ש- $GCD(a, \phi(n)) = 1$.
המספר a ישמש כאקספוננט של המפתח הפומבי.

הערה 3.3.5 לעתים קרובות משתמשים בראשוני של פרמה (הסבר בהמשך), ומאד מקובל להשתמש במספר $a = 2^{16} + 1 = 65537$. זה מספר ראשוני, והוא "תופס" מעט ביטים.
כדי שיתקיים התנאי $GCD(a, \phi(n)) = 1$ מספיק לבדוק (או לבחור את p, q בצורה המתאימה) ש- $a \nmid (p-1)$ וגם $a \nmid (q-1)$.
בגלל שהמספר הזה פומבי הוא יכול להיות סטנדרטי והבחירה שלו לא חשובה.

3. נחשב את d – ההפכי של a מודולו $\phi(n)$.
כלומר $ad = 1 \pmod{\phi(n)} = (1 + k\phi(n))$.
d הוא האקספוננט של המפתח הסודי שישמש לפיענוח.

4. לצורך ההצפנה מפרסמים בפומבי את n ואת a.

5. לפענוח משתמשים ב- d.
לכן כדי לשמור על סודיות המספרים p, q צריכים להיות ראשוניים גדולים מאד ולא ידועים.
זו אחת הסיבות שחיפוש של מספרים ראשוניים גדולים הוא "שאלה של מליון דולר" (הסברים בהמשך).

תהליך ההצפנה:

1. הופכים את המסר M למספר m שצריך להיות קטן מ- n.
הדרך הפשוטה ביותר היא לתת מספר לכל אות וכל סימן ואז להפוך את המסר למספר m.
אם $m > n$ אז אפשר לחלק את המסר לחלקים m_i שמקיימים $m_i < n$.

2. מחשבים את המספר $c = m^a \pmod{n}$. זהו המסר המוצפן, ואותו מעבירים.
אם מישהו קורא את המסר בדרך, הוא לא יכול לשחזר את m שממנו קיבלנו את c.

כשמתקבל המסר c, מחשבים:

$$c^d = m^{ad} = m^{1+k\phi(n)} = m \pmod{n}$$

מכיוון ש- $m < n$ מקבלים את m.

הערה 3.3.6 למה משתמשים במכפלה של שני ראשוניים?
כי לצורך הפענוח צריך לדעת את הגורמים של n. הבעיה של פירוק מספר לגורמים ראשוניים היא בעיה קשה חישובית.
ככל שהגורמים קרובים יותר ל- $\sqrt{n}$ כך קשה יותר למצוא אותם בחיפוש שיטתי.

[14] Ron Rivest, Adi Shamir, Leonard Adleman

3.3.2 מספרים ראשוניים

תרגיל 3.3.7. הוכיחו כי $n = 2^k - 1$ יכול להיות ראשוני רק אם k ראשוני.

הערה 3.3.8

1. המספרים מהצורה $2^k - 1$ כאשר k ראשוני נקראים מספרי מרסן[15].
בהתאם הראשוניים שבהם נקראים ראשוניים של מרסן.

2. לא לכל k ראשוני המספר $2^k - 1$ הוא ראשוני.
ה- k הראשוני הקטן ביותר שעבורו $2^k - 1$ לא ראשוני הוא $k = 11$:

$$2^{11} - 1 = 2047 = 23 \times 89.$$

3. המספר הראשוני הגדול ביותר הידוע היום הוא ראשוני של מרסן: $2^{82,589,933} - 1$.

4. לא ידוע האם יש מספר סופי או אינסופי של ראשוניים של מרסן.
כמו כן גם לא ידוע האם בין מספרי מרסן יש מספר סופי או אינסופי של מספרים לא ראשוניים.

תרגיל 3.3.9. הוכיחו כי $n = 2^k + 1$ יכול להיות ראשוני רק אם $k = 2^m$.

הערה 3.3.10

1. מספרים מהצורה $2^{2^m} + 1$ נקראים מספרי פרמה.
בהתאם, הראשוניים ביניהם נקראים ראשוני פרמה.

2. עד היום ידועים רק 5 ראשוני פרמה, $m = 0, 1, 2, 3, 4$.
אוילר הראה ש- $2^{2^5} + 1$ הוא לא ראשוני.

3. מאז עוד לא נמצא מספר פרמה נוסף שהוא ראשוני, אבל לא ידוע האם כל מספרי פרמה עם $m > 4$ הם לא ראשוניים.

4. יתרה מזו, כמו במקרה של מספרי מרסן, לא ידוע האם יש מספר סופי או אינסופי של ראשוני פרמה, והאם בין מספרי פרמה יש מספר סופי או אינסופי של מספרים לא ראשוניים.

- בשביל הצפנת RSA דרושים מספרים ראשוניים גדולים.
- איך אפשר לבדוק אם מספר הוא ראשוני או לא? במילים אחרות: איך למצוא ראשוניים גדולים?
- השאלה לא קלה, ומסוף שנות ה- 70 (RSA התפרסם ב- 1977) יש עבודה רבה בנושא.
- ברור שבדיקה ישירה, כלומר חלוקה של המועמד p בכל השלמים $m \leq \sqrt{p}$ היא ארוכה מדי, ולכן מחפשים אלגוריתמים יעילים יותר.
- על פי המשפט הקטן של פרמה, אם p ראשוני אז לכל $a < p$ מתקיים $a^{p-1} = 1 \pmod p$.
- בגלל ש- p אי זוגי, השוויון מתקיים עבור $a = 1$ ו- $a = p - 1$, ולכן מספיק לבדוק $1 < a < p - 1$.
- הרעיון הוא לקחת כמה מספרים קטנים מ- p ולחשב את $a^{p-1} \pmod p$.
אם אחד מהם לא שווה ל- 1 אז p לא ראשוני.
- ברור שבגלל ש- p גדול יהיה קל יותר לבדוק ערכי a קטנים (נניח $2, 3$).

[15] Marin Mersenne 1588 - 1648

- אם p לא ראשוני ו- $a^{p-1} = 1 \pmod p$ אז a נקרא p-שקרן.
- אם $a^{p-1} \neq 1 \pmod p$ אז a נקרא p-עד.

הבעיה של שיטת פרמה היא שיש אינסוף לא ראשוניים p כאלה ש- 2 ו- 3 הם p-שקרנים.
יתרה מזו, יש אינסוף לא ראשוניים שמקיימים: אם $(a,p)=1$ אז $a^{p-1} = 1 \pmod p$, ולכן אם לא מצאנו p-עד אחרי כמה נסיונות זה עדיין לא אומר ש- p ראשוני.

אלגוריתם יעיל בהרבה שנמצא בשימוש נרחב הוא אלגוריתם מילר - רבין[16]:

יהי $p \in \mathbb{N}$ ראשוני. נסתכל במשוואה

$$x^2 - 1 = (x-1)(x+1) = 0 \pmod p$$

בגלל ש- $(\mathbb{Z}_p^*, \cdot)$ היא חבורה, לא קיימים $a,b \in \mathbb{Z}_p^*$ כך ש- $ab=0$.
לכן הפתרונות היחידים הם $x = \pm 1 \pmod p$.
כעת $p > 2$ וראשוני, כלומר הוא אי זוגי. לכן $p-1 = 2^s r$ כאשר $s,r \in \mathbb{N}$ ו- r אי זוגי.
לכל $a < p$ מתקיים $a^{2^s r} = 1 \pmod p$, ולכן השורש הריבועי שלו הוא ± 1.
לכן לכל $a < p$ חייב להתקיים אחד מהשניים: או ש- $a^r = 1 \pmod p$ או שקיים $0 \le d < s$ כך ש- $a^{2^d r} = -1 \pmod p$.

יהי $p-1 = 2^s r$. ניקח $a < p$ ונתחיל לבדוק האם $a^r = 1 \pmod p$.
אם לא, אז נתחיל לבדוק עבור $0 \le d < s$ האם $a^{2^d r} = -1 \pmod p$.
אם a מקיים $a^r \neq 1 \pmod p$ אז a נקרא p-עד חזק.
אם p לא ראשוני, אז תמיד יש לו p-עד חזק.
בפועל לא בודקים כל $a < p$, אלא רק חלק מהם (אלגוריתם הסתברותי).
רבין הוכיח שאם p לא ראשוני אז לכל היותר רבע מהערכים האפשריים של a יכולים להטעות אותנו.

[16] Gary Miller
מיכאל רבין

3.4 תתי חבורות נורמליות וחבורת מנה

3.4.1 תת חבורה נורמלית

הגדרה 3.4.1. תהי $(G,\cdot)$ חבורה ו- $\emptyset \neq H, K \subseteq G$. נגדיר $HK := \{hk : h \in H, k \in K\}$.

