האוניברסיטה
הפתוחה

אלגברה לינארית

כרך ב יחידות 8-5

האוניברסיטה הפתוחה

אלגברה לינארית 1

פרקים 5–8

20109
מהדורה פנימית
לא למכירה ולא להפצה
מק"ט 20109-5049

Linear Algebra 1
Volume II
Dr. Elad Paran

צוות הקורס

מהדורה שנייה

כתיבה: ד"ר אלעד פארן
עריכה מתמטית: ד"ר ציפי ברגר
אסיסטנטית: אסתר גרונהט
יועצים: פרופ' דניאלה ליבוביץ, פרופ' דן הרן, ד"ר גיל אלון, ד"ר מרים רוסט
עורכת: יהודית גוגנהיימר
איורים: רונית בורלא
עימוד: מנוחה מורביץ
התקנה והבאה לדפוס: טלי מאן

מהדורה ראשונה

כתיבה: פרופ' אלי לוין, פרופ' דניאלה ליבוביץ, פרופ' אברהם אורנשטיין, פרופ' אורי לירון, פרופ' דב סמט, פרופ' איתמר פיטובסקי
יועצים: פרופ' אברהם גינזבורג, פרופ' אמנון יקימובסקי, פרופ' מיכאל משלר

הדפסה דיגיטלית – אלול תשע"ו, ספטמבר 2016

בית ההוצאה לאור של האוניברסיטה הפתוחה, הקריה ע"ש דורותי דה רוטשילד, דרך האוניברסיטה 1, ת"ד 808, רעננה 4353701.
The Open University of Israel, The Dorothy de Rothschild Campus, 1 University Road, P.O.Box 808, Raanana 4353701.
Printed in Israel.

17 18 19 20 21 22 23 24 25

תוכן עניינים כללי

כרך א

כרך ב

כרך ג

תוכן העניינים

פרק 5: שדות סופיים

מבוא

בסעיף 1.2 שבפרק 1 עסקנו בשדות סופיים ובחשבון מודולרי (חשבון על־ידי חילוק עם שארית) כאמצעי להגדרת פעולות כפל וחיבור על קבוצות סופיות מסוימות. הראינו טבלאות פעולה של שדות סופיים מסוימים (למשל עבור שדה סופי בן 7 איברים), וטענו, ללא הוכחה, כי לכל מספר ראשוני p קיים שדה סופי בן p איברים. בפרק זה נעמיק ונרחיב את הדיון בתורת המספרים, באריתמטיקה מודולרית ובשדות סופיים, ובפרט נוכיח את הטענה דלעיל. כמו כן נלמד כיצד לבצע חישובים בשדות אלה, וכיצד לפתור בעיות באלגברה לינארית מעל שדות אלה.

5.1 חילוק עם שארית

נפתח בהגדרה פורמלית של מושג המוכר לכם היטב.

הגדרה 5.1.1 התחלקות

יהיו a,b מספרים שלמים.

אם קיים מספר שלם q כך ש־ $a = qb$, נאמר כי a **מתחלק ב־** b. על b נאמר במקרה זה שהוא **מחלק את** a, ונסמן $b|a$.

דוגמאות

$5|20$ (5 מחלק את 20, או 20 מתחלק ב־5) כי $20 = 4 \cdot 5$;

$(-5)|20$, כי $20 = (-4)(-5)$.

הערות

א. כל מספר שלם a מתחלק ב־1 (כלומר $1|a$), כי $a = a \cdot 1$.

ב. כל מספר שלם $a \neq 0$ מתחלק בעצמו (כלומר $a|a$), כי $a = 1 \cdot a$.

ג. 0 מתחלק בכל $b \neq 0$ (כלומר $b|0$), כי $0 = 0b$.

ד. אם $b|a$ ו־ $c|b$ אז $c|a$,
כי אם q מספר שלם כך ש־ $a = qb$, ו־ t שלם כך ש־ $b = tc$, אז $a = qb = q(tc) = (qt)c$.

ה. אם $c|a$ וגם $c \mid b$, אז $c|(a+b)$ וכן $c|(a-b)$,
כי אם q,t מספרים שלמים כך ש־ $a = qc,\ b = tc$, אז:

$$a + b = (q + t)c, \quad a - b = (q - t)c$$

ו. אם $c|a$ ו־ b מספר שלם כלשהו, אז $c|ab$, כי אם q מספר שלם כך ש־ $a = qc$, אז:

$$ab = (bq)c$$

ז. $b|a$ אם ורק אם $(-b)|a$,
כי $a = qb$ אם ורק אם $a = (-q)(-b)$, לכל מספר שלם q.

בין אם $b|a$ ובין אם לאו, תמיד ניתן "לחלק את a ב־ b עם שארית", כפי שלמדתם בבית הספר היסודי. למשל, נחלק את 11 ב־ 4. המספר 4 "נכנס" ב־11 פעמיים, שהרי $2 \cdot 4 = 8$ קטן מ־11, אך $3 \cdot 4 = 12$ גדול מ־11. כשמחסירים מ־11 את $2 \cdot 4$ נותרת שארית 3. שימו לב שהשארית שהתקבלה היא מספר אי־שלילי, קטן מ־ 4 (המספר שבו חילקנו). זוהי תופעה כללית:

משפט 5.1.2 חילוק עם שארית

יהי a מספר **שלם** ויהי b מספר **טבעי**.[1] קיים זוג יחיד (q,r) של מספרים שלמים, כך ש־

א. $a = qb + r$

ב. $0 \le r < b$

למספר q קוראים **המנה** של חילוק a ב־ b,[2] ולמספר r קוראים **השארית** של חילוק a ב־ b.[3]

לפני שנוכיח את המשפט, נדגים:

דוגמאות

א. $a = 11,\ b = 4$: כפי שצוין לפני ההגדרה,

$$11 = 2 \cdot 4 + 3,\ \ 0 \le 3 < 4$$

מנת החילוק של 11 ב־ 4 היא אפוא $q = 2$, והשארית היא $r = 3$.

שימו לב שמתקיים גם

$$11 = 1 \cdot 4 + 7$$

וכן

$$11 = 3 \cdot 4 + (-1)$$

אבל $4 \not< 7$, ו־ $0 \not\le (-1)$, כלומר הזוגות $(q,r) = (1,7)$ ו־ $(q,r) = (3,-1)$ אינם מקיימים את תנאי ב של המשפט.

ב. $a = 20,\ b = 7$. במקרה זה:

$$20 = 2 \cdot 7 + 6,\quad 0 \le 6 < 7$$

המנה היא 2 והשארית היא 6, כלומר $(q,r) = (2,6)$.

ג. $a = 55,\ b = 11$. כאן:

$$55 = 5 \cdot 11 + 0,\ \ 0 \le 0 < 11$$

המנה היא 5 והשארית 0, כלומר $(q,r) = (5,0)$.

בדוגמאות עד כה, המספר a, שאותו חילקנו ב־ b, היה גדול מ־ b. במשפט 5.1.2 אין דרישה כזאת לגבי a. בדוגמאות הבאות מתקיים $a \le b$.

ד. $a = 11,\ b = 11$.

$$11 = 1 \cdot 11 + 0,\ 0 \le 0 < 11$$

המנה היא 1, השארית היא 0, $(q,r) = (1,0)$.

ה. $a = 8,\ b = 11$.

$$8 = 0 \cdot 11 + 8,\ 0 \le 8 < 11$$

המנה היא 0, השארית היא 8, $(q,r) = (0,8)$.

1 תזכורת: מספר טבעי הוא מספר שלם חיובי.

2 האות q נבחרה לציון quotient – מנה.

3 האות r נבחרה לציון remainder – שארית.

ו. $a = 0,\ \ b = 4$.

$$0 = 0 \cdot 4 + 0,\ \ 0 \le 0 < 4$$

במקרה זה $(q,r) = (0,0)$.

ז. $a = -29,\ \ b = 8$.

$$-29 = (-4) \cdot 8 + 3,\ \ 0 \le 3 < 8$$

המנה היא -4, השארית היא 3, $(q,r) = (-4,3)$.

הוכחת משפט 5.1.2

ראשית נוכיח את המשפט עבור $a \ge 0$.

נתחיל בהוכחת **הקיום** של זוג מספרים שלמים (q,r) העונה על הדרישות.

נתבונן בקבוצה:

$$A = \{n \mid nb \le a \text{ שלם אי־שלילי המקיים } n\}$$

A אינה קבוצה ריקה, כי $0 \in A$.

A היא קבוצה סופית, כי לכל $n > a$ מתקיים

$$nb > ab \ge a$$

כלומר $nb \not\le a$, ולכן $A \subseteq \{0,1,2,\ldots,a\}$.

נבחר את המספר המְרַבִּי בקבוצה A, ונסמן אותו ב־ q.

q הוא מספר שלם אי־שלילי, המקיים $qb \le a$, והוא המספר המרבי המקיים תכונות אלה.

כמו כן נסמן:

$$r = a - qb$$

הזוג (q,r) עונה על הדרישות: אכן, לפי בחירת r מתקיים $a = qb + r$ ו־ $r \ge 0$. כמו כן, $r < b$, כי אילו היה $r \ge b$ היה מתקיים $a - qb \ge b$. לכן $a \ge (q+1)b$, בסתירה למְרַבִּיוּת של q.

להוכחת **היחידות** של (q,r), נניח שגם הזוג (t,s) עונה על הדרישות, כלומר t ש־ ו־ s מספרים **שלמים** כך ש־

$$a = tb + s,\ \ 0 \le s < b$$

אם $t > q$, אז לפי המרביות של q מתקיים $tb > a$, כלומר $s < 0$, בסתירה להנחה $s \ge 0$.

אם $t < q$ אז $t \le q - 1$, ולכן

$$s = a - tb \ge a - (q-1)b = a - qb + b = r + b \ge b$$

בסתירה להנחה $s < b$.

לכן בהכרח $t = q$, ולכן גם $s = r$.

להשלמת ההוכחה נטפל במקרה $a < 0$.

במקרה זה $-a > 0$. לכן, לפי מה שכבר הוכחנו, יש זוג יחיד (q,r) של מספרים שלמים, כך ש־

$$-a = qb + r,\ 0 \le r < b$$

לפיכך,

אם $r = 0$ אז $-a = qb + 0$, ואז

$$a = (-q)b + 0$$

כלומר הזוג $(q_1, r_1) = (-q, 0)$ עונה על הדרישות,

ואם $0 < r < b$, אז

$$a = (-q)b - r = (-q-1)b + (b-r)$$

ומתקיים $0 < b-r < b$, כלומר הזוג $(q_1, r_1) = (-q-1, b-r)$ עונה על דרישות המשפט:

$$a = q_1 b + r_1,\ \ 0 \le r_1 < b$$

היחידות של הזוג (q_1, r_1) נובעת מן היחידות של הזוג (q, r).

מ.ש.ל.

שאלה 5.1.1

יהיו: a מספר שלם, b מספר טבעי. הוכיחו ש־ $b|a$ אם ורק אם שארית החילוק של a ב־ b היא 0.

התשובה בעמוד 39

שאלה 5.1.2

יהי b מספר טבעי. הוכיחו כי שארית החילוק של 0 ב־ b היא 0, וכך גם מנת החילוק.

התשובה בעמוד 39

שאלה 5.1.3

מצאו את מנת החילוק ואת השארית כאשר:

א. $a = 25,\ \ b = 7$.

ב. $a = 140,\ \ b = 22$.

ג. $a = -24,\ \ b = 5$.

ד. $a = 0$ ו־ b מספר טבעי כלשהו.

ה. a, b מספרים טבעיים, $a < b$.

התשובה בעמוד 39

שאלה 5.1.4

במשפט החילוק עם שארית, המספר b, שבו חילקנו את a, היה שלם **חיובי**.

הנה גרסה כללית יותר של המשפט, שממנה הסרנו את מגבלת החיוביות של b:

יהיו a, b מספרים **שלמים**, $b \ne 0$. קיים זוג יחיד (q, r) של מספרים שלמים, כך ש־

א. $a = qb + r$

ב. $0 \le r < |b|$

הוכיחו את הגרסה הזאת.

התשובה בעמוד 39

5.2 אריתמטיקה מודולרית

משפט החילוק עם שארית מבטיח, כי שארית החילוק של מספר שלם במספר טבעי נתון n היא מספר שלם, אי־שלילי, וקטן מ־ n, הנקבע באופן יחיד. אפשר, כמובן, שמספרים שונים ישאירו אותה שארית בחילוק ב־ n. למשל, 5 ו־ 8 משאירים אותה שארית בחילוק ב־ 3.

הגדרה 5.2.1

יהי n מספר טבעי, ויהיו a,b מספרים שלמים.

אם a ו־ b משאירים אותה שארית בחילוק ב־ n, נאמר כי a **קוֹנְגְרוּאֶנְטִי** (או **שקול**) **ל־** b **מודולו** n, ונרשום:[1]

$$a \underset{\bmod n}{\equiv} b$$

כאשר a **אינו** שקול ל־ b מודולו n נרשום:

$$a \underset{\bmod n}{\not\equiv} b$$

דוגמאות

8 ו־ 5 משאירים אותה שארית בחילוק ב־ 3 (השארית 2), ולכן:

$$8 \underset{\bmod 3}{\equiv} 5$$

8 ו־ 15 משאירים אותה שארית בחילוק ב־ 7 (השארית 1), ולכן:

$$8 \underset{\bmod 7}{\equiv} 15$$

8 מתחלק ב־ 4 (ללא שארית), ואילו 5 משאיר שארית 1 בחילוק ב־ 4, ולכן:

$$8 \underset{\bmod 4}{\not\equiv} 5$$

לתרגול, מלאו במשבצות הריקות את המתאים מבין הסימנים $\equiv$ או $\not\equiv$:[2]

$$14 \underset{\bmod 4}{\square} 4, \quad 14 \underset{\bmod 5}{\square} 4, \quad 22 \underset{\bmod 7}{\square} 5, \quad 22 \underset{\bmod 5}{\square} 7$$

◀

הערה

התבנית $x \underset{\bmod n}{\equiv} y$ מתארת יחס בין מספרים שלמים: זוג (a,b) של מספרים שלמים עומד ביחס הזה אם a ו־ b משאירים אותה שארית בחילוק ב־ n. יחס זה, המכונה **קוֹנְגְרוּאֶנְצִיָה מודולו** n, הוא בעל התכונות האלה:

א. **רפלקסיביות:** לכל מספר שלם a מתקיים: $a \underset{\bmod n}{\equiv} a$.

ב. **סימטריה:** אם $b \underset{\bmod n}{\equiv} a$ אז $a \underset{\bmod n}{\equiv} b$.

ג. **טרנזיטיביות:** אם $a \underset{\bmod n}{\equiv} b$ וגם $b \underset{\bmod n}{\equiv} c$, אז $a \underset{\bmod n}{\equiv} c$.

---

1 סימון אחר הוא $a \equiv b (\bmod n)$.

2 $14 \underset{\bmod 4}{\not\equiv} 4, \quad 14 \underset{\bmod 5}{\equiv} 4, \quad 22 \underset{\bmod 7}{\not\equiv} 5, \quad 22 \underset{\bmod 5}{\equiv} 7$

בהמשך תתבקשו להוכיח את שלוש התכונות הללו, אך לפני כן נעיר כמה הערות נוספות.

כאשר יחס בין איברים של קבוצה נתונה הוא רפלקסיבי, סימטרי וטרנזיטיבי, היחס נקרא **שקילות**.[3]
לאור ההערה לעיל נגזר הכינוי החלופי ליחס $\underset{\operatorname{mod} n}{\equiv}$, שהוא: **שקילות מודולו** n.

המספר 0 משאיר שארית 0 בחילוק ב־n, כי $0 = 0 \cdot n + 0$. לפיכך המספרים השקולים ל־0 מודולו n הם המספרים שמשאירים שארית 0 בחילוק ב־n, שהם המספרים שמתחלקים ב־n.

במילים אחרות:

- a מתחלק ב־n אם ורק אם:

$$a \underset{\operatorname{mod} n}{\equiv} 0$$

שקילות מודולו 1

כל מספר שלם מתחלק ב־1, הווי אומר: לכל a שלם מתקיים $a \underset{\operatorname{mod} 1}{\equiv} 0$. לפיכך, **לכל** a,b שלמים:

$$a \underset{\operatorname{mod} 1}{\equiv} b$$

שקילות מודולו 2

שארית החילוק ב־2 של מספר שלם היא 0 אם המספר זוגי, ו־1 אם המספר אי־זוגי. לפיכך,
אם a,b שניהם זוגיים, או שניהם אי־זוגיים, אז:

$$a \underset{\operatorname{mod} 2}{\equiv} b$$

אם אחד מבין a,b זוגי, והאחר אי־זוגי, אז:

$$a \underset{\operatorname{mod} 2}{\not\equiv} b$$

טענה 5.2.2

יהי n מספר טבעי, ויהיו a,b מספרים שלמים.
$a \underset{\operatorname{mod} n}{\equiv} b$ אם ורק אם $a-b$ מתחלק ב־n.

הוכחה

נחלק את a ואת b ב־n, ונסמן את השאריות ב־r,s בהתאמה, כלומר:

$$a = qn + r, \; b = tn + s$$

לכן:

$$(a-b) = (q-t)n + (r-s)$$

אם $a \underset{\operatorname{mod} n}{\equiv} b$, אז $r = s$, ואז

$$(a-b) = (q-t)n$$

כלומר $a-b$ מתחלק ב־n.

3 ביחס שכזה כבר נתקלנו בפרק 1 - יחס שקילות השורה בין מטריצות.

להוכחת הכיוון ההפוך, נשים לב שמאחר ש־

$$(r-s)=(a-b)-(q-t)n$$

נובע שאם $a-b$ מתחלק ב־ n אז $(r-s)$, שהוא הפרש של שני מספרים שמתחלקים ב־ n, מתחלק ב־ n, ולכן גם $s-r=-(r-s)$ מתחלק ב־ n. $(r-s)$ ו־ $(s-r)$ קטנים מ־ n ואחד מהם הוא מספר אי־שלילי. אבל בין המספרים $0,1,\ldots,n-1$ יש רק מספר אחד שמתחלק ב־ n, והוא המספר 0. לכן $r=s$, כלומר $a \underset{\text{mod}\, n}{\equiv} b$.

מ.ש.ל.

שאלה 5.2.1

בהסתמך על טענה 5.2.2, הוכיחו את שלוש התכונות המופיעות בהערה שאחרי הגדרה 5.2.1. כלומר, הוכיחו שיחס הקונגרואנציה (מודולו מספר טבעי נתון) הוא יחס שקילות.

התשובה בעמוד 39

שאלה 5.2.2

בדקו האם זוגות המספרים הבאים שקולים מודולו 3 ומודולו 4.

א. $9,3$

ב. $-9,-3$

ג. $-9,3$

ד. $2,14$

ה. $1,5$

ו. $7,17$

התשובה בעמוד 39

כעת נראה שסכומים ומכפלות של מספרים השקולים מודולו n, הם שקולים מודולו n, וביתר דיוק:

משפט 5.2.3

יהי n מספר טבעי, ויהיו a,b,c,d מספרים שלמים.

אם

$$a \underset{\text{mod}\, n}{\equiv} c\,,\quad b \underset{\text{mod}\, n}{\equiv} d$$

אז

$$(a+b) \underset{\text{mod}\, n}{\equiv} (c+d)$$

וכן:

$$ab \underset{\text{mod}\, n}{\equiv} cd$$

הוכחה

לפי טענה 5.2.2, $(a-c)$ ו־ $(b-d)$ מתחלקים ב־ n, כלומר ישנם q,t שלמים כך ש־

$$a-c=qn,\quad b-d=tn$$

נבדוק את ההפרש, $(a+b)-(c+d)$:

$$(a+b)-(c+d)=(a-c)+(b-d)=qn-tn=(q-t)n$$

ההפרש מתחלק ב־ n, לכן לפי טענה 5.2.2:

$$(a+b)\underset{\text{mod}\,n}{\equiv}(c+d)$$

כעת נבדוק את ההפרש $ab-cd$:

$$ab-cd=(c+qn)(d+tn)-cd=qdn+ctn+qntn$$

ההפרש מתחלק ב־ n, לכן, שוב לפי טענה 5.2.2:

$$ab\underset{\text{mod}\,n}{\equiv}cd$$

מ.ש.ל.

סימון 5.2.4

שארית החילוק של מספר שלם a במספר טבעי n תסומן $a_{\text{mod}\,n}$.[4]

דוגמאות

$8=1\cdot 5+\mathbf{3}$, לכן:

$$8_{\text{mod}\,5}=3$$

$14=2\cdot 7+\mathbf{0}$, לכן:

$$14_{\text{mod}\,7}=0$$

לצורך תרגול, השלימו:[5] $9_{\text{mod}\,5}=$ __; $3_{\text{mod}\,2}=$ __; $18_{\text{mod}\,4}=$ __; $(-25)_{\text{mod}\,6}=$ __

מספרים שקולים מודולו n הם מספרים שמשאירים אותה שארית בחילוק ב־ n. לשון אחר:

- $a\underset{\text{mod}\,n}{\equiv}b$ אם ורק אם $a_{\text{mod}\,n}=b_{\text{mod}\,n}$.

הטענות שלהלן נובעות מיידית מההגדרות. ודאו שאתם מבינים אותן ויודעים לנמקן.

- לכל n טבעי ולכל a שלם,
  - א. $0\le a_{\text{mod}\,n}<n$.
  - ב. $a-a_{\text{mod}\,n}$ מתחלק ב־ n.
  - ג. $a\underset{\text{mod}\,n}{\equiv}a_{\text{mod}\,n}$.
  - ד. $a_{\text{mod}\,n}=0$ אם ורק אם $n|a$.
  - ה. אם $0\le a<n$, אז $a_{\text{mod}\,n}=a$.
  - ו. $(a_{\text{mod}\,n})_{\text{mod}\,n}=a_{\text{mod}\,n}$.

4 סימון מקובל אחר: $\bar{a}_n$

5 $9_{\text{mod}\,5}=4;\ 3_{\text{mod}\,2}=1;\ 18_{\text{mod}\,4}=2;\ (-25)_{\text{mod}\,6}=5$

שתי מסקנות מיידיות של משפט 5.2.3 מקלות מאוד על חישוב שאריות מודולו n:

למה 5.2.5

אם b מתחלק ב־n, אז $(a+b)_{\bmod n} = a_{\bmod n}$.

הוכחה

אם b מתחלק ב־n, אז $b \underset{\bmod n}{\equiv} 0$, לכן, לפי משפט 5.2.3,

$$a+b \underset{\bmod n}{\equiv} a+0=a$$

ופירוש הדבר הוא:

$$(a+b)_{\bmod n} = a_{\bmod n}$$

מ.ש.ל.

שימו לב שהמספר b הנזכר בלמה 5.2.5 הוא מספר שלם כלשהו, המתחלק במספר n, לאו דווקא חיובי. לפי הלמה, אם ברצוננו לחשב את $a_{\bmod n}$, נוכל תחילה להוסיף ל־a, או לחסר ממנו, מספר חיובי b אשר קל לראות כי הוא מתחלק ב־n, ורק אז לחלק עם שארית. למשל, כדי לחשב בקלות את $125_{\bmod 6}$, נחסר ממנו 120 (אשר ברור כי הוא מתחלק ב־6) ונקבל:

$$125_{\bmod 6} = (125-120)_{\bmod 6} = 5_{\bmod 6} = 5$$

דוגמה

נחשב את $1127_{\bmod 5}$. 1000 מתחלק ב־5, לכן $1127_{\bmod 5} = 127_{\bmod 5}$; 100 מתחלק ב־5, לכן $127_{\bmod 5} = 27_{\bmod 5}$. מכאן כבר קל לראות את התוצאה הסופית: $27_{\bmod 5} = 2$.

בשיטה שתיארנו אפשר להשתמש גם כדי להמיר חישובי שאריות חילוק של מספרים שליליים, בחישובים במספרים חיוביים (שהם נוחים יותר). נחשב למשל את $(-842)_{\bmod 3}$. תחילה נוסיף 900 ונקבל:

$$(-842)_{\bmod 3} = (900-842)_{\bmod 3} = 58_{\bmod 3}$$

נפעיל את הלמה שוב ונקבל:

$$58_{\bmod 3} = (58-30)_{\bmod 3} = 28_{\bmod 3} = 1$$

◄

מסקנה שימושית נוספת היא:

למה 5.2.6

יהיו: n מספר טבעי, a,b מספרים שלמים. אזי:

$$(a+b)_{\bmod n} = (a_{\bmod n} + b_{\bmod n})_{\bmod n}$$

וכן:

$$(a \cdot b)_{\bmod n} = (a_{\bmod n} \cdot b_{\bmod n})_{\bmod n}$$

הוכחה

עלינו להראות:

$$a+b \underset{\text{mod}\,n}{\equiv} a_{\text{mod}\,n}+b_{\text{mod}\,n}$$

וכן:

$$a\cdot b \underset{\text{mod}\,n}{\equiv} a_{\text{mod}\,n}\cdot b_{\text{mod}\,n}$$

טענות אלה נובעות מיידית ממשפט 5.2.3, לאור העובדה שלכל מספר שלם x, $x \underset{\text{mod}\,n}{\equiv} x_{\text{mod}\,n}$

מ.ש.ל.

לפי למה 5.2.6, אם ברצוננו לחשב את שארית החילוק ב־ n של סכום או מכפלה של מספרים שלמים, אפשר לחשב את שאריות החילוק של המחוברים (או הגורמים), ורק אחר כך לחברם (או לכפול אותם) ולמצוא את השארית של הסכום (או המכפלה). למשל,

$$(125+58)_{\text{mod}\,6}=(125_{\text{mod}\,6}+58_{\text{mod}\,6})_{\text{mod}\,6}=(5+4)_{\text{mod}\,6}=9_{\text{mod}\,6}=3$$

$$(125\cdot 58)_{\text{mod}\,6}=(125_{\text{mod}\,6}\cdot 58_{\text{mod}\,6})_{\text{mod}\,6}=(5\cdot 4)_{\text{mod}\,6}=20_{\text{mod}\,6}=2$$

שאלה 5.2.3

חשבו ביעילות:

א. $(140+78)_{\text{mod}\,3}$, $(140\cdot 78)_{\text{mod}\,3}$.

ב. $(182-45)_{\text{mod}\,7}$, $(182\cdot(-45))_{\text{mod}\,7}$.

ג. $(10145+28983)_{\text{mod}\,4}$, $(10145\cdot 28983)_{\text{mod}\,4}$.

ד. $(1240+95)_{\text{mod}\,11}$, $(1240\cdot 95)_{\text{mod}\,11}$

התשובה בעמוד 40

הגדרה 5.2.7

יהי n מספר טבעי.

1. $(a+b)_{\text{mod}\,n}$ מכונה **הסכום מודולו** n **של** a **ו־** b;
   הפעולה על קבוצת המספרים השלמים $\mathbb{Z}$, המתאימה לכל $a,b\in\mathbb{Z}$ את סכומם מודולו n, נקראת **חיבור מודולו** n. היא תסומן $+_n$. אם כן:
   $$a +_n b := (a+b)_{\text{mod}\,n}$$
2. $(a\cdot b)_{\text{mod}\,n}$ מכונה **המכפלה מודולו** n **של** a **ו־** b;
   הפעולה על קבוצת המספרים השלמים $\mathbb{Z}$, המתאימה לכל $a,b\in\mathbb{Z}$ את מכפלתם מודולו n, נקראת **כפל מודולו** n. היא תסומן $\cdot_n$. אם כן:
   $$a \cdot_n b := (a\cdot b)_{\text{mod}\,n}$$

שאלה 5.2.4

הוכיחו את השוויונות:

$$a +_n b = a_{\bmod n} +_n b_{\bmod n}$$

$$a \cdot_n b = a_{\bmod n} \cdot_n b_{\bmod n}$$

התשובה בעמוד 40

שאלה 5.2.5

חשבו את הסכומים ואת המכפלות המודולריים הבאים:

א. $5 +_6 3$, $5 \cdot_6 3$

ב. $12 +_6 2$, $12 \cdot_6 2$

ג. $14 +_4 -3$, $14 \cdot_4 -3$

ד. $-40 +_{12} -4$, $-40 \cdot_{12} -4$

התשובה בעמוד 40

למה 5.2.8

יהי n מספר טבעי. פעולות החיבור והכפל מודולו n הן חילופיות וקיבוציות; כמו כן, הכפל מודולו n מתפלג מעל החיבור מודולו n.

הוכחה

חילופיות

עלינו להראות שלכל $a,b \in \mathbb{Z}$:

$$a +_n b = b +_n a$$

$$a \cdot_n b = b \cdot_n a$$

כלומר, שלכל $a,b \in \mathbb{Z}$:

$$(a+b)_{\bmod n} = (b+a)_{\bmod n}$$

$$(a \cdot b)_{\bmod n} = (b \cdot a)_{\bmod n}$$

השוויונות הללו נובעים מיידית מן החילופיות של החיבור והכפל הרגילים:

$$a + b = b + a$$

$$a \cdot b = b \cdot a$$

קיבוציות

עלינו להראות שלכל $a,b,c \in \mathbb{Z}$:

$$(a +_n b) +_n c = a +_n (b +_n c)$$

כלומר, שלכל $a,b,c \in \mathbb{Z}$:

$$\left((a+b)_{\bmod n} + c\right)_{\bmod n} = \left(a + (b+c)_{\bmod n}\right)_{\bmod n}$$

כלומר, שלכל $a,b,c \in \mathbb{Z}$:

$$(a+b)_{\bmod n} + c \underset{\bmod n}{\equiv} a + (b+c)_{\bmod n}$$

אכן, מאחר שלכל x שלם, $x \underset{\bmod n}{\equiv} x_{\bmod n}$, הרי שמתקיים:

$$(a+b)_{\bmod n} \underset{\bmod n}{\equiv} (a+b)$$

$$(b+c)_{\bmod n} \underset{\bmod n}{\equiv} (b+c)$$

לכן, לפי משפט 5.2.3:

$$(a+b)_{\bmod n} + c \underset{\bmod n}{\equiv} (a+b)+c = a+(b+c) \underset{\bmod n}{\equiv} a + (b+c)_{\bmod n}$$

פילוג הכפל מודולו n מעל החיבור מודולו n

עלינו להראות שלכל $a,b,c \in \mathbb{Z}$:

$$a \cdot_n (b +_n c) = a \cdot_n b +_n a \cdot_n c$$

כלומר שלכל $a,b,c \in \mathbb{Z}$:

$$\left(a\left((b+c)_{\bmod n}\right)\right)_{\bmod n} = \left((ab)_{\bmod n} + (ac)_{\bmod n}\right)_{\bmod n}$$

כלומר שלכל $a,b,c \in \mathbb{Z}$:

$$a\left((b+c)_{\bmod n}\right) \underset{\bmod n}{\equiv} (ab)_{\bmod n} + (ac)_{\bmod n}$$

אכן, לפי משפט 5.2.3 מתקיים:

$$a(b+c)_{\bmod n} \underset{\bmod n}{\equiv} a(b+c) = ab + ac \underset{\bmod n}{\equiv} (ab)_{\bmod n} + (ac)_{\bmod n}$$

מ.ש.ל.

מכלל הטענות שהוכחנו עד כה נובע, שבחישובי סכומים מודולו n, סדר המחוברים וסדר הביצוע של חיבורי זוגות אינם משפיעים על התוצאה, ושבכל שלב של החישוב אפשר להוסיף לכל מחובר, או לגרוע ממנו, כל מספר שהוא שמתחלק ב־ n. בפרט, במהלך החישוב אפשר להמיר כל מחובר בשארית החילוק שלו ב־ n. במחובר שהוא מכפלה של גורמים אפשר להחליף כל גורם בכל מספר ששקול לו מודולו n, ובפרט אפשר להמיר כל גורם בשארית החילוק שלו ב־ n.

דוגמה

1. נחשב את $4^{62}{}_{\bmod 7}$.

תחילה נשים לב כי

$$4^2 = 16 \underset{\bmod 7}{\equiv} 2, \quad 4^3 = 64 \underset{\bmod 7}{\equiv} 1$$

וכי:

$$4^{62} = \left(4^3\right)^{20} 4^2$$

$$\left(4^3\right)^{20} 4^2 \underset{\bmod 7}{\equiv} 1^{20} \cdot 2 = 2$$

לפיכך:

$$4^{62}{}_{\bmod 7} = 2$$

▸

שאלה 5.2.6

חשבון:

א. $7^{31}{}_{\bmod 12}$

ב. $21^{35}{}_{\bmod 6}$

התשובה בעמוד 40

יהי n מספר טבעי. שארית החילוק ב־ n של כל מספר שלם a היא שלם אי־שלילי הקטן מ־ n, כלומר היא אחד מבין המספרים $0,1,\ldots,(n-1)$.

נסמן:

$$\mathbb{Z}_n = \{0,1,\ldots,(n-1)\}$$

את האמור לעיל נוכל לנסח כך: לכל $x \in \mathbb{Z}$,

$$x_{\bmod n} \in \mathbb{Z}_n$$

מובן אפוא שלכל $a,b \in \mathbb{Z}$, $(a+b)_{\bmod n}$ ו־ $(ab)_{\bmod n}$ הם איברים של $\mathbb{Z}_n$.

כלומר, לכל $a,b \in \mathbb{Z}$,

$$a +_n b \in \mathbb{Z}_n\,,\quad a \cdot_n b \in \mathbb{Z}_n$$

ובפרט, לכל $a,b \in \mathbb{Z}_n$:

$$a +_n b \in \mathbb{Z}_n\,,\quad a \cdot_n b \in \mathbb{Z}_n$$

את ההבחנה האחרונה נוכל לנסח כך:

מסקנה 5.2.9

הקבוצה $\mathbb{Z}_n$ **סגורה** ביחס לחיבור מודולו n וביחס לכפל מודולו n.

למה 5.2.10

בקבוצה $\mathbb{Z}_n$, המספר 0 הוא ניטרלי ביחס לחיבור מודולו n.

הוכחה

עלינו להראות שלכל $a \in \mathbb{Z}_n$:

$$a +_n 0 = 0 +_n a = a$$

מאחר שחיבור מודולו n הוא חילופי, מספיק שנראה כי:

$$a +_n 0 = a$$

אכן, לכל $a \in \mathbb{Z}_n$ מתקיים $0 \le a < n$, ולכן:

$$a_{\bmod n} = a$$

לפיכך:

$$a +_n 0 = (a+0)_{\bmod n} = a_{\bmod n} = a$$

מ.ש.ל.

שימו לב

השוויון $a +_n 0 = 0 +_n a$ מתקיים **לכל** $a \in \mathbb{Z}$, לפי למה 5.2.8. אולם ב־ $\mathbb{Z}$, המספר 0 אינו ניטרלי ביחס לחיבור מודולו n, כי אם $a \geq n$ אז $a +_n 0 \neq a$, שהרי:

$$a +_n 0 = (a + 0)_{\bmod n} = a_{\bmod n} < n$$

זוהי אחת הסיבות שבגללן נתמקד בהמשך בתכונות פעולות החיבור והכפל מודולו n כאשר אנו רואים אותן כפעולות על הקבוצה $\mathbb{Z}_n = \{0,1,\ldots,(n-1)\}$.

למה 5.2.11

יהי $n > 1$. ב־ $\mathbb{Z}_n$, המספר 1 הוא ניטרלי ביחס לכפל מודולו n.

הערות

א. טענת למה 5.2.11 היא, שלכל $a \in \mathbb{Z}_n$:

$$1 \cdot_n a = a \cdot_n 1 = a$$

שימו לב שהשוויון $1 \cdot_n a = a \cdot_n 1$ מתקיים **לכל** $a \in \mathbb{Z}$ (למה 5.2.8), אבל המספר 1 אינו ניטרלי ב־ $\mathbb{Z}$ ביחס לכפל מודולו n. כי אם $a \geq n$, אז $a \cdot_n 1 \neq a$, שהרי:

$$a \cdot_n 1 = (a \cdot 1)_{\bmod n} = a_{\bmod n} < n$$

ב. הסייג $n > 1$ הוא חיוני; עבור $n = 1$, $\mathbb{Z}_n = \mathbb{Z}_1 = \{0\}$, כלומר $1 \notin \mathbb{Z}_1$.

שאלה 5.2.7

הוכיחו את למה 5.2.11.

התשובה בעמוד 41

למה 5.2.12

לכל איבר בקבוצה $\mathbb{Z}_n$ יש איבר נגדי ביחס לפעולת החיבור $+_n$.

הוכחה

ברור ש־ $0 \in \mathbb{Z}_n$ נגדי לעצמו. אם $a \in \mathbb{Z}_n$ ו־ $a \neq 0$ אז $0 < a < n$, לכן גם $0 < n - a < n$, ומכאן ש־ $(n-a) \in \mathbb{Z}_n$ ומתקיים:

$$(n-a) +_n a = \left((n-a) + a\right)_{\bmod n} = n_{\bmod n} = 0$$

מ.ש.ל.

הערה

שימו לב שלֶמָּה 5.2.12 מראה את קיומו של איבר נגדי לכל איבר ב־ $\mathbb{Z}_n$, אך יתר על כן - היא מורה על דרך פשוטה למציאתו. הנגדי של כל איבר $a \in \mathbb{Z}_n$ השונה מאפס הוא $n - a$, והנגדי של איבר האפס הוא איבר האפס עצמו.

לקבוצה $\mathbb{Z}_n$, בצירוף הפעולות $\cdot_n , +_n$, קוראים **חוג המספרים השלמים מודולו** n, ובקיצור -**החוג** $\mathbb{Z}_n$. לפעולות $+_n$ ו־$\cdot_n$ על $\mathbb{Z}_n$ נקרא **החיבור והכפל** (בהתאמה) **של החוג** $\mathbb{Z}_n$, וכאשר מוקד העניין הוא $\mathbb{Z}_n$ עבור איזשהו n קבוע, לרוב נסמן את הפעולות $+_n$ ו $\cdot_n$ פשוט על־ידי $+$ ו־$\cdot$.

נעיר כי החוג $\mathbb{Z}_n$ הוא מקרה פרטי של מבנה אלגברי מופשט הנקרא **חוג**. לא נביא את ההגדרה הכללית כאן, ולא נזדקק לה.

אם תחזרו לעיין בהגדרת מושג **השדה**,[6] תמצאו שעבור $n > 1$, הקבוצה $F = \mathbb{Z}_n$, עם פעולות החיבור והכפל של החוג $\mathbb{Z}_n$ (דהיינו עם החיבור והכפל מודולו n), עונה כמעט על כל הדרישות המופיעות בה: $\mathbb{Z}_n$ סגורה לגבי שתי הפעולות הללו (מסקנה 5.2.9); שתי הפעולות הן חילופיות וקיבוציות (למה 5.2.8); ב־ $\mathbb{Z}_n$ יש איבר ניטרלי ביחס לחיבור מודולו n (למה 5.2.10), ויש בה איבר ניטרלי ביחס לכפל מודולו n (למה 5.2.11); איברי $\mathbb{Z}_n$ הפיכים לגבי החיבור (למה 5.2.12); הכפל מודולו n מתפלג מעל החיבור מודולו n (למה 5.2.8). הדרישה היחידה המופיעה בהגדרת השדה שעדיין לא התייחסנו אליה, היא דרישת ההפיכות של איברי $\mathbb{Z}_n$ השונים מ־ 0, ביחס לכפל מודולו n.

לערכים קטנים של n, קל לרשום את לוח הכפל מודולו n על $\mathbb{Z}_n$, ולברר באמצעותו את שאלת קיום ההופכיים לאיברי $\mathbb{Z}_n$ השונים מ־ 0.

לפניכם, זה לצד זה, לוח הכפל מודולו 6 על הקבוצה $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$, ולוח הכפל מודולו 7 על הקבוצה $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$.

לוח הכפל מודולו 6 על $\mathbb{Z}_6$

$\cdot_6$	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

לוח הכפל מודולו 7 על $\mathbb{Z}_7$

$\cdot_7$	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

6 הגדרה 1.2.1 בפרק 1.

מלוח הכפל הימני רואים, כי האיברים היחידים של $\mathbb{Z}_6$ שהם הפיכים ביחס ל־ $\cdot_6$, הם 1 ו־ 5 (כל אחד מהם הופכי לעצמו). מלוח הכפל השמאלי רואים, שכל $0 \neq a \in \mathbb{Z}_7$ הוא הפיך (1 ו־ 6 הופכיים כל אחד לעצמו, 2 ו־ 4 הופכיים זה לזה, 3 ו־ 5 הופכיים זה לזה). אם כן, החוג $\mathbb{Z}_6$ אינו שדה, והחוג $\mathbb{Z}_7$ הוא שדה.

מתבקשת השאלה, לאילו ערכים של n החוג $\mathbb{Z}_n$ הוא שדה? התשובה (שבפרק 1 ניתנה ללא הוכחה) היא, שהחוג $\mathbb{Z}_n$ הוא שדה אם ורק אם n ראשוני. הטענה הזאת תוכח בסעיף 5.4, מיד לאחר שנבסס (בסעיף 5.3) את הרקע הבסיסי הדרוש בנוגע למספרים ראשוניים.

לסיום הסעיף נביא שימוש בסיסי ומעניין לאריתמטיקה מודולרית. ייתכן שזכור לכם מלימודי בית הספר היסודי, הקריטריון המוכר להתחלקות מספר טבעי ב־ 3:
מספר טבעי n מתחלק ב־ 3 אם ורק אם סכום ספרותיו מתחלק ב־ 3.

נוכיח קריטריון זה. אכן, אם הספרות של n (משמאל לימין) הן $a_1,\dots,a_k$, אז:

$$n = 10^{k-1}a_1 + 10^{k-2}a_2 + \cdots + 10a_{k-1} + a_k$$

$10 \underset{\bmod 3}{\equiv} 1$, לכן $10^2 \underset{\bmod 3}{\equiv} 1^2 = 1$, ובאינדוקציה על החזקה מקבלים כי לכל $i \geq 1$, $10^i \underset{\bmod 3}{\equiv} 1$. לכן:

$$10^{k-1}a_1 + 10^{k-2}a_2 + \cdots + 10a_{k-1} + a_k \underset{\bmod 3}{\equiv} 1\cdot a_1 + 1\cdot a_2 + \cdots + 1\cdot a_{k-1} + a_k$$

כלומר:

$$n \underset{\bmod 3}{\equiv} a_1 + \cdots + a_{k-1} + a_k$$

או:

$$n_{\bmod 3} = (a_1 + \cdots + a_{k-1} + a_k)_{\bmod 3}$$

אם כן, שארית החילוק ב־ 3 של n, שווה לשארית החילוק ב־ 3 של סכום ספרותיו. בפרט, n מתחלק ב־ 3 אם ורק אם סכום ספרותיו מתחלק ב־ 3.

שאלה 5.2.8

יהי n מספר טבעי.

א. הוכיחו ש־ n מתחלק ב־ 9 אם ורק אם סכום הספרות שלו מתחלק ב־ 9.

ב. בדקו האם המספר 123554524987738785 מתחלק ב־ 3; ב־ 9.

התשובה בעמוד 41

שאלה 5.2.9 (שאלת רשות)

יהי n מספר טבעי. מצאו קריטריון חישובי לבדוק האם n מתחלק ב־11. בדקו האם 123554524987738785 מתחלק ב־11.

התשובה בעמוד 41

5.3 המשפט היסודי של האריתמטיקה

בסעיף זה נוכיח את אחד המשפטים החשובים בתורת המספרים - המשפט היסודי של האריתמטיקה. לאחר מכן נשתמש במשפט זה כדי להוכיח תכונה יסודית של המספרים הראשוניים.

הגדרה 5.3.1 מספר ראשוני

נאמר שמספר טבעי $n \geq 2$ הוא **ראשוני** אם המספרים הטבעיים היחידים המחלקים אותו הם 1 ו־n. מספר טבעי $n \geq 2$ שאינו ראשוני (כלומר מספר שיש לו מחלק טבעי נוסף, פרט לעצמו ול־1), נקרא מספר **פריק**.

הערות

א. שימו לב, לצורך ההגדרה זו אנו בוחנים רק מחלקים טבעיים (כלומר, שלמים חיוביים). למספר 2, למשל, יש ארבעה מחלקים **שלמים** - $1, 2, -1, -2$, אך רק שני מחלקים **טבעיים** - $1, 2$, ולכן הוא מספר ראשוני.

ב. שימו לב לדרישה $n \geq 2$. איננו רואים את המספר 1 כראשוני, למרות שהוא מתחלק רק ב־1 (הוא עצמו).

ג. כיצד בודקים אם מספר נתון n הוא ראשוני? אפשר, כמובן, לעבור על כל המספרים הטבעיים עד n, ולבדוק אילו מהם מחלקים אותו. עבור מספרים גדולים בדיקה זו עלולה להיות מייגעת מאוד. באמצעים פשוטים למדי אפשר לייעל את הבדיקה,[1] אך לא נעסוק בכך במסגרת קורס זה.

ד. הנה רשימה של כל המספרים הראשוניים עד 50:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$$

ה. כל מספר זוגי מתחלק ב־2. לכן 2 הוא הראשוני הזוגי היחיד.

בהערה ד לעיל מנינו את כל המספרים הראשוניים עד 50. תוכלו להמשיך עוד ועוד כרצונכם, על־ידי בדיקת כל מספר לעצמו (כמובן, ככל שמתקדמים, הבדיקה מתארכת). נשאלת השאלה: האם הרשימה מסתיימת מתישהו? מסתבר שלא: רשימת המספרים הראשוניים היא אינסופית. זוהי אחת התוצאות העתיקות בתורת המספרים, שהוכחה לראשונה על־ידי המתמטיקאים היוונים. לפני שנוכיח את המשפט, נוכיח את הלמה הבאה:

למה 5.3.2

כל מספר טבעי $n \geq 2$ מתחלק במספר ראשוני.

---

1 תוכלו להשתכנע בקלות כי מספיק לנסות לחלק את המספר n בכל המספרים הטבעיים שאינם עולים על $\sqrt{n}$, אך גם בדיקה זו עלולה לארוך זמן רב מאוד עבור ערכי n גדולים.

הוכחה

נניח בשלילה שטענת הלמה אינה מתקיימת. אזי קיימים מספרים טבעיים גדולים מ־1 שאינם מתחלקים במספר ראשוני, ונסמן ב־ n את המספר הטבעי המזערי מביניהם. בפרט, n איננו ראשוני (משום שהוא מתחלק בעצמו). לכן, קיים k טבעי המחלק את n כך ש־ $1 < k < n$. לאור הנחת המזעריות על n, המספר k מתחלק במספר ראשוני כלשהו, נאמר p. אך מכיוון ש־ p מחלק את k ו־ k מחלק את n, p מחלק את n, סתירה.

מ.ש.ל.

משפט 5.3.3

יש אינסוף מספרים ראשוניים.

הוכחה

נניח בשלילה שיש רק מספר סופי של מספרים ראשוניים, ונסמנם $p_1, p_2, \ldots, p_n$. נתבונן במספר $k = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. לכל $1 \le i \le n$, שארית החילוק של k ב־ p_i היא 1, לכן k אינו מתחלק באף אחד מהראשוניים האלה. אך לפי הנחתנו - אלה **כל** המספרים הראשוניים, ולכן k אינו מתחלק באף מספר ראשוני, בסתירה ללמה 5.3.2.

מ.ש.ל.

למה 5.3.4

כל מספר טבעי $n \ge 2$ הוא ראשוני, או מכפלה של כמה מספרים ראשוניים.

הוכחה

נוכיח את הטענה באינדוקציה על n. עבור $n = 2$ הטענה נכונה, שהרי 2 ראשוני. נניח שהטענה נכונה לכל אחד מן המספרים $2, \ldots, n-1$, כלומר שכל אחד מאלה הוא ראשוני או מכפלה של ראשוניים, ונוכיח את הטענה עבור n. אם n ראשוני, סיימנו. אחרת, לפי למה 5.3.2, n מתחלק בראשוני p, שבהכרח קטן ממנו. נסמן ב־ k את מנת החילוק של n ב־ p, כלומר $n = kp$. בהכרח $k \ge 2$, כי אם $k = 1$ אז $n = p$ הוא ראשוני. כמו כן, בהכרח מתקיים $k < n$, כי $p \ge 2$. לפי הנחת האינדוקציה, נוכל לכתוב את k כמכפלה $p_1 \cdot p_2 \cdot \ldots \cdot p_n$ של מספרים ראשוניים. מכאן נקבל הצגה של n כמכפלה של ראשוניים:

$$n = k \cdot p = p_1 \cdot p_2 \cdot \ldots \cdot p_n \cdot p$$

מ.ש.ל.

ניתן לראות מספר ראשוני p כמכפלה בת גורם אחד (המספר עצמו) של מספרים ראשוניים. טענה 5.3.4 קובעת שכל מספר טבעי n, $n \ge 2$, הוא מכפלה של ראשוניים. המספרים הראשוניים הם אפוא מעין אבני בניין שמהם נוצרים, באמצעות כפל, כל המספרים הטבעיים.

שאלה 5.3.1

כתבו את המספרים $7, 21, 24$ כמכפלות של ראשוניים.

התשובה בעמוד 42

כעת נשאל: בכמה דרכים אפשר לכתוב מספר טבעי נתון כמכפלה של ראשוניים?

נתבונן במספר $n = 6$. נוכל להציג אותו כמכפלה של ראשוניים כך: $n = 2 \cdot 3$. נוכל, כמובן, לכתוב גם $n = 3 \cdot 2$. תוכלו לבדוק ישירות, כי אלה שתי הדרכים היחידות לכתוב את 6 כמכפלה של מספרים ראשוניים. כמובן, יש קשר הדוק בין שתי ההצגות הללו - למעשה, זוהי אותה ההצגה, רק בשינוי סדר הגורמים. נאמר מעתה כי קיימת דרך **יחידה, עד כדי סדר הגורמים**, להציג את 6 כמכפלה של מספרים ראשוניים.

דוגמה

נתבונן במספר $n = 18$. תוכלו לוודא ישירות, כי ההצגות היחידות של 18 כמכפלה של ראשוניים הן:

$$18 = 2 \cdot 3 \cdot 3 = 3 \cdot 2 \cdot 3 = 3 \cdot 3 \cdot 2$$

גם ל־ 18 יש אפוא הצגה יחידה, עד כדי סדר הגורמים, כמכפלה של ראשוניים. שימו לב כי בהצגה יחידה זו, הגורם הראשוני 3 מופיע פעמיים.

קל לבדוק ישירות שגם למספרים $15, 25, 30$ יש הצגה יחידה כמכפלה של ראשוניים, עד כדי סדר הגורמים.[2]

זו איננה תופעה מקרית - כל מספר טבעי ניתן להצגה יחידה, עד כדי סדר הגורמים, כמכפלה של מספרים ראשוניים. ◀

משפט 5.3.5 המשפט היסודי של האריתמטיקה

כל מספר טבעי $n \geq 2$ ניתן להצגה **יחידה**, עד כדי סדר הגורמים,[3] כמכפלה של מספרים ראשוניים.

הוכחה[4]

קיומה של ההצגה הוכח בלמה 5.3.4. האתגר כעת הוא להראות את יחידותה.

נניח בשלילה שיש מספרים טבעיים, אשר הצגתם כמכפלה של גורמים ראשוניים אינה יחידה.

יהי N המספר הטבעי הקטן ביותר שיש לו יותר מהצגה אחת כמכפלה של ראשוניים.

המספר N אינו ראשוני, כי ההצגה של מספר ראשוני p כ־ $p = p$ ("מכפלה" בת גורם אחד), היא ההצגה היחידה שלו כמכפלה של ראשוניים. בכל פירוק של N לגורמים ראשוניים ישנם לפחות 2 גורמים.

2 הנה ההצגות: $30 = 2 \cdot 3 \cdot 5, \quad 25 = 5 \cdot 5, \quad 15 = 3 \cdot 5$.

3 מעתה נקצר ונאמר "הצגה יחידה", כאשר כוונתנו תמיד ל"הצגה יחידה עד כדי סדר הגורמים".

4 הוכחת משפט 5.3.5 היא בחזקת חומר רשות.

תהיינה אפוא $q_1 \cdot q_2 \cdot \ldots \cdot q_m$,$p_1 \cdot p_2 \cdot \ldots \cdot p_k$ הצגות **שונות** של N כמכפלת ראשוניים.

(1) $$N = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_m$$

נוכל להניח, בלא הגבלת הכלליות, כי

$$p_1 \le p_2 \le \cdots \le p_k$$

$$q_1 \le q_2 \le \cdots \le q_m$$

וכן כי:

$$p_1 \le q_1$$

מההנחה האחרונה נובע שמתקיימת בדיוק אחת משתי האפשרויות: $p_1 = q_1$ או $p_1 < q_1$.
בכל מקרה, נצביע על מספר טבעי M קטן מ־N, שיש לו שתי הצגות שונות כמכפלה של ראשוניים, בסתירה למזעריות של N.

א. $p_1 = q_1$. במקרה זה נבחר:

$$M = p_2 \cdot \ldots \cdot p_k$$

$p_1 \ge 2$, לכן $M < p_1 M = N$, כלומר:

$$M < N$$

לאור (1), מן השוויון $p_1 = q_1$ נובע כי

$$N = p_1 \cdot p_2 \cdot \ldots \cdot p_k = p_1 \cdot q_2 \cdot \ldots \cdot q_m$$

ולכן:

$$M = p_2 \cdot \ldots \cdot p_k = q_2 \cdot \ldots \cdot q_m$$

$p_2 \cdot \ldots \cdot p_k$ ו־ $q_2 \cdot \ldots \cdot q_m$ הן הצגות **שונות** של M כמכפלת ראשוניים, כי אילו היה $k = m$, ולכל i, $2 \le i \le k$, היה $p_i = q_i$, אז מכך ובתוספת $p_1 = q_1$, היינו מקבלים ש־ $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ ו־ $q_1 \cdot q_2 \cdot \ldots \cdot q_m$ הן אותה הצגה של N.
אם כן, $M < N$, וההצגה של M כמכפלת ראשוניים איננה יחידה.

ב. $p_1 < q_1$. במקרה זה נבחר:

(2) $$M = (q_1 - p_1) q_2 \cdot \ldots \cdot q_m$$

לפי (1),

(3) $$M = q_1(q_2 \cdot \ldots \cdot q_m) - p_1(q_2 \cdot \ldots \cdot q_m) = N - p_1(q_2 \cdot \ldots \cdot q_m) < N$$

בהכרח מתקיים $p_1 > 2$, כי אם $p_1 = 2$, אז מכך ש־ $N = p_1 \cdots p_k$ נקבל ש־ N זוגי, בעוד שמההצגה $N = q_1 \cdots q_m$, שכל הראשוניים המופיעים בה גדולים מ־ 2, ולכן אי־זוגיים, נקבל ש־ N אי־זוגי.

מכך ש־ $2 < p_1 < q_1$ נובע ש־ p_1, q_1 שניהם אי־זוגיים, ולכן:

$$2 \le (q_1 - p_1)$$

המספר $(q_1 - p_1)$ ניתן אפוא להצגה כמכפלה של ראשוניים. יהיו $r_1, \ldots, r_s$ מספרים ראשוניים (אחד או יותר), כך ש־

(4) $$(q_1 - p_1) = r_1 \cdot \ldots \cdot r_s$$

נוכיח ש־ p_1 שונה מכל ה־ r_i־ים. אכן, אם $p_1 = r_i$ לאיזשהו i, אז p_1 מחלק את $(q_1 - p_1)$, ולכן p_1 מחלק את q_1. אבל $1 < p_1 < q_1$, וזו סתירה לראשוניות q_1.

לפי (2) (הגדרת M) ו־(4):

$$M = r_1 \cdot \ldots \cdot r_s \cdot q_2 \cdot \ldots \cdot q_m \qquad (5)$$

ב־(5) מוצג M כמכפלה של ראשוניים ש־ p_1 לא מופיע ביניהם, כי כבר הראינו ש־ p_1 שונה מכל r_i, ו־ p_1 שונה גם מכל אחד מבין $q_2, \ldots, q_m$, שהרי $p_1 < q_2 \leq \ldots \leq q_m$.
כעת נמצא הצגה של M כמכפלה של ראשוניים, שבה p_1 מופיע.
לפי (3):

$$M = N - p_1 \cdot q_2 \cdot \ldots \cdot q_m$$

היות ש־ N מתחלק ב־ p_1 (לפי (1)), גם M מתחלק ב־ p_1. נוכל לבטא אפוא:

$$M = p_1 \cdot u \qquad (6)$$

אם $u = 1$ אז

$$M = p_1$$

ואם $u \geq 2$ אז ניתן להציגו כמכפלת ראשוניים, נאמר

$$u = t_1 \cdot \ldots \cdot t_l$$

ואז לפי (6):

$$M = p_1 \cdot t_1 \cdot \ldots \cdot t_l$$

אם כן, בכל מקרה:

$$M = p_1 \cdot t_1 \cdot \ldots \cdot t_l \text{ או } M = p_1 \qquad (7)$$

ל־ M יש אפוא הצגה כמכפלה של (אחד או יותר) גורמים ראשוניים, שבה p_1 מופיע.
ההצגות (5) ו־(7) הן הצגות שונות של M כמכפלת ראשוניים, שהרי p_1 מופיע באחת אך לא באחרת.

אם כן, גם הפעם מצאנו $M < N$, שההצגה שלו כמכפלת ראשוניים איננה יחידה.
הנחת השלילה, שלפיה יש מספרים שפירוקם לגורמים ראשוניים אינו יחיד, הובילה לסתירה. מכך נסיק שההצגה של כל מספר טבעי גדול מ־1 כמכפלת ראשוניים היא יחידה.

מ.ש.ל.

הערה

בניסוח המשפט הנחנו כי $n \geq 2$. נוכל אף להכליל את המשפט למקרה ה"טריוויאלי" שבו $n = 1$, אם נחשוב על המספר 1 כעל מכפלה "ריקה" – כלומר מכפלה של אפס גורמים ראשוניים. מעתה נאמץ מוסכמה זו, המאפשרת לנסח את המשפט היסודי של האריתמטיקה באופן אלגנטי יותר:

- **כל מספר טבעי ניתן להצגה יחידה כמכפלה של מספרים ראשוניים.**

למשפט היסודי מסקנות שימושיות רבות, ותורת המספרים כולה נשענת עליו. נביא מסקנה יסודית אחת, שתשמש אותנו בסעיף הבא:

מסקנה 5.3.6

יהי p מספר ראשוני. אם a,b מספרים טבעיים כך ש־ $p|ab$, אזי בהכרח $p|a$ או $p|b$.

הוכחה

נכתוב את a,b כמכפלות של מספרים ראשוניים: $a = p_1 \cdot p_2 \cdot \ldots \cdot p_r, \quad b = q_1 \cdot q_2 \cdot \ldots \cdot q_s$. לפי הנתון, קיים טבעי c כך ש־ $ab = pc$. בהצגה של pc כמכפלה של מספרים ראשוניים מופיע p, לכן גם בהצגה $ab = p_1 \cdot p_2 \cdot \ldots \cdot p_r \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_s$ מופיע p. כלומר $p = p_i$ או $p = q_i$, עבור איזשהו אינדקס i. במקרה הראשון $p|a$, ובשני $p|b$.

מ.ש.ל.

שאלה 5.3.2

הראו שגם הטענה ה"הפוכה" לטענת מסקנה 5.3.6 נכונה, כלומר הראו: אם $p \geq 2$ הוא מספר טבעי בעל התכונה, שאם הוא מחלק מכפלה ab של מספרים שלמים, אז הוא מחלק לפחות אחד מבין a,b, אז p הוא ראשוני.[5]

התשובה בעמוד 42

שאלה 5.3.3

השתמשו במשפט היסודי של האריתמטיקה כדי להוכיח את העובדה הקלאסית: המספר הממשי $\sqrt{2}$ אינו רציונלי. הדרכה: הניחו בשלילה כי $\sqrt{2}$ מספר רציונלי, כתבו אותו כמנה של שני מספרים שלמים, ותנו את דעתכם למספר הפעמים שהראשוני 2 מופיע בפירוק לראשוניים של המונה והמכנה (אם הוא מופיע כלל).

התשובה בעמוד 42

שאלה 5.3.4

יהי p מספר ראשוני. הוכיחו את התוצאות הבאות על סמך מסקנה 5.3.6:

א. אם a,b מספרים **שלמים** כך ש־ $p|ab$, אזי בהכרח $p|a$ או $p|b$.

ב. אם a מספר שלם, n מספר טבעי, ו־ $p|a^n$, אזי $p|a$.

התשובה בעמוד 42

5 אם כן, התכונה המופיעה במסקנה 5.3.6 מאפיינת את המספרים הראשוניים, ולכן ניתן להשתמש בה כאפיון חלופי למספרים הראשוניים. למעשה, טבעי יותר להשתמש בתכונה זו להגדרת המספרים הראשוניים – הגדרה זו מאפשרת להרחיב את המושג "ראשוני" לעצמים החורגים מעולם המספרים השלמים – אך בכך לא נעסוק במסגרת קורס זה.

5.4 שדות ראשוניים

בסעיף זה נענה על השאלה שבה סיימנו את סעיף 5.2 – עבור אילו ערכי $n \geq 2$ החוג $\mathbb{Z}_n$ הוא שדה?

משפט 5.4.1

יהי $n \geq 2$ מספר טבעי. הקבוצה $\mathbb{Z}_n$, עם פעולות החיבור והכפל מודולו n, מהווה שדה אם ורק אם n הוא מספר ראשוני.

הכלי המרכזי שעליו נישען בהוכחת משפט 5.4.1 הוא מסקנה 5.3.6. תחילה נוכיח את הלמה הבאה:[1]

למה 5.4.2

תהי A קבוצה סופית, ותהי f פונקציה מ־A ל־A. אזי f חד־חד־ערכית אם ורק אם f על.

הוכחה

בלא הגבלת הכלליות, נניח כי A איננה ריקה.[2] נניח כי ב־A ישנם n איברים, ונסמן $A = \{a_1, \ldots, a_n\}$. אם f חד־חד־ערכית, אזי האיברים $f(a_1), \ldots, f(a_n)$ כולם שונים זה מזה – ולכן מדובר ב־n איברים שונים. כלומר, בקבוצה $\operatorname{Im} f = f(A) = \{f(a_1), \ldots, f(a_n)\}$ החלקית ל־A, יש n איברים – כמספר איברי A, ולכן זוהי הקבוצה A כולה. נסיק אפוא ש־f על.

להפך, אם f איננה חד־חד ערכית, פירוש הדבר הוא כי לפחות שניים מבין האיברים $f(a_1), \ldots, f(a_n)$ מתלכדים, ולכן בקבוצה $f(A) = \{f(a_1), \ldots, f(a_n)\}$ יש לכל היותר $n-1$ איברים, וממילא f איננה על.

מ.ש.ל.

הוכחת משפט 5.4.1

תחילה נניח כי n מספר ראשוני. כדי להראות ש־$\mathbb{Z}_n$ הוא שדה, נותר לנו להראות (ראו דיון בסוף סעיף 5.2) כי לאיבר $a \in \mathbb{Z}_n$ השונה מאפס יש הופכי. כדי להראות זאת, נתבונן בפונקציה $f_a : \mathbb{Z}_n \to \mathbb{Z}_n$ המוגדרת על־ידי $f_a(k) = a \cdot_n k$. תחילה נראה כי פונקציה זו היא חד־חד־ערכית. אכן, נניח כי $f_a(k) = f_a(m)$ עבור $k, m \in \mathbb{Z}_n$ כלשהם, כאשר בלא הגבלת הכלליות נניח ש־$k \geq m$. אזי $a \cdot_n k = a \cdot_n m$, ולכן מתקיים לפי למה 5.2.8, $a \cdot_n (k-m) = 0$, כלומר $n \mid a \cdot (k-m)$. אך מכיוון ש־n מספר ראשוני, נסיק לפי שאלה 5.3.2 ש־$n \mid a$ או $n \mid (k-m)$. האפשרות הראשונה לא תיתכן, כי הנחנו ש־$0 \neq a \in \mathbb{Z}_n$. האפשרות השנייה, שבהכרח מתקיימת, פירושה ש־$n \mid k-m$, אך $0 \leq k-m \leq k < n$, ולכן $k-m$ הוא אפס, כלומר $k = m$.

1 למה זו איננה שייכת לתחום האלגברה – זוהי טענה כללית אודות פונקציות על קבוצות סופיות, וייתכן שכבר נתקלתם בה במהלך לימודיכם.

2 לא קיימות פונקציות מקבוצה ריקה לעצמה, ולכן במקרה זה **הטענה מתקיימת באופן ריק**.

בזאת הראינו שהפונקציה f_a היא חד־חד־ערכית, ולכן לפי למה 5.4.2 היא גם על. בפרט קיים $b \in \mathbb{Z}_n$ כך ש־ $f_a(b) = a \cdot_n b = 1$. כלומר, האיבר $b \in \mathbb{Z}_n$ הוא הופכי ל־ a. נסיק ש־ $\mathbb{Z}_n$ שדה.

בכיוון ההפוך, נניח כי n הוא מספר פריק, כלומר ש־ n ניתן לכתיבה בצורה $n = ab$, כאשר $1 < a,b < n$. נניח בשלילה ש־ $\mathbb{Z}_n$ הוא שדה. השוויון $n = ab$ (במספרים השלמים) פירושו $a \cdot_n b = 0$, ולכן בשדה $\mathbb{Z}_n$ מתקיים $ab = 0$. אך מאחר ש־ $1 < a,b < n$, בשדה $\mathbb{Z}_n$ מתקיים $a,b \neq 0$. בזאת קיבלנו סתירה למסקנת שאלה 1.2.3.

מ.ש.ל.

משפט 5.4.1 נותן בידינו משפחה של שדות סופיים - משפחת השדות מהצורה $\mathbb{Z}_p$, לכל p ראשוני. שדות אלה נקראים **שדות ראשוניים**. נציין שגם שדה המספרים הרציונליים $\mathbb{Z}$ מכונה שדה ראשוני, למרות שמספר איבריו אינסופי ולא מספר טבעי ראשוני. לא נסביר כאן מדוע, אך נציין ששדה זה, ואוסף השדות מהצורה $\mathbb{Z}_p$, הם **כל** השדות המכונים במתמטיקה **שדות ראשוניים**.

במהלך הוכחת משפט 5.4.1 הראינו שעבור p ראשוני יש ב־ $\mathbb{Z}_p$ הופכי לכל איבר שאינו אפס - אך לא הצבענו על דרך למציאת ההופכי. עבור ראשוניים גדולים, יש צורך בשיטה יעילה לביצוע משימה זו. בסעיף 5.6, שהוא בחזקת חומר רשות, נתאר שיטה כזאת - ואתם מוזמנים לעיין בו. עם זאת, עבור ראשוניים קטנים, נוכל למצוא כל הופכי באופן ישיר, על־ידי בדיקת כל איברי השדה, כפי שהדגמנו בסוף סעיף 5.2. לאור זאת, עבור ראשוניים קטנים מצויים בידיכם כל הכלים לביצוע כל פעולות החשבון הבסיסיות בשדה $\mathbb{Z}_p$ - חיבור, חיסור, כפל, וחילוק.

שאלה 5.4.1

בשדות $\mathbb{Z}_{17}$ ו־ $\mathbb{Z}_{31}$, מצאו את ההופכיים לאיברים 3, 12.

התשובה בעמוד 42

שאלה 5.4.2

א. בשדה $\mathbb{Z}_{17}$, חשבו את $(15/12) \cdot 5 + 3$.

ב. בשדה $\mathbb{Z}_{31}$, חשבו את $(14/12) \cdot (17/3)$.

ג. בשדה $\mathbb{Z}_7$, חשבו את $(-13/3) \cdot (15/3) / (13/9)$.

התשובה בעמוד 42

את הידע שצברנו על אודות ביצוען הטכני של פעולות החישוב בשדות ראשוניים (קטנים), נוכל לנצל כדי לפתור בעיות באלגברה לינארית, כגון פתרון מערכות משוואות, היפוך מטריצות וחישוב דטרמיננטות. בתרגילים הבאים תתבקשו לפתור שאלות מסוג זה. פתרו את השאלות בדיוק באותו באופן שתרגלתם בפרקים הקודמים (שבהן הדוגמאות היו לרוב מעל הממשיים), כאשר אתם מבצעים את פעולות החשבון בשדה המתאים.

שאלה 5.4.3

פתרו את מערכת המשוואות הבאה מעל השדה $\mathbb{Z}_{11}$:

$$\begin{aligned} 3x + \; y + z &= 1 \\ 2x + \; y + 3z &= 2 \\ x + 2y + 3z &= 1 \end{aligned}$$

התשובה בעמוד 43

שאלה 5.4.4

פתרו את מערכת המשוואות הבאה מעל השדה $\mathbb{Z}_{13}$:

$$\begin{aligned} x + y \quad &= 0 \\ x \quad + z &= 1 \\ y + z &= 1 \end{aligned}$$

התשובה בעמוד 43

שאלה 5.4.5

מעל השדה $\mathbb{Z}_{13}$, בדקו אם המטריצה הבאה הפיכה, ואם כן - מצאו את המטריצה ההופכית לה:

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

התשובה בעמוד 44

שאלה 5.4.6

מעל השדה $\mathbb{Z}_{17}$, חשבו את הדטרמיננטה הבאה:

$$\begin{vmatrix} 3 & 2 & 0 & 1 \\ 1 & 3 & 0 & 16 \\ 1 & 0 & 2 & 1 \\ 2 & 1 & 0 & 2 \end{vmatrix}$$

התשובה בעמוד 44

שאלה 5.4.7

בדקו האם הוקטורים $(1,0,3),(1,2,4),(2,2,2) \in (\mathbb{Z}_5)^3$ תלויים לינארית (מעל $\mathbb{Z}_5$).

התשובה בעמוד 44

5.5 שדות סופיים שאינם ראשוניים

סעיף זה הוא סעיף רשות.

ראינו בסעיף הקודם כי $\mathbb{Z}_n$ הוא שדה אם ורק אם n הוא מספר ראשוני. האם נוכל להסיק שהשדות הסופיים היחידים הם כאלה שמספר האיברים בהם הוא מספר ראשוני? לא! כל שהראינו הוא שהקבוצה $\mathbb{Z}_n$, עם הפעולות שהגדרנו, אינה מהווה שדה כאשר n אינו ראשוני. אך א־פריורי אין מניעה לקיומה של קבוצה אחרת בת n איברים (עם פעולות חיבור וכפל מסוימות) המהווה שדה. אכן, מיד נראה דוגמה לשדה סופי שמספר איבריו אינו ראשוני. האם קיים שדה בן n איברים לכל $n \geq 2$? מתברר שלא.

משפט 5.5.1
יהי $n \geq 2$ מספר טבעי. קיים שדה בן n איברים אם ורק אם n הוא **חזקה** של מספר ראשוני.