דוגמא 3.4.2. יהיו $G = S_3$, $H = \{(1,2), e\}$ ו- $K = \{(2,3), e\}$.
אז

$$
\begin{aligned}
HK &= \{(2,3), e, (1,2), (1,2,3)\} \\
KH &= \{(2,3), e, (1,2), (1,3,2)\}
\end{aligned}
$$

למה 3.4.3. תהי $(G,\cdot)$ חבורה עם $H, K < G$. אז $HK < G$ אם ורק אם $HK = KH$.

הערה 3.4.4. בדוגמא הקודמת $HK \neq KH$ ולכן HK היא לא תת חבורה.

הוכחה. ניקח שני איברים $h_1k_1, h_2k_2 \in HK$ (כאשר $h_1, h_2 \in H$ ו- $k_1, k_2 \in K$).
אם $HK = KH$ אז קיימים $h_3 \in H, k_3 \in K$ כך ש- $k_1k_2^{-1}h_2^{-1} = h_3k_3$ ואז

$$h_1k_1\left(h_2k_2\right)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1h_3k_3 \in HK$$

ולכן $HK < G$.

בכיוון ההפוך, אם $HK < G$ אז $h = he \in HK$ לכל $h \in H$ ובדומה $k = ek \in HK$ לכל $k \in K$.
לכן לכל $kh \in KH$ מתקיים $kh \in HK$ כי זו מכפלה של שני איברים בחבורה HK ומכאן $KH \subseteq HK$.
כעת, כל איבר $hk \in HK$ הוא הפכי של איזשהו איבר בחבורה $hk = \left(\bar{h}\bar{k}\right)^{-1} = \bar{k}^{-1}\bar{h}^{-1} \in KH$, ולכן $HK \subseteq KH$
והראינו ש- $HK = KH$.

$\square$

מסקנה 3.4.5. אם $(G,\cdot)$ חבורה אבלית ו- $H, K < G$ אז $HK < G$.

הערה 3.4.6. אם G לא אבלית ו- $H, K < G$, אז $HK = KH$ לא גורר $hk = kh$ לכל $h \in H$ ו- $k \in K$.

משפט 3.4.7 (עקרון חישוב)**.** תהי $(G,\cdot)$ חבורה עם $H, K < G$ סופיות. אז הקבוצה HK היא סופית מסדר

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

הוכחה. ברור שבקבוצה HK יש $|H| \cdot |K|$ איברים, אבל יתכן שחלקם מייצגים את אותם איברים בחבורה.
זאת אומרת, יתכן ש- $hk = h'k'$ כאשר $h \neq h'$ ו/או $k \neq k'$. צריך לבדוק מתי זה קורה:
לכל איבר $t \in H \cap K$ מקבלים $hk = (ht)\left(t^{-1}k\right)$, ולכן כל איבר ב- HK מיוצג לפחות ע"י $|H \cap K|$ מכפלות ב- HK.
מצד שני, אם $hk = h'k'$ אז $t = h^{-1}h' = k\left(k'\right)^{-1} \in H \cap K$, ואז $h' = ht$ ו- $k' = t^{-1}k$.
לכן כל איבר בחבורה HK מיוצג בדיוק ע"י $|H \cap K|$ מכפלות מהצורה hk.
מכאן ש-

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

$\square$

מסקנה 3.4.8. תהי $(G,\cdot)$ חבורה סופית עם $H,K<G$ כך ש- $|H|\cdot|K|>|G|$. אז $H\cap K\neq\{e\}$.
בפרט, אם $|H|>\sqrt{|G|}$ וגם $|K|>\sqrt{|G|}$ אז $H\cap K\neq\{e\}$.

הוכחה. $KH\subseteq G$ ולכן $|HK|<|G|$, כך שאם $|H|\cdot|K|>|G|$ אז לפי משפט 3.4.7: $|H\cap K|>1$. □

מסקנה 3.4.9. תהי $(G,\cdot)$ חבורה סופית עם $H,K<G$. אם $(|H|\cdot|K|)\nmid(|G|\cdot|H\cap K|)$ אז HK היא לא תת חבורה.

הוכחה. אם $HK<G$ אז לפי משפט לגרנז' $|HK|\mid|G|$ ולפי משפט 3.4.7 זה שקול ל- $(|H|\cdot|K|)\mid(|G|\cdot|H\cap K|)$.
□

מסקנה 3.4.10. תהי G חבורה סופית מסדר $|G|=pm$ כאשר p ראשוני ו- $m<p$.
אז ל- G יש תת חבורה יחידה מסדר p.

הוכחה. יהיו $H,K<G$ מסדר $|H|=|K|=p$.
אז לפי מסקנה 3.4.8 החבורה $H\cap K$ היא מסדר גדול מ- 1.
מצד שני, $H\cap K<H$ כך שהסדר שלה מחלק את הסדר של H (לפי משפט לגרנז').
בגלל ש- p ראשוני מקבלים $|H\cap K|=p$ כלומר $H=K$ וזו תת חבורה יחידה. □

למה 3.4.11. תהי G חבורה ו- $H<G$. יהי $g\in G$, ונגדיר

$$g^{-1}Hg:=\left\{g^{-1}hg:h\in H\right\}$$

אז $g^{-1}Hg$ היא תת חבורה של G.

הוכחה. ברור ש- $g^{-1}Hg\neq\emptyset$. ניקח שני איברים $g^{-1}h_1g,g^{-1}h_2g\in g^{-1}Hg$, אז

$$\left(g^{-1}h_1g\right)\left(g^{-1}h_2g\right)^{-1}=g^{-1}h_1gg^{-1}h_2^{-1}g=g^{-1}h_1h_2^{-1}g\in g^{-1}Hg$$

כי $h_1h_2^{-1}\in H$. □

הגדרה 3.4.12. תהי G חבורה עם $H<G$. יהי $g\in G$. אז תת החבורה $g^{-1}Hg$ נקראת תת חבורה צמודה ל- H.

הערה 3.4.13. 1. הצמדה היא יחס שקילות.

2. $|H|=|g^{-1}Hg|$ כי ההעתקה $h\mapsto g^{-1}hg$ היא חח"ע ועל.

הגדרה 3.4.14. תהי G חבורה. תת חבורה $N<G$ נקראת נורמלית אם לכל $g\in G$ ולכל $n\in N$ מתקיים $g^{-1}ng\in N$.

דרך נוספת לכתוב זאת היא $g^{-1}Ng\subseteq N$.
במילים אחרות, N נורמלית אם כל תת חבורה צמודה לה היא תת חבורה של N.
נסמן נורמליות של תת חבורה ע"י $N\lhd G$.

דוגמא 3.4.15. תהי G חבורה כלשהי. אז $\{e\}\lhd G$ ו- $G\lhd G$. אלה תתי חבורות נורמליות טריוויאליות.

דוגמא 3.4.16. תהי G חבורה אבלית. אז כל תת חבורה שלה היא נורמלית.

דוגמא 3.4.17. $G = S_3$ ו- $H = \{(1,2), e\}$. אפשר לחשב

$$(2,3)(1,2)(2,3) = (1,3,2) \notin H$$

ולכן H היא לא תת חבורה נורמלית.
לעומת זאת $N = \{(1,2,3), (1,3,2), e\}$ היא נורמלית (כותבים $N \lhd S_3$).

דוגמא 3.4.18. תהי G חבורה סופית מסדר $|G| = pm$ כאשר p ראשוני ו- $m < p$.
אז ל- G יש תת חבורה נורמלית N מסדר p.
אכן, לפי משפט קושי לחבורה מסדר pm יש תת חבורה מסדר p.
לפי מסקנה 3.4.10 החבורה הזו יחידה.
לפי למה לכל $g \in G$ מתקיים ש- $g^{-1}Ng < G$ היא תת חבורה מסדר p, ולכן $N = g^{-1}Ng$ לכל $g \in G$, זאת אומרת $N \lhd G$.

משפט 3.4.19. תהי G חבורה ו- $N < G$. הטענות הבאות שקולות:

1. $N \lhd G$.
2. לכל $g \in G$ מתקיים $g^{-1}Ng = N$.
3. לכל $g \in G$ מתקיים $gN = Ng$.
4. לכל $g, h \in G$ מתקיים $gNhN = ghN$.

הוכחה. א. ברור שאם $g^{-1}Ng = N$ אז $g^{-1}Ng \subseteq N$ כלומר $N \lhd G$.
מצד שני, אם $N \lhd G$ אז לכל $g \in G$ מתקיים $g^{-1}Ng \subseteq N$ וגם $gNg^{-1} \subseteq N$ וזה גורר

$$N = g^{-1}\left(gNg^{-1}\right)g \subseteq gNg^{-1}$$

ולכן יש שוויון, והראינו 1 $\iff$ 2.
ב. אם $g^{-1}Ng = N$ אז $Ng = g\left(g^{-1}Ng\right) = gN$.
באותו אופן $gN = Ng$ גורר $N = g^{-1}(gN) = g^{-1}Ng$.
זה מראה ש- 2 $\iff$ 3.
ג. נשים לב שלכל $H < G$ מתקיים $HH = H$, כי מצד אחד כל איבר ב- HH הוא מכפלה של שני איברים ב- H ולכן הוא ב- H, כלומר $HH \subseteq H$. מצד שני $H = eH \subseteq HH$ ויש שוויון.
אם $gN = Ng$ לכל $g \in G$, אז

$$aNbN = a(Nb)N = a(bN)N = (ab)NN = (ab)N$$

ומצד שני, אם לכל $g, h \in G$ מתקיים $gNhN = ghN$ אז בפרט לכל $g \in G$ מתקיים

$$g^{-1}Ng = g^{-1}Nge \subseteq g^{-1}NgN = g^{-1}gN = N$$

כלומר $N \lhd G$ ולכן לפי החלקים הקודמים $gN = Ng$ לכל $g \in G$. □

למה 3.4.20. תהי $(G, \cdot)$ חבורה ו- $H < G$ כך ש- $[G : H] = 2$. אז $H \lhd G$.

הוכחה. ניקח $g \in G \setminus H$. אז $G = H \sqcup Hg$ וגם $G = H \sqcup gH$.
מכאן מקבלים $gH = Hg$ ויש רק שתי מחלקות, לכן לפי משפט 3.4.19 נובע $H \lhd G$. □

דוגמא 3.4.21. $A_n \lhd S_n$.

הערה 3.4.22. $G \rhd N$ ו- $N \rhd K$ לא גורר $K \lhd G$!
למשל ניקח $G = D_8 = \left\langle a, b : a^4 = b^2 = e, ab = ba^3 \right\rangle$.
נסתכל ב- $N = \left\langle a^2, b \right\rangle = \left\{ a^2, b, a^2b, e \right\}$.
אפשר לראות ש- $[G:N] = 2$ ולכן $N \lhd G$.
כמו כן, N אבלית ולכן כל תת חבורה שלה נורמלית. ניקח $K = \{b, e\}$ ואז $G \rhd N \rhd K$ אבל $K \ntriangleleft G$:

$$aba^{-1} = (ba^3)a^{-1} = ba^2 \notin K.$$

למה 3.4.23. תהי G חבורה.

1. אם $N \lhd G$ ו- $K < G$ אז $NK < G$.
2. אם $N \lhd G$ ו- $K < G$ אז $N \cap K \lhd K$.
3. אם $N, M \lhd G$ אז $N \cap M \lhd G$ ו- $NM \lhd G$.

הוכחה. 1. מכיוון ש- $N \lhd G$ אז לכל $k \in K$ ו- $n \in N$ קיים $\tilde{n} \in N$ המקיים $kn = \tilde{n}k$.
בפרט קיים $n_3 \in N$ המקיים $k_1k_2^{-1}n_2^{-1} = n_3k_1k_2^{-1}$ ואז

$$n_1k_1(n_2k_2)^{-1} = n_1k_1k_2^{-1}n_2^{-1} = n_1n_3k_1k_2^{-1} \in NK$$

ולכן $NK < G$.

2. נסתכל על $n_1 \in N \cap K$:
בגלל ש- $N \lhd G$ אז לכל $k \in K < G$ יש $n_2 \in N$ כך ש- $kn_1 = n_2k$, וזה אומר ש- $N \cap K \lhd K$.

3. נתון ש- $gN = Ng$ וגם $gM = Mg$. אז

(א) לכל $k \in N \cap M$ ולכל $g \in G$ מתקיים $gkg^{-1} \in N \cap M$, ולכן $N \cap M \lhd G$.
(ב) $gNM = NgM = NMg$ ולכן $NM \lhd G$.

□

אם G אבלית אז כל תת חבורה שלה היא נורמלית.
האם הטענה ההפוכה נכונה? כלומר, אם G חבורה שכל תת חבורה שלה היא נורמלית, האם G בהכרח אבלית?
התשובה שלילית. נראה דוגמא בעמוד הבא.

דוגמא 3.4.24. $G = Q$ חבורת הקווטרניונים -

$$Q = \left\langle i, j, k : i^2 = j^2 = k^2 = ijk = -1 \right\rangle$$

זו החבורה $Q = \{i, -i, j, -j, k, -k, -1, 1\}$ ו- $|Q| = 8$.
ל- Q יש כמובן שתי תת חבורות טריוויאליות, ויש שלוש תת חבורות מסדר 4:

$$\langle i \rangle = \{i, -1, -i, 1\}, \ \langle j \rangle = \{j, -1, -j, 1\}, \ \langle k \rangle = \{k, -1, -k, 1\}$$

הן נורמליות כי הן מאינדקס 2.

יש תת חבורה אחת מסדר 2:

$$\langle -1\rangle = \{-1,1\}$$

נבדוק שהיא נורמלית:

$$i(-1)(i)^{-1} = i(-1)(-i) = i^2 = -1$$

ובדיוק באותו אופן $j(-1)(j)^{-1} = k(-1)(k)^{-1} = -1$.

לכן $\langle -1\rangle \lhd Q$ ולכן כל תת חבורה של Q היא נורמלית, אבל Q לא אבלית: $ij = k \neq -k = ji$.

3.4.2 חבורת מנה

הגדרה 3.4.25. תהי G חבורה ו- $N \lhd G$.
קבוצת המחלקות השמאליות

$$G/N := \{gN : g \in G\}$$

יחד עם פעולת המכפלה $\cdot : G/N \times G/N \to G/N$ המוגדרת ע"י

$$(gN, hN) \mapsto ghN$$

נקראת חבורת המנה של G לפי N.

משפט 3.4.26. תהי G חבורה ו- $N \lhd G$. אז $(G/N, \cdot)$ היא חבורה.

הוכחה. $N \in G/N$, לכן $\emptyset \neq G/N$.
נבדוק שהפעולה $\cdot : G/N \times G/N \to G/N$ מקיימת את אקסיומות החבורה:

1. לפי סעיף 4 של משפט 3.4.19 $gN \cdot hN = ghN \in G/N$, ולכן יש סגירות.
2. לכל $g,h,k \in G$ מתקיים

$$gN(hNkN) = gN \cdot hkN = ghkN$$
$$(gNhN)kN = ghN \cdot kN = ghkN$$

ולכן הפעולה אסוציאטיבית.

3. $N = eN$ היא היחידה של G/N ולכל $g \in G$ מתקיים

$$gN = gN \cdot eN = geN = egN = eN \cdot gN.$$

4. לכל $gN \in G/N$

$$gN \cdot g^{-1}N = gg^{-1}N = N = g^{-1}N \cdot gN.$$

□

דוגמא 3.4.27. נסתכל ב- $G = (\mathbb{Z},+)$ ותהי $N = n\mathbb{Z} < G$ כאשר $n \in \mathbb{N} \setminus \{1\}$.
אז N נורמלית (כי G אבלית וכל תת חבורה שלה נורמלית).

חבורת המנה היא

$$G/N = \{i + n\mathbb{Z} | 0 \leq i < n\}.$$

הפעולה היא

$$(i + n\mathbb{Z}) + (j + n\mathbb{Z}) = (i + j) \pmod n + n\mathbb{Z}.$$

למה 3.4.28. תהי G חבורה ו- $N \lhd G$. אז $|G/N| = [G : N]$.
בפרט אם G סופית אז $|G/N| = \frac{|G|}{|N|}$.

הוכחה. $|G/N| = [G : N]$ נובע מההגדרה של G/N.
לפי משפט לגרנז' מקבלים שאם G סופית אז $|G/N| = \frac{|G|}{|N|}$. □

הגדרה 3.4.29. חבורה G נקראת פשוטה אם אין לה תת חבורות נורמליות לא טריוויאליות.

ניתן לחשוב על החבורות הפשוטות בתור "אבני הבניין" שמהן ניתן לבנות חבורות אחרות.
איך נראות חבורות פשוטות?
התשובה קלה לחבורות אבליות וקשה מאד לחבורות לא אבליות:

טענה 3.4.30. תהי G חבורה אבלית. אז G פשוטה אם ורק אם היא סופית והסדר שלה הוא מספר ראשוני.