ממשפט 5.5.1 נובע, בפרט, כי קיימים שדות בני $5^3 = 125$, $3^2 = 9$, $2^3 = 8$ ו־ $2^{12} = 4096$ איברים, אך לא קיים שדה בן 6 איברים.

לא נוכיח את משפט 5.5.1 במסגרת קורס זה, אך נביא דוגמה אחת לשדה סופי שמספר איבריו אינו ראשוני. לאור משפט 5.5.1, השדה הקטן ביותר שמספר איבריו אינו ראשוני הוא בן $2^2 = 4$ איברים. אנו נבנה שדה זה באופן דומה לאופן שבו בנינו שדה בן שני איברים בפרק 1 (מומלץ שתחזרו ותעיינו בסעיף 1.2) – ניקח קבוצה בת ארבעה איברים, וננסה לחלץ את טבלאות החיבור והכפל מתוך אקסיומות השדה (התנאים המופיעים בהגדרת השדה).

כדי להגדיר את השדה, תחילה עלינו לבחור את קבוצת איבריו. "תפקידיהם" של שניים מהאיברים מוכתב לנו מראש – איבר האפס, שאותו נסמן ב־ 0, ואיבר היחידה, שאותו נסמן ב־1. על שני האיברים האחרים איננו יודעים דבר, א־פריורי, ולכן נסמן אותם באמצעות זוג סמלים שרירותי, למשל x, y. הקבוצה היא, אם כן, $F = \{0, 1, x, y\}$. ברצוננו לבנות טבלאות פעולה, אחת עבור החיבור (בשדה שאותו אנו מנסים לבנות), ואחת עבור הכפל, כך שכל התנאים בהגדרת השדה יתקיימו. חלק משורות הטבלאות ועמודות הטבלאות מוכתב לנו מכך ש־ 0 ניטרלי ביחס לחיבור, 1 ניטרלי ביחס לכפל, ומכך שלכל $a \in F$ מתקיים $a \cdot 0 = 0$:

$+$	0	1	x	y
0	0	1	x	y
1	1			
x	x			
y	y			

$\cdot$	0	1	x	y
0	0	0	0	0
1	0	1	x	y
x	0	x		
y	0	y		

כדי למלא את שאר השורות, נסתמך על העובדה שכל איבר של השדה מופיע בהכרח בכל אחת מהן (מדוע?). למשל, נבדוק מהו $x^2 (= x \cdot x)$: לא ייתכן כי $x^2 = 0$, כי אז (על־ידי כפל ב־ x^{-1}) נקבל

$x = 0$. באופן דומה, לא ייתכן כי $x^2 = x$, כי אז $x = 1$. אם $x^2 = 1$, אז $xy = y$ (כי בשורה השלישית של טבלת הכפל צריך להופיע כל איבר), ולכן $x = 1$, סתירה.

נסיק אפוא שבהכרח $x^2 = y$, וכדי להשלים את השורה השלישית בטבלת הכפל, בהכרח מתקיים $xy = 1$. באופן דומה, $y^2 = x$. כלומר קיבלנו שטבלת הכפל היא:

$\cdot$	0	1	x	y
0	0	0	0	0
1	0	1	x	y
x	0	x	y	1
y	0	y	1	x

נותר להשלים את טבלת החיבור. תחילה נשאל מהו -1 (כלומר, מהו האיבר הנגדי ל־1)? לא ייתכן $-1 = 0$, כי אז $1 = 0$. אם $-1 = x$, אז

$$0 = x0 = x(1 + x) = x + x^2 = x + y$$

ולכן $x = -y$. נסיק ש־ $-y = -1$, ולכן $y = 1$, סתירה. לכן לא ייתכן כי $x = -1$. באופן דומה מראים כי לא ייתכן ש־ $y = -1$. לכן נותרנו עם האפשרות $-1 = 1$, כלומר $1 + 1 = 0$. מכאן נקבל: $0 = x0 = x(1 + 1) = x + x$, ובאופן דומה $y + y = 0$. טבלת החיבור בשלב זה נראית כך:

$+$	0	1	x	y
0	0	1	x	y
1	1	0		
x	x		0	
y	y			0

לא ייתכן ש־ $x = 1 + x$, כי אז $1 = 0$. לכן בהכרח $y = 1 + x$. באופן דומה, $x = 1 + y$.

$+$	0	1	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	
y	y	x		0

הערך האפשרי היחיד שנותר עבור $x + y$ הוא 1, ובזאת השלמנו את טבלת החיבור:

$+$	0	1	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	1
y	y	x	1	0

שימו לב, לא הוכחנו שהקבוצה הנידונה, בצירוף זוג הפעולות המתוארות בטבלאות שבנינו, מהווה שדה. כל שהראינו הוא ש**אם** ניתן להגדיר פעולות על הקבוצה ההופכות אותה לשדה, הרי בהכרח פעולות אלה מתוארות על־ידי הטבלאות שבנינו. עתה יש לבדוק שהפעולות המתוארות אכן מקיימות את כל תנאי הגדרה 1.2.1. בדיקה זו נשאיר לכם.

5.6 האלגוריתם של אוקלידס

סעיף זה הוא סעיף רשות.

בסעיף זה נתאר שיטה יעילה למציאת ההופכי של איבר בכל שדה סופי ראשוני.

בהינתן מספר **שלם** n השונה מאפס, נסמן ב־$[n]$ את אוסף כל המספרים הטבעיים המחלקים את n.[1] אוסף זה הוא קבוצה סופית של מספרים טבעיים הכוללת בהכרח את 1. למשל: $[1]=\{1\},\ [2]=\{1,2\},\ [3]=\{1,3\},\ [4]=\{1,2,4\}$.

באופן דומה, גם $[-1]=\{1\},\ [-2]=\{1,2\},\ [-3]=\{1,3\},\ [-4]=\{1,2,4\}$, מאחר שלכל מספר שלם n, המחלקים הטבעיים של n הם המחלקים הטבעיים של $-n$.

שאלה 5.6.1

כתבו את $[5],[6],[7],[8],[9],[10]$.

התשובה בעמוד 45

בהינתן זוג מספרים שלמים שונים מאפס[2] n,m, נסמן ב־$[n,m]$[3] את אוסף המספרים הטבעיים המחלקים את n וגם את m. כלומר, $[n,m]=[n]\cap[m]$.

למשל: $[6,9]=\{1,2,3,6\}\cap\{1,3,9\}=\{1,3\}$. ברור כי $[n,m]=[m,n]$.

שאלה 5.6.2

חשבו את $[12,1],[12,2],[12,5],[12,6],[12,12],[12,15]$.

התשובה בעמוד 45

למה 5.6.1

לכל מספר שלם n השונה מאפס מתקיים:

א. $[n,1]=\{1\}$.

ב. $[n,n]=[n]$.

ג. $[n,m]=[m]$ לכל שלם m המחלק את n.

הוכחה

חלקים א ו־ב הם מקרה פרטי של חלק ג. נוכיח את חלק ג: אם m מחלק את n אז $[m]\subseteq[n]$, ולכן $[n,m]=[m]\cap[n]=[m]$.

מ.ש.ל.

1 זהו סימון זמני, למען הנוחות, שישמש אותנו בפרק זה בלבד.

2 אנו מדירים את אפס מן הדיון הנוכחי, משום ש**כל** מספר שלם מחלק אותו.

3 גם סימון זה מוגבל לפרק הנוכחי.

הגדרה 5.6.2 מחלק משותף מרבי

יהיו n,m מספרים שלמים שונים מאפס. למספר הגדול ביותר בקבוצה $[n,m]$ קוראים **המחלק המשותף המְרַבִּי** של n ו־ m, ומסמנים אותו ב־ $\gcd(n,m)$.[4] כלומר, $\gcd(n,m)$ הוא המספר הטבעי הגדול ביותר המחלק גם את n וגם את m.

דוגמה

מאחר ש־ $[6,9] = \{1,3\}$, מתקיים $\gcd(6,9) = 3$;

מאחר ש־ $[14,-8] = \{1,2,7,14\} \cap \{1,2,4,8\} = \{1,2\}$, מתקיים $\gcd(14,-8) = 2$;

מאחר ש־ $[5,-9] = \{1,5\} \cap \{1,3,9\} = \{1\}$ מתקיים $\gcd(5,-9) = 1$. ◀

שאלה 5.6.3

חשבו את $\gcd(12,1), \gcd(12,2), \gcd(12,5), \gcd(12,12), \gcd(12,15)$.

התשובה בעמוד 46

הערה

יש המרחיבים את הגדרת המחלק המשותף המרבי גם למקרה שבו אחד המספרים הוא אפס, והשני שונה מאפס. במקרה זה, המחלק המשותף המרבי יהיה המספר השני בערכו המוחלט, שכן כל מספר שלם מחלק את אפס. כך למשל, $\gcd(0,-3) = 3$.

למה 5.6.3

לכל n שלם מתקיים:

א. $\gcd(n,1) = 1$.

ב. $\gcd(n,n) = n$.

ג. $\gcd(n,m) = |m|$[5] לכל שלם m המחלק את n.

הוכחה

חלקים א ו־ב הם מקרה פרטי של חלק ג. נוכיח את חלק ג. אם m מחלק את n, אז לפי חלק ג של למה 5.6.1 המחלקים הטבעיים המשותפים של n ו־ m הם בדיוק המחלקים הטבעיים של m. הגדול מביניהם הוא m אם m חיובי, ו־ $-m$ אם m שלילי. כלומר:

$$\gcd(n,m) = |m|$$

מ.ש.ל.

כיצד נמצא את המחלק המשותף המרבי של זוג מספרים שלמים n,m? הדרך הברורה מאליה היא לכתוב במפורש את כל המחלקים הטבעיים המשותפים (כלומר, את איברי $[n,m]$) ולמצוא את

4 gcd הם ראשי התיבות של greatest common divisor – מחלק משותף מרבי.

5 $|m|$ הוא הערך המוחלט של m. שימו לב כי זהו תמיד המספר הגדול ביותר בקבוצה $[m]$ (בהנחה ש- $m \neq 0$).

האיבר הגדול ביותר בקבוצה זו. עבור מספרים גדולים, דרך זו אינה מעשית. דרך יעילה לחישוב המחלק המשותף המרבי מכונה **האלגוריתם של אוקלידס**. שיטה זו מבוססת על ההבחנה הבאה:

טענה 5.6.4

יהי a מספר **שלם** ויהי b מספר **טבעי**. יהיו q,r זוג מספרים שלמים כך ש־ $a = bq + r$.[6] אזי $\gcd(a,b) = \gcd(b,r)$.

הוכחה

אם k מספר טבעי המחלק את a ואת b, אזי k מחלק גם את bq, ולכן גם את $r = a - bq$. באופן דומה, אם k מספר טבעי המחלק את b ואת r, אזי k מחלק גם את $a = bq + r$. משילוב הבחנות אלו נקבל, שהמחלקים המשותפים של a ו־ b הם בדיוק המחלקים המשותפים של b ו־ r, וממילא מתקיים $\gcd(a,b) = \gcd(b,r)$.

מ.ש.ל.

נסביר כיצד להשתמש בטענה 5.6.4 לצורך חישוב מחלק משותף מרבי:

נניח כי נתונים בפנינו זוג מספרים שלמים שונים מאפס a,b, ואנו מעוניינים לחשב את $\gcd(a,b)$. בלא הגבלת הכלליות, נוכל להניח כי שני המספרים חיוביים: אם אחד מהם שלילי, נחליף את סימנו. נוכל גם להניח כי $a \geq b$, אחרת נחליף בין שני המספרים. אם $b|a$ סיימנו, כי $\gcd(a,b) = b$ לפי למה 5.6.3. אחרת, נחלק עם שארית, כלומר נכתוב $a = bq + r$, כאשר r,q שלמים ו־ $0 \leq r < b$, ונסמן $a_1 = b,\ b_1 = r$.

לפי טענה 5.6.4, $\gcd(a,b) = \gcd(a_1,b_1)$, ומתקיים $0 \leq b_1 < b$. שוב, אם $b_1|a_1$ סיימנו.

אחרת, נבצע שוב חלוקה עם שארית, ונקבל באופן דומה זוג מספרים a_2,b_2 כך ש־ $\gcd(a_1,b_1) = \gcd(a_2,b_2)$ ו־ $0 \leq b_2 < b_1 < b$.

נמשיך ונחזור על תהליך זה, ונקבל סדרה $(a,b),(a_1,b_1),(a_2,b_2),\ldots,(a_k,b_k)$ של זוגות מספרים שלכולם אותו מחלק משותף מרבי. מכיוון שערכו של b_i קטן בכל צעד, התהליך בהכרח מסתיים - כלומר נגיע לזוג a_k,b_k שבו $b_k|a_k$, ואז:

$$\gcd(a,b) = \gcd(a_1,b_1) = \gcd(a_2,b_2) = \ldots = \gcd(a_k,b_k) = b_k$$

התהליך שתיארנו נקרא **האלגוריתם של אוקלידס**.

---

6 שימו לב, בהכרח קיים זוג מספרים שלמים המקיים תנאי זה, לפי משפט החלוקה עם שארית.

דוגמה

נחשב את המחלק המשותף המירבי של 78 ו־-225. נעשה זאת בשלבים:

שלב מקדים: למען הנוחות, נעבור למספרים חיוביים: $\gcd(-225,78) = \gcd(225,78)$.

שלב ראשון: נחלק עם שארית: $225 = 78 \cdot 2 + 69$, לכן $\gcd(225,78) = \gcd(78,69)$.

שלב שני: נחלק עם שארית: $78 = 69 \cdot 1 + 9$, לכן $\gcd(78,69) = \gcd(69,9)$.

שלב שלישי: נחלק עם שארית: $69 = 9 \cdot 7 + 6$, לכן $\gcd(69,9) = \gcd(9,6)$.

שלב רביעי: נחלק עם שארית: $9 = 6 \cdot 1 + 3$, לכן $\gcd(9,6) = \gcd(6,3)$.

מכיוון ש־$3|6$, התהליך הסתיים. משרשור השוויונות שקיבלנו נסיק:

$$\gcd(-225,78) = \gcd(6,3) = 3$$

▸

שאלה 5.6.4

השתמשו באלגוריתם של אוקלידס לחישוב $\gcd(1048,326)$.

התשובה בעמוד 46

להבחנה שעמדה בבסיסו של האלגוריתם של אוקלידס (טענה 5.6.4) יש מסקנה שימושית נוספת.

טענה 5.6.5

יהיו a,b מספרים שלמים שונים מאפס. אז קיימים מספרים שלמים x,y כך ש־$\gcd(a,b) = ax + by$. כלומר, ניתן להציג את המחלק המשותף המרבי $\gcd(a,b)$ כצירוף לינארי של a,b **במקדמים שלמים**.[7]

הוכחה

על־ידי החלפת סימנים, והחלפה בין המספרים a ו־b, נוכל להניח בלא הגבלת הכלליות כי $a \geq b > 0$.

עבור מקרה זה, נוכיח את הטענה באינדוקציה על a. אם $a = 1$, אזי בהכרח $b = 1$ (כי $a \geq b > 0$) ומתקיים $\gcd(a,b) = \gcd(1,1) = 1 = 1 \cdot 1 + 0 \cdot 1$.

נניח כי הטענה נכונה לכל $1 \leq c < a$, ונוכיח עבור a.

אם $a = b$ אז $\gcd(a,b) = a = 1 \cdot a + 0 \cdot b$.

אחרת (אם $a < b$), נחלק עם שארית: $a = bq + r$, כאשר r,q שלמים ו־$0 \leq r < b$. לפי הנחת האינדוקציה קיימים שלמים x,y כך ש־$\gcd(b,r) = xb + yr$. לפי טענה 5.6.4, נקבל:

$$\gcd(a,b) = \gcd(b,r) = xb + yr = xb + y(a - bq) = ya + (x - yq)b$$

בזאת הצגנו את $\gcd(a,b)$ כצירוף לינארי של a,b במקדמים השלמים $y, x - yq$.

מ.ש.ל.

---

7 המקדמים כאן הם x,y.

דוגמה

עבור $\gcd(15,9) = 3$, נוכל לכתוב $3 = (-1) \cdot 15 + 2 \cdot 9$. המקדמים כאן הם $-1,2$.

כעת נשאל - כיצד מוצאים בהצגה כזאת, באופן כללי, את המקדמים של המחלק המשותף המרבי של a,b? האסטרטגיה שנפעיל כרוכה באסטרטגיה שמיישם האלגוריתם של אוקלידס למציאת המחלק המשותף המרבי עצמו. ההבחנה ביסודו של האלגוריתם היא כי אם נבצע חלוקה עם שארית $a = bq + r$, נוכל להחליף את הזוג a,b בזוג b,r. באמצעות חזרות הולכות ונשנות של חילופים כאלה, שבהם המספר השני הולך וקטן, נגיע בסופו של דבר למצב שבו המספר השני מחלק את הראשון, ואז סיימנו. ◀

לצורך מציאת המקדמים שאותם אנו מבקשים עתה, נציג הבחנות קשורות.

הבחנה א

נניח כי $a = bq + r$, ונניח כי הצלחנו להציג את $g = \gcd(a,b) = \gcd(b,r)$ כצירוף לינארי במקדמים שלמים של b,r, נאמר $g = xb + yr$. מתוך הצגה זו, נקבל מיד גם הצגה של a,b כצירוף לינארי במקדמים שלמים של b,r, שכן $\gcd(a,b) = ya + (x - yq)b$ (ראינו זאת במהלך הוכחת טענה 5.6.5).

הבחנה ב

הבחנה א מאפשרת לנו לבצע סדרת צעדים המקטינה את זוג המספרים שעליו אנו עובדים. כעת נדון בצעד האחרון: מה נעשה כאשר הגענו לזוג a,b המקיים $b|a$? אך זה פשוט: $\gcd(a,b) = b = 1 \cdot b + 0 \cdot a$.

בזאת השלמנו את הדיון התיאורטי. כעת נדגים כיצד מוצאים, הלכה למעשה, את המקדמים המבוקשים בחישוב המחלק המשותף המרבי של זוג מספרים נתון.

דוגמה

בדוגמה שלאחר טענה 5.6.4, השתמשנו באלגוריתם של אוקלידס כדי להראות ש־

$$\gcd(-225,78) = 3$$

נחזור בקצרה על השלבים שביצענו:

שלב מקדים: מעבר למספרים חיוביים: $\gcd(-225,78) = \gcd(225,78)$.

שלב ראשון: חילוק עם שארית: $225 = 78 \cdot 2 + 69$, לכן $\gcd(225,78) = \gcd(78,69)$.

שלב שני: חילוק עם שארית: $78 = 69 \cdot 1 + 9$, לכן $\gcd(78,69) = \gcd(69,9)$.

שלב שלישי: חילוק עם שארית: $69 = 9 \cdot 7 + 6$, לכן $\gcd(69,9) = \gcd(9,6)$.

שלב רביעי: חילוק עם שארית: $9 = 6 \cdot 1 + 3$, לכן $\gcd(9,6) = \gcd(6,3) = 3$.

כעת נעבור על השלבים **מהסוף להתחלה**, ובכל שלב נציג את $\gcd(-225,78) = 3$ כצירוף לינארי במקדמים שלמים של זוג האיברים בשלב המתאים.

בשלב הרביעי: $9 = 6 \cdot 1 + 3$, לכן:

$$3 = 9 - 1 \cdot 6 \tag{1}$$

בשלב השלישי: $69 = 9 \cdot 7 + 6$, לכן $6 = 69 - 7 \cdot 9$. נציב זאת ב־(1) ונקבל:

$$3 = 9 - 1 \cdot 6 = 9 - 1 \cdot (69 - 7 \cdot 9) = 8 \cdot 9 - 1 \cdot 69 \tag{2}$$

בשלב השני: $78 = 69 \cdot 1 + 9$, לכן $9 = 78 - 1 \cdot 69$. נציב זאת ב־(2) ונקבל:

$$3 = 8 \cdot 9 - 1 \cdot 69 = 8 \cdot (78 - 1 \cdot 69) - 1 \cdot 69 = 8 \cdot 78 - 9 \cdot 69 \tag{3}$$

בשלב הראשון: $225 = 78 \cdot 2 + 69$, לכן $69 = 225 - 78 \cdot 2$. נציב זאת ב־(3) ונקבל:

$$3 = 8 \cdot 78 - 9 \cdot 69 = 8 \cdot 78 - 9 \cdot (225 - 2 \cdot 78) = 26 \cdot 78 - 9 \cdot 225 \tag{4}$$

לסיום קיבלנו

$$3 = 26 \cdot 78 - 9 \cdot 225 = 9 \cdot (-225) + 26 \cdot 78$$

ובכך קיבלנו את ההצגה המבוקשת. ◀

שאלה 5.6.5

הציגו את $\gcd(1048,326)$ כצירוף לינארי במקדמים שלמים של $1048, 326$. היעזרו בחישובים שערכתם בשאלה 5.6.4, ועקבו אחר הצעדים שביצענו בדוגמה האחרונה.

התשובה בעמוד 46

שאלה 5.6.6

השתמשו באלגוריתם של אוקלידס לחישוב $\gcd(919,25)$, והציגו אותו כצירוף לינארי במקדמים שלמים של $919, 25$.

התשובה בעמוד 46

כעת נראה כיצד להשתמש באלגוריתם של אוקלידס למציאת ההופכי בשדה סופי ראשוני: אם $0 \neq b \in \mathbb{Z}_p$, אז b זר ל־p, ולכן קיימים שלמים x, y כך ש־$xb + yp = 1$. אזי $xb \underset{\text{mod } p}{\equiv} 1$, ולכן גם $x_{\text{mod } p} \in \mathbb{Z}_p$ מקיים $x_{\text{mod } p} b \underset{\text{mod } p}{\equiv} 1$, כלומר $x_{\text{mod } p} b = 1$ בשדה $\mathbb{Z}_p$, ולכן $b^{-1} = x_{\text{mod } p}$. כיצד נמצא את השלם x (ואת בן זוגו y)? התשובה - באמצעות האלגוריתם של אוקלידס.

דוגמה

ניתן לבדוק כי המספר 919 הוא מספר ראשוני, ולכן $\mathbb{Z}_{919}$ הוא שדה. כיצד נמצא את ההופכי ל־25 בשדה זה? דרך אחת היא לנסות ולבדוק כל אחד מאיברי השדה, בזה אחר זה. אך חישוב זה עלול לערב מאות בדיקות שונות! במקום זאת, נפעל בהתאם לשיטה שתיארנו לעיל. תחילה (באמצעות האלגוריתם של אוקלידס) נציג את 1 כצירוף לינארי במקדמים שלמים של $919, 25$. כבר עשיתם זאת בשאלה 5.6.6 (אם דילגתם על השאלה - חזרו אליה עתה ובצעו את החישוב - אל תסתכלו בתשובה!). קיבלנו:

$$1 = 919 \cdot 4 - 25 \cdot 147 = 919 \cdot 4 + 25 \cdot (-147)$$

לכן, $25^{-1} = (-147)_{\text{mod } 919} = 919 - 147 = 772$. ◀

שאלה 5.6.7

א. בשדה $\mathbb{Z}_{17}$, חשבו את 12^{-1}.

ב. בשדה $\mathbb{Z}_{919}$, חשבו את 12^{-1}.

ג. בשדה $\mathbb{Z}_{919}$, חשבו את 0^{-1}.

התשובה בעמוד 47

תשובות לשאלות בפרק 5

תשובה 5.1.1 **השאלה בעמוד 8**

נרשום $a = qb + r$, כאשר $0 \le r < b$. אם שארית החילוק היא $r = 0$, אזי $a = qb$ ולכן a מתחלק ב־b. להפך, אם a מתחלק ב־b, אזי קיים מספר שלם q' כך ש־$a = q'b = q'b + 0$. מיחידות הזוג (q,r), נסיק ש־$(q,r) = (q',0)$ ובפרט $r = 0$.

תשובה 5.1.2 **השאלה בעמוד 8**

מתקיים: $0 = b \cdot 0 + 0,\ 0 \le 0 < b$.

תשובה 5.1.3 **השאלה בעמוד 8**

א. $a = 25, b = 7$. במקרה זה $25 = 7 \cdot 3 + 4$; המנה היא $q = 3$, השארית $r = 4$.

ב. $a = 140, b = 22$. במקרה זה $140 = 22 \cdot 6 + 8$; המנה היא $q = 6$, השארית $r = 8$.

ג. $a = -24, b = 5$. במקרה זה $-24 = 5 \cdot (-5) + 1$; המנה היא $q = -5$, השארית $r = 1$.

ד. במקרה זה $0 = 0 \cdot b + 0$; המנה היא $q = 0$, השארית $r = 0$.

ה. במקרה זה $a = 0 \cdot b + a$; המנה היא $q = 0$, השארית $r = a$.

תשובה 5.1.4 **השאלה בעמוד 8**

עבור $b > 0$ הטענה זהה לזו של משפט 5.1.1 שכבר הוכח, כי $|b| = b$.

עבור $b < 0$, $|b| = -b > 0$. לפי משפט החילוק עם שארית, קיים זוג יחיד (q,r) של מספרים שלמים כך ש־

$$a = q(-b) + r,\ 0 \le r < |b|$$

כלומר

$$a = (-q)b + r,\ 0 \le r < |b|$$

ומכאן שהזוג $(-q,r)$ עונה על הדרישות. היחידות נובעת מיידית מן היחידות של הזוג (q,r).

תשובה 5.2.1 **השאלה בעמוד 11**

א. כל מספר שלם a מקיים $n \mid a - a (= 0)$, ולכן $a \underset{\bmod n}{\equiv} a$.

ב. אם $n \mid a - b$, אזי גם $n \mid (a-b) \cdot (-1)$, כלומר $n \mid b - a$.

ג. אם $n \mid a - b, n \mid b - c$, אזי n מחלק גם את הסכום $a - b + b - c = a - c$.

תשובה 5.2.2 **השאלה בעמוד 11**

א. $9 \underset{\bmod 3}{\equiv} 3,\ 9 \underset{\bmod 4}{\not\equiv} 3$

ב. $-9 \underset{\bmod 3}{\equiv} -3,\ -9 \underset{\bmod 4}{\not\equiv} -3$

ג. $-9 \underset{\bmod 3}{\equiv} 3,\ -9 \underset{\bmod 4}{\not\equiv} 3$

ד. $2 \underset{\bmod 3}{\equiv} 14,\ 2 \underset{\bmod 4}{\equiv} 14$

ה. $1 \underset{\text{mod}3}{\equiv} 5,\ 1 \underset{\text{mod}4}{\equiv} 5$

ו. $7 \underset{\text{mod}3}{\equiv} 17,\ 7 \underset{\text{mod}4}{\not\equiv} 17$

תשובה 5.2.3 **השאלה בעמוד 14**

א.
$$(140+78)_{\text{mod}3} = (140_{\text{mod}3} + 78_{\text{mod}3})_{\text{mod}3} = (2+0)_{\text{mod}3} = 2$$
$$(140 \cdot 78)_{\text{mod}3} = (140_{\text{mod}3} \cdot 78_{\text{mod}3})_{\text{mod}3} = (2 \cdot 0)_{\text{mod}3} = 0$$

ב.
$$(182 \cdot (-45))_{\text{mod}7} = (0 \cdot 3)_{\text{mod}7} = 0 \qquad ,(182-45)_{\text{mod}7} = (0-3)_{\text{mod}7} = 4$$

ג.
$$(10145 + 28983)_{\text{mod}4} = (45+83)_{\text{mod}4} = (1+3)_{\text{mod}4} = 0$$
$$(10145 \cdot 28983)_{\text{mod}4} = (45 \cdot 83)_{\text{mod}4} = (1 \cdot 3)_{\text{mod}4} = 3$$

ד.
$$(1240+95)_{\text{mod}11} = (1100+140+99-4)_{\text{mod}11} = (140-4)_{\text{mod}11}$$
$$= (30-4)_{\text{mod}11} = (26)_{\text{mod}11} = 4$$

ה.
$$(1240 \cdot 95)_{\text{mod}11} = (140 \cdot (-4))_{\text{mod}11} = (30 \cdot 7)_{\text{mod}11}$$
$$= (8 \cdot 7)_{\text{mod}11} = 56_{\text{mod}11} = 1$$

תשובה 5.2.4 **השאלה בעמוד 15**

השוויונות המסומנים ב־ * הם לפי הגדרה 5.2.7, השוויונות המסומנים ב־ ** הם לפי למה 5.2.6:

$$a +_n b \overset{*}{=} (a+b)_{\text{mod}\,n} \overset{**}{=} (a_{\text{mod}\,n} + b_{\text{mod}\,n})_{\text{mod}\,n} \overset{*}{=} a_{\text{mod}\,n} +_n b_{\text{mod}\,n}$$

$$a \cdot_n b \overset{*}{=} (a \cdot b)_{\text{mod}\,n} \overset{**}{=} (a_{\text{mod}\,n} \cdot b_{\text{mod}\,n})_{\text{mod}\,n} \overset{*}{=} a_{\text{mod}\,n} \cdot_n b_{\text{mod}\,n}$$

תשובה 5.2.5 **השאלה בעמוד 15**

$8 = 5 + 3$, שארית החילוק של 8 ב־ 6 היא 2, לכן $3 +_6 5 = 2$. באופן דומה מחשבים ומקבלים: $2 = 12 +_6 2$, $3 = 14 +_4 3-$, $4 = (-40) +_{12} 4-$, ועבור הכפל: $3 \cdot_6 5 = 15_{\text{mod}6} = 3$, $0 = 24_{\text{mod}6} = 12 \cdot_6 2$, $0 = -42_{\text{mod}6} = 14 \cdot_6 3-$, ולבסוף $4 = 2 \cdot_6 2 = (-40) \cdot_6 (-4)$.

תשובה 5.2.6 **השאלה בעמוד 17**

א.
$$7^{31}{}_{\text{mod}12} = (7^2)^{15} \cdot 7_{\text{mod}12} = (49)^{15} \cdot 7_{\text{mod}12} = 1^{15} \cdot 7_{\text{mod}12}$$
$$= 1 \cdot 7_{\text{mod}12} = 7_{\text{mod}12} = 7$$

ב. מתקיים:

$$21^{35}{}_{\text{mod}6} = 3^{35}{}_{\text{mod}6}$$

כעת שימו לב ש־ $3 \cdot 3 = 3_{\text{mod}6}$, ובאינדוקציה נובע כי $3^n{}_{\text{mod}6} = 3$ לכל n טבעי, ולכן:

$$21^{35}{}_{\text{mod}6} = 3^{35}{}_{\text{mod}6} = 3$$

תשובה 5.2.7 **השאלה בעמוד 18**

הוכחת הלמה אנלוגית להוכחת למה 5.2.10 - עם כפל במקום חיבור.

תשובה 5.2.8 **השאלה בעמוד 20**

א. שוב נרשום את הספרות של n (משמאל לימין) כ־ $a_1,\dots,a_k$, ואז:

$$n = 10^{k-1}a_1 + 10^{k-2}a_2 + \cdots + 10a_{k-1} + a_k$$

$10 \underset{\mathrm{mod}\,9}{\equiv} 1$, לכן $10^2 \underset{\mathrm{mod}\,9}{\equiv} 1^2 = 1$, ובאינדוקציה על החזקה - לכל $i \ge 1$, $10^i \underset{\mathrm{mod}\,9}{\equiv} 1$

לכן,

$$10^{k-1}a_1 + 10^{k-2}a_2 + \cdots + 10a_{k-1} + a_k \underset{\mathrm{mod}\,9}{\equiv} 1\cdot a_1 + 1\cdot a_2 + \cdots + 1\cdot a_{k-1} + a_k$$

כלומר

$$n \underset{\mathrm{mod}\,9}{\equiv} a_1 + \cdots + a_{k-1} + a_k$$

הווי אומר:

$$n_{\mathrm{mod}\,9} = (a_1 + \cdots + a_{k-1} + a_k)_{\mathrm{mod}\,9}$$

אם כן, שארית החילוק ב־ 9 של n, שווה לשארית החילוק ב־ 9 של סכום ספרותיו. בפרט, n מתחלק ב־ 9 אם ורק אם סכום ספרותיו מתחלק ב־ 9.

ב. סכום הספרות של המספר 123554524987738785 הוא 93. סכום הספרות של 93 הוא 12, שאינו מתחלק ב־ 9, אך מתחלק ב־ 3. לכן גם המספר 123554524987738785 אינו מתחלק ב־ 9, אך מתחלק ב־ 3.

תשובה 5.2.9 **השאלה בעמוד 20**

גם הפעם נרשום את הספרות של n (משמאל לימין) כ־ $a_1,\dots,a_k$, כך ש־

$$n = 10^{k-1}a_1 + 10^{k-2}a_2 + \cdots + 10a_{k-1} + a_k$$

כעת נבחין כי $10 \underset{\mathrm{mod}\,11}{\equiv} -1$, לכן $10^i \underset{\mathrm{mod}\,11}{\equiv} (-1)^i$ לכל i טבעי. לכן:

$$n = 10^{k-1}a_1 + 10^{k-2}a_2 + \cdots + 10a_{k-1} + a_k \underset{\mathrm{mod}\,11}{\equiv} a_k - a_{k-1} + \ldots + (-1)^{k-1}a_1$$

לכן כדי לבדוק האם מספר נתון מתחלק ב־11, עלינו לחבר ולחסר את ספרותיו לסירוגין, החל מספרת האחדות, ולבדוק אם התוצאה שהתקבלה מתחלקת ב־11.

עבור 123554524987738785 נקבל:

$$123554524987738785 =$$
$$5-8+7-8+3-7+7-8+9-4+2-5+4-5+5-3+2-1 \underset{\mathrm{mod}\,11}{\equiv} 6$$

ולכן 123554524987738785 לא מתחלק ב־11.

תשובה 5.3.1 **השאלה בעמוד 23**

7 הוא ראשוני בעצמו, $24 = 2 \cdot 2 \cdot 2 \cdot 3$, $21 = 7 \cdot 3$.

תשובה 5.3.2 **השאלה בעמוד 26**

נניח כי $p = ab$. בפרט $p|ab$, ולכן בלא הגבלת הכלליות $p|a$. נרשום $a = pc$ ונקבל $p = pcb$. מכאן ש־ $bc = 1$, ולכן בהכרח $b = c = 1$ ולכן $p = a, b = 1$. נסיק ש־ p ראשוני.

תשובה 5.3.3 **השאלה בעמוד 26**

נניח בשלילה ש־ $\sqrt{2}$ רציונלי. אז קיימים מספרים טבעיים $m,n \in \mathbb{N}$ כך ש־ $\sqrt{2} = \frac{m}{n}$ ולכן $2n^2 = m^2$.

בהצגה היחידה של m,n כמכפלות של ראשוניים, הראשוני 2 מופיע איזשהו מספר טבעי של פעמים, או שאינו מופיע כלל. אם כן, נוכל לרשום

$$m = 2^e p_1 \cdot p_2 \cdot \ldots \cdot p_r , n = 2^f q_1 \cdot q_2 \cdot \ldots \cdot q_s$$

כאשר $p_1, p_2, \ldots, p_r, q_1, \ldots, q_s$ ראשוניים השונים מ־ 2, והחזקות e, f הן אי־שליליות.
מהמשוואה $2n^2 = m^2$ נקבל:

$$2^{2f+1} q_1^2 \cdot q_2^2 \cdot \ldots \cdot q_s^2 = 2^{2e} p_1^2 \cdot p_2^2 \cdot \ldots \cdot p_r^2$$

נוכל לראות שוויון זה כשתי הצגות של אותו מספר כמכפלה של ראשוניים, ולכן (בגלל יחידות ההצגה) הראשוני 2 מופיע אותו מספר של פעמים בשתי ההצגות. אך בהצגה הימנית מספר ההופעות של 2 הוא זוגי ($2e$), ואילו בהצגה השמאלית מספר ההופעות אי־זוגי ($2f + 1$), סתירה.

תשובה 5.3.4 **השאלה בעמוד 26**

א. אם c מספר שלם כלשהו, אזי $p|c$ אם ורק אם $p|(-c)$. אם $a = 0$ או $b = 0$, הטענה נכונה באופן טריוויאלי. נוכל אם כן להניח בלא הגבלת הכלליות ש־ a,b טבעיים, והטענה נובעת ממסקנה 5.3.6.

ב. המקרה של $n = 2$ נובע מחלק א עבור $b = a$. המקרה הכללי נובע באינדוקציה.

תשובה 5.4.1 **השאלה בעמוד 28**

מאחר ש־ $3 \cdot 6 \underset{\text{mod}17}{\equiv} 1$, כלומר $3 \cdot_7 6 = 1$, נסיק שבשדה $\mathbb{Z}_{17}$ מתקיים השוויון $3 \cdot 6 = 1$, ולכן ההופכי של 3 ב־ $\mathbb{Z}_{17}$ הוא 6. כמו כן מתקיים $12 \cdot_7 10 = 1$ ($120 = 7 \cdot 17 + 1$), ולכן ההופכי של 12 ב־ $\mathbb{Z}_{17}$ הוא 10. באופן דומה, ודאו כי בשדה $\mathbb{Z}_{31}$ מתקיים $3^{-1} = 21$, $12^{-1} = 13$.

תשובה 5.4.2 **השאלה בעמוד 28**

את כל החישובים מבצעים כרגיל, כאשר בכל פעולת חילוק יש לכפול בהופכי של המכנה (שאותו מחשבים בנפרד, אם לא עשינו זאת כבר). כך מקבלים (שימו לב לתכסיסי הקיצור שביצענו):

א.

$$(15/12) \cdot 5 + 3 = 15 \cdot 10 \cdot 5 + 3 = 15 \cdot 50 + 3 \underset{\substack{\uparrow \\ 51=17\cdot 3=0}}{=} 15 \cdot (-1) + 3$$

$$= -15 + 3 = 2 + 3 = 5$$

ב.

$$(14/12)\cdot(17/3) = 14\cdot 13\cdot 17/3 = 14\cdot 13\cdot 17\cdot 21 = 182\cdot 17\cdot 21$$
$$= 27\cdot 17\cdot 21 = 459\cdot 21 = 25\cdot 21 = 525 = 29$$

ג.

$$(-13/3)\cdot(15/3)\,/\,(13/9) = (1/3)\cdot(1/3)\,/\,(-1/9)$$
$$= -(1/3)\cdot(1/3)\,/\,(1/3^2) = -(1/3^2)\,/\,(1/3^2) = -1 = 6$$

תשובה 5.4.3 **השאלה בעמוד 29**

נכתוב את מטריצת המקדמים המתאימה ונדרג אותה, כאשר את פעולות החשבון אנו מבצעים בשדה $\mathbb{Z}_{11}$:

$$\left(\begin{array}{ccc|c} 3 & 1 & 1 & 1 \\ 2 & 1 & 3 & 2 \\ 1 & 2 & 3 & 1 \end{array}\right) \xrightarrow{R_1 \leftrightarrow R_3} \left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 2 & 1 & 3 & 2 \\ 3 & 1 & 1 & 1 \end{array}\right) \xrightarrow{R_2 \to R_2 - 2R_1} \left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 8 & 8 & 0 \\ 3 & 1 & 1 & 1 \end{array}\right) \xrightarrow{R_3 \to R_3 - 3R_1}$$

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 8 & 8 & 0 \\ 0 & 6 & 3 & 9 \end{array}\right) \xrightarrow{R_2 \to 8^{-1} R_2} \left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 6 & 3 & 9 \end{array}\right) \xrightarrow{R_3 \to 6^{-1} R_3} \left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 6 & 7 \end{array}\right) \xrightarrow{R_3 \to R_3 - R_2}$$

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 5 & 7 \end{array}\right) \xrightarrow{R_3 \to 5^{-1} R_3} \left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 8 \end{array}\right) \xrightarrow[R_2 \to R_2 - R_3]{R_1 \to R_1 - 3R_3} \left(\begin{array}{ccc|c} 1 & 2 & 0 & 10 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 8 \end{array}\right) \xrightarrow{R_1 \to R_1 - 2R_2}$$

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 4 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 8 \end{array}\right)$$

למערכת פתרון יחיד: $x = 4, y = 3, z = 8$.

תשובה 5.4.4 **השאלה בעמוד 29**

נכתוב את מטריצת המקדמים המתאימה ונדרג אותה, כאשר את פעולות החשבון אנו מבצעים בשדה $\mathbb{Z}_{13}$:

$$\left(\begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{array}\right) \xrightarrow{R_2 \to R_2 - R_1} \left(\begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 0 & 12 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{array}\right) \xrightarrow{R_2 \to R_2 - 12R_3} \left(\begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 0 & 0 & 2 & 2 \\ 0 & 1 & 1 & 1 \end{array}\right) \xrightarrow{R_1 \to R_1 - R_3}$$

$$\left(\begin{array}{ccc|c} 1 & 0 & 12 & 12 \\ 0 & 0 & 2 & 2 \\ 0 & 1 & 1 & 1 \end{array}\right) \xrightarrow{R_2 \leftrightarrow R_3} \left(\begin{array}{ccc|c} 1 & 0 & 12 & 12 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 \end{array}\right) \xrightarrow{R_3 \to 2^{-1} R_3} \left(\begin{array}{ccc|c} 1 & 0 & 12 & 12 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right) \xrightarrow{R_1 \to R_1 - 12R_3}$$

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right) \xrightarrow{R_2 \to R_2 - R_3} \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{array}\right)$$

מכאן כי למערכת פתרון יחיד: $x = 0, y = 0, z = 1$.

תשובה 5.4.5 **השאלה בעמוד 29**

נפעל בשיטה שלמדנו בפרק 3 – נדרג בו־זמנית את המטריצה ואת מטריצת היחידה:

$$\left(\begin{array}{ccc|ccc}1&1&0&1&0&0\\1&0&1&0&1&0\\0&1&1&0&0&1\end{array}\right)\xrightarrow{R_2\to R_2-R_1}\left(\begin{array}{ccc|ccc}1&1&0&1&0&0\\0&12&1&12&1&0\\0&1&1&0&0&1\end{array}\right)\xrightarrow{R_2\to R_2-12R_3}$$

$$\left(\begin{array}{ccc|ccc}1&1&0&1&0&0\\0&0&2&12&1&1\\0&1&1&0&0&1\end{array}\right)\xrightarrow{R_1\to R_1-R_3}\left(\begin{array}{ccc|ccc}1&0&12&1&0&12\\0&0&2&12&1&1\\0&1&1&0&0&1\end{array}\right)\xrightarrow{R_2\leftrightarrow R_3}$$

$$\left(\begin{array}{ccc|ccc}1&0&12&1&0&12\\0&1&1&0&0&1\\0&0&2&12&1&1\end{array}\right)\xrightarrow{R_3\to 2^{-1}R_3}\left(\begin{array}{ccc|ccc}1&0&12&1&0&12\\0&1&1&0&0&1\\0&0&1&6&7&7\end{array}\right)\xrightarrow{R_1\to R_1-12R_3}$$

$$\left(\begin{array}{ccc|ccc}1&0&0&7&7&6\\0&1&1&0&0&1\\0&0&1&6&7&7\end{array}\right)\xrightarrow{R_2\to R_2-R_3}\left(\begin{array}{ccc|ccc}1&0&0&7&7&6\\0&1&0&7&6&7\\0&0&1&6&7&7\end{array}\right)$$

נסיק שהמטריצה הפיכה, והמטריצה שהתקבלה בצד ימין היא המטריצה ההופכית (ודאו על־ידי כפל ישיר).

תשובה 5.4.6 **השאלה בעמוד 29**

נפתח לפי עמודה שלישית ונקבל:

$$\begin{vmatrix}3&2&0&1\\1&3&0&16\\1&0&2&1\\2&1&0&2\end{vmatrix}=2\begin{vmatrix}3&2&1\\1&3&16\\2&1&2\end{vmatrix}\overset{R_1\to R_1-3R_2}{=}2\begin{vmatrix}0&10&4\\1&3&16\\2&1&2\end{vmatrix}$$

$$\overset{R_3\to R_3-2R_2}{=}2\begin{vmatrix}0&10&4\\1&3&16\\0&12&4\end{vmatrix}=-2\begin{vmatrix}10&4\\12&4\end{vmatrix}=-2(40-48)$$

$$=-2(-8)=16$$

תשובה 5.4.7 **השאלה בעמוד 29**

עלינו לבדוק האם קיימים סקלרים x,y,z ב־$\mathbb{Z}_5$, שאינם כולם אפס, כך שמתקיים:

$$x(1,0,3)+y(1,2,4)+z(2,2,2)=0$$

באופן שקול, עלינו לבדוק האם קיים פתרון לא־טריוויאלי למערכת המשוואות הבאה מעל $\mathbb{Z}_5$:

$$\begin{aligned} x + y + 2z &= 0 \\ 2y + 2z &= 0 \\ 3x + 4y + 2z &= 0 \end{aligned}$$

נדרג את המטריצה המתאימה:

$$\left(\begin{array}{ccc|c} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 3 & 4 & 2 & 0 \end{array}\right) \xrightarrow{R_3 \to R_3 - 3R_1} \left(\begin{array}{ccc|c} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right) \xrightarrow{R_2 \to R_2 - 2R_3; R_2 \leftrightarrow R_3}$$

$$\left(\begin{array}{ccc|c} 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) \xrightarrow{R_2 \to 2^{-1} R_2} \left(\begin{array}{ccc|c} 1 & 1 & 2 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) \xrightarrow{R_1 \to R_1 - R_2}$$

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

מהצורה הקנונית שאליה הגענו אנו רואים כי ישנו משתנה חופשי (המשתנה השלישי), וממילא קיימים למערכת פתרונות לא־טריוויאלים. נסיק שהווקטורים תלויים לינארית.

תשובה 5.6.1 **השאלה בעמוד 32**

$$\begin{aligned} [5] &= \{1,5\} \\ [6] &= \{1,2,3,6\} \\ [7] &= \{1,7\} \\ [8] &= \{1,2,4,8\} \\ [9] &= \{1,3,9\} \\ [10] &= \{1,2,5,10\} \end{aligned}$$

תשובה 5.6.2 **השאלה בעמוד 32**

$$\begin{aligned} [12,1] &= \{1\} \\ [12,2] &= \{2\} \\ [12,5] &= \{1\} \\ [12,6] &= \{1,2,3,6\} (= [6]) \\ [12,12] &= \{1,2,3,4,6,12\} (= [12]) \\ [12,15] &= \{1,2,3\} \end{aligned}$$

תשובה 5.6.3 **השאלה בעמוד 33**

$$\gcd(12,1) = \max\{1\} = 1$$
$$\gcd(12,2) = \max\{2\} = 2$$
$$\gcd(12,5) = \max\{1\} = 1$$
$$\gcd(12,6) = \max\{1,2,3,6\} = \{6\}$$
$$\gcd(12,12) = \max\{1,2,3,4,6,12\} = [12]$$
$$\gcd(12,15) = \max\{1,2,3\} = 3$$

תשובה 5.6.4 **השאלה בעמוד 35**

שלב ראשון: נחלק עם שארית: $1048 = 326 \cdot 3 + 70$, לכן $\gcd(1048,326) = \gcd(326,70)$.

שלב שני: נחלק עם שארית: $326 = 70 \cdot 4 + 46$, לכן $\gcd(326,70) = \gcd(70,46)$.

שלב שלישי: נחלק עם שארית: $70 = 46 \cdot 1 + 24$, לכן $\gcd(70,46) = \gcd(46,24)$.

שלב רביעי: נחלק עם שארית: $46 = 24 \cdot 1 + 22$, לכן $\gcd(46,24) = \gcd(24,22)$.

שלב חמישי: נחלק עם שארית: $24 = 22 \cdot 1 + 2$, לכן $\gcd(24,22) = \gcd(22,2)$.

בזאת סיימנו (שהרי $2|22$). נסיק ש־ $\gcd(1048,326) = \gcd(22,2) = 2$.

תשובה 5.6.5 **השאלה בעמוד 37**

נעקוב אחר חמשת השלבים שביצענו בתשובה 5.6.4, ונציב מהסוף להתחלה, כמו שעשינו בדוגמה:

$$2 = 24 - 22 = 24 - (46 - 24) = 2 \cdot 24 - 46$$
$$= 2 \cdot (70 - 46) - 46 = 2 \cdot 70 - 3 \cdot 46 =$$
$$2 \cdot 70 - 3 \cdot (326 - 70 \cdot 4) = 14 \cdot 70 - 3 \cdot 326$$
$$= 14 \cdot (1048 - 3 \cdot 326) - 3 \cdot 326$$
$$= 14 \cdot 1048 - 45 \cdot 326$$

תשובה 5.6.6 **השאלה בעמוד 37**

נבצע את סדרת החלוקות עם שארית:

$$919 = 25 \cdot 36 + 19$$
$$25 = 19 \cdot 1 + 6$$
$$19 = 6 \cdot 3 + 1$$

מכאן כי: $\gcd(919,25) = \gcd(6,1) = 1$. כעת נלך מהסוף להתחלה:

$$1 = 19 - 6 \cdot 3$$
$$= 19 - (25 - 19 \cdot 1) \cdot 3 = 19 \cdot 4 - 25 \cdot 3$$
$$= (919 - 25 \cdot 36) \cdot 4 - 25 \cdot 3$$
$$= 919 \cdot 4 - 25 \cdot 147$$

תשובה 5.6.7 **השאלה בעמוד 38**

א. בדיקה ישירה מעלה כי $12^{-1} = 10$. אכן, $12 \cdot 10 = 120 = 1 + 7 \cdot 17$.

ב. באמצעות האלגוריתם של אוקלידס, נקבל:

$$1 = (-5) \cdot 919 + 383 \cdot 12$$

לכן $12^{-1} = 383_{\mathrm{mod}\,919} = 383$.

ג. זוהי שאלה מכשילה - איבר האפס לעולם אינו הפיך!

פרק 6: שדה המספרים המרוכבים

6.1 הרחבת שדות

בסעיף 1.2 הגדרנו את מושג השדה. השדה היסודי שממנו שאבנו השראה להגדרה הכללית של שדה היה שדה המספרים הרציונליים. משהבאנו את ההגדרה הכללית, ראינו מיד כי גם אוסף המספרים הממשיים, ביחד עם פעולות החיבור והכפל הרגילות, מהווה שדה. בין שני שדות אלה קיים קשר המזדקר לעין - כל מספר רציונלי הוא גם מספר ממשי. אך מתברר שהקשר עמוק אף יותר.

נניח כי בפנינו שדה נתון $(F,+_F,\cdot_F)$,[1] ונניח כי $K\subseteq F$ תת־קבוצה. ניתן לחבר כל זוג איברים של K (שהרי החיבור מוגדר עבור כל זוג איברים של F, ובפרט עבור כל זוג איברים של K). במובן זה נאמר שפעולת החיבור $+_F$ על F **משרה** פעולת חיבור על K, שנסמנה $+_K$. אומרים גם שהפעולה $+_K$ היא **צמצום** ל־K של הפעולה $+_F$. שימו לב, הפעולה $+_K$ פועלת על זוג איברים נתון בדיוק כפי שפועלת הפעולה $+_F$; ההבדל היחיד הוא בקבוצה שעליה מוגדרת הפעולה! בדומה לכך, פעולת הכפל $\cdot_F$ על F משרה פעולה $\cdot_K$ על K. כעת נוכל לבדוק אם הקבוצה K, בצירוף זוג הפעולות $+_K$ ו־$\cdot_K$, מהווה שדה - כלומר האם מתקיימים עבורה כל התנאים של הגדרה 1.2.1. אם התשובה חיובית, נאמר ש־$(K,+_K,\cdot_K)$ הוא **תת־שדה** של $(F,+_F,\cdot_F)$. ננסח זאת כהגדרה:

הגדרה 6.1.1 תת־שדה

יהיו $(F,+_F,\cdot_F)$ ו־$(K,+_K,\cdot_K)$ שדות. נאמר ש־$(K,+_K,\cdot_K)$ הוא **תת־שדה** של $(F,+_F,\cdot_F)$,[2] אם הקבוצה K היא תת־קבוצה של F, ואם הפעולות של השדות מתיישבות זו עם זו במובן הבא: לכל $x,y\in K$ מתקיים $x+_F y=x+_K y$ ו־$x\cdot_F y=x\cdot_K y$.

הערה

לאור ההגדרה, אם K הוא תת־שדה של F, פירוש הדבר הוא שהפעולות של שני השדות הן "אותן הפעולות" כאשר מצטמצמים ל־K. לכן, כדי להימנע מסרבול טכני, לרוב לא נשתמש בסימונים נפרדים עבור הפעולות על F והפעולות על K, ונשתמש בסימוני הקיצור $+,\cdot$ גם כאשר אנו רואים את הפעולות הללו כפעולות על F, וגם כאשר אנו רואים אותן (על־ידי צמצום) כפעולות על K.

דוגמה א

אוסף המספרים הממשיים $\mathbb{R}$ הוא שדה ביחס לפעולות החיבור והכפל הרגילות. גם אוסף המספרים הרציונליים $\mathbb{Q}$ הוא שדה ביחס לפעולות החיבור והכפל הרגילות עליו (שהן הצמצום של פעולות החיבור והכפל על $\mathbb{R}$). לכן שדה המספרים הרציונליים $\mathbb{Q}$ הוא תת־שדה של שדה המספרים הממשיים $\mathbb{R}$.

◀

---

1 אנו מסמנים כאן את כל רכיבי השדה, ללא קיצורים - F היא קבוצת איברי השדה, $+_F$ פעולת החיבור, ו־$\cdot_F$ פעולת הכפל.

2 או בקיצור, ש־K הוא תת־שדה של F.

דוגמה ב

אוסף המספרים השלמים $\mathbb{Z}$ אינו שדה ביחס לפעולות החיבור והכפל הרגילות (כפי שראינו בסעיף 1.2), וממילא אינו תת־שדה של $\mathbb{Q}$, וגם אינו תת־שדה של $\mathbb{R}$. ◄

דוגמה ג

הקבוצה (הסופית) $\{0,1\}$ היא תת־קבוצה של $\mathbb{Q}$. האם קבוצה זו, עם פעולות החיבור והכפל הרגילות, היא תת־שדה של $\mathbb{Q}$? לא! אחת הדרישות בהגדרה 1.2.1 (דרישה א) היא סגירות ביחס לחיבור. כאן $1+1=2\notin\{0,1\}$, ולכן דרישה זו אינה מתקיימת. שימו לב שעל אותה הקבוצה $\{0,1\}$ הגדרנו פעולות אחרות (חיבור וכפל מודולו 2) שהפכו אותה לשדה, שלו קראנו בשם $\mathbb{Z}_2$. למרות ש־$\mathbb{Z}_2$ הוא שדה, ולמרות שקבוצת איבריו מוכלת ב־$\mathbb{Q}$, $\mathbb{Z}_2$ אינו תת־שדה של $\mathbb{Q}$, שכן הפעולות עליו אינן מתקבלות על־ידי צמצום של הפעולות על $\mathbb{Q}$. אכן, בשדה $\mathbb{Q}$, ערכו של הסכום $1+1$ הוא 2, ואילו בשדה $\mathbb{Z}_2$, ערכו של הסכום $1+1$ הוא 0. ◄

שאלה 6.1.1

האם השדה $\mathbb{Z}_2$ הוא תת־שדה של השדה $\mathbb{Z}_5$?

התשובה בעמוד 125

נניח שנתון לנו שדה F ותת־שדה שלו K. פירוש הוא הדבר ש־K שדה "קטן יותר" מ־F,[3] ובאופן שקול – ש־F "גדול יותר".[4] נציין עובדה זו באמצעות המונח הבא:

הגדרה 6.1.2 שדה־הרחבה

נאמר ש־F הוא **שדה־הרחבה** של K, אם K הוא תת־שדה של F.

דוגמה

מאחר ש־$\mathbb{Q}$ הוא תת־שדה של $\mathbb{R}$, $\mathbb{R}$ הוא שדה־הרחבה של $\mathbb{Q}$. ◄

הדוגמה לעיל היא היחידה שנתנו עד כה לשדה ולשדה הרחבה שלו. האם קיימות דוגמאות נוספות? תשובה טריוויאלית ניתנת על־ידי ההבחנה הבאה – כל שדה הוא תת־שדה של עצמו (ובאופן שקול, כל שדה הוא שדה־הרחבה של עצמו).

טענה 6.1.3

יהי F שדה. אזי F הוא תת־שדה של F.

---

3 או לפחות לא "גדול יותר".

4 או לפחות לא "קטן יותר".

הוכחה

אין מה להוכיח - F הוא בוודאי תת־קבוצה של עצמו, והפעולות הן אותן הפעולות.

מ.ש.ל.

כך למשל, $\mathbb{Q}$ הוא תת־שדה של עצמו, $\mathbb{Z}_2$ תת־שדה של עצמו, וכולי. אם ברצוננו למצוא דוגמאות נוספות לשדה ולתת־שדה שלו (באופן שקול - שדה ושדה הרחבה שלו), נראה כי עלינו לבחון שדות שונים, ולנסות למצוא תת־קבוצות שלהן המהוות שדות ביחס לאותן פעולות. במבט ראשון, כל בדיקה כזאת נראית מייגעת - עלינו לעבור על כל התנאים (הרבים) שבהגדרה 1.2.1, ולבדוק האם כולם מתקיימים. אך מתברר שנוכל לקצר בדיקות אלה באופן משמעותי, כפי שנובע מהטענה הבאה:

טענה 6.1.4

יהי F שדה ותהי K תת־קבוצה של F. אזי K תת־שדה של F אם ורק אם מתקיים:

א. K סגורה לגבי פעולות החיבור והכפל.

ב. K מכילה את 0, איבר האפס של F, ואת 1, איבר היחידה של F. יתר על כן, 0 הוא איבר האפס של K, ו־1 הוא איבר היחידה של K.

ג. לכל $x \in K$ מתקיים $-x \in K$.

ד. לכל $x \neq 0$ ב־K מתקיים $x^{-1} \in K$.

הוכחה

נסמן ב־$+, \cdot$ את פעולות החיבור והכפל על F.

תחילה נניח כי K תת־שדה של F, ונוכיח כי מתקיימות התכונות א-ד:

א. מכיוון ש־K עצמו הוא שדה, ברור שמתקיימת תכונה א - תכונת הסגירות לגבי החיבור והכפל.

ב. לפי התנאי הרביעי בהגדרת השדה, K מכיל איבר ניטרלי ביחס לחיבור, נסמנו 0_K,[5] ואיבר ניטרלי ביחס לכפל, נסמנו 1_K.[6] מאחר ש־0 ניטרלי ביחס לחיבור ב־F, מתקיים $0_K + 0 = 0_K$. מצד שני, מאחר ש־0_K הוא איבר האפס של K, מתקיים $0_K + 0_K = 0_K$. לכן ב־F מתקיים $0 + 0_K = 0_K = 0_K + 0_K$. נשמיט 0_K ונקבל $0_K = 0$. באופן דומה מראים כי $1_K = 1$. הוכחנו אם כן את תכונה ב.

ג. יהי $x \in K$. נסמן ב־$-x$ את הנגדי של x ב־F, כלומר $x + (-x) = 0$. אך ל־x קיים גם נגדי y ב־K, כלומר $x + y = 0_K$. מכיוון ש־$0_K = 0$, מתקיים $x + y = x + (-x) = 0$. נשמיט את x ונקבל $y = -x$. $y \in K$ ולכן $-x \in K$.

ד. ההוכחה דומה להוכחה של ג.

כעת נוכיח את הכיוון ההפוך. נניח כי K מקיימת את התכונות א-ד, ונוכיח כי K תת־שדה, כלומר נוכיח ש־K הוא שדה.

5 שימו לב, אין זה ברור א־פריורי שאיבר זה הוא איבר האפס 0 של F - עלינו להוכיח זאת.

6 גם כאן, אין זה ברור שאיבר זה הוא 1.

אם נתבונן בהגדרת השדה, נראה כי כל שנותר להוכיח הוא את תכונות הקיבוציות, החילופיות, וכלל הפילוג. קיומן של כל אחת מתכונות אלה עבור איברי K נובעת מיידית מקיומן עבור איברי F. נוכיח לדוגמה את תכונת החילופיות של החיבור:

יהיו $x, y \in K$. אלה הם בפרט איברים של F, ומחילופיות החיבור ב־F נקבל $x + y = y + x$, כדרוש.

מ.ש.ל.

טענה 6.1.4 מקצרת בהרבה את הבדיקות שעלינו לעשות כדי לבדוק אם תת־קבוצה נתונה של שדה מסוים היא תת־שדה שלו - איננו צריכים לבדוק את קיום כל התנאים בהגדרת השדה, אלא רק את ארבעת התנאים המופיעים בטענה 6.1.4.

כעת ננצל את טענה 6.1.4 כדי למצוא הרחבת שדות חדשה. כדי לבנות הרחבה כזאת, עלינו לבחור שדה כלשהו F, ולנסות למצוא בתוכו תת־שדה K השונה מ־F. תחילה ננסה לעשות זאת כאשר F הוא הדוגמה הראשונה לשדה שפגשנו - שדה המספרים הרציונליים. עלינו למצוא איזושהי תת־קבוצה $K \subseteq \mathbb{Q}$, העונה על תנאי טענה 6.1.4. **נניח** שמצאנו קבוצה כזאת, וננסה להסיק מסקנות אודותיה. לאור טענה 6.1.4, בהכרח $0,1 \in K$. כמו כן, מכיוון ש־K סגורה לחיבור, כל מספר טבעי n שייך ל־K, שכן נוכל לרשום את n כסכום של 1־ים. יתר על כן, גם הנגדי $-n$ שייך ל־K. מכאן נסיק שכל מספר שלם n שייך ל־K. אבל אז גם ההופכי של כל שלם (שונה מאפס) שייך ל־K, כלומר $\frac{1}{n} \in K$ לכל $0 \neq n \in \mathbb{Z}$. כעת נתבונן במספר רציונלי שרירותי $\frac{m}{n} \in \mathbb{Q}$, כאשר $m,n \in \mathbb{Z}$ ו־$n \neq 0$. נוכל לרשום את המספר כך: $\frac{m}{n} = m \cdot \frac{1}{n}$. לאור האמור לעיל, זוהי מכפלה של שני איברים של K, ומכיוון ש־K סגורה לגבי הכפל, $\frac{m}{n} \in \mathbb{Q}$. הראינו שכל מספר רציונלי שייך ל־K, ולכן $K \in \mathbb{Q}$!

את מסקנות הדיון האחרון ננסח כמשפט:

משפט 6.1.5

לשדה המספרים הרציונליים $\mathbb{Q}$ אין תת־שדות פרט לעצמו.

במילים אחרות, השדה $\mathbb{Q}$ הוא שדה **מזערי**. האם פגשנו כבר בשדות נוספים בעלי תכונה זו? על כך תענו בשאלה הבאה.

שאלה 6.1.2

הוכיחו כי לכל מספר ראשוני p, לשדה $\mathbb{Z}_p$ אין תת־שדות פרט לעצמו.

התשובה בעמוד 125

בפרק 5 ציינו שהשדה $\mathbb{Q}$, וכל אחד מהשדות $\mathbb{Z}_p$, נקראים שדות ראשוניים. הסיבה ל"ראשוניותם" טמונה בהיותם שדות מזעריים (כפי שראינו שזה עתה).[7] למעשה, אלה השדות המזעריים היחידים. לא נוכיח עובדה זו.

אם נעיין בדיון שבמסגרתו הוכחנו את משפט 6.1.5, נראה כי הוכחנו אף יותר:

משפט 6.1.6

יהי F שדה־הרחבה של $\mathbb{Q}$, ויהי K תת־שדה של F. אזי $K \subseteq \mathbb{Q}$.

שאלה 6.1.3

הוכיחו את משפט 6.1.6.

התשובה בעמוד 125

ניסיוננו למצוא דוגמה חדשה להרחבה לא־טריוויאלית של שדה, על־ידי מציאת תת־שדה של $\mathbb{Q}$, כשל. כדי לתת דוגמה להרחבת שדות חדשה יהיה עלינו לתאר שדה חדש, שאותו לא פגשנו עד כה. המשך סעיף זה מוקדש לבניית דוגמה כזאת. חומר זה הוא בגדר חומר רשות (אם כי אנו סבורים שהוא מאיר עיניים), ואתם רשאים לדלג לסעיף הבא - שבו תפגשו דוגמה נוספת להרחבה של שדה, בעלת חשיבות מרכזית במתמטיקה כולה.

כדי לבנות את הדוגמה הרצויה לנו, נעבור לשדה ה"מוכר ביותר" אחרי שדה המספרים הרציונליים - שדה המספרים הממשיים $\mathbb{R}$, וננסה למצוא לו תת־שדה חדש K. לאור משפט 6.1.6, בהכרח $\mathbb{Q} \subseteq K$. מכיוון שאנו מחפשים שדה חדש - חייב להיות ב־K מספר שאינו רציונלי. האם נתקלנו כבר במספר ממשי שאינו רציונלי? כן! בסעיף 5.3 ראינו שהמספר הממשי $\sqrt{2}$ אינו רציונלי. נניח אם כן, שהשדה K מכיל את $\sqrt{2}$. מהסגירות לכפל נובע ש־K בהכרח מכיל גם כל כפולה של $\sqrt{2}$ במספר רציונלי, ומהסגירות לחיבור - גם כל סכום של מספר כזה ומספר רציונלי. כלומר, כל מספר ממשי מהצורה $a+\sqrt{2}b$, כאשר $a,b \in \mathbb{Q}$, שייך ל־K. האם השדה K (שאנו מנסים לבנות) מכיל איברים נוספים? ברצוננו להראות שאינו **חייב** להכיל איברים נוספים. כלומר, שאוסף המספרים הממשיים מהצורה לעיל מהווה שדה.

טענה 6.1.7

נסמן ב־$\mathbb{Q}\left(\sqrt{2}\right)$ את אוסף המספרים הממשיים מהצורה $a+\sqrt{2}b$, כאשר $a,b \in \mathbb{Q}$. אזי $\mathbb{Q}\left(\sqrt{2}\right)$ הוא תת־שדה של $\mathbb{R}$.

7 האנלוגיה למספרים הראשוניים טמונה בכך שמספרים אלה "מזעריים ביחס לכפל" - למספר ראשוני אין מחלקים פרט לעצמו (ופרט למחלק הטריוויאלי 1).

הוכחה

ראשית, ברור ש- $\mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{R}$.

נוכיח כעת את קיום ארבע התכונות המופיעות בטענה 6.1.4.

א. יהיו $a+\sqrt{2}b,\ c+\sqrt{2}d$ איברים של $\mathbb{Q}\left(\sqrt{2}\right)$ (כלומר $a,b,c,d \in \mathbb{Q}$). אזי הסכום

$$(a+\sqrt{2}b)+(c+\sqrt{2}d)=(a+c)+\sqrt{2}(b+d)$$

שייך גם הוא ל- $\mathbb{Q}\left(\sqrt{2}\right)$ (שכן $a+b,\ c+d$ גם הם רציונליים). באופן דומה, גם המכפלה

$$(a+\sqrt{2}b)\cdot(c+\sqrt{2}d)=(ac+2bd)+\sqrt{2}(ad+bc)$$

שייכת ל- $\mathbb{Q}\left(\sqrt{2}\right)$.

ב. ברור ש- $0,1 \in \mathbb{Q}\left(\sqrt{2}\right)$, כי $0=0+\sqrt{2}\cdot 0,\ 1=1+\sqrt{2}\cdot 0$.

ג. לכל $a+\sqrt{2}b$ ב- $\mathbb{Q}\sqrt{2}$, גם $-(a+\sqrt{2}b)=(-a)+\sqrt{2}(-b)$ שייך ל- $\mathbb{Q}\sqrt{2}$.

ד. יהי $x=a+\sqrt{2}b$ איבר שונה מאפס של $\mathbb{Q}\left(\sqrt{2}\right)$. ברור כי $a,b\in\mathbb{Q}$. נשים לב ש- $a^2 \neq 2b^2$, אחרת - a/b הוא שורש רציונלי של 2. כמו כן, $a^2-2b^2 \in \mathbb{Q}$. נתבונן באיבר $\dfrac{a}{a^2-2b^2}+\sqrt{2}\dfrac{(-b)}{a^2-2b^2}$ של $\mathbb{Q}\left(\sqrt{2}\right)$, ונראה כי הוא הופכי ל- $x=a+\sqrt{2}b$. אכן:

$$\left(\frac{a}{a^2-2b^2}+\sqrt{2}\frac{(-b)}{a^2-2b^2}\right)(a+\sqrt{2}b)=\frac{a^2-2b^2}{a^2-2b^2}+\sqrt{2}\frac{ab-ba}{a^2-2b^2}=1+\sqrt{2}\cdot 0=1$$

מ.ש.ל.

מצאנו, אם כן, שדה $\mathbb{Q}\left(\sqrt{2}\right)$, המכיל ממש את $\mathbb{Q}$, ומוכל ב- $\mathbb{R}$. יתר על כן, השדה $\mathbb{Q}\left(\sqrt{2}\right)$ מוכל ממש ב- $\mathbb{R}$. כלומר, יש מספרים ממשיים שאינם שייכים ל- $\mathbb{Q}\left(\sqrt{2}\right)$. לא נוכיח עובדה זו כאן,[8] אך נציין שהמספר הממשי π, למשל, אינו שייך ל- $\mathbb{Q}\left(\sqrt{2}\right)$. השדה $\mathbb{Q}\left(\sqrt{2}\right)$, אם כן, הוא שדה הרחבה "חדש" של $\mathbb{Q}$, ו- $\mathbb{R}$ הוא שדה הרחבה של $\mathbb{Q}\left(\sqrt{2}\right)$, שהרי $\mathbb{Q}\left(\sqrt{2}\right)$ הוא שדה המוכל (ממש) ב- $\mathbb{R}$.

8 תלמידים שמכירים את המושג "עוצמה" יוכלו להוכיח זאת בקלות - ודאו כי עוצמת קבוצת איברי השדה $\mathbb{Q}\left(\sqrt{2}\right)$ היא $\aleph_0$, בעוד עוצמת קבוצת המספרים הרציונליים היא $\aleph$, וממילא קבוצות אלה שונות, ולכן גם השדות הנידונים שונים.

6.2 שדה המספרים המרוכבים

לשדה הממשיים $\mathbb{R}$ יש תכונות שימושיות רבות, ובעיות רבות במתמטיקה ובמדעים ניתנות לתיאור בשדה זה. אך לשדה זה "מגרעת" משמעותית, המקשה על פתרונן של בעיות רבות - לא לכל מספר יש שורש ריבועי בשדה. יתר על כן, לכל מספר ממשי שלילי x, לא קיים מספר ממשי y המקיים $y^2 = x$. בסעיף זה ברצוננו לבצע מהלך שמטרתו "לתקן" בעיה זו, על־ידי מציאת **שדה־הרחבה** של $\mathbb{R}$ שבו יהיה שורש לכל מספר. השדה שנבנה הוא אובייקט קלאסי במתמטיקה, המכונה **שדה המספרים המרוכבים**. בנייתו של שדה המספרים המרוכבים היא תוצאה של תהליך היסטורי ארוך, הכרוך בהתפתחות המתמטיקה (והאלגברה בפרט) והפיסיקה. המהלך שנבצע נועד להראות כיצד "מגיעים" מתוך מוטיבציה מתמטית, בסדרה של צעדים מחשבתיים, להגדרה פורמלית של שדה המספרים המרוכבים. תיאור המהלך הוא בגדר **חומר רשות**, ובסוף הסעיף נביא בכתב מודגש תמצית קצרה המסכמת את כל שעליכם לדעת אודות שדה זה.