הוכחה. בגלל שבחבורה אבלית כל תת חבורה היא נורמלית, אז אבלית היא פשוטה אם ורק אם אין לה תת חבורות לא טריוויאליות.
נניח ש- G אינסופית. ניקח $e \neq a \in G$ ונסתכל ב- $\langle a \rangle$.
אם $G \neq \langle a \rangle$ אז מצאנו תת חבורה לא טריוויאלית. מצד שני, אם $G = \langle a \rangle$ אז G היא חבורה ציקלית אינסופית הנוצרת על ידי a, כלומר $G = \left\{a^i | i \in \mathbb{Z}\right\}$.
נסתכל ב- $H = \left\langle a^2 \right\rangle$. מקבלים ש- $\{e\} \subsetneq H \subsetneq G$ ואז H תת חבורה לא טריוויאלית ולכן G לא פשוטה.
כעת נניח ש- G סופית. אם היא מסדר ראשוני אז היא פשוטה לפי משפט לגרנז'.
אם היא מסדר לא ראשוני $|G| = mn$ כאשר $m, n > 1$, אז שוב ניקח $e \neq a \in G$ ונסתכל ב- $\langle a \rangle \lhd G$.
אם $G \neq \langle a \rangle$ אז G לא פשוטה.
אם $G = \langle a \rangle$ אז G היא חבורה ציקלית מסדר mn. נסתכל ב- $b = a^m$: זה איבר מסדר n ולכן $H = \langle b \rangle$ היא תת חבורה נורמלית מסדר n.
מצאנו תת חבורה נורמלית לא טריוויאלית ולכן G לא פשוטה. □

לגבי חבורות פשוטות לא אבליות: המיון ואפיון שלהן היו אחת הבעיות הגדולות של המתמטיקה במאה ה- 20 (הושלם סופית ב- 2004).
כמה עובדות על חבורות פשוטות לא אבליות:

- החבורה הלא אבלית הפשוטה הקטנה ביותר היא A_5 (מסדר 60).
- A_n היא חבורה פשוטה לכל $n \geq 5$.
- חבורה מסדר אי זוגי וחבורה מסדר 2^k (עבור $k > 1$) הן תמיד לא פשוטות.
- יש עוד 16 משפחות של חבורות פשוטות. חלקן משפחות אינסופיות (כמו A_n) וחלקן סופיות.
- יש עוד קבוצה של 26 חבורות פשוטות יוצאות דופן. הקטנה ביניהן היא מסדר $7920 = 11 \cdot 5 \cdot 3^2 \cdot 2^4$.

- ○ בין החבורות יוצאות הדופן, השנייה הגדולה ביותר היא מסדר

$$
\begin{aligned}
&2^{41} \cdot 313 \cdot 56 \cdot 72 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47 \\
&= 4154781481226426191177580544000000
\end{aligned}
$$

מכנים אותה "Baby Monster".

- ○ הגדולה ביותר - "The Monster" היא מסדר

$$
\begin{aligned}
&2^{46} \cdot 320 \cdot 59 \cdot 76 \cdot 112 \cdot 133 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \\
&= 808017424794512875886459904961710757005754368000000000 \approx 8 \times 10^{53}
\end{aligned}
$$

- ○ החלק הקשה הוא להוכיח שאין חבורות פשוטות נוספות.
- ○ מהמשפחות האינסופיות הפשוטות ניתן לבנות גם חבורות לא אבליות אינסופיות פשוטות.

3.5 איזומורפיזם של חבורות

3.5.1 הומומורפיזם, גרעין ותמונה

הגדרה 3.5.1. תהינה $\left(\hat{G},*\right),(G,\cdot)$ חבורות. העתקה $\phi:G\to\hat{G}$ נקראת הומומורפיזם (של חבורות) אם לכל $g,h\in G$ מתקיים $\phi(g\cdot h)=\phi(g)*\phi(h)$.

1. יהיו $\left(\hat{G},*\right),(G,\cdot)$ חבורות ו- $\hat{e}\in\hat{G}$ איבר היחידה. אז $\phi:G\to\hat{G}$ המוגדר על ידי $\phi(g)=\hat{e}$ הוא הומומורפיזם.
   זהו ההומומורפיזם הטריוויאלי.

2. תהי $(G,\cdot)$ חבורה, ונגדיר הומומורפיזם $\phi(g)=g$.

3. יהיו $G=(\mathbb{Z},+)$ ו- $\hat{G}=(\mathbb{Z}_n,+)$ כאשר $1<n\in\mathbb{N}$. אז $\phi(m)=m \pmod n$ הוא הומומורפיזם.

4. ההעתקה $\phi:GL_n(F)\to F^*$ המוגדרת על ידי $\phi(M)=\det M$ היא הומומורפיזם.

5. נגדיר $\phi:GL_n(F)\to F$ על ידי $\phi(M)=\operatorname{trace} M$. האם זה הומומורפיזם?

6. נגדיר $\phi:S_n\to\{1,-1\}$ על ידי $\phi(\sigma)=\operatorname{sign}\sigma$. אז ϕ הוא הומומורפיזם.

למה 3.5.2. יהי $\phi:G\to\hat{G}$ הומומורפיזם של חבורות. אז:

א. $\phi(e)=\hat{e}$.

ב. $\phi(a^{-1})=(\phi(a))^{-1}$.

הוכחה. תרגיל. □

הגדרה 3.5.3. תהינה $G,\hat{G}$ חבורות ו- $\phi:G\to\hat{G}$ הומומורפיזם.

1. הגרעין של ϕ הוא
$$\ker\phi=\{g\in G:\phi(g)=\hat{e}\}.$$

2. התמונה של ϕ היא
$$\operatorname{Im}\phi=\{\phi(g):g\in G\}.$$

למה 3.5.4. יהי $\phi:G\to\hat{G}$ הומומורפיזם של חבורות. אז

א. $\ker\phi\lhd G$.

ב. $\operatorname{Im}\phi<\hat{G}$.

הוכחה. 1. ניקח $a,b\in\ker\phi$.
אז

$$\begin{aligned}\phi(ab^{-1})&=\phi(a)\phi(b^{-1})\\&=\hat{e}\left(\phi(b)\right)^{-1}=\hat{e}\hat{e}=\hat{e}\end{aligned}$$

לכן $\ker\phi < G$.
כדי לראות שהיא נורמלית נבדוק שלכל $k \in \ker\phi$ ולכל $g \in G$ מתקיים $gkg^{-1} \in \ker\phi$:
אכן,

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)\hat{e}\left(\phi(g)\right)^{-1} = \hat{e},$$

כלומר $\ker\phi \lhd G$.

2. נשים לב ש- $\mathrm{Im}\phi \neq \emptyset$ כי $\hat{e} \in \mathrm{Im}\phi$ לפי למה 3.5.2.
נסתכל על $h_1, h_2 \in \mathrm{Im}\phi$ ויהיו $g_1, g_2 \in G$ כך ש- $\phi(g_1) = h_1$ ו- $\phi(g_2) = h_2$.
אז

$$h_1 h_2^{-1} = \phi(g_1)\left(\phi(g_2)\right)^{-1} = \phi(g_1)\phi\left(g_2^{-1}\right) = \phi(g_1 g_2^{-1}) \in \mathrm{Im}\phi$$

כי $g_1 g_2^{-1} \in G$.
זה מראה ש- $\mathrm{Im}\phi < \hat{G}$.

□

למה 3.5.5. תהינה $G, \hat{G}$ חבורות ו- $\phi : G \to \hat{G}$ הומומורפיזם על. נסמן $K = \ker\phi$.
לכל $\hat{g} \in \hat{G}$ נגדיר

$$\phi^{-1}(\hat{g}) := \{g \in G : \phi(g) = \hat{g}\}$$

אז $\phi^{-1}(\hat{g}) = gK$ כאשר g הוא איבר כלשהו המקיים $\phi(g) = \hat{g}$.

הסבר: זה אומר שאוסף כל המקורות של איבר מסוים הוא מחלקה שמאלית של $\ker\phi$.

הוכחה. יהי $k \in K$, אז ברור ש- $\phi(gk) = \phi(g)\phi(k) = \phi(g) = \hat{g}$, כלומר $gK \subseteq \phi^{-1}(\hat{g})$.
בכיוון ההפוך, אם $h \in \phi^{-1}(\hat{g})$ אז נסמן $k = g^{-1}h$,
ואז $\phi(k) = \phi\left(g^{-1}\right)\phi(h) = \hat{g}^{-1}\hat{g} = e$.
כלומר $k = g^{-1}h \in K$, או במילים אחרות $h \in gK$.
זה אומר ש- $\phi^{-1}(\hat{g}) \subseteq gK$ ולכן $\phi^{-1}(\hat{g}) = gK$. □

הגדרה 3.5.6. תהינה $G, \hat{G}$ חבורות ויהי $\phi : G \to \hat{G}$ הומומורפיזם.

1. אם לכל $\hat{g} \in \hat{G}$ יש מקור ב- G אז אומרים ש- ϕ הוא על או אפימורפיזם.

2. אם לכל $\hat{g} \in \mathrm{Im}\phi$ יש מקור יחיד ב- G אז אומרים ש- ϕ הוא חד-חד ערכי או מונומורפיזם.

3. הומומורפיזם חד-חד ערכי ועל נקרא איזומורפיזם.
אם קיים איזומורפיזם כזה, החבורות $G, \hat{G}$ נקראות איזומורפיות ומסמנים $G \cong \hat{G}$.

למה 3.5.7. תהינה $G, \hat{G}$ חבורות ויהי $\phi : G \to \hat{G}$ הומומורפיזם. אז ϕ הוא חח"ע אם ורק אם $\ker\phi = \{e\}$.

-

הוכחה. נניח ש- ϕ חח"ע. אז $\phi(g) = \hat{e}$ אם ורק אם $g = e$, כלומר $\ker\phi = \{e\}$.
להיפך - נניח ש- $\ker\phi = \{e\}$, ויהיו $a, b \in G$ כך ש- $\phi(a) = \phi(b)$.
אז $\phi(ab^{-1}) = \phi(a)\phi\left(b^{-1}\right) = \phi(a)\phi(b)^{-1} = \hat{e}$
וזה אומר ש- $ab^{-1} \in \ker\phi$.
לכן $ab^{-1} = e$, או במילים אחרות $a = b$ וזה מראה ש- ϕ חח"ע. □

מסקנה 3.5.8. הומומורפיזם ϕ הוא איזומורפיזם אם ורק אם ϕ הוא על וגם $\ker\phi = \{e\}$.

למה 3.5.9. תהי G חבורה ו- $N \lhd G$. אז $\phi : G \to {}^{G}\!/\!_{N}$ המוגדרת ע"י $\phi(g) = gN$ היא אפימורפיזם, ו- $\ker\phi = N$.

הוכחה. לפי ההגדרה ${}^{G}\!/\!_{N}$ היא אוסף של מחלקות שמאליות, ולכן ברור ש- ϕ על.
נבדוק שזה הומומורפיזם:

$$\phi(gh) = ghN = gNhN = \phi(g)\phi(h).$$

נבדוק את הגרעין:

$$\ker\phi = \{g \in G | gN = N\} = N.$$

□

הערה 3.5.10

1. איזומורפיזם של חבורות הוא יחס שקילות, וחבורות איזומורפיות "מתנהגות" בצורה זהה.
2. כדי לבדוק אם שתי חבורות הן איזומורפיות צריך לבנות הומומורפיזם ביניהן שיהיה על, ולבדוק שהגרעין שלו הוא $\{e\}$.
   זה לא תמיד קל.

3.5.2 משפטי איזומורפיזם

משפט 3.5.11 (משפט האיזומורפיזם הראשון)**.** תהיינה $G, \hat{G}$ חבורות ו- $\phi : G \to \hat{G}$ הומומורפיזם על $\hat{G}$.
אז $\hat{G} \cong {}^{G}\!/\!_{\ker\phi}$.

הוכחה. נתונים $\phi : G \to \hat{G}$ על ו- $\psi : G \to {}^{G}\!/\!_{\ker\phi}$ כאשר $\psi(g) = g\ker\phi$ לכל $g \in G$.

נגדיר $\tau : {}^{G}\!/\!_{\ker\phi} \to \hat{G}$ ע"י $\tau(g\ker\phi) = \phi(g)$.

$$\begin{tikzcd}
G \arrow[r, "\phi"] \arrow[d, "\psi"'] & \hat{G} \\
{}^{G}\!/\!_{\ker\phi} \arrow[ur, dashed, "\tau"'] &
\end{tikzcd}$$

צריך לבדוק ש:

1. τ מוגדר היטב.
2. τ הוא הומומרפיזם.
3. τ על.
4. τ חח"ע.

נבדוק:

1. יהיו $g, h \in G$ כך ש- $g\ker\phi = h\ker\phi$.
   זה אומר שקיים $k \in \ker\phi$ כך ש- $g = hk$, ואז

$$\tau(g\ker\phi) = \phi(g) = \phi(hk) = \phi(h)\phi(k) = \phi(h) = \tau(h\ker\phi).$$

2. לכל $g,h\in G$ מקבלים

$$\begin{aligned}\tau\left(g\ker\phi\cdot h\ker\phi\right)&=\tau\left(gh\ker\phi\right)=\phi(gh)\\&=\phi(g)\phi(h)=\tau(g\ker\phi)\tau(h\ker\phi)\end{aligned}$$

3. נבדוק ש- $\tau : {}^{G}\!/_{\ker\phi}\to\hat{G}$ על:
לכל $\hat{g}\in\hat{G}$ קיים $g\in G$ כך ש- $\phi(g)=\hat{g}$, אז $\tau(g\ker\phi)=\phi(g)=\hat{g}$.

4. לפי למה 3.5.7 מספיק לבדוק ש- $\ker\tau=\{\ker\phi\}$:

$$\begin{aligned}&\tau(g\ker\phi)=\hat{e}\\\Longleftrightarrow&\phi(g)=\hat{e}\\\Longleftrightarrow&g\in\ker\phi\\\Longleftrightarrow&g\ker\phi=\ker\phi\end{aligned}$$

ולכן $\ker\tau=\{\ker\phi\}$ שהוא איבר היחידה ב- ${}^{G}\!/_{\ker\phi}$.

קיבלנו ש- τ הוא איזומורפיזם ולכן $\hat{G}\cong {}^{G}\!/_{\ker\phi}$. □

מסקנה 3.5.12. כל תמונה הומומורפית של G איזומורפית לאיזושהי חבורת מנה של G.
מספר התמונות ההומומורפיות השונות עד כדי איזומורפיזם שווה למספר תתי החבורות הנורמליות של G.

הערה 3.5.13. אם $G\cong\hat{G}$ זה לא אומר שהאיזומורפיזם הוא יחיד.
למשל $G=\left\langle g:g^7=e\right\rangle$.
נגדיר $\phi_i(g)=g^i$ לכל $1\le i\le 7$.
קל לבדוק ש- $\{\phi_i\}_{i=1}^{6}$ הם איזומורפיזמים ו- $\phi_7:G\to\{e\}$.

מסקנה 3.5.14. תהי G חבורה פשוטה ו- $\hat{G}\neq\{\hat{e}\}$.
אם קיים הומומורפיזם $\phi:G\to\hat{G}$ על $\hat{G}$ אז $\hat{G}\cong G$.

הוכחה. הגרעין של ϕ הוא תת חבורה נורמלית ב- G.
מכיוון ש- G פשוטה, יש לה רק שתי תתי חבורות נורמליות G ו- $\{e\}$.
הגרעין לא יכול להיות G (כי אז התמונה היא $\{\hat{e}\}$), ולכן ϕ הוא איזומורפיזם. □

למה 3.5.15. תהיינה $G,\hat{G}$ חבורות ויהי $\phi:G\to\hat{G}$ הומומורפיזם על $\hat{G}$. נסמן $K=\ker\phi$.

1. לכל $\hat{H}<\hat{G}$ נגדיר $H=\phi^{-1}\left(\hat{H}\right)=\left\{g\in G:\phi(g)\in\hat{H}\right\}$. זו קבוצת המקורות של $\hat{H}$.
אז $H<G$ כך ש- $K\subseteq H$.
אם בנוסף $\hat{H}\lhd\hat{G}$ אז $H\lhd G$.

2. תהי $H<G$ כך ש- $K\subseteq H$.
אז $\hat{H}=\phi(H)<\hat{G}$ ואם $H\lhd G$ אז $\hat{H}\lhd\hat{G}$.
אם בנוסף G סופית אז $|H|=|K|\cdot|\hat{H}|$.

הוכחה. תרגיל. □

משפט 3.5.16 (משפט קושי לחבורות אבליות סופיות). תהי G חבורה אבלית סופית, ויהי p ראשוני כך ש- $p \mid |G|$.
אז קיים איבר $a \in G$ כך ש- $o(a) = p$.

ניסוח אחר של המשפט: בתנאים הנ"ל ל- G יש תת חבורה מסדר p.

הוכחה. נוכיח את המשפט באינדוקציה על $|G|$.
אם $|G| = 2$ אז $G = \{a, e\}$ ו- $o(a) = 2$.
נניח שהטענה נכונה לכל G עם $o(G) \le n-1$ ונראה עבור $o(G) = n$.
אם n ראשוני אז G חבורה ציקלית וכל $e \ne a \in G$ מקיים $o(a) = n$ – הראשוני היחיד שמחלק את $|G|$.
אם n לא ראשוני אז ניקח $e \ne a \in G$, ונסמן $H = \langle a \rangle$.
אם $H = G$ אז זו חבורה ציקלית עם יוצר a, וכמו כן $|G| = mp$. נסתכל ב- $b = a^m$.
ברור ש- $b \ne e$ לפי הגדרת הסדר, וגם $b^p = a^{mp} = e$, לכן b הוא איבר מסדר p.
אם $H \ne G$ אז יש שתי אפשרויות: או ש- $p \mid |H|$ ואז לפי הנחת האינדוקציה ל- H יש איבר מסדר p, או ש- $p \nmid |H|$.
אם $p \nmid |H|$ אז $p \mid |G/H|$ וגם $|G/H| < n$.
לכן, לפי הנחת האינדוקציה קיים $g \in G$ כך ש- gH מסדר p, ב- G/H, כלומר $g^p H = H$.
במילים אחרות, $g^p = a^j$ לאיזשהו j.
יהי k הסדר של a^j, אז $\left(g^k\right)^p = a^{jk} = e$.
נשאר רק להראות ש- $g^k \ne e$.
נזכור ש- $(p, k) = 1$ ולכן קיימים $s, t \in \mathbb{Z}$ כך ש- $sp + tk = 1$.
אז אם $g^k = e$ נקבל

$$g = g^{sp+tk} = (g^p)^s \left(g^k\right)^t = a^{js} e^t \in \langle a \rangle = H.$$

וזו סתירה להנחה. □

משפט 3.5.17 (משפט סילו לחבורות אבליות). תהי G חבורה אבלית סופית ויהיו p ראשוני ו- $k \in \mathbb{N}$ כך ש- $p^k \mid |G|$ וגם $p^{k+1} \nmid |G|$.
אז ל- G יש תת חבורה יחידה מסדר p^k.