כדי "למצוא" את שדה המספרים המרוכבים, ננסה לבצע דיון תיאורטי על אודות אופיים המשוער של איברים בשדה זה, ומתוך דיון זה "לחלץ" את הגדרתם. מטרתנו, אם כן, היא למצוא שדה הרחבה F של $\mathbb{R}$, כך שיהיה ב־ F שורש ריבועי לכל מספר ממשי. כלומר, לכל $x \in \mathbb{R}$ יהיה קיים $y \in F$ כך ש־ $y^2 = x$.

הבחנה מקדימה, שתקל על עבודתנו, היא שאת הדרישה "לכל מספר ממשי יהיה שורש ב־ F", נוכל לרכך ולדרוש במקומה כי למספר הממשי -1 יהיה שורש ב־ F. אכן, אם מצאנו שדה F שכזה, שבו יש איבר y המקיים $y^2 = -1$, יהיה בשדה גם שורש לכל מספר ממשי שלילי. נראה זאת:

אם $x \in \mathbb{R}$ מספר שלילי כלשהו, אז נסמן ב־ $\sqrt{-x}$ את השורש (החיובי) של המספר החיובי $-x$, ונקבל כי האיבר $y\sqrt{-x}$ מקיים $\left(y\sqrt{-x}\right)^2 = y^2(-x) = (-1)(-x) = x$, כפי שרצינו.

אם כן, **נניח** שמצאנו שדה הרחבה F של שדה הממשיים, שבו קיים שורש ל־ -1. נסמן שורש זה ב־ i.[1] $i \in F$, ומאחר ש־ F סגור לחיבור ולכפל, גם המכפלה $2i$ שייכת ל־ F, ובאופן כללי יותר - כל מכפלה מהצורה $i \cdot b$, כאשר b ממשי, שייכת ל־ F. כמו כן, מאחר ש־ F סגור לחיבור, גם כל סכום מהצורה $a + ib$, כאשר a ו־ b ממשיים, הוא איבר של F. האם F מכיל איברים נוספים? ייתכן שכן, אך ברצוננו להראות שלצרכינו שלנו די באוסף האיברים ב־ F שזה עתה תיארנו, כדי לספק את דרישתנו:

---

1 האות i נבחרה לציון imaginary - **דמיוני**. אנו "מדמיינים" יצור מתמטי חדש, בעל התכונה שריבועו הוא המספר -1.

טענה 6.2.1

יהי F שדה הרחבה של $\mathbb{R}$, ונניח כי קיים איבר $i \in F$ המקיים $i^2 = -1$. אזי $K = \{a + ib | a,b \in \mathbb{R}\}$ [2] הוא תת־שדה של F.

הוכחה

אם $a + ib,\ c + id \in K$, אזי גם הסכום

$$(a + ib) + (c + id) = (a + c) + i(b + d) \qquad (1)[3]$$

שייך ל־ K, כי a,b,c,d הם מספרים ממשיים, ולכן גם $a + c,\ b + d$ הם מספרים ממשיים. באופן דומה, המכפלה:

$$\begin{aligned}(a + ib) \cdot (c + id) &= ac + iad + ibc + i^2bd \\ &= ac + i(ad + bc) + (-1)bd = (ac - bd) + i(ad + bc)\end{aligned} \qquad (2)$$

שייכת ל־ K. לכן K סגור לחיבור ולכפל.

כמו כן, K מכיל כל מספר ממשי, ובפרט מכיל את $0,1$.[4]

האיבר הנגדי של איבר $a + ib \in K$ הוא $-a + i(-b)$, כי

$$a + ib + \left(-a + i(-b)\right) = 0 + i0 = 0 + 0 = 0$$

וגם הוא שייך ל־ K.

על פי טענה 6.1.4, נותר להראות שההופכי של איבר $0 \neq a + ib \in K$ שייך גם הוא ל־ K. ואכן, נבחין כי האיבר

$$\frac{a}{a^2 + b^2} + i\frac{(-b)}{a^2 + b^2}$$

הוא הופכי ל־ $a + ib$ (בדקו ישירות).

מ.ש.ל.

מה משמעות הטענה שזה עתה הוכחנו? שימו לב שלא הוכחנו את קיום השדה F. כל שהראינו הוא, ש**אם** קיים שדה כזה F (כלומר, שדה הרחבה של הממשיים המכיל שורש ל־ -1, שאותו סימנו ב־ i), אזי התת־קבוצה $K = \{a + ib | a,b \in \mathbb{R}\}$ גם היא שדה. תת־שדה זה מכיל בוודאי את הממשיים (הציבו $b = 0$) ואת i (הציבו $a = 0,\ b = 1$).

מדוע אנו מתבוננים בתת־השדה K? בשדה F שממנו יצאנו, אין אנו יודעים כיצד "נראים" האיברים, ואין אנו יודעים דבר על הגדרת הפעולות בשדה זה, פרט לכך שהן מרחיבות את הפעולות

2 שימו לב, סימון החיבור המופיע בהגדרת K הוא החיבור בשדה F, והביטוי ib הוא קיצור עבור $i \cdot b$, כאשר הכפל כאן הוא הכפל בשדה F.

3 ודאו נכונות השוויון על פי תכונות החיבור והכפל בשדה.

4 שימו לב, - המספרים הממשיים $0,1$ הם איבר האפס ואיבר היחידה של F, שכן זהו שדה הרחבה של הממשיים.

על $\mathbb{R}$, וכי $i^2 = -1$. לעומת זאת, בתת־השדה K יש לנו תיאור פשוט לאיברים, ובאמצעות תיאור זה אנו מסוגלים גם לתאר בקלות את פעולת החיבור (ראו שוויון (1) בהוכחת טענה 6.2.1) ואת פעולת הכפל (ראו שוויון (2) בהוכחת טענה 6.2.1).

כלומר, מצאנו תת־שדה בעל תיאור נוח, ובעל התכונות הרצויות לנו. כעת נבצע את הצעד המכריע - נהפוך את הקערה על פיה, ונשתמש בתיאור שמצאנו כדי **להגדיר** שדה בעל התכונות המבוקשות.

הגדרה 6.2.2 שדה המספרים המרוכבים

נסמן ב־ $\mathbb{C}$ את אוסף כל הביטויים מהצורה $a + ib$, כאשר a,b מספרים ממשיים. נגדיר על $\mathbb{C}$ פעולות חיבור $+_{\mathbb{C}}$ וכפל $\cdot_{\mathbb{C}}$, באופן הבא:

$$(a + ib) +_{\mathbb{C}} (c + id) = (a + c) + i(b + d)$$

$$(a + ib) \cdot_{\mathbb{C}} (c + id) = (ac - bd) + i(ad + bc)$$

לאיברי $\mathbb{C}$ נקרא **מספרים מרוכבים**.[5]

הערה

הביטויים מהצורה $a + ib$ המופיעים בהגדרה 6.2.2 הם ביטויים פורמליים בלבד. בשלב זה האות i מהווה סמל בלבד - אות המופיעה על הנייר; יתר על כן, גם לסימן ה־ $+$ המופיע בביטוי $a + ib$ אין מלכתחילה משמעות כחיבור. שני ביטויים פורמליים כאלה, $a + ib$ ו־ $c + id$, הם שווים, אם ורק אם הם זהים לחלוטין, כלומר אם $a = c, b = d$.

טענה 6.2.3

הקבוצה $\mathbb{C}$, בצירוף זוג הפעולות שהגדרנו, מהווה שדה.

הוכחה

יש לוודא כי כל תנאי הגדרה 1.2.1 מתקיימות. את קיום דרישות א–ג (סגירות, קיבוציות, וחילופיות הפעולות), וכן את כלל הפילוג, נשאיר לקוראים לבדוק ישירות בעצמם, באמצעות הגדרת הפעולות. נעבור לבדוק את יתר הדרישות. האיבר $0 + i0$ ניטרלי ביחס לחיבור, שכן

$$(a + ib) +_{\mathbb{C}} (0 + i0) = (a + 0) + i(b + 0) = a + ib$$

לכל a,b ממשיים.

באופן דומה תוכלו לבדוק כי לכל מספר מרוכב $a + ib$ יש איבר נגדי, האיבר $(-a) + i(-b)$.

האיבר $1 + i0$ הוא איבר יחידה ב־ $\mathbb{C}$, שכן לכל a,b ממשיים מתקיים:

$$(a + ib) \cdot_{\mathbb{C}} (1 + i0) = (a \cdot 1 - b \cdot 0) + i(a \cdot 0 + b \cdot 1) = a + ib$$

5 מספרים מרוכבים - Complex numbers

לבסוף, לכל $a + ib$ השונה מ־$0 + i0$ (כלומר $a \neq 0$, או $b \neq 0$), קיים איבר הופכי, האיבר $\frac{a}{a^2 + b^2} + i\frac{(-b)}{a^2 + b^2}$. אכן:

$$\begin{aligned}&\left(\frac{a}{a^2 + b^2} + i\frac{(-b)}{a^2 + b^2}\right)(a + ib)\\ &\quad = \left(\frac{a}{a^2 + b^2}a - \frac{(-b)}{a^2 + b^2}b\right) + i\left(\frac{a}{a^2 + b^2}b + \frac{(-b)}{a^2 + b^2}a\right)\\ &\quad = \frac{a^2 + b^2}{a^2 + b^2} + i\frac{ab - ba}{a^2 + b^2} = 1 + i0\end{aligned}$$

מ.ש.ל.

נדגיש שוב שהגדרנו את האיברים $a + ib$ כביטויים בלבד – מלכתחילה האות i והסימן $+$ מהווים סמלים פורמליים ללא משמעות נוספת. כדי לתת לביטויים אלה את המשמעות הרצויה, **נזהה** כל מספר ממשי a עם הזוג $a + i0$; כלומר, נראה את המספר הממשי a כסימון מקוצר עבור המספר המרוכב $a + i0$. בעזרת זיהוי זה, אנו רואים את שדה המספרים הממשיים כתת־שדה של שדה המספרים המרוכבים.[6] באופן דומה, נראה את האות הבודדת i כסימון מקוצר עבור הביטוי $0 + i1$.
כעת נשים לב שאת המספר המרוכב $a + ib$ נוכל לכתוב, בהתאם להגדרת הפעולות לעיל, כך:

$$a + ib = (a + i0) +_{\mathbb{C}} (0 + ib) = (a + i0) +_{\mathbb{C}} (0 + i1) \cdot_{\mathbb{C}} (b + i0) = a +_{\mathbb{C}} i \cdot_{\mathbb{C}} b$$

הביטוי ib מקבל אם כן משמעות כתוצאת הכפל $i \cdot_{\mathbb{C}} b$ (בהתאם לכלל הכפל שהגדרנו), וסימן ה־$+$ המופיע בביטוי $a + ib$ מקבל משמעות כסכום (בהתאם לכלל החיבור ב־$\mathbb{C}$) של a ו־ib.
לאור האמור לעיל, נרשה לעצמנו מעתה לסמן את פעולת החיבור $+_{\mathbb{C}}$ בקצרה על־ידי $+$, ואת פעולת הכפל $\cdot_{\mathbb{C}}$ נסמן בקצרה על־ידי $\cdot$. כמו כן, נשים לב כי מתקיים

$$i^2 = (0 + i1)(0 + i1) = (0 \cdot 0 - 1 \cdot 1) + i(0 \cdot 1 + 1 \cdot 0) = -1 + i0 = -1$$

כפי שרצינו.

בנוסף, נוכל לראות את המספר המרוכב $a + i(-b)$ כסכום של שני המספרים המרוכבים a ו־$i(-b)$, והאחרון אינו אלא הנגדי של ib, כלומר $i(-b) = -ib$. לכן $a + i(-b) = a + (-(ib))$, ונסכים לרשום $a - ib$ במקום $a + i(-b)$.

כמו כן, את המספר המרוכב $a + ib$ אפשר לראות כסכום של המספרים המרוכבים a ו־ib, ואת ib כמכפלה של i ו־b, ומכיוון שהכפל הוא חילופי, $ib = bi$. מעתה והלאה לא נקפיד להציג מספר מרוכב דווקא בצורה $a + ib$ אלא נרשום במקומו לפעמים $a + bi$.

6 כאן יש לוודא – ותוכלו לעשות זאת בקלות – כי פעולות החיבור והכפל של המספרים הממשיים הן צמצום פעולות החיבור והכפל של המספרים המרוכבים שהגדרנו לעיל.

אם דקויות הדיון לעיל נראות לכם מבלבלות - אין צורך כי תתעכבו עליהן. את שעליכם לזכור נסכם כך:

- **השדה $\mathbb{C}$ הוא שדה הרחבה של שדה המספרים הממשיים. כלומר, זהו שדה המכיל בתוכו את כל המספרים הממשיים, ופעולות החיבור והכפל המוגדרות עליו מרחיבות את פעולות החיבור והכפל הרגילות של מספרים ממשיים.**
- **ב־ $\mathbb{C}$ קיים איבר i המקיים את השוויון** $i^2 = -1$.
- **עבור כל איבר $z \in \mathbb{C}$, קיים זוג יחיד (a,b) של מספרים ממשיים כך שמתקיים** $z = a + ib$.

בזאת סיימנו את הדיון התיאורטי בהגדרת שדה המספרים המרוכבים. בסעיפים הבאים נראה כיצד עובדים עם מספרים מרוכבים, הלכה למעשה.

6.3 החלק הממשי והחלק המדומה

באמצעות תכונות החיבור והכפל בשדה, והעובדה כי $i^2 = -1$, נוכל לבצע על נקלה חישובים בשדה המספרים המרוכבים, המערבים פעולות חיבור וכפל.

דוגמה

ב־ $\mathbb{C}$, נחשב את ערך הביטוי:

$$\left(\frac{1}{2}+i\right)(3+i)+(5+i)(-i)(1+i)$$

ערכו של המחובר הראשון הוא:

$$\left(\frac{1}{2}+i\right)(3+i)=\frac{3}{2}+3i+\frac{1}{2}i+i^2=\frac{3}{2}+(-1)+\left(3+\frac{1}{2}\right)i=\frac{1}{2}+\frac{7}{2}i$$

ערכו של המחובר השני, $(5+i)(-i)(1+i)$, הוא:

$$(5+i)(-i)(1+i)=(1-5i)(1+i)=1-5i+i-5i^2=1-5(-1)-4i=6-4i$$

מכאן נקבל את ערכו של הביטוי כולו:

$$\left(\frac{1}{2}+\frac{7}{2}i\right)+(6-4i)=\frac{13}{2}-\frac{1}{2}i$$

▶

שאלה 6.3.1

בטאו את המספרים הבאים בצורה $a+ib$.

א. i^3

ב. $(2i)\cdot i\cdot 3$

ג. $2i+5i$

ד. $(2i)^5$

ה. $\left(\sqrt{2}i\right)^2$

התשובה בעמוד 125

הגדרה 6.3.1

יהי $z=a+ib$ [1] מספר מרוכב כלשהו, כאשר (a,b) מספרים ממשיים.

a נקרא **החלק הממשי** של z.

b נקרא **החלק המדומה** של z.

את החלק הממשי של z נסמן ב־ $\operatorname{Re} z$.[2]

את החלק המדומה של z נסמן ב־ $\operatorname{Im} z$.[3]

1 נהוג לסמן מספר מרוכב באות z.

2 Re – ראש התיבה Real שמשמעה "ממשי".

3 Im – ראש התיבה Imaginary שמשמעה "מדומה". למרבה הצער, סימון זה משמש במתמטיקה גם לציון התמונה של פונקציה. אך אין חשש לבלבול, משום שהאחד מתייחס למספרים מרוכבים והאחר לפונקציות.

שימו לב, החלק הממשי והחלק המדומה של המספר המרוכב z, **שניהם מספרים ממשיים**.[4]

הערות

א. לכל מספר מרוכב z מתקיים:

$$z = \operatorname{Re} z + i \cdot \operatorname{Im} z$$

ב. המספר המרוכב z הוא **ממשי**, אם ורק אם מתקיים:

$$\operatorname{Im} z = 0$$

ג. נאמר שמספר המרוכב z הוא **מדומה**,[5] אם:

$$\operatorname{Re} z = 0$$

ד. שני מספרים מרוכבים $z = a + ib$ ו־ $w = c + id$ הם שווים, אם ורק אם החלקים הממשיים והחלקים המדומים שלהם שווים זה לזה, כלומר $a = c,\ b = d$.

שאלה 6.3.2

ציינו מהו $\operatorname{Re} z$ ומהו $\operatorname{Im} z$ עבור כל אחד מהמספרים המרוכבים שלפניכם:

א. $z = -i$

ב. $z = i^2$

ג. $z = 5 + 8i$

ד. $z = -3 - \frac{1}{2}i$

ה. $z = 7$

התשובה בעמוד 125

שאלה 6.3.3

יהיו z_1 ו־ z_2 שני מספרים מרוכבים.

בטאו בעזרת $\operatorname{Re} z_1$, $\operatorname{Re} z_2$, $\operatorname{Im} z_1$, $\operatorname{Im} z_2$ את:

א. $\operatorname{Re}(z_1 + z_2)$

ב. $\operatorname{Re}(z_1 \cdot z_2)$

ג. $\operatorname{Im}(z_1 + z_2)$

ד. $\operatorname{Im}(z_1 \cdot z_2)$

התשובה בעמוד 125

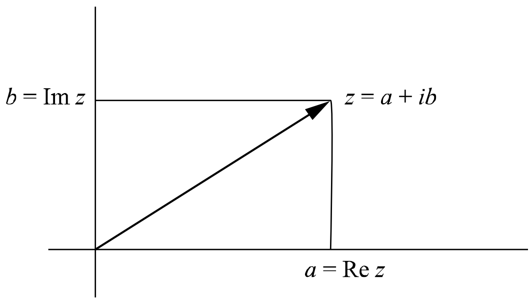
אפשר להציג את שדה המספרים המרוכבים בדרך גיאומטרית כך:

לכל מספר מרוכב $z \in \mathbb{C}$ נוכל להתאים זוג מספרים ממשיים - הזוג $(\operatorname{Re} z, \operatorname{Im} z)$. התאמה זו היא, בבירור, חד־חד ערכית ועל (ודאו!).

4 נהוג לסמן את החלק הממשי והמדומה של מספר מרוכב באותיות לטיניות קטנות עוקבות (כגון a,b) או אותיות יווניות קטנות עוקבות (כגון α,β).

5 יש שאומרים "מדומה טהור".

את זוג המספרים הממשיים $(\mathrm{Re}\,z, \mathrm{Im}\,z)$ המתאים למספר המרוכב z נוכל לראות (כפי שלמדתם בפרק 2) כנקודה במישור. החלק הממשי $\mathrm{Re}\,z$, מציין את שיעור ה־x של הנקודה, ואילו החלק המדומה $\mathrm{Im}\,z$, מציין את שיעור ה־y של הנקודה. מעתה, לעיתים קרובות נתייחס למספר מרוכב z כאל נקודה במישור, כאשר כוונתו לנקודה הנקבעת על־ידי הזוג הסדור (או, הוקטור) הנתון על־ידי $(\mathrm{Re}\,z, \mathrm{Im}\,z)$. למישור, כאשר רואים את נקודותיו כמספרים מרוכבים, נהוג לקרוא **המישור המרוכב**.



שאלה 6.3.4

הציגו במישור המרוכב את המספרים המרוכבים הבאים:

$$-1-i,\ \ -1+i,\ \ 1-i,\ \ 1+i,\ \ 0,\ \ 3-4i$$

התשובה בעמוד 126

שאלה 6.3.5

מהו הקשר בין הצגתו במישור של המספר המרוכב z והמספר $-z$?

התשובה בעמוד 126

שימו לב שחיבור מספרים מרוכבים מתבצע על־ידי חיבור החלק הממשי בנפרד והחלק המדומה בנפרד, כלומר (מנקודת מבט גיאומטרית) – חיבור רכיב רכיב. כפי שלמדתם בפרק 2, באופן גיאומטרי חיבור זה נעשה על פי כלל המקבילית.

6.4 הצמוד והערך המוחלט

הגדרה 6.4.1

יהי $z=a+ib$ מספר מרוכב. **המספר הצמוד של** z, או בקיצור **הצמוד** של z, שסימנו $\bar{z}$, מוגדר על־ידי:

$$\bar{z}:=a-ib$$

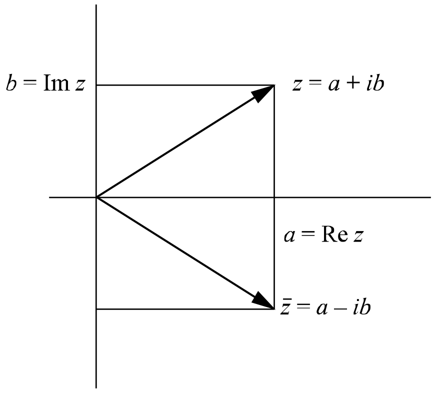
דוגמה

א. אם $z=1+i$, אז $\bar{z}=1-i$

ב. $\overline{3+i5}=3-i5$

ג. $\overline{4-i2}=4+i2$

מבחינה גיאומטרית, הנקודה $\bar{z}$ במישור המרוכב היא הנקודה הסימטרית ל־ z ביחס לציר הממשי (ראו איור).



▸

שאלה 6.4.1

חשבו את $\bar{z}$ עבור:

א. $z=-5+i$

ב. $z=-7i$

ג. $z=-\sqrt{2}$

התשובה בעמוד 126

משפט 6.4.2 תכונות יסודיות של הצמוד

לכל $z, z_1, z_2 \in \mathbb{C}$ מתקיים:

א. $\overline{\overline{z}} = z$ [1]

ב. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$

ג. $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$

ד. $z + \overline{z} = 2\operatorname{Re} z$

ה. $z - \overline{z} = 2i\operatorname{Im} z$

ו. $z = \overline{z}$ אם ורק אם z ממשי.

שאלה 6.4.2

הוכיחו את משפט 6.4.2.

התשובה בעמוד 127

שאלה 6.4.3

יהיו z מספר מרוכב ו־α מספר ממשי.

הוכיחו כי:

$$\overline{\alpha z} = \alpha \overline{z}$$

התשובה בעמוד 127

שאלה 6.4.4

הוכיחו כי:

$$\overline{z_1 - z_2} = \overline{z_1} - \overline{z_2}$$

התשובה בעמוד 127

שאלה 6.4.5

הוכיחו, באינדוקציה על n, כי לכל $z_1, \ldots, z_n \in \mathbb{C}$ מתקיים:

א. $\overline{z_1 + \ldots + z_n} = \overline{z_1} + \ldots + \overline{z_n}$

ב. $\overline{z_1 z_2 \cdots z_n} = \overline{z_1}\,\overline{z_2} \cdots \overline{z_n}$

התשובה בעמוד 127

שאלה 6.4.6

הוכיחו כי לכל n טבעי:

$$\overline{z^n} = (\overline{z})^n$$

התשובה בעמוד 128

1 $\overline{\overline{z}}$ הוא הצמוד של המספר המרוכב $\overline{z}$.

שאלה 6.4.7

א. הראו שאם z הוא שורש של המשוואה הריבועית

$$\alpha x^2 + \beta x + \gamma = 0$$

כאשר α, β ו־γ ממשיים, אז גם $\bar{z}$ הוא שורש של אותה משוואה.

ב. הראו שאם z הוא שורש של המשוואה

$$\alpha_n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_1 x + \alpha_0 = 0$$

כאשר $\alpha_n, \alpha_{n-1}, \ldots, \alpha_0$ ממשיים, אז גם $\bar{z}$ הוא שורש של אותה משוואה.

התשובה בעמוד 128

הגדרה 6.4.3

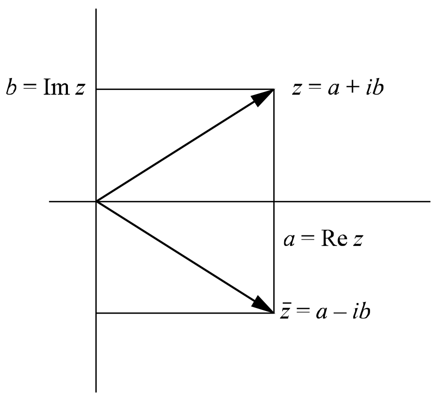
יהי $z = a + ib$ מספר מרוכב.

הערך המוחלט של z, שסימונו $|z|$, הוא המספר הממשי האי־שלילי המוגדר כך:

$$|z| \stackrel{\text{def}}{=} \sqrt{a^2 + b^2}$$

כלומר, $|z| = \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2}$.

מבחינה גיאומטרית, $|z|$ הוא המרחק, במישור המרוכב, של הנקודה z מראשית הצירים, וזאת לפי משפט פיתגורס (התבוננו במשולש ישר הזווית שבאיור).



דוגמאות

$$|3 - 4i| = \sqrt{3^2 + (-4)^2} = \sqrt{25} = 5$$

$$|1 + 2i| = \sqrt{1^2 + 2^2} = \sqrt{5}$$

$$|2i| = |0 + 2i| = \sqrt{0^2 + 2^2} = 2$$

$$|5| = |5 + 0i| = \sqrt{5^2 + 0^2} = 5$$

$$|-3| = |-3 + 0i| = \sqrt{(-3)^2 + 0^2} = 3$$

◀

הערה

ברור (כמו בשתי הדוגמאות האחרונות) כי הערך המוחלט על שדה המספרים המרוכבים הוא הרחבה של הערך המוחלט כפי שהכרנוהו בשדה הממשיים.[2]

שאלה 6.4.8

חשבו:

א. $|7+2i|$

ב. $|1-i|$

ג. $|-i|$

ד. $|0|$

ה. $|-\sqrt{2}|$

התשובה בעמוד 129

שאלה 6.4.9

מהי הצורה הגיאומטרית של קבוצת הנקודות במישור המרוכב המוגדרת על־ידי:

$$\left\{z \,\middle|\, z \in \mathbb{C}, |z| \le 5\right\}$$

התשובה בעמוד 130

במשפט שלהלן נעמוד על הקשר שבין הערך המוחלט לבין הצמוד של מספר מרוכב.

משפט 6.4.4

לכל מספר מרוכב z מתקיים:

א. $|z| = |\overline{z}|$

ב. $z\overline{z} = |z|^2$

הוכחה

א. אם $z = a + ib$, אז $\overline{z} = a - ib$ ולכן:

$$|z| = \sqrt{a^2 + b^2} = \sqrt{a^2 + (-b)^2} = |\overline{z}|$$

ב. $z\overline{z} = (a+ib)(a-ib) = a^2 - abi + bai - b^2i^2 = a^2 + b^2 = |z|^2$

מ.ש.ל.

שאלה 6.4.10

מהי המשמעות הגיאומטרית של חלק א במשפט זה?

התשובה בעמוד 130

---

2 כלומר, הערך המוחלט של מספר מרוכב, שהוא ממשי, הוא הערך המוחלט ה"רגיל" של המספר הממשי, שהרי לכל מספר ממשי α מתקיים $|a| = \sqrt{a^2} = \sqrt{a^2 + 0^2} = |a + i0|$.

שאלה 6.4.11

הוכיחו:

א. $\operatorname{Re} z \leq |\operatorname{Re} z| \leq |z|$

ב. $\operatorname{Im} z \leq |\operatorname{Im} z| \leq |z|$

ג. $|z| \leq |\operatorname{Re} z| + |\operatorname{Im} z|$

התשובה בעמוד 130

משפט 6.4.5 תכונות יסודיות של הערך המוחלט

יהיו z, z_1, z_2 מספרים מרוכבים. אזי:

א. $|z| \geq 0$

וכן, $|z| = 0$ אם ורק אם $z = 0$.

ב. $|z_1 z_2| = |z_1||z_2|$

ג. $|z_1 + z_2| \leq |z_1| + |z_2|$ [3]

ד. $|-z| = |z|$

הוכחה

את הוכחת החלקים א ו־ד נשאיר לקוראים, המתבקשים לשים לב גם למשמעות הגיאומטרית של הטענות שבחלקים אלה.[4]

ב. עתה נוכיח כי $|z_1 z_2| = |z_1||z_2|$, וזאת מתוך הסתמכות על כך שלכל z:

$$z\bar{z} = |z|^2$$ [5]

ואמנם:

$$|z_1 z_2|^2 = (z_1 z_2)(\overline{z_1 z_2}) = (z_1 z_2)(\bar{z}_1 \bar{z}_2)$$

$$= (z_1 \bar{z}_1)(z_2 \bar{z}_2) = |z_1|^2 |z_2|^2 = (|z_1||z_2|)^2$$

הווי אומר:

$$|z_1 z_2|^2 = (|z_1||z_2|)^2$$

מאחר שעל פי הגדרת הערך המוחלט, $|z_1 z_2| \geq 0$ וכן $|z_1| \geq 0$ ו־ $|z_2| \geq 0$, נוכל להסיק מן השוויון שלעיל כי:

$$|z_1 z_2| = |z_1||z_2|$$

ג. [6] $$|z_1 + z_2|^2 = (z_1 + z_2)(\overline{z_1 + z_2})$$

[7] $$= (z_1 + z_2)(\bar{z}_1 + \bar{z}_2)$$

---

3 אי־שוויון זה מכונה אי־שוויון המשולש.

4 ראו בשאלה העוקבת.

5 זהו תוכנו של חלק ב במשפט 6.4.4.

6 משפט 6.4.4, חלק ב.

$$= z_1\overline{z}_1 + z_1\overline{z}_2 + z_2\overline{z}_1 + z_2\overline{z}_2$$

$$\overset{8}{=} |z_1|^2 + \left(z_1\overline{z}_2 + \overline{z_1\overline{z}_2}\right) + |z_2|^2$$

$$\overset{9}{=} |z_1|^2 + 2\operatorname{Re}(z_1\overline{z}_2) + |z_2|^2$$

$$\overset{10}{\le} |z_1|^2 + 2|z_1\overline{z}_2| + |z_2|^2$$

$$\overset{11}{=} |z_1|^2 + 2|z_1||\overline{z}_2| + |z_2|^2$$

$$\overset{12}{=} |z_1|^2 + 2|z_1||z_2| + |z_2|^2 = \left(|z_1| + |z_2|\right)^2$$

משני קצות השרשרת אנו מקבלים:

$$|z_1 + z_2|^2 \le \left(|z_1| + |z_2|\right)^2$$

מאחר שערכים מוחלטים הם אי־שליליים, נוכל להסיק מכך כי:

$$|z_1 + z_2| \le |z_1| + |z_2|$$

מ.ש.ל.

שאלה 6.4.12

הוכיחו את חלקים א ו־ד שבמשפט 6.4.5.

התשובה בעמוד 131

את החלקים ב ו־ג של המשפט הקודם קל להכליל באינדוקציה:

שאלה 6.4.13

יהיו $z, z_1, \ldots, z_n \in \mathbb{C}$. הוכיחו כי:

א. $|z_1 + \ldots + z_n| \le |z_1| + \ldots + |z_n|$

ב. $|z_1 z_2 \ldots z_n| \le |z_1||z_2|\ldots|z_n|$

ג. הסיקו מן הסעיף הקודם כי:

$$|z|^n = |z|^n$$

התשובה בעמוד 132

תוך שימוש בצמוד ובערך המוחלט נוכל להציג את ההופכי של מספר מרוכב $z \ne 0$ כך:

7 משפט 6.4.2, חלק ב.
8 משפט 6.4.4, חלק ב, ומשפט 6.4.2 חלקים א, ג.
9 משפט 6.4.2, חלק ד.
10 שאלה 6.4.11, חלק א.
11 חלק ב של משפט זה.
12 משפט 6.4.4, חלק א.

טענה 6.4.6

לכל מספר מרוכב $z \neq 0$, מתקיים:

$$z^{-1} = \frac{\overline{z}}{|z|^2}$$

הוכחה

כפי שראינו:

$$z\overline{z} = |z|^2$$

עבור $z \neq 0$ מתקיים $|z| \neq 0$, ולכן נוכל לחלק את שני אגפי השוויון ב- $|z|^2$ ולקבל:

$$\frac{z\overline{z}}{|z|^2} = 1$$

כלומר

$$z \cdot \frac{\overline{z}}{|z|^2} = 1$$

ולכן:

$$z^{-1} = \frac{\overline{z}}{z^2}$$

מ.ש.ל.

דוגמאות

א. נחשב את z^{-1} עבור $z = 1 + i$.

$$z^{-1} = (1+i)^{-1} = \frac{\overline{(1+i)}}{|1+i|^2} = \frac{1-i}{2} = \frac{1}{2} - \frac{1}{2}i$$

ואמנם:

$$\underbrace{(1+\mathrm{i})}_{z}\underbrace{\left(\frac{1}{2} - \frac{1}{2}i\right)}_{z^{-1}} = 1$$

ב. נחשב את z^{-1} עבור $z = 3 + 4i$.

$$z^{-1} = (3+4i)^{-1} = \frac{\overline{3+4i}}{|3+4i|^2} = \frac{3-4i}{25} = \frac{3}{25} - \frac{4}{25}i$$

כדי להשתכנע שלא טעינו בחשבון בדקו כי מתקיים:

$$\underbrace{(3+4\mathrm{i})}_{z}\underbrace{\left(\frac{3}{25} - \frac{4}{25}i\right)}_{z^{-1}} = 1$$

שאלה 6.4.14

חשבו את z^{-1} עבור:

א. $z = i$

ב. $z = 5$

ג. $z = 3 - 4i$

התשובה בעמוד 132

מן השוויון שבמשפט 6.4.6 נוכל לגזור בנקל נוסחה פשוטה לחילוק, שתאפשר לנו להציג מנה של מספרים מרוכבים בצורה $a + bi$.

עבור z_1 מרוכב כלשהו ו־ $z_2 \neq 0$:

$$\frac{z_1}{z_2} \underset{\substack{\uparrow \\ \text{לפי הגדרת} \\ \text{החילוק}}}{=} z_1 \cdot z_2^{-1} \underset{\substack{\uparrow \\ \text{לפי משפט} \\ 6.4.6}}{=} z_1 \cdot \frac{\bar{z}_2}{|z_2|^2} = \frac{z_1 \cdot \bar{z}_2}{|z_2|^2} \qquad (*)$$

דוגמה

נחשב, למשל, את המנה $\frac{1+i}{2+i}$:

לפי (*)

$$\frac{1+i}{2+i} = \frac{(1+i)(\overline{2+i})}{|2+i|^2} = \frac{(1+i)(2-i)}{5} = \frac{3}{5} + \frac{1}{5}i$$

▶

הערה

אם בשוויון (*) נציב $z_2\bar{z}_2$ במקום $|z_2|^2$, נקבל:

$$\frac{z_1}{z_2} = \frac{z_1\bar{z}_2}{z_2\bar{z}_2}$$

אי לכך, כדי להציג את המנה $\frac{z_1}{z_2}$ $(z_2 \neq 0)$ בצורה $a + bi$, כל שעלינו לעשות הוא **לכפול את המונה ואת המכנה בצמוד של המכנה**.

דוגמה

לחישוב $\frac{1+i}{1+2i}$ נכפול את המונה ואת המכנה ב־ $1 - 2i$ (שהוא הצמוד של $1 + 2i$) ונקבל:

$$\frac{1+i}{1+2i} = \frac{(1+i)(1-2i)}{(1+2i)(1-2i)} = \frac{3-i}{5}$$

▶

שאלה 6.4.15

חשבון:

א. $\frac{-1+3i}{7+i}$

ב. $\frac{2-3i}{1+4i}$

ג. $\frac{1+i}{\sqrt{2}+i}$

ד. $\frac{5}{1+2i}$

ה. $\frac{1}{i}$

התשובה בעמוד 132

שאלה 6.4.16

הוכיחו כי עבור $z \neq 0$ ו־ w מספר מרוכב כלשהו:

א. $\overline{z^{-1}} = (\overline{z})^{-1}$

ב. $\overline{\left(\frac{w}{z}\right)} = \frac{\overline{w}}{\overline{z}}$

התשובה בעמוד 133

שאלה 6.4.17

הוכיחו כי עבור $z \neq 0$ ו־ w מרוכב כלשהו:

א. $\left|z^{-1}\right| = |z|^{-1}$

ב. $\left|\frac{w}{z}\right| = \frac{|w|}{|z|}$

התשובה בעמוד 133

עתה, משלמדנו כיצד לבצע את פעולות ה"חשבון" הבסיסיות בשדה המספרים המרוכבים, נוכל לפתור בעיות באלגברה לינארית מעל שדה זה, כפי שעשינו בפרקים הקודמים.

שאלה 6.4.18

פתרו את מערכת המשוואות הבאה מעל שדה המספרים המרוכבים:

$$\begin{aligned}
3x - \quad & iy + \quad & 5z &= 7-i2 \\
-x + \quad & (1+i)y + \quad & 2z &= -i \\
(1-i)x - \quad & y + \quad & (1+i)z &= 3-i
\end{aligned}$$

התשובה בעמוד 134

שאלה 6.4.19

חשבו את הדטרמיננטה של המטריצה:

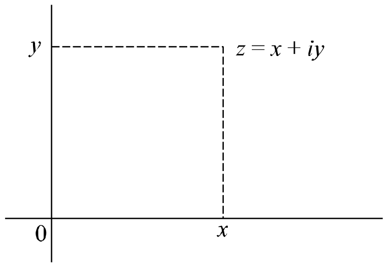
$$\begin{bmatrix} 2-i & 3 & i \\ 2i & 1+2i & -1 \\ 1-2i & -i & 1+i \end{bmatrix}$$

האם מטריצה זו הפיכה?

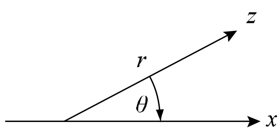
התשובה בעמוד 134

6.5 ההצגה הקוטבית של מספר מרוכב

כפי שלמדנו בסעיף 6.3, אנו רואים את המספרים המרוכבים, באופן גיאומטרי, כנקודות במישור. המספר המרוכב $z = x + iy$ מתואר במישור על־ידי הנקודה ששיעוריה (x, y). זוג המספרים (x, y) נקרא **השיעורים הקרטזיים**[1] **של הנקודה** z **במישור המרוכב** (ראו איור).



ניתן לאפיין את הנקודות במישור גם באמצעות **קואורדינאטות קוטביות**[2] כך: כל נקודה z במישור המרוכב מאופיינת על־ידי מרחקה r מראשית הצירים, והזווית θ שיוצר הישר שעליו מונח הוקטור היוצא מהראשית אל z עם הכיוון החיובי של ציר ה־ x (ראו איור).[3]



זוג סדור, (r, θ), המאפיין את הנקודה z בדרך זו, מכונה **שיעורים קוטביים של הנקודה** z. הזווית θ מכונה ה**ארגומנט** של z.

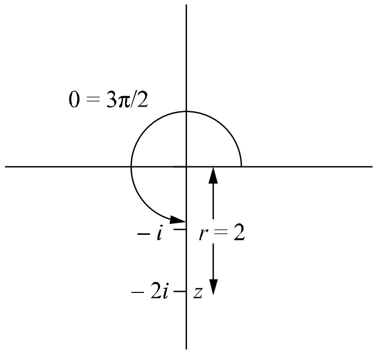
דוגמה

$$(r, \theta) = (2, 3\pi/2)$$

זוהי הנקודה שמרחקה מהראשית הוא 2, והזווית שהיא יוצרת עם הקרן החיובית של ציר ה־ x היא בת $3\pi/2$ רדיאנים.

מתוך האיור דלהלן אתם למדים כי שיעוריה הקרטזיים של נקודה זו הם $(0, -2)$, כלומר זוהיהנקודה $z = -2i$.

1 לפעמים נאמר "הקואורדינטות הקרטזיות" במקום "השיעורים הקרטזיים".
2 בלעז: קואורדינטות פולאריות.
3 עבור הנקודה $z = (0,0)$ לא מוגדרת הזווית θ. נקודה זו מאופיינת בכך שמרחקה מן הראשית הוא אפס.



שאלה 6.5.1

מה הם המספרים המרוכבים ששיעוריהם הקוטביים הם:

א. $\theta = 0 \quad r = 3$

ב. $\theta = \frac{9}{4}\pi \quad r = \sqrt{2}$

ג. $r = 2 \quad \theta = -\frac{\pi}{2}$

ד. $(r,\theta) = (5,\pi)$

ה. $(r,\theta) = (5,3\pi)$

ו. $(r,\theta) = \left(-5,\frac{\pi}{2}\right)$

תשובה בעמוד 134

בוודאי הבחנתם בשאלה האחרונה ובדוגמאות שקדמו לה, שניתן לתאר נקודה אחת במישור באמצעות שיעורים קוטביים שונים.

דוגמאות

$$(r,\theta) = (\sqrt{2},\pi/4)$$

וגם

$$(r,\theta) = (\sqrt{2},9\pi/4)$$

שניהם שיעורים קוטביים המתארים את הנקודה:

$$z = 1 + i$$

כמו כן,

$$(r,\theta) = \left(2,\frac{3}{2}\pi\right)$$

וגם

$$(r,\theta) = \left(2,-\frac{\pi}{2}\right)$$

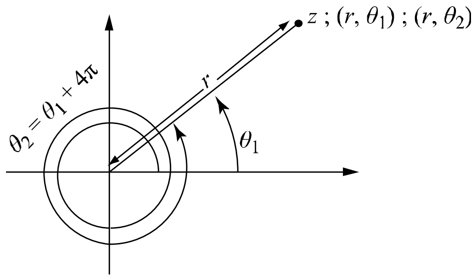
מתארים שניהם את הנקודה:

$$z = -2i$$

באופן כללי, אם

$$\theta_2 = \theta_1 + 2k\pi$$

כאשר k הוא מספר שלם (חיובי, שלילי או אפס), אז (r,θ_1) ו־ (r,θ_2) מייצגות אותה נקודה z במישור (ראו איור).



אפשר לנסח את האמור בפסקה האחרונה בקצרה כך:

הארגומנט של מספר מרוכב שונה מאפס נקבע עד כדי תוספת כפולה שלמה של 2π.

עד כאן טיפלנו בשאלה כיצד למצוא את שיעוריה הקרטזיים של נקודה z אשר שיעוריה הקוטביים הם (r,θ). נעבור כעת לשאלה ההפוכה: כיצד למצוא את שיעוריה הקוטביים של נקודה z שונה מאפס אשר שיעוריה הקרטזיים הם (x,y). ראשית, השיעור הקוטבי r הוא המרחק של z מן הראשית, וזה אינו אלא הערך המוחלט $|z|$.

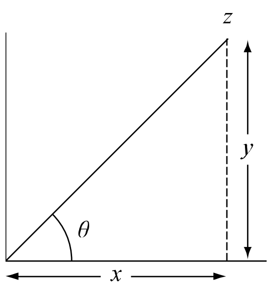
לכן:

$$r = \sqrt{x^2 + y^2}$$

אשר ל־ θ - אם $x \neq 0$ אז מן האיור הבא אנו למדים כי

$$\tan\theta = \frac{y}{x}$$

ואם $x = 0$ אז z הוא מספר מדומה ונמצא אפוא על הציר המדומה. לכן $\theta = \frac{\pi}{2}$ או $\theta = \frac{3}{2}$.



דוגמה א

נמצא את שיעוריה הקוטביים של הנקודה:

$$z = -1 - i$$

א. $r = |z| = \sqrt{(-1)^2 + (-1)^2} = \sqrt{2}$

ב. $\tan\theta = \frac{-1}{-1} = 1$

השוויון שב־ב מתקיים, למשל, עבור $\theta = \frac{\pi}{4}$ וכן עבור $\theta = \frac{\pi}{4} + \pi n$ לכל n שלם - זאת משום ש־ $\tan$ היא פונקציה מחזורית בעלת מחזור π. נבחין כי קיים הבדל בין המקרה שבו n זוגי והמקרה שבו n אי־זוגי. עבור n זוגי, הנקודה במישור המתאימה לזוג $\theta = \frac{\pi}{4} + \pi n,\ r = \sqrt{2}$ נמצאת ברביע הראשון ולכן היא אינה מתאימה לנקודה $z = -1 - i$. לעומת זאת, עבור n אי־זוגי הנקודה נמצאת ברביע השלישי וזוהי אכן הנקודה $z = -1 - i$.

שימו לב, מהאמור לעיל אנו למדים שערכו של $\tan\theta$ אינו מַספיק כדי לקבוע את הארגומנט.

דרך נוחה לתיאור אוסף כל הזוויות מהצורה $\theta = \frac{\pi}{4} + \pi n$, כאשר n שלם אי־זוגי, היא $\theta = \frac{\pi}{4} + \pi(2k+1)$, כאשר k שלם כלשהו.

אולם,

$$\frac{\pi}{4} + \pi(2k+1) = \frac{5\pi}{4} + 2\pi k$$

ולכן שיעוריה הקוטביים של הנקודה $z = -1 - i$ (ששיעוריה הקרטזיים הם $(-1,-1)$), הם

$$(r,\theta) = \left(\sqrt{2}, \frac{5\pi}{4} + 2\pi k\right)$$

כאשר k שלם כלשהו. ◀

דוגמה ב

נמצא את שיעוריה הקוטביים של:

$$z = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

א. $r = \sqrt{\left(-\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2} = 1$

ב. $\tan\theta = -\sqrt{3}$

נציע הפעם גישה מעט שונה מזו שנקטנו בדוגמה א (אך שקולה לה), להתבוננות בארגמונט. השוויון שב־ב מתקיים עבור הארגומנט

$$\theta = \frac{2\pi}{3}$$

וכן עבור:

$$\theta = \frac{5\pi}{3}$$

אלה כל הזוויות בין 0 ל־ 2π שעבורן מתקיים השוויון. על פי סימני הקואורדינטות הקרטזיות, $(x < 0,\ y > 0)$, z נמצאת ברביע השני, ולכן הקואורדינאטות הקוטביות של z הן $\left(1, \frac{2\pi}{3}\right)$. תוספת של כפולה שלמה של 2π לארגומנט אינו משנה את הנקודה המתאימה, ולכן כל הקואורדינטות המתאימות לתיאור הנקודה הן

$$\left(1, \frac{2}{3}\pi + 2\pi k\right)$$

כאשר k שלם כלשהו. ◄

שאלה 6.5.2

חשבו את השיעורים הקוטביים של המספרים המרוכבים הבאים:

א. $-1 + i$

ב. $\frac{1}{2} - \frac{\sqrt{3}}{2}i$

ג. i^3

ד. $(1 + i)^3$

תשובה בעמוד 136

תהי $z \neq 0$ נקודה במישור המרוכב ששיעוריה הקוטביים הם (r, θ), ושיעוריה הקרטזיים הם (x, y).

נקל לוודא כי

$$\frac{x}{r} = \cos\theta$$

וכי:

$$\frac{y}{r} = \sin\theta$$

ולאחר כפל המשוואות ב־ r:

$$x = r\cos\theta$$

$$y = r\sin\theta$$

הווי אומר, השיעורים הקרטזיים של z הם:

$$(x, y) = (r\sin\theta,\ r\sin\theta)$$

ולכן:

$$z = x + iy = r\cos\theta + ir\sin\theta$$

או:

$$z = r(\cos\theta + i\sin\theta)$$

תיאור זה של המספר המרוכב z נקרא **הצגה טריגונומטרית של** z.[4]

4 כאשר $z = 0$, ניתן להציגו בצורה טריגונומטרית על־ידי $0 = 0(\cos\theta + i\sin\theta)$, כאשר θ היא זווית כלשהי.

ל־ z יש הצגות טריגונומטריות רבות, שכן, כאמור לעיל, הארגומנט של z נקבע עד כדי תוספת של כפולה שלמה של 2π.

שאלה 6.5.3

z_1, z_2 ו־ z_3 נתונים על־ידי:

$$z_1 = 5\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{6}\right)$$

$$z_2 = -2\left(\cos\frac{\pi}{5} + i\sin\frac{\pi}{5}\right)$$

$$z_3 = 7\left(\cos\frac{\pi}{7} - i\sin\frac{\pi}{7}\right)$$

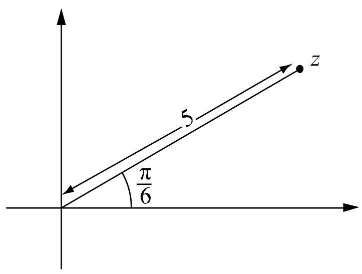
ציינו מדוע כל אחת מן ההצגות של המספרים z_1, z_2 ו־ z_3 אינה הצגה טריגונומטרית (בהתאם להגדרה שנתנו לעיל), ומצאו הצגות טריגונומטריות של z_1, z_2 ו־ z_3.

תשובה בעמוד 138

דוגמה

נמצא את ההצגה $x+iy$ התאימה ל־ z:

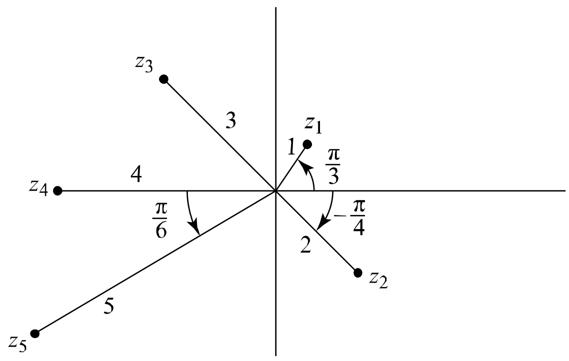
$$z = r(\cos\theta + i\sin\theta) = 5\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right) = 5\left(\frac{\sqrt{3}}{2} + i\frac{1}{2}\right) = \frac{5\sqrt{3}}{2} + \frac{5}{2}i$$



▸

שאלה 6.5.4

הציגו בצורה $x + iy$ את חמש הנקודות המוצגות באיור שלפניכם.

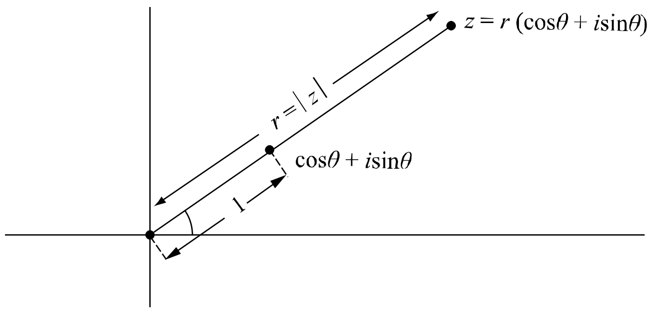


תשובה בעמוד 140

בהצגתו הטריגונומטרית, נתון מספר מרוכב $z \neq 0$ כמכפלה של מספר ממשי חיובי r (הלא הוא ערכו המוחלט של z) במספר מרוכב $(\cos\theta + i\sin\theta)$. ערכו המוחלט של הגורם האחרון הוא:

$$|\cos\theta + i\sin\theta| = \sqrt{\cos^2\theta + \sin^2\theta} = 1$$

היחס הגיאומטרי בין $(\cos\theta + i\sin\theta)$ לבין z מומחש באיור שלפניכם:



ננסה עתה למצוא את ההצגה הטריגונומטרית של מכפלת שני מספרים מרוכבים z_1, z_2, בעזרת ההצגות הטריגונומטריות של z_1 ושל z_2.

נניח:

$$z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$$

$$z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$$

חישוב מכפלתם של z_1 ו־ z_2 ייתן:

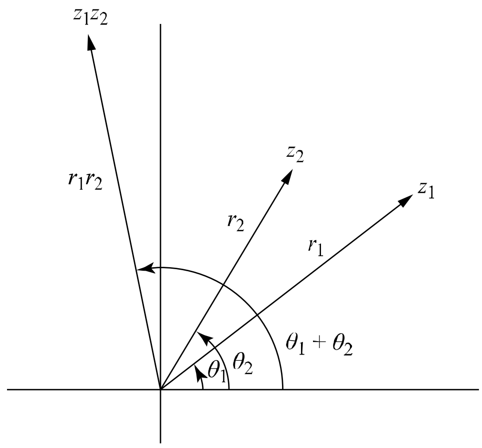
$$z_1z_2 = r_1(\cos\theta_1 + i\sin\theta_1)\cdot r_2(\cos\theta_2 + i\sin\theta_2)$$

$$= z_1z_2\left[(\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i(\cos\theta_1\sin\theta_2 + \sin\theta_1\cos\theta_2)\right]$$

בעזרת הזהויות הטריגונומטריות הידועות עבור sin ו־ cos של סכום זוויות נקבל את **כלל המכפלה**:

$$z_1z_2 = r_1r_2\left(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)\right)$$

אגף ימין מהווה, כמובן, הצגה טריגונומטרית של z_1z_2, שבה **ערכו המוחלט** של z_1z_2 הוא r_1r_2, דהיינו מכפלת הערכים המוחלטים של z_1 ו־ z_2, ואילו ה**ארגומנט** של z_1z_2 הוא $\theta_1+\theta_2$, כלומר סכום הארגומנטים של z_1 ו־ z_2.



שאלה 6.5.5

א. מצאו את ההצגה הטריגונומטרית של $\bar{z}$ מתוך ההצגה הטריגונומטרית של z.

ב. מצאו את ההצגה הטריגונומטרית של z^{-1} מתוך ההצגה הטריגונומטרית של z, כאשר $z \neq 0$.

ג. יהיו:

$$z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$$

$$0 \neq z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$$

מצאו את ההצגה הטריגונומטרית של המספר $\frac{z_1}{z_2}$.

תשובה בעמוד 141

בעזרת כלל המכפלה נוכל לחשב בנקל חזקות שלמות של מספרים מרוכבים. למשל, אם

$$z = r(\cos\theta + i\sin\theta)$$

אז:

$$z^2 = r\cdot r\big(\cos(\theta+\theta) + i\sin(\theta+\theta)\big) = r^2(\cos 2\theta + i\sin 2\theta) \tag{1}$$

נחשב עתה את z^3:

$$z^3 = z^2\cdot z = r^2(\cos 2\theta + i\sin 2\theta)\cdot r(\cos\theta + i\sin\theta)$$

$$= r^3\big(\cos(2\theta+\theta) + i\sin(2\theta+\theta)\big)$$

$$= r^3(\cos 3\theta + i\sin 3\theta)$$

לא יקשה עליכם להכליל את שתי הדוגמאות הקודמות ולהוכיח באינדוקציה כי לכל n טבעי:

$$z^n = r^n(\cos n\theta + i\sin n\theta)$$

אבל ברור שמתקיים גם:

$$z^n = r^n(\cos\theta + i\sin\theta)^n$$

ומכאן:

$$(\cos\theta + i\sin\theta)^n = (\cos n\theta + i\sin n\theta)$$

נוסחה זו נקראת **נוסחת דה־מואבר** (De Moivre).

נוסחת דה מואבר עשויה לסייע לנו להציג את הפונקציות הטריגונומטריות $\cos n\theta$ ו־ $\sin n\theta$ בעזרת $\sin\theta$ ו־ $\cos\theta$.

שאלה 6.5.6

השתמש בנוסחת דה־מואבר עבור $n = 3$ כדי להציג את $\sin 3\theta$ ו־ $\cos 3\theta$ בעזרת $\sin\theta$ ו־ $\cos\theta$.

תשובה בעמוד 142

6.6 שורשים של מספר מרוכב

נראה עתה שימוש בהצגה הטריגונומטרית לשם מציאת פתרונותיה של המשוואה

$$x^n - 1 = 0 \tag{1}$$

מעל המרוכבים.

מעל הממשיים יש למשוואה זו שני פתרונות לכל היותר: 1 הוא פתרון, וכאשר n זוגי, גם -1 הוא פתרון. אולם מעל המרוכבים, למשוואה (1) יש n **פתרונות בדיוק**! פתרונות אלה מכונים **שורשי היחידה מסדר** n. נמצא את ההצגה הטריגונומטרית של n השורשים הללו.

אם z הוא שורש של המשוואה (1), אז $z^n = 1$ ולכן:

$$\left|z^n\right| = 1$$

ומכאן כי

$$|z|^n = 1$$

ולכן:[1]

$$|z| = 1$$

הצגתו הטריגונומטרית של z תהיה אפוא:

$$z = 1(\cos\theta + i\sin\theta) = \cos\theta + i\sin\theta$$

על פי נוסחת דה־מואבר נקבל:

$$z^n = \cos n\theta + i\sin n\theta$$

ולכן

$$\cos n\theta + i\sin n\theta = 1 = \cos 0 + i\sin 0 = \cos(n0) + i\sin(n0)$$

ומצאנו, אם כן, פתרון ראשון למשוואה (1), שנסמנו z_0:[2]

$$z_0 = \cos 0 + i\sin 0 = 1$$

ומניין יימצאו יתר הפתרונות?

נשים לב שלמספר 1 יש הצגות טריגונומטריות נוספות. למשל:

$$1 = \cos 2\pi + i\sin 2\pi$$

לכן, עבור ארגומנט θ_1 שיקיים

$$n\theta_1 = 2\pi$$

או

$$\theta_1 = \frac{2\pi}{n}$$

יתקיים:

$$\cos n\theta_1 + i\sin n\theta_1 = \cos 2\pi + i\sin 2\pi = 1$$

כלומר, גם

$$z_1 = \cos\theta_1 + i\sin\theta_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

הינו פתרון למשוואה (1).

1 זכרו כי $|z|$ הינו מספר ממשי חיובי. לכן $|z|^n = 1$ אם ורק אם $|z| = 1$.

2 ואכן: $z_0^n = 1$.

ההמשך ברור מאליו.

כל הצגותיו הטריגונומטריות של 1 הן

$$\cos 2\pi k + i\sin 2\pi k = 1$$

כאשר k הוא מספר שלם כלשהו.

לכן, קבוצת כל הארגומנטים θ שעבורם מתקיים

$$\cos n\theta + i\sin n\theta = 1$$

כוללת את כל הארגומנטים θ המקיימים

$$n\theta = 2\pi k$$

או

$$\theta = \frac{2\pi k}{n}$$

עבור k שלם כלשהו.

מצאנו, אם כך, שקבוצת הפתרונות של המשוואה $x^n - 1 = 0$ היא הקבוצה:

$$\left\{ z \,\middle|\, z = \cos\frac{2\pi k}{n} + i\sin\theta\frac{2\pi}{n},\ \text{שלם כלשהו } k \right\}$$

נרשום את n הפתרונות המתאימים לערכים $k = 0,\ldots,n-1$:

$$\begin{cases} z_0 = \cos\frac{2\pi\cdot 0}{n} + i\sin\theta\frac{2\pi\cdot 0}{n} = 1 \\ z_1 = \cos\frac{2\pi\cdot 1}{n} + i\sin\theta\frac{2\pi\cdot 1}{n} \\ z_2 = \cos\frac{2\pi\cdot 2}{n} + i\sin\theta\frac{2\pi\cdot 2}{n} \\ \vdots \\ z_k = \cos\frac{2\pi\cdot k}{n} + i\sin\theta\frac{2\pi\cdot k}{n} \\ \vdots \\ z_{n-1} = \cos\frac{2\pi\cdot(n-1)}{n} + i\sin\theta\frac{2\pi\cdot(n-1)}{n} \end{cases} \tag{2}$$

קל לבדוק שהמספרים $z_0,\ldots,z_{n-1}$ שונים זה מזה.

שאלה 6.6.1

הוכיחו את הטענה האחרונה.

התשובה בעמוד 142

אם נמשיך ונציב $k = n, n+1,\ldots$ לא נקבל מספרים חדשים. כך, למשל:

$$z_n = \cos\frac{2\pi\cdot n}{n} + i\sin\frac{2\pi\cdot n}{n} = \cos 2\pi + i\sin 2\pi = z_0$$

$$z_{n+1} = \cos\frac{2\pi\cdot(n+1)}{n} + i\sin\frac{2\pi\cdot(n+1)}{n}$$

$$= \cos\left(\frac{2\pi}{n} + 2\pi\right) + i\sin\left(\frac{2\pi}{n} + 2\pi\right)$$

$$= \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} = z_1$$

שאלה 6.6.2

הוכיחו שלכל k שלם, המספר

$$\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$$

שווה לאחד המספרים $z_0,\ldots,z_{n-1}$ דלעיל.

התשובה בעמוד 143

הוכחנו אפוא כי למשוואה

$$x^n - 1 = 0$$

יש בדיוק n פתרונות שונים במרוכבים, והם אלה הרשומים בנוסחה (2).

נבחן כמה מקרים פרטיים:

א. עבור $n = 2$, המשוואה (1) היא

$$x^2 - 1 = 0$$

ופתרונותיה הם:

$$z_0 = \cos\theta + i\sin\theta = 1$$

$$z_1 = \cos\frac{2\pi \cdot 1}{2} + i\sin\frac{2\pi \cdot 1}{2} = -1$$

ב. עבור $n = 3$, המשוואה (1) היא

$$x^3 - 1 = 0$$

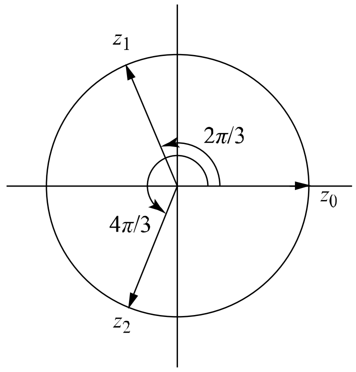
ופתרונותיה הם:

$$z_0 = 1$$

$$z_1 = \cos\frac{2\pi \cdot 1}{3} + i\sin\frac{2\pi \cdot 1}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

$$z_2 = \cos\frac{2\pi \cdot 2}{3} + i\sin\frac{2\pi \cdot 2}{3} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$$

ראו איור.



שאלה 6.6.3

תארו באיור את ארבעת הפתרונות של המשוואה $x^4 - 1 = 0$ ואת חמשת הפתרונות של המשוואה $x^5 - 1 = 0$.

התשובה בעמוד 143

נתבונן עתה במשוואה כללית יותר,

$$x^n - w = 0 \tag{3}$$

כאשר w הוא מספר מרוכב נתון, שונה מאפס.

תהי

$$w = \rho(\cos\alpha + i\sin\alpha)$$

הצגה טריגונומטרית של המספר w, ויהי

$$z = r(\cos\theta + i\sin\theta)$$

פתרון של המשוואה (3).

מנוסחת דה־מואבר נקבל כי

$$z^n = r^n(\cos n\theta + i\sin n\theta)$$

ולכן:

$$r^n(\cos n\theta + i\sin n\theta) = \rho(\cos\alpha + i\sin\alpha)$$

שוויון זה הינו שוויון בין שני מספרים מרוכבים הרשומים בצורה טריגונומטרית. מכאן מתחייב שהערכים המוחלטים שלהם שווים, והארגומנטים נבדלים ב־ $2\pi k$ (k מספר שלם). כלומר:

$$r^n = \rho \quad , \qquad n\theta = \alpha + 2\pi k$$

או:

$$r = \sqrt[n]{\rho} \quad , \quad \theta = \frac{\alpha + 2\pi k}{n}$$

כלומר, פתרונותיה של משוואה (3) הם מן הצורה

$$\sqrt[n]{\rho}\left(\cos\frac{\alpha + 2\pi k}{n} + i\sin\frac{\alpha + 2\pi k}{n}\right) \tag{4}$$

כאשר k מספר שלם כלשהו.

אם נציב ב־(4) $k=0,1,\ldots,n-1$, נקבל n מספרים:

$$\begin{cases} z_0 = \sqrt[n]{\rho}\left(\cos\dfrac{\alpha}{n} + i\sin\dfrac{\alpha}{n}\right) \\ z_1 = \sqrt[n]{\rho}\left(\cos\dfrac{\alpha+2\pi}{n} + i\sin\dfrac{\alpha+2\pi}{n}\right) \\ \vdots \\ z_{n-1} = \sqrt[n]{\rho}\left(\cos\dfrac{\alpha+2\pi(n-1)}{n} + i\sin\dfrac{\alpha+2\pi(n-1)}{n}\right) \end{cases} \tag{5}$$

קל לבדוק (כמו שעשיתם עבור שורשי היחידה) ש־ n המספרים הללו שונים זה מזה וכי אין מקבלים מספרים נוספים אם מציבים בנוסחה (4) מספר שלם k כלשהו.

כלומר, n המספרים הרשומים ב־(5) הם **כל הפתרונות** של המשוואה (3), או בלשון אחר - **אלה הם n השורשים ה־ n-ים של המספר הנתון** w.

שאלה 6.6.4

מצאו את כל הפתרונות של:

א. $x^3 = 8$

ב. $x^2 = i$

ג. $x^4 = -1$

התשובה בעמוד 144

6.7 פולינומים

בסעיף הקודם דנו בשורשים של מספר מרוכב, וראינו שלכל מספר מרוכב w שונה מאפס, יש למשוואה $x^n = w$ בדיוק n שורשים. כעת ברצוננו להרחיב את הדיון לשורשים של **פולינומים** כלליים. בסעיף זה נגדיר מהו פולינום, נדון בפעולות בסיסיות על פולינומים, ונגדיר מהו שורש של פולינום. בהמשך הפרק נמקד את הדיון בשורשים של פולינומים מעל שדה המספרים המרוכבים.

הגדרה 6.7.1 פולינום

יהי F שדה. פולינום מעל F במשתנה x [1] (או בקצרה, **פולינום**) הוא **ביטוי** מהצורה

$$P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$$

כאשר n הוא מספר שלם אי־שלילי, ו־ $a_0,\ldots,a_n$ הם סקלרים בשדה F. לסקלרים $a_0,\ldots,a_n$ קוראים **המקדמים** של הפולינום.

דוגמאות

- $1 + 19x + 3x^2$ הוא פולינום מעל $\mathbb{R}$.
- $1 + 23x + \sqrt{2}x^2 + 0x^2 + (-\pi)x^3 + 0x^4$ גם הוא פולינום מעל $\mathbb{R}$.
- $1 + 1x + 1x^2 + 0x^2 + 1x^3 + 0x^4 + 1x^5$ גם הוא פולינום מעל $\mathbb{R}$; את אותו הביטוי נוכל לראות גם כפולינום מעל השדה $\mathbb{Z}_2$, אם נפרש את המקדמים כאיברים של שדה זה.

$0 + ix + 3x^2 + (1 - 3i)x^4$ הוא פולינום מעל $\mathbb{C}$. ◀

הערה

פולינום **אינו** פונקציה, אלא **ביטוי** – רצף סמלים מהצורה המופיעה בהגדרה 6.7.1.[2] למרות זאת, מבחינות רבות, פולינומים דומים בתכונותיהם לפונקציות (מהצורה דלעיל), כפי שנראה בהמשך.

הגדרה 6.7.2 שוויון פולינומים

יהיו $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, $Q(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$ פולינומים מעל שדה F, ונניח ש־ $m \geq n$. נאמר שהפולינומים $P(x)$ ו־ $Q(x)$ **שווים**, ונסמן $P(x) = Q(x)$, אם מתקיים $a_i = b_i$ לכל $0 \leq i \leq n$, ו־ $b_i = 0$ לכל $n < i \leq m$.

אחרת נאמר שהפולינומים **שונים**.[3] כלומר, שני פולינומים הם שווים אם כל המקדמים שלהם שווים (לפי הסדר), לאחר שהשמטנו אפסים "מיותרים".

---

1 הבחירה בסמל x היא שרירותית, וניתן היה לבחור סמל אחר. אפשרויות נפוצות אחרות הן t,z,u,X.

2 על מהות ההבדל בין פולינומים ופונקציות מהצורה הנידונה נרחיב בהמשך הקורס, אך על הבדל עקרוני נוכל להצביע על רגל אחת כבר עתה – הפולינומים $x, x^2, x^3, \ldots$ הם כולם פולינומים **שונים** (ראו הגדרה 6.7.2), ולכן יש אינסוף פולינומים שונים מעל כל שדה. לעומת זאת, אם F שדה סופי אזי ישנו מספר סופי בלבד של פונקציות מהשדה לעצמו.

3 שימו לב שהנחנו כי $n \geq m$, ותמיד נוכל להניח זאת על־ידי החלפת השמות של m,n במידת הצורך.

למשל, הפולינום $3 + 0x + 2x^2$ שווה לפולינום $3 + 0x + 2x^2 + 0x^3 + 0x^4$, אך שונה מהפולינום $3 + 0x + 2x^2 + 0x^3 + 0x^4 + 7x^5$.

הערות

א. נהוג להשמיט גורמים שמופיע לצידם המקדם 0. לפיכך, את הפולינום $3 + 0x + 2x^2$ ניתן לרשום בקיצור כ־ $3 + 2x^2$, ואת הפולינום $3 + 0x + 2x^2 + 0x^3 + 0x^4 + 7x^5$ כ־ $3 + 2x^2 + 7x^5$.

ב. נהוג אף לא לציין במפורש מקדמי 1 המופיעים לצד "חזקה" חיובית של x. כך, למשל, את $1 + 1x + 1x^2$ נהוג לכתוב כ־ $1 + x + x^2$.

ג. לפולינום המוגדר מעל שדה המספרים הממשיים נקרא **פולינום ממשי**, ולפולינום המוגדר מעל שדה המספרים המרוכבים נקרא **פולינום מרוכב**.

ד. נהוג "להוציא החוצה" סימני מינוס. כך למשל, את הפולינום הממשי $-3 + (-7)x + (-1)x^2$ נכתוב כ־ $-3 - 7x - x^2$.

ה. אם נקבל את המוסכמה המקובלת לרשום x^0 במקום 1, נוכל להציג פולינום כללי $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ בצורה חסכונית יותר באמצעות הסימן סיגמא: $\sum_{i=0}^{n} a_ix^i$.

ו. לעיתים נוח לסמן את הפולינום $P(x)$ בקצרה על־ידי P, אם אין חשש לבלבול.

שימו לב שלפי הגדרה 6.7.2, כל הפולינומים (מעל שדה נתון) שבהם מופיעים **רק** מקדמי 0, שווים זה לזה, כלומר הם אותו הפולינום. לפולינום זה נקרא **פולינום האפס** (מעל השדה הנידון). לפיכך $0, 0 + 0x, 0 + 0x + 0x^2$ הן כולן דרכי רישום שקולות לפולינום האפס.

הגדרה 6.7.3 מעלת פולינום

יהי $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ פולינום שאינו פולינום האפס.

לאינדקס המרבי k שעבורו $a_k \neq 0$ נקרא **מעלת הפולינום** (או **דרגת הפולינום**), ונסמנו $\deg P$.[4]

את מעלת פולינום האפס נגדיר להיות $\deg(0) \overset{\text{def}}{=} -\infty$.

הערה

הסימון $-\infty$ מציין "מינוס אינסוף". הגדרה זו פירושה שאת פולינום האפס אנו רואים כפולינום מיוחד בעל מעלה "מאוד קטנה" - הרבה יותר מכל פולינום שונה מאפס. כמו כן נאמץ את המוסכמה שניתן לחבר את הביטוי $-\infty$ עם כל מספר שלם, והסכום יישאר $-\infty$, וכן שהסכום של $-\infty$ עם עצמו גם הוא $-\infty$.

שאלה 6.7.1

מהי מעלתם של הפולינומים הממשיים הבאים?

א. $1 + x^3$

ב. $x + x^{12}$

ג. x

4 לעיתים אף נשמיט את הסוגריים ונכתוב בקצרה $\deg P$. deg הוא קיצור של המילה degree - מעלה.

ד. 0

ה. $0+0x^3$

ו. 1

ז. 2

התשובה בעמוד 145

סימון 6.7.4

נסמן את אוסף כל הפולינומים מעל שדה F במשתנה x ב־ $F[x]$.

אם n מספר טבעי, אז נסמן ב־ $F_n[x]$ את אוסף כל הפולינומים מעל F שמעלתם קטנה מ־ n.

הערות

א. נזכיר שאנו רואים את הביטוי $-\infty$ כקטן מכל מספר טבעי, ולכן פולינום האפס שייך לכל אחת מן הקבוצות $F_n[x]$.

ב. הקבוצה $F_1[x]$ כוללת פולינומים שמעלתם **קטנה** מ־1, כלומר פולינומים שניתן לכתוב ללא אף מופע של חזקה של x. פולינומים כאלה נוכל לראות כאילו הם סקלרים בשדה. כלומר, אנו מזהים את **הפולינום** $P(x)=a_0$ (שמעלתו 0 או $-\infty$) עם **הסקלר** a_0. פולינומים כאלה נקראים גם **פולינומים קבועים**.

ג. פולינומים שמעלתם 1 בדיוק נקראים **פולינומים ליניאריים**. פולינומים שמעלתם 2 בדיוק נקראים **פולינומים ריבועיים**.

הגדרה 6.7.5 סכום פולינומים

יהיו $P(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n,\ Q(x)=b_0+b_1x+b_2x^2+\ldots+b_mx^m\in F[x]$, ונניח ש־ $m\ge n$ (תמיד נוכל להניח זאת, על־ידי הוספת מקדמי אפס, במידת הצורך). **הסכום** של $P(x)$ ו־ $Q(x)$ הוא הפולינום $(P+Q)(x)$ המוגדר על־ידי:

$$(P+Q)(x)\overset{\text{def}}{=}(a_0+b_0)+(a_1+b_1)x+(a_n+b_n)x^n+b_{n+1}x^{n+1}+\ldots+b_mx^m$$

במילים: הסכום של שני פולינומים מתקבל על־ידי חיבור המקדמים שלהם (בסדר המתאים), ואם "חסרים" מקדמים באחד מהם – בסכום יופיעו מקדמיו של האחר (ניתן לראות זאת כאילו הוספנו מקדמי אפס במקום המקדמים "החסרים").

הערות

- ביטוי מהצורה a_kx^k נקרא **מונום**, והוא סוג פשוט במיוחד של פולינום.
- תוכלו להשתכנע בקלות שפעולת חיבור הפולינומים היא **חילופית** ו**קיבוצית**. אנא ודאו זאת לעצמכם.
- נובע אפוא מכך שנוכל לכתוב את המונומים a_kx^k המופיעים בפולינום $P(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n$ באיזה סדר שנרצה, שכן נוכל לראות פולינום זה כסכום כל המונומים המופיעים בו. בפרט מתקיים:

$$P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n = a_nx^n + \ldots + a_2x^2 + a_1x + a_0$$

(בהצגה הראשונה המונומים מופיעים בסדר עולה של החזקות, ואילו בהצגה השנייה בסדר יורד.)

שאלה 6.7.2

חשבו את הסכומים הבאים של פולינומים ממשיים:

א. $(1 + x^3) + (x + 2x + x^3 + 3x^4)$

ב. $(1 + x^3) + (x - 2x^2 - x^3 + 3x^4)$

ג. $(x^3 + 1) + (-x^3 - 1)$

ד. $(1 + x^3) + (0)$

התשובה בעמוד 145

הערות

א. בחלק ד של שאלה 6.7.2 סכמתם פולינום מסוים עם פולינום האפס, וראיתם שהתוצאה היא הפולינום הראשון. זהו כמובן המצב הכללי - לכל פולינום P מתקיים $P + 0 = 0 + P = P$ (ודאו!). כלומר, פולינום האפס ניטרלי ביחס לפעולת החיבור.

ב. אם $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ פולינום, נסמן ב־ $-P(x)$ את הפולינום $(-a_0) + (a_1)x + (-a_2)x^2 + \ldots + (-a_n)x^n$. ברור כי מתקיים $P(x) + \left(-P(x)\right) = 0$.

ג. נוכל להגדיר את ההפרש בין שני פולינומים $P(x), Q(x)$ על־ידי: $P(x) - Q(x) \overset{\text{def}}{=} P(x) + \left(-Q(x)\right)$.

טענה 6.7.6

יהיו $P(x), Q(x)$ פולינומים מעל שדה F. אזי:

$$\deg(P + Q) \le \max\{\deg P, \deg Q\}$$

הוכחה

אם אחד הפולינומים הוא פולינום האפס, הסכום הוא הפולינום האחר (ראו ההערה דלעיל), והטענה מתקיימת לאור הנחתנו כי $-\infty$ קטן מכל מספר. נניח אם כן, כי שני הפולינומים שונים מאפס, ונסמן $\deg(P) = n, \deg(Q) = m$. כלומר, הפולינומים הנידונים הם מהצורה

$$P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n, \quad Q(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$$

כאשר $a_n \ne 0,\ b_m \ne 0$. ללא הגבלת הכלליות, נוכל להניח כי $m \ge n$, כלומר $\max(m,n) = m$. הפולינום $(P + Q)(x)$ הוא הפולינום

$$(a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_n + b_n)x^n + b_{n-1}x^{n-1} + \ldots + b_mx^m$$

שמעלתו **לכל היותר** $m = \max\{m,n\}$.

מ.ש.ל.

דוגמה

נסמן $P(x)=1+x+x^2,\ Q(x)=1+x^2$. אם נראה פולינומים אלה כפולינומים ממשיים, אזי $(P+Q)(x)=2+x+2x^2$ הוא פולינום ממעלה $2=\max\{\deg P,\deg Q\}=\deg P=\deg Q$.

לעומת זאת, אם נראה את הפולינומים הללו כמוגדרים מעל השדה $\mathbb{Z}_2$, אז מאחר שבשדה זה $1+1=0$, נקבל כי $(P+Q)(x)$, ולכן $\deg(P+Q)=1<2=\max\{\deg P,\deg Q\}$. ◀

הגדרה 6.7.7 כפל פולינומים

יהיו $P(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n,\ Q(x)=b_0+b_1x+b_2x^2+\ldots+b_mx^m\in F[x]$.

נגדיר את **המכפלה** $(P\cdot Q)(x)$ [5] על־ידי:

$$(P\cdot Q)(x)=\sum_{\substack{0\le i\le n\\ 0\le j\le m}} a_ib_jx^{i+j}$$

הערה

חישוב מכפלת פולינומים, בהתאם לכלל שבהגדרה דלעיל, לרוב נותן תוצאה המערבת סכומים של מונומים בעלי אותה מעלה.[6] לאחר חישוב המכפלה, ניתן לקבץ את המונומים בעלי אותה המעלה ולהציג את המכפלה בצורה ה"רגילה" המופיעה בהגדרה 6.7.2. למעשה, הגדרת הכפל מאפשרת לכפול פולינומים בקלות על־ידי פתיחת סוגריים והפעלת חוק הפילוג. תוכלו לבדוק זאת בדוגמאות הבאות ובשאלה העוקבת להן.

דוגמאות

נחשב כמה מכפלות של פולינומים ממשיים:

$$\begin{aligned}(1+3x)\cdot(2+2x)&=1\cdot 2+1\cdot 2x+(3\cdot 2)x+(3\cdot 2)x^{1+1}\\&=2+2x+6x+6x^2=2+8x+6x^2\end{aligned}$$

מעתה והלאה לא נטרח לרשום את הסוגריים סביב המקדמים כפי שעשינו במכפלה דלעיל.

$$\begin{aligned}(1+3x+5x^2)\cdot(2+2x)&=1\cdot 2+1\cdot 2x+3\cdot 2x+3\cdot 2x^{1+1}+5\cdot 2x^2+5\cdot 2x^{2+1}\\&=2+8x+16x^2+10x^3\end{aligned}$$

$$\begin{aligned}(1+x+x^3)\cdot(2+x^2)&=(1+x+0x^2+x^3)\cdot(2+0x+x^2)\\&=1\cdot 2+1\cdot 0x+1\cdot 1x^2+1\cdot 2x+1\cdot 0x^{1+1}+1\cdot 1x^{2+1}+0\cdot 2x^2+0\cdot 0x^{1+2}\\&\quad+0\cdot 1x^{2+2}+1\cdot 2x^3+1\cdot 0x^{1+3}+1\cdot 1x^{2+3}\\&=2+0x+x^2+2x+0x^2+1x^3+0x^2+0x^3+0x^4+2x^3+0x^4+x^5\\&=2+2x+x^2+3x^3+x^5\end{aligned}$$

◀

---

5 לרוב נשמיט את סימן הכפל ונכתוב בקיצור $(PQ)(x)$, או PQ.

6 נזכירכם – מונום הוא פולינום מהצורה c_kx^k.

שאלה 6.7.3

חשבו את המכפלות הבאות:

א. $(1+x^3)\cdot(x+2x+x^3)$

ב. $(1+x)\cdot(2+x)$

ג. $(1+x+x^2+x^3+x^4+x^5+x^6+x^7)\cdot(1-x)$

ד. $(1+x+x^2+x^3+x^4+x^5+x^6+x^7)\cdot(0)$

התשובה בעמוד 146

הערה

המקרה שבחלק ד של שאלה 6.7.3 ניתן להכללה - המכפלה של כל פולינום בפולינום האפס היא פולינום האפס, וזאת מאחר שכל אחד מן המחוברים המופיעים בהגדרה 6.7.7 הוא אפס במקרה זה.

טענה 6.7.8

א. כפל פולינומים הוא חילופי. כלומר, לכל זוג פולינומים P,Q מעל שדה נתון, $PQ=QP$.

ב. כפל פולינומים הוא קיבוצי. כלומר, לכל שלושה פולינומים P,Q,R מעל שדה נתון, $(PQ)R=P(QR)$.

ג. כפל פולינומים מתפלג מעל החיבור. כלומר, לכל שלושה פולינומים P,Q,R מעל שדה נתון, $P(Q+R)=PQ+PR$.

הוכחה

הטענה נובעת באופן ישיר מתוך הגדרה 6.7.7. אנו נוכיח את חלק א, ונשמיט את הוכחת חלקים ב ו־ג (שאותה יוכלו הקוראים החרוצים להשלים בנקל).

נרשום: $P(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n,\ Q(x)=b_0+b_1x+b_2x^2+\ldots+b_mx^m$

לפי הגדרה 6.7.7, $(PQ)(x)=\sum_{0\le i\le n, 0\le j\le m} a_ib_jx^{i+j}$. אם נחליף את שמות האינדקסים i,j, נקבל ש־ $(PQ)(x)$ הוא:

$$\sum_{\substack{0\le j\le n\\0\le i\le m}} a_jb_ix^{j+i} = \sum_{\substack{0\le i\le m\\0\le j\le n}} b_ia_jx^{i+j}$$

בשוויון הסתמכנו על חילופיות הכפל בשדה (שלפיה $a_jb_i=b_ia_j$), ועל כך ש־ $x^{i+j}=x^{j+i}$ לכל i,j. הביטוי שקיבלנו באגף ימין שווה, לפי הגדרה 6.7.7, ל־ $(QP)(x)$.

מ.ש.ל.

הערה

לאור טענה 6.7.8 נוכל להגדיר **חזקה** של פולינום $P(x)$ במספר טבעי k - זהו הפולינום $P^k(x)$ (או בקיצור P^k) המתקבל על־ידי כפל $P(x)$ בעצמו k פעמים (כאשר לאור טענה 6.7.8 אין זה משנה באיזה סדר כופלים). אם $P(x)$ פולינום שונה מאפס, מקובל גם להגדיר: $P^0(x)\overset{\text{def}}{=}1$.

כפי שהערנו לאחר הגדרה 6.7.7, הגדרת הכפל של פולינומים אינה נותנת נוסחה ישירה עבור המקדמים המופיעים במכפלת הפולינומים כסכום מונומים ממעלות שונות. הטענה הבאה נותנת נוסחה מפורשת עבור המקדמים.

טענה 6.7.9

אם $P(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n, \ \ Q(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_m x^m \in F[x]$,
אז

$$(PQ)(x) = c_0 + c_1 x + \ldots + c_{m+n} x^{m+n}$$

כאשר $c_k = \sum_{\substack{i+j=k \\ 0\le i\le n, 0\le j\le m}} a_i b_j$.

הוכחה

יהי k מספר שלם אי־שלילי. אם $a_i b_j x^{i+j}$ הוא אחד המונומים המופיעים בהגדרת הכפל $(PQ)(x)$, אזי $a_i b_j x^{i+j}$ תורם לחישוב המקדם של x^k ב־ $(PQ)(x)$ אם ורק אם החזקה $i+j$ של x היא k, כלומר $i+j=k$. מכיוון שבכל מונום כזה מתקיים $i \le n, j \le m$, מתקיים גם $i+j \le m+n$, ולכן אין ב־ $(PQ)(x)$ אף מונום ממעלה גדולה מ־ $m+n$. עבור $k \le m+n$, המקדם של x^k הוא סכום המקדמים של המונומים המתאימים, כלומר:

$$c_k = \sum_{\substack{i+j=k \\ 0\le i\le n, 0\le j\le m}} a_i b_j$$

מ.ש.ל.

הגדרה 6.7.10 מקדם עליון; פולינום מתוקן

יהי $P(x) \in F[x]$ פולינום שונה מאפס, ונסמן $n = \deg P$.
במקרה זה נוכל לרשום $P(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$, כאשר $a_n \ne 0$.
המקדם a_n נקרא **המקדם העליון** של $P(x)$, ונאמר ש־ $P(x)$ הוא **פולינום מתוקן** אם המקדם העליון שלו הוא 1.

שאלה 6.7.4

בדקו אילו מהפולינומים הבאים הם פולינומים מתוקנים:

א. $1 + x^3$

ב. $1 + 2x^2$

ג. $(1+x) + (2+x)$

ד. $(1+x)\cdot(2+x)$

התשובה בעמוד 146

טענה 6.7.11

יהיו $P(x),Q(x)$ פולינומים מעל שדה F.

א. המקדם העליון של $P(x)\cdot Q(x)$ הוא מכפלת המקדמים העליונים של $P(x)$ ושל $Q(x)$.

ב. אם $P(x),Q(x)$ הם פולינומים מתוקנים, אזי גם $(PQ)(x)$ הוא מתוקן.

ג. מתקיים השוויון:

$$\deg(PQ) = \deg P + \deg Q$$

הוכחה

אם $P(x) = 0$ או $Q(x) = 0$, הטענה על כל חלקיה מתקיימת באופן טריוויאלי.

אחרת - $P(x) \neq 0,\ Q(x) \neq 0$, ונסמן $n = \deg(P),\ m = \deg(Q)$. אזי נוכל לרשום

$$P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n, \quad Q(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$$

כאשר $a_n \neq 0,\ b_m \neq 0$. לפי טענה 6.7.9 מתקיים

$$(PQ)(x) = c_0 + c_1x + c_2x^2 + \ldots + c_nx^n$$

כאשר $c_k = \sum_{\substack{i+j=k \\ 0\le i\le n, 0\le j\le m}} a_ib_j$. בפרט,

$$c_{m+n} = \sum_{\substack{i+j=m+n \\ 0\le i\le n, 0\le j\le m}} a_ib_j$$

אך שימו לב שאם $i \le n$ וגם $j \le m$, אז השוויון $i + j = m + n$ מתקבל רק כאשר $i = n,\ j = m$, ולכן $c_{m+n} = a_nb_m$, ובכך הוכחנו את חלק א.

אם $a_n = b_m = 1$ אזי גם $c_{m+n} = a_nb_m = 1\cdot 1 = 1$, ובכך הוכחנו את חלק ב.

לבסוף, מאחר ש־ $a_n \neq 0,\ b_m \neq 0$ אז מתקיים גם $c_{m+n} = a_nb_m \neq 0$, ולפי הגדרה 6.7.3 קיבלנו כי $\deg(PQ) = m + n = \deg P + \deg Q$.

מ.ש.ל.

שאלה 6.7.5

א. יהיו $P(x),Q(x)$ פולינומים מעל שדה כלשהו כך ש־ $P(x)Q(x) = 0$. הוכיחו ש־ $P(x) = 0$ או $Q(x) = 0$.

ב. הסיקו שאם $P(x),Q(x),R(x)$ פולינומים מעל שדה כך ש־ $P(x)Q(x) = P(x)R(x)$ ו־ $P(x) \neq 0$, אזי $Q(x) = R(x)$.

התשובה בעמוד 146

הגדרה 6.7.12 הצבה בפולינום

יהי $P(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \in F[x]$ פולינום ויהי $\alpha \in F$ סקלר. נגדיר את **ההצבה** $P(\alpha)$ של a ב־ P על־ידי:

$$P(\alpha) = a_0 + a_1 \alpha + a_2 \alpha^2 + \ldots + a_n \alpha^n$$

כלומר, $P(\alpha)$ הוא הסקלר המתקבל על־ידי החלפת כל מופע של x ב־ $P(x)$ ב־ α, וחישוב ערך הביטוי שהתקבל (בהתאם לפעולות בשדה).

שאלה 6.7.6

עבור כל אחד מן הפולינומים הממשיים הבאים, חשבו את $P(0), P(1), P(2)$.

א. $1 + x^3$

ב. $1 + 2x^2$

ג. $2 - x + 2x^2$

התשובה בעמוד 146

הערה

באופן כללי, הצבה של סקלר בפולינום כרוכה בחישוב שעשוי להיות מייגע עבור פולינומים ממעלה גבוהה. מקרה פשוט שבו קל תמיד לחשב את ההצבה (גם עבור פולינומים ממעלה גבוהה), הוא המקרה שבו הסקלר המוצב הוא אפס. אכן, אם נרשום $P(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ אזי נקבל כי:

$$P(0) = a_0 + a_1 0 + a_2 0^2 + \ldots + a_n 0^n = a_0$$

למקדם a_0 קוראים **המקדם החופשי** של $P(x)$.

טענה 6.7.13

יהיו $P(x), Q(x) \in F(x)$ פולינומים ויהי $\alpha \in F$ סקלר. אזי מתקיים:

א. $(P + Q)(\alpha) = P(\alpha) + Q(\alpha)$

ב. $(PQ)(\alpha) = P(\alpha) Q(\alpha)$

טענה 6.7.13 נובעת ישירות מהגדרת הסכום והכפל של פולינומים, ונוותר על הוכחתה.

הגדרה 6.7.14 שורש של פולינום

יהי $P(x) \in F(x)$ פולינום ויהי $\alpha \in F$ סקלר. נאמר ש־ α הוא **שורש** של P אם $P(\alpha) = 0$.

דוגמאות

א. הסקלר 1 הוא שורש של הפולינום הממשי $x^2 + x - 2$.

ב. הסקלר $\frac{1}{\sqrt{2}}(1+i)$ הוא שורש של הפולינום המרוכב $x^2 - i$ (ודאו!).

ג. הסקלר 1 הוא שורש של הפולינום $x^2 + x \in \mathbb{Z}_2[x]$ (ודאו!).

שאלה 6.7.7

הוכיחו כי הסקלר 0 הוא שורש של הפולינום $P(x) \in F(x)$ אם ורק אם המקדם החופשי של P הוא 0.

התשובה בעמוד 146

שאלה 6.7.8

יהיו $P(x) \in F(x)$ פולינומים ויהי $\alpha \in F$ סקלר. הוכיחו ש־α הוא שורש של המכפלה PQ אם ורק אם α הוא שורש של P או שורש של Q.

התשובה בעמוד 147

שימו לב, נוכל לראות כל פולינום ממשי גם כפולינום מרוכב (שהרי כל מספר ממשי הוא גם מספר מרוכב, שחלקו המדומה הוא 0), ולכן עבור פולינומים ממשיים נוכל לחפש את שורשיהם הממשיים, אך גם המרוכבים. לפולינום $x^2 + 1$ למשל, אין שורשים ממשיים, אך יש שני שורשים מרוכבים, $\pm i$. בהמשך הפרק נדון בהרחבה בשורשיהם של פולינומים. כדי שנוכל לעשות זאת, נזדקק לטכניקה נוספת לטיפול בפולינומים - חילוק עם שארית. על כך תלמדו בסעיף הבא.

6.8 חילוק פולינומים עם שארית

בסעיף הקודם הגדרנו חיבור וכפל של פולינומים. מתברר כי ישנו דמיון רב בין פעולות אלה לפעולות החיבור והכפל של מספרים שלמים. נתבונן, למשל, בסכום הבא של מספרים שלמים: $14234 + 61113$. בבית הספר היסודי למדתם כיצד לחשב סכום כזה בעזרת "תרגיל חיבור":

$$\begin{array}{r} 14234 \\ + \\ 61113 \\ \hline 75347 \end{array}$$

החישובים בתרגיל כזה מבוצעים על־ידי "חיבור אנכי", עמודה עמודה, כאשר במידת הצורך "מעבירים אחד" לעמודה הבאה (בתרגיל שהדגמנו לא הייתה העברה כזאת).

כעת נבצע את אותו תרגיל שוב, אך הפעם נכתוב את המספרים באופן מעט שונה - לפי פיתוח העשרוני:

$$\begin{array}{l} 1\cdot 10^4 + 4\cdot 10^3 + 2\cdot 10^2 + 3\cdot 10^1 + 4 \\ + \\ 6\cdot 10^4 + 1\cdot 10^3 + 1\cdot 10^2 + 1\cdot 10^1 + 3 \\ \hline 7\cdot 10^4 + 5\cdot 10^3 + 3\cdot 10^2 + 4\cdot 10^1 + 7 \end{array}$$

גם בצורת כתיבה (מייגעת) זו, החיבור מתבצע באופן "אנכי" - עמודה עמודה, כאשר העמודות הן הספרות המופיעות ליד החזקות המתאימות של 10.

כעת נתבונן בסכום הבא של פולינומים ממשיים:

$$(x^4 + 4x^3 + 2x^2 + 3x^1 + 4) + (6x^4 + x^3 + x^2 + x^1 + 3)$$

נחשב סכום זה על־ידי כתיבת תרגיל חיבור, באופן דומה לתרגיל חיבור המספרים שבחנו:

$$\begin{array}{l} 1x^4 + 4x^3 + 2x^2 + 3x^1 + 4 \\ + \\ 6x^4 + 1x^3 + 1x^2 + 1x^1 + 3 \\ \hline 7x^4 + 5x^3 + 3x^2 + 4x^1 + 7 \end{array}$$

לאור הגדרת חיבור הפולינומים, ברור כי גם כאן החיבור מבוצע באופן אנכי, כאשר העמודות מורכבות מהסקלרים המופיעים לצד ה"חזקות" המתאימות של x.

על־ידי כתיבה בבסיס 10, אנו רואים דמיון בין חישוב סכום של מספרים, כגון הסכום

$$(1\cdot 10^4 + 4\cdot 10^3 + 2\cdot 10^2 + 3\cdot 10^1 + 4) + (6\cdot 10^4 + 1\cdot 10^3 + 1\cdot 10^2 + 1\cdot 10^1 + 3)$$

ובין סכום של פולינומים, כגון הסכום:

$$(1x^4 + 4x^3 + 2x^2 + 3x^1 + 4) + (6x^4 + 1x^3 + 1x^2 + x^1 + 3)$$

למעשה, בדוגמאות שבחנו החישוב היה זהה לחלוטין, לאחר שרשמנו x במקום 10.

כעת נתבונן בדוגמה נוספת, הפעם כזאת שיש בה "העברת אחד". נשווה בין חישוב סכום המספרים

$$(2\cdot10^2+4\cdot10^1+8)+(6\cdot10^2+2\cdot10^1+3)\qquad(=248+623)$$

ובין חישוב סכום הפולינומים:

$$(2x^2+4x^1+8)+(6x^2+2x^1+3)$$

תחילה נחבר דווקא את הפולינומים, "עמודה עמודה":

$$\begin{array}{l} \quad 2x^2+4x^1+8 \\ + \\ \quad \underline{6x^2+2x^1+3} \\ \quad 8x^2+6x^1+11 \end{array}$$

נקבל שהסכום הוא $8x^2+6x^1+11$.

כעת נחבר את המספרים. בשלב ראשון נחבר אותם עמודה עמודה, בדיוק כמו שחיברנו את הפולינומים (כלומר, כאילו במקום 10 מופיע x):

$$\begin{array}{l} \quad 2\cdot10^2+4\cdot10^1+8 \\ + \\ \quad \underline{6\cdot10^2+2\cdot10^1+3} \\ \quad 8\cdot10^2+6\cdot10^1+11 \end{array}$$

התשובה שקיבלנו, $8\cdot10^2+6\cdot10^1+11$, היא כמובן התשובה ה"נכונה" - זהו סכום המספרים שחיברנו, אך כדי להציגו בהצגה העשרונית הרגילה, יהיה עלינו "להעביר אחד" מעמודת היחידות, שחרגה מ־ 10, לעמודת העשרות. התוצאה שנקבל היא $8\cdot10^2+7\cdot10^1+1$, כלומר 871.

הדוגמאות הפשוטות שבחנו מלמדות על המצב הכללי. חיבור פולינומים וחיבור מספרים מתבצע באופן טכני בצורה זהה, פרט לכך שכאשר מחברים מספרים, ייתכן שצריך ל"העביר אחד" כדי לקבל את התשובה הסופית. אם כך, חיבור פולינומים הוא דווקא פשוט יותר מחיבור מספרים!

האנלוגיה שראינו בין חיבור מספרים וחיבור פולינומים תקפה גם עבור הכפל - כפל פולינומים מתבצע בצורה זהה לכפל מספרים (לאחר החלפת x ב־ 10), פרט להעברות אפשריות של אחדות במקרה של כפל מספרים. לא נטרח להדגים חישובי כפל - הקוראים מוזמנים לרשום לעצמם "תרגילי כפל" פשוטים ולהשתכנע בנכונות האמור.

בשלב זה נעיר שהאנלוגיה בין עולם הפולינומים ועולם המספרים היא רחבה ועמוקה, הרבה מעבר למה שניתן לראות מהדמיון ה"חישובי" הנידון. האנלוגיה מתבטאת באופן מרשים במיוחד במקרה שבו השדה שמעליו מוגדרים הפולינומים הוא סופי, והיוותה גורם מניע מרכזי בהתפתחות המתמטיקה במאה העשרים (ועד היום). על כך לא נוכל להרחיב במסגרת קורס זה, אך על נקודת דמיון נוספת, שתהיה שימושית לצרכינו בהמשך הקורס, נצביע כאן. בפרק הקודם למדתם את משפט ה"חילוק עם שארית" של מספרים שלמים. לנוחיותכם, נחזור על המשפט כאן:[1]

1 זהו המשפט בגרסה הכללית שלו - ראו שאלה 5.1.4 בפרק 5.

משפט החילוק עם שארית (של מספרים שלמים)

יהיו a,b מספרים שלמים, כאשר $b \neq 0$. קיים זוג יחיד q,r של מספרים שלמים, כך ש־

א. $a = qb + r$

ב. $0 \leq r < |b|$

למספר q קוראים ה**מנה**, ולמספר r קוראים **השארית** של חילוק a ב־ b.

משפט אנלוגי מתקיים עבור פולינומים:

משפט 6.8.1 חילוק פולינומים עם שארית

יהיו $a(x),b(x)$ פולינומים מעל שדה F,[2] כאשר $b(x) \neq 0$. קיים זוג יחיד $q(x),r(x)$ של פולינומים מעל F, כך ש־

א. $a(x) = q(x)b(x) + r(x)$

ב. $\deg(r(x)) < \deg(b(x))$ [3]

הערות

א. לפולינום $q(x)$ קוראים ה**מנה**, ולפולינום $r(x)$ קוראים **השארית**, של חילוק $a(x)$ ב־ $b(x)$.

ב. אם שארית החלוקה היא פולינום האפס, נאמר ש־ $a(x)$ **מתחלק** ב־ $b(x)$, וש־ $b(x)$ **מחלק** את $a(x)$.

הוכחת משפט 6.8.1

נתחיל בהוכחת ה**קיום** של הזוג $q(x),r(x)$.

נתבונן בקבוצת הפולינומים:

$$A = \{a(x) - q(x)b(x) \mid q(x) \in F(x)\}$$

A איננה קבוצה ריקה, כי הפולינום $a(x)$ בבירור שייך לה. מעלותיהם של הפולינומים ב־ A הם מספרים שלמים אי־שליליים, או $-\infty$ אם פולינום האפס שייך ל־ A. נבחר איבר $r(x)$ ב־ A בעל **מעלה מזערית**, ונסמן $r(x) = a(x) - b(x)q(x)$ עבור פולינום מתאים $q(x)$. עלינו להראות ש־ $\deg(r(x)) < \deg(b(x))$.

אם $r(x) = 0$ אז מאחר ש־ $b(x) \neq 0$, מתקיים $\deg(b(x)) \geq 0 > -\infty = \deg(r(x))$.

נניח ש־ $r(x) \neq 0$. נרשום

$$r(x) = r_0 + r_1 x + \ldots + r_n x^n$$

$$b(x) = b_0 + b_1 x + \ldots + b_m x^m$$

כאשר $r_n, b_m \neq 0$, $n = \deg(r(x)), m = \deg(b(x))$. נניח בשלילה ש־ $n \geq m$.

2 עד כה נהגנו לסמן פולינומים באותיות גדולות כגון P,Q. הפעם בחרנו להשתמש באותיות קטנות כדי להדגיש את הדמיון בין שני המשפטים.

3 כאן מעלת הפולינומים ממלאת את "תפקיד" גודלם (בערך מוחלט) של המספרים במשפט החילוק עם שארית. לדרישה $0 \leq r$ אין מקבילה בחילוק עם פולינומים.

נתבונן בפולינום

$$c(x)=r(x)-\frac{r_n}{b_m}x^{n-m}b(x)=r_nx^n+\ldots+r_1x+r_0-\left(r_nx^n+\frac{r_nb_{m-1}}{b_m}x^{n-1}+\ldots\right)$$

המונומים r_nx^n ו־ $-r_nx^n$ המופיעים באגף ימין מבטלים זה את זה, ולכן מעלת הפולינום $c(x)$ קטנה מ־ n. נוכל להציג את $c(x)$ כך:

$$c(x)=r(x)-\frac{r_n}{b_m}x^{n-m}b(x)=a(x)-q(x)b(x)-\frac{r_n}{b_m}x^{n-m}b(x)$$

$$=a(x)-\left(q(x)+\frac{r_n}{b_m}x^{n-m}\right)b(x)$$

ולכן $c(x)$ הוא פולינום ב־ A, בסתירה להנחת מזעריות מעלת $r(x)$. לכן $\deg(r(x))<\deg(b(x))$.
נוכיח עתה את יחידות הזוג $q(x),r(x)$.

נניח ש־ $p(x),s(x)$ זוג פולינומים המקיימים $a(x)=p(x)b(x)+s(x)$ ו־ $\deg(s(x))<\deg(b(x))$.
מאחר ש־ $a(x)=q(x)b(x)+r(x)=p(x)b(x)+s(x)$ נקבל:

$$r(x)-s(x)=p(x)b(x)-q(x)b(x)=b(x)\big(p(x)-q(x)\big)$$

אם $p(x)-q(x)\neq 0$, אז $\deg\big(p(x)-q(x)\big)\geq 0$, ולכן מעלת אגף ימין היא

$$\deg\big(b(x)\big)+\deg\big(p(x)-q(x)\big)\geq\deg\big(b(x)\big)$$

לפי טענה 6.7.11ג.
אך מכיוון ש־ $\deg\big(r(x)\big),\deg\big(s(x)\big)<\deg\big(b(x)\big)$, גם $\deg\big(r(x)-s(x)\big)<\deg\big(b(x)\big)$, סתירה.
נסיק מכך ש־ $p(x)-q(x)=0$, כלומר $p(x)=q(x)$, ולכן גם:

$$r(x)=a(x)-q(x)b(x)=a(x)-p(x)b(x)=s(x)$$

מ.ש.ל.

בשלב זה ברצוננו להדגים חילוק עם שארית עבור פולינומים; תוך כדי הדגמה נלמד כיצד למצוא את המנה והשארית בחילוק שכזה. גם כאן, יהיה זה שימושי להתבונן תחילה בחילוק ארוך של מספרים, ואז ליישם את האנלוגיה בין מספרים ופולינומים.

דוגמה

נחלק עם שארית את המספר $134(=1\cdot 10^2+3\cdot 10^1+4)$ במספר $11(=1\cdot 10^1+1)$, על־ידי כתיבת תרגיל "חילוק ארוך", כפי שלומדים בבית־הספר היסודי:

$$\begin{array}{r} \boxed{12} \\ 11\overline{)134} \\ \underline{110} \\ 24 \\ \underline{22} \\ \boxed{2} \end{array}$$

המנה היא 12, השארית היא 2.

נסביר בפירוט את השלבים בחישוב דלעיל.

- בשלב הראשון, אנו בודקים כמה ספרות מופיעות במנה - כלומר, מהי החזקה הגדולה ביותר של 10 שמופיעה בה.
- במנה לא יכולות להיות יותר משתי ספרות - לו היו במנה שלוש ספרות (או יותר), אזי במכפלתה ב־11 היו לפחות ארבע ספרות, ולכן המכפלה הייתה גדולה מהמספר התלת־ספרתי 134.
- האם במנה יש שתי ספרות? כן - משום ש־ $110 = 11 \cdot 10$. מה תהיה ספרת העשרות במנה? בהכרח 1, משום ש־ $24 = 110 - 134$. לכן בשלב ראשון, נרשום את ספרת העשרות:

$$\begin{array}{r} 1 \\ 11\overline{)134} \end{array}$$

- ה"תרומה" של ספרת העשרות במנה, למכפלת המנה ב־11, היא $110 = 11 \cdot 10$. נחסיר מספר זה מ־ 134:

$$\begin{array}{r} 1 \\ 11\overline{)134} \\ \underline{110} \\ 24 \end{array}$$

בזאת סיימנו את השלב הראשון - חישוב ספרת העשרות של המנה (שהיא 1). פירוש הדבר הוא שהמספר 11 "נכנס" $1 \cdot 10^1 = 10$ פעמים" בתוך 134. אם נחסיר את ה"תרומה" של 11, שהיא $110 = 11 \cdot 10$, נקבל $134 - 110 = 24$.

- כעת נחשב את ספרת היחידות במנה. הספרה הגדולה ביותר שמכפלתה ב־11 קטנה מ־ 24 היא 2, ולכן ספרת היחידות היא 2 (כלומר, המנה בחלוקה היא 12). נרשום זאת:

$$\begin{array}{r} 12 \\ 11\overline{)134} \\ \underline{110} \\ 24 \end{array}$$

- נכפול עתה את ספרת היחידות שקיבלנו ב־11, ושוב נחסיר:

$$\begin{array}{r} 12 \\ 11\overline{)134} \\ \underline{110} \\ 24 \\ \underline{22} \\ 2 \end{array}$$

המספר שקיבלנו, 2, הוא השארית המבוקשת. נסביר מדוע:
בשלב הראשון קיבלנו כי $134 = 11 \cdot 10 + 24$, ובשלב השני ראינו ש־ $24 = 11 \cdot 2 + 2$.
אם נאחד את שני השלבים, נקבל:

$$134 = 11 \cdot 10 + 24 = 11 \cdot 10 + 11 \cdot 2 + 2 = 11 \cdot 12 + 2$$

שאלה 6.8.1

חקו את הדוגמה דלעיל וחשבו את מנת החלוקה והשארית כאשר אנו מחלקים:

א. את המספר 342 ב־23.

ב. את המספר 1024 ב־82.

התשובה בעמוד 147

דוגמה

חילוק עם שארית של פולינומים מתבצע באופן דומה מאוד (ולמעשה הוא אף פשוט יותר). נסביר כיצד עושים זאת תוך הדגמת חילוק עם שארית של הפולינום הממשי $8x^2+6x^1+11$ בפולינום (הממשי) $2x+3$. נעבוד שלב שלב:

- מעלתו של $8x^2+6x^1+11$ היא 2, ומעלתו של $2x+3$ היא 1. מעלת המנה תהיה הפרש המעלות $2-1=1$. כלומר, החזקה הגבוהה ביותר של x שתופיע במנה היא 1. המקדם שיופיע לצד חזקה זו הוא המספר שמכפלתו ב־2 (המקדם העליון ב־$2x+3$) היא 8, כלומר $8/2=4$. נוכל להתחיל לכתוב "תרגיל חילוק":

$$\begin{array}{r} 4x \\ 2x+3\overline{\smash{)}\,8x^2+6x^1+11} \end{array}$$

- המכפלה של $4x$ ב־$2x+3$ היא $8x^2+12x$. נחסיר פולינום זה מ־$8x^2+6x^1+11$:

$$\begin{array}{r} 4x \\ 2x+3\overline{\smash{)}\,8x^2+6x^1+11} \\ \underline{8x^2+12x^1} \\ -6x+11 \end{array}$$

- המקדם של x^0 (המקדם החופשי - שהוא האנלוג כאן לספרת היחידות בדוגמאות "המספריות") הוא זה שמכפלתו ב־2 (המקדם העליון ב־$2x+3$) היא -6, כלומר $-3=\frac{-6}{2}$. כעת נוכל להשלים את החישוב:

$$\begin{array}{r} 4x-3 \\ 2x+3\overline{\smash{)}\,8x^2+6x+11} \\ \underline{8x^2+12x} \\ -6x+11 \\ \underline{-6x-9} \\ 20 \end{array}$$

אם כן, מנת החילוק היא $4x-3$, והשארית 20 (שימו לב שבמקרה זה השארית היא פולינום קבוע - אין זה המצב באופן כללי, כפי שתראו בדוגמה הבאה). ודאו לעצמכם כי אכן מתקיים $8x^2+6x^1+11=(2x+3)(4x-3)+20$. ◀

דוגמה

נחלק את הפולינום הממשי x^3+x^2+2x+2 בפולינום x^2+1:

- מעלתו של x^3+x^2+2x+2 היא 3, ומעלתו של x^2+1 היא 2 – מעלת המנה תהיה $3-2=1$, כלומר החזקה הגבוהה ביותר של x שתופיע במנה היא 1. המקדם שיופיע לצד חזקה זו הוא המספר הממשי שמכפלתו ב־1 (המקדם העליון ב־ x^2+1) היא 1, כלומר 1.

$$\begin{array}{r} 1\cdot x \\ x^2+1\overline{\big)\, x^3+x^2+2x+2} \end{array}$$

- נחסיר את $(x^2+1)\cdot x\ (=x^3+x)$ מ־ x^3+x^2+2x+2 ונקבל:

$$\begin{array}{r} x \\ x^2+1\overline{\big)\, x^3+x^2+2x+2} \\ \underline{x^3+0x^2+x} \\ x^2+x+2 \end{array}$$

- המקדם החופשי במנה הוא זה שמכפלתו ב־1 (המקדם העליון ב־ x^2+1) היא 1 (המקדם של x^2 בהפרש שקיבלנו), כלומר שוב 1, ולכן מנת החלוקה היא $x+1$. כעת נוכל להשלים את החישוב:

$$\begin{array}{r} x+1 \\ x^2+1\overline{\big)\, x^3+x^2+2x+2} \\ \underline{x^3+0x^2+x} \\ x^2+x+2 \\ \underline{x^2+0x+1} \\ x+1 \end{array}$$

ההפרש שקיבלנו, $x+1$, הוא שארית החלוקה. ◀

שאלה 6.8.2

חקו את הדוגמאות דלעיל וחשבו את מנת החלוקה ואת שארית החלוקה של הפולינומים הממשיים הבאים:

א. x^2+1 ב־ $2x+1$

ב. $x^4+x^3+x^2+3$ ב־ x^2+2

התשובה בעמוד 147

עד כה הדגמנו חילוק עם שארית של פולינומים ממשיים, אך נוכל לחלק עם שארית פולינומים מעל כל שדה באותו אופן בדיוק, כאשר נקפיד לבצע את פעולות החשבון בין המקדמים בשדה המתאים.

דוגמה

נחלק עם שארית את הפולינום x^2+1 בפולינום $x-i$, מעל המרוכבים:

- שלב ראשון: המנה היא פולינום ממעלה $2-1=1$, שמקדמו העליון הוא $1/1=1$:

$$\begin{array}{r l} & x \\ x-i \big) & \overline{x^2+1} \\ & \underline{x^2-ix} \\ & ix+1 \end{array}$$

- שלב שני: המקדם החופשי של המנה הוא הסקלר המרוכב שמכפלתו ב־1 (המקדם העליון ב־ $x-i$) הוא i, כלומר $i/1=i$:

$$\begin{array}{r l} & x+i \\ x-i \big) & \overline{x^2+1} \\ & \underline{x^2-ix} \\ & ix+1 \\ & \underline{ix+1} \\ & 0 \end{array}$$

קיבלנו שמנת החלוקה היא $x+i$ ושארית החלוקה היא פולינום האפס - כלומר הפולינום x^2+1 מתחלק (ללא שארית) בפולינום $x-i$. ואכן, ודאו כי $(x+i)\cdot(x-i)=x^2+1$. ▸

שאלה 6.8.3

חלקו עם שארית:

א. את x^2+i ב־ $x-1$, מעל המרוכבים.

ב. את x^2+1 ב־ $x+1$, מעל השדה $\mathbb{Z}_2$.

התשובה בעמוד 148

בעזרת משפט החילוק עם שארית, נוכל להוכיח תוצאה כללית אודות מספר השורשים האפשרי לפולינום ממעלה נתונה. לפני שנציג תוצאה זו, נביא את הלמה החשובה הבאה:

למה 6.8.2

יהי $P(x)$ פולינום מעל שדה כלשהו F, ויהי $\alpha\in F$ סקלר. אזי α הוא שורש של $P(x)$ אם ורק אם $P(x)$ מתחלק בפולינום $x-\alpha$.

הוכחה

על פי משפט החלוקה עם שארית נוכל לרשום $P(x)=Q(x)(x-\alpha)+R(x)$, כאשר $Q(x),R(x)$ הם פולינומים מעל F, ומעלתו של $R(x)$ קטנה מ־ $\deg(x-\alpha)=1$, כלומר $R(x)$ פולינום קבוע. לפי טענה 6.7.13 מתקיים:

$$P(\alpha)=Q(\alpha)(\alpha-\alpha)+R(\alpha)=Q(\alpha)\cdot 0+R(\alpha)=R(\alpha)$$

לכן α הוא שורש של $P(x)$ אם ורק אם הוא שורש של $R(x)$. אך מכיוון ש־$R(x)$ הוא פולינום קבוע, α הוא שורש של $R(x)$ אם ורק אם $R(x) = 0$ (ודאו זאת לעצמכם!), כלומר אם ורק אם $x - \alpha$ מחלק את $P(x)$.

מ.ש.ל.

מסקנה 6.8.3

יהי $P(x)$ פולינום שונה מאפס ממעלה n, מעל שדה כלשהו F. אזי ל־$P(x)$ יש לכל היותר n שורשים שונים ב־F.

הוכחה

נוכיח את המסקנה באינדוקציה על $n = \deg P$.

ראשית, מכיוון שהנחנו ש־$P(x)$ הוא פולינום שונה מאפס, מתקיים $n \geq 0$.

אם $n = 0$ אז $P(x)$ הוא קבוע a, כאשר $a \neq 0$. לפולינום זה אין שורשים, כלומר יש לו $n = 0$ שורשים.

נניח כי הטענה נכונה לכל הפולינומים ממעלה n, ויהי $P(x)$ פולינום ממעלה $n+1$. אם ל־$P(x)$ אין שורשים, הטענה מתקיימת באופן טריוויאלי. לכן נניח כי ל־$P(x)$ יש לפחות שורש אחד, נאמר α. לפי למה 6.8.2 מתקיים $P(x) = Q(x)(x-\alpha)$ עבור איזשהו פולינום $Q(x)$. אם β הוא שורש כלשהו של $P(x)$, אז לפי טענה 6.7.8, $Q(\beta)(\beta - \alpha) = 0$, ולכן $\beta = \alpha$ או $Q(\beta) = 0$. כלומר, כל שורש שונה מ־α של $P(x)$ הוא בהכרח שורש של $Q(x)$. בנוסף, α הוא שורש של $P(x)$ - ייתכן שהוא גם שורש של $Q(x)$ וייתכן שלא. לכן, אם מספר שורשי $Q(x)$ הוא k, אז מספר שורשי $P(x)$ הוא לכל היותר $k+1$.

לפי טענה 6.7.11 מתקיים

$$n + 1 = \deg P = \deg Q + \deg(x - \alpha) = \deg Q + 1$$

ולכן $\deg Q = n$. לפי הנחת האינדוקציה, ל־$Q(x)$ ישנם לכל היותר n שורשים, כלומר $k \leq n$, ולכן נסיק שלפולינום $P(x)$ לכל היותר $n+1$ שורשים.

מ.ש.ל.

הערה

מסקנה 6.8.3 מבטיחה שלפולינום ממעלה n יש **לכל היותר** n שורשים שונים - אין היא מבטיחה קיומם של n שורשים **בדיוק**. לדוגמה, לפולינום הממשי הריבועי $x^2 + 2x + 1$ יש שורש בודד (השורש -1), ואילו לפולינום הממשי $x^2 + 5$ אין שורשים (ממשיים) בכלל.

שאלה 6.8.4

במסקנה 6.8.3 הנחנו שהפולינום שונה מאפס. מדוע הדרנו את פולינום האפס מנוסח המשפט?

התשובה בעמוד 148

מסקנה 6.8.4

יהי F שדה אינסופי, ויהיו $P(x),Q(x) \in F[x]$ פולינומים כך ש־$P(\alpha) = Q(\alpha)$ לכל $\alpha \in F$. אזי הפולינומים $P(x),Q(x)$ שווים זה לזה.

הוכחה

נסמן $R(x) = P(x) - Q(x)$. אזי $R(\alpha) = P(\alpha) - Q(\alpha) = 0$ לכל $\alpha \in F$, ובפרט ל־$R(x)$ יש אינסוף שורשים שונים. לפי מסקנה 6.8.3, $R(x) = 0$, ולכן $P(x) = Q(x)$.

מ.ש.ל.

נדגיש כי מסקנה 6.8.4 אינה מתקיימת ללא ההנחה כי השדה F הוא אינסופי. למשל, אם $F = \mathbb{Z}_2$ ואם $P(x) = x, Q(x) = x^2$, אזי $P(x), Q(x)$ הם פולינומים שונים, ובכל זאת מתקיים $P(1) = Q(1) = 1$, $P(0) = Q(0) = 0$, כלומר $P(\alpha) = Q(\alpha)$ לכל $\alpha \in F$.

6.9 המשפט היסודי של האלגברה

בסעיף 6.6 טיפלנו בסוגיית מציאת השורשים של פולינומים מרוכבים מטיפוס מסוים, בלי "לקרוא לילד בשמו". התבוננו שם בפולינום $P(x) = x^n - 1$, כאשר n מספר טבעי. שורש של פולינום זה הוא סקלר α המקיים $\alpha^n = 1$. במונחי סעיף 6.6, שורש של הפולינום $P(x) = x^n - 1$ הוא שורש יחידה מסדר n. אם כן, אנו יודעים בדיוק כיצד נראים כל שורשי הפולינום הזה (כפי שראינו בסעיף 6.6). לאחר מכן אף הרחבנו את הדיון ותיארנו את כל שורשי הפולינום $x^n - w$, כאשר w מספר מרוכב כלשהו.

עבור פולינומים כלליים (לאו דווקא מהצורה הנידונה) ממעלה נמוכה, ניתן למצוא את שורשיהם באמצעות נוסחאות ידועות (הנוסחה למציאת שורשיהם של פולינומים ממשיים/מרוכבים ממעלה 2, למשל, ודאי מוכרת לכם[1]). עבור פולינומים כלליים ממעלה גבוהה אין, למרבה הצער, נוסחה למציאת שורשיהם. למרות זאת, קיימות תוצאות חשובות על אודות הקיום של שורשים כאלה ועל מספרם - תוצאות המכלילות את מה שלמדתם בסעיף 6.6 - שם ראיתם שלכל מספר מרוכב w השונה מאפס ישנם בדיוק n שורשים מסדר n. נפתח בתוצאה היסודית הבאה:

משפט 6.9.1 המשפט היסודי של האלגברה

יהי $P(x)$ פולינום ממשי/מרוכב ממעלה גדולה מאפס.[2] אזי ל־ $P(x)$ יש שורש מרוכב.

המשפט היסודי של האלגברה הוכח לראשונה על־ידי גאוס ב־1799. לא נוכל להביא הוכחה למשפט במסגרת קורס זה (הקוראים המעוניינים יוכלו ללמוד את הוכחתו בהמשך לימודיהם, במסגרת הקורסים **פונקציות מרוכבות** או **הרחבת שדות ותורת גלואה**). עם זאת, בהסתמך על המשפט, נוכל לבסס תוצאה מדויקת על אודות "כמות" השורשים המרוכבים של פולינום ממשי/מרוכב; את המובן המדויק של "כמות השורשים" נבהיר בהמשך הסעיף.

שאלה 6.9.1

יהי F שדה ויהיו $\alpha_1, \alpha_2, \dots, \alpha_n$ סקלרים. נתבונן בפולינום:

$$P(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n)$$

א. מהי המעלה של $P(x)$?

ב. מה הם כל השורשים של $P(x)$ ב־ F?

התשובה בעמוד 148

התשובה בעמוד 148

נתבונן בפולינום מהצורה $P(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n)$ מעל שדה F. לפי חלק ב של שאלה 6.9.1, השורשים של $P(x)$ הם הסקלרים $\alpha_1, \alpha_2, \dots, \alpha_n$ (ורק אלה). האם פירוש הדבר כי

---

1 השורשים של $ax^2 + bx + c$, כאשר $a \neq 0$, הם $\frac{-b - \sqrt{b^2 - 4ac}}{2a}$, $\frac{-b + \sqrt{b^2 - 4ac}}{2a}$. קיימות נוסחאות בעלות אופי דומה (אם כי ארוכות ומסובכות יותר) גם עבור פולינומים ממעלה שלישית ורביעית.

2 כלומר, פולינום שאינו קבוע.

לפולינום יש בדיוק n שורשים? ייתכן שתתפתו לענות בחיוב, אך שימו לב - לא הנחנו כי הסקלרים $\alpha_1,\alpha_2,\ldots,\alpha_n$ שונים זה מזה! לפולינום הממשי $(x-1)(x-3)(x-5)$ יש שלושה שורשים - $1,3,5$, אך לפולינום $(x-1)^2(x-4)$, למשל, יש שני שורשים בלבד - 1 ו־ 4. עם זאת, ייתכן שהרגשתם שבין שני השורשים הללו יש הבדל מהותי - לשורש 4 יש מופע אחד בלבד ב־ $(x-1)^2(x-4)$, בעוד השורש 1 "מופיע פעמיים" (שכן $(x-1)^2=(x-1)(x-1)$) - זהו שורש "כפול".

נדרשת, אם כן, הגדרה שתיתן מובן מדויק להבדל שבין השורשים בדוגמאות הללו. לצורך זה נקדים כמה טענות עזר.

למה 6.9.2

יהי $P(x)$ פולינום מעל שדה F ויהי k מספר טבעי. אזי $\deg(P^k(x))=k\deg(P(x))$.

שאלה 6.9.2

א. הוכיחו את למה 6.9.2.

ב. יהי $\alpha\in F$ סקלר. מהי המעלה של $(x-\alpha)^k$?

התשובה בעמוד 149

למה 6.9.3

יהי $P(x)$ פולינום שונה מאפס מעל שדה F, ונניח ש־ $P(x)$ מתחלק בפולינום $Q(x)$. אזי $\deg\left(Q(x)\right)\le\deg\left(P(x)\right)$.

הוכחה

לפי הנתון קיים פולינום $S(x)$ כך ש־ $P(x)=S(x)Q(x)$. לפי טענה 6.7.11 מתקיים $\deg P(x)=\deg S(x)+\deg Q(x)$. שימו לב, מאחר ש־ $P(x)$ שונה מאפס, גם הפולינומים $S(x),Q(x)$ שונים מאפס, ולכן כל שלוש המעלות המופיעות בשוויון לעיל הם מספרים שלמים אי־שליליים. נסיק ש־ $\deg P(x)=\deg S(x)+\deg Q(x)\ge\deg Q(x)$.

מ.ש.ל.

משילובן של מסקנות למה 6.9.3 ושאלה 6.9.1 אנו מקבלים:

למה 6.9.4

יהי $P(x)$ פולינום ממעלה חיובית מעל שדה F, ונניח ש־ $P(x)$ מתחלק בפולינום $(x-\alpha)^k$, כאשר $\alpha\in F$ סקלר ו־ k מספר טבעי. אזי $k\le\deg\left(P(x)\right)$.

כעת נוכל להגדיר:

הגדרה 6.9.5 ריבוי של שורש של פולינום

יהי $P(x)$ פולינום ממעלה חיובית מעל שדה F, ויהי $\alpha \in F$ שורש של $P(x)$. **הריבוי** של השורש α בפולינום $P(x)$ הוא המספר הטבעי המרבי k שעבורו הפולינום $(x-\alpha)^k$ מחלק את $P(x)$.

הערות

א. כאשר ברור באיזה פולינום מדובר, לרוב נקצר ונאמר "הריבוי של השורש α" בלא ציון הפולינום $P(x)$.

ב. לפי למה 6.8.2, היותו של α שורש של $P(x)$ מבטיח כי $x-\alpha=(x-\alpha)^1$ מחלק את $P(x)$, וממילא קיים מספר טבעי k שעבורו $(x-\alpha)^k$ מחלק את $P(x)$. יתר על כן, אם k מספר טבעי שכזה, אזי בהכרח $k \le \deg(P)$ לפי למה 6.7.4, ולכן הריבוי של שורש של פולינום הוא מספר טבעי מוגדר היטב החסום על־ידי מעלת הפולינום.

שאלה 6.9.3

א. הראו שאם $(x-\alpha)^k$ מחלק פולינום $P(x)$ עבור מספר טבעי k, אזי גם $(x-\alpha)^m$ מחלק את $P(x)$, לכל $m \le k$.

ב. הראו שאם $P(x)=(x-\alpha)^k Q(x)$ עבור מספר טבעי k ו־α אינו שורש של $Q(x)$, אזי הריבוי של השורש α של $P(x)$ הוא k.

התשובה בעמוד 149

את מסקנת חלק ב של שאלה 6.9.3 ננסח מחדש כך:

למה 6.9.5

יהי $P(x)$ פולינום מעל שדה כלשהו F, ויהי $\alpha \in F$ שורש של $P(x)$. אזי הריבוי של α ב־$P(x)$ הוא k אם ורק אם קיים פולינום $Q(x)$ כך ש־$P(x)=(x-\alpha)^k Q(x)$ ו־α אינו שורש של $Q(x)$.

נניח כי בפנינו פולינום שונה מאפס $P(x)$, ונניח כי מצאנו שסקלר מסוים α הוא שורש של $P(x)$. כיצד נבדוק מהו הריבוי של השורש α?

בשלב ראשון, נחלק את $P(x)$ ב־$x-\alpha$ (בשיטת החילוק עם שארית שלמדנו בסעיף הקודם, מובטח לנו ששארית החלוקה כאן היא אפס), ונרשום $P(x)=(x-\alpha)P_1(x)$. יש שתי אפשרויות - או ש־α הוא שורש של $P_1(x)$, או שלא:

אם α אינו שורש של $P_1(x)$ אזי לפי למה 6.9.5 הריבוי של α הוא 1.

אם α הוא שורש של $P_1(x)$, אז לפי למה 6.8.2, $x-\alpha$ מחלק גם את $P_1(x)$. במקרה זה נבצע שלב שני, ונרשום $P_1(x)=(x-\alpha)P_2(x)$, כלומר $P(x)=(x-\alpha)^2 P_2(x)$. כמו בשלב הראשון, אם α אינו שורש של $P_2(x)$, נסיק מלמה 6.9.5 שהריבוי של α הוא 2.

אם α הוא שורש של $P_2(x)$, נצטרך לבצע חלוקה נוספת ולהמשיך לשלב נוסף של חישוב. על תהליך זה נחזור שוב ושוב - ומובטח לנו שהתהליך יסתיים, משום שהריבוי של כל שורש חסום על־ידי מעלת הפולינום.

דוגמה

נתבונן בפולינום הממשי $P(x) = x^3 - x^2 - x + 1$. הסקלר 1 הוא שורש של הפולינום (בדקו!). נחשב את הריבוי שלו:

בשלב ראשון, נחלק את $P(x)$ ב־ $x-1$, ונקבל $P(x) = (x-1)P_1(x)$ כאשר $P_1(x) = x^2 - 1$ (בדקו!). מאחר ש־1 הוא גם שורש של $P_1(x)$ (בדקו!) נחלק שוב, ונקבל $P_1(x) = (x-1)P_2(x)$, כאשר $P_2(x) = x+1$. מאחר ש־1 אינו שורש של $P_2(x)$, החישוב הסתיים - קיבלנו ש־ $P(x) = (x-1)^2 P_2(x)$, ולפי למה 6.9.5 הריבוי של 1 הוא 2.

לפולינום $P(x)$ יש שורש נוסף - השורש -1.

ראינו ש־ $P(x) = (x-1)^2(x+1) = \big(x-(-1)\big)(x-1)^2$, ומכיוון ש־$-1$ אינו שורש של $(x-1)^2$, הריבוי של השורש -1 הוא 1, לפי למה 6.9.5. ◀

הערה

על שורש של פולינום שריבויו 1 אומרים שהוא שורש **פשוט**; וכאשר ריבויו גדול מ־1 אומרים שהוא שורש **מְרוּבֶּה**. בדוגמה הקודמת -1 הוא שורש פשוט, בעוד שהשורש 1 הוא שורש מרובה.

שאלה 6.9.4

בכל אחד מהמקרים הבאים, בדקו מהו הריבוי של השורש α:

א. $P(x) = x^2 - 4$, $\alpha = 2$, מעל שדה הממשיים.

ב. $P(x) = x^3 + x^2 - x - 1$, $\alpha = -1$, מעל שדה הממשיים.

ג. $P(x) = x^3 - 3x^2 + 3x - 1$, $\alpha = 1$, מעל שדה הממשיים.

ד. $P(x) = x^2 + 1$, $\alpha = i$, מעל שדה המרוכבים.

ה. $P(x) = x^2 + 1$, $\alpha = 1$, מעל השדה $\mathbb{Z}_2$.

התשובה בעמוד 149

טענה 6.9.6

יהי $P(x)$ פולינום שונה מאפס ממעלה n מעל שדה המספרים המרוכבים. אז ניתן לכתוב את $P(x)$ בצורה

$$P(x) = c(x-\alpha_1)\cdot(x-\alpha_2)\cdot\ldots\cdot(x-\alpha_n)$$

כאשר $\alpha_1, \alpha_2, \ldots, \alpha_n$ היא סדרת מספרים מרוכבים הכוללת את כל שורשי $P(x)$ (ייתכן שחלק מן השורשים מופיעים כמה פעמים), ו־ c הוא המקדם העליון של $P(x)$ (אם $n = 0$ אז לא מופיעים גורמים מהצורה $x - \alpha_i$ כלל).

הוכחה

נוכיח את הטענה באינדוקציה על n.

אם $n = 0$ אז $P(x)$ הוא פולינום קבוע שונה מאפס c, וקבוע זה הוא גם המקדם העליון של $P(x)$.
נניח שהטענה נכונה לכל פולינום ממעלה n, ויהי $P(x)$ פולינום ממעלה $n+1$.

לפי המשפט היסודי של האלגברה (משפט 6.9.1) יש ל־ $P(x)$ שורש מרוכב כלשהו, נסמנו α_{n+1}. לפי למה 6.8.2 קיים פולינום מרוכב $Q(x)$ כך ש־ $P(x) = (x-\alpha_{n+1})Q(x)$. שימו לב ש־

$$n+1 = \deg\big(P(x)\big) = \deg(x-\alpha_{n+1}) + \deg\big(Q(x)\big) = 1 + \deg\big(Q(x)\big)$$

ולכן $n = \deg\big(Q(x)\big)$. לפי הנחת האינדוקציה נוכל לכתוב

$$Q(x) = c(x-\alpha_1)\cdot(x-\alpha_2)\cdot\ldots\cdot(x-\alpha_n)$$

כאשר $\alpha_1,\ldots,\alpha_n$ הם השורשים המרוכבים של $Q(x)$, ו־ c הוא המקדם העליון של $Q(x)$. נסיק ש־

$$P(x) = c(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n)\cdot(x-\alpha_{n+1})$$

ברור ש־ $\alpha_1,\ldots,\alpha_{n+1}$ הם כל שורשי $P(x)$, ולפי טענה 6.7.11א המקדם העליון של $P(x)$ הוא מכפלת המקדם העליון של $Q(x)$ במקדם העליון של $x-\alpha_{n+1}$, כלומר $c\cdot 1 = c$.

מ.ש.ל.

בטענה 6.9.6 הסקלרים $\alpha_1,\ldots,\alpha_n$ הם כל השורשים של הפולינום $P(x)$, אך לא הנחנו כי שורשים אלה שונים זה מזה – בהחלט ייתכן שיש חזרות. נוכיח כעת תוצאה חריפה יותר המתייחסת גם להיבט זה.

משפט 6.9.7

יהי $P(x)$ פולינום שונה מאפס ממעלה n מעל שדה המספרים המרוכבים ויהיו $\alpha_1,\ldots,\alpha_m$ כל השורשים **השונים** של $P(x)$. אזי ניתן לכתוב את $P(x)$ בצורה הבאה

$$P(x) = c(x-\alpha_1)^{k_1}\cdot(x-\alpha_2)^{k_2}\cdot\ldots\cdot(x-\alpha_n)^{k_n}$$

כאשר c הוא המקדם העליון של $P(x)$, הריבוי של השורש α_i הוא k_i לכל $1 \le i \le m$, ומתקיים $k_1+\ldots+k_m = n$.

הוכחה

על פי טענה 6.9.6 נוכל לכתוב $P(x) = c\cdot(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n)$, כאשר $\alpha_1,\ldots,\alpha_n$ הם השורשים המרוכבים של $P(x)$, ו־ c הוא המקדם העליון של $P(x)$. על־ידי שינוי סדר האיברים (במידת הצורך) נוכל להניח שמתוך השורשים $\alpha_1,\ldots,\alpha_n$, השורשים $\alpha_1,\ldots,\alpha_m$ הם כולם שונים זה מזה, בעוד ש־ $\alpha_{m+1},\ldots,\alpha_n$ הם חזרות על איברים מתוך $\alpha_1,\ldots,\alpha_n$. לכל $1 \le i \le m$, נסמן את מספר החזרות של

הסקלר α_i בסדרה $\alpha_1,\dots,\alpha_n$ ב־ k_i. אז מאחר שבסדרה $\alpha_1,\dots,\alpha_n$ יש n איברים, מתקיים $k_1+\dots+k_m=n$. את ההצגה $P(x)=c\cdot(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n)$ נוכל לכתוב מחדש כ־

$$P(x)=c(x-\alpha_1)^{k_1}\cdot(x-\alpha_2)^{k_2}\cdot\ldots\cdot(x-\alpha_m)^{k_m}$$

לפי למה 6.9.5, k_i הוא הריבוי של השורש α_i, לכל $1\le i\le m$, שכן α_i אינו שורש של הפולינום $\prod\limits_{\substack{1\le j\le m\\ j\ne i}}(x-\alpha_j)^{k_j}$.

מ.ש.ל.

שימו לב לטענה האחרונה במשפט 6.9.7 המבטיחה שמספר השורשים של פולינום מרוכב נתון (שאינו קבוע), **כאשר סופרים כל שורש בהתאם לריבוי שלו**, שווה למעלת הפולינום. ניתן לראות זאת כמעין טענה הפוכה למסקנה 6.8.3, עבור פולינומים מרוכבים.

הערה

שימו לב, משפט 6.9.7 מתקיים עבור פולינומים מרוכבים בלבד, ולא מעל שדה כללי, ובפרט לא מעל שדה הממשיים. עם זאת, נוכל לראות כל פולינום ממשי גם כפולינום מרוכב, ובתור שכזה המשפט יהיה תקף גם עבורו.

דוגמה

נתבונן בפולינום $P(x)=2x^3-4x^2+2x-4$. ניתן להראות כי השורש הממשי היחיד של פולינום זה הוא 2, וכי מעל הממשיים לא קיימת לפולינום הצגה מהצורה המופיעה במשפט 6.9.7 (נסו להבהיר זאת לעצמכם). לעומת זאת, מעל המרוכבים נוכל להציג פולינום זה בצורה $P(x)=2(x+i)\big(x-(-i)\big)(x-2)$ (בדקו!). השורשים המרוכבים של $P(x)$ הם אפוא $i,-i,2$, הריבוי של כל אחד מהם הוא 1, והמקדם העליון של $P(x)$ הוא 2. ◀

בסעיף 6.6 ראיתם שלפולינום $P(x)=x^n-w$ (כאשר n מספר טבעי ו־ w מספר מרוכב כלשהו) יש בדיוק n שורשים מרוכבים - נסמנם $\zeta_1,\dots,\zeta_n$. לפי משפט 6.9.7, מתקיים $P(x)=(x-\zeta_1)^{k_1}\cdot(x-\zeta_2)^{k_2}\cdot\ldots\cdot(x-\zeta_n)^{k_n}$, כאשר הריבוי של ζ_i הוא k_i לכל $1\le i\le n$, ומתקיים $k_1+\dots+k_n=n$. מאחר שכל אחד מה־k_i־ים הוא מספר טבעי, נובע ש־ $k_i=1$ לכל $1\le i\le n$. כלומר, כל אחד מהשורשים מסדר n של w הוא שורש פשוט של הפולינום x^n-w.

משפט 6.9.7 נותן בידינו תיאור אלגנטי לפולינום מרוכב בעזרת שורשיו, אך אינו מצביע על שיטה למציאת תיאור זה - אין בידינו מתכון למציאת השורשים של פולינום מרוכב נתון שמעלתו גדולה מארבע. עם זאת, עבור פולינומים בעלי מקדמים רציונליים, ניתן, במקרים מסוימים, למצוא שורשים גם בלא נוסחה כללית. זהו נושאו של הסעיף הבא.

6.10 שורשים של פולינומים בעלי מקדמים רציונליים

בסעיף זה נתאר שיטה שימושית למציאת כל השורשים הרציונליים של פולינומים בעלי מקדמים רציונליים. נפתח בטענה הבאה:

טענה 6.10.1 הלמה של גאוס[1]

יהי $P(x)$ פולינום מתוקן שכל מקדמיו הם מספרים שלמים. אם α שורש רציונלי של $P(x)$, אזי α הוא מספר שלם.

הוכחה

נרשום

$$P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

ונציג את השורש α כשבר "מצומצם", כלומר בצורה $\alpha = \frac{r}{s}$, כאשר r ו־s הם מספרים שלמים **זרים** (כלומר, אין להם מחלק טבעי משותף גדול מ־1).[2] בלא הגבלת הכלליות נוכל להניח ש־s חיובי (על־ידי החלפת סימניהם של r ו־s במידת הצורך). מאחר ש־$\alpha = \frac{r}{s}$ הוא שורש של הפולינום, נקבל:

$$\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \ldots + a_1\left(\frac{r}{s}\right) + a_0 = 0$$

נכפול שוויון זה ב־s^n, נחסר משני האגפים r^n, ונקבל:

$$-r^n = a_{n-1}r^{n-1}s + a_{n-2}r^{n-2}s^2 + \ldots + a_1 rs^{n-1} + a_0 s^n$$

$$= (a_{n-1}r^{n-1} + a_{n-2}r^{n-2}s + \ldots + a_1 rs^{n-2} + a_0 s^{n-1})s$$

בתוך הסוגריים באגף ימין רשום מספר **שלם**, ומכאן ש־s מחלק את r^n. אם p מספר ראשוני המחלק את s, אזי p מחלק את r^n, ולכן p מחלק את r, לפי שאלה 5.3.4, וזאת בסתירה להיותם של r ו־s זרים. נסיק ש־s אינו מתחלק באף מספר ראשוני, ולכן לפי המשפט היסודי של האריתמטיקה נקבל ש־$s = 1$. לכן:

$$\alpha = \frac{r}{s} = \frac{r}{1} = r$$

כלומר, α הוא שלם.

מ.ש.ל.

1 יש כמה תוצאות קרובות המכונות במתמטיקה בשם "הלמה של גאוס"; הגרסה שהבאנו כאן אינה החריפה ביותר, אך נסתפק בה לצרכינו הנוכחיים.

2 כל מספר רציונלי ניתן לכתוב כשבר מצומצם. אם a,b הם מספרים שלמים כאשר $a \neq 0$ ואם g הוא המחלק המשותף המרבי של a ו־b, אזי קל לראות שהמספרים $a' = \frac{a}{g}$ ו־$b' = \frac{b}{g}$ זרים ומתקיים $\frac{a}{b} = \frac{a'}{b'}$.

דוגמה

$x^2 - 2$ הוא פולינום מתוקן שמקדמיו שלמים. קל להיווכח שאין לו שורשים שלמים, ולכן לפי למה 6.10.1 כל שורש ממשי של פולינום זה הוא אי־רציונלי. כך קיבלנו הוכחה נוספת לכך ש־ $\sqrt{2}$ הוא אי־רציונלי (הוכחה אחרת ראיתם בשאלה 5.3.3). ◄

טענה 6.10.2

יהי $P(x)$ פולינום מתוקן שכל מקדמיו הם מספרים שלמים. אם α הוא שורש שלם של $P(x)$, אז α מחלק את המקדם החופשי של $P(x)$.

הוכחה

נרשום:

$$P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

מאחר ש־ α הוא שורש של $P(x)$, מתקיים:

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

ומכאן:

$$\alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1) = -a_0$$

הביטוי הרשום בסוגריים באגף שמאל הוא מספר שלם. מאחר ש־ α מחלק את אגף שמאל, נובע ש־ α מחלק גם את אגף ימין, ולכן α מחלק גם את a_0.