הוכחה. נתחיל מהוכחת קיום באינדוקציה על k.
אם $k = 1$ אז הטענה נכונה לפי משפט קושי.
נניח שזה נכון לחבורה H כאשר $p^{k-1} \mid |H|$ וגם $p^k \nmid |H|$, ונראה שזה נכון ל- G.
לפי משפט קושי יש ל- G איבר a מסדר p.
כל תת חבורה היא נורמלית ב- G ולכן $\hat{G} = G/\langle a \rangle$ היא חבורה אבלית עם $|\hat{G}| = \frac{|G|}{p}$.
לכן לפי הנחת האינדוקציה ל- $\hat{G}$ יש תת חבורה $\hat{H}$ מסדר p^{k-1}.
נגדיר $\phi : G \to \hat{G}$ הומומורפיזם קנוני אז לפי למה 3.5.15 יש ל- G תת חבורה מסדר p^k.
נוכיח יחידות:
נניח ש- H ו- K הן תת חבורות מסדר p^k.
לפי טענה מהפרק הקודם KH היא תת חבורה של G, ולפי עקרון החישוב

$$|KH| = \frac{|K| \cdot |H|}{|K \cap H|} = \frac{p^{2k}}{|K \cap H|}.$$

לפי משפט לגרנז', סדר של תת חבורה מחלק את סדר החבורה, כך ש- $|K \cap H| = p^k$.
מכאן בהכרח $H = K$. □

משפט 3.5.18 (משפטי איזומורפיזם השני והשלישי). 1. יהיו G ו- $\hat{G}$ חבורות ו- $\phi : G \to \hat{G}$ הומומורפיזם על.

תהי $\hat{G} \lhd \hat{H}$ ו- H מקור שלה ב- G.

אז $G/H \cong \hat{G}/\hat{H}$.

ניסוח נוסף: אם $H, K \lhd G$ ו- $K \subseteq H$ אז

$$G/H \cong (G/K)/(H/K).$$

2. תהי G חבורה ו- $N \lhd G$, $H < G$.

אז $H \cap N \lhd H$ ו-

$$H/H\cap N \cong HN/N.$$

3.6 החבורה הסימטרית

3.6.1 מושגים והגדרות

הגדרה 3.6.1. תמורה על $\{1,2,\dots,n\}$ היא פונקציה חח"ע ועל

$$\sigma:\{1,2,\dots,n\}\to\{1,2,\dots,n\}.$$

מסמנים ב- S_n את קבוצת כל התמורות על $\{1,2,\dots,n\}$.

טענה 3.6.2. הקבוצה S_n היא חבורה למחצה ביחס לפעולת ההרכבה, משום שהרכבת פונקציות חח"ע ועל היא גם חח"ע ועל, ופעולת ההרכבה היא אסוציאטיבית.

ההעתקה $id:\{1,2,\dots,n\}\to\{1,2,\dots,n\}$ המוגדרת על ידי $id:x\mapsto x$ היא כמובן חח"ע ועל, ולכן היא תמורה.
ברור שמתקיים

$$id\circ\sigma=\sigma\circ id=\sigma$$

לכל $\sigma\in S_n$.
כל פונקציה חח"ע ועל היא גם הפיכה,
לכן לכל תמורה σ קיימת תמורה τ כך ש- $\sigma\circ\tau=\tau\circ\sigma=id$.
מסמנים את התמורה הזו $\tau=\sigma^{-1}$, והיא כמובן ההופכית לתמורה σ.

טענה 3.6.3. S_n עם פעולת ההרכבה והאיבר הניטרלי id היא חבורה.

החבורה S_n נקראת "חבורת הסימטריה" או "החבורה הסימטרית".

- מסמנים כרגיל ב- σ^k את ההרכבה של σ עם עצמה k פעמים,
  וב- σ^{-k} את ההרכבה של σ^{-1} עם עצמה k פעמים.
- $\sigma^0=id$ לכל $\sigma\in S_n$.
- חוקי החזקות המוכרים חלים גם כאן.

שאלה 3.6.4. מהו הסדר של S_n?

תשובה 3.6.5. ננסה למנות את כל האפשרויות לבנות תמורה:
יש n אפשרויות לתמונה של 1. אחרי שנבחרה תמונה של 1 נשארו $n-1$ אפשרויות לתמונה של 2, וכך הלאה.
בסה"כ יש

$$n\cdot(n-1)\cdot(n-2)\cdot\dots\cdot2\cdot1=n!$$

אפשרויות לבנות תמורה על $\{1,2,\dots,n\}$, ולכן $|S_n|=n!$.

דוגמא 3.6.6. בחבורה S_3 יש $3!=6$ תמורות:

1. תמורת הזהות.
2. החלפה של 1 ו- 2.
3. החלפה של 1 ו- 3.

4. החלפה של 2 ו- 3.
5. המעגל $1 \to 3 \to 2 \to 1$.
6. המעגל $3 \to 1 \to 2 \to 3$.

הגדרה 3.6.7. מעגל הוא תמורה מהצורה $k_1 \to k_2 \to \cdots \to k_m \to k_1$.
המספר m הוא מספר האיברים שמופיעים במעגל, והוא נקרא האורך של המעגל.

כתיבה: את המעגל $1 \to 3 \to 2 \to 1$ כותבים בצורה (123).
יש כמה דרכים מקובלות לכתיבה של תמורות:

1. כותבים שתי שורות של המספרים $1,\ldots,n$ זו מעל זו. בשורה העליונה מופיעים המקורות ובשורה השנייה התמונות, כאשר כל תמונה נכתבת מתחת למקור שלה. למשל:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

זו התמורה $\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 2, \sigma(4) = 4$.

2. אפשר לכתוב שתי שורות או שני טורים של המספרים $\{1, 2, \ldots, n\}$, וחצים ממקור לתמונה. למשל:

$$\begin{tikzcd} 1 \arrow[drr] & 2 \arrow[dl] & 3 \arrow[dl] & 4 \arrow[d] \\ 1 & 2 & 3 & 4 \end{tikzcd}$$

(זו אותה התמורה שראינו בעמוד הקודם).

3. אפשר לכתוב תמורה לפי המעגלים המרכיבים אותה. למשל $\sigma = (132)(4)$.
מקובל להשמיט מעגלים מאורך 1, לכן במקרה שלנו אפשר לכתוב $\sigma = (132)$.

4. דרך נוספת היא לצייר גרף מכוון בו הקודקודים הם המספרים והחצים מתארים את הפעולה של σ.

$$\begin{tikzcd} 1 \arrow[d] & 2 \arrow[l] \\ 3 \arrow[ur] & 4 \end{tikzcd}$$

קודקוד שלא מחובר בחץ לאף קודקוד אחר מסמן איבר שמועתק לעצמו.
בדוגמא הזו $\sigma(4) = 4$.

תרגיל 3.6.8. הראו שבהינתן $\sigma \in S_n$ ומספר $x \in \{1, 2, \ldots, n\}$, קיימת חזקה טבעית k כך ש- $\sigma^k(x) = x$.

פתרון 3.6.9. נסתכל בקבוצה

$$\{x, \sigma(x), \sigma^2(x), \ldots\}$$

ברור שזו תת קבוצה של $\{1, 2, \ldots, n\}$ ולכן היא סופית.
מכאן שקיימות שתי חזקות m ו- ℓ כך ש-

$$\sigma^\ell(x) = \sigma^m(x)$$

נניח בה"כ ש- $m > \ell$, ונסמן $k = m - \ell$.
נפעיל את $\sigma^{-\ell}$ על שני האגפים ונקבל

$$\begin{aligned}\sigma^{-\ell} \circ \left(\sigma^{\ell}(x)\right) &= \sigma^{-\ell}\left(\sigma^{m}(x)\right)\\ \left(\sigma^{-\ell} \circ \sigma^{\ell}\right)(x) &= \left(\sigma^{-\ell} \circ \sigma^{m}\right)(x)\\ id(x) &= \sigma^{m-\ell}(x)\\ x &= \sigma^{k}(x)\end{aligned}$$

תרגיל 3.6.10. יהי $x \in \{1,2,\ldots,n\}$ ו- $\sigma \in S_n$. נסמן ב- k את החזקה המינימלית של σ שמקיימת $\sigma^k(x) = x$.
להוכיח ש-

$$x, \sigma(x), \sigma^2(x), \ldots$$

הם k מספרים שונים זה מזה (כלומר "שונים בזוגות" - אין בהם שניים שווים).