מ.ש.ל.

דוגמה

נוכיח כי לפולינום

$$P(x) = x^2 + x + 1$$

אין שורשים רציונליים.

$P(x)$ הוא פולינום מתוקן שמקדמיו שלמים, ולכן לפי טענה 6.10.1, כל שורש רציונלי שלו הוא שלם. אבל, לפי טענה 6.10.2, כל שורש שלם של פולינום זה חייב לחלק את המקדם החופשי של $P(x)$ שהוא 1, ולכן המועמדים היחידים לשורשים רציונליים של $P(x)$ הם 1 ו־ -1.

בדיקה ישירה מראה כי אלה אינם שורשים של $P(x)$, ולכן אין ל־ $P(x)$ שורשים רציונליים. ◄

שימו לב, המשפט היסודי של האלגברה מבטיח שלפולינום הנתון $P(x)$ יש שורש **מרוכב** כלשהו - כל שהראינו הוא שאין ל־ $P(x)$ שורש **רציונלי**.

הטענה הבאה מכלילה את טענה 6.10.2. הוכחת הטענה היא בחזקת חומר רשות, ותוכלו לדלג עליה.

טענה 6.10.3

יהי $P(x)$ פולינום שמקדמיו שלמים.[3] אם $\alpha = \frac{r}{s}$ הוא שורש של $P(x)$, כאשר r ו־ s מספרים שלמים שונים מאפס וזרים, אזי r מחלק את המקדם החופשי של $P(x)$ ו־ s מחלק את המקדם העליון של $P(x)$.

הוכחה

נרשום:

$$P(x) = a_n x^n + \cdots + a_0$$

מאחר ש־ α הוא שורש, מתקיים $a_n \alpha^n + \cdots + a_0 = 0$, כלומר:

$$a_n \left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1 \frac{r}{s} + a_0 = 0$$

נכפול שוויון זה ב־ s^n ונקבל:

$$a_n r^n + a_{n-1} s r^{n-1} + \cdots + a_1 s^{n-1} r + a_0 s^n = 0$$

כלומר:

$$r(a_n r^{n-1} + a_{n-1} s r^{n-2} + a_{n-2} s^2 r^{n-3} + \cdots + a_1 s^{n-1}) = -a_0 s^n$$

המספר r מופיע במכפלה המופיעה באגף שמאל, ולכן מחלק את המכפלה $a_0 s^n$ המופיעה באגף ימין. מאחר שהמספרים r ו־ s זרים, נובע מכך ש־ r מחלק את a_0.[4]

על־ידי העברת אגפים, נוכל לכתוב את השוויון האחרון גם כך:

$$-\alpha_n r^n = s(\alpha_{n-1} r^{n-1} + \alpha_{n-2} s r^{n-2} + \cdots + \alpha_1 s^{n-2} r + \alpha_0 s^{n-1})$$

הפעם מופיע המספר s במכפלה (באגף ימין), ולכן מחלק את המכפלה $a_n r^n$. מאחר ש־ r ו־ s זרים, נובע ש־ s מחלק את a_n.

מ.ש.ל.

טענה 6.10.3 נותנת בידינו **מתכון למציאת כל השורשים הרציונליים של פולינום בעל מקדמים רציונליים**:

נניח כי לפנינו פולינום שונה מאפס $Q(x) = a_0 + a_1 x + \ldots + a_m x^m$ בעל מקדמים רציונליים.

א. נסמן ב־ k את האינדקס הקטן ביותר כך ש־ $a_k \neq 0$. אזי 0 הוא שורש של $Q(x)$ אם ורק אם $k > 0$ (שאלה 6.7.7), ונותר למצוא את השורשים הרציונליים השונים מ־ 0 של $Q(x)$. נרשום

3 שימו לב, הפעם איננו מניחים שהפולינום מתוקן.

4 זהו תרגיל שלא תתקשו לפתור בעזרת הכלים שרכשתם בסעיף 5.3.

$Q(x) = x^k(a_k + a_{k+1}x + ... + a_m x^{m-k})$. אזי השורשים השונים מ־ 0 של $Q(x)$ הם בדיוק השורשים של הפולינום $Q_1(x) = a_k + a_{k+1}x + ... + a_m x^{m-k}$.

ב. המקדמים של $Q_1(x)$ הם מספרים רציונליים, ועל־ידי כפל במכנה המשותף נוכל להניח כי כולם מספרים שלמים.[5]

ג. כעת נוכל להפעיל את טענה 6.10.3: כדי למצוא את השורשים של $Q_1(x)$ עלינו לעבור על כל מחלק שלם אפשרי r של המקדם החופשי של $Q_1(x)$ ועל כל מחלק אפשרי s של המקדם העליון של $Q_1(x)$, ולבדוק האם $\alpha = \frac{r}{s}$ הוא שורש של $Q_1(x)$.

דוגמה

נמצא את כל השורשים הרציונליים של $Q(x) = x^3 - \frac{3}{2}x^2 + \frac{1}{2}x$.

המקדם החופשי של $Q(x)$ הוא 0, ולכן 0 הוא שורש של $Q(x)$ ומתקיים $Q(x) = x\left(x^2 - \frac{3}{2}x + \frac{1}{2}\right)$. נותר למצוא את השורשים הרציונליים של $Q_1(x) = x^2 - \frac{3}{2}x + \frac{1}{2}$, או באופן שקול – למצוא את השורשים הרציונליים של $2Q_1(x) = 2x^2 - 3x + 1$. כאן המקדם החופשי הוא 1, ומחלקיו השלמים הם ± 1; המקדם העליון הוא 2, ומחלקיו השלמים הם $\pm 1, \pm 2$. לכן המועמדים היחידים לשורשים הם $\pm 1, \pm\frac{1}{2}$. על־ידי הצבה ישירה תוכלו לוודא שמתוך אלה, רק $\frac{1}{2}$, 1 הם אכן שורשים. מצאנו אם כן, שהשורשים הרציונליים של $Q(x)$ הם $0, 1, \frac{1}{2}$.

▸

שאלה 6.10.1

האם לפולינום $Q(x)$ שבדוגמה יש שורשים ממשיים נוספים, פרט לשורשים הרציונליים שמצאנו?

התשובה בעמוד 150

שאלה 6.10.2

מצאו את כל השורשים הרציונליים של הפולינום $P(x) = 2x^4 - 3x^3 - 3x^2 + 7x - 3$.

התשובה בעמוד 150

דוגמה

נתבונן בפולינום $Q(x) = 3x^4 - 6x^3 + 4x^2 - 10x + 2$. בהתאם למתכון שתואר לעיל, המועמדים היחידים לשורשים רציונליים של הפולינום הם $\pm 1; \pm 2; \pm\frac{1}{3}; \pm\frac{2}{3}$. בדיקה ישירה מעלה כי אף אחד ממספרים אלה אינו שורש של הפולינום – ומכאן שאין לפולינום שורשים רציונליים.

▸

5 אם $c \neq 0$ הוא המכנה המשותף, נחליף את $Q_1(x)$ ב־ $cQ_1(x)$ – השורשים הרציונליים של $Q_1(x)$ הם בבירור השורשים הרציונליים של $cQ_1(x)$.

השיטה שהדגמנו לעיל מאפשרת למצוא את השורשים הרציונליים של פולינום בעל מקדמים רציונליים, אך במקרים מסוימים ניתן להיעזר בה באופן עקיף כדי למצוא גם שורשים לא רציונליים של פולינום.

דוגמה

נתבונן בפולינום $P(x) = 4x^4 - 4x^3 - 7x^2 + 8x - 2$. באמצעות השיטה שתיארנו, תוכלו להיווכח כי השורש הרציונלי היחיד של $P(x)$ הוא $\frac{1}{2}$. מכאן נובע ש־ $P(x)$ מתחלק ב־ $x - \frac{1}{2}$, ומתקיים:

$$P(x) = \left(4x^3 - 2x^2 - 8x + 4\right)\left(x - \frac{1}{2}\right)$$

גם $4x^3 - 2x^2 - 8x + 4$ מתחלק ב־ $x - \frac{1}{2}$, ומתקיים:

$$4x^3 - 2x^2 - 8x + 4 = (4x^2 - 8)\left(x - \frac{1}{2}\right)$$

ולסיכום:

$$p(x) = (4x^2 - 8)\left(x - \frac{1}{2}\right)^2$$

ברור מה הם השורשים של $4x^2 - 8$ - אלה הם המספרים (הלא־רציונליים) $\pm\sqrt{2}$. נסיק מכך שהשורשים של $P(x)$ הם $\frac{1}{2}, \pm\sqrt{2}$. ◄

שאלה 6.10.3

מצאו את כל השורשים של הפולינום $Q(x) = x^4 - 2x^3 - 5x^2 + 4x + 6$.

התשובה בעמוד 150

6.11 הנגזרת

במסגרת הדוגמאות והשאלות בסעיף הקודם, נדרשנו לעיתים תכופות לחשב את ריבויו של שורש של פולינום, ובפרט לבדוק אם שורש נתון של פולינום הוא שורש פשוט. בסעיף זה נתאר בוחן לפשטותו של שורש, המסתמך על מושג הנגזרת.

הגדרה 6.11.1 נגזרת של פולינום

יהי $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in F[x]$ פולינום מעל שדה F. **הנגזרת** של $P(x)$ היא הפולינום $a_1 + 2a_2x + 3a_3x^2 + \ldots + na_nx^{n-1}$.[1] פולינום זה יסומן ב־ $P'(x)$.

אפשר לרשום גם:

$$(a_0 + a_1x + a_2x^2 + \ldots + a_nx^n)' = a_1 + 2a_2x + 3a_3x^2 + \ldots + na_nx^{n-1}$$

הערה

ייתכן שנתקלתם כבר במושג "נגזרת של פונקציה" במסגרת לימודיכם המתמטיים. כאן הגדרנו נגזרת של פולינום (מעל שדה כלשהו) - ונדגיש שוב כי פולינום איננו פונקציה. ישנו קשר הדוק בין שני המושגים, אך לא נרחיב על כך כאן את הדיון, ונעבוד על בסיס הגדרה 6.11.1.

דוגמאות

מעל הממשיים מתקיים:

$$(2 + 3x)' = 3$$
$$(2 + 3x + 5x^2)' = 3 + 10x$$
$$(2 + 3x + 5x^2 + x^3)' = 3 + 10x + 3x^2$$
$$(2)' = 0$$

מעל המרוכבים מתקיים:

$$(2 + ix)' = i$$
$$\left(2 + ix + (i+1)x^2\right)' = i + 2(i+1)x$$

ומעל השדה $\mathbb{Z}_2$ מתקיים:

$$(1 + x + x^2 + x^3)' = 1 + 2x + 3x^2 = 1 + 0x + x^2 = 1 + x^2$$

◀

טענה 6.11.2 נגזרת של סכום פולינומים

יהיו $P(x), Q(x)$ פולינומים. מתקיים השוויון: $\left(P(x) + Q(x)\right)' = P'(x) + Q'(x)$.

---

1 שימו לב, הביטוי 2 המופיע בהגדרת הנגזרת מציין את הסקלר $1+1$ בשדה הנתון F. הביטוי 3 מציין את $1+1+1$, וכן הלאה.

הוכחה

נרשום:

$$P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n\,,\ Q(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m \in F[x]$$

על־ידי הוספת מקדמי אפס, נוכל להניח ש־ $n = m$. מתקיים:

$$\begin{aligned}\left(P(x)+Q(x)\right)' &= P'(x)+Q'(x)=\left((a_0+b_0)+(a_1+b_1)x+\ldots+(a_n+b_n)x^n\right)'\\ &= (a_1+b_1)+2(a_2x+b_2)x+\ldots+n(a_n+b_n)x^{n-1}\\ &= a_1+b_1+2a_2+2b_2x+\ldots+na_nx^{n-1}+nb_nx^{n-1}\\ &= (a_1+2a_2x+\ldots+na_nx^{n-1})+(b_1+2a_2x+\ldots+nb_nx^{n-1})\\ &= P'(x)+Q'(x)\end{aligned}$$

מ.ש.ל.

שאלה 6.11.1

יהיו $P_1(x),\ldots,P_n(x)$ פולינומים מעל שדה מסוים. הוכיחו ש־

$$\left(P_1(x)+\ldots+P_n(x)\right)' = P_1'(x)+\ldots+P_n'(x)$$

התשובה בעמוד 150

טענה 6.11.3

יהי $P(x) \in F[x]$ פולינום ויהי $c \in F$ סקלר. אזי $(cP(x))' = cP'(x) \in F[x]$.

הוכחה

השוויון מתקבל ישירות מן ההגדרה: נרשום $Q(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, ונקבל:

$$\begin{aligned}\left(cP(x)\right)' &= (ca_0+ca_1x+ca_2x^2+\ldots+ca_nx^n)'\\ &= ca_1+2ca_2x+3ca_3x^2+\ldots+nca_nx^{n-1}\\ &= c(a_1+2a_2x+3a_3x^2+\ldots+na_nx^{n-1})\\ &= cP'(x)\end{aligned}$$

מ.ש.ל.

לפני הטענה הבאה, נציג למה שתסייע לנו בהוכחתה:

למה

יהי $Q(x) \in F[x]$ פולינום, ויהי $P(x)$ המונום x^m עבור איזשהו m טבעי. אזי:

$$\left(P(x)Q(x)\right)' = P'(x)Q(x) + P(x)Q'(x)$$

הוכחה

נרשום $Q(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$. אזי:

$$\begin{aligned}\left(x^m(a_0 + a_1x + a_2x^2 + \dots + a_nx^n)\right)' &= \left(a_0x^m + a_1x^{m+1} + a_2x^{m+2} + \dots + a_nx^{m+n}\right)' \\ &= ma_0x^{m-1} + (m+1)a_1x^m + (m+2)a_2x^{m+1} + \dots + (m+n)a_nx^{m+n-1} \\ &= (ma_0x^{m-1} + ma_1x^m + ma_2x^{m+1} + \dots + ma_nx^{m+n-1}) + (a_1x^m + 2a_2x^{m+1} \\ &\qquad + \dots + na_nx^{m+n-1}) \\ &= mx^{m-1}(a_0 + a_1x + a_2x^2 + \dots + a_nx^n) + x^m(a_1 + 2a_2x + \dots + na_nx^{n-1}) \\ &= P'(x)Q(x) + P(x)Q'(x)\end{aligned}$$

מ.ש.ל.

טענה 6.11.4

יהיו $P(x)Q(x)$ פולינומים כלשהם מעל שדה F. אזי:

$$\left(P(x)Q(x)\right)' = P'(x)Q(x) + P(x)Q'(x)$$

הוכחה

נרשום $P(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$. אזי לפי שאלה 6.11.3:

$$\begin{aligned}&\left((a_0 + a_1x + a_2x^2 + \dots + a_nx^n)Q(x)\right)' \\ &= \left(\left(a_0Q(x)\right) + \left((a_1xQ(x)\right) + \left((a_2x^2Q(x)\right) + \dots + \left(a_nx^nQ(x)\right)\right)' \\ &= \left(a_0Q(x)\right)' + \left(a_1xQ(x)\right)' + \left(a_0x^2Q(x)\right)' + \dots + \left(a_nx^n)Q(x)\right)'\end{aligned}$$

לפי טענה 6.11.3, נוכל "להוציא החוצה" את המקדמים ולכתוב ביטוי זה כך:

$$a_0Q'(x) + a_1\left(xQ(x)\right)' + a_2\left(x^2Q(x)\right)' + \dots + a_n\left(x^nQ(x)\right)'$$

ולפי הלמה הקודמת, ביטוי זה שווה ל-

$$\begin{aligned}a_0Q'(x) + a_1xQ'(x) + a_1Q(x) + a_2x^2Q'(x) + 2a_2xQ(x) + \ldots + a_nx^nQ'(x) + na_nx^{n-1}Q(x)\\ = (a_0Q'(x) + a_1xQ'(x) + a_2x^2Q'(x) + \ldots + a_nx^nQ'(x)) + (a_1Q(x) + 2a_2xQ(x)\\ + \ldots + na_nx^{n-1}Q(x))\\ = (a_0 + a_1x + a_2x^2 + \ldots + a_nx^n)Q'(x) + (a_1 + 2a_2x + \ldots + na_nx^{n-1})Q(x)\\ = P(x)Q'(x) + P'(x)Q(x)\end{aligned}$$

מ.ש.ל.

שאלה 6.11.2

יהי k מספר טבעי ויהי α סקלר בשדה F. השתמשו בטענה 6.11.4 כדי להוכיח שהנגזרת של הפולינום $(x-\alpha)^k \in F$ היא $k(x-\alpha)^{k-1}$.

התשובה בעמוד 150

כעת נוכל להוכיח את הבוחן המבוקש:

טענה 6.11.5

יהי $P(x) \in F[x]$ פולינום ויהי $\alpha \in F$ שורש של $P(x)$. אזי α הוא שורש פשוט של $P(x)$ אם ורק אם $P'(\alpha) \neq 0$, כלומר אם ורק אם α אינו שורש של $P'(x)$.

הוכחה

יהי k הריבוי של השורש α, ונרשום $P(x) = (x-\alpha)^k Q(x)$, כאשר α אינו שורש של $Q(x)$. לפי טענה 6.11.4 ושאלה 6.11.2, מתקיים:

$$P'(x) = k(x-\alpha)^{k-1}Q(x) + (x-\alpha)^k Q'(x) = (x-\alpha)^{k-1}\left(kQ(x) + (x-\alpha)Q'(x)\right)$$

אם α הוא שורש פשוט של $P(x)$ אזי $k=1$, $P'(x) = Q(x) + (x-\alpha)Q'(x)$, ולכן:

$$P'(\alpha) = Q(\alpha) + (\alpha-\alpha)Q'(\alpha) = Q(\alpha) + 0 = Q(\alpha) \neq 0$$

בכיוון ההפוך, נניח ש־$P'(\alpha) \neq 0$ ונוכיח כי α הוא שורש פשוט של $P(x)$. אחרת - α הוא שורש מרובה של $P(x)$, כלומר $k \geq 2$, לכן α הוא שורש של $(x-\alpha)^{k-1}$, ולכן α הוא גם שורש של $P'(x) = (x-\alpha)^{k-1}\left(kQ(x) + (x-\alpha)Q'(x)\right)$, וקיבלנו סתירה, כדרוש.

מ.ש.ל.

שאלה 6.11.3

השתמשו בטענה 6.11.5 כדי לבדוק במקרים הבאים האם השורש α של הפולינום הממשי הנתון הוא שורש פשוט:

א. $\alpha = 1,\ P(x) = x^3 - 2x^2 + x$

ב. $\alpha = 0,\ P(x) = x^3 - 2x^2 + x$

ג. $\alpha = -1,\ P(x) = x^3 + x^2 + x + 1$

התשובה בעמוד 151

תשובות לשאלות בפרק 6

תשובה 6.1.1 **השאלה בעמוד 52**

לא! בשדה $\mathbb{Z}_2$ מתקיים $1+1=0$, ואילו ב־$\mathbb{Z}_5$ מתקיים $1+1=2$.

תשובה 6.1.2 **השאלה בעמוד 54**

נניח כי K תת־שדה של $\mathbb{Z}_p$. לפי טענה 6.1.4, $1 \in K$. כל איבר של $\mathbb{Z}_p$ הוא סכום של מספר סופי של 1־ים, ולכן (בזכות הסגירות לחיבור) שייך ל־K.

תשובה 6.1.3 **השאלה בעמוד 55**

נחזור, מילה במילה, על הטיעון שהוביל למשפט 6.1.5: לאור טענה 6.1.4, בהכרח $0,1 \in K$. כמו כן, מכיוון ש־K סגורה לחיבור, כל מספר טבעי n שייך ל־K, שכן נוכל לרשום את n כסכום של 1־ים. יתר על כן, גם הנגדי $-n$ שייך ל־K. נסיק כי כל מספר שלם n שייך ל־K. אבל אז גם ההופכי של כל שלם שונה מאפס שייך ל־K, כלומר $\frac{1}{n} \in K$ לכל $0 \neq n \in \mathbb{Z}$.

כעת נתבונן במספר רציונלי שרירותי $\frac{m}{n} \in \mathbb{Q}$, כאשר $m,n \in \mathbb{Z}$ ו־$n \neq 0$. נוכל לרשום את המספר כך: $\frac{m}{n} = m \cdot \frac{1}{n}$. לאור האמור לעיל, זוהי מכפלה של שני איברים של K, ומכיוון ש־K סגורה לגבי הכפל, $\frac{m}{n} \in K$, ומכאן ש־$\mathbb{Q} \subseteq K$.

תשובה 6.3.1 **השאלה בעמוד 62**

א. $i^3 = i^2 \cdot i = (-1)\cdot i = -i = 0 - i1$

ב. $(2i)\cdot i \cdot 3 = 6i^2 = -6 = -6 + i0$

ג. $2i + 5i = 7i = 0 + i7$

ד. $(2i)^5 = 2^5 \cdot i^5 = 32 \cdot i^2 \cdot i^2 \cdot i = 32i = 0 + i32$

ה. $(\sqrt{2}i)^2 = 2i^2 = -2 = -2 + i0$

תשובה 6.3.2 **השאלה בעמוד 63**

א. $\operatorname{Im} z = -1,\quad \operatorname{Re} z = 0 \quad ; \quad z = -i = 0 + i(-1)$

ב. $\operatorname{Im} z = 0,\quad \operatorname{Re} z = -1 \quad ; \quad z = i^2 = -1 = -1 + i0$

ג. $\operatorname{Im} z = 8,\quad \operatorname{Re} z = 5 \quad ; \quad z = 5 + i8$

ד. $\operatorname{Im} z = -\frac{1}{2},\quad \operatorname{Re} z = -3 \quad ; \quad z = -3 - i\frac{1}{2}$

ה. $\operatorname{Im} z = 0,\quad \operatorname{Re} z = 7 \quad ; \quad z = 7 = 7 + i0$

תשובה 6.3.3 **השאלה בעמוד 63**

א + ג.

$$z_1 = \operatorname{Re} z_1 + i \operatorname{Im} z_1$$

$$z_2 = \operatorname{Re} z_2 + i \operatorname{Im} z_2$$

ולכן

$$z_1 + z_2 = \operatorname{Re} z_1 + \operatorname{Re} z_2 + i(\operatorname{Im} z_1 + \operatorname{Im} z_2)$$

כלומר:

$$\operatorname{Re}(z_1 + z_2) = \operatorname{Re} z_1 + \operatorname{Re} z_2$$

$$\operatorname{Im}(z_1 + z_2) = \operatorname{Im} z_1 + \operatorname{Im} z_2$$

ב+ד.

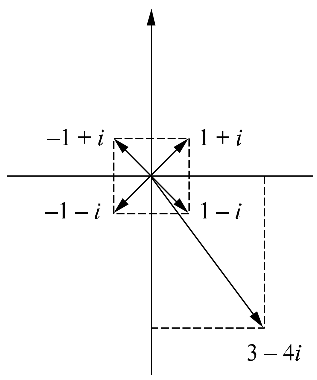
$$\begin{aligned} z_1 \cdot z_2 &= (\operatorname{Re} z_1 + i \operatorname{Im} z_1) \cdot (\operatorname{Re} z_2 + i \operatorname{Im} z_2) \\ &= \operatorname{Re} z_1 \operatorname{Re} z_2 - \operatorname{Im} z_1 \operatorname{Im} z_2 + i(\operatorname{Re} z_1 \operatorname{Im} z_2 + \operatorname{Im} z_1 \operatorname{Re} z_2) \end{aligned}$$

ולכן

$$\operatorname{Re}(z_1 \cdot z_2) = \operatorname{Re} z_1 \operatorname{Re} z_2 - \operatorname{Im} z_1 \operatorname{Im} z_2$$

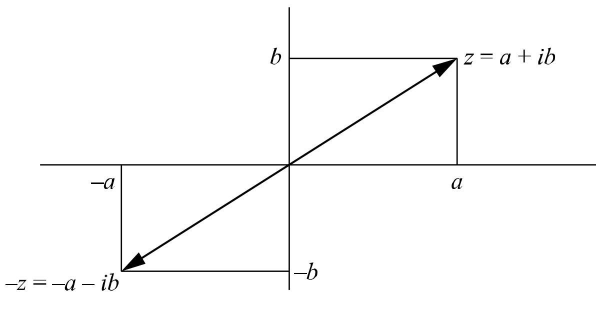
$$\operatorname{Im}(z_1 \cdot z_2) = \operatorname{Re} z_1 \operatorname{Im} z_2 + \operatorname{Im} z_1 \operatorname{Re} z_2$$

תשובה 6.3.4 **השאלה בעמוד 64**



תשובה 6.3.5 **השאלה בעמוד 64**

המספר $-z = -a - ib$ הוא המספר הסימטרי ל־ $z = a + ib$ ביחס לראשית - ראו איור להלן.



תשובה 6.4.1 **השאלה בעמוד 65**

על פי הגדרת המספר הצמוד נקבל:

א. $\overline{-5 + i} = -5 - i$

ב. $\overline{-7i} = \overline{0 - 7i} = 0 + 7i = 7i$

ג. $\overline{-\sqrt{2}} = \overline{-\sqrt{2} + 0i} = -\sqrt{2} - 0i = -\sqrt{2}$

תשובה 6.4.2 **השאלה בעמוד 66**

בתשובה זו נסמן $z=\alpha+i\beta,\ \ z_1=\alpha_1+i\beta_1,\ \ z_2=\alpha_2+i\beta_2$.

א. $\overline{\overline{z}}=\overline{\overline{\alpha+i\beta}}=\overline{\alpha-i\beta}=\alpha+i\beta=z$

ב. $\overline{z_1+z_2}=\overline{(\alpha_1+i\beta_1)+(\alpha_2+i\beta_2)}=\overline{(\alpha_1+\alpha_2)+i(\beta_1+\beta_2)}$

$$=(\alpha_1+\alpha_2)-i(\beta_1+\beta_2)=\alpha_1-i\beta_1+\alpha_2-i\beta_2=\overline{z_1}+\overline{z_2}$$

ג. $\overline{z_1z_2}=\overline{(\alpha_1+i\beta_1)\cdot(\alpha_2+i\beta_2)}=\overline{\alpha_1\alpha_2-\beta_1\beta_2+i(\alpha_1\beta_2+\alpha_2\beta_1)}$

$$=\alpha_1\alpha_2-\beta_1\beta_2-i(\alpha_1\beta_2+\alpha_2\beta_1)=(\alpha_1-i\beta_1)(\alpha_2-i\beta_2)=\overline{z_1}\,\overline{z_2}$$

ד. $z+\overline{z}=(\alpha+i\beta)+\overline{(\alpha+i\beta)}=(\alpha+i\beta)+(\alpha-i\beta)=2\alpha+i0=2\operatorname{Re}z$

ה. $z-\overline{z}=(\alpha+i\beta)-\overline{(\alpha+i\beta)}=(\alpha+i\beta)-(\alpha-i\beta)=2i\beta=2i\operatorname{Im}z$

ו. כזכור, z ממשי אם ורק אם $\beta=0$. כמו כן, השוויון $\alpha+i\beta=\alpha-i\beta$ מתקיים אם ורק אם $\beta=-\beta$, דהיינו אם ורק אם $\beta=0$.

ולכן

$$z=\alpha+i\beta=\alpha-i\beta=\overline{z}$$

אם ורק אם $\beta=0$, דהיינו אם ורק אם z ממשי.

תשובה 6.4.3 **השאלה בעמוד 66**

אם α מספר ממשי אז:[1]

$$\overline{\alpha}=\alpha$$

עתה, מחלק ג של משפט 6.4.2 נקבל כי:

$$\overline{\alpha z}=\overline{\alpha}\,\overline{z}=\alpha\overline{z}$$

תשובה 6.4.4 **השאלה בעמוד 66**

ההפרש, z_1-z_2, אינו אלא הסכום $z_1+(-1)z_2$.

נשים לב ש־ -1 הינו מספר ממשי, ולכן נקבל מחלק ב של משפט 6.4.2 ומהשאלה הקודמת כי:

$$\overline{z_1-z_2}=\overline{z_1+(-1)z_2}=\overline{z_1}+\overline{(-1)z_2}=\overline{z_1}+(-1)\overline{z_2}=\overline{z_1}-\overline{z_2}$$

תשובה 6.4.5 **השאלה בעמוד 66**

א. עבור $n=2$ הטענה כבר הוכחה במשפט 6.4.2.

נניח עתה שהטענה נכונה עבור $n=k$, כלומר נניח שלכל k מספרים מרוכבים $z_1,\dots,z_k$ מתקיים:

$$\overline{z_1+\ldots+z_k}=\overline{z_1}+\ldots+\overline{z_k}$$

1 על פי חלק ו של משפט 6.4.2.

אז עבור $k+1$ מספרים מרוכבים נתונים, $z_1,\ldots,z_{k+1}$, מתקיים:

$$\overline{z_1+\ldots+z_{k+1}} = \overline{(z_1+\ldots+z_k)+z_{k+1}}$$

$$= \overline{z_1+\ldots+z_k} + \overline{z}_{k+1} = \overline{z}_1+\ldots+\overline{z}_k + \overline{z}_{k+1}$$

על פי משפט 6.4.2 חלק ב
על פי הנחת האינדוקציה

כפי שרצינו להוכיח.

ב. עבור $n=2$ הטענה נכונה (משפט 6.4.2, חלק ג).
נניח שעבור $n=k$ מתקיים:

$$\overline{z_1\ldots z_k} = \overline{z}_1\ldots\overline{z}_k$$

אז עבור $n=k+1$:

$$\overline{z_1\ldots z_{k+1}} = \overline{(z_1\ldots z_k)z_{k+1}}$$

$$= \overline{z_1\ldots z_k}\,\overline{z}_{k+1} = \overline{z}_1\ldots\overline{z}_k\overline{z}_{k+1}$$

על פי משפט 6.4.2 חלק ג
על פי הנחת האינדוקציה

כפי שרצינו להוכיח.

תשובה 6.4.6 **השאלה בעמוד 66**

נציב בנוסחה $\overline{z_n\cdot\ldots\cdot z_n} = \overline{z}_n\ldots\overline{z}_n$, שהוכחה בתשובה הקודמת,

$$z_1=z, z_2=z,\ldots,z_n=z$$

ונקבל:

$$\overline{z^n} = \underbrace{\overline{z\cdot\ldots\cdot z}}_{\substack{n\\\text{גורמים}}} = \underbrace{\overline{z}\cdot\ldots\cdot\overline{z}}_{\substack{n\\\text{גורמים}}} = (\overline{z})^n$$

תשובה 6.4.7 **השאלה בעמוד 67**

א. יהי z מספר מרוכב שהוא שורש של המשוואה

$$\alpha x^2+\beta x+\gamma=0$$

אז מתקיים השוויון:

$$\alpha z^2+\beta z+\gamma=0 \qquad (1)$$

עלינו להראות כי גם $\overline{z}$ הוא שורש של אותה המשוואה, כלומר כי מתקיים:

$$\alpha(\overline{z})^2+\beta\overline{z}+\gamma=0 \qquad (2)$$

המספרים המרוכבים $\alpha z^2+\beta z+\gamma$ ו־ 0 שווים (על פי (1)) ולכן שווים גם המספרים הצמודים להם. כלומר, מ־(1) נובע כי:[2]

$$\overline{\alpha z^2+\beta z+\gamma} = \overline{0} = 0 \qquad (3)$$

2 $\overline{0}=0$, שכן 0 הוא מספר ממשי. כמו כן השוויון הימני בשורה הראשונה של (5) מסתמך על שאלה 6.4.6.

אבל על פי משפט 6.4.2:

$$\overline{\alpha z^2 + \beta z + \gamma} = \overline{\alpha z^2} + \overline{\beta z} + \overline{\gamma} \qquad (4)$$

מאחר ש־ α, β ו־ γ הם מספרים ממשיים, נקבל:[3]

$$\begin{cases} \overline{\alpha z^2} = \alpha \overline{z^2} = \alpha \overline{z}^2 \\ \overline{\beta z} = \beta \overline{z} \\ \overline{\gamma} = \gamma \end{cases} \qquad (5)$$

ולכן מ־(3), (4) ו־(5) נקבל כי

$$\overline{\alpha z^2 + \beta z + \gamma} = \alpha(\overline{z})^2 + \beta\overline{z} + \gamma = 0$$

והשוויון האחרון אינו אלא השוויון (2).

הוכחנו, אם כן, כי $\overline{z}$ הוא שורש של המשוואה הריבועית הנתונה.

ב. על פי הנתון:

$$a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0 = 0$$

ולכן גם

$$\overline{a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0} = \overline{0} = 0$$

אבל על פי תכונות הצמוד, נובע מכך כי:[4]

$$a_n(\overline{z})^n + a_{n-1}(\overline{z})^{n-1} + \ldots + a_1\overline{z} + a_0 = 0$$

כלומר, $\overline{z}$ הוא שורש של אותה המשוואה.

תשובה 6.4.8 **השאלה בעמוד 68**

א. $|7 + 2i| = \sqrt{49 + 4} = \sqrt{53}$

ב. $|1 - i| = \sqrt{1^2 + (-1)^2} = \sqrt{2}$

ג. $|-i| = \sqrt{0^2 + (-1)^2} = 1$

ולפי ההערה שלפני השאלה:

ד. $|0| = |0 + 0i| = \sqrt{0^2 + 0^2} = 0$

ה. $\left|-\sqrt{2}\right| = \sqrt{(-\sqrt{2})^2 + 0^2} = \sqrt{2}$

---

3 משפט 6.4.2.

4 זכרו כי $a_0, a_1, \ldots, a_{n-1}, a_0$ הינם מספרים ממשיים.

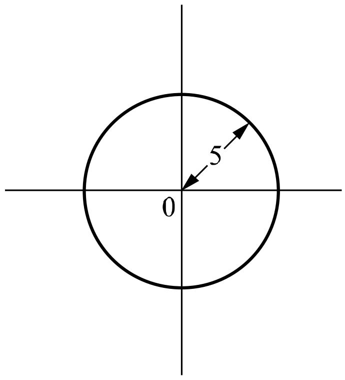
תשובה 6.4.9 **השאלה בעמוד 68**

$$|z| \le 5$$

פירושו של דבר שמרחקה של הנקודה z מן הראשית במישור המרוכב קטן מ־5 או שווה לו. ולכן הקבוצה

$$\{z \,|\, |z| \le 5\}$$

מורכבת מכל הנקודות שבעיגול ברדיוס 5 שמרכזו בראשית (כולל הנקודות על שפת העיגול).



תשובה 6.4.10 **השאלה בעמוד 68**

המרחקים של z ו־ $\bar{z}$ מן הראשית שווים זה לזה. אם נחוג מעגל סביב הראשית שרדיוסו $|z|$, תימצא $\bar{z}$ על המעגל הזה.

תשובה 6.4.11 **השאלה בעמוד 69**

נסמן:

$$z = \alpha + i\beta$$

אז:

$$\operatorname{Re} z = \alpha, \quad \operatorname{Im} z = \beta, \quad |z| = \sqrt{\alpha^2 + \beta^2}$$

א. עלינו להוכיח כי:

$$\alpha \le |\alpha| \le \sqrt{\alpha^2 + \beta^2} \tag{1}$$

ברור שלכל α ממשי מתקיים $\alpha \le |\alpha|$.

נשאר להוכיח כי:

$$|\alpha| \le \sqrt{\alpha^2 + \beta^2} \tag{2}$$

$|\alpha| \ge 0$, ולכן כדי להוכיח את אי־השוויון (2) די שנוכיח כי:[5]

$$\alpha^2 \le \alpha^2 + \beta^2$$

אולם אי־שוויון זה נכון לגבי כל שני מספרים ממשיים α ו־ β, שכן לכל β ממשי, $\beta^2 \ge 0$.

5 העלינו בריבוע את שני האגפים של (2).

ב. עלינו להוכיח כי:

$$\beta \le |\beta| \le \sqrt{\alpha^2 + \beta^2} \qquad (3)$$

האי־שוויון (3) אינו אלא האי־שוויון (1) עצמו, שבו הוחלפו התפקידים של α ו־ β, ולכן נכונותו של (3) נובעת מהסעיף הקודם.

ג. עלינו להוכיח כי לכל α, β ממשיים:

$$\sqrt{\alpha^2 + \beta^2} \le |\alpha| + |\beta| \qquad (4)$$

נעלה בריבוע את שני אגפי האי־שוויון ונקבל שמספיק להוכיח כי:

$$\alpha^2 + \beta^2 \le \alpha^2 + 2|\alpha||\beta| + \beta^2$$

או:

$$0 \le 2|\alpha||\beta|$$

אולם אי־שוויון זה בוודאי נכון, ומכאן שגם האי־שוויון (4) נכון לכל α ו־ β ממשיים.

תשובה 6.4.12 **השאלה בעמוד 70**

נוכיח את חלק א של המשפט הטוען:

לכל z, $|z| \ge 0$; ובנוסף $|z| = 0$ אם ורק אם $z = 0$.

נסמן:

$$z = \alpha + i\beta$$

ואז:

$$|z| = \sqrt{\alpha^2 + \beta^2}$$

כזכור, $\sqrt{x}$ מציין את השורש האי־שלילי של x, ולכן לכל z:

$$|z| \ge 0$$

$|z| = 0$ אם ורק אם $\sqrt{\alpha^2 + \beta^2} = 0$, אבל שוויון אחרון זה מתקיים אם ורק אם $\alpha^2 + \beta^2 = 0$, כלומר אם ורק אם $\alpha = 0$ וגם $\beta = 0$, דהיינו אם ורק אם $z = 0 + i0 = 0$.

נוכיח את חלק ד, הטוען:

$$|z| = |-z|$$

אם

$$z = \alpha + i\beta$$

אז:

$$-z = -\alpha - i\beta$$

ולכן:

$$|-z| = \sqrt{(-\alpha)^2 + (-\beta)^2} = \sqrt{\alpha^2 + \beta^2} = |z|$$

תשובה 6.4.13 **השאלה בעמוד 70**

א. עבור $n = 2$ מתקיים:[6]

$$|z_1 + z_2| \le |z_1| + |z_2|$$

נניח שעבור $n = k$ מתקיים:

$$|z_1 + \ldots + z_k| \le |z_1| + \ldots + |z_k|$$

יהיו עתה $z_1, \ldots, z_{k+1}$, $k + 1$ מספרים מרוכבים כלשהם.[7]

$$|z_1 + \ldots + z_k + z_{k+1}| \le |z_1 + \ldots + z_k| + |z_{k+1}| \le |z_1| + \ldots + |z_k| + |z_{k+1}|$$

ב. ההוכחה אנלוגית לחלוטין להוכחה הקודמת ונשאירה לקורא.

ג. בנוסחה

$$|z_1 \ldots z_n| = |z_1| \ldots |z_n|$$

שאותה נתבקשתם להוכיח ב־ב, נציב

$$z_1 = z_2 = \ldots = z_n = z$$

ונקבל את השוויון הדרוש:

$$|z^n| = |z|^n$$

תשובה 6.4.14 **השאלה בעמוד 72**

נשתמש בנוסחה:

$$z^{-1} = \frac{\bar{z}}{|z|^2}$$

א. $z = i$

$$z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{\bar{i}}{|i|^2} = \frac{\overline{0 + 1 \cdot i}}{1} = 0 - 1 \cdot i = -i$$

ב. $z = 5$

$$z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{\bar{5}}{|5|^2} = \frac{5}{25} = \frac{1}{5}$$

ג. $z = 3 - 4i$

$$z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{\overline{3 - 4 \cdot i}}{\sqrt{3^2 + 4^2}} = \frac{3 + 4 \cdot i}{25} = \frac{3}{25} + \frac{4}{25}i$$

תשובה 6.4.15 **השאלה בעמוד 73**

א. $$\frac{-1 + 3i}{7 + i} = \frac{(-1 + 3i)(7 - i)}{(7 + i)(7 - i)} = \frac{-4 + 22i}{50} = -\frac{4}{50} + \frac{22}{50}i$$

ב. $$\frac{2 - 3i}{1 + 4i} = \frac{(2 - 3i)(1 - 4i)}{(1 + 4i)(1 - 4i)} = \frac{-10 - 11i}{17} = -\frac{10}{17} - \frac{11}{17}i$$

---

6 על פי חלק ג של משפט 6.4.5, אי־שוויון המשולש.

7 שוב על פי חלק ג של משפט 6.4.5.

ג. $\frac{1+i}{\sqrt{2}+i} = \frac{(1+i)(\sqrt{2}-i)}{(\sqrt{2}+i)(\sqrt{2}-i)} = \frac{\sqrt{2}+1+(\sqrt{2}-1)i}{3} = \frac{\sqrt{2}+1}{3} + \frac{\sqrt{2}-1}{3}i$

ד. $\frac{5}{1+2i} = \frac{5(1-2i)}{(1+2i)(1-2i)} = \frac{5-10i}{5} = 1-2i$

ה. $\frac{1}{i} = \frac{-i}{i(-i)} = \frac{-i}{1} = -i$

תשובה 6.4.16 **השאלה בעמוד 73**

א. מאחר ש־

$$z \cdot z^{-1} = 1$$

הרי

$$\overline{z \cdot z^{-1}} = \overline{1} = 1$$

ולכן:

$$\overline{z} \cdot \overline{z^{-1}} = 1$$

משמעות השוויון האחרון היא כי ההופכי של $\overline{z}$ (דהיינו $(\overline{z})^{-1}$) הוא $\overline{z^{-1}}$, כלומר:

$$\overline{z^{-1}} = (\overline{z})^{-1}$$

ב. על פי הגדרת החילוק ובהסתמך על הסעיף הקודם:

$$\overline{\left(\frac{w}{z}\right)} = \overline{w \cdot z^{-1}} = \overline{w} \cdot \overline{z^{-1}} = \overline{w} \cdot (\overline{z})^{-1} = \frac{\overline{w}}{\overline{z}}$$

תשובה 6.4.17 **השאלה בעמוד 73**

א. $z \cdot z^{-1} = 1$

ולכן:

$$|z \cdot z^{-1}| = |1| = 1$$

ומכאן:

$$|z| \cdot |z^{-1}| = 1$$

כלומר, $|z^{-1}|$ הוא ההופכי של $|z|$, דהיינו:

$$|z^{-1}| = |z|^{-1}$$

ב. על פי הסעיף הקודם:

$$\left|\frac{u}{z}\right| = |u \cdot z^{-1}| = |u| \cdot |z^{-1}| = |u| \cdot |z|^{-1} = \frac{|u|}{|z|}$$

תשובה 6.4.18 **השאלה בעמוד 73**

נרשום את מטריצת המקדמים של המערכת ונדרג אותה:

$$\begin{bmatrix} 3 & -i & 5 & 7-2i \\ -1 & 1+i & 2 & -i \\ 1-i & -1 & 1+i & 3-i \end{bmatrix} \xrightarrow{R_2 \to -R_2} \begin{bmatrix} 3 & -i & 5 & 7-2i \\ 1 & -1-i & -2 & i \\ 1-i & -1 & 1+i & 3-i \end{bmatrix} \xrightarrow{R_2 \leftrightarrow R_1}$$

$$\begin{bmatrix} 1 & -1-i & -2 & i \\ 3 & -i & 5 & 7-2i \\ 1-i & -1 & 1+i & 3-i \end{bmatrix} \xrightarrow[R_3 \to R_3-(1-i)R_1]{R_2 \to R_2-3R_1} \begin{bmatrix} 1 & -1-i & -2 & i \\ 0 & 3+2i & 11 & 7-5i \\ 0 & 1 & 3-i & 2-2i \end{bmatrix} \xrightarrow{R_2 \leftrightarrow R_3}$$

$$\begin{bmatrix} 1 & -1-i & -2 & i \\ 0 & 1 & 3-i & 2-2i \\ 0 & 3+2i & 11 & 7-5i \end{bmatrix} \xrightarrow[R_3 \to R_3-(3+2i)R_2]{R_1 \to R_1+(1+i)R_2} \begin{bmatrix} 1 & 0 & 2+2i & 4+i \\ 0 & 0 & 3-i & 7-5i \\ 0 & 1 & -3i & -3-3i \end{bmatrix} \xrightarrow{R_3 \to \frac{-1}{3i}R_3}$$

$$\begin{bmatrix} 1 & 0 & 2+2i & 4+i \\ 0 & 1 & 3-i & 2-2i \\ 0 & 0 & 1 & 1-i \end{bmatrix} \xrightarrow[R_2 \to R_2-(3-i)R_3]{R_1 \to R_1-2(1+i)R_3} \begin{bmatrix} 1 & 0 & 0 & i \\ 0 & 1 & 0 & 2i \\ 0 & 0 & 1 & 1-i \end{bmatrix}$$

כלומר, המערכת הנתונה שקולה למערכת

$$\begin{aligned} x \qquad\qquad &= i \\ y \qquad &= 2i \\ z &= 1-i \end{aligned}$$

ולכן למערכת יש פתרון יחיד והוא השלשה $(i, 2i, 1-i)$.

תשובה 6.4.19 **השאלה בעמוד 74**

$$\begin{vmatrix} 2-i & 3 & i \\ 2i & 1+2i & -1 \\ 1-2i & -i & 1+i \end{vmatrix} \overset{R_3 \to R_3+R_2}{=} \begin{vmatrix} 2-i & 3 & i \\ 2i & 1+2i & -1 \\ 1 & 1+i & i \end{vmatrix} \overset{\substack{R_1 \to R_1-(2-i)R_3 \\ R_2 \to R_2-2iR_3}}{=} \begin{vmatrix} 0 & -i & -1-i \\ 0 & 3 & 1 \\ 1 & 1+i & i \end{vmatrix}$$

נפתח לפי עמודה ראשונה:

$$= 1\begin{vmatrix} -i & -1-i \\ 3 & 1 \end{vmatrix} = -i - 3(-1-i) = 3+2i$$

דטרמיננטת המטריצה אינה אפס, ולכן המטריצה הפיכה.

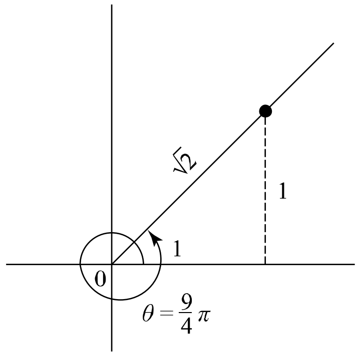
תשובה 6.5.1 **השאלה בעמוד 76**

א. אם $\theta = 0$, אז הנקודה נמצאת על הקרן החיובית של ציר ה־x ומרוחקת מהראשית ב־3 יחידות.

ולכן שיעוריה הקרטזיים הם $(3,0)$ והמספר המרוכב המתאים לה הוא המספר הממשי $z = 3$.

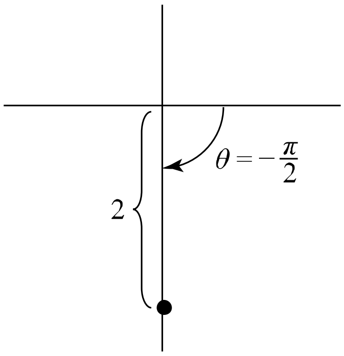
ב. $\theta = \frac{9}{4}\pi = 2\pi + \frac{\pi}{4}$

לכן הנקודה נמצאת על חוצה הזווית של הרביע הראשון ומרחקה מן הראשית הוא $\sqrt{2}$ (ראו איור).



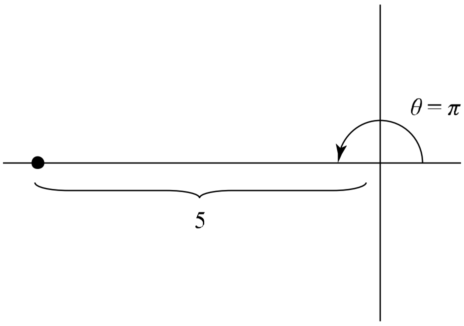
ממשפט פיתגורס נקבל בנקל ששיעוריה הקרטזיים של הנקודה הם $(1,1)$, ומכאן שהמספר המרוכב המתאים לה הוא $z = 1 + i$.

ג. הנקודה מתוארת באיור:



שיעוריה הקרטזיים של הנקודה הם, אם כן, $(0,-2)$, והמספר המרוכב המתאים לה הוא המספר המדומה $z = -2i$.

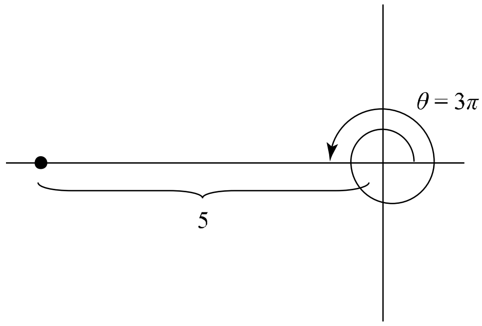
ד. הנקודה מתוארת באיור



שיעוריה הקרטזיים הם $(-5,0)$ והמספר המרוכב המתאים לה הוא המספר הממשי $z = -5$.

ה. $\theta = 3\pi = 2\pi + \pi$

ולכן זוהי אותה הנקודה כמו שב־ד (ראו איור).



ולכן שיעוריה הקרטזיים הם $(-5,0)$.

ו. הזוג $\left(-5,\frac{\pi}{2}\right)$ איננו מתאר שיעורים קוטביים של נקודה במישור, כי לגבי כל זוג שיעורים קוטביים (r,θ) מתקיים $r \geq 0$.

תשובה 6.5.2 **השאלה בעמוד 79**

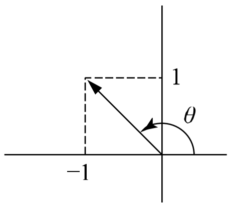
א. למספר המרוכב $z = -1 + i$ מתאימה נקודה ששיעוריה הקרטזיים הם $(-1,1)$, ומכאן:

$$r = |z| = \sqrt{(-1)^2 + 1^2} = \sqrt{2}$$

$$\theta = \frac{3\pi}{4} + 2\pi k$$

ולכן שיעוריה הקוטביים של הנקודה הם:

$$(r,\theta) = \left(\sqrt{2},\ \frac{3\pi}{4} + 2\pi k\right)$$



ב. אם:

$$z = \frac{1}{2} - \frac{\sqrt{3}}{2}i$$

אז:

$$r = |z| = \sqrt{\frac{1}{4} + \frac{3}{4}} = 1$$

וגם:

$$\tan\theta = \left(\frac{-\sqrt{3}}{2}\right) : \left(\frac{1}{2}\right) = -\sqrt{3}$$

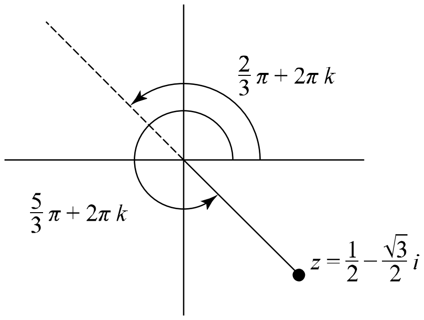
ולפיכך $\theta = \frac{2\pi}{3} + 2\pi k$ או $\theta = \frac{5\pi}{3} + 2\pi k$.

מאחר ש־ z נמצאת ברביע הרביעי (ראו איור להלן), מתקיים:

$$\theta = \frac{5\pi}{3} + 2\pi k$$

ולכן שיעוריה הקרטזיים של הנקודה הם:

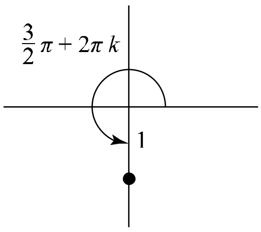
$$(r,\theta) = \left(1,\ \frac{5\pi}{3} + 2\pi k\right)$$



ג. $i^3 = i \cdot i^2 = i(-1) = -i$

ולכן הנקודה i^3 אינה אלא הנקודה $-i$. נקודה זו מתוארת באיור שלהלן, שממנו עולה ששיעוריה הקוטביים הם:

$$(r,\theta) = \left(1,\ \frac{3\pi}{2} + 2\pi k\right)$$



ד. על פי נוסחת כפל מקוצר:

$$(1+i)^3 = 1 + 3i + 3i^2 + i^3 = 1 + 3i - 3 - i = -2 + 2i$$

לפיכך:

$$r = |z| = \sqrt{(-2)^2 + 2^2} = \sqrt{8} = 2\sqrt{2}$$

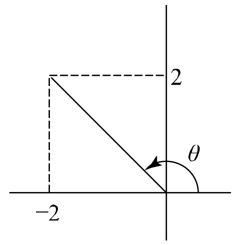
וגם:

$$\tan\theta = -1$$

לכן $\theta = \frac{3\pi}{4} + 2\pi k$ או $\theta = \frac{7\pi}{4} + 2\pi k$.

הנקודה $-2+2i$ נמצאת ברביע השני, ולכן נקבל ששיעוריה הקוטביים הם:

$$(r,\theta)=\left(2\sqrt{2},\ \frac{3\pi}{4}+2\pi k\right)$$



תשובה 6.5.3 **השאלה בעמוד 80**

א. ההצגה

$$z_1=5\left(\cos\frac{\pi}{3}+i\sin\frac{\pi}{6}\right)$$

אינה ההצגה הטריגונומטרית של המספר z_1, כיוון ש־ $\frac{\pi}{6}\neq\frac{\pi}{3}$.

כדי למצוא את ההצגה הטריגונומטרית של המספר z_1 נרשום:[8]

$$z_1=5\left(\frac{1}{2}+\frac{1}{2}i\right)=\frac{5}{2}(1+i)$$

מכאן:

$$r=|z_1|=\frac{5}{2}\sqrt{2}$$

$$\tan\theta=1$$

מאחר ש־ z_1 נמצא ברביע הראשון, נסיק מן השוויון האחרון שהארגומנט θ הוא:[9]

$$\theta=\frac{\pi}{4}$$

ולכן הצגתו הטריגונומטרית של z_1 היא:

$$z_1=\frac{5}{2}\sqrt{2}\left(\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}\right)$$

ב. ההצגה

$$z_2=-2\left(\cos\frac{\pi}{5}+i\sin\frac{\pi}{5}\right)$$

אינה ההצגה הטריגונומטרית של z_2, שכן -2 אינו מספר חיובי.

---

8 $\cos\frac{\pi}{3}=\sin\frac{\pi}{6}=\frac{1}{2}$

9 וגם $\frac{\pi}{4}+2\pi k$

נמצא, אם כן, את ההצגה הטריגונומטרית של z_2:

$$|z_2| = |-2|\left|\cos\frac{\pi}{5} + i\sin\frac{\pi}{5}\right| = 2\sqrt{\cos^2\frac{\pi}{5} + \sin^2\frac{\pi}{5}} = 2$$

$$\tan\theta = \frac{-2\sin\frac{\pi}{5}}{-2\cos\frac{\pi}{5}} = \tan\frac{\pi}{5}$$

מכאן:[10]

$$\theta = \frac{\pi}{5}$$

או:[11]

$$\theta = \frac{\pi}{5} + \pi = \frac{6\pi}{5}$$

מאחר ש־ z_2 נמצא ברביע השלישי, הארגומנט θ הוא:[12]

$$\theta = \frac{6\pi}{5}$$

ולכן הצגתו הטריגונומטרית של z_2 היא:

$$z_2 = 2\left(\cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5}\right)$$

ג. ההצגה

$$z_3 = 7\left(\cos\frac{\pi}{7} - i\sin\frac{\pi}{7}\right)$$

אינה הצגתו הטריגונומטרית של z_3, כיוון שבהצגה זו מופיע סימן **מינוס** בין $\cos$ ו־ $i\sin$.

נמצא את ההצגה הטריגונומטרית של z_3:

$$|z_3| = |7|\left|\cos\frac{\pi}{7} - i\sin\frac{\pi}{7}\right| = 7\sqrt{\cos^2\frac{\pi}{7} + \sin^2\frac{\pi}{7}} = 7$$

$$\tan\theta = \frac{-7\sin\frac{\pi}{7}}{7\cos\frac{\pi}{7}} = -\tan\frac{\pi}{7} = \tan\frac{6}{7}\pi$$

מכאן:[13]

$$\theta = \frac{6\pi}{7}$$

---

10 וגם $\theta = \frac{\pi}{5} + 2\pi k$

11 וגם $\theta = \frac{6\pi}{5} + 2\pi k$

12 שכן שיעוריו הקרטזיים של המספר הם $\left(-2\cos\frac{\pi}{5},\ -2\sin\frac{\pi}{5}\right)$ ושניהם שליליים.

13 וגם $\theta = \frac{6\pi}{7} + 2\pi k$

או:[14]

$$\theta = \frac{13\pi}{7}$$

מאחר ש־ z_3 נמצא ברביע הרביעי, נקבל שהארגומנט של z_3 הוא:

$$\theta = \frac{13\pi}{7}$$

ולכן הצגתו הטריגונומטרית של z_3 היא:

$$z_3 = 7\left(\cos\frac{13\pi}{7} + i\sin\frac{13\pi}{7}\right)$$

תשובה 6.5.4 **השאלה בעמוד 81**

א. לפי האיור, שיעוריה הקוטביים של z_1 הם:

$$(r,\theta) = \left(1, \frac{\pi}{3}\right)$$

ולכן:

$$z_1 = r(\cos\theta + i\sin\theta) = 1\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right) = \frac{1}{2} + i\frac{\sqrt{3}}{2}$$

ב. לפי האיור, שיעוריו הקוטביים של z_2 הם:

$$(r,\theta) = \left(2, -\frac{\pi}{4}\right)$$

ולכן:

$$z_2 = 2\left[\cos\left(-\frac{\pi}{4}\right) + i\sin\left(-\frac{\pi}{4}\right)\right] = 2\left(\frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}\right) = \sqrt{2} - i\sqrt{2}$$

ג. הנקודה z_3 נמצאת על הקרן הנגדית לזו שעליה נמצאת z_2, ולכן הארגומנט של z_3 שווה ל־ $\frac{3\pi}{4}$.
מכאן:

$$z_3 = 3\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right) = 3\left(-\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right)$$

ד. הנקודה z_4 מתארת מספר ממשי שלילי -4.
כלומר:

$$z_4 = -4 = -4 + 0 \cdot i$$

ה. לפי האיור, שיעוריו הקוטביים של z_5 הם:

$$(r,\theta) = \left(5, \frac{7}{6}\pi\right)$$

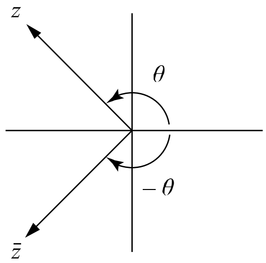
ולכן:

$$z_5 = 5\left(\cos\frac{7}{6}\pi + i\sin\frac{7}{6}\pi\right) = 5\left(-\frac{\sqrt{3}}{2} - \frac{1}{2}i\right) = \frac{-5\sqrt{3}}{2} - \frac{5}{2}i$$

14 וגם $\theta = \frac{13\pi}{7} + 2\pi k$

תשובה 6.5.5 **השאלה בעמוד 82**

א. אם הארגומנט של z הוא θ, אז הארגומנט של הצמוד, $\overline{z}$, הוא $-\theta$ (ראו איור להלן).



כמו כן:

$$|\overline{z}| = |z| = r$$

לכן, אם:

$$z = r(\cos\theta + i\sin\theta)$$

אז:

$$\overline{z} = r(\cos(-\theta) + i\sin(-\theta))$$

ב. נניח כי $z = r(\cos\theta + i\sin\theta)$.

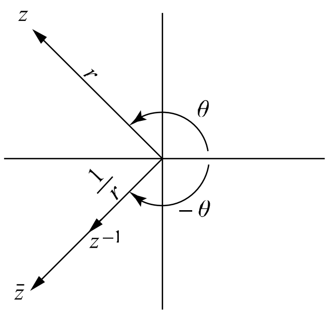
כזכור:[15]

$$|z^{-1}| = |z|^{-1} = \frac{1}{|z|} = \frac{1}{r}$$

כמו כן:[16]

$$z^{-1} = \frac{\overline{z}}{|z|^2}$$

כלומר, z^{-1} הוא כפולה של $\overline{z}$ במספר ממשי, ולכן הנקודה z^{-1} נמצאת על אותה קרן שעליה נמצאת $\overline{z}$ ומכאן שהארגומנט של z^{-1} הוא $-\theta$ (ראו איור).



מכאן:

$$z^{-1} = \frac{1}{r}(\cos(-\theta) + i\sin(-\theta))$$

15 חלק א של שאלה 6.4.17

16 משפט 6.4.6.

ג. על פי הגדרת החילוק:

$$\frac{z_1}{z_2} = z_1 \cdot z_2^{-1}$$

על פי הנתון:

$$z_1 = r_1\left(\cos\theta_1 + i\sin\theta_1\right)$$

ועל פי חלק ב של השאלה:

$$z_2^{-1} = \frac{1}{r_2}\left(\cos(-\theta_2) + i\sin(-\theta_2)\right)$$

ולכן הצגתה הטריגונומטרית של המכפלה $z_1 \cdot z_2^{-1}$ היא:

$$z_1 \cdot z_2^{-1} = \frac{r_1}{r_2}\left(\cos\left(\theta_1 + (-\theta_2)\right) + i\sin\left(\theta_1 + (-\theta_2)\right)\right)$$

או:

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}\left(\cos(\theta_1 - \theta_2) + i\sin(\theta_1 - \theta_2)\right)$$

קיבלנו, אם כן, כי הערך המוחלט של המנה $\frac{z_1}{z_2}$ הוא מנת הערכים המוחלטים של z_1 ו־z_2, ואילו הארגומנט של המנה הוא **הפרש** הארגומנטים של z_1 ו־z_2.

תשובה 6.5.6 **השאלה בעמוד 83**

על פי נוסחת דה־מואבר עבור $n = 3$:

$$(\cos\theta + i\sin\theta)^3 = \cos 3\theta + i\sin 3\theta$$

ועל פי נוסחת כפל מקוצר:

$$(\cos\theta + i\sin\theta)^3 = \cos^3\theta + 3\cos^2\theta \cdot i\sin\theta + 3\cos\theta(i\sin\theta)^2 + (i\sin\theta)^3$$

$$= \cos^3\theta - 3\cos\theta\sin^2\theta + i(3\cos^2\theta\sin\theta - \sin^3\theta)$$

מ־(1) ומ־(2) נקבל כי:

$$\cos 3\theta + i\sin 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta + i(3\cos^2\theta\sin\theta - \sin^3\theta)$$

ומכאן:

$$\cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta$$

$$\cos 3\theta = 3\cos^2\theta\sin\theta - \sin^3\theta$$

תשובה 6.6.1 **השאלה בעמוד 85**

נתבונן בשני מספרים כלשהם מן האוסף הנדון:

$$z_p = \cos\frac{2\pi p}{n} + i\sin\frac{2\pi p}{n}$$

$$z_q = \cos\frac{2\pi q}{n} + i\sin\frac{2\pi q}{n}$$

$(0 \le p < q \le n-1)$.

לו היה

$$z_p = z_q$$

היינו מקבלים ש־ $\frac{2\pi p}{n}$ ו־ $\frac{2\pi q}{n}$ נבדלים בכפולה שלמה של 2π.

אולם:

$$0 < \frac{2\pi q}{n} - \frac{2\pi p}{n} = \frac{2\pi}{n}(q-p) \le \frac{2\pi(n-1)}{n} < 2\pi$$

מסקנה:

$$z_p \ne z_q$$

תשובה 6.6.2 **השאלה בעמוד 86**

כפי שלמדתם בפרק 5, כל מספר שלם k נוכל לחלק (עם שארית) ב־ n ולהציגו בצורה

$$k = pn + q$$

כאשר p ו־ q הם מספרים שלמים וכן $0 \le q < n$. לכן:

$$\frac{2\pi k}{n} = \frac{2\pi(pn+q)}{n} = 2\pi p + \frac{2\pi q}{n}$$

ומכאן:

$$\cos\frac{2\pi k}{n} = \cos\frac{2\pi q}{n}$$

וגם:

$$\sin\frac{2\pi k}{n} = \sin\frac{2\pi q}{n}$$

כלומר

$$\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = \cos\frac{2\pi q}{n} + i\sin\frac{2\pi q}{n} = z_q$$

כאשר $0 \le q \le n-1$.

תשובה 6.6.3 **השאלה בעמוד 87**

א. ארבעת הפתרונות של המשוואה

$$x^4 - 1 = 0$$

הם:

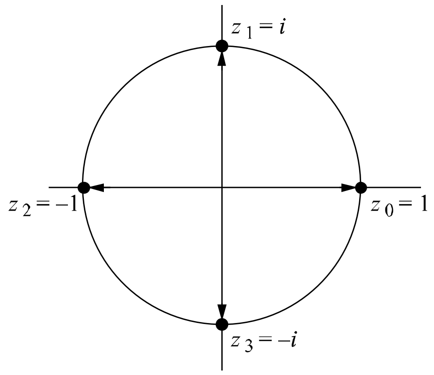
$$z_0 = \cos\left(\frac{2\pi\cdot 0}{4}\right) + i\sin\left(\frac{2\pi\cdot 0}{4}\right) = 1$$

$$z_1 = \cos\frac{2\pi\cdot 1}{4} + i\sin\frac{2\pi\cdot 1}{4} = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = i$$

$$z_2 = \cos\frac{2\pi\cdot 2}{4} + i\sin\frac{2\pi\cdot 2}{4} = \cos\pi + i\sin\pi = -1$$

$$z_3 = \cos\frac{2\pi\cdot 3}{4} + i\sin\frac{2\pi\cdot 3}{4} = \cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2} = -i$$

ותיאורם הגיאומטרי הוא:

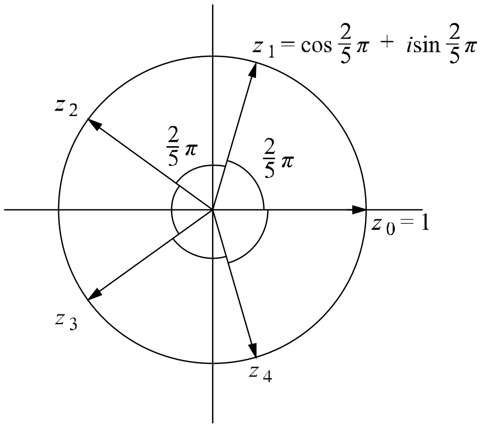


ב. תיאורם הגיאומטרי של חמשת הפתרונות של המשוואה

$$x^5 - 1 = 0$$

הוא:

$$z_1 = \cos\frac{2}{5}\pi + i\sin\frac{2}{5}\pi$$



תשובה 6.6.4 **השאלה בעמוד 88**

א. נרשום את ההצגה הטריגונומטרית של המספר 8:

$$8 = 8(\cos 0 + i\sin 0)$$

לכן כל הפתרונות של המשוואה

$$x^3 = 8$$

הם:

$$z_0 = \sqrt[3]{8}\left(\cos 0 + i\sin 0\right) = 2$$

$$z_1 = \sqrt[3]{8}\left(\cos\frac{2\pi\cdot 1}{3} + i\sin\frac{2\pi\cdot 1}{3}\right) = -1 + i\sqrt{3}$$

$$z_2 = \sqrt[3]{8}\left(\cos\frac{2\pi\cdot 2}{3} + i\sin\frac{2\pi\cdot 2}{3}\right) = -1 - i\sqrt{3}$$

ב. כל הפתרונות של המשוואה

$$x^2 = i = 1\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right)$$

הם:

$$z_0 = 1\left(\cos\frac{\pi/2}{2} + i\sin\frac{\pi/2}{2}\right) = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$$

$$z_1 = 1\left(\cos\frac{\frac{\pi}{2}+2\pi}{2} + i\sin\frac{\frac{\pi}{2}+2\pi}{2}\right) = \cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4} = -\frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}$$

ג. כל הפתרונות של המשוואה

$$x^4 = -1 = 1(\cos\pi + i\sin\pi)$$

הם:

$$z_0 = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$$

$$z_1 = \cos\frac{\pi+2\pi}{4} + i\sin\frac{\pi+2\pi}{4} = -\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}$$

$$z_2 = \cos\frac{\pi+4\pi}{4} + i\sin\frac{\pi+4\pi}{4} = -\frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}$$

$$z_3 = \cos\frac{\pi+6\pi}{4} + i\sin\frac{\pi+6\pi}{4} = \frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}$$

תשובה 6.7.1 **השאלה בעמוד 90**

א. 3

ב. 12

ג. 1

ד. $-\infty$

ה. גם זו הצגה של פולינום האפס, שמעלתו $-\infty$.

ו. 0

ז. 0

תשובה 6.7.2 **השאלה בעמוד 92**

א. $(1+x^3) + (x + 2x + x^3 + 3x^4) = 1 + x + 2x + 2x^3 + 3x^4$
$= 1 + 3x + 2x^3 + 3x^4$

ב. $(1+x^3) + (x - 2x^2 - x^3 + 3x^4) = 1 + x - 2x^2 + 2x^3 + 3x^4$

ג. $(1+x^3) + (-1 - x^3) = 0$

ד. $(1+x^3) + (0) = 1 + x^3$

תשובה 6.7.3 **השאלה בעמוד 94**

על־ידי הצבה בהגדרה 6.7.7 וקיבוץ מונומים בדומה לדוגמאות, נקבל:

א. $(1+x^3)\cdot(x+2x^2+x^3)=x+2x^2+x^3+x^4+2x^5+x^6$

ב. $(1+x)\cdot(2+x)=2+3x+x^2$

ג. $(1+x+x^2+x^3+x^4+x^5+x^6+x^7)\cdot(1-x)=1-x^8$

ד. $(1+x+x^2+x^3+x^4+x^5+x^6+x^7)\cdot 0=0$

תשובה 6.7.4 **השאלה בעמוד 95**

א. מאחר ש $1+x^3$ פירושו $1+1x^3$, המקדם העליון הוא 1, ולכן זהו פולינום מתוקן.

ב. המקדם העליון כאן שונה מ־1, ולכן הפולינום אינו מתוקן.

ג. $(1+x)+(2+x)=3+2x$ ולכן המקדם העליון כאן שונה מ־1, ולכן הפולינום אינו מתוקן.

ד. $(1+x)\cdot(2+x)=2+3x+x^2$ ולכן המקדם העליון הוא 1, ולפנינו פולינום מתוקן.

תשובה 6.7.5 **השאלה בעמוד 96**

א. לפי טענה 6.7.11 מתקיים $-\infty=\deg\big(P(x)Q(x)\big)=\deg\big(P(x)\big)+\deg\big(Q(x)\big)$, ומכך נובע ש־ $\deg\big(Q(x)\big)=-\infty$ או $\deg\big(P(x)\big)=-\infty$, ולכן $P(x)=0$ או $Q(x)=0$.

ב. אם $P(x)Q(x)=P(x)R(x)$, אזי $P(x)\big(Q(x)-R(x)\big)=0$, ולכן לפי חלק א מתקיים $P(x)=0$ או $Q(x)-R(x)=0$. אבל נתון כי $P(x)\neq 0$, ולכן $Q(x)-R(x)=0$, כלומר $Q(x)=R(x)$.

תשובה 6.7.6 **השאלה בעמוד 97**

א. לפי הגדרה 6.7.12:

$$(1+x^3)(0)=1+0^3=1$$

$$(1+x^3)(1)=1+1^3=2$$

$$(1+x^3)(2)=1+2^3=9$$

ב.

$$(1+2x^3)(0)=1$$

$$(1+2x^3)(1)=3$$

$$(1+2x^3)(2)=17$$

ג.

$$(2-x+2x^2)(0)=2$$

$$(2-x+2x^2)(1)=3$$

$$(2-x+2x^2)(2)=8$$

תשובה 6.7.7 **השאלה בעמוד 98**

כפי שהערנו, המקדם החופשי של $P(x)$ הוא $P(0)$, ולכן ערכו הוא אפס אם ורק אם $P(0)=0$.

תשובה 6.7.8 **השאלה בעמוד 98**

לפי חלק ב של טענה 6.7.13 מתקיים $(PQ)(\alpha) = P(\alpha)Q(\alpha)$, ולכן α הוא שורש של $(PQ)(x)$ אם ורק אם $P(\alpha)Q(\alpha) = 0$, כלומר אם ורק אם $P(\alpha) = 0$ או $Q(\alpha) = 0$ (זכרו ש־$P(\alpha)$ ו־$Q(\alpha)$ הם סקלרים).

תשובה 6.8.1 **השאלה בעמוד 104**

א.

$$\begin{array}{r@{\,}l} & \boxed{14} \\ 23\,\big) & 342 \\ & \underline{230} \\ & 112 \\ & \underline{92} \\ & 20 \end{array}$$

המנה היא 14, השארית 20.

ב.

$$\begin{array}{r@{\,}l} & \boxed{12} \\ 82\,\big) & 1024 \\ & \underline{820} \\ & 204 \\ & \underline{164} \\ & 40 \end{array}$$

המנה היא 12, השארית 40.

תשובה 6.8.2 **השאלה בעמוד 105**

א.

$$\begin{array}{r@{\,}l} & \frac{1}{2}x - \frac{1}{4} \\ 2x+1\,\big) & x^2 + 0x + 1 \\ & \underline{x^2 + \frac{1}{2}x} \\ & -\frac{1}{2}x + 1 \\ & \underline{-\frac{1}{2}x - \frac{1}{4}} \\ & \frac{5}{4} \end{array}$$

המנה היא $\frac{1}{2}x - \frac{1}{4}$, השארית $\frac{5}{4}$.

ב.

$$\begin{array}{r}
x^2+x-1 \\
x^2+2\overline{\big)\,x^4+x^3+x^2+0x+3} \\
\underline{x^4\qquad +2x^2\qquad\qquad} \\
x^3-x^2+0x+3 \\
\underline{x^3\qquad +2x\qquad} \\
-x^2-2x+3 \\
\underline{-x^2\qquad -2} \\
-2x+5
\end{array}$$

המנה היא x^2+x-1, השארית $-2x+5$.

תשובה 6.8.3 **השאלה בעמוד 106**

א.

$$\begin{array}{r}
x+1 \\
x-1\overline{\big)\,x^2+0x+i} \\
\underline{x^2-x\qquad} \\
x+i \\
\underline{x-1} \\
i+1
\end{array}$$

המנה היא $x+1$, השארית היא $i+1$ (שימו לב שזהו סקלר - פולינום קבוע).

ב.

$$\begin{array}{r}
x+1 \\
x+1\overline{\big)\,x^2+0x+1} \\
\underline{x^2+x\qquad} \\
x+1 \\
\underline{x+1} \\
0
\end{array}$$

המנה היא $x+1$, השארית היא 0.

תשובה 6.8.4 **השאלה בעמוד 107**

אם $P(x)$ הוא פולינום האפס אזי **כל** סקלר בשדה הוא שורש של הפולינום.

תשובה 6.9.1 **השאלה בעמוד 109**

א. מטענה 6.7.11 נובע באינדוקציה שהמעלה של מכפלת מספר כלשהו של פולינומים היא סכום המעלות, ולכן במקרה זה מעלת הפולינום היא n.

ב. ברור כי כל אחד מן הסקלרים $\alpha_1,\alpha_2,\dots,\alpha_n\in F$ הוא שורש של הפולינום $P(x)$. ברצוננו להראות שאלה **כל** השורשים של $P(x)$. אכן, נניח כי $\beta\in F$ הוא שורש של $P(x)$. אזי מתקיים:

$$(\beta-\alpha_1)\cdot(\beta-\alpha_2)\cdot\ldots\cdot(\beta-\alpha_n)=0$$

זוהי מכפלה של סקלרים בשדה שערכה 0, ולכן אחד מן הגורמים במכפלה הוא עצמו 0. כלומר, קיים $1 \le i \le n$ שעבורו $\beta - \alpha_i = 0$, ולכן $\beta = \alpha_i$.

תשובה 6.9.2 **השאלה בעמוד 110**

א. כפי שציינו בתשובה 6.9.1, המעלה של מכפלת פולינומים היא סכום המעלות, ולכן במקרה זה

$$\deg\left(P(x)^k\right) = k\deg\left(P(x)\right)$$

ב. לפי למה 6.9.2, $\deg\left((x-\alpha)^k\right) = k\deg\left((x-\alpha)\right) = k$.

תשובה 6.9.3 **השאלה בעמוד 111**

א. אם $(x-\alpha)^k$ מחלק את $P(x)$ אז $P(x) = (x-\alpha)^k Q(x)$ עבור פולינום מסוים $Q(x)$, ומתקיים עבור כל $m \le k$:

$$P(x) = (x-\alpha)^k Q(x) = (x-\alpha)^m (x-\alpha)^{k-m} Q(x)$$

ולכן $(x-\alpha)^m$ מחלק את $P(x)$.

ב. ב. $P(x) = (x-\alpha)^k Q(x)$. לפי הגדרת הריבוי, ברור כי הריבוי של α הוא לפחות k. נניח בשלילה שהריבוי גדול מ־k. אזי מתקיים $P(x) = (x-\alpha)^m R(x)$ עבור פולינום מסוים $R(x)$, כאשר $m > k$. מתקיים, אם כן, השוויון:

$$P(x) = (x-\alpha)^m R(x) = (x-\alpha)^k Q(x)$$

ולכן (על־ידי העברת אגפים והוצאת גורם משותף)

$$(x-\alpha)^k \left((x-\alpha)^{m-k} R(x) - Q(x)\right) = 0$$

ונסיק ש־

$$(x-\alpha)^{m-k} R(x) = Q(x)$$

אך משוויון זה נובע ש־α שורש של $Q(x)$, סתירה.

תשובה 6.9.4 **השאלה בעמוד 112**

א. על־ידי חילוק ב־$x-2$ נקבל $P(x) = (x-2)(x+2)$. מאחר ש־2 אינו שורש של $x+2$, הריבוי שלו הוא 1.

ב. כאן נקבל $P(x) = (x+1)^2(x-1) = \left(x-(-1)\right)^2(x-1)$, ולכן הריבוי של -1 הוא 2.

ג. כאן $P(x) = x^3 - 3x^2 + 3x - 1 = (x-1)^3$, ולכן הריבוי של 1 הוא 3.

ד. $P(x) = x^2 + 1 = (x-i)(x+i)$, ולכן הריבוי של i הוא 1.

ה. מעל השדה $\mathbb{Z}_2$ מתקיים $x^2 + 1 = (x+1)^2 = (x-1)^2$, ולכן הריבוי של 1 הוא 2.

תשובה 6.10.1 **השאלה בעמוד 118**

לפי מסקנה 6.8.3, לפולינום ממשי ממעלה 3 יש לכל היותר שלושה שורשים ממשיים שונים. מכיוון שכבר מצאנו שלושה שורשים (רציונליים, ובפרט ממשיים) שונים לפולינום, אין לו שורשים ממשיים נוספים.

תשובה 6.10.2 **השאלה בעמוד 118**

המועמדים האפשריים הם $\pm\frac{1}{2},\pm\frac{3}{2},\pm 1,\pm 3$, ועל־ידי הצבה מגלים שמתוך אלה רק $1,-\frac{3}{2}$ הם שורשים.

תשובה 6.10.3 **השאלה בעמוד 119**

$$Q(x) = x^4 - 2x^3 - 5x^2 + 4x + 6$$

זהו פולינום מתוקן. המועמדים לשורשים רציונליים הם השלמים המחלקים את 6, כלומר $\pm 1,\pm 2,\pm 3,\pm 6$. הצבה מעלה כי מתוך אלה, רק $-1,3$ הם שורשים של הפולינום. יתר על כן, תוכלו לבדוק ששני השורשים הללו הם שורשים פשוטים של הפולינום. על־ידי חילוק הפולינום ב־ $(x+1)(x-3)$ נקבל ש־ $Q(x) = (x+1)(x-3)(x^2-2)$. השורשים של $x^2 - 2$ הם כמובן $\pm\sqrt{2}$, ולכן השורשים של $Q(x)$ הם $-1,3,\pm\sqrt{2}$.

תשובה 6.11.1 **השאלה בעמוד 121**

נוכיח באינדוקציה על n.

עבור $n = 1$ הטענה מתקיימת באופן טריוויאלי, ועבור $n = 2$ הטענה מתקיימת לפי טענה 6.11.2.

נניח עתה שהטענה נכונה עבור n מסוים, ונוכיח ל־ $n+1$:

יהיו $P_1(x)+\ldots+P_n(x)$ פולינומים. לפי הנחת האינדוקציה,

$$\left(P_1(x)+\ldots+P_n(x)\right)' = P_1(x)'+\ldots+P_n(x)'$$

אך לפי המקרה של סכום של שני פולינומים נקבל:

$$\left(\left(P_1(x)+\ldots+P_n(x)\right)+P_{n-1}(x)\right)' = \left(P_1(x)+\ldots+P_n(x)\right)' + P_{n+1}(x)'$$
$$= \left(P_1(x)'+\ldots+P_n(x)'\right)+P_{n-1}(x)' = P_1(x)'+\ldots+P_n(x)'+P_{n+1}(x)'$$

תשובה 6.11.2 **השאלה בעמוד 123**

נוכיח שהנגזרת של הפולינום $F \ni (x-\alpha)^k$ היא $k(x-\alpha)^{k-1}$, באינדוקציה על k.

אם $k = 1$ הטענה מתקיימת, שכן $\left((x-\alpha)^1\right)' = 1$, ו־ $1 = 1(x-\alpha)^0 = k(x-\alpha)^{k-1}$.

נניח שהטענה נכונה עבור k טבעי מסוים, ונוכיח ל־ $k+1$. לפי טענה 6.11.4 ולפי הנחת האינדוקציה, נקבל

$$\left((x-\alpha)^{k+1}\right)' = \left((x-\alpha)^k\cdot(x-\alpha)\right)' = k(x-\alpha)^{k-1}\cdot(x-\alpha)+(x-\alpha)^k\cdot 1$$
$$= k(x-\alpha)^k + (x-\alpha)^k = (k+1)(x-\alpha)^k$$

כדרוש.

תשובה 6.11.3 **השאלה בעמוד 123**

א. $P(x) = x^3 - 2x^2 + x$, $P(1) = 0$, ולכן 1 הוא שורש של $P(x)$.

$P'(x) = 3x^2 - 4x + 1$ ומתקיים $P'(1) = 3 - 4 + 1 = 0$, לכן 1 אינו שורש פשוט של $P(x)$.

ב. $P(x)$ הוא הפולינום שבחלק א, 0 הוא שורש שלו.

כאן מתקיים $P'(0) = 1 \neq 0$, לכן 0 הוא שורש פשוט של $P(x)$.

ג. $P(x) = x^3 + x^2 + x + 1$, -1 הוא שורש שלו.

$P'(x) = 3x^2 + 2x + 1$ ומתקיים $P'(-1) = 3 - 2 + 1 = 2 \neq 0$, לכן -1 הוא שורש פשוט של $P(x)$.

פרק 7: מרחבים ליניאריים

7.1 הגדרת המרחב הלינארי

בפרק 1 חקרנו פעולות כלליות על קבוצות. גילינו דמיון בתכונותיהן של פעולות טבעיות רבות על קבוצות שונות, כגון חילופיות, קיבוציות, קיום איבר ניטרלי, וכן הלאה. מושג המפתח שאותו ביססנו הוא מושג השדה - קבוצה המצוידֶת בזוג פעולות ("חיבור" ו"כפל"), המקיימות שלל תכונות רצויות.

לאחר מכן, בפרק 2, חקרנו את ה"מרחב" F^n - אוסף ה־ n־יות מעל שדה נתון F. גם על אובייקט זה הגדרנו פעולת חיבור (חיבור רכיב רכיב), וראינו כי זו מקיימת את אותן התכונות ה"רצויות" שמקיים החיבור על F עצמו. לא כך הדבר בנוגע לכפל - לא הגדרנו פעולת כפל בין n־יות, אלא "פעולת כפל" מצומצמת יותר - כפל n־יה בסקלר מתוך השדה F, וראינו כי גם ל"פעולה" זו תכונות שימושיות רבות. בפרק זה נבצע שוב תהליך של הכללה - נגדיר מושג כללי של "מרחב לינארי", המורכב מקבוצה שעליה מוגדרות פעולת "חיבור" ו"פעולה" של כפל איבר השייך למרחב בסקלר הלקוח משדה נתון.

שימו לב כי בפרק 1 הגדרנו פעולה על קבוצה נתונה A כהתאמה המקבלת כקלט זוג סדור של איברים של A, ומחזירה כפלט איבר של A. הכפל בסקלר ב־ F^n, וכן במרחב הלינארי הכללי שאותו נגדיר מיד, אינו פעולה במובן זה - הוא מקבל כקלט איבר של המרחב וסקלר מן השדה, ומחזיר כפלט איבר של המרחב. למרות חריגה זו נרשה לעצמנו להשתמש במונח "פעולה" גם עבור התאמה מטיפוס זה. נעיר כי לא קשה להגדיר מושג כללי ורחב יותר של "פעולה", המקבלת כקלט איברים של קבוצות שונות (ואפילו יותר משתי קבוצות), אך לא נעשה זאת במסגרת קורס זה.

נפתח, אם כן, בהגדרת המושג מרחב לינארי.

הגדרה 7.1.1 מרחב לינארי מעל שדה

יהי F שדה. קבוצה V, שעליה מוגדרת פעולת חיבור $+$ בין זוג איברים של V, וכן פעולת כפל בסקלר $\cdot$ בין איבר של V וסקלר מ־ F [1], תיקרא **מרחב לינארי מעל** F [2], אם מתקיימות התכונות הבאות:

תכונות החיבור

א. **סגירות:** לכל $u,v \in V$, $\quad u + v \in V$

ב. **קיבוציות:** לכל $u,v,w \in V$, $\quad (u + v) + w = u + (v + w)$

ג. **חילופיות:** לכל $u,v \in V$, $\quad u + v = v + u$

---

1 כדי להימנע מסרבול מיותר, אנו נרשה לעצמנו להשתמש באותו הסמל $+$ לציון פעולת החיבור ב־ V ולציון פעולת החיבור בשדה F. באופן דומה, נשתמש בסמל $\cdot$ לציון פעולת הכפל בסקלר ולציון הכפל בשדה.

2 שם נרדף למרחב לינארי שנשתמש בו לעיתים הוא **מרחב וקטורי**, ולעיתים אף נקצר ונשתמש במילה **מרחב** בלבד.

ד. קיים ב־ V **איבר ניטרלי** לגבי החיבור, שאותו נסמן ב־ 0.[3] כלומר,
לכל $v \in V$, $\quad v + 0 = v$

ה. לכל $v \in V$ קיים ב־ V איבר, שיסומן $-v$, המקיים:

$$v + (-v) = 0$$

$-v$ מכונה **איבר נגדי** ל־ v.

תכונות הכפל בסקלר

א. **סגירות:** לכל $v \in V$ ולכל $\lambda \in F$,[4] $\quad \lambda \cdot v \in F$

ב. **פילוג הכפל בסקלר מעל החיבור ב־ V:**
לכל $u,v \in V$ ולכל $\lambda \in F$, $\quad \lambda(u + v) = \lambda u + \lambda v$

ג. **פילוג הכפל בסקלר מעל החיבור ב־ F:**
לכל $v \in V$ ולכל $\lambda\mu \in F$, $\quad (\lambda + \mu)v = \lambda v + \mu v$

ד. **קיבוציות:**
לכל $v \in V$ ולכל $\lambda, \mu \in F$, $\quad (\lambda\mu)v = \lambda(\mu v)$

ה. **כפל באיבר היחידה:**
אם 1 הוא איבר היחידה של השדה F, אז לכל $v \in V$, $\quad 1 \cdot v = v$

הערה

לאיברים של מרחב לינארי נקרא **וקטורים**, להבדיל מאיברי השדה שמעליו מוגדר המרחב, שלהם נקרא, כצפוי, **סקלרים**. וקטורים יסומנו בדרך כלל באותיות לטיניות כגון u,v,w, וסקלרים באותיות יווניות כגון λ, μ.

דוגמה א – המרחבים F^n ו־ F

F^n עם פעולות החיבור והכפל בסקלר שהגדרנו בפרק 2, הוא מרחב לינארי מעל F, כפי שתתבקשו להראות בשאלה הבאה. ◀

מכאן שכל שדה F הוא מרחב לינארי מעל עצמו, ובפרט קבוצת המספרים הממשיים $\mathbb{R}$, עם פעולת החיבור הרגיל ופעולת הכפל הרגיל כ"כפל בסקלר", היא מרחב לינארי מעל $\mathbb{R}$ עצמו.

נעיר כאן שבפרק 2 סימנו את איברי F^n באותיות לטיניות זקופות ומודגשות $\mathbf{a}, \mathbf{b}, \mathbf{c}$, ואת הסקלרים, איברי F, באותיות לטיניות s,t. כאשר נעסוק במרחבים כלליים, ניצמד לסימון שעליו הכרזנו בהערה שלפני הדוגמה.

---

3 בהמשך הסעיף נראה שאיבר זה נקבע ביחידות. שימו לב שאנו משתמשים באותו הסמל 0 לציון האיבר הניטרלי לגבי החיבור ב־ V ו ב־ F. בדרך כלל ברור מתוך ההקשר לאיזה איבר ניטרלי אנחנו מתכוונים ואין חשש לבלבול. אם נרצה להבחין בין השניים, נרשום 0_V או 0_F.

4 לרוב נקצר ונכתוב λv במקום $\lambda \cdot v$, תוך השמטת סימן הכפל.

שאלה 7.1.1

הוכיחו את האמור בדוגמה א.

התשובה בעמוד 199

דוגמה ב – שדה הרחבה כמרחב ליניארי

בשאלה הבאה תראו ש־

א. $\mathbb{R}$ הוא מרחב ליניארי מעל שדה המספרים הרציונליים $\mathbb{Q}$, כאשר החיבור הוא החיבור הרגיל ב־ $\mathbb{R}$, והכפל בסקלר (במספר רציונלי) הוא הכפל הרגיל ב־ $\mathbb{R}$.

ב. שדה המספרים המרוכבים $\mathbb{C}$ הוא מרחב ליניארי מעל שדה המספרים הממשיים $\mathbb{R}$, כאשר החיבור הוא החיבור הרגיל ב־ $\mathbb{C}$, והכפל בסקלר (במספר ממשי) הוא הכפל הרגיל ב־ $\mathbb{C}$.

ובאופן כללי:

ג. כל שדה הוא מרחב ליניארי מעל כל תת־שדה שלו. ◄

שאלה 7.1.2

א. הוכיחו את האמור בדוגמה ב.

ב. האם $\mathbb{Q}$ הוא מרחב ליניארי מעל $\mathbb{R}$ ביחס לפעולות החיבור והכפל הרגילות?

ג. (רשות) יהי V מרחב ליניארי כלשהו מעל שדה F, ויהי K תת־שדה של F. הראו ש־ V הוא מרחב ליניארי גם מעל K, ביחס לאותן הפעולות.

התשובה בעמוד 199

דוגמה ג – מרחבי מטריצות

נסמן ב־ $\mathbf{M}^F_{m\times n}$ את קבוצת כל המטריצות מסדר $m\times n$ מעל שדה F,[5] דהיינו את קבוצת כל המטריצות מסדר $m\times n$ שאיבריהן לקוחים מתוך השדה F. בפרק 3 הגדרנו את פעולת החיבור של מטריצות כאלה בעזרת פעולת החיבור בשדה F על־ידי:

$$[a_{ij}]_{m\times n}+[b_{ij}]_{m\times n}\overset{\text{def}}{=}[(a_{ij}+b_{ij})]_{m\times n}$$

(באגף שמאל מציין ה־"$+$" חיבור מטריצות, ובאגף ימין חיבור בשדה F.)

כמו כן הגדרנו את פעולת הכפל בסקלר עבור $\lambda\in F$ ו־ $[a_{ij}]_{m\times n}\in\mathbf{M}^F_{m\times n}$ כך:

$$\lambda[a_{ij}]_{m\times n}\overset{\text{def}}{=}[\lambda a_{ij}]_{m\times n}$$

(הכפל באגף שמאל הוא כפל בסקלר, ובאגף ימין הוא כפל בשדה F.) ◄

שאלה 7.1.3

הוכיחו כי $\mathbf{M}^F_{m\times n}$, עם הפעולות שתוארו לעיל, הוא מרחב ליניארי מעל F.

התשובה בעמוד 199

5 בפרק 3, כאשר הגדרנו אוסף זה, סימנו אותו ב־ $\mathbf{M}^F_{m\times n}(F)$; מעתה נרשה לעצמנו להשתמש בסימון הקומפקטי יותר $\mathbf{M}^F_{m\times n}$.

שאלה 7.1.4

א. האם $\mathbf{M}^{\mathbb{C}}_{m\times n}$, אוסף המטריצות מסדר $m \times n$ מעל שדה המרוכבים $\mathbb{C}$, הוא מרחב לינארי מעל שדה הממשיים $\mathbb{R}$ ביחס לפעולות הרגילות של חיבור מטריצות וכפל מטריצות בסקלר?

ב. האם $\mathbf{M}^{\mathbb{R}}_{m\times n}$ הוא מרחב לינארי מעל $\mathbb{C}$ ביחס לפעולות הרגילות של חיבור מטריצות וכפל בסקלר?

התשובה בעמוד 199

שאלה 7.1.5

בדקו אם קבוצת המטריצות הריבועיות הממשיות מסדר 2, שכל ארבעת איבריהן שונים זה מזה, היא מרחב לינארי מעל $\mathbb{R}$, ביחס לפעולות הרגילות.

התשובה בעמוד 200

שאלה 7.1.6

נסמן ב־ S את קבוצת כל המטריצות הריבועיות האלכסוניות מסדר n, מעל שדה F. נגדיר את פעולות החיבור $+_S$ והכפל בסקלר $\cdot_S$ כך:

לכל $A, B \in S$,

$$A +_S B = AB$$

לכל $\lambda \in F, A \in S$,

$$A \cdot_S A = \lambda A$$

כלומר, ה"חיבור" מוגדר כפעולת ה**כפל** של מטריצות ב־ $\mathbf{M}^{F}_{n\times n}$, והכפל בסקלר מוגדר כפעולת הכפל בסקלר הרגילה ב־ $\mathbf{M}^{F}_{n\times n}$. האם עם הפעולות האלה S היא מרחב לינארי מעל F?

התשובה בעמוד 200

דוגמה ד – מרחב הפתרונות של מערכת לינארית הומוגנית

תהי

$$\begin{array}{ccccccc} a_{11}x_1 & + & \dots & + & a_{1n}x_n & = & 0 \\ \vdots & & & & \vdots & & \\ a_{m1}x_1 & + & \dots & + & a_{mn}x_n & = & 0 \end{array}$$

מערכת לינארית הומוגנית של m משוואות ב־ n משתנים מעל שדה כלשהו F.

נסמן ב־ T את אוסף כל הפתרונות, $(c_1,\dots,c_n) \in F^n$, של מערכת זו.

שאלה 7.1.7

הוכיחו כי T הוא מרחב לינארי מעל F, ביחס לחיבור הרגיל ולכפל בסקלר הרגיל ב־ F^n.

התשובה בעמוד 201

▶

שאלה 7.1.8

תהי

$$\begin{array}{ccccccc} a_{11}x_1 & + & \dots & + & a_{1n}x_n & = & b_1 \\ \vdots & & & & \vdots & & \\ a_{m1}x_1 & + & \dots & + & a_{mn}x_n & = & b_m \end{array}$$

מערכת ליניארית **אי־הומוגנית** מעל $\mathbb{R}$.

הוכיחו כי קבוצת פתרונותיה אינה מרחב ליניארי מעל $\mathbb{R}$ (ביחס לחיבור ולכפל בסקלר הרגילים ב־ $\mathbb{R}^n$).

התשובה בעמוד 201

דוגמה ה – מרחב הפולינומים מעל שדה

יהי F שדה כלשהו. נזכירכם כי את קבוצת כל הפולינומים מעל F סימנו ב־ $F[x]$. בפרק 6 הגדרנו חיבור וכפל בין פולינומים, ומכך נובע בפרט שהגדרנו כפל של פולינום בסקלר, שכן נראה את הסקלר כפולינום קבוע (ראו הערה ב בעקבות סימון 6.7.4). כמו כן נזכירכם, כי את אוסף כל הפולינומים מעל F שמעלתם קטנה ממספר טבעי נתון n סימנו ב־ $F_n[x]$. תוכלו להשתכנע בקלות, על סמך התכונות שהוכחנו בסעיף 6.7, כי $F[x]$ ו־ $F_n[x]$ שניהם מרחבים ליניאריים מעל F ביחס לפעולות הנזכרות. ◀

שאלה 7.1.9

בדקו אם אוסף הפולינומים ממעלה 4 **בדיוק**, שמקדמיהם ממשיים, הוא מרחב ליניארי מעל שדה הממשיים ביחס לפעולות הנזכרות.

התשובה בעמוד 201

שאלה 7.1.10

א. בדקו אם אוסף הפולינומים שמקדמיהם **שלמים**, הוא מרחב ליניארי מעל $\mathbb{R}$ ביחס לאותן הפעולות.

ב. האם $\mathbb{C}[x]$ (אוסף הפולינומים שמקדמיהם מרוכבים) הוא מרחב ליניארי מעל $\mathbb{R}$ ביחס לאותן הפעולות?

ג. האם $\mathbb{R}[x]$ (הפולינומים עם מקדמים ממשיים) הוא מרחב ליניארי מעל $\mathbb{C}$ ביחס לאותן הפעולות?

התשובה בעמוד 201

שאלה 7.1.11

הקבוצה K נתונה על־ידי:

$$K = \{P(x) \in \mathbb{R}[x] \mid P(1) = 0\}$$

האם K הוא מרחב ליניארי מעל $\mathbb{R}$ ביחס לפעולות הרגילות?

התשובה בעמוד 202

הדוגמאות שניתנו עד כה ממחישות בעליל את האופי הכללי של המושג "מרחב לינארי". על מנת להבליט כלליות זו עוד יותר, הנה דוגמה נוספת, מפתיעה במקצת.

דוגמה ו – מרחב הפונקציות הממשיות

נתבונן באוסף כל הפונקציות $f : \mathbb{R} \to \mathbb{R}$.

עבור שתי פונקציות, $f : \mathbb{R} \to \mathbb{R}$, $g : \mathbb{R} \to \mathbb{R}$, **הסכום** $f+g$ הוא הפונקציה מ־ $\mathbb{R}$ ל־ $\mathbb{R}$, שערכה עבור x ממשי נתון על־ידי:

$$(f+g)(x) \overset{\text{def}}{=} f(x) + g(x)$$

המכפלה של פונקציה $f : \mathbb{R} \to \mathbb{R}$ בסקלר $\lambda \in \mathbb{R}$ היא הפונקציה מ־ $\mathbb{R}$ ל־ $\mathbb{R}$, שערכה עבור x ממשי כלשהו נתון על־ידי:

$$(\lambda f)(x) \overset{\text{def}}{=} \lambda \cdot f(x)$$

שאלה 7.1.12

הוכיחו שהקבוצה

$$\{f \mid f : \mathbb{R} \to \mathbb{R}\}$$

של כל הפונקציות הממשיות היא מרחב לינארי מעל $\mathbb{R}$ ביחס לפעולות שתוארו לעיל.

התשובה בעמוד 202

דוגמה ז – מרחב הסדרות הממשיות

נסמן ב־ $\mathbb{R}^{\mathbb{N}}$ את אוסף כל **הסדרות האינסופיות** של מספרים ממשיים. סדרה באוסף היא מעין וקטור אינסופי, $(a_1, a_2, a_3, \ldots)$, שכל רכיביו הם מספרים ממשיים. נסמן סדרה כזאת בקצרה על־ידי $(a_k)_{k\in\mathbb{N}}$. כך למשל, $(k+1)_{k\in\mathbb{N}}$ הוא סימון מקוצר עבור הסדרה $(2,3,4,5,\ldots)$. לעיתים נקצר עוד יותר, ובמקום $(a_k)_{k\in\mathbb{N}}$ נכתוב פשוט (a_k).

הסכום $(a_k + b_k)$ של שתי סדרות אינסופיות (a_k) ו־ (b_k) מוגדר על־ידי:

$$(a_k) + (b_k) \overset{\text{def}}{=} (a_k + b_k)$$

והמכפלה $\lambda(a_k)$ $(\lambda \in \mathbb{R})$ מוגדרת על־ידי:

$$\lambda(a_k) \overset{\text{def}}{=} (\lambda a)_k$$

שאלה 7.1.13

הוכיחו כי $\mathbb{R}^{\mathbb{N}}$ עם הפעולות שתוארו לעיל, הוא מרחב לינארי מעל $\mathbb{R}$.

התשובה בעמוד 204

7.2 תכונות בסיסיות של מרחבים ליניאריים

התכונות הבסיסיות שנמנה בסעיף זה נובעות במישרין מתכונות החיבור והכפל בסקלר שבהגדרת המרחב הליניארי. מבין התכונות הללו, אלה שמבוססות רק על תכונות החיבור, לא זו בלבד שהן מתקיימות בכל מרחב ליניארי, אלא גם בכל שדה, שהרי אקסיומות החיבור במרחב ליניארי זהות לאקסיומות החיבור בשדה. אין אפוא תימה בעובדה שאת מרבית התכונות הנזכרות כאן פגשנו כבר בסעיף העוסק בשדות בפרק 1 (סעיף 1.2), ושההוכחות כאן זהות לאלה שניתנו שם. נחזור כאן על ההוכחות כדי לחסוך לקוראינו עבודת דפדוף מיותרת. עם זאת, אנו ממליצים בפני הסטודנטים החרוצים לנסות כוחם בהוכחות אלה לפני קריאת ההוכחות הכתובות.

נפתח בתכונת הקיבוציות המוכללת (למרות שזוהי התכונה היחידה שאין בכוונתנו להוכיח), אך תחילה נדגים.

שאלה 7.2.1

יהיו v_1, v_2, v_3, v_4, v_5 חמישה וקטורים במרחב ליניארי V.

הוכיחו כי:

א. $v_1 + \left(v_2 + (v_3 + v_4)\right) = \left((v_1 + v_2) + v_3\right) + v_4$

ב. $\left(\left((v_1 + v_2) + v_3\right) + v_4\right) + v_5 = v_1 + \left(v_2 + \left(v_3 + (v_4 + v_5)\right)\right)$

התשובה בעמוד 205

פעולת החיבור במרחב ליניארי מתאימה לכל זוג סדור של וקטורים, וקטור חדש, שהוא סכומם. בהינתן n וקטורים $(n \geq 2)$, נוכל, על־ידי הכנסת סוגריים, לחבר את כל n הוקטורים, כשכל אחת מ־ $(n-1)$ פעולות החיבור מתבצעת, כמובן, בין שני וקטורים. את הסוגריים אפשר להכניס באופנים שונים (כמו בשאלה 7.2.1, למשל), אלא שבכל פעם תתקבל אותה תוצאה. תכונה זו נקראת **תכונת הקיבוציות המוכללת**, ואפשר להוכיח באינדוקציה על n בהסתמך על תכונת הקיבוציות בלבד. לא נביא כאן את ההוכחה, כי היא מייגעת בפרטיה למרות שהיא פשוטה בכללותה.

בשל תכונת הקיבוציות המוכללת נוכל לרשום את הסכום של n וקטורים, $v_1, \ldots, v_n$, פשוט בצורה

$$v_1 + v_2 + \ldots + v_n$$

בלי לציין כלל את מקומם של הסוגריים. מובן שהסכום של n וקטורים מתוך מרחב ליניארי V הוא עצמו וקטור ב־ V.

שאלה 7.2.2

יהיו v_1, v_2, v_3, v_4 ארבעה וקטורים במרחב ליניארי.

א. הוכיחו כי

$$v_1 + v_2 + v_3 + v_4 = v_1 + v_3 + v_4 + v_2 \qquad (*)$$

וציינו על אילו מתכונות המרחב הליניארי הסתמכתם בתשובתכם.

ב. האם השוויון (*) נכון גם כאשר v_i $(1 \le i \le 4)$ הם איברים בשדה F ו־"$+$" הוא החיבור בשדה F?

התשובה בעמוד 206

התכונות שבמשפט הבא הן הכללות של תכונות "הפילוג".

משפט 7.2.1

יהי V מרחב לינארי מעל שדה F.

א. לכל $v \in V$ ו־ $\lambda_1,\dots,\lambda_n \in F$:

$$(\lambda_1 + \dots + \lambda_n)v = \lambda_1 v + \dots + \lambda_n v$$

ב. לכל $v_1,\dots,v_n \in V$ ו־ $\lambda \in F$:

$$\lambda(v_1 + \dots + v_n) = \lambda v_1 + \dots + \lambda v_n$$

שאלה 7.2.3

הוכיחו את המשפט (באינדוקציה על n).

התשובה בעמוד 206

משפט 7.2.2

יהי V מרחב לינארי (מעל שדה F).

א. ב־ V יש איבר ניטרלי **יחיד** (לגבי החיבור).

ב. לכל איבר ב־ V יש איבר נגדי **יחיד** (לגבי החיבור).

הוכחה

את יחידותו של האיבר הניטרלי של קבוצה ביחס לפעולה נתונה, הוכחנו באופן כללי בפרק 1 (מסקנה 1.1.7), ובפרט מתקיימת היחידות עבור פעולת החיבור במרחבים לינאריים.

את הוכחת יחידות האיבר הנגדי השלימו בעצמכם (תוכלו להיעזר בהוכחה דומה של יחידות האיבר הנגדי בשדה - טענה 1.2.2 בפרק 1).

מ.ש.ל.

משפט 7.2.3

יהי V מרחב לינארי מעל שדה F.

א. אם וקטור $v \in V$ מקיים $v + v = v$, אז בהכרח $v = 0$.

ב. לכל $\lambda \in F$, $\lambda 0 = 0$.

ג. לכל $v \in V$, $0v = 0$.

ד. $\lambda v = 0$ אם ורק אם $\lambda = 0$ או $v = 0$.

ה. לכל $v \in V$, $(-1)v = -v$.

הוכחה

א. נניח כי $v \in V$ מקיים $v + v = v$.

נוסיף לשני אגפי השוויון את הווקטור הנגדי, $(-v)$, ונקבל:

$$(v+v)+(-v)=v+(-v)$$

כלומר

$$(v+v)+(-v)=0$$

ולכן:

$$v+\big(v+(-v)\big)=0$$

כלומר

$$v+0=0$$

או

$$v=0$$

כפי שרצינו להוכיח.

ב. וקטור האפס, 0, מקיים

$$0=0+0$$

ולכן לכל $\lambda \in F$:

$$\lambda 0=\lambda(0+0)\underset{\text{פילוג}}{=}\lambda 0+\lambda 0$$

הווקטור $\lambda 0$ הוא, אם כן, בעל התכונה שסכומו עם עצמו שווה לעצמו.

על פי חלק א של המשפט, נובע מכך כי:

$$\lambda 0=0$$

ג. איבר האפס בשדה F מקיים

$$0+0=0$$

ולכן לכל $v \in V$,

$$(0+0)v=0v$$

כלומר

$$0v+0v=0v$$

ולכן על פי הטענה שבחלק א:

$$0v=0$$

ד. אם $\lambda = 0$ או $v = 0$, אז $\lambda v = 0$, על סמך הטענות שבחלקים ב ו־ג במשפט זה.

בכך הוכח כיוון אחד של הטענה שבחלק ג.

להוכחת הכיוון ההפוך נניח כי $\lambda v = 0$.

אם $\lambda = 0$, אין מה להוכיח. נניח אפוא כי $\lambda \neq 0$.

נכפול את שני אגפי השוויון $\lambda v = 0$ ב־λ^{-1} (λ^{-1} הוא האיבר ההופכי ל־λ בשדה F), ונקבל:

(1) $$\lambda^{-1}(\lambda v)=\lambda^{-1}0$$

אבל, על פי חלק ב,

(2) $$\lambda^{-1}0=0$$

וכמו כן, על פי תכונות הכפל בסקלר:

$$\lambda^{-1}(\lambda v) = (\lambda^{-1}\lambda)v = 1v = v \qquad (3)$$

מהצבת התוצאות (2) ו־(3) ב־(1) נקבל

$$v = 0$$

כפי שרצינו להוכיח.

ה. על פי חלק ג, לכל $v \in V$:

$$0v = 0$$

כמו כן, מתקיים בשדה F

$$1 + (-1) = 0$$

ולכן לכל $v \in V$:

$$\big(1 + (-1)\big)v = 0$$

אבל מתכונות הכפל בסקלר נובע כי

$$\big(1 + (-1)\big)v = 1v + (-1)v = v + (-1)v$$

ולכן קיבלנו כי לכל $v \in V$,

$$v + (-1)v = 0$$

הווי אומר, $(-1)v$ הוא וקטור נגדי ל־ v.
מיחידות הוקטור הנגדי נובע כי $(-1)v$ הוא הוקטור הנגדי ל־ v, כלומר:

$$(-1)v = -v$$

מ.ש.ל.

שאלה 7.2.4

הוכיחו כי לכל $\lambda \in F$ ולכל $v \in V$:

$$(-\lambda)v = \lambda(-v) = -(\lambda v)$$

התשובה בעמוד 206

משפט 7.2.4

יהי V מרחב לינארי מעל שדה F, ויהיו $u, v \in V$. אז:

א. $-(-v) = v$

ב. $-(u + v) = (-u) + (-v)$

שאלה 7.2.5

הוכיחו את משפט 7.2.4.

(להוכחת חלק ב חשבו את $\big((-u) + (-v)\big) + (u + v)$.)

התשובה בעמוד 207

הגדרה 7.2.5

יהי V מרחב ליניארי ויהיו $u,v \in V$ וקטורים כלשהם. **ההפרש** $u - v$ מוגדר על־ידי

$$u - v \overset{\text{def}}{=} u + (-v)$$

שאלה 7.2.6

יהי V מרחב ליניארי מעל שדה F ויהיו $u,v,w \in V$.

הוכיחו כי:

א. $u - (v + w) = (u - v) - w$

ב. $u - (v - w) = (u - v) + w$

ג. $u - v = 0 \Leftrightarrow u = v$

התשובה בעמוד 207

7.3 תת־מרחבים

חלק מן המרחבים הלינאריים שתוארו בסעיף 7.1, היו תת־קבוצות של מרחבים גדולים יותר.

דוגמאות

א. קבוצת הפתרונות של מערכת לינארית הומוגנית מעל שדה F, היא מרחב לינארי (מעל F), והיא קבוצה חלקית של המרחב הלינארי F^n (מעל F).

ב. קבוצת הפולינומים $F_n[x]$ - אוסף כל הפולינומים מעל $\mathbf{Sp}(K \cup T)$ ממעלה קטנה ממספר טבעי נתון n, היא תת־קבוצה של $F[x]$ - מרחב הפולינומים מעל F, והיא עצמה מרחב לינארי.

ג. קבוצת כל הפולינומים הממשיים המתאפסים עבור $x = 1$, אף היא מרחב לינארי (ראו שאלה 7.1.11).

▸

הגדרה 7.3.1

תת־קבוצה W של מרחב לינארי V מעל שדה F נקראת **תת־מרחב של** V, אם W עצמה היא מרחב לינארי מעל F לגבי פעולות החיבור והכפל בסקלר של המרחב V.

הדוגמאות א–ג דלעיל הן דוגמאות של תת־מרחבים (ודאו זאת לעצמכם).

שאלה 7.3.1

יהי V מרחב לינארי מעל שדה F ויהי U תת־מרחב של V.

א. הוכיחו כי 0, האיבר הניטרלי לגבי החיבור ב־ V, שייך ל־ U, והוא האיבר הניטרלי ביחס לחיבור ב־ U.

ב. הוכיחו שלכל איבר v ב־ U, $-v$, האיבר הנגדי ל־ v ב־ V, שייך ל־ U, והוא האיבר הנגדי ל־ v ב־ U.

התשובה בעמוד 208

במהלך פתרון חלק מהשאלות בסעיף 7.1 נוכחתם לדעת כי חלק מן התכונות של מרחב לינארי מתקיימות ב**כל תת־קבוצה** של מרחב לינארי. אם תעקבו אחר רשימת התכונות שבהגדרת המרחב הלינארי תמצאו שכדי לוודא ש**תת־קבוצה** W של מרחב לינארי V, היא עצמה מרחב לינארי, אין צורך לאמת מחדש את קיומן של **כל** הדרישות, כי רובן מתקיימות ממילא בכל תת־קבוצה. די לוודא כי W סגורה ביחס לפעולות החיבור והכפל בסקלר, כי וקטור האפס של V שייך גם ל־ W, וכי לכל וקטור v ב־ W, גם הנגדי לו $(-v)$ שייך ל־ W. הווי אומר, כדי לוודא שתת־קבוצה W של מרחב לינארי V היא תת־מרחב של V, יש לוודא כי:

1. אם $w_1, w_2 \in W$ אז $w_1 + w_2 \in W$
2. אם $w \in W$, $\lambda \in W$, אז $\lambda w \in W$
3. $0 \in W$

4. אם $w \in W$, אז גם $-w \in W$

האם הכרחי לאמת את קיומם של כל ארבעת התנאים הללו?

שאלה 7.3.2

א. הוכיחו כי התנאי (4) נובע מ־(2).

ב. האם גם התנאי (3) נובע מ־(2)?

התשובה בעמוד 208

מתשובה 7.3.2 נוכל להסיק שקבוצה חלקית **לא ריקה** W, של מרחב ליניארי V, מקיימת את התכונות (3) ו־(4) כל אימת שמתקיימת התכונה (2). נוכל, אם כן, לסכם את הדיון בניסוח הבוחן הבא:

משפט 7.3.2

תהי W תת־קבוצה של מרחב ליניארי V מעל שדה F.

אזי W היא תת־מרחב של V אם ורק אם:

א. $W \neq \phi$

ב. לכל $w_1, w_2 \in W$ גם $w_1 + w_2 \in W$

ג. לכל $w \in W$ ו־$\lambda \in W$ גם $\lambda w \in W$

ניתן לאחד את התנאים ב ו־ג שבמשפט 7.3.2 לתנאי אחד:

משפט 7.3.2′

תהי W תת־קבוצה של מרחב ליניארי V מעל שדה F.

אזי W היא תת־מרחב של V אם ורק אם:

א. $W \neq \phi$

ב. לכל $w_1, w_2 \in W$ ולכל זוג סקלרים $\lambda_1, \lambda_2 \in W$,

$$\lambda_1 w_1 + \lambda_2 w_2 \in W$$

שאלה 7.3.3

הוכיחו את משפט 7.3.2′.

התשובה בעמוד 208

שאלה 7.3.4

א. הוכיחו כי הקבוצה

$$W = \left\{(a_1, \ldots, a_n) \in \mathbb{R}^n \middle| a_1 = 0\right\}$$

היא תת־מרחב של $\mathbb{R}^n$.

ב. הוכיחו כי קבוצת הווקטורים ב־ $\mathbb{R}^n$ שסכום רכיביהם הוא 0, דהיינו הקבוצה

$$W_0 = \left\{ (a_1, \ldots, a_n) \in \mathbb{R}^n \,\middle|\, \sum_{i=1}^{n} a_i = 0 \right\}$$

היא תת־מרחב של $\mathbb{R}^n$.

ג. יהי $\mathbf{a}$ וקטור נתון כלשהו ב־ $\mathbb{R}^3$.[1] הוכיחו כי הקבוצה

$$W_1 = \left\{ \lambda \mathbf{a} \,\middle|\, \lambda \in \mathbb{R} \right\}$$

היא תת־מרחב של $\mathbb{R}^3$.

מהו התיאור הגיאומטרי של קבוצת איברי תת־מרחב זה?

ד. יהיו $\mathbf{a}, \mathbf{b}$ שני וקטורים כלשהם ב־ $\mathbb{R}^3$. הוכיחו כי קבוצת הצירופים הלינאריים של $\mathbf{a}$ ו־ $\mathbf{b}$, דהיינו הקבוצה

$$W_2 = \left\{ \lambda \mathbf{a} + \mu \mathbf{b} \,\middle|\, \lambda, \mu \in \mathbb{R} \right\}$$

היא תת־מרחב של $\mathbb{R}^3$.

מהו התיאור הגיאומטרי של תת־מרחב זה?

התשובה בעמוד 209

שאלה 7.3.5

א. קבעו אילו מן הישרים ב־ $\mathbb{R}^2$ הם תת־מרחבים של $\mathbb{R}^2$.

ב. קבעו אילו מן הישרים ב־ $\mathbb{R}^3$ הם תת־מרחבים של $\mathbb{R}^3$.

התשובה בעמוד 211

שאלה 7.3.6

א. הוכיחו כי לכל מרחב V שיש בו יותר מווקטור אחד, יש לפחות שני תת־מרחבים, והם V ו־ $\{0\}$.

ב. מצאו דוגמה למרחב שיש בו אינסוף איברים ואין לו יותר משני תת־מרחבים.

התשובה בעמוד 211

כדי להוכיח את המשפט הבא נשתמש במשפט הבוחן 7.3.2.

משפט 7.3.3 חיתוך של תת־מרחבים

אם W_1 ו־ W_2 הם תת־מרחבים של מרחב לינארי V (מעל שדה F), אזי החיתוך $W_1 \cap W_2$ אף הוא תת־מרחב של V.

---

1 כאשר נדון בווקטורים ב־ F^n, ובפרט ב־ $\mathbb{R}^n$, נסמן אותם באות לטינית זקופה ומודגשת, כפי שנהגנו בפרק 2. וקטורים במרחבים כלליים יסומנו, כפי שהסכמנו, באותיות לטיניות נטויות ולא מודגשות.

הוכחה

נוכיח כי הקבוצה $W_1 \cap W_2$ מקיימת את התנאים שבבוחן (משפט 7.3.2).

א. $W_1 \cap W_2$ מכיל את וקטור האפס של V, שכן 0 הוא איבר ב־W_1 וגם ב־W_2.

ב. יהיו $u,v \in W_1 \cap W_2$. עלינו להראות כי $u+v \in W_1 \cap W_2$.

1. מאחר ש־$u,v \in W_1$ ומאחר ש־W_1 תת־מרחב של V, הרי:

$$u+v \in W_1 \qquad (1)$$

2. מאחר ש־$u,v \in W_2$ ומאחר ש־W_2 תת־מרחב של V, הרי:

$$u+v \in W_2 \qquad (2)$$

מ־(1) ומ־(2) נובע כי:

$$u+v \in W_1 \cap W_2$$

ג. יהי $w \in W_1 \cap W_2$, ויהי $\lambda \in F$ סקלר כלשהו. עלינו להראות כי:

$$\lambda w \in W_1 \cap W_2$$

1. מאחר ש־$w \in W_1$ ומאחר ש־W_1 תת־מרחב של V, הרי:

$$\lambda w \in W_1 \qquad (1)$$

2. באותו אופן, מתוך $w \in W_2$ נובע:

$$\lambda w \in W_2 \qquad (2)$$

מ־(1) ומ־(2) נובע כי:

$$\lambda w \in W_1 \cap W_2$$

מ.ש.ל.

הערה

את האמור במשפט 7.3.3 ניתן להכליל לחיתוך של שלושה, ארבעה או מספר כלשהו של תת־מרחבים, ואף לחיתוך של אוסף כלשהו (אולי אינסופי) של תת־מרחבים. נאמר בקצרה: **חיתוך של תת־מרחבים הוא תת־מרחב**. הוכחת הכללה זו דומה להוכחת משפט 7.3.3, ונשמיטה.

שאלה 7.3.7

יהי F שדה סופי בעל p איברים. כמה איברים יש:

א. במרחב $V = F^2$? בתת־מרחב $W = \mathrm{Sp}(\{(1,1)\})$?

ב. במרחב הפולינומים $V = F[x]$? בתת־מרחב $W = F_n[x]$?

התשובה בעמוד 211

7.4 צירופים לינאריים

בפרק 2 הגדרנו מהו צירוף לינארי של וקטורים ב־ $\mathbb{R}^n$. כעת נגדיר מהו צירוף לינארי של וקטורים במרחב לינארי כללי. תוכלו לבדוק ולוודא כי ההגדרה שבפרק 2 היא מקרה פרטי של ההגדרה הכללית שלהלן.

הגדרה 7.4.1 צירוף לינארי

יהי V מרחב לינארי מעל שדה F, ויהיו $v_1,\ldots,v_n$ וקטורים כלשהם מתוך V.

סכום מהטיפוס

$$\lambda_1 v_1 + \ldots + \lambda_n v_n \quad \left(= \sum_{i=1}^{n} \lambda_i v_i\right)$$

שבו $\lambda_1,\ldots,\lambda_n$ הם סקלרים מתוך F, מכונה **צירוף לינארי של הוקטורים** $v_1,\ldots,v_n$ **עם המקדמים** $\lambda_1,\ldots,\lambda_n$.

הערות

א. צירוף לינארי עשוי להיות צירוף לינארי של וקטור אחד, של שני וקטורים, של שלושה וקטורים, ובאופן כללי של **מספר סופי** כלשהו של וקטורים מתוך V. על כל פנים, צירוף לינארי הוא לעולם **סכום של מספר סופי** של מחוברים.

ב. ברור שצירוף לינארי של וקטורים ב־ V אף הוא וקטור ב־ V.

ג. על וקטור v, הניתן להצגה כצירוף לינארי של וקטורים $v = \lambda_1 v_1 + \ldots + \lambda_n v_n$, אומרים גם שהוא **תלוי לינארית** ב־ $v_1,\ldots,v_n$.

ד. נכליל את המינוח שבהערה הקודמת: תהי S קבוצת וקטורים במרחב לינארי V (לאו דווקא סופית). נאמר על וקטור v שהוא **תלוי לינארית** ב־ S אם v הוא צירוף לינארי של וקטורים מתוך S (כלומר, קיימים מספר סופי של וקטורים ב־ S ש־ v הוא צירוף לינארי שלהם).

ה. המקדמים בצירוף לינארי הם סקלרים מתוך F. חלקם, ואפילו כולם, עשויים להיות שווים ל־ 0. אי לכך, ברור שוקטור האפס, $0 \in V$, הוא צירוף לינארי של כל n וקטורים מתוך V, שהרי לכל $v_1,\ldots,v_n \in V$ מתקיים:

$$0v_1 + 0v_2 + \ldots + 0v_n = 0$$

ו. אם וקטור $v \in V$ הוא צירוף לינארי של וקטורים $v_1,\ldots,v_n \in V$,

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

($\lambda_i \in F$, לכל i, $1 \le i \le n$)

ואם $u_1,\ldots,u_k$ הם וקטורים כלשהם ב־ V,

אז v הוא גם צירוף לינארי של $v_1,\ldots,v_n$, $u_1,\ldots,u_k$, שהרי:

$$\lambda_1 v_1 + \ldots + \lambda_n v_n = \lambda_1 v_1 + \ldots + \lambda_n v_n + 0u_1 + \ldots + 0u_k$$

נבחן כמה דוגמאות.

דוגמה א

כל וקטור במרחב $\mathbb{R}^3$ הוא צירוף ליניארי של $\mathbf{e}_1 = (1,0,0)$, $\mathbf{e}_2 = (0,1,0)$, $\mathbf{e}_3 = (0,0,1)$, כי עבור כל $\mathbf{a} = (\lambda_1, \lambda_2, \lambda_3)$ ב־ $\mathbb{R}^3$ מתקיים:

$$\mathbf{a} = \lambda_1\mathbf{e}_1 + \lambda_2\mathbf{e}_2 + \lambda_3\mathbf{e}_3$$

(ודאו!)

▶

דוגמה ב

הפולינום

$$P(x) = 4x^4 + 2x^3 - 5x^2 + 7x + 10$$

תלוי ליניארית בפולינומים:

$$Q_1(x) = x^3 + x^2 \ , \ Q_2(x) = -x^2 + x + 2 \ , \ Q_3(x) = x^4 - x^2 + x + 1$$

כי:

$$P(x) = 2Q_1(x) + 3Q_2 + 4Q_3(x)$$

(ודאו!)

▶

דוגמה ג

אם v הוא וקטור במרחב ליניארי V, אז v תלוי ליניארית ב־ V, שכן $v = 1 \cdot v$.

▶

דוגמה ד

תהי K קבוצת המטריצות האלכסוניות מסדר 3×3 מעל הממשיים, שאיבריהן אינם חיוביים.

המטריצה $\begin{bmatrix} -1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -3 \end{bmatrix}$ תלויה ליניארית ב־ K, שכן היא ניתנת לתיאור כצירוף ליניארי של איברים ב־ K:

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -3 \end{bmatrix} = 1\begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} - 2\begin{bmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix} + 3\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

▶

שאלה 7.4.1

א. הציגו את הפולינום $-4x^2 + 2x + 3$ כצירוף ליניארי של הפולינומים 1, $1+x$, $1+x^2$.

ב. האם המטריצה $\begin{bmatrix} 2 & 3 \\ 2 & 3 \end{bmatrix}$ תלויה ליניארית במטריצות: $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ ו־ $\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$?

ג. נתבונן ב־ $\mathbb{R}$ כמרחב ליניארי מעל שדה המספרים הרציונליים $\mathbb{Q}$. האם $\sqrt{2}$ תלוי ליניארית בקבוצת המספרים הרציונליים?

התשובה בעמוד 212

7.5 התת־מרחב הנפרש על־ידי קבוצה

קבוצה לא ריקה K, שהיא חלקית למרחב לינארי V, היא תת־מרחב אם ורק אם היא סגורה לגבי חיבור וקטורים וכפל וקטורים בסקלר (משפט 7.3.2). לכן אם תת־קבוצה K (לא ריקה של V) אינה תת־מרחב של V, הרי שהיא אינה סגורה לגבי החיבור או לגבי הכפל בסקלר או לגבי שניהם גם יחד. אי־היותה של K תת־מרחב מתבטא בכך ש"חסרים" ב־K וקטורים. מתעוררת, אם כן, השאלה כיצד להרחיב את K באופן שיתקבל תת־מרחב.

דוגמה

תהי $K \subseteq \mathbb{R}^4$ קבוצה בת איבר אחד:

$$K = \{(5,-5,0,0)\}$$

▶

שאלה 7.5.1

הוכיחו כי K אינה תת־מרחב של $\mathbb{R}^4$.

התשובה בעמוד 212

K אמנם אינה תת־מרחב של $\mathbb{R}^4$ אבל קיימים תת־מרחבים של $\mathbb{R}^4$ המכילים את K. למשל, $\mathbb{R}^4$ עצמו הוא תת־מרחב של $\mathbb{R}^4$ המכיל את K. דוגמאות נוספות לתת־מרחבים של $\mathbb{R}^4$ המכילים את K, תמצאו בשאלה הבאה.

שאלה 7.5.2

תהי K הקבוצה שבדוגמה שלעיל, ותהיינה U,V,W התת־קבוצות של $\mathbb{R}^4$ הנתונות על־ידי:

$$U = \{(\alpha,\beta,\gamma,\delta) \mid \alpha+\beta+\gamma+\delta = 0,\ \ \alpha,\beta,\gamma,\delta \in \mathbb{R}\}$$

$$V = \{(\alpha,\beta,0,0) \mid \alpha,\beta \in \mathbb{R}\}$$

$$W = \{(\alpha,-\alpha,0,0) \mid \alpha \in \mathbb{R}\}$$

א. הוכיחו כי הקבוצות U,V ו־W הן תת־מרחבים של $\mathbb{R}^4$, המכילים את K.

ב. הראו כי $W \subseteq U$ וכי $W \subseteq V$.

ג. הוכיחו כי כל תת־מרחב של $\mathbb{R}^4$, המכיל את K, מכיל גם את W.

התשובה בעמוד 213

מן השאלה האחרונה אנו למדים ש־W הוא מרחב "מזערי" בין כל התת־מרחבים המכילים את K, שהרי הוא מוכל בכל אחד מהתת־מרחבים הללו. כדי לאפיין מרחבים מזעריים כאלה במקרה הכללי, נוסיף מושג חדש.

תהי K תת־קבוצה של מרחב ליניארי, ונסמן ב־ $\text{Sp}(K)$ את אוסף כל הצירופים הליניאריים של וקטורים מתוך K.[1]

הקבוצה $\text{Sp}(K)$ מכילה את כל הצירופים הליניאריים של וקטור אחד מתוך K (כלומר, את כל הוקטורים מהטיפוס λv, שבהם $v \in K$ ו־ λ סקלר כלשהו), וכן את כל הצירופים הליניאריים של שני וקטורים מתוך K (כלומר, את כל הוקטורים מהטיפוס $\lambda u + \mu v$, שבהם $u, v \in K$ ו־ λ, μ סקלרים כלשהם), ובאופן כללי - את כל הצירופים הליניאריים מהטיפוס $\lambda_1 v_1 + \ldots + \lambda_n v_n$, שבהם $v_1, \ldots, v_n \in F$ ו־ $\lambda_1, \ldots, \lambda_n \in F$. טענת המשפט שלהלן היא שהאוסף $\text{Sp}(K)$ הוא תת־מרחב המכיל את K; יתרה מזו, $\text{Sp}(K)$ הוא "מזערי" במובן זה שהוא מוכל בכל תת־מרחב המכיל את K.

משפט 7.5.1

תהי K קבוצה חלקית לא ריקה של מרחב ליניארי V (מעל שדה F), ויהי $\text{Sp}(K)$ אוסף כל הצירופים הליניאריים של וקטורים מתוך K. אזי:

א. $\text{Sp}(K)$ הוא תת־מרחב של V המכיל את K.

ב. אם W הוא תת־מרחב של V המכיל את K, אז W מכיל גם את $\text{Sp}(K)$.

הוכחה

א. נוכיח כי האוסף $\text{Sp}(K)$ מקיים את תנאי משפט הבוחן 7.3.2.

1. $\text{Sp}(K)$ אינו ריק כי $K \subseteq \text{Sp}(K)$ ו־ K אינה ריקה.
2. יהיו u, v שני וקטורים כלשהם ב־ $\text{Sp}(K)$, ויהיו λ ו־ μ סקלרים כלשהם.

נוכיח כי:

$$\lambda u + \mu v \in \text{Sp}(K)$$

$u \in \text{Sp}(K)$ $\Leftarrow$ קיימים וקטורים $u_1, \ldots, u_p \in K$ וקיימים סקלרים $\alpha_1, \ldots, \alpha_p \in F$, המקיימים:

$$u = \alpha_1 u_1 + \ldots + \alpha_p u_p \qquad (1)$$

$v \in \text{Sp}(K)$ $\Leftarrow$ קיימים וקטורים $v_1, \ldots, v_q \in K$ וקיימים סקלרים $\beta_1, \ldots, \beta_q \in F$, המקיימים:

$$v = \beta_1 v_1 + \ldots + \beta_q v_q \qquad (2)$$

מ־(1) ומ־(2) נובע כי:

$$\lambda u + \mu v = \lambda(\alpha_1 u_1 + \ldots + \alpha_p u_p) + \mu(\beta_1 v_1 + \ldots + \beta_q v_q)$$

כלומר:

$$\lambda u + \mu v = \lambda\alpha_1 u_1 + \ldots + \lambda\alpha_p u_p + \mu\beta_1 v_1 + \ldots + \mu\beta_q v_q \qquad (3)$$

1 מקור הסימון $\text{Sp}(K)$ יובהר בהמשך.

(3) היא הצגה של $\lambda u + \mu v$ כצירוף לינארי של הוקטורים $v_1,\dots,v_q$, $u_1,\dots,u_p$ מתוך K, ולכן מעצם הגדרת $\mathrm{Sp}(K)$ מתקיים $\lambda u + \mu v \in \mathrm{Sp}(K)$, כפי שרצינו להוכיח.

מצאנו כי האוסף $\mathrm{Sp}(K)$ מקיים את תנאי משפט הבוחן '7.3.2, והוא אפוא תת־מרחב של V.
ברור כי כל וקטור v ב־ K שייך ל־ $\mathrm{Sp}(K)$, שכן $v = 1 \cdot v$, כלומר $K \subseteq \mathrm{Sp}(K)$.

ב. כעת נוכיח כי אם W הוא תת־מרחב של V, ואם $K \subseteq W$, אז גם $\mathrm{Sp}(K) \subseteq W$. לשם כך, נוכיח כי כל איבר של $\mathrm{Sp}(K)$ בהכרח שייך ל־ W.
יהי

$$\alpha_1 u_1 + \ldots + \alpha_n u_n$$

איבר כלשהו ב־ $\mathrm{Sp}(K)$ (כלומר, צירוף לינארי כלשהו של וקטורים מתוך K).
לכל i $(1 \le i \le n)$

$$u_i \in K$$

ולכן $u_i \in W$.
מתוך כך ש־ W תת־מרחב, נובע כי לכל i $(1 \le i \le n)$

$$\alpha_i u_i \in W$$

ולכן גם

$$\sum_{i=1}^{n} \alpha_i u_i \in W$$

(שוב, מאחר ש־ W הוא תת־מרחב).

מ.ש.ל.

שימו לב, משפט 7.5.1 נותן בידינו כלי נוסף לבדוק האם קבוצת איברים מסוימת היא תת־מרחב – אם ניתן להציג אותה בצורה $\mathrm{Sp}(K)$ (עבור איזושהי K), אזי היא אכן תת־מרחב.

הגדרה 7.5.2

יהי V מרחב לינארי (מעל שדה F) ותהי K תת־קבוצה לא ריקה של V.
התת־מרחב $\mathrm{Sp}(K)$, שאיבריו הם כל הצירופים הלינאריים של וקטורים מתוך K, נקרא **התת־מרחב הנפרש (או הנוצר)** על־ידי U.

על הקבוצה U אומרים שהיא **קבוצת יוצרים** של $\mathrm{Sp}(K)$ וגם שהיא **פורשת** את המרחב $\mathrm{Sp}(K)$.
בפרט, אם $\mathrm{Sp}(K) = V$, אומרים שהתת־קבוצה K **פורשת** את המרחב V.

הערות

א. האותיות Sp שבסימן $\mathrm{Sp}(K)$ הן ראשי התיבה Span, שמשמעה פְּרִישָׂה.
ב. יש המרחיבים את ההגדרה למקרה שבו K היא הקבוצה הריקה, על־ידי $\mathrm{Sp}(K) = \{0\}$.

מושג הפרישה של קבוצת וקטורים במרחב ליניארי שהגדרנו זה עתה מכליל את מושג הפרישה שהגדרנו בפרק 2, הגדרה 2.7.1. שם ההגדרה הייתה תקפה עבור המרחב F^n, ואילו ההגדרה כאן תקפה עבור מרחב ליניארי כללי. שימו לב שבמסדרת הגדרה 2.7.1 קבענו גם מתי **סדרת** וקטורים ב־F^n פורשת את F^n. למען השלמות נביא כאן הגדרה מקבילה עבור מרחבים כלליים:

הגדרה '7.5.2

נאמר שסדרת וקטורים $(v_1,\ldots,v_n)$ במרחב ליניארי V **פורשת** את V אם הקבוצה $\{v_1,\ldots,v_n\}$ פורשת את V.

הערות

א. שימו לב שבסדרת הוקטורים $(v_1,\ldots,v_n)$ תיתכנה חזרות, ובמקרה זה הקבוצה $\{v_1,\ldots,v_n\}$ תכלול פחות מ־n וקטורים.

ב. אם סדרת הוקטורים $(v_1,\ldots,v_n)$ פורשת את V, נאמר גם בקצרה כי "הוקטורים $v_1,\ldots,v_n$ פורשים את V".

המרחב הנוצר על־ידי הקבוצה K, כלומר $\mathrm{Sp}(K)$, מכיל את K ומוכל בכל תת־מרחב המכיל את K. תכונה זו היא תכונה ה**מאפיינת** את התת־מרחב $\mathrm{Sp}(K)$, כפי שמורה השאלה הבאה.

שאלה 7.5.3

תהי K קבוצת וקטורים לא־ריקה במרחב ליניארי V, ויהי W תת־מרחב המכיל את K ומוכל בכל תת־מרחב המכיל את K. הוכיחו כי:

$$W = \mathrm{Sp}(K)$$

התשובה בעמוד 213

כבר תיארנו לעיל את $\mathrm{Sp}(K)$ כתת־מרחב "מזערי" בשל העובדה שהוא מוכל בכל תת־מרחב המכיל את K. עתה, משראינו כי $\mathrm{Sp}(K)$ הוא היחיד בעל תכונה זו (בין כל התת־מרחבים המכילים את K), נהיה רשאים לומר כי $\mathrm{Sp}(K)$ הוא **התת־מרחב המזערי** המכיל את K.

שאלה 7.5.4

מצאו את התת־מרחב הנפרש על־ידי איברי הבסיס הסטנדרטי $\mathbf{e}_1,\ldots,\mathbf{e}_n$ של $\mathbb{R}^n$.

(כלומר, תארו את $\mathrm{Sp}(\{\mathbf{e}_1,\ldots,\mathbf{e}_n\})$.)

התשובה בעמוד 214

שאלה 7.5.5

א. נתבונן בוקטורים $\mathbf{a} = (1,2,0)$ ו־$\mathbf{b} = (3,5,0)$ ב־$\mathbb{R}^3$.

תארו, בדרך אלגברית ובצורה גיאומטרית, את:

$$\mathrm{Sp}(\{\mathbf{a},\mathbf{b}\})$$

ב. מצאו ב־$\mathbb{R}^3$ שני וקטורים אחרים, $\mathbf{c}$ ו־$\mathbf{d}$, שאינם $\mathbf{a}$ ו־$\mathbf{b}$, שעבורם:

$$\mathrm{Sp}(\{\mathbf{a},\mathbf{b}\}) = \mathrm{Sp}(\{\mathbf{c},\mathbf{d}\})$$

(כלומר, מצאו שני וקטורים אחרים, שאינם $\mathbf{a}$ ו־$\mathbf{b}$, הפורשים אותו תת־מרחב כמו $\mathbf{a}$ ו־$\mathbf{b}$.)

התשובה בעמוד 214

שאלה 7.5.6

הוכיחו כי קבוצת הפולינומים $\{1,x,x^2,x^3\}$ היא קבוצת יוצרים של המרחב $F_4[x]$, כלומר הוכיחו כי:

$$F_4[x] = \mathrm{Sp}(\{1,x,x^2,x^3\})$$

להזכירכם: $F_4[x]$ הוא מרחב הפולינומים שמעלתם קטנה מ־4 עם מקדמים מן השדה F (בתוספת פולינום האפס).

התשובה בעמוד 215

שאלה 7.5.7

א. הוכיחו כי שש המטריצות

$$E^{(1,1)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad E^{(1,2)} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$E^{(1,3)} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \qquad E^{(2,1)} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

$$E^{(2,2)} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \qquad E^{(2,3)} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

פורשות את מרחב המטריצות A.

ב. הוכיחו כי גם הקבוצה בעלת שבעת האיברים

$$\left\{E^{(1,1)}, E^{(1,2)}, E^{(1,3)}, E^{(2,1)}, E^{(2,3)}, \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}\right\}$$

פורשת את $\mathbf{M}_{2\times 3}^{\mathbb{R}}$.

התשובה בעמוד 216

שאלה 7.5.8

א. תהי U תת־קבוצה לא־ריקה של מרחב לינארי V. הוכיחו כי U תת־מרחב של V אם ורק אם:

$$\mathrm{Sp}(U) = U$$

ב. הוכיחו כי לכל תת־קבוצה לא ריקה K של מרחב ליניארי V מתקיים:

$$\mathrm{Sp}\big(\mathrm{Sp}(K)\big) = \mathrm{Sp}(K)$$

התשובה בעמוד 217

שאלה 7.5.9

תארו את התת־מרחב של $\mathbf{M}_{2\times 2}^{\mathbb{R}}$ הנפרש על־ידי הקבוצה הכוללת

א. את שלוש המטריצות:

$$E^{(1,1)} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad ; \quad E^{(1,2)} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \quad ; \quad E^{(1,2)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

ב. את המטריצה:

$$L = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

התשובה בעמוד 217

שאלה 7.5.10

מצאו את התת־מרחב של מרחב הפולינומים מעל $\mathbb{R}$, הנפרש על־ידי קבוצת הפולינומים:

$$\{x, x^2, x^3, x^4\}$$

התשובה בעמוד 218

שאלה 7.5.11

יהי V מרחב ליניארי (מעל שדה F), ויהיו $v_1,\dots,v_n$, n וקטורים ב־ V.

א. הוכיחו כי לכל סקלר λ השונה מ־ 0:

$$\mathrm{Sp}(\{v_1,\dots,v_n\}) = \mathrm{Sp}(\{v_1,\dots,v_{i-1}, \lambda v_1, v_{i-1},\dots,v_n\})$$

ב. הוכיחו כי לכל F $\lambda \in$:

$$\mathrm{Sp}(\{v_1,\dots,v_n\}) = \mathrm{Sp}(\{v_1,\dots,v_{j-1}, v_j + \lambda v_1, v_{j+1},\dots,v_n\})$$

התשובה בעמוד 218

שאלה 7.5.12

תהי $A = [a_{ij}]$ מטריצה מסדר $m \times n$ מעל שדה F.

$$A = \begin{bmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ a_{m1} & \cdots & \cdots & a_{mn} \end{bmatrix}$$

נסמן ב־ $\mathbf{a}_i$ $(1 \le i \le m)$ את הוקטור ב־ F^n שרכיביו הם איברי השורה ה־ i של A, כלומר לכל i $(1 \le i \le m)$:

$$\mathbf{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in})$$

כעת, נתבונן במרחב הנפרש על־ידי הוקטורים $\mathbf{a}_i$, כלומר נתבונן ב־

$$\mathrm{Sp}(\{\mathbf{a}_1, , \ldots, \mathbf{a}_m\})$$

מרחב זה מכונה **מרחב השורות של** A.