פתרון 3.6.11. נניח בשלילה שקיימות שתי חזקות שונות $0 \le \ell < m \le k-1$ שמקיימות $\sigma^{\ell}(x) = \sigma^{m}(x)$.
נפעיל את $\sigma^{-\ell}$ על שני האגפים ונקבל $x = \sigma^{m-\ell}(x)$,
אבל $0 < m - \ell < k$ וזה סותר את המינימליות של k.

מסקנה 3.6.12. בהינתן תמורה $\sigma \in S_n$ אפשר להסתכל בגרף המכוון שקודקודיו הם $\{1,2,\ldots,n\}$ ולכל מספר $x \in \{1,2,\ldots,n\}$ יש חץ היוצא ממנו אל $\sigma(x)$.
לפי מה שראינו קודם, המספר x הוא חלק ממעגל פשוט באורך k:

$$x, \sigma(x), \sigma^2(x), \ldots, \sigma^{k-1}(x)$$

ואפשר להגדיר יחס שקילות על $\{1,2,\ldots,n\}$: שני מספרים שקולים אם ורק אם הם חלק מאותו המעגל ביחס לתמורה σ.
זה אומר שאפשר לפרק את התמורה לאוסף של מעגלים פשוטים זרים.

נסתכל על תמורה שהיא מעגל מאורך k:

$$\sigma = (x_1, x_2, \ldots, x_k).$$

כדי שחזקה ℓ של σ תהיה הזהות צריך להתקיים $\sigma^{\ell}(x_1) = x_1$.
בגלל ש- x_1 הוא חלק ממעגל באורך k, זה קורה רק כאשר $k \mid \ell$ ולכן הסדר של σ מתחלק ב- k.
מצד שני, $\sigma^k = id$ ולכן הסדר של σ מחלק את k, ומקבלים ש- $o(\sigma) = k$.
כל תמורה ניתן לכתוב כהרכבה של מעגלים זרים

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_m$$

כך שכל תמורה σ_i היא מעגל.
המעגלים זרים, ולכן $\sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i$.
כדי שהתמורה σ^k תהיה הזהות עבור k מסוים, צריך ש- σ_i^k תהיה הזהות. אבל זה אומר ש- k חייב להתחלק באורך המעגל σ_i.
לכן מתקיים

$$o(\sigma) = \operatorname{lcm}(o(\sigma_1), o(\sigma_2), \ldots, o(\sigma_m)).$$

קיבלנו את הטענה הבאה:

טענה 3.6.13. הסדר של תמורה הוא הכפולה המשותפת הקטנה ביותר של אורכי המעגלים הזרים המרכיבים אותה.

תרגיל 3.6.14. מצאו את הסדר של התמורה

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 7 & 10 & 8 & 9 & 4 & 6 & 5 & 2 \end{pmatrix}.$$

פתרון 3.6.15. נכתוב את התמורה כמכפלה של מעגלים זרים:

$$\sigma = (1,3,7,4,10,2)(5,8,6,9)$$

ויש כאן שני מעגלים, אחד באורך 6 ואחד באורך 4.
מכאן שהסדר של σ הוא 12.

תרגיל 3.6.16. כתבו את "לוח הכפל" של S_3.

פתרון 3.6.17.

$\circ$	id	(12)	(13)	(23)	(123)	(132)
id	id	(12)	(13)	(23)	(123)	(132)
(12)	(12)	id	(132)	(123)	(23)	(13)
(13)	(13)	(123)	id	(132)	(12)	(23)
(23)	(23)	(132)	(123)	id	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	id
(132)	(132)	(23)	(12)	(13)	id	(123)

הערה 3.6.18. שימו לב שבתרגיל הקודם ראינו $(12) \circ (23) = (132)$. אלה שני מעגלים באורך 2 אבל המכפלה שלהם היא מסדר 3.
זו דוגמא לכך שהסדר של מכפלת מעגלים אינו בהכרח הכפולה המשותפת הקטנה ביותר של הסדרים שלהם. זה נכון רק כאשר המעגלים מתחלפים זה עם זה (וזה נכון כאשר מדובר במעגלים זרים).

טענה 3.6.19. כל תמורה אפשר לכתוב כהרכבה של מעגלים מאורך 2.

הוכחה. מספיק להראות שכל מעגל אפשר לפרק למעגלים באורך 2.
אכן,

$$(1,2,\dots,n) = (12) \circ (23) \circ \cdots \circ (n-1,n).$$

$\square$

הגדרה 3.6.20. מעגל באורך 2 נקרא חילוף.

טענה 3.6.21. כל תמורה ניתן לכתוב כהרכבה של מעגלים מאורך 2, כלומר מכפלה של חילופים (לאו דוקא זרים).

דוגמא 3.6.22. את המעגל $(1,2,\dots,n)$ אפשר לכתוב

$$(1,2,\dots,n) = (1,2)(2,3)\cdots(n-1,n)$$

אבל אפשר גם

$$(1,2,\dots,n) = (1,n)(1,n-1)\cdots(1,2)$$

חידה 3.6.23. מקס מניח בשורה 100 קלפים עם המספרים מ- 1 עד 100 בסדר שהוא בוחר, עם הפנים כלפי מטה. הוא נותן להדר מספר x, והיא צריכה למצוא את הקלף שעליו מופיע המספר x תוך 50 נסיונות לכל היותר. ראדה לא יודעת מהו x, אבל היא יודעת את סדר הקלפים בשורה, ומותר לה לעשות חילוף אחד (בין שני קלפים).
מהי האסטרטגיה שראדה והדר צריכות להסכים עליה כדי להבטיח ניצחון במשחק?

(פתרון בשיעור הבא)

הגדרה 3.6.24. בהינתן חבורה G ואיברים $g,h\in G$, מגדירים הצמדה של h על ידי g בתור כפל של h משמאל ב- g ומימין ב- g^{-1}.
אומרים שהאיבר המתקבל ghg^{-1} הוא איבר צמוד ל- h.

נסמן $h\sim h'$ אם קיים איבר $g\in G$ כך ש- $h^{'}=ghg^{-1}$ ונקרא ליחס $\sim$ "יחס הצמידות".

טענה 3.6.25. יחס הצמידות בחבורה הוא יחס שקילות.

הוכחה.
- לכל h מתקיים $h=ehe^{-1}$ ולכן $h\sim h$.
- נניח $h_1\sim h_2$ אז $h_2=gh_1g^{-1}$ ולכן $h_1=g^{-1}h_2(g^{-1})^{-1}$ כלומר $h_2\sim h_1$.
- נניח $h_1\sim h_2$ וגם $h_2\sim h_3$.
  אז $h_2=g_1h_1g_1^{-1}$ וגם $h_3=g_2h_2g_2^{-1}$.
  מכאן
$$h_3=g_2g_1h_1g_1^{-1}g_2^{-1}=(g_2g_1)h_1(g_2g_1)^{-1}$$
  ולכן $h_1\sim h_3$.

□

דוגמא 3.6.26.
1. בחבורה S_3 מתקיים $(1,3,2)\sim(1,2,3)$ וגם $(2,3)\sim(1,3)\sim(1,2)$. ברור ש- id צמודה רק לעצמה.
2. בחבורה אבלית תמיד $ghg^{-1}=h$ (לכל g) ולכן איברים צמודים הם בהכרח שווים.

הגדרה 3.6.27. מחלקות שקילות של יחס ההצמדה נקראות מחלקות צמידות.

תרגיל 3.6.28. להוכיח שאם $h_1\sim h_2$ אז $o(h_1)=o(h_2)$.

פתרון 3.6.29. נניח ש- $o(h_1)=n<\infty$.
אז $h_2=gh_1g^{-1}$ ולכן
$$h_2^n=\underbrace{gh_1g^{-1}\cdots gh_1g^{-1}}_{n\text{ פעמים}}=gh_1^ng^{-1}=geg^{-1}=e$$
ומקבלים ש- $o(h_2)\le n$.
אבל בגלל הסימטריות של יחס הצמידות זה פועל גם בכיוון ההפוך ומקבלים שאם הסדר של אחד מהם הוא סופי אז הסדר של השני גם סופי, ולכן הם שווים.
אחרת, הסדרים של שניהם אינסופיים ולכן הם שווים.

תרגיל 3.6.30. נתונות שתי תמורות σ,τ כך ש- $\sigma=(a_1,a_2,\ldots,a_k)$. מצאו את $\tau\cdot\sigma\cdot\tau^{-1}$.

פתרון 3.6.31. לכל $i \in \{1, \dots, k\}$ התמורה τ^{-1} שולחת את $\tau(a_i)$ ל- a_i.
התמורה σ שולחת אותו ל- a_{i+1} (פרט ל- a_k שנשלח ל- a_1), ואז τ שולחת אותו ל- $\tau(a_{i+1})$.
לכן מתקבל המעגל

$$\tau \cdot \sigma \cdot \tau^{-1} = (\tau(a_1), \tau(a_2), \dots, \tau(a_k))$$

האיברים שאינם במעגל, כלומר שונים מ- $\tau(a_1), \tau(a_2), \dots, \tau(a_k)$ נשלחים לאיברים ששונים מ- $a_1, a_2, \dots, a_k$ על ידי τ^{-1} ולכן σ שולחת אותם לעצמם. לבסוף התמורה τ מחזירה אותם למקור שלהם.

תרגיל 3.6.32. להוכיח ששני מעגלים מאותו אורך הם צמודים.

פתרון 3.6.33. נסתכל על המעגלים $\sigma = (a_1, a_2, \dots, a_k)$ ו- $\sigma' = (a'_1, a'_2, \dots, a'_k)$ ונסתכל על התמורה τ ששולחת כל a_i ל- a'_i.
מדובר על שתי קבוצות של מספרים בגודל k מתוך $\{1, \dots, n\}$ שמועתקות אחת לשנייה. נשארים $n-k$ איברים במקור שמועתקים ל- $n-k$ האיברים הנותרים בטווח, בכל דרך שהיא.
אז לפי הטענה הקודמת $\tau \cdot \sigma \cdot \tau^{-1} = \sigma'$.

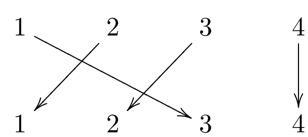
מסקנה 3.6.34. שתי תמורות $\sigma, \sigma' \in S_n$ הן צמודות אם ורק אם לכל מספר טבעי k, מספר המעגלים באורך k בכתיבה של σ כהרכבה של מעגלים זרים שווה למספר המעגלים מאורך k בכתיבה של σ' כהרכבה של מעגלים זרים.

דוגמא 3.6.35.
1. אם תמורה אחת מורכבת משני מעגלים זרים באורך 3 כל אחד, ובשנייה שני מעגלים מאורך 3 ואורך 5, אז הן אינן צמודות.
2. אם שתי תמורות מורכבות משני מעגלים באורך 7 ומעגל אחד באורך 4, אז הן צמודות.

3.6.2 זוגיות של תמורות

בהינתן תמורה, אפשר לרשום אותה כגרף דו-צדדי מכוון, שמתאר לאן כל מספר נשלח.
סופרים את מספר החיתוכים בין הקשתות בגרף, ואומרים שהתמורה "זוגית" אם מספר החיתוכים זוגי, ו"אי-זוגית" אם מספר החיתוכים אי-זוגי.
מבחינה מתמטית, סופרים את k שהוא מספר הזוגות (i,j) של מספרים המקיימים $1 \le i < j \le n$ וגם $\sigma(i) > \sigma(j)$.
זוג (i,j) המקיים את התנאי הזה נקרא היפוך.

דוגמא 3.6.36. בתמורה



מספר החיתוכים הוא 2, ולכן זו תמורה זוגית.

הגדרה 3.6.37. פונקציית הסימן היא פונקציה $\mathrm{sign} : S_n \to \{-1, 1\}$ שמוגדרת

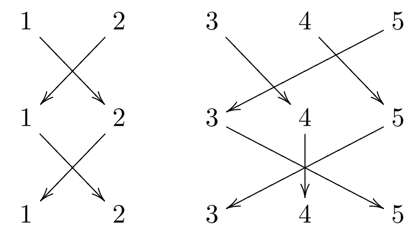
$$\mathrm{sign}(\sigma) = (-1)^k$$

כאשר k הוא מספר החיתוכים.

הערה 3.6.38. ברור שעבור תמורת הזהות $id \in S_n$ מתקיים $\mathrm{sign}(id) = 1$.

טענה 3.6.39. $\mathrm{sign}(\tau \circ \sigma) = \mathrm{sign}(\tau) \cdot \mathrm{sign}(\sigma)$.

הוכחה. נביט בהרכבת התמורות, בצורה של שרשור גרפים דו-צדדיים.



כעיקרון מספר החיתוכים הוא מספר החיתוכים בשתי התמורות. אבל יכול להיות מצב ששני חיתוכים "מבטלים זה את זה", כמו בשרשור של המעגל $(1,2)$ עם עצמו.
במקרה כזה, שני החיתוכים נופלים מהסכום, וזה לא משנה את הזוגיות. □

טענה 3.6.40 $\mathrm{sign}(\sigma)=\mathrm{sign}(\sigma^{-1})$.

הוכחה. מצד אחד, $\mathrm{sign}(\sigma\circ\sigma^{-1})=\mathrm{sign}(id)=1$.
מצד שני

$$\mathrm{sign}(\sigma\circ\sigma^{-1})=\mathrm{sign}(\sigma)\cdot\mathrm{sign}(\sigma^{-1})$$

כלומר

$$\mathrm{sign}(\sigma)\cdot\mathrm{sign}(\sigma^{-1})=1$$

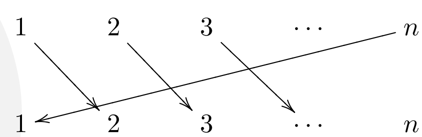
ולכן הזוגיות של σ ושל σ^{-1} שווה. □

תרגיל 3.6.41. הראו שלשתי תמורות צמודות יש אותו סימן.

פתרון 3.6.42.

$$\begin{aligned}\mathrm{sign}(\tau\sigma\tau^{-1})&=\mathrm{sign}(\tau)\,\mathrm{sign}(\sigma)\,\mathrm{sign}(\tau^{-1})=\mathrm{sign}(\tau)\,\mathrm{sign}(\sigma)\,\mathrm{sign}(\tau)\\&=\mathrm{sign}(\tau)^2\,\mathrm{sign}(\sigma)=\mathrm{sign}(\sigma)\end{aligned}$$

במעגל מאורך n יש $n-1$ היפוכים:



לכן הסימן של מעגל כזה הוא $(-1)^{n-1}$.
זה אומר שמעגל מאורך זוגי הוא תמורה אי-זוגית, ומעגל מאורך אי-זוגי הוא תמורה זוגית.

מסקנה 3.6.43. אם $\sigma=(i,j)\in S_n$ אז $\mathrm{sign}(\sigma)=-1$.

במילים: חילוף הוא תמורה אי זוגית.
זה ברור, כי חילוף הוא מעגל באורך 2.
ראינו שאפשר להציג כל מעגל כמכפלה של חילופים (לא בהכרח זרים).

מסקנה 3.6.44 1. אם $\sigma\in S_n$ היא מכפלה של m חילופים אז $\mathrm{sign}(\sigma)=(-1)^m$.

2. תהי $\sigma \in S_n$ ויהי $(i,j) \in S_n$ חילוף, אז

$$\text{sign}(\sigma \circ (i,j)) = \text{sign}((i,j) \circ \sigma) = -\text{sign}(\sigma).$$

הגדרה 3.6.45. נסמן ב- A_n את קבוצת התמורות הזוגיות ב- S_n.

משפט 3.6.46. $A_n \lhd S_n$, ומתקיים $|A_n| = \frac{n!}{2}$.

הוכחה. תחילה נראה ש- $A_n < S_n$.

- $A_n \neq \emptyset$, כי $id \in A_n$.
- יהיו $\sigma, \tau \in A_n$. אז
$$\text{sign}(\sigma \circ \tau) = \text{sign}(\sigma) \cdot \text{sign}(\tau) = 1 \cdot 1 = 1$$
ולכן $\sigma \circ \tau \in A_n$.
- ראינו שלתמורות הופכיות יש אותו סימן, לכן אם $\sigma \in A_n$ אז גם $\sigma^{-1} \in A_n$.

כעת נראה ש- $|A_n| = \frac{n!}{2}$.
נסמן ב- B_n את קבוצת התמורות האי זוגיות (כמובן שזו לא תת חבורה).
אז ברור ש- S_n היא איחוד זר של A_n ו- B_n.
נגדיר פונקציה $f : A_n \to B_n$ על ידי
$$f(\sigma) = \sigma \circ (1,2)$$

לפי ההגדרה, אם $\sigma \in A_n$ אז $f(\sigma) \in B_n$.
אפשר להגדיר פונקציה הפוכה, $g : B_n \to f_n$ על ידי

$$g(\tau) = \tau \circ (1,2)$$

זה אומר ש- f הפיכה, ולכן היא חד חד ערכית ועל.
קיבלנו ש-
$$|A_n| = |B_n|$$

ולכן

$$|S_n| = |A_n \cup B_n| = |A_n| + |B_n| = 2|A_n|$$
$$\Longrightarrow |A_n| = \frac{n!}{2}$$

לכן מתקיים $[S_n : A_n] = 2$ ולפי משפט קודם מקבלים $A_n \lhd S_n$.
ניתן גם לראות ישירות ש- A_n סגורה להצמדה, כי לתמורות צמודות יש אותו סימן (הוכחנו בשיעור קודם). □

הערה 3.6.47. במהלך ההוכחה האחרונה ראינו גם ש- $B_n = (1,2)A_n$, כלומר שקבוצת התמורות האי זוגיות היא מחלקה ימנית (או שמאלית) של A_n.

מפתח