תהי $B = [b_{ij}]_{m\times n}$ מטריצה מסדר $m \times n$ שהיא שקולת־שורה ל־ A, ונסמן ב־ $\mathbf{b}_i$ $(1 \le i \le m)$ את הוקטור ב־ F^n שרכיביו הם איברי השורה ה־ i־ית של B.

הוכיחו כי:

$$\mathrm{Sp}(\{\mathbf{a}_1, , \ldots, \mathbf{a}_m\}) = \mathrm{Sp}(\{\mathbf{b}_1, , \ldots, \mathbf{b}_m\})$$

בניסוח מילולי המסבר את האוזן: למטריצות שקולות־שורה יש אותו מרחב שורות.

התשובה בעמוד 219

שאלה 7.5.13

יהיו V מרחב לינארי, K תת־קבוצה לא ריקה של V, ויהי v וקטור כלשהו ב־ V.
הוכיחו כי

$$\mathrm{Sp}(K \cup \{v\}) = \mathrm{Sp}(K)$$

אם ורק אם v תלוי לינארית ב־ K.

התשובה בעמוד 220

שאלה 7.5.14

א. הוכיחו כי לא קיימת קבוצה **סופית** של פולינומים מעל שדה F, הפורשת את $F[x]$.

ב. מצאו קבוצת יוצרים של המרחב $F[x]$.

התשובה בעמוד 220

הגדרה 7.5.3

יהי V מרחב לינארי. אומרים ש־ V **נוצר סופית** אם ורק אם קיימת קבוצה סופית היוצרת את V.

בהתאם להגדרה זו תנוסח הטענה שבשאלה הקודמת כך:

מרחב הפולינומים מעל שדה F **אינו נוצר סופית**.

שאלה 7.5.15

א. הוכיחו כי לכל $n \ge 1$, המרחב הלינארי F^n מעל השדה F נוצר סופית.

ב. הוכיחו כי המרחב הלינארי $\mathbf{M}^F_{m\times n}$ נוצר סופית.

התשובה בעמוד 221

הקיום של קבוצת יוצרים אחת של V, שהיא סופית, מספיק לכך ש־ V יהיה נוצר סופית, ללא תלות בשאלה כמה איברים יש בקבוצות יוצרים אחרות של V. הבעיה הבאה שבה נעסוק נוגעת לקשר שבין קבוצות שונות הפורשות אותו מרחב.

משפט 7.5.4

יהי V מרחב ליניארי (מעל שדה F), ותהיינה K ו־ T תת־קבוצות לא ריקות של V. אז

$$\mathrm{Sp}(K) = \mathrm{Sp}(T)$$

אם ורק אם מתקיימים שני התנאים:

א. כל וקטור ב־ K הוא צירוף ליניארי של וקטורים מתוך T (ובניסוח אחר: $K \subseteq \mathrm{Sp}(T)$).

ב. כל וקטור ב־ T הוא צירוף ליניארי של וקטורים מתוך K (ובניסוח אחר: $T \subseteq \mathrm{Sp}(K)$).

הוכחה

כיוון ראשון:

אם $\mathrm{Sp}(K) = \mathrm{Sp}(T)$, אז כל וקטור ב־ $\mathrm{Sp}(K)$ נמצא גם ב־ $\mathrm{Sp}(T)$, ומאחר ש־ $K \subseteq \mathrm{Sp}(K)$, נובע מכך ש־ $K \subseteq \mathrm{Sp}(T)$, הווי אומר – כל וקטור ב־ K הוא צירוף ליניארי של וקטורים מתוך T.

באותו אופן בדיוק (תוך החלפת התפקידים בין K ו־ T בפִּסקה האחרונה), מוכיחים כי כל וקטור ב־ T הוא צירוף ליניארי של איברים מ־ K.

כיוון שני:

נניח כי $K \subseteq \mathrm{Sp}(T)$ וכי $T \subseteq \mathrm{Sp}(K)$, ונוכיח:

$$\mathrm{Sp}(K) = \mathrm{Sp}(T)$$

מההנחה $K \subseteq \mathrm{Sp}(T)$ נובע ש־ $\mathrm{Sp}(T)$ הוא תת־מרחב המכיל את K.

אולם $\mathrm{Sp}(K)$ מוכל בכל תת־מרחב המכיל את K, כלומר:

$$\mathrm{Sp}(K) \subseteq \mathrm{Sp}(T) \qquad (1)$$

באותו אופן בדיוק, נובע מתוך ההנחה $T \subseteq \mathrm{Sp}(K)$ כי:

$$\mathrm{Sp}(T) \subseteq \mathrm{Sp}(K) \qquad (2)$$

מ־(1) ומ־(2) נובע כמובן השוויון:

$$\mathrm{Sp}(K) = \mathrm{Sp}(T)$$

מ.ש.ל.

שאלה 7.5.16

א. האם מתוך $T \subseteq K$ נובע $\mathrm{Sp}(K) \subseteq \mathrm{Sp}(T)$?

ב. האם מתוך $K \subseteq \mathrm{Sp}(T)$ נובע $\mathrm{Sp}(K) \subseteq \mathrm{Sp}(T)$?

ג. האם מתוך $K \subseteq \mathrm{Sp}(T)$ נובע $K \subseteq T$?

ד. האם מתוך $K \subset T$ (חלקית ממש!) נובע $\mathrm{Sp}(K) \subset \mathrm{Sp}(T)$?

התשובה בעמוד 221

שאלה 7.5.17

א. הוכיחו:

$$\mathrm{Sp}(K) \cup \mathrm{Sp}(T) \subseteq \mathrm{Sp}(K \cup T)$$

ב. בדקו האם בהכרח:

$$\mathrm{Sp}(K) \cup \mathrm{Sp}(T) = \mathrm{Sp}(K \cup T)$$

ג. הוכיחו:

$$\mathrm{Sp}(K \cap T) \subseteq \mathrm{Sp}(K) \cap \mathrm{Sp}(T)$$

ד. בדקו האם בהכרח:

$$\mathrm{Sp}(K \cap T) = \mathrm{Sp}(K) \cap \mathrm{Sp}(T)$$

התשובה בעמוד 222

לסיום הסעיף, נראה כיצד למצוא קבוצת יוצרים למרחב (או תת־מרחב) נתון.

דוגמה

נתונה המטריצה $B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$.

נמצא קבוצה פורשת לתת־מרחב $U = \{A \in \mathbf{M}_{2\times 2}(\mathbb{R}) \mid AB = BA\}$ של $\mathbf{M}_{2\times 2}(\mathbb{R})$.

שלב ראשון:

תהי $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ מטריצה מעל $\mathbb{R}$. אז חישוב קל מראה ש־ $A \in U \Leftrightarrow \begin{cases} b = 0 \\ d = a \end{cases} \Leftrightarrow A = \begin{pmatrix} a & 0 \\ c & a \end{pmatrix}$.

מצאנו את האיבר הכללי של U.

שלב שני:

נכתוב את הביטוי עבור איבר כללי כסכום של שתי מטריצות, שבכל אחת מופיע פרמטר אחד:
$A = \begin{pmatrix} a & 0 \\ c & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}$, כאשר c, a ממשיים כלשהם.

שלב שלישי:

נוציא את הפרמטר המתאים מכל מטריצה בסכום, ונקבל: $A = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + c\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$

נסיק כי $U = \mathrm{Sp}\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right\}$ והקבוצה $\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right\}$ פורשת את U.

◀

שאלה 7.5.18

א. תהי U קבוצת כל הפולינומים ב־ $\mathbb{R}_4[x]$ ש־1 הוא שורש שלהם.
ודאו בעצמכם ש־ U הוא תת־מרחב, ומצאו לו קבוצה פורשת.

ב. חזרו על השאלה שבחלק א עבור W - קבוצת כל הפולינומים ב־ $\mathbb{R}_4[x]$ ש־ 1 ו־ 2 הם שורשים שלהם.

התשובה בעמוד 223

7.6 סכום של תת־מרחבים

בסעיף 7.2 מצאנו כי החיתוך של שני תת־מרחבים הוא עצמו תת־מרחב. לעומתו, האיחוד של שני תת־מרחבים אינו בהכרח תת־מרחב, כפי שתראו בשאלה הבאה.

שאלה 7.6.1

תהיינה U ו־ W התת־קבוצות של $\mathbb{R}^3$ המוגדרות על־ידי:

$$U = \{(a,b,c) \mid a+b+c=0,\ a,b,c \in \mathbb{R}\}$$

$$U = \{(0,0,d) \mid d \in \mathbb{R}\}$$

א. הוכיחו כי U ו־ W הם תת־מרחבים של $\mathbb{R}^3$.

ב. הוכיחו כי $W \cup U$ אינו תת־מרחב של $\mathbb{R}^3$.

התשובה בעמוד 224

שאלה 7.6.2

א. יהיו U ו־ W תת־מרחבים של מרחב לינארי V (מעל שדה F).
הוכיחו כי האיחוד, $W \cup U$, הוא עצמו תת־מרחב של V אם ורק אם $W \subseteq U$ או $U \subseteq W$.

ב. מצאו דוגמה לשני תת־מרחבים של $\mathbb{R}^2$ שאיחודם אינו תת־מרחב של $\mathbb{R}^2$.

התשובה בעמוד 224

ובכן, האיחוד של שני תת־מרחבים U ו־ W של מרחב לינארי V אינו בהכרח תת־מרחב של V. לעומת זאת, ברור שאיחוד זה הוא קבוצת וקטורים חלקית ל־ V. לפיכך, קיימים כמובן תת־מרחבים של V המכילים את $W \cup U$.

למשל, V עצמו הוא תת־מרחב של V המכיל את $W \cup U$. כפי שראינו בסעיף הקודם, מבין כל התת־מרחבים של V המכילים את $W \cup U$, הקטן ביותר הוא $\mathrm{Sp}(U \cup W)$ (המרחב הנפרש על־ידי $W \cup U$). בסעיף זה נלמד לתאר את $\mathrm{Sp}(U \cup W)$ כ"**סכום של התת־מרחבים** U ו־ W".

הגדרה 7.6.1

יהי V מרחב לינארי מעל שדה F, ותהיינה S ו־ T שתי קבוצות חלקיות ל־ V. אוסף כל הוקטורים ב־ V שהם סכומים של וקטור מתוך S ווקטור מתוך T, מכונה **הסכום של הקבוצות** S ו־ T, וסימנו $S+T$.

הווי אומר:

$$S+T \overset{\text{def}}{=} \{s+t \mid s \in S,\ t \in T\}$$

שאלה 7.6.3

תהיינה S, T ו־ K שלוש קבוצות חלקיות של מרחב ליניארי V מעל שדה F.

הוכיחו:

א. $S+T=T+S$

ב. $(S+T)+K=S+(T+K)$

התשובה בעמוד 225

דוגמה

יהיו ℓ_1 ו־ ℓ_2 שני ישרים שונים ב־ $\mathbb{R}^3$, העוברים דרך ראשית הצירים. הסכום $\ell_1+\ell_2$ הוא אוסף כל הוקטורים ב־ $\mathbb{R}^3$ שהם סכומים של וקטור מתוך ℓ_1 עם וקטור מתוך ℓ_2.

יהי $\mathbf{a}_1$ וקטור כלשהו על ℓ_1, שונה מ־ $\mathbf{0}$, ויהי $\mathbf{a}_2$ וקטור כלשהו על ℓ_2, שונה מ־ $\mathbf{0}$.

כזכור,

$$\ell_1=\left\{\lambda\mathbf{a}_1 \middle| \lambda\in\mathbb{R}\right\} \quad , \quad \ell_2=\left\{\lambda\mathbf{a}_2 \middle| \lambda\in\mathbb{R}\right\}$$

ולכן:

$$\ell_1+\ell_2=\left\{\lambda\mathbf{a}_1+\mu\mathbf{a}_2 \middle| \lambda,\mu\in\mathbb{R}\right\}$$

מבחינה גיאומטרית, $\ell_1+\ell_2$ הוא המישור ב־ $\mathbb{R}^3$ הנקבע על־ידי הישרים ℓ_1 ו־ ℓ_2. שני הישרים ℓ_1 ו־ ℓ_2 מוכלים כמובן במישור זה.

מבחינה אלגברית, ℓ_1 ו־ ℓ_2 שניהם תת־מרחבים של $\mathbb{R}^3$, וגם סכומם, $\ell_1+\ell_2$, הוא תת־מרחב של $\mathbb{R}^3$ [1] המכיל כל אחד מן התת־מרחבים ℓ_1 ו־ ℓ_2. תופעה זו אינה מקרית. **לעולם** סכום של שני תת־מרחבים הוא תת־מרחב. זהו תוכן המשפט הבא.

▸

משפט 7.6.2

יהיו U ו־ W שני תת־מרחבים של מרחב ליניארי V מעל שדה F. אזי, הסכום $U+W$ הוא תת־מרחב של V המכיל את U ואת W. יתר על כן, $U+W$ הוא התת־מרחב הקטן ביותר של V בעל תכונה זו.

הוכחה

ראשית, נוכיח כי $U+W$ הוא תת־מרחב, וזאת על־ידי כך שנראה כי הקבוצה $U+W$, שהיא חלקית ל־ V, ממלאת את תנאי משפט הבוחן לתת־מרחבים (משפט 7.3.2).

א. נוכיח כי $U+W$ אינה ריקה: כל אחת מהקבוצות U ו־ W היא תת־מרחב של V, ולכן וקטור האפס של V, 0, שייך לכל אחת מהן. מן השוויון

$$0+0=0$$

נובע כי $0\in U+W$, וממילא $U+W$ אינה ריקה.

---

1 ראו שאלה 7.3.4.

ב. נניח כי $v_1, v_2 \in U + W$. כל אחד משני וקטורים אלה ניתן, אם כן, להצגה כסכום וקטורים מ־ U ומ־ W

$$v_1 = u_1 + w_1$$

$$v_2 = u_2 + w_2$$

כאשר $u_1, u_2 \in U$ ו־ $w_1, w_2 \in W$.

סכום הוקטורים v_1 ו־ v_2 הוא:

$$v_1 + v_2 = (u_1 + w_1) + (u_2 + w_2) = (u_1 + u_2) + (w_1 + w_2)$$

ברור כי:

$$u_1 + u_2 \in U$$

וכן:

$$w_1 + w_2 \in W$$

ולכן:

$$v_1 + v_2 \in U + W$$

ג. נוכיח כי $U + W$ סגורה לגבי הכפל בסקלר, והפעם בקצרה.

לכל $u \in U$, $w \in W$, $\lambda \in F$:

$$\lambda(u + w) = \lambda u + \lambda w \in U + W$$

מתוך א–ג נובע כי הקבוצה $U + W$ היא תת־מרחב של V.

להשלמת ההוכחה עלינו להראות עוד כי התת־מרחב $U + W$ מכיל את U ואת W. טענה זו נובעת במישרין מכך ש־ $0 \in U$ ו־ $0 \in W$, ומכך שלכל $u \in U$ ולכל $w \in W$:

$$u = u + 0 \ \ ; \ \ w = 0 + w$$

לאור מה שהוכחנו, $U + W$ הוא מרחב המכיל כל צירוף לינארי של וקטורים מתוך הקבוצה $U \cup W$, ולכן הוא מכיל את $\mathrm{Sp}(U \cup W)$. אך ברור ש־ $U + W$ מוכל ב־ $\mathrm{Sp}(U \cup W)$, שכן כל וקטור ב־ U מוכל ב־ $\mathrm{Sp}(U \cup W)$, וכל וקטור ב־ W מוכל ב־ $\mathrm{Sp}(U \cup W)$. כלומר $U + W$ מתלכד עם המרחב $\mathrm{Sp}(U \cup W)$. כפי שראינו בסעיף הקודם, מרחב זה הוא התת־מרחב המזערי המכיל את $U \cup W$, כלומר מכיל הן את U והן את W.

מ.ש.ל.

את הגדרת הסכום של שתי קבוצות ואת משפט 7.6.2 ניתן להכליל בקלות עבור מספר **סופי** כלשהו של מחוברים.

הגדרה 7.6.3

יהי V מרחב ליניארי מעל שדה F, ותהיינה $T_1,\ldots,T_n$ קבוצות חלקיות של V.

הסכום $T_1+\ldots+T_n$ מוגדר כך:

$$T_1+\ldots+T_n \overset{\text{def}}{=} \{t_1+\ldots+t_n \mid t_i \in T_i, 1 \le i \le n \text{ לכל}\}$$

הערות

א. בהגדרה 7.6.3 הסתמכנו על תכונת הקיבוציות המוכללת.

ב. מתוך תכונת החילופיות (המוכללת) נובע כי הסכום של מספר סופי כלשהו של תת־קבוצות של מרחב V אינו תלוי בסדר המחוברים.

משפט 7.6.4

הסכום $U_1+\ldots+U_n$ של מספר סופי כלשהו של תת־מרחבים, של מרחב ליניארי V (מעל שדה F), הוא עצמו תת־מרחב של V.

שאלה 7.6.4

הוכיחו את משפט 7.6.4.

התשובה בעמוד 226

שאלה 7.6.5

יהיו U ו־ W שני תת־מרחבים של מרחב ליניארי V מעל שדה F.

הוכיחו כי $U+W=U$ אם ורק אם $W \subseteq U$.

התשובה בעמוד 226

שאלה 7.6.6

יהיו $U_1,\ldots,U_n$ תת־מרחבים של מרחב ליניארי V מעל שדה F.

א. הוכיחו כי:

$$U_1 \cup \ldots \cup U_n \subseteq U_1+\ldots+U_n$$

ב. הוכיחו כי:

$$\mathrm{Sp}(U_1 \cup \ldots \cup U_n) = U_1+\ldots+U_n$$

התשובה בעמוד 227

משאלה 7.6.6 נקבל את המסקנה הבאה:

מסקנה 7.6.5

הסכום $U_1+\ldots+U_n$ של תת־מרחבים $U_1,\ldots,U_n$ של מרחב לינארי V, הוא התת־מרחב הקטן ביותר של V המכיל את $U_1,U_2,\ldots,U_n$.

שאלה 7.6.7

יהיו U ו־ W שני תת־מרחבים של מרחב לינארי V.

הראו כי:

$U \cup W = U + W$ אם ורק אם $W \subseteq U$ או $U \subseteq W$.

התשובה בעמוד 227

שאלה 7.6.8

יהיו $U = \mathrm{Sp}(S)$, $W = \mathrm{Sp}(T)$ שני תת־מרחבים של מרחב לינארי V, כאשר S, T תת־קבוצות לא ריקות של V. הוכיחו כי:

$$U + W = \mathrm{Sp}(S) + \mathrm{Sp}(T) = \mathrm{Sp}(S \cup T)$$

התשובה בעמוד 227

7.7 סכום ישר של תת־מרחבים

שאלה 7.7.1

תהיינה U_1 ו־ U_2 תת־קבוצות של $\mathbb{R}^3$ המוגדרות על־ידי:

$$U_1 = \{(a,b,c) \mid a+b+c=0\}$$

$$U_2 = \{(a,b,c) \mid a=c\}$$

א. בשאלה 7.6.1 הוכחתם ש־ U_1 הוא תת־מרחב. הוכיחו כי גם U_2 הוא תת־מרחב של $\mathbb{R}^3$.

ב. הראו כי:

$$U_1 + U_2 = \mathbb{R}^3$$

ג. מצאו וקטור ב־ $\mathbb{R}^3$ שניתן להציגו בשתי דרכים שונות כסכום של וקטור אחד מתוך U_1 ווקטור שני מתוך U_2. (נסו להציג את וקטור האפס.)

התשובה בעמוד 228

שאלה 7.7.2

תהיינה U_1 ו־ U_2 תת־קבוצות של $\mathbb{R}^3$ המוגדרות על־ידי:

$$U_1 = \{(a,0,0) \mid a \in \mathbb{R}\}$$

$$U_2 = \{(0,b,c) \mid b,c \in \mathbb{R}\}$$

א. הוכיחו כי U_1 ו־ U_2 הן תת־מרחבים של $\mathbb{R}^3$. (מה הם תיאוריהם הגיאומטריים?)

ב. הוכיחו כי:

$$U_1 + U_2 = \mathbb{R}^3$$

ג. הראו כי לכל וקטור ב־ $\mathbb{R}^3$ יש הצגה **יחידה** כסכום של וקטור מתוך U_1 ווקטור מתוך U_2.

התשובה בעמוד 229

בשתי השאלות האחרונות הצגנו את $\mathbb{R}^3$ כסכום של שני תת־מרחבים של $\mathbb{R}^3$. ודאי הבחנתם בהבדל שבין שני הסכומים.

במקרה השני, בניגוד למקרה הראשון, לכל וקטור ב־ $\mathbb{R}^3$ יש הצגה **יחידה** כסכום של וקטור מתוך U_1 ווקטור מתוך U_2. את ההבדל הזה מתארים באמירה שבמקרה השני (בניגוד לראשון), הסכום $U_1 + U_2$ הוא **סכום ישר**.

הגדרה 7.7.1

יהיו U_1 ו־ U_2 שני תת־מרחבים של מרחב לינארי V מעל שדה F.

נאמר כי התת־מרחב W הוא **סכום ישר** של U_1 ו־ U_2 ונרשום[1]

$$W = U_1 \oplus U_2$$

אם ורק אם מתקיימים שני תנאים:

א. $W = U_1 + U_2$

ב. לכל וקטור ב־ W יש הצגה **יחידה** כסכום של וקטור ב־ U_1 ווקטור ב־ U_2.

הערה חשובה

השימוש בסימון $\oplus$ (להבדיל מסימן ה"סכום" הרגיל $+$) עלול לתת לקורא את הרושם המוטעה כאילו הגדרנו כאן פעולה חדשה על תת־מרחבים של מרחב נתון, אך לא כך הדבר. בהינתן זוג תת־מרחבים U_1 ו־ U_2, המרחב $U_1 \oplus U_2$ מוגדר רק כאשר במרחב הסכום $W = U_1 + U_2$ יש לכל וקטור הצגה יחידה כאמור לעיל,[2] ובמקרה שהסכום מוגדר, המרחב $U_1 \oplus U_2$ **שווה** למרחב $U_1 + U_2$.

דוגמאות

א. בשאלה 7.7.2 הראינו כי $U_1 + U_2 = \mathbb{R}^3$, וכי לכל וקטור ב־ $\mathbb{R}^3$ יש הצגה **יחידה** כסכום של וקטור מתוך U_1 ווקטור מתוך U_2.

אפשר לסכם, אם כן, את מסקנת השאלה כך:

$$\mathbb{R}^3 = U_1 \oplus U_2$$

ב. נתבונן בתת־מרחבים של $\mathbb{R}^3$ משאלה 7.6.1:

$$U = \{(a,b,c) \mid a+b+c=0\}$$

$$W = \{(0,0,d) \mid d \in \mathbb{R}\}$$

ונוכיח כי:

$$\mathbb{R}^3 = U \oplus W$$

עלינו להוכיח שני דברים:

1. $\mathbb{R}^3 = U + W$
2. לכל וקטור ב־ $\mathbb{R}^3$ יש הצגה **יחידה** כסכום של וקטור מתוך U ווקטור מתוך W.

נוכיח תחילה את א:

יהי $(x,y,z) \in \mathbb{R}^3$ וקטור כלשהו. עלינו להראות כי ניתן להציגו כסכום של שני וקטורים, האחד – וקטור שסכום רכיביו הוא אפס (וקטור ב־ U), והאחר – וקטור ששני רכיביו הראשונים הם אפסים (וקטור ב־ W). הנה הצגה כזאת:

1 נעיר שאין קשר בין הסימון $\oplus$ שבו אנו משתמשים כאן לציון סכום ישר לבין הסימון $\oplus$ שבו השתמשנו בפרק 2 לציון סכום גיאומטרי של וקטורים.

2 הדבר דומה במקצת לשימוש בסימון $/$ עבור פעולת החילוק של מספרים ממשיים. הביטוי x/y מוגדר רק כאשר המכנה y שונה מאפס, ובמקרה זה הוא מתאר את תוצאת החלוקה של x ב־ y.

$$(x,y,z) = (\underset{\in U}{x,y,-x-y}) + (0,0,\underset{\in W}{z+x+y})$$

הסבירו לעצמכם כיצד נובע מכאן ש־ $\mathbb{R}^3 = U + W$.

נוכיח את ב:

נשתמש בעובדה שהחיתוך $U \cap W$ אינו מכיל אלא את וקטור האפס של $\mathbb{R}^3$, $\mathbf{0} = (0,0,0)$, ובסימנים:[3]

$$U \cap W = \{\mathbf{0}\}$$

נניח כי $u_1 + w_1$ ו־ $u_2 + w_2$ הן שתי הצגות של וקטור נתון $v \in \mathbb{R}^3$ כסכום של וקטור מתוך U עם וקטור מתוך W, כלומר נניח כי

$$v = u_1 + w_2 = u_2 + w_2$$

כאשר $u_1, u_2 \in U$, $w_1, w_2 \in W$.

נוכיח כי שתי ההצגות בהכרח מתלכדות זו עם זו, כלומר כי:

$$u_1 = u_2 \;,\quad w_1 = w_2$$

מתוך השוויון:

$$u_1 + w_1 = u_2 + w_2$$

נובע:

$$u_1 - u_2 = w_2 - w_1 \tag{1}$$

באגף שמאל של (1) רשום וקטור הנמצא ב־ U, ובאגף ימין שלו רשום וקטור של W. אולם הוקטור היחיד הנמצא גם ב־ U וגם ב־ W הוא $\mathbf{0}$, כלומר

$$u_1 - u_2 = w_2 - w_1 = \mathbf{0}$$

ומכאן ש־ $u_1 = u_2$ ו־ $w_1 = w_2$, כפי שרצינו להוכיח.

מ.ש.ל.

▸

בהוכחת חלק ב בדוגמה האחרונה לא הסתמכנו על אופיים הספציפי של המרחבים U ו־ W אלא רק על העובדה שהחיתוך של U ו־ W הוא $\{\mathbf{0}\}$. אי לכך יכולה אותה הוכחה לשמש גם להוכחת טענה כללית יותר.

משפט 7.7.2

יהי V מרחב ליניארי, ויהיו U ו־ W תת־מרחבים של V.

$V = U \oplus W$ אם ורק אם מתקיימים שני התנאים:

א. $V = U + W$

ב. $U \cap W = \{0\}$

---

3 הוקטור היחיד ב־ $\mathbb{R}^3$, שסכום רכיביו הוא אפס ושני רכיביו הראשונים הם אפסים, הוא $(0,0,0)$.

שאלה 7.7.3

הוכיחו את משפט 7.7.2.

התשובה בעמוד 230

שאלה 7.7.4

א. תהי $S^{\mathbb{R}}_{n\times n}$ קבוצת כל המטריצות הסימטריות מסדר $n\times n$ מעל הממשיים.
הוכיחו כי $S^{\mathbb{R}}_{n\times n}$ היא תת־מרחב של $\mathbf{M}^{\mathbb{R}}_{n\times n}$.

ב. תהי $A^{\mathbb{R}}_{n\times n}$ קבוצת המטריצות האנטי־סימטריות ב־ $\mathbf{M}^{\mathbb{R}}_{n\times n}$.
הוכיחו כי $A^{\mathbb{R}}_{n\times n}$ היא תת־מרחב של $\mathbf{M}^{\mathbb{R}}_{n\times n}$.
(זכרו: מטריצה ריבועית $A=[a_{ij}]_{n\times n}$ היא אנטי־סימטרית אם ורק אם $a_{ij}=-a_{ji}$ לכל i,j ($1\le i,j\le n$).)

ג. תהי A מטריצה כלשהי ב־ $\mathbf{M}^{\mathbb{R}}_{n\times n}$, ונגדיר את המטריצות B ו־ C על־ידי:

$$B=A+A^t$$

$$C=A-A^t$$

(זכרו: A^t היא המטריצה המשוחלפת של A:
אם $A=[a_{ij}]_{n\times n}$ ואם $A^t=[a^t_{ij}]_{n\times n}$, אז לכל i,j: $a^t_{ij}=a_{ji}$)
הוכיחו כי B היא מטריצה סימטרית, וכי C היא מטריצה אנטי־סימטרית.

ד. עבור $A\in A^{\mathbb{R}}_{n\times n}$, אמתו את הזהות:

$$A=\frac{A+A^t}{2}+\frac{A-A^t}{2}$$

ה. הוכיחו כי:

$$M^{\mathbb{R}}_{n\times n}=S^{\mathbb{R}}_{n\times n}\oplus A^{\mathbb{R}}_{n\times n}$$

התשובה בעמוד 231

שאלה 7.7.5

יהיו U ו־ W תת־מרחבים של מרחב לינארי V, ונניח כי:

$$V=U+W$$

הוכיחו: אם לוקטור האפס $0\in V$ יש הצגה **יחידה** כסכום של וקטור מתוך U ווקטור מתוך W, אז:

$$V=U\oplus W$$

(שימו לב, השוויון $0=0+0$ צופן בחובו הצגה של 0 כאיבר של $U+W$. לפיכך, אם ל־ $\mathbf{0}$ יש הצגה **יחידה**, אתם יודעים בדיוק מהי.)

התשובה בעמוד 233

מהטענה שבשאלה האחרונה נסיק משפט בוחן נוסף לסכום ישר:

משפט 7.7.3

יהי V מרחב ליניארי, ויהיו U ו־ W תת־מרחבים של V. אזי

$$V = U \oplus W$$

אם ורק אם מתקיימים שני התנאים:

א. $V = U + W$

ב. $0 = 0 + 0$ היא ההצגה היחידה של וקטור האפס, $0 \in V$, כסכום של וקטור מתוך U ווקטור מתוך W.

הגדרה 7.7.4

יהיו $U_1,\dots,U_n$ תת־מרחבים של מרחב ליניארי V. אומרים על תת־מרחב W של V כי הוא **הסכום הישר** של $U_1,\dots,U_n$, ומסמנים

$$W = U_1 \oplus \dots \oplus U_n$$

אם ורק אם מתקיימים שני תנאים:

א. $W = U_1 + U_2 + \dots + U_n$

ב. לכל וקטור $w \in W$ יש הצגה **יחידה** מהצורה

$$w = u_1 + \dots + u_n$$

כאשר $u_1 \in U_i$ לכל i $(1 \le i \le n)$.

הערה

בשל תכונת החילופיות, אין הסכום תלוי בסדר המחוברים.

משפט הבוחן הבא, 7.7.5, מכליל את משפט הבוחן הראשון לסכום ישר (משפט 7.7.2):

משפט 7.7.5

יהי V מרחב ליניארי, ויהיו $U_1,\dots,U_n$ תת־מרחבים של V.

נסמן את הסכום של כל התת־מרחבים U_i $(1 \le i \le n)$, **פרט** ל־ U_j, כך:

$$U_1 + \dots + \hat{U}_j + \dots + U_n$$

(שימו לב, התת־מרחב שמעליו מופיע הסימן $\wedge$ הוא זה **שאינו** משתתף בסכום.)

אז

$$W = U_1 \oplus \dots \oplus U_n$$

אם ורק אם מתקיימים שני התנאים:

א. $V = U_1 + \dots + U_n$

ב. לכל j $(1 \le j \le n)$:

$$U_j \cap (U_1 + \dots + \hat{U}_j + \dots + U_n) = \{0\}$$

משפט 7.7.6

יהי V מרחב לינארי, ויהיו $U_1,\ldots,U_n$ תת־מרחבים של V.

אז

$$V = U_1 \oplus \ldots \oplus U_n$$

אם ורק אם מתקיימים שני התנאים:

א. $V = U_1 + \ldots + U_n$

ב. ההצגה $\underset{U_1}{\underset{\in}{0}} + \ldots + \underset{U_n}{\underset{\in}{0}} = 0$ היא ההצגה היחידה של 0 כסכום של וקטורים מתוך $U_1,\ldots,U_n$.

שאלה 7.7.6

א. הוכיחו את משפט 7.7.5.

ב. הוכיחו את משפט 7.7.6.

התשובה בעמוד 233

שאלה 7.7.7

א. מצאו שלושה תת־מרחבים U_1,U_2,U_3 של $\mathbb{R}^2$, שעבורם מתקיימות שלוש הדרישות שלהלן גם יחד:

1. $\mathbb{R}^2 = U_1 + U_2 + U_3$
2. $U_1 \cap U_2 = U_2 \cap U_3 = U_3 \cap U_1 = \{\mathbf{0}\}$
3. $\mathbb{R}^2$ **אינו** הסכום הישר של U_1, U_2 ו־U_3.

ב. נמקו מדוע הדוגמה שבחלק א אינה סותרת את משפט הבוחן 7.7.5.

התשובה בעמוד 235

שאלה 7.7.8

נתבונן בוקטורים הבאים במרחב $\mathbb{R}^4$:

$$\mathbf{e}_1 = (1,0,0,0)\ ,\quad \mathbf{e}_2 = (0,1,0,0)\ ,\quad \mathbf{e}_3 = (0,0,1,0)\ ,\quad \mathbf{e}_4 = (0,0,0,1)$$

$$\mathbf{d}_1 = (1,1,0,0)\ ,\quad \mathbf{d}_2 = (0,1,1,0)\ ,\quad \mathbf{d}_3 = (0,0,1,1)$$

א. הוכיחו כי:

$$\mathrm{Sp}(\{\mathbf{e}_1,\mathbf{e}_2\}) = \mathrm{Sp}(\{\mathbf{e}_1\}) \oplus \mathrm{Sp}(\{\mathbf{e}_2\})$$

ב. האם מתקיים:

$$\left\{(a_1,2a_2,a_2,0) \mid a_1,a_2 \in \mathbb{R}\right\} = \mathrm{Sp}(\{\mathbf{e}_1,\mathbf{e}_2\}) + \mathrm{Sp}(\{\mathbf{d}_2\})$$

ג. חשבו את הסכום

$$\mathrm{Sp}(\{\mathbf{d}_1\}) + \mathrm{Sp}(\{\mathbf{d}_2\}) + \mathrm{Sp}(\{\mathbf{d}_3\})$$

וקבעו אם סכום זה הוא ישר.

ד. הוכיחו כי

$$\mathbb{R}^4 = \mathrm{Sp}(\{\mathbf{e}_1\}) + \mathrm{Sp}(\{\mathbf{d}_1\}) + \mathrm{Sp}(\{\mathbf{d}_2\}) + \mathrm{Sp}(\{\mathbf{d}_3\})$$

ובדקו אם סכום זה הוא ישר.

ה. הוכיחו כי הסכום

$$\mathrm{Sp}(\{\mathbf{e}_3\}) + \mathrm{Sp}(\{\mathbf{d}_3\})$$

הוא ישר.

ו. הוכיחו כי הסכום

$$\mathrm{Sp}(\{\mathbf{e}_3\}) + \mathrm{Sp}(\{\mathbf{e}_4\})$$

הוא ישר.

ז. הוכיחו כי:

$$\mathrm{Sp}(\{\mathbf{e}_3\}) \oplus \mathrm{Sp}(\{\mathbf{d}_3\}) = \mathrm{Sp}(\{\mathbf{e}_3\}) \oplus \mathrm{Sp}(\{\mathbf{e}_4\})$$

(שימו לב: הסכומים בשני האגפים הם ישרים, לפי הטענות שבחלקים ה, ו של השאלה. שימו לב עוד לכך, שהשוויון מתקיים למרות ש־$\mathrm{Sp}(\{\mathbf{d}_3\}) \neq \mathrm{Sp}(\{\mathbf{e}_4\})$!)

התשובה בעמוד 235

7.8 מרחב הפולינומים ומרחב הפונקציות

סעיף זה הוא סעיף רשות.

בסעיף 7.1 ראינו דוגמאות רבות למרחבים לינאריים. אחת הדוגמאות המעניינות שעסקנו בה היא מרחב הפונקציות הממשיות מעל שדה המספרים הממשיים. כעת נכליל את מה שעשינו, ונתבונן בפונקציות המוגדרות מעל שדה כלשהו F.

נסמן את אוסף כל הפונקציות מ־ F ל־ F ב־ F^F. על אוסף זה נגדיר פעולת חיבור ופעולת כפל בסקלר כך:

בהינתן שתי פונקציות $f, g \in F^F$, **הסכום** $f + g$ הוא הפונקציה ב־ F^F, המקיימת לכל $x \in F$:

$$(f+g)(x) \overset{\text{def}}{=} f(x) + g(x)$$

המכפלה של פונקציה $f \in F^F$ בסקלר $\lambda \in F$ היא הפונקציה ב־ F^F, המקיימת לכל $x \in F$:

$$(\lambda f)(x) \overset{\text{def}}{=} \lambda \cdot f(x)$$

שאלה 7.8.1

הוכיחו כי F^F הוא מרחב לינארי מעל F לגבי הפעולות שהגדרנו.

התשובה בעמוד 239

דוגמה נוספת למרחב לינארי שבה עסקנו, היא מרחב הפולינומים $F[x]$ מעל שדה F. כמו כן, ראינו בסעיף 6.7 כי ניתן **להציב** סקלר $\alpha \in F$ בפולינום $P(x) = a_0 + a_1 x + \ldots + a_n x^n$ ולחשב את ערכו של הסקלר $P(\alpha) \overset{\text{def}}{=} a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n$.

האפשרות להציב סקלרים בפולינום מאפשרת **לפרש פולינומים כפונקציות**:

בהינתן **פולינום** $P(x) = a_0 + a_1 x + \ldots + a_n x^n$, נוכל להתאים לו את **הפונקציה** $f_P : F \to F$, המוגדרת על־ידי $f_P(\alpha) = P(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n$ לכל $\alpha \in F$. באופן זה אנו מקבלים העתקה ממרחב **הפולינומים**, $F[x]$, לתוך מרחב הפונקציות, F^F.

לאור האמור, ניתן להתפתות ולזהות פולינומים עם הפונקציות המתאימות להן. אך כאן טמונה מלכודת. נתבונן בפולינומים הבאים: $P = x,\ Q = x^2$. בוודאי שמדובר בפולינומים שונים, שהרי מעלותיהם שונות. אך האם הפונקציות המתאימות לפולינומים אלה, f_P ו־ f_Q, הן פונקציות שונות? מתברר כי התשובה תלויה בשדה F.

נפתח במקרה שבו $F = \mathbb{R}$ הוא שדה המספרים הממשיים. במקרה זה מתקיים, למשל, $f_P(2) = P(2) = 2$, ואילו $f_Q(2) = Q(2) = 2^2 = 4 \neq 2$, וממילא הפונקציות f_P ו־ f_Q שונות.

לעומת זאת, נתבונן במקרה שבו $F = \mathbb{Z}_2$. כדי לבדוק האם הפונקציות f_P ו־ f_Q מתלכדות, עלינו לבדוק האם הן מקבלות את אותן ערכים עבור כל ערכי התחום, $F = \mathbb{Z}_2$. מאחר שב־ $\mathbb{Z}_2 = \{0,1\}$ יש שני איברים בלבד, אפשר לבדוק לגבי כל איברי השדה. ואמנם, מתקיים $f_P(0) = 0,\ f_Q(1) = 1$, אך גם $f_Q(0) = 0^2 = 0,\ f_Q(1) = 1^2 = 1$. אנו רואים ששתי הפונקציות הן למעשה אותה הפונקציה - פונקציית הזהות על השדה $\mathbb{Z}_2$!

לאור האמור לעיל, אנו למדים שעלינו להיזהר ולהבדיל בין פולינומים לבין **פונקציות פולינומיאליות**.

הגדרה 7.8.1

יהי F שדה ויהי $P \in F[x]$.

הפונקציה $f_P : F \to F$, המוגדרת על־ידי

$$f_P(\alpha) = P(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n \qquad (\text{לכל } \alpha \in F),$$

נקראת **פונקציה פולינומיאלית**.

דוגמה

יהי F שדה כלשהו, ונתבונן **בפונקציה** $g : F \to F$ המוגדרת על ידי:

$$g(x) = 1 + x + (x+1)^2$$

כעת נתבונן בפולינום $P(x) = 2 + 3x + x^2$.

לכל $\alpha \in F$ מתקיים

$$f_P(\alpha) = P(\alpha) = 2 + 3\alpha + \alpha^2 = 1 + \alpha + 1 + 2\alpha + \alpha^2 = 1 + \alpha + (1+\alpha)^2$$

כאשר בשוויון האחרון השתמשנו בתכונות הרגילות של החיבור והכפל בשדה. קיבלנו, אם כן, כי הפונקציה g מתלכדת עם הפונקציה f_P, ולכן g היא פונקציה פולינומיאלית.

◄

ברצוננו לתהות כעת על טיבה של פונקציה זו:

כאשר $F = \mathbb{R}$, סביר שנתקלתם בפונקציות מטיפוס זה (וייתכן אף שחקרתם את תכונותיה הגיאומטריות - לפונקציה זו מתאימה **פרבולה** במישור).

לעומת זאת, כאשר $F = \mathbb{Z}_2$, טיבה של פונקציה זו עשוי להפתיע אתכם. תחילה נבחין, כי בשדה זה מתקיים $3 = 1+1+1 = 1$, $2 = 1+1 = 0$, ולכן במקרה זה הפולינום $P(x) = 2 + 3x + x^2$ **שווה** לפולינום $0 + 1\cdot x + x^2 = x + x^2$.

מכאן, ש־ $f_P(0) = 0 + 0^2 = 0$, אך גם $f_P(1) = 1 + 1^2 = 1 + 1 = 0$. כלומר, הפונקציה המתאימה לפולינום P היא פונקציית האפס, למרות ש־ P אינו פולינום האפס.

שאלה 7.8.2

תארו את הפונקציה f_P המתאימה לפולינום $P(x) = 1 + 2x + x^3$, במקרים $F = \mathbb{Z}_2$ ו־$F = \mathbb{Z}_3$.

התשובה בעמוד 239

ראינו, אם כן, כי באופן כללי ייתכן שלפולינומים שונים מתאימות פונקציות זהות. אבל, מסתבר שכאשר השדה שמעליו אנו עובדים הוא שדה אינסופי, אין הדבר אפשרי – זוהי מסקנה 6.8.4 בפרק הקודם. נדגיש את המקרה הממשי והמרוכב של מסקנה זו:

משפט 7.8.2

נניח כי $F = \mathbb{R}$ או $F = \mathbb{C}$. אם $P,Q \in F[x]$ הם זוג פולינומים שונים, אזי הפונקציות f_P ו־f_Q הן פונקציות שונות.

לאור משפט 7.8.2, יש **המזהים** במקרה הממשי/מרוכב בין פולינום והפונקציה המתאימה לו – כלומר, יש הרואים פולינום כאילו הוא עצמו הפונקציה הפולינומיאלית המתאימה לו. מכיוון שענייננו בסעיף זה הוא דיון כללי במהותם של פולינומים, נקפיד להבחין בין פולינום לפונקציה.

משפט 7.8.3

אוסף כל הפונקציות הפולינומיאליות ב־F^F הוא תת־מרחב של F^F.

שאלה 7.8.3

הוכיחו את משפט 7.8.3.

התשובה בעמוד 240

לאור משפט 7.8.3, מתבקש לשאול: האם תת־מרחב הפונקציות הפולינומיאליות ב־F^F הוא תת־מרחב ממש, או שהוא המרחב כולו? כלומר, האם קיימות פונקציות שאינן פולינומיאליות? במקרה הממשי התשובה חיובית. למשל, ניתן להראות (ולא נעשה זאת כאן) שהפונקציה הטריגונומטרית $f(x) = \sin x$ אינה פולינומיאלית.[1] דוגמה נוספת היא הפונקציה $f \in \mathbb{R}^{\mathbb{R}}$ המוגדרת על־ידי $f(x) = x^{-1}$ לכל x ממשי שאינו אפס, ו־$f(0) = 0$ – זו איננה פונקציה פולינומיאלית (גם עובדה זו לא נוכיח). ייתכן שהערות אלה נראות כמיותרות, שהרי פונקציות פולינומיאליות הן פונקציות בעלות צורה מיוחדת – האין זה ברור מאליו שלא כל פונקציה היא כזאת? כלל וכלל לא!

1 קוראים יודעי חשבון אינפיניטסימלי יוכלו גם להשתכנע בקלות כי כל פונקציה ממשית שאינה רציפה אינה פולינומיאלית.

שאלה 7.8.4

יהי F שדה ותהי $f \in F^F$ מוגדרת על־ידי $f(x) = x^{-1}$ לכל סקלר x שאינו אפס, וכן $f(0) = 0$.
האם פונקציה זו היא פונקציה פולינומיאלית, כאשר:

א. $F = \mathbb{Z}_2$?
ב. $F = \mathbb{Z}_3$?

התשובה בעמוד 240

בשאלה 7.8.4 ראיתם דוגמה לפונקציה שאינה "נראית" פולינומיאלית, ובכל זאת היא כזאת. מתברר שכאשר השדה F סופי, כל הפונקציות ב־ F^F הן פולינומיאליות. נסיים סעיף זה בהוכחת משפט מפתיע זה. לשם כך נזדקק ללמה הבאה:

למה 7.8.4

יהי F שדה. מכפלה של פונקציות פולינומיאליות ב־ F^F היא פונקציה פולינומיאלית.

שאלה 7.8.5

הוכיחו את למה 7.8.4.

התשובה בעמוד 240

למה 7.8.5

יהי F שדה סופי, ויהיו $a,b \in F$. אזי הפונקציה המוגדרת על־ידי $f(a) = b$ ו־ $f(a') = 0$ לכל $a' \neq a$ ב־ F היא פונקציה פולינומיאלית.

הוכחה

מאחר ש־ F הוא שדה סופי, נוכל לרשום את קבוצת איבריו כך: $F = \{a_1,...,a_n\}$, כאשר $a_1 = a$.
יהי c הסקלר: $c = a_1 - b(a_1 - a_2)^{-1}(a_1 - a_3)^{-1} \cdot ... \cdot (a_1 - a_n)^{-1}$, ונתבונן בפונקציה $g \in F^F$ המוגדרת על־ידי $g(x) = (x-c)(x-a_2) \cdot ... \cdot (x-a_n)$.

כל אחת מן הפונקציות $x-c, x-a_2,...,x-a_n$ היא בבירור פונקציה פולינומיאלית, ולכן לפי למה 7.8.4 גם g היא כזאת.

נותר להראות ש־ $g = f$:
אכן, לכל $i \neq 1$ מתקיים

$$g(a_i) = (a_i - c)(a_i - a_2) \cdot ... \cdot (a_i - a_i) \cdot ... \cdot (a_i - a_n) = 0 = f(a_i)$$

ואילו:

$$g(a) = g(a_1) = (a_1 - c)(a_1 - a_2) \cdot \ldots \cdot (a_1 - a_n)$$
$$= b(a_1 - a_2)^{-1}(a_1 - a_3)^{-1} \cdot \ldots \cdot (a_1 - a_n)^{-1}(a_1 - a_2) \cdot \ldots \cdot (a_1 - a_n) = b$$

נסיק ש־ $g = f$, ולכן f היא פונקציה פולינומיאלית.

מ.ש.ל.

משפט 7.8.6

יהי F שדה סופי. כל הפונקציות ב־ F^F הן פולינומיאליות.

הוכחה

תהי $g \in F^F$. נרשום את איברי F כך: $F = \{a_1, \ldots, a_n\}$. נסמן $b_i = g(a_i)$ לכל i, ונגדיר את הפונקציה g_i על־ידי $g_i(a_i) = b_i$ ו־ $g_i(a_j) = 0$, לכל $j \neq i$. אזי לכל i מתקיים:

$$g(a_i) = b_i = 0 + \ldots + 0 + b_i + 0 \ldots + 0$$
$$= g_1(a_i) + \ldots + g_{i-1}(a_i) + g_i(a_i) + g_{i+1}(a_i) \ldots + g_n(a_i)$$
$$= (g_1 + \ldots + g_n)(a_i)$$

כלומר, הפונקציה g היא סכום הפונקציות $g_1, \ldots, g_n$. כל אחת מפונקציות אלה היא פונקציה פולינומיאלית, לפי למה 7.8.5. לפי משפט 7.8.3, אוסף כל הפונקציות הפולינומיאליות סגור לחיבור, ולכן גם g היא פונקציה פולינומיאלית, כפי שרצינו להראות.

מ.ש.ל.

תשובות לשאלות בפרק 7

תשובה 7.1.1 **השאלה בעמוד 157**

כל התכונות של F^n כמרחב ליניארי מעל F נובעות במישרין מההגדרות ומהמשפטים שבסעיף 1.3 – עיינו במשפטים 1.3.3 ו־1.3.5.

בפרט נכון הדבר לגבי המרחב F^1. אולם F^1 הוא אוסף כל ה"יחידיות" הסדורות, וכפי שעשינו עד כה – אנו מזהים מרחב זה עם השדה F עצמו. כלומר, F הוא מרחב ליניארי מעל עצמו, וכמובן גם $\mathbb{R}$ הוא מרחב ליניארי מעל $\mathbb{R}$.

תשובה 7.1.2 **השאלה בעמוד 157**

א. תכונות החיבור ב־ $\mathbb{R}$ כמרחב ליניארי מתקיימות, שכן אלה הן תכונות החיבור ב־ $\mathbb{R}$ כשדה. תכונות כפל בסקלר **רציונלי** מתקיימות, שכן הן נכונות לכפל במספרים ממשיים, כי $\mathbb{R}$ הוא מרחב ליניארי מעל $\mathbb{R}$ (ראו בשאלה הקודמת), ובפרט הן נכונות לכפל במספרים רציונליים. טיעון זה תקף גם אם נחליף את $\mathbb{R}$ בשדה כלשהו F, ואת $\mathbb{Q}$ בתת־שדה כלשהו של F. אם כך, כל שדה הוא מרחב ליניארי מעל כל תת־שדה שלו. בפרט, שדה המספרים המרוכבים הוא מרחב ליניארי מעל $\mathbb{R}$, וכמובן $\mathbb{R}$ הוא מרחב ליניארי מעל $\mathbb{Q}$.

ב. $\mathbb{Q}$ אינו מרחב ליניארי מעל $\mathbb{R}$, כי, למשל, תכונת הסגירות לגבי הכפל בסקלר אינה מתקיימת בו. לדוגמה, 1 הוא איבר ב־ $\mathbb{Q}$, וכפל בסקלר $\sqrt{2}$ (השייך ל־ $\mathbb{R}$) ייתן $\sqrt{2}\cdot 1=\sqrt{2}$ שאינו שייך ל־ $\mathbb{Q}$.

ג. בדומה לסעיף א – כל הדרישות בהגדרת מרחב ליניארי מתקיימות ממילא לאור קיומן בשדה הגדול יותר.

תשובה 7.1.3 **השאלה בעמוד 157**

$\mathbf{M}_{m\times n}^F$ הוא מרחב ליניארי מעל F לגבי הפעולות המתוארות לפני השאלה, על־סמך המשפטים 3.3.3 ו־3.3.5 בפרק 3.

תשובה 7.1.4 **השאלה בעמוד 158**

א. תכונות החיבור א–ה שבהגדרת המרחב הליניארי, מתקיימות ב־ $\mathbf{M}_{m\times n}^C$ כבכל מרחב $\mathbf{M}_{m\times n}^F$ (ראו שאלה 7.1.3).

תכונות הכפל בסקלר מתקיימות לגבי הכפל בסקלרים ממשיים, שהרי הם בפרט מספרים מרוכבים.

ב. $\mathbf{M}_{m\times n}^{\mathbb{R}}$ אינו סגור לגבי הכפל בסקלרים מרוכבים. נתבונן, למשל, במטריצה:

$$E^{(1,1)}=\begin{bmatrix}1 & 0 & \dots & 0\\ 0 & 0 & \dots & \vdots\\ \vdots & \vdots & & \vdots\\ 0 & 0 & \dots & 0\end{bmatrix}$$

מטריצה זו נמצאת ב־ $\mathbf{M}_{m\times n}^{\mathbb{R}}$. כפל של $E^{(1,1)}$ בסקלר המרוכב i ייתן

$$i \cdot E^{(1,1)} = \begin{bmatrix} i & 0 & \dots & 0 \\ 0 & 0 & \dots & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}$$

ומטריצה זו אינה נמצאת ב־ $\mathbf{M}_{m\times n}^{\mathbb{R}}$, שהרי לא כל רכיביה ממשיים.

לכן $\mathbf{M}_{m\times n}^{\mathbb{R}}$ אינו מרחב לינארי מעל $\mathbb{C}$.

תשובה 7.1.5 **השאלה בעמוד 158**

קבוצה זו אינה סגורה לגבי פעולת החיבור. למשל $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ ו־ $\begin{bmatrix} -1 & -2 \\ -3 & -4 \end{bmatrix}$ שתיהן מטריצות בקבוצה,

אולם סכומן הוא המטריצה $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ שכל איבריה שווים, ולכן אינה בקבוצה.

לכן הקבוצה שבשאלה אינה מרחב לינארי מעל $\mathbb{R}$.

תשובה 7.1.6 **השאלה בעמוד 158**

S – קבוצת המטריצות הריבועיות האלכסוניות מסדר n מעל F.

לכל $A,B \in S$:

$$A +_S B = AB$$

לכל $\lambda \in F,\ A \in S$:

$$\lambda \cdot_S A = \lambda A$$

נבדוק אם S היא מרחב לינארי מעל F.

מכיוון שקשה להבחין ממבט ראשון בתכונה של מרחב לינארי שאינה מתקיימת, נעבור על התכונות אחת אחת. אם נגיע לתכונה שאינה מתקיימת – נסיק ש־ S אינה מרחב לינארי מעל F, ואם כל התכונות מתקיימות – נסיק כמובן ש־ S היא מרחב לינארי מעל F בפעולות שלעיל.

נפתח בבדיקה של תכונות החיבור:

תהיינה A, B ו־ C מטריצות ב־ S:

$$A = \begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{bmatrix},\quad B = \begin{bmatrix} b_1 & & 0 \\ & \ddots & \\ 0 & & b_n \end{bmatrix},\quad C = \begin{bmatrix} c_1 & & 0 \\ & \ddots & \\ 0 & & c_n \end{bmatrix}$$

א. בפרק 3 הוכחנו כי מכפלת מטריצות אלכסוניות היא מטריצה אלכסונית, ולכן S סגורה לחיבור וקטורים.

ב. קיבוציות החיבור ב־ S:

$$(A +_S B) +_S C = (AB) +_S C = (AB)C = A(BC) = A +_S (BC) = A +_S (B +_S C)$$

כאן הסתמכנו על קיבוציות הכפל ב־ $M_{n\times n}^{F}$.

ג. חילופיות החיבור ב־ S:

$$A +_S B = AB = \begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{bmatrix}\begin{bmatrix} b_1 & & 0 \\ & \ddots & \\ 0 & & b_n \end{bmatrix} = \begin{bmatrix} a_1b_1 & & 0 \\ & \ddots & \\ 0 & & a_nb_n \end{bmatrix}$$

$$= \begin{bmatrix} b_1a_1 & & 0 \\ & \ddots & \\ 0 & & b_na_n \end{bmatrix} = BA = B +_S A$$

כאן הסתמכנו על קיבוציות הכפל ב־ F.

ד. קיים ב־ S איבר ניטרלי ביחס לחיבור, והוא המטריצה $I = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$, שכן:

$$A +_S I = AI = A$$

ה. אבל, לא לכל מטריצה אלכסונית ב־ S יש איבר נגדי ביחס לחיבור. למשל, מטריצת האפס O שייכת ל־ S, ולכל מטריצה A ב־ S, $O +_S A = OA = O$, ולכן לא קיימת מטריצה A ב־ S שעבורה $O +_S A = I$. לכן אין ל־ O איבר נגדי ביחס לחיבור, ומשום כך S **אינו** מרחב ליניארי מעל F לגבי הפעולות שהוגדרו.

תשובה 7.1.7 **השאלה בעמוד 158**

א. את הסגירות של T, קבוצת הפתרונות למערכת משוואות ליניארית הומוגנית, לגבי החיבור ולגבי הכפל בסקלר, הוכחנו בפרק 1 בשאלה 1.5.7.

ב. תכונות הקיבוציות והחילופיות של חיבור ב־ T, וכן תכונות הכפל בסקלר, נובעות מקיום תכונות אלה ב־ F^n.

ג. קיים איבר ניטרלי ביחס לחיבור ב־ T, שכן איבר האפס של F^n שייך ל־ T.

ד. לכל $\mathbf{a} \in T$ גם $(-1)\mathbf{a} \in T$ על פי א. אולם $(-1)\mathbf{a} = -\mathbf{a}$, ולכן קיים ל־ $\mathbf{a}$ איבר נגדי ב־ T.

תשובה 7.1.8 **השאלה בעמוד 159**

קבוצת הפתרונות של מערכת אי־הומוגנית אינה סגורה לגבי החיבור ולגבי הכפל בסקלר (ראו שאלה 1.5.8 בפרק 1), וממילא אינה מרחב ליניארי.

תשובה 7.1.9 **השאלה בעמוד 159**

קבוצה זו אינה סגורה ביחס לחיבור, שכן, למשל x^4 ו־ $-x^4$ שניהם פולינומים ממעלה 4, אולם סכומם הוא פולינום האפס שאינו ממעלה רביעית.

תשובה 7.1.10 **השאלה בעמוד 159**

א. כפל פולינום שמקדמיו שלמים, בסקלר ממשי, איננו בהכרח פולינום שמקדמיו שלמים. למשל, כפל הפולינום $P(x) = x$ ב־ $\frac{1}{2}$ ייתן $\frac{1}{2}x$. לכן, אוסף הפולינומים שמקדמיהם שלמים אינו מרחב ליניארי מעל $\mathbb{R}$.

ב. $\mathbb{C}[x]$ הוא מרחב לינארי מעל $\mathbb{R}$, שכן:

1. כל תכונות החיבור של מרחב לינארי מתקיימות ב־$\mathbb{C}[x]$, כפי שהן מתקיימות בכל מרחב פולינומים $F[x]$.
2. $\mathbb{C}[x]$ הוא מרחב לינארי מעל $\mathbb{C}$, ולכן מתקיימות בו כל התכונות של כפל בסקלרים **מרוכבים**, ובפרט מתקיימות בו תכונות הכפל בסקלרים **ממשיים**.

ג. $\mathbb{R}[x]$ אינו מרחב לינארי מעל $\mathbb{C}$, שכן כפל של פולינום שונה מ־ 0 שמקדמיו ממשיים במספר מרוכב שאינו ממשי, נותן פולינום שמקדמיו אינם ממשיים, כלומר $\mathbb{R}[x]$ אינו סגור לכפל בסקלר מרוכב.

תשובה 7.1.11 **השאלה בעמוד 159**

$$K = \left\{P(x) \in \mathbb{R}[x] \;\middle|\; P(1) = 0\right\}$$

K הוא מרחב לינארי מעל $\mathbb{R}$, שכן:

א. K סגורה ביחס לחיבור: אכן, אם $P,Q \in K$, אז $0 = 0 + 0 = P(1) + Q(1) = (P+Q)(1)$, ולכן $P(x) + Q(x) \in K$.

ב. עבור $P \in K$ ו־ λ **ממשי**, $(\lambda P)(1) = \lambda P(1) = \lambda 0 = 0$ ולכן גם $\lambda P \in K$.

ג. הקיום של תכונות הקיבוציות והחילופיות של החיבור ב־ K, ושל תכונות הכפל בסקלר של איברי K, מובטח בשל קיום תכונות אלה במרחב $\mathbb{R}[x]$.

ד. פולינום ה־ 0 נמצא ב־ K והוא איבר ניטרלי ביחס לחיבור ב־ K.

ה. אם $P \in K$, אז גם $-P \in K$, שכן $-P(1) = 0$, ולכן לכל איבר ב־ K יש איבר נגדי ב־ K.

תשובה 7.1.12 **השאלה בעמוד 160**

נראה שמתקיימות כל התכונות של החיבור והכפל בסקלר.

נפתח בתכונות החיבור:

תהיינה f, g ו־ h פונקציות כלשהן מ־ $\mathbb{R}$ ל־ $\mathbb{R}$.

א. סגירות ביחס לחיבור:

על פי הגדרת החיבור, $f+g$ גם היא פונקציה מ־ $\mathbb{R}$ ל־ $\mathbb{R}$.

ב. קיבוציות החיבור:

לכל x ב־ $\mathbb{R}$,

$$\begin{aligned}\big((f+g)+h\big)(x) &= (f+g)(x) + h(x)\\ &= f(x) + g(x) + h(x) = f(x) + \big(g(x) + h(x)\big)\\ &= f(x) + (g+h)(x) = \big(f + (g+h)\big)(x)\end{aligned}$$

לכן:

$$(f+g)+h = f+(g+h)$$

ג. חילופיות החיבור:

לכל x ב־ $\mathbb{R}$,

$$(f+g)(x) = f(x)+g(x)$$
$$= g(x)+f(x) = (g+f)(x)$$

כלומר:

$$f+g = g+f$$

ד. איבר ניטרלי ביחס לחיבור:

נסמן ב־ $0(x)$ את הפונקציה הקבועה המתאימה לכל x ממשי את הערך 0.

לכל x ממשי מתקיים:

$$(f+0)(x) = f(x)+0(x) = f(x)+0 = f(x)$$

ולכן:

$$f+0 = f$$

הפונקציה 0 היא, אם כך, איבר ניטרלי ביחס לחיבור.

ה. איברים נגדיים ביחס לחיבור:

עבור פונקציה נתונה f נגדיר את הפונקציה $-f$ על־ידי:

$$(-f)(x) = -f(x)$$

ברור כי לכל x ממשי:

$$(-f+f)(x) = (-f)(x)+f(x) = -f(x)+f(x) = 0 = 0(x)$$

כלומר:

$$-f+f = 0$$

נעבור לתכונות הכפל בסקלר:

תהיינה f, g ו־ h פונקציות כלשהן מ־ $\mathbb{R}$ ל־ $\mathbb{R}$, ו־ λ, μ מספרים ממשיים.

א. על פי הגדרת הכפל בסקלר במרחב שלנו, לכל λ ממשי, λf היא פונקציה מ־ $\mathbb{R}$ ל־ $\mathbb{R}$.

ב. לכל x ממשי,

$$[\lambda(f+g)](x) = \lambda[(f+g)(x)] = \lambda[f(x)+g(x)]$$
$$= \lambda f(x)+\lambda g(x) = (\lambda f)(x)+(\lambda g)(x)$$
$$= (\lambda f+\lambda g)(x)$$

ולכן:

$$\lambda(f+g) = \lambda f+\lambda g$$

ג. לכל x ממשי,

$$[(\lambda+\mu)f](x) = (\lambda+\mu)f(x)$$
$$= \lambda f(x)+\mu f(x) = (\lambda f+\mu f)(x)$$

כלומר:

$$(\lambda + \mu)f = \lambda f + \mu f$$

ד. לכל x ממשי,

$$\left[(\lambda\mu)f\right](x) = (\lambda\mu)f(x) = \lambda\left(\mu f(x)\right)$$
$$= \left[\lambda(\mu f)\right](x)$$

לכן:

$$(\lambda\mu)f = \lambda(\mu f)$$

ה. עבור המספר הממשי 1 מתקיים לכל x ממשי:

$$(1 \cdot f)(x) = 1 \cdot f(x) = f(x)$$

ולכן:

$$1 \cdot f = f$$

תשובה 7.1.13 **השאלה בעמוד 160**

נפתח בתכונות החיבור:

א. סכום של שתי סדרות אינסופיות של מספרים ממשיים אף הוא סדרה אינסופית, ולכן $\mathbb{R}^N$ סגור לחיבור וקטורים.

ב. היות שפעולת החיבור של מספרים ממשיים חילופית, נובע כי:

$$(a_k) + (b_k) = (a_k + b_k) = (b_k + a_k) = (b_k) + (a_k)$$

כלומר, פעולת החיבור של סדרות אינסופיות חילופית.

ג. באופן דומה, היות שפעולת החיבור של המספרים הממשיים קיבוצית, נובע כי פעולת החיבור של סדרות אינסופיות של מספרים ממשיים גם היא קיבוצית (ודאו!).

ד. הסדרה $(0,0,\ldots,0,\ldots)$ היא סדרה אינסופית, ולכל סדרה אינסופית $(a_1,\ldots,a_k,\ldots)$ מתקיים:

$$(a_1,\ldots,a_k,\ldots) + (0,\ldots,0,\ldots) = (a_1 + 0,\ldots,a_k + 0,\ldots) = (a_1,\ldots,a_k,\ldots)$$

ולכן הסדרה $(0,\ldots,0,\ldots)$ היא איבר ניטרלי ביחס לחיבור.

ה. לכל סדרה $(a_1,\ldots,a_k,\ldots)$ מתאימה הסדרה $(-a_1,\ldots,-a_k,\ldots)$, וסכומן הוא הסדרה $(0,\ldots,0,\ldots)$, שהיא האיבר הניטרלי ב־ $\mathbb{R}^N$. כלומר, לכל איבר ב־ $\mathbb{R}^N$ יש איבר נגדי ביחס לחיבור.

נעבור לתכונות הכפל בסקלר:

א. לכל סדרה $(a_1,\ldots,a_k,\ldots)$, ולכל $\lambda \in \mathbb{R}$ מתקיים:

$$\lambda(a_1,\ldots,a_k,\ldots) = (\lambda a_1,\ldots,\lambda a_k,\ldots)$$

ולכן $\mathbb{R}^N$ סגורה לכפל בסקלר.

ב. אם $(a_1,\ldots,a_k,\ldots)$ ו־ $(b_1,\ldots,b_k,\ldots)$ הן סדרות אינסופיות של מספרים ממשיים, ואם $\lambda \in \mathbb{R}$, אז:

$$\begin{aligned}
&\lambda\left[(a_1,\ldots,a_k,\ldots)+(b_1,\ldots,b_k,\ldots)\right]\\
&=\lambda(a_1+b_1,\ldots,a_k+b_k,\ldots)\\
&=\left(\lambda(a_1+b_1),\ldots,\lambda(a_k+b_k),\ldots\right)\\
&=\left(\lambda a_1+\lambda b_1,\ldots,\lambda a_k+\lambda b_k,\ldots\right)=\left(\lambda a_1,\ldots,\lambda a_k,\ldots\right)+\left(\lambda b_1,\ldots,\lambda b_k,\ldots\right)\\
&=\lambda\left(a_1,\ldots,a_k,\ldots\right)+\lambda\left(b_1,\ldots,b_k,\ldots\right)
\end{aligned}$$

ג. אם $(a_1,\ldots,a_k,\ldots)$ סדרה אינסופית, ואם $\lambda,\mu \in \mathbb{R}$, אז:

$$\begin{aligned}
&(\lambda+\mu)(a_1,\ldots,a_k,\ldots)\\
&=((\lambda+\mu)a_1,\ldots,(\lambda+\mu)a_k,\ldots)\\
&=(\lambda a_1+\mu a_1,\ldots,\lambda a_k+\mu a_k,\ldots)\\
&=(\lambda a_1,\ldots,\lambda a_k,\ldots)+(\mu a_1,\ldots,\mu a_k,\ldots)\\
&=\lambda(a_1,\ldots,a_k,\ldots)+\mu(a_1,\ldots,a_k,\ldots)
\end{aligned}$$

ד. אם $(a_1,\ldots,a_k,\ldots)$ סדרה אינסופית ו־ λ,μ מספרים ממשיים, אז:

$$\begin{aligned}
&(\lambda\mu)(a_1,\ldots,a_k,\ldots)=((\lambda\mu)a_1,\ldots,(\lambda\mu)a_k,\ldots)\\
&=\left(\lambda(\mu a_1),\ldots,\lambda(\mu a_k),\ldots\right)=\lambda(\mu a_1,\ldots,\mu a_k,\ldots)=\lambda\left(\mu(a_1,\ldots,a_k,\ldots)\right)
\end{aligned}$$

ה. $1\cdot(a_1,\ldots,a_k,\ldots)=(a_1,\ldots,a_k,\ldots)$.

מכאן נובע כי $\mathbb{R}^N$ מרחב ליניארי מעל $\mathbb{R}$.

תשובה 7.2.1 **השאלה בעמוד 161**

בהוכחה נעשה שימוש חוזר בתכונת הקיבוציות של החיבור.

א.

$$\begin{aligned}
v_1+\left(v_2+(v_3+v_4)\right)&=(v_1+v_2)+(v_3+v_4)\\
&=\left((v_1+v_2)+v_3\right)+v_4
\end{aligned}$$

ב.

$$\begin{aligned}
&\left(\left((v_1+v_2)+v_3\right)+v_4\right)+v_5=\left((v_1+v_2)+v_3\right)+(v_4+v_5)\\
&=\left((v_1+v_2)+\left(v_3+(v_4+v_5)\right)\right)=v_1+\left(v_2+\left(v_3+(v_4+v_5)\right)\right)
\end{aligned}$$

תשובה 7.2.2 **השאלה בעמוד 161**

א.

$$v_1 + v_2 + v_3 + v_4 \underset{\downarrow}{=} v_1 + (v_2 + v_3) + v_4$$

על פי תכונת הקיבוציות
המוכללת, ניתן להכניס סוגריים
בכל סדר שהוא

$$\underset{\downarrow}{=} v_1 + \big((v_3 + v_2) + v_4\big) \underset{\downarrow}{=} v_1 + \big(v_3 + (v_2 + v_4)\big)$$

חילופיות קיבוציות

$$\underset{\downarrow}{=} v_1 + \big(v_3 + (v_4 + v_2)\big) \underset{\downarrow}{=} v_1 + v_3 + v_4 + v_2$$

חילופיות
בשל הקיבוציות המוכללת
ניתן לוותר על הסוגריים

ב. ההוכחה בסעיף הקודם מתאימה גם לחיבור בשדה. תכונות הקיבוציות והחילופיות שבהן מדובר בסעיף זה תהיינה הפעם תכונות של החיבור בשדה.

תשובה 7.2.3 **השאלה בעמוד 162**

א. נוכיח באינדוקציה על מספר הסקלרים n.

עבור $n = 1$:

$$\lambda_1 \cdot v = \lambda_1 \cdot v$$

נניח שהטענה נכונה עבור $n = k$, ונוכיח אותה עבור $n = k + 1$:

$$(\lambda_1 + \ldots + \lambda_k + \lambda_{k+1})v = \big[(\lambda_1 + \ldots + \lambda_k) + \lambda_{k+1}\big]v$$

$$\underset{\downarrow}{=} (\lambda_1 + \ldots + \lambda_k)v + \lambda_{k+1}v \underset{\downarrow}{=} \lambda_1 v + \ldots + \lambda_k v + \lambda_{k+1}v$$

תכונת הפילוג
הנחת האינדוקציה
של כפל בסקלר

ב. נוכיח באינדוקציה על מספר הוקטורים n.

עבור $n = 1$:

$$\lambda v_1 = \lambda v_1$$

נניח שהטענה נכונה עבור $n = k$, ונוכיח אותה עבור $n = k + 1$:

$$\lambda(v_1 + \ldots + v_{k+1})v = \lambda\big((\mathrm{v}_1 + \ldots + v_k) + v_{k+1}\big)$$

$$\underset{\downarrow}{=} \lambda(v_1 + \ldots + v_k) + \lambda v_{k+1} \underset{\downarrow}{=} \lambda v_1 + \ldots + \lambda v_k + \lambda v_{k+1}$$

תכונת הפילוג
הנחת האינדוקציה
של כפל בסקלר

תשובה 7.2.4 **השאלה בעמוד 164**

.1

$$\lambda v + (-\lambda)v \underset{\downarrow}{=} \big[\lambda + (-\lambda)\big]v = 0v = 0$$

פילוג

מכאן ש־ $(-\lambda)v$ הוא האיבר הנגדי של λv , כלומר:

$$(-\lambda)v = -(\lambda v)$$

.2

$$\lambda v + \lambda(-v) \underset{\substack{\uparrow \\ \text{פילוג}}}{=} \lambda[v + (-v)] = \lambda \cdot 0 = 0$$

לכן $\lambda(-v)$ הוא האיבר הנגדי של λv, כלומר:

$$\lambda(-v) = -(\lambda v)$$

תשובה 7.2.5

השאלה בעמוד 164

א. לאור יחידות האיבר הנגדי, מן השוויון

$$v + (-v) = 0$$

אנו יכולים להסיק ש־ v הוא האיבר הנגדי היחיד של $-v$, כלומר:

$$v = -(-v)$$

ב.

$$(u+v) + [(-u) + (-v)] \underset{\substack{\uparrow \\ \text{קיבוציות וחילופיות}}}{=} [u + (-u)] + [v + (-v)]$$

$$= 0 + 0 = 0$$

מכאן ש־ $[(-u) + (-v)]$ הוא האיבר הנגדי של $u + v$, כלומר:

$$(-u) + (-v) = -(u + v)$$

תשובה 7.2.6

השאלה בעמוד 165

א.

$$u - (v + w) \underset{\substack{\uparrow \\ \text{הגדרת ההפרש}}}{=} u + [-(v + w)]$$

$$= u + [(-v) + (-w)] = [u + (-v)] + (-w) = (u - v) - w$$

ב.

$$u - (v - w) = u + \left[-\left(v + (-w)\right)\right]$$

$$= u + \left[(-v) + \left(-(-w)\right)\right] = u + \left((-v) + w\right)$$

$$= \left(u + (-v)\right) + w = (u - v) + w$$

ג. 1. אם $v = u$, אז:

$$u - v = u - u = u + (-u) = 0$$

2. נניח $u - v = 0$, כלומר $u + (-v) = 0$, ולכן u הוא הנגדי של $-v$.
כלומר

$$u = -(-v)$$

ולכן:

$$u = v$$

תשובה 7.3.1 **השאלה בעמוד 166**

א. U הוא תת־מרחב של V, ולכן הוא עצמו מרחב לינארי, ויש בו איבר ניטרלי שנסמנו $0'$. אז:

$$0' + 0' = 0'$$

שוויון זה הוא, כמובן, גם שוויון במרחב V, ולכן:

$$0' = 0$$

$0' \in U$ ולכן גם $0 \in U$, וברור שהוא האיבר הניטרלי ביחס לחיבור ב־ U.

ב. יהי v איבר ב־ U ונניח ש־ u הוא איבר נגדי ל־ v ב־ U.
אזי:

$$v + u = 0$$

שוויון זה הוא, כמובן, גם שוויון ב־ V, ולכן בשל יחידות האיבר הנגדי ב־ V:

$$u = -v$$

אבל $u \in U$, כלומר $-v \in U$, וברור שהוא האיבר הנגדי ל־ v ב־ U.

תשובה 7.3.2 **השאלה בעמוד 167**

א. נניח שלכל $w \in W$ ו־ $\lambda \in F$, גם $\lambda w \in W$. בפרט, לכל $w \in W$, $(-1)w \in W$.
אולם $(-1)w = -w$, ולכן לכל $w \in W$ גם $-w \in W$.

ב. התנאי (3) נובע מ־(2) רק כאשר הקבוצה W **אינה ריקה**. במקרה כזה קיים w ב־ W, ועל פי (2) גם $0 \cdot w \in W$. אולם $0 \cdot w = 0$, ולכן $0 \in W$. אולם כאשר הקבוצה W ריקה, ברור שוקטור האפס אינו איבר שלה ו־(3) אינו מתקיים.

תשובה 7.3.3 **השאלה בעמוד 167**

התנאי א, $W \neq \phi$, זהה בשני המשפטים. נשאר להוכיח שקיום התנאים ב ו־ג במשפט 7.3.2 שקול לקיום התנאי ב במשפט $7.3.2'$.

1. נניח שמתקיימים התנאים ב ו־ג במשפט 7.3.2, כלומר, W סגורה לגבי החיבור ולגבי הכפל בסקלר, ויהיו $w_1, w_2 \in W$ ו־ $\lambda_1, \lambda_2 \in F$. אז, בשל הסגירות לגבי הכפל בסקלר, $\lambda_1 w_1, \lambda_2 w_2 \in W$, ובשל הסגירות לגבי החיבור,

$$\lambda_2 w_2 + \lambda_1 w_1 \in W$$

וזהו תנאי ב במשפט $7.3.2'$.

2. נניח שמתקיים תנאי ב במשפט $7.3.2'$, אז בפרט עבור $w_1, w_2 \in W$ מתקיים $1 \cdot w_1 + 1 \cdot w_2 \in W$, כלומר:

$$w_1 + w_2 \in W$$

כמו כן מתקיים, בפרט, שלכל $w \in W$, $\lambda \in F$, $\lambda w + 0w \in W$, כלומר

$$\lambda w \in W$$

ואלה הם תנאים ב ו־ג במשפט 7.3.2.

תשובה 7.3.4 **השאלה בעמוד 167**

א.

$$W = \left\{(a_1,\ldots,a_n) \in \mathbb{R}^n \;\middle|\; a_1 = 0\right\}$$

1. וקטור האפס מוכל ב־ W ולכן W אינה ריקה.

2. אם $\mathbf{a} = (a_1,\ldots,a_n)$ ו־ $\mathbf{b} = (b_1,\ldots,b_n)$ ב־ W, אז $a_1 = b_1 = 0$.

$$\mathbf{a} + \mathbf{b} = (a_1 + b_1,\ldots,a_n + b_n)$$

אולם $a_1 = b_1 = 0 + 0 = 0$, ולכן $\mathbf{a} + \mathbf{b} \in W$.

3. אם $\mathbf{a} = (a_1,\ldots,a_n)$ נמצא ב־ W ו־ λ סקלר, אז:

$$\lambda\mathbf{a} = (\lambda a_1,\ldots,\lambda a_n)$$

מכיוון ש־ $\lambda a_1 = \lambda 0 = 0$, הרי גם $\lambda\mathbf{a} \in W$.

מסקנה

W היא תת־מרחב של $\mathbb{R}^n$.

ב.

$$W_0 = \left\{(a_1,\ldots,a_n) \in \mathbb{R}^n \;\middle|\; \sum_{i=1}^{n} a_i = 0\right\}$$

1. הקבוצה W_0 אינה ריקה, כי, למשל, $(0,\ldots,0) \in W_0$.

2. יהיו $(b_1,\ldots,b_n)$ ו־ $(a_1,\ldots,a_n)$ וקטורים ב־ W_0. אז $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i = 0$, ולכן

$$\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i = 0 + 0 = 0$$

ולכן W_0 סגורה לחיבור וקטורים.

3. אם $(a_1,\ldots,a_n) \in \mathrm{W}$ ו־ λ מספר ממשי כלשהו, אז

$$\lambda(a_1,\ldots,a_n) = (\lambda a_1,\ldots,\lambda a_n)$$

$$\sum_{i=1}^{n} \lambda a_i = \lambda \sum_{i=1}^{n} a_i = \lambda \cdot 0$$

ולכן W_0 סגורה לכפל בסקלר. נסיק ש־ W_0 היא אכן תת־מרחב של $\mathbb{R}^n$.

ג.
$$W_1 = \{\lambda \mathbf{a} | \lambda \in \mathbb{R}\}$$

1. W_1 אינה ריקה, שכן $\mathbf{a} \in W_1$.
2. נראה ש־ W_1 סגורה לגבי החיבור:
אם $\mathbf{c}, \mathbf{d} \in W_1$, אז קיימים סקלרים λ ו־ μ כך ש־
$$\mathbf{c} = \lambda \mathbf{a},\ \mathbf{d} = \mu \mathbf{a}$$
מכיוון ש־
$$\mathbf{c} + \mathbf{d} = \lambda \mathbf{a} + \mu \mathbf{a} = (\lambda + \mu)\mathbf{a}$$
הרי שגם $\mathbf{c} + \mathbf{d}$ הוא כפולה בסקלר של $\mathbf{a}$ ולכן נמצא ב־ W_1.
3. W_1 סגורה לגבי הכפל בסקלר:
יהי $\mathbf{c} = \lambda \mathbf{a}$ וקטור ב־ W_1 ו־ μ סקלר. אזי
$$\mu \mathbf{c} = \mu(\lambda \mathbf{a}) = (\mu\lambda)\mathbf{a}$$
ולכן $\mu \mathbf{c} \in W_1$.

מכאן נסיק ש־ W_1 היא תת־מרחב של $\mathbb{R}^3$. כפי שראינו בפרק 2, התיאור הגיאומטרי של תת־מרחב זה הוא ישר ב־ $\mathbb{R}^3$ שעובר דרך הראשית.

ד.
$$W_2 = \{\lambda \mathbf{a} + \mu \mathbf{b} | \lambda, \mu \in \mathbb{R}\}$$

1. W_2 איננה ריקה. למשל, וקטור האפס המתקבל כצירוף לינארי של $\mathbf{a}$ ו־ $\mathbf{b}$ $(0\mathbf{a} + 0\mathbf{b} = \mathbf{0})$ נמצא ב־ W_2.
2. W_2 סגורה לגבי החיבור. אכן - יהיו $\mathbf{c}, \mathbf{d}$ וקטורים ב־ W_2. קיימים סקלרים λ_1, λ_2 ו־ μ_1, μ_2 כך ש־
$$\mathbf{c} = \lambda_1 \mathbf{a} + \mu_1 \mathbf{b}$$
$$\mathbf{d} = \lambda_2 \mathbf{a} + \mu_2 \mathbf{b}$$
$$\begin{aligned}\mathbf{c} + \mathbf{d} &= \lambda_1 \mathbf{a} + \mu_1 \mathbf{b} + \lambda_2 \mathbf{a} + \mu_2 \mathbf{b} \\ &= (\lambda_1 + \lambda_2)\mathbf{a} + (\mu_1 + \mu_2)\mathbf{b}\end{aligned}$$
ולכן:
$$\mathbf{c} + \mathbf{d} \in W_2$$
3. W_2 סגורה לגבי הכפל בסקלר.
יהי $\mathbf{c}$ וקטור ב־ W_2, ו־ η סקלר. קיימים סקלרים λ ו־ μ כך ש־
$$\mathbf{c} = \lambda \mathbf{a} + \mu \mathbf{b}$$
ולכן:
$$\begin{aligned}\eta \mathbf{c} &= \eta(\lambda \mathbf{a} + \mu \mathbf{b}) = \eta(\lambda \mathbf{a}) + \eta(\mu \mathbf{b}) \\ &= (\eta\lambda)\mathbf{a} + (\eta\mu)\mathbf{b}\end{aligned}$$

כלומר:

$$\eta \mathbf{c} \in W_2$$

התיאור הגיאומטרי של תת־מרחב זה הוא מישור ב־ $\mathbb{R}^3$ שעובר דרך ראשית הצירים.

תשובה 7.3.5 **השאלה בעמוד 168**

א. תת־מרחב חייב להכיל את וקטור האפס, ולכן ישר שהוא תת־מרחב של $\mathbb{R}^2$ חייב להכיל את הראשית. כל ישר המכיל את הראשית הוא אוסף כל הכפולות של וקטור אחד בסקלר, ולכן, כפי שראינו בשאלה הקודמת, הוא תת־מרחב. מכאן שישר ב־ $\mathbb{R}^2$ הוא תת־מרחב אם ורק אם הוא עובר בראשית.

ב. מישור ב־ $\mathbb{R}^3$, שהוא תת־מרחב, חייב להכיל את וקטור האפס, כלומר לעבור בראשית. מישור העובר בראשית הוא אוסף כל הצירופים הליניאריים של שני וקטורים, ולכן כפי שראינו בשאלה הקודמת, הוא תת־מרחב. מכאן שמישור ב־ $\mathbb{R}^3$ הוא תת־מרחב אם ורק אם הוא עובר בראשית.

תשובה 7.3.6 **השאלה בעמוד 168**

א. אם V הוא מרחב ליניארי, אז V הוא בפרט תת־מרחב של עצמו, כי $V \subseteq V$. גם הקבוצה $\{0\}$ היא תת־מרחב, שכן:

1. $\{0\}$ אינה ריקה.
2. $\{0\}$ סגורה לגבי החיבור $(0+0=0)$.
3. $\{0\}$ סגורה לגבי הכפל בסקלר ($\lambda 0 = 0$ לכל סקלר λ).

מאחר שב־ V יש יותר מאיבר אחד, הרי ש־ $V \neq \{0\}$, ולכן יש ל־ V לפחות שני תת־מרחבים.

ב. מרחב המספרים הממשיים $\mathbb{R}$ (כמרחב ליניארי מעל $\mathbb{R}$) מכיל אינסוף איברים. נראה שאין ל־ $\mathbb{R}$ תת־מרחבים פרט ל־ $\mathbb{R}$ ו־ $\{0\}$:

אכן, אם W הוא תת־מרחב של $\mathbb{R}$ שאינו $\{0\}$, אז קיים ב־ W וקטור $v \neq 0$. מאחר ש־ W תת־מרחב, הוא בפרט סגור לכפל בסקלר, ולכן נמצאות ב־ W כל הכפולות של v במספרים ממשיים, ומאחר ש־ $v \neq 0$, הרי אוסף כל הכפולות הללו הוא המרחב $\mathbb{R}$,[1] כלומר $W = \mathbb{R}$.

מכאן שכל תת־מרחב של $\mathbb{R}$ הוא $\{0\}$ או $\mathbb{R}$.

תשובה 7.3.7 **השאלה בעמוד 169**

א. כל וקטור במרחב $V = F^2$ נקבע על פי זוג הקואורדינטות שלו, ולכן יש בדיוק $p \cdot p = p^2$ איברים במרחב.

בתת־מרחב $W = \mathrm{Sp}\{(1,1)\}$ יש בדיוק p וקטורים, כמספר הכפולות בסקלר של הוקטור $(1,1)$.

ב. מרחב הפולינומים $V = F[x]$ הוא מרחב אינסופי, למרות שהשדה F סופי. למשל, הסדרה $1, x, x^2, \ldots$ היא סדרה של אינסוף איברים שונים במרחב.

בתת־מרחב $W = F_n[x]$, כל פולינום $p = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ נקבע על פי n מקדמיו, ולכן יש בו p^n איברים.

1 הסבירו לעצמכם מדוע.

תשובה 7.4.1 **השאלה בעמוד 171**

א.
$$\begin{aligned}-4(1+x^2)+2(1+x)+5(1) &= -4-4x^2+2+2x+5\\ &= -4x^2+2x+3\end{aligned}$$

זוהי הצגה של הפולינום $-4x^2+2x+3$ כצירוף לינארי של הפולינומים $1+x^2$, $1+x$ ו־1.

ב. אם המטריצה $\begin{bmatrix}2&3\\2&3\end{bmatrix}$ תלויה לינארית במטריצות $\begin{bmatrix}1&1\\0&0\end{bmatrix}$ ו־$\begin{bmatrix}0&0\\1&1\end{bmatrix}$, אזי קיימים סקלרים λ_2,λ_1 שעבורם:

$$\begin{bmatrix}2&3\\2&3\end{bmatrix}=\lambda_1\begin{bmatrix}1&1\\0&0\end{bmatrix}+\lambda_2\begin{bmatrix}0&0\\1&1\end{bmatrix}$$

כלומר

$$\begin{bmatrix}2&3\\2&3\end{bmatrix}=\begin{bmatrix}\lambda_1&\lambda_1\\\lambda_2&\lambda_2\end{bmatrix}$$

וזה, כמובן, לא ייתכן, ולכן $\begin{bmatrix}2&3\\2&3\end{bmatrix}$ אינה תלויה לינארית במטריצות $\begin{bmatrix}1&1\\0&0\end{bmatrix}$ ו־$\begin{bmatrix}0&0\\1&1\end{bmatrix}$.

ג. אילו $\sqrt{2}$ היה תלוי לינארית בקבוצת המספרים הרציונליים, אז הוא היה צירוף לינארי של מספרים רציונליים עם מקדמים שגם הם מתוך שדה הרציונליים, כלומר היה מתקיים

$$\sqrt{2}=\sum_{i=1}^{n}\lambda_i r_i$$

כאשר λ_i ו־r_i הם מספרים רציונליים לכל i $(1\le i\le)$. מאחר שהתוצאות של כפל מספרים רציונליים ושל חיבור מספרים רציונליים אף הן מספרים רציונליים, נובע כי $\sum_{i=1}^{n}\lambda_i r_i$ הוא מספר רציונלי, בעוד ש־$\sqrt{2}$ הוא אי־רציונלי.

לכן $\sqrt{2}$ אינו תלוי לינארית בקבוצת המספרים הרציונליים.

תשובה 7.5.1 **השאלה בעמוד 172**

K אינה סגורה לגבי החיבור, כי, למשל, הוקטור

$$(5,-5,0,0)+(5,-5,0,0)=(10,-10,0,0)$$

אינו ב־K.

תשובה 7.5.2 **השאלה בעמוד 172**

$$U = \{(\alpha,\beta,\gamma,\delta) | \alpha + \beta + \gamma + \delta = 0,\ \ \alpha,\beta,\gamma,\delta \in \mathbb{R}\}$$

$$V = \{(\alpha,\beta,0,0) | \alpha,\beta \in \mathbb{R}\}$$

$$W = \{(\alpha,-\alpha,0,0)\ |\ _{\text{ממשי}}\alpha\}\ W = \{(\alpha,-\alpha,0,0) | \alpha \in \mathbb{R}\}$$

א. נוכיח כי U, V ו־ W הן תת־מרחבים של $\mathbb{R}^4$, המכילים את K.

1. U היא בעצם מרחב הפתרונות של המערכת ההומוגנית המורכבת מהמשוואה הבודדת $x+y+z+w=0$, ולכן היא תת־מרחב של $\mathbb{R}^4$.[2] כמו כן, $K \subseteq U$, שכן $5+(-5)+0+0=0$.
2. V אינה ריקה. נקל לוודא כי היא סגורה לגבי החיבור ולגבי הכפל בסקלר. לכן V היא תת־מרחב של $\mathbb{R}^4$. ברור ש־ V $(5,-5,0,0) \in V$, כלומר $K \subseteq V$.
3. W אינה ריקה. נראה שהיא סגורה לגבי החיבור ולגבי הכפל בסקלר.
עבור

$$(\alpha,-\alpha,0,0),(\beta,-\beta,0,0) \in W$$

מתקיים:

$$(\alpha,-\alpha,0,0) + (\beta,-\beta,0,0) = (\alpha+\beta,-\alpha-\beta,0,0) = (\alpha+\beta,-(\alpha+\beta),0,0)$$

לכן סכום הוקטורים נמצא ב־ W.
עבור λ ממשי

$$\lambda(\alpha,-\alpha,0,0) = (\lambda\alpha,-(\lambda\alpha),0,0)$$

והוקטור הזה אף הוא ב־ W. לכן W תת־מרחב של $\mathbb{R}^4$, וברור גם ש־ $K \subseteq W$.

ב. סכום הרכיבים של וקטור שצורתו $(\alpha,-\alpha,0,0)$ הוא $\alpha+(-\alpha)+0+0=0$, ולכן $K \subseteq U$. כמו כן, מאחר ששתי הקואורדינטות האחרונות של וקטור שצורתו $(\alpha,-\alpha,0,0)$ הן 0, הרי שהוא נמצא ב־ V, כלומר $W \subseteq V$.

ג. נניח ש־ M הוא תת־מרחב של $\mathbb{R}^4$ המכיל את $(5,-5,0,0)$. כתת־מרחב, M מכיל גם את כל כפולותיו בסקלר של וקטור זה, כלומר את כל הוקטורים שצורתם $(5\lambda,-5\lambda,0,0)$. מאחר ש־ λ יכול להיות כל מספר ממשי, קבוצת וקטורים זו היא בדיוק W, כלומר $W \subseteq M$.

תשובה 7.5.3 **השאלה בעמוד 175**

תהי K קבוצת וקטורים לא־ריקה במרחב ליניארי V, ויהי W תת־מרחב המכיל את K ומוכל בכל תת־מרחב המכיל את K. נוכיח כי:

$$W = \mathrm{Sp}(K)$$

2 ראו דוגמה ד בסעיף 7.1.

$\mathrm{Sp}(K)$ מוכל בכל תת־מרחב המכיל את K. מאחר ש־ W הוא תת־מרחב המכיל את K, הרי ש־

(1) $$\mathrm{Sp}(K) \subseteq W$$

בנוסף, W מוכל בכל תת־מרחב המכיל את K, ומאחר ש־ $\mathrm{Sp}(K)$ מכיל את K ו־ $\mathrm{Sp}(K)$ הוא תת־מרחב, הרי ש־

(2) $$W \subseteq \mathrm{Sp}(K)$$

מ־(1) ומ־(2) נובע כי:

$$W = \mathrm{Sp}(K)$$

תשובה 7.5.4 **השאלה בעמוד 175**

על פי הגדרת התת־מרחב הנפרש על־ידי קבוצת וקטורים, מתקיים:

(1) $$\mathrm{Sp}(\{\mathbf{e}_1,\dots,\mathbf{e}_n\}) \subseteq \mathbb{R}^n$$

עתה, יהי $\mathbf{a} = (a_1,\dots,a_n)$ וקטור כלשהו ב־ $\mathbb{R}^n$. אז

$$\mathbf{a} = a_1\mathbf{e}_1,\dots,a_n\mathbf{e}_n$$

ולכן

$$\mathbf{a} \in \mathrm{Sp}(K)$$

ומכאן:

(2) $$\mathbb{R}^n \subseteq \mathrm{Sp}(\{\mathbf{e}_1,\dots,\mathbf{e}_n\})$$

מ־(1) ומ־(2) נובע כי:

$$\mathrm{Sp}(\{\mathbf{e}_1,\dots,\mathbf{e}_n\}) = \mathbb{R}^n$$

תשובה 7.5.5 **השאלה בעמוד 175**

א. $\mathbf{a} = (1,2,0)$ ו־ $\mathbf{b} = (3,5,0)$.

1. נראה כי:

$$\mathrm{Sp}(\{\mathbf{a},\mathbf{b}\}) = \left\{(\lambda_1,\lambda_2,0) \;\middle|\; \text{ממשיים } \lambda_1,\lambda_2\right\}$$

כל וקטור ב־ $\mathrm{Sp}(\{\mathbf{a},\mathbf{b}\})$ הוא צירוף לינארי של $\mathbf{a}$ ו־ $\mathbf{b}$, ולכן הקואורדינטה השלישית שלו היא אפס. כלומר:

$$\mathrm{Sp}(\{\mathbf{a},\mathbf{b}\}) \subseteq \left\{(\lambda_1,\lambda_2,0) \;\middle|\; \lambda_1,\lambda_2 \in \mathbb{R}\right\}$$

נותר להוכיח כי:

$$\left\{(\lambda_1,\lambda_2,0)\right\} \subseteq \mathrm{Sp}(\{\mathbf{a},\mathbf{b}\})$$

נתבונן בוקטור כלשהו מהצורה $(\lambda_1,\lambda_2,0)$. וקטור זה יימצא ב־ $\mathrm{Sp}(\{\mathbf{a},\mathbf{b}\})$ אם יימצאו סקלרים α ו־ β שעבורם:

$$(\lambda_1,\lambda_2,0) = \alpha\mathbf{a} + \beta\mathbf{b}$$

כלומר:

$$(\lambda_1,\lambda_2,0) = \alpha(1,2,0) + \beta(3,5,0)$$

α ו־ β כאלה קיימים אם יש פתרון למערכת הליניארית:

$$\alpha + 3\beta = \lambda_1$$

$$2\alpha + 5\beta = \lambda_2$$

למערכת זו קיים פתרון, שכן הדטרמיננטה של מטריצת המקדמים שלה שונה מ־ 0. ניתן, אם כן, להציג את $(\lambda_1,\lambda_2,0)$ כצירוף ליניארי של **a** ושל **b**, ולכן

$$\{(\lambda_1,\lambda_2,0)\} \subseteq \mathrm{Sp}(\{\mathbf{a},\mathbf{b}\})$$

והוכחנו את הדרוש.

2. מבחינה גיאומטרית נמצאים שני הוקטורים **a** ו־ **b** במישור x-y והם אינם על ישר אחד העובר דרך הראשית. אוסף הצירופים הליניאריים שלהם הוא אפוא המישור כולו.

ב. נגדיר:

$$\mathbf{c} = (1,0,0)$$

$$\mathbf{d} = (0,1,0)$$

$$\mathrm{Sp}(\{\mathbf{c},\mathbf{d}\}) \subseteq \{(\lambda_1\mathbf{c} + \lambda_2\mathbf{d}) \mid \lambda_1,\lambda_2 \in \mathbb{R}\}$$

$$= \{(\lambda_1,0,0) + (0,\lambda_2,0) \mid \lambda_1,\lambda_2 \in \mathbb{R}\}$$

$$= \{(\lambda_1,\lambda_2,0) \mid \lambda_1,\lambda_2 \in \mathbb{R}\} = \mathrm{Sp}(\{\mathbf{a},\mathbf{b}\})$$

באופן כללי יותר, אם **c** ו־ **d** הם וקטורים כלשהם במישור x-y שאינם על ישר אחד שעובר דרך הראשית, אז המרחב הנפרש על ידיהם הוא מישור x-y, ולכן לכל שני וקטורים כאלה:

$$\mathrm{Sp}(\{\mathbf{a},\mathbf{b}\}) = \mathrm{Sp}(\{\mathbf{c},\mathbf{d}\})$$

תשובה 7.5.6 **השאלה בעמוד 176**

נוכיח כי:

$$F_4[x] = \mathrm{Sp}(\{1,x,x^2,x^3\})$$

ברור כי:

$$\mathrm{Sp}(\{1,x,x^2,x^3\}) \subseteq F_4[x]$$

כעת, יהי

$$P(x) = a_0 + a_1x + a_2x^2 + a_3x^3$$

פולינום ב־ $F_4[x]$.

$P(x)$ הוא צירוף לינארי של הפולינומים $1,x,x^2,x^3$ עם המקדמים a_0,a_1,a_2 ו־ a_3 בהתאמה, ולכן

$$F_4[x] \subseteq \mathrm{Sp}(\{1,x,x^2,x^3\})$$

ומכאן:

$$F_4[x] = \mathrm{Sp}(\{1,x,x^2,x^3\})$$

תשובה 7.5.7 **השאלה בעמוד 176**

א. נוכיח כי:

$$\mathbf{M}_{2\times 3}^{\mathbb{R}} = \mathrm{Sp}\left(\left\{E^{(1,1)},E^{(1,2)},E^{(1,3)},E^{(2,1)},E^{(2,2)},E^{(2,3)}\right\}\right)$$

ברור כי:

$$\mathbf{M}_{2\times 3}^{\mathbb{R}} \supseteq \mathrm{Sp}\left(\left\{E^{(1,1)},E^{(1,2)},E^{(1,3)},E^{(2,1)},E^{(2,2)},E^{(2,3)}\right\}\right)$$

כעת, עבור מטריצה כלשהי A ב־ $\mathbf{M}_{2\times 3}^{\mathbb{R}}$,

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}$$

מתקיים:

$$A = a_{11}E^{(1,1)} + a_{12}E^{(1,2)} + a_{13}E^{(1,3)} + a_{21}E^{(2,1)} + a_{22}E^{(2,2)} + a_{23}E^{(2,3)}$$

כלומר,

$$A \in \mathrm{Sp}\left(\left\{E^{(1,1)},E^{(1,2)},E^{(1,3)},E^{(2,1)},E^{(2,2)},E^{(2,3)}\right\}\right)$$

וזאת, לכל A ב־ $\mathbf{M}_{2\times 3}^{\mathbb{R}}$, ולכן:

$$\mathbf{M}_{2\times 3}^{\mathbb{R}} \subseteq \mathrm{Sp}\left(\left\{E^{(1,1)},E^{(1,2)},E^{(1,3)},E^{(2,1)},E^{(2,2)},E^{(2,3)}\right\}\right)$$

כלומר:

$$\mathbf{M}_{2\times 3}^{\mathbb{R}} = \mathrm{Sp}\left(\left\{E^{(1,1)},E^{(1,2)},E^{(1,3)},E^{(2,1)},E^{(2,2)},E^{(2,3)}\right\}\right)$$

ב. נוכיח כי גם הקבוצה בעלת שבעת האיברים

$$\left\{E^{(1,1)},E^{(1,2)},E^{(1,3)},E^{(2,1)},E^{(2,3)},\begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix},\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}\right\}$$

היא קבוצת יוצרים של $\mathbf{M}_{2\times 3}^{\mathbb{R}}$.

תהי A כמו בחלק א. אזי:

$$A = \begin{bmatrix} a_{11} & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & a_{12} & 0 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & a_{13}-a_{23} \\ 0 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 0 \\ a_{21} & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 0 & a_{22}-a_{23} & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & a_{23} \\ 0 & a_{23} & a_{23} \end{bmatrix}$$

$$= a_{11}E^{(1,1)} + a_{12}E^{(1,2)} + (a_{13} - a_{23})E^{(1,3)}$$

$$+a_{21}E^{(2,1)} + (a_{22} - a_{23})E^{(2,2)} + a_{23}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

הראינו אפוא שכל מטריצה A ב־ $\mathbf{M}_{2\times 3}^{\mathbb{R}}$ ניתנת להצגה כצירוף ליניארי של חלק משבע המטריצות הנתונות בשאלה זו. מכאן נובע בקלות שקבוצת שבע המטריצות אלה פורשת את $M_{2\times 3}^{\mathbb{R}}$.

תשובה 7.5.8 **השאלה בעמוד 176**

א. כיוון ראשון: נניח ש־ U תת־מרחב של V, ונוכיח כי:

$$\mathrm{Sp}(U) = U$$

ברור כי:

$$U \subseteq \mathrm{Sp}(U)$$

אולם $\mathrm{Sp}(U)$ מוכל בכל תת־מרחב המכיל את U, ובפרט - מאחר ש־ U תת־מרחב המכיל את U, מתקיים

$$\mathrm{Sp}(U) \subseteq U$$

ולכן:

$$\mathrm{Sp}(U) = U$$

כיוון שני: נניח ש־ $U = \mathrm{Sp}(U)$. מהנתון U איננה ריקה, ויהיו $u,v \in U$, ויהי λ סקלר. אז $u + v = 1\cdot u + 1\cdot v \in \mathrm{Sp}(U)$, ולכן $u + v \in U$. באופן דומה, $\lambda u \in \mathrm{Sp}(U) = U$. הקבוצה U סגורה אם כן לחיבור וכפל בסקלר, ולכן מהווה תת־מרחב.

ב. לכל תת־קבוצה לא ריקה K של מרחב ליניארי V, $\mathrm{Sp}(K)$ הוא תת־מרחב של V, ולכן לפי חלק א:

$$\mathrm{Sp}\big(\mathrm{Sp}(K)\big) = \mathrm{Sp}(K)$$

תשובה 7.5.9 **השאלה בעמוד 177**

א.
$$\mathrm{Sp}\left(\left\{E^{(1,1)}, E^{(2,2)}, M\right\}\right)$$

$$= \left\{A \in \mathbf{M}_{2\times 3}^{\mathbb{R}} \;\middle|\; A = \lambda_1 E^{(1,1)} + \lambda_2 E^{(2,2)} + \lambda_3 M\right\}$$

$$= \left\{A \in \mathbf{M}_{2\times 3}^{\mathbb{R}} \;\middle|\; A = \begin{bmatrix} \lambda_1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & \lambda_2 \end{bmatrix} + \begin{bmatrix} 0 & \lambda_3 \\ \lambda_3 & 0 \end{bmatrix}\right\}$$

$$= \left\{A \in \mathbf{M}_{2\times 3}^{\mathbb{R}} \;\middle|\; A = \begin{bmatrix} \lambda_1 & \lambda_3 \\ \lambda_3 & \lambda_2 \end{bmatrix}\right\}$$

לכן תת־מרחב זה הוא קבוצת כל המטריצות מסדר 2×2 שבהן $a_{12} = a_{21}$, כלומר קבוצת כל המטריצות הסימטריות מסדר 2×2 מעל הממשיים.

ב.

$$\mathrm{Sp}(\{L\}) = \left\{ A \in \mathbf{M}_{2\times 3}^{\mathbb{R}} \;\middle|\; A = \lambda \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\}$$

$$= \left\{ A \in \mathbf{M}_{2\times 3}^{\mathbb{R}} \;\middle|\; A = \begin{bmatrix} 0 & \lambda \\ -\lambda & 0 \end{bmatrix} \right\}$$

כלומר, תת־מרחב זה הוא קבוצת כל המטריצות מסדר 2×2 שעבורן $a_{11} = a_{22} = 0$ ו־ $a_{12} = -a_{21}$, כלומר קבוצת כל המטריצות האנטי־סימטריות מסדר 2×2 מעל הממשיים.

תשובה 7.5.10 **השאלה בעמוד 177**

התת־מרחב של מרחב הפולינומים מעל $\mathbb{R}$, הנפרש על־ידי קבוצת הפולינומים

$$\{x, x^2, x^3, x^4\}$$

מכיל את כל הפולינומים ב־$\mathbb{R}_5[x]$, שהמקדם החופשי שלהם a_0 הוא 0, ואלה הם בדיוק כל הפולינומים ב־$\mathbb{R}_5[x]$ שמתאפסים ב־$x = 0$.

תשובה 7.5.11 **השאלה בעמוד 177**

א. נניח כי $v \in \mathrm{Sp}(\{v_1, \ldots, v_n\})$. אזי קיימים סקלרים $\mu_1, \ldots, \mu_n$ כך ש־

$$v = \mu_1 v_1 + \ldots + \mu_i v_i + \ldots + \mu_n v_n$$

מאחר ש־ $\lambda \neq 0$, הרי ש־

$$v = \mu_1 v_1 + \ldots + \mu_{i-1} v_{i-1} + \left(\frac{\mu_i}{\lambda}\right)(\lambda v_i) + \ldots + \mu_n v_n$$

ומכאן ש־

$$v \in \mathrm{Sp}\left(\left\{v_1, \ldots, v_{i-1}, \lambda v_i, v_{i+1}, \ldots, v_n\right\}\right)$$

מאידך גיסא, אם

$$v \in \mathrm{Sp}\left(\left\{v_1, \ldots, v_{i-1}, \lambda v_i, v_{i+1}, \ldots, v_n\right\}\right)$$

אז קיימים סקלרים $\mu_1, \ldots, \mu_n$ כך ש־

$$v = \mu_1 v_1 + \ldots + \mu_i (\lambda v_i) + \ldots + \mu_n v_n$$

כלומר

$$v = \mu_1 v_1 + \ldots + (\mu_i \lambda) v_i + \ldots + \mu_n v_n$$

ולכן:

$$v \in \mathrm{Sp}(\{v_1, \ldots, v_n\})$$

משתי הטענות שהוכחו כאן נובעת טענת חלק א.

ב. יהי $v = \mu_1 v_1 + \ldots + \mu_n v_n$ וקטור כלשהו ב־ $v \in \mathrm{Sp}(\{v_1,\ldots,v_n\})$.

$$v = \mu_1 v_1 + \ldots + (\mu_i - \lambda\mu_j)v_i + \ldots + \mu_j(v_j + \lambda v_i) + \ldots + \mu_n v_n$$

ולכן:

$$v \in \mathrm{Sp}\left(\left\{v_1,\ldots,v_{j-1},v_j + \lambda v_i,v_{j+1},\ldots,v_n\right\}\right)$$

כמו כן, אם $v = \mu_1 v_1 + \ldots + \mu_j(v_j + \lambda v_i) + \ldots + \mu_n v_n$ הוא וקטור ב־

$$\mathrm{Sp}\left(\left\{v_1,\ldots,v_{j-1},v_j + \lambda v_i,v_{j+1},\ldots,v_n\right\}\right)$$

אז

$$v = \mu_1 v_1 + \ldots + (\mu_i - \lambda\mu_j)v_i + \ldots + \mu_j v_j + \ldots + \mu_n v_n$$

ולכן:

$$v \in \mathrm{Sp}(\{v_1,\ldots,v_n\})$$

ומכאן ש־

$$\mathrm{Sp}(\{v_1,\ldots,v_n\}) = \mathrm{Sp}\left(\left\{v_1,\ldots,v_{j-1},v_j + \lambda v_i,v_{j+1},\ldots,v_n\right\}\right)$$

תשובה 7.5.12 **השאלה בעמוד 177**

די להראות שאם A' היא מטריצה שהתקבלה מ־ A על־ידי פעולה אלמנטרית **אחת**, אז ל־ A' ול־ A יש אותו מרחב שורות. אם כך, אז גם סדרה של פעולות אלמנטריות נותנת סדרת מטריצות שמרחב השורות של כל אחת מהן שווה לזה של קודמתה, ובסופו של דבר מרחב השורות של המטריצה האחרונה שווה למרחב השורות של המטריצה הראשונה. נוכיח אפוא את הטענה לגבי שלוש הפעולות האלמנטריות:

1. ברור שהחלפת שתי שורות של המטריצה A זו בזו, אינה משנה את קבוצת השורות וממילא לא את המרחב שהן פורשות.
2. אם נכפול את השורה ה־ i של A בסקלר λ שונה מ־ 0, יהיו שורות המטריצה החדשה

$$\mathbf{a}_1,\ldots,\lambda\mathbf{a}_i,,\ldots,\mathbf{a}_m$$

וכבר הוכחנו בשאלה הקודמת כי:

$$\mathrm{Sp}(\{\mathbf{a}_1,\mathbf{a}_i,\ldots,\mathbf{a}_m\}) = \mathrm{Sp}(\{\mathbf{a}_1,\lambda\mathbf{a}_i,\ldots,\mathbf{a}_m\})$$

3. אם נוסיף כפולה ב־ λ של השורה ה־ i לשורה ה־ j, יהיו שורות המטריצה החדשה:

$$\mathbf{a}_1,\ldots,\mathbf{a}_{j-1},\mathbf{a}_j + \lambda\mathbf{a}_i,\mathbf{a}_{j+1},\ldots,\mathbf{a}_m$$

ובשאלה הקודמת הוכחנו כי:

$$\mathrm{Sp}\left(\{\mathbf{a}_1,\ldots,\mathbf{a}_m\}\right) = \mathrm{Sp}\left(\{\mathbf{a}_1,\ldots,\mathbf{a}_{j-1},\mathbf{a}_j + \lambda\mathbf{a}_i,\mathbf{a}_{j+1},\ldots,\mathbf{a}_m\}\right)$$

תשובה 7.5.13 **השאלה בעמוד 178**

עלינו להוכיח כי $\mathrm{Sp}(K \cup \{v\}) = \mathrm{Sp}(K)$ אם ורק אם v תלוי לינארית ב־ K.

נניח אפוא כי v תלוי לינארית ב־ K, ונוכיח כי $\mathrm{Sp}(K \cup \{v\}) = \mathrm{Sp}(K)$:

ראשית, לכל $v \in V$ מתקיים $\mathrm{Sp}(K) \subseteq \mathrm{Sp}(K \cup \{v\})$. לכן מספיק להוכיח כי

$$\mathrm{Sp}(K \cup \{v\}) \subseteq \mathrm{Sp}(K)$$

על פי ההנחה קיימים סקלרים $\lambda_1,\ldots,\lambda_n$ ווקטורים $v_1,\ldots,v_n$ כך ש־

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

אם $u \in \mathrm{Sp}(K \cup (v))$, אז קיימים סקלרים $\mu_1,\ldots,\mu_m,\mu_{m+1}$ ווקטורים $u_1,\ldots,u_m$ ב־ K כך ש־

$$u = \mu_1 u_1 + \ldots + \mu_m u_m + \mu_{m+1} v$$

אבל במקרה זה נוכל לרשום

$$u = \mu_1 u_1 + \ldots + \mu_m u_m + \mu_{m+1}\lambda_1 v_1 + \ldots + \mu_{m+1}\lambda_n v_n$$

ומאחר ש־ $u_1,\ldots,u_m, v_1,\ldots,v_n$ הם וקטורים ב־ K, הרי ש־ $u \in \mathrm{Sp}(K)$, והוכחנו, אם כן, כי

$$\mathrm{Sp}(K \cup (v)) \subseteq \mathrm{Sp}(K)$$

כדרוש.

נניח עתה כי $\mathrm{Sp}(K) = \mathrm{Sp}(K \cup (v))$ ונוכיח כי v תלוי לינארית ב־ K:

ברור כי $v \in \mathrm{Sp}(K \cup (v))$, ולכן על פי ההנחה, $v \in \mathrm{Sp}(K)$.

כלומר, קיימים סקלרים $\lambda_1,\ldots,\lambda_n$ ווקטורים $v_1,\ldots,v_n$ ב־ K כך ש־

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

הווי אומר, v תלוי לינארית ב־ K.

תשובה 7.5.14 **השאלה בעמוד 178**

א. תהי $\{P_1(x),\ldots,P_n(x)\}$ קבוצה סופית כלשהי של פולינומים מעל F. נראה כי היא אינה פורשת את $F[X]$:

תהי m המעלה הגבוהה ביותר של הפולינומים בקבוצה זו.

המעלה של כל פולינום $\lambda_1 P_1(x) + \ldots + \lambda_n P_n(x)$, שהוא צירוף לינארי של איברי קבוצה זו, קטנה מ־ m או שווה לו.

אם כך, אי־אפשר לקבל על־ידי צירופים לינאריים של איברי קבוצה זו פולינומים שמעלתם גדולה מ־ m, ולכן הקבוצה שלעיל אינה פורשת את $F[X]$.

ב. הקבוצה האינסופית $\{1,x,x^2,x^4,\dots,x^n,\dots\}$, הכוללת את כל החד־איברים מהצורה x^i, כאשר $i=0,1,2,\dots$, פורשת את $F[X]$. זאת משום שכל פולינום הוא צירוף ליניארי של מספר סופי של פולינומים מקבוצה זו. מקדמי הצירוף הם כמובן מקדמי הפולינום.

תשובה 7.5.15 **השאלה בעמוד 178**

א. כפי שראינו, המרחב F^n נפרש על־ידי n הוקטורים

$$\mathbf{e}_1=(1,0,\dots,0)$$
$$\vdots$$
$$\mathbf{e}_n=(0,0,\dots,1)$$

ולכן נוצר סופית.

ב. $M^F_{m\times n}$ נוצר על־ידי קבוצת המטריצות

$$\left\{E^{(i,j)}\;\middle|\;1\le i\le m\,,\,1\le j\le n\right\}$$

המוגדרות על־ידי

$$E^{(i,j)}=\begin{array}{cl} \begin{array}{c}\text{עמודה } j\\ \downarrow\end{array} & \\ \begin{bmatrix}0 & \vdots & 0\\ \cdots & 1 & \cdots\\ 0 & \vdots & 0\end{bmatrix} & \leftarrow i \text{ שורה} \end{array}$$

שכן כל מטריצה $A=[a_{ij}]$ ב־ $\mathbf{M}^F_{m\times n}$ ניתנת להצגה כצירוף ליניארי:

$$A=\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}E^{(i,j)}$$

תשובה 7.5.16 **השאלה בעמוד 179**

א. האם מתוך $T\subseteq K$ נובע $\mathrm{Sp}(K)\subseteq\mathrm{Sp}(T)$? כן. אם $K\subseteq T$, אז כל צירוף ליניארי של איברי K הוא בפרט צירוף ליניארי של איברי T, ולכן:

$$\mathrm{Sp}(K)\subseteq\mathrm{Sp}(T)$$

ב. האם מתוך $K\subseteq\mathrm{Sp}(T)$ נובע $\mathrm{Sp}(K)\subseteq\mathrm{Sp}(T)$? כן. $\mathrm{Sp}(K)$ מוכל בכל תת־מרחב שמכיל את K, ובפרט מוכל בתת־מרחב $\mathrm{Sp}(T)$.

ג. האם מתוך $K\subseteq\mathrm{Sp}(T)$ נובע $K\subseteq T$? לא. למשל, אם V מרחב ליניארי, ו־ $v\in V$ שונה מאפס, אז $\{0\}\subseteq\mathrm{Sp}\{v\}$, אבל $\{0\}\not\subseteq\{v\}$.

ד. האם מתוך $K \subset T$ (חלקית ממש!) נובע $\mathrm{Sp}(K) \subset \mathrm{Sp}(T)$? - לא. נתבונן בתת־קבוצות K ו־T של $\mathbb{R}^2$:

$$K = \{(1,0),(0,1)\}$$

$$T = \{(1,0),(0,1),(1,1)\}$$

ברור ש־

$$K \subset T$$

ובכל זאת

$$\mathrm{Sp}(K) = \mathrm{Sp}(T) = \mathbb{R}^2$$

כלומר:

$$\mathrm{Sp}(K) \not\subset \mathrm{Sp}(T)$$

תשובה 7.5.17 **השאלה בעמוד 180**

א. $K \subseteq K \cup T$, ולכן לפי חלק א של השאלה הקודמת:

$$\mathrm{Sp}(K) \subseteq \mathrm{Sp}(K \cup T)$$

באותו אופן גם:

$$\mathrm{Sp}(T) \subseteq \mathrm{Sp}(K \cup T)$$

מאחר שגם $\mathrm{Sp}(K)$ וגם $\mathrm{Sp}(T)$ מוכלות ב־$\mathrm{Sp}(K \cup T)$, יוצא כי:

$$\mathrm{Sp}(K) \cup \mathrm{Sp}(T) \subseteq \mathrm{Sp}(K \cup T)$$

ב. השוויון $\mathrm{Sp}(K) \cup \mathrm{Sp}(T) = \mathrm{Sp}(K \cup T)$ לא בהכרח מתקיים.
למשל, אם K ו־T הן הקבוצות ב־$\mathbb{R}^2$

$$K = \{(0,1)\}$$

$$T = \{(1,0)\}$$

אז

$$\mathrm{Sp}(K \cup T) = \mathrm{Sp}(\{1,0\},\{0,1\}) = \mathbb{R}^2$$

ואילו

$$\mathrm{Sp}(K) = \{(0,\lambda) | \lambda \in \mathbb{R}\}$$

$$\mathrm{Sp}(T) = \{(\lambda,0) | \lambda \in \mathbb{R}\}$$

ולכן $\mathrm{Sp}(K) \cup \mathrm{Sp}(T)$ הוא אוסף הוקטורים שבהם לפחות אחת הקואורדינטות היא 0 (כלומר, אלה הם ציר ה־x וציר ה־y), וברור ש־

$$\mathrm{Sp}(K) \cup \mathrm{Sp}(T) \subset \mathrm{Sp}(K \cup T)$$

ג. $K \cap T \subseteq K$, ולכן לפי חלק א של השאלה הקודמת,

$$\mathrm{Sp}(K \cap T) \subseteq \mathrm{Sp}(K)$$

ובדומה:

$$\mathrm{Sp}(K \cap T) \subseteq \mathrm{Sp}(T)$$

לכן:

$$\text{Sp}(K \cap T) \subseteq \text{Sp}(K) \cap \text{Sp}(T)$$

ד. השוויון $\text{Sp}(K \cap T) = \text{Sp}(K) \cap \text{Sp}(T)$ לא בהכרח מתקיים.
נתבונן בקבוצות K ו- T ב- $\mathbb{R}^2$:

$$K = \{(1,0),(0,1)\}$$

$$T = \{(1,0),(0,2)\}$$

קל לאשר כי:

$$\text{Sp}(K) = \text{Sp}(T) = \mathbb{R}^2$$

ולכן:

$$\text{Sp}(K) \cap \text{Sp}(T) = \mathbb{R}^2$$

אולם

$$\text{Sp}(K \cap T) = \text{Sp}(\{(1,0)\}) \neq \mathbb{R}^2$$

כי למשל: $(0,1) \in \mathbb{R}^2$, אבל $(0,1) \notin \text{Sp}(K \cap T)$.

תשובה 7.5.18 **השאלה בעמוד 181**

א. יהי $P(x)$ פולינום כלשהו ב- $\mathbb{R}_4[x]$:

$$P(x) = a_0 + a_1x + a_2x^2 + a_3x^3$$

אם $P(x)$ שייך ל- U, אז $P(1) = 0$, כלומר:

$$a_0 + a_1 + a_2 + a_3 = 0$$

כלומר:

$$a_0 = -a_1 - a_2 - a_3$$

ולכן:

$$\begin{aligned} P(x) &= -a_1 - a_2 - a_3 + a_1x + a_2x^2 + a_3x^3 \\ &= a_1(x-1) + a_2(x^2-1) + a_3(x^3-1) \end{aligned}$$

מכאן אפשר להראות (השלימו בעצמכם) שהקבוצה $\{x-1, x^2-1, x^3-1\}$ פורשת את U.
יש כמובן קבוצות נוספות שפורשות את U, ליתר דיוק - יש אינסוף קבוצות כאלה.
נסו להוכיח, למשל, שגם הקבוצה $\{x-1,(x-1)^2,(x-1)^3\}$ פורשת את U.

ב. כמו בחלק א, יהי $P(x)$ פולינום כלשהו ב- $\mathbb{R}_4[x]$:

$$P(x) = a_0 + a_1x + a_2x^2 + a_3x^3$$

אם $P(x)$ שייך ל- W, אז $P(1) = 0$ וגם $P(2) = 0$, כלומר:

$$a_0 + a_1 + a_2 + a_3 = 0$$

$$a_0 + 2a_1 + 4a_2 + 8a_3 = 0$$

מכאן אפשר להראות שמתקיים

$$a_0 = 2a_2 + 6a_3$$

$$a_1 = -3a_2 - 7a_3$$

ולכן:

$$P(x) = 2a_2 + 6a_3 + (-3a_2 - 7a_3)x + a_2x^2 + a_3x^3$$
$$= a_2(2 - 3x + x^2) + a_3(6 - 7x + x^3)$$

מכאן נובע (השלימו בעצמכם) שהקבוצה $\left\{2 - 3x + x^2, 6 - 7x + x^3\right\}$ פורשת את W.
נסו להוכיח, למשל, שגם הקבוצה $\left\{(x-1)(x-2), x(x-1)(x-2)\right\}$ פורשת את W.

תשובה 7.6.1 **השאלה בעמוד 182**

$$U = \left\{(a,b,c) \middle| a + b + c = 0,\ a,b,c \in \mathbb{R}\right\}$$

$$U = \left\{(0,0,d) \middle| d \in \mathbb{R}\right\}$$

א. קל לבדוק (ישירות) שהקבוצות הנדונות אינן ריקות, וסגורות לחיבור ולכפל בסקלר. לפיכך הן אכן תת־מרחבים.

ב. הקבוצה $U \cup W$ אינה סגורה לגבי החיבור:

כי, למשל, $(1,1,-2) \in U$ ו־ $(0,0,2) \in W$, ולכן כל אחד מהוקטורים האלה הוא ב־ $U \cup W$.
סכום הוקטורים הוא:

$$(1,1,-2) + (0,0,2) = (1,1,0)$$

אולם $(1,1,0) \notin U$ וגם $(1,1,0) \notin W$, ולכן $(1,1,0) \notin U \cup W$.

תשובה 7.6.2 **השאלה בעמוד 182**

א. נתון כי U ו־ W הם תת־מרחבים של V. יש להוכיח כי:
$U \cup W$ הוא תת־מרחב של V אם ורק אם $U \subseteq W$ או $W \subseteq U$.

כיוון ראשון:

אם $U \subseteq W$ אז $U \cup W = W$ ולכן $U \cup W$ תת־מרחב.
באותו אופן, אם $W \subseteq U$ אז $U \cup W = U$ ולכן $U \cup W$ תת־מרחב.

כיוון שני:

נניח כי $U \cup W$ הוא תת־מרחב של V, ונוכיח כי $U \subseteq W$ או $W \subseteq U$.
נוכיח בדרך השלילה. אם ההנחה לא מתקיימת, אז $U \not\subseteq W$ ו־ $W \not\subseteq U$.
לכן קיים איבר $w \in W$ כך ש־ $w \notin U$, וכן איבר $u \in U$ כך ש־ $u \notin W$.
ברור כי $u, w \in U \cup W$, ומאחר שלפי הנחתנו $U \cup W$ הוא תת־מרחב, הרי שהוא סגור לחיבור, ולכן:

$$u + w \in U \cup W \qquad (1)$$

מכאן ש־ $u + w \in U$ או $u + w \in W$ (או שניהם גם יחד).
נניח $u + w \in W$.

מאחר ש־ W תת־מרחב, הרי $-w \in W$, ובגלל הסגירות ביחס לחיבור ב־ W:

$$(u+w)+(-w) \in W$$

כלומר $u \in W$, בסתירה להנחתנו, ולכן:

$$u+w \notin W \qquad (2)$$

אולם אם $u+w \in U$, אז בדומה לטיעון הקודם, $-u+(u+w) \in U$, כלומר $w \in U$, ושוב בסתירה להנחתנו. מכאן ש־

$$u+w \notin U \qquad (3)$$

מ־(2) ומ־(3) נובע

$$u+w \notin U \cup W$$

בסתירה ל־(1).

ב. נגדיר:

$$U = \{(a,0) | a \in \mathbb{R}\}$$

$$W = \{(0,b) | b \in \mathbb{R}\}$$

קל להראות ש־ U ו־ W הם תת־מרחבים של $\mathbb{R}^2$.

בהתאם לחלק א, $W \cup U$ אינו תת־מרחב, שכן אף אחד מבין התת־מרחבים U ו־ W אינו מוכל ברעהו.

תשובה 7.6.3 **השאלה בעמוד 183**

תהיינה S,T,K קבוצות חלקיות ל־ V.

א. יהי $s+t$ וקטור כלשהו ב־ $S+T$, כאשר $s \in S$ ו־ $t \in T$.
מחילופיות החיבור במרחב נובע כי $s+t=t+s$ ולכן $s+t \in T+S$, ומכאן ש־ $S+T \subseteq T+S$.

באופן דומה, אפשר להראות כי

$$T+S \subseteq S+T$$

ולכן:

$$S+T = T+S$$

ב. יהי $(s+t)+k$ וקטור כלשהו ב־ $(S+T)+K$ כאשר $s \in S$, $t \in T$ ו־ $k \in K$.
מקיבוציות החיבור במרחב ליניארי נובע כי

$$(s+t)+k = s+(t+k)$$

ולכן $(S+T)+K \subseteq S+(T+K)$.
באופן דומה, נוכל להראות כי

$$S+(T+K) \subseteq (S+T)+K$$

ומכאן ש־

$$(S+T)+K = S+(T+K)$$

תשובה 7.6.4 **השאלה בעמוד 185**

א. אם $U_1,\ldots,U_n$ תת־מרחבים של V, אז 0 (וקטור האפס של V) שייך לכל אחד מתת־מרחבים אלה:

$$0 = \underset{U_1}{\underset{\in}{0}} + \ldots + \underset{U_n}{\underset{\in}{0}}$$

לכן $0 \in U_1 + \ldots + U_n$, ולכן $U_1 + \ldots + U_n$ אינה ריקה.

ב. נוכיח באינדוקציה על n כי $U_1 + \ldots + U_n$ סגורה לחיבור וקטורים ולכפל בסקלר.
עבור $n = 2$, $U_1 + U_2$ סגורה לחיבור וקטורים ולכפל בסקלר לפי משפט 7.6.2.
נניח כי הסכום של כל n תת־מרחבים סגור לחיבור ולכפל בסקלר, ונוכיח כי הסכום של $n+1$ תת־מרחבים סגור לחיבור ולכפל בסקלר.

$$U_1 + \ldots + U_n + U_{n+1} = (U_1 + \ldots + U_n) + U_{n+1}$$

$W = U_1 + \ldots + U_n$ סגור לחיבור ולכפל בסקלר, לפי הנחת האינדוקציה, ואילו $W + U_{n+1}$ סגור ביחס לחיבור ולכפל בסקלר, לפי משפט 7.6.2. מכאן ש־ $U_1 + \ldots + U_{n+1}$ סגור לחיבור ולכפל בסקלר.

תשובה 7.6.5 **השאלה בעמוד 185**

נוכיח כי כאשר U,W תת־מרחבים, אז $U + W = U \Leftrightarrow W \subseteq U$

כיוון ראשון:

נניח כי $U + W = U$.

לפי משפט 7.6.2,

$$W \subseteq U + W \qquad (1)$$

ולפי הנחתנו, $U + W = U$, ולכן (1) משמעו $W \subseteq U$.

כיוון שני:

נניח כי $W \subseteq U$.

כל וקטור ב־ $U + W$ ניתן להצגה כסכום של וקטור מתוך U ווקטור מתוך W. כיוון שכל וקטור ב־ W הוא גם ב־ U, לפי ההנחה, הרי שכל וקטור ב־ $U + W$ ניתן להצגה כסכום של שני וקטורים מתוך U, ובשל כך הוא עצמו נמצא ב־ U.

הווי אומר:

$$U + W \subseteq U \qquad (2)$$

אולם על פי משפט 7.6.2:

$$U \subseteq U + W \qquad (3)$$

מ־(2) ומ־(3) נובע כי:

$$U + W = U$$

תשובה 7.6.6 **השאלה בעמוד 185**

א. יהי w וקטור כלשהו השייך לאיחוד $U_1 \cup \ldots \cup U_n$. w בוודאי שייך לפחות לאחד המרחבים $U_1, \ldots, U_n$. נניח כי $w \in U_i$ $(1 \le i \le n)$, אזי

$$w = \underset{\uparrow}{0} + 0 + \ldots + 0 + \underset{\uparrow}{w} + 0 + \ldots + \underset{\uparrow}{0}$$

מחובר ראשון   מחובר i מחובר n-י

ולכן $w \in U_1 + \ldots + U_n$.

הוכחנו כי כל וקטור באיחוד $U_1 \cup \ldots \cup U_n$ שייך לסכום $U_1 + \ldots + U_n$, ולכן:

$$U_1 \cup \ldots \cup U_n \subseteq U_1 + \ldots + U_n$$

ב. $U_1 + \ldots + U_n$ הוא תת־מרחב המכיל את האיחוד $U_1 \cup \ldots \cup U_n$.
$\mathrm{Sp}(U_1 \cup \ldots \cup U_n)$ בוודאי מוכל בכל תת־מרחב המכיל את $U_1 \cup \ldots \cup U_n$, ולכן:

$$\mathrm{Sp}(U_1 \cup \ldots \cup U_n) \subseteq U_1 + \ldots + U_n \qquad (1)$$

אבל לכל וקטור w ב־ $U_1 + \ldots + U_n$ קיימת הצגה כ־

$$u_1 + \ldots + u_n$$

שבה לכל i, $(1 \le i \le n)$, $u_i \in U_i$.
הצגה זו היא צירוף ליניארי של וקטורים מתוך $U_1 \cup \ldots \cup U_n$, ובשל כך בוודאי היא שייכת ל־ $\mathrm{Sp}(U_1 \cup \ldots \cup U_n)$. לפיכך:

$$U_1 + \ldots + U_n \subseteq \mathrm{Sp}(U_1 \cup \ldots \cup U_n) \qquad (2)$$

מ־(1) ומ־(2) נובע כי:

$$\mathrm{Sp}(U_1 \cup \ldots \cup U_n) = U_1 + \ldots + U_n$$

תשובה 7.6.7 **השאלה בעמוד 186**

נוכיח כי כאשר U, W תת־מרחבים, אז:
$U \cup W = U + W$ אם ורק אם $U \subseteq W$ או $W \subseteq U$.
לפי השאלה הקודמת:

$$\mathrm{Sp}(U \cup W) = U + W$$

אבל לפי שאלה 7.5.8, $U \cup W$ הוא תת־מרחב אם ורק אם:

$$\mathrm{Sp}(U \cup W) = U \cup W$$

לפיכך $U \cup W$ הוא תת־מרחב אם ורק אם:

$$U \cup W = U + W$$

אבל ראינו בשאלה 7.6.2 ש־ $U \cup W$ הוא תת־מרחב אם ורק אם $U \subseteq W$ או $W \subseteq U$.
לפיכך, $U \cup W = U + W$ אם ורק אם $U \subseteq W$ או $W \subseteq U$.

תשובה 7.6.8 **השאלה בעמוד 186**

ברור כי $\mathrm{Sp}(S) \subseteq \mathrm{Sp}(S \cup T)$ וכן $\mathrm{Sp}(T) \subseteq \mathrm{Sp}(S \cup T)$. מאחר ש־ $\mathrm{Sp}(S \cup T)$ הוא תת־מרחב, הוא סגור לסכומים, ומכאן נובע כי $\mathrm{U} + \mathrm{W} = \mathrm{Sp}(S) + \mathrm{Sp}(T) \subseteq \mathrm{Sp}(S \cup T)$.

בכיוון ההפוך, נתבונן בוקטור $v \in \mathrm{Sp}(S \cup T)$. נוכל לרשום וקטור זה כצירוף לינארי $v = \sum_{i=1}^{n} \lambda_i v_i$, כאשר $\lambda_1, \ldots, \lambda_n$ סקלרים ו־ $v_1, \ldots, v_n \in S \cup T$. אזי לכל $1 \le i \le n$ מתקיים $\lambda_i v_i \in \mathrm{Sp}(S) = U \subseteq U + W$ או $\lambda_i v_i \in \mathrm{Sp}(\mathrm{T}) = W \subseteq U + W$, ובכל מקרה $\lambda_i v_i \in U + W$. מכיוון ש־ $U + W$ הוא תת־מרחב, הוא סגור לסכומים, ולכן $\mathrm{v} \in U + W$. נסיק כי $\mathrm{Sp}(\mathrm{S} \cup \mathrm{T}) \subseteq U + W$ ולכן $\mathrm{Sp}(\mathrm{S} \cup \mathrm{T}) = U + W$, כדרוש.

תשובה 7.7.1 **השאלה בעמוד 187**

$$U_1 = \{(a,b,c) \mid a + b + c = 0\}$$

$$U_2 = \{(a,b,c) \mid a = c\}$$

א. עלינו להוכיח כי U_2 הוא תת־מרחב של $\mathbb{R}^3$.

נשים לב שהוקטורים שב־ U_2 צורתם היא: (a,b,a).

U_2 בוודאי אינו ריק, שכן $(0,0,0) \in U_2$. כמו כן, לכל שני וקטורים u,v ב־ U_2 ולכל שני סקלרים ממשיים λ, μ מתקיים

$$\lambda u + \mu v \in U_2$$

שכן

$$\lambda(a,b,a) + \mu(c,d,c) = (\lambda a + \mu c, \lambda b + \mu d, \lambda a + \mu c)$$

והוקטור שבאגף ימין - רכיבו הראשון שווה לרכיבו השלישי. נסיק אפוא ש־ U_2 הוא תת־מרחב של $\mathbb{R}^3$.

ב. עלינו להוכיח כי:

$$U_1 + U_2 = \mathbb{R}^3$$

כל וקטור $(a,b,c) \in \mathbb{R}^3$ ניתן להצגה כ־

$$(a,b,c) = (0, a - c, c - a) + (a, b + c - a, a) \tag{1}$$

המחובר הראשון באגף ימין של (1) הוא ב־ U_1 והמחובר השני הוא ב־ U_2.

לפיכך:

$$\mathbb{R}^3 \subseteq U_1 + U_2$$

אולם ברור כי

$$\mathbb{R}^3 \supseteq U_1 + U_2$$

ולכן:

$$\mathbb{R}^3 = U_1 + U_2$$

ג. הנה שתי הצגות שונות של וקטור האפס של $\mathbb{R}^3$ כסכום של וקטור מתוך U_1 ווקטור מתוך U_2:

1. $(0,0,0) = (0,0,0) + (0,0,0)$
2. $(0,0,0) = (1,-2,1) + (-1,2,-1)$

תשובה 7.7.2 **השאלה בעמוד 187**

$U_1 = \{(a,0,0) \mid a \text{ ממשי כלשהו}\}$

$U_2 = \{(0,b,c) \mid b,c \text{ ממשים כלשהם}\}$

א. נוכיח כי U_1 הוא תת־מרחב:

1. U_1 אינה ריקה כי $(0,0,0) \in U_1$.
2. $\lambda(a,0,0) + \mu(b,0,0) = (\lambda a + \mu b, 0, 0)$

ומכאן שלכל $u,v \in U_1$ ולכל $\lambda,\mu \in \mathbb{R}$:

$$\lambda u + \mu v \in U_1$$

לפיכך, U_1 הוא תת־מרחב.

נוכיח כי U_2 הוא תת־מרחב.

1. U_2 אינה ריקה כי $(0,0,0) \in U_2$.
2. $\lambda(0,b,c) + \mu(0,d,e) = (0, \lambda b + \mu d, \lambda c + \mu e)$

ומכאן שלכל $u,v \in U_2$ ולכל $\lambda,\mu \in \mathbb{R}$,

$$\lambda u + \mu v \in U_2$$

ולכן U_2 הוא תת־מרחב.

U_1 הוא ציר ה־x ב־$\mathbb{R}^3$ ו־U_2 הוא המישור y-z ב־$\mathbb{R}^3$.

ב. לכל $(a,b,c) \in \mathbb{R}^3$:

$$(a,b,c) = (a,0,0) + (0,b,c) \qquad (1)$$

כלומר, לכל וקטור ב־$\mathbb{R}^3$ יש הצגה כסכום של וקטור מתוך U_1 ווקטור מתוך U_2.

ולכן:

$$\mathbb{R}^3 \subseteq U_1 + U_2$$

אולם ברור כי

$$\mathbb{R}^3 \supseteq U_1 + U_2$$

ולכן:

$$\mathbb{R}^3 = U_1 + U_2$$

ג. נניח כי

$$(a,0,0) + (0,b,c) = (d,0,0) + (0,e,f)$$

הן שתי הצגות של אותו וקטור כסכום של וקטורים מ־U_1 ומ־U_2.

נחבר את הוקטורים בכל אגף ונקבל:

$$(a,b,c) = (d,e,f)$$

ומכאן

$$a = d\ ;\ \ b = e\ ;\ \ c = f$$

ולכן שתי ההצגות מתלכדות.

לפיכך, לכל וקטור ב־$\mathbb{R}^3$ יש הצגה יחידה כסכום של וקטור מתוך U_1 ווקטור מתוך U_2.

תשובה 7.7.3 **השאלה בעמוד 190**

כיוון ראשון:

יהיו U,W תת־מרחבים של V, ונניח כי $V = U \oplus W$.

לפי הגדרת סכום ישר נובע כי $V = U + W$.

כעת, U הוא תת־מרחב ולכן $0 \in U$, וכן W הוא תת־מרחב ולכן $0 \in W$.

מכאן ש־ $0 \in U \cap W$.

נראה כי $U \cap W = \{0\}$, כלומר כי לא ייתכן שהחיתוך של U ו־ W מכיל וקטורים נוספים, פרט לוקטור האפס. נניח בשלילה שקיים וקטור $v \neq 0$, השייך ל־ $U \cap W$. מאחר שחיתוך זה הוא תת־מרחב, הרי שגם $(-v) \in U \cap W$. בפרט נובע מכך כי $v \in U$ ו־ $(-v) \in W$.

עתה נוכל לרשום שתי הצגות **שונות** לוקטור האפס כסכום של וקטור מתוך U עם וקטור מתוך W, כך:

1. $0 = \underset{U}{\underset{\in}{0}} + \underset{W}{\underset{\in}{0}}$

2. $0 = \underset{U}{\underset{\in}{v}} + \underset{W}{\underset{\in}{(-v)}}$

וזאת בסתירה ליחידות ההצגה של כל וקטור ב־ $U \oplus W$.

כיוון שני:

נניח כי $V = U + W$ וכי $U \cap W = \{0\}$, ונוכיח כי לכל וקטור ב־ V יש הצגה יחידה כסכום של וקטור מתוך U ווקטור מתוך W.

ואכן, יהי v וקטור ב־ V ונניח כי יש לו שתי הצגות:

$$v = \underset{U}{\underset{\in}{u_1}} + \underset{W}{\underset{\in}{w_1}} = \underset{U}{\underset{\in}{u_2}} + \underset{W}{\underset{\in}{w_2}} \tag{1}$$

אזי:

$$u_1 - u_2 = w_2 - w_1$$

אבל $u_1 - u_2 \in U$, שכן U תת־מרחב וכן $w_2 - w_1 \in W$, שכן W תת־מרחב, ולכן $u_1 - u_2$ (המופיע גם בשם $w_2 - w_1$) שייך ל־ $U \cap W$, ולכן $u_1 - u_2 = 0$ וגם $w_2 - w_1 = 0$.

כלומר $u_1 = u_2$ וגם $w_2 = w_1$, ולכן שתי ההצגות מתלכדות, הווי אומר - לכל וקטור יש הצגה יחידה כלעיל, ומכאן ש־

$$V = U \oplus W$$

תשובה 7.7.4 **השאלה בעמוד 190**

א. נראה כי $S_{n\times n}^{\mathbb{R}}$ היא תת־מרחב של $\mathbf{M}_{n\times n}^{\mathbb{R}}$:

1. הקבוצה $S_{n\times n}^{\mathbb{R}}$ אינה ריקה, כי למשל מטריצת האפס מסדר $n\times n$, היא סימטרית, ולכן שייכת ל־ $S_{n\times n}^{\mathbb{R}}$.

2. אם A,B הן מטריצות ב־ $S_{n\times n}^{\mathbb{R}}$, כלומר אם A ו־ B הן מטריצות ממשיות סימטריות מסדר $n\times n$ מעל $\mathbb{R}$, אז גם סכומן $A+B$ היא מטריצה סימטרית כזאת (ראו שאלה 3.3.7), כלומר שייכת ל־ $S_{n\times n}^{\mathbb{R}}$.
לפיכך $S_{n\times n}^{\mathbb{R}}$ סגורה לגבי החיבור.

3. אם A היא איבר ב־ $S_{n\times n}^{\mathbb{R}}$, כלומר סימטרית וכן מקיימת $A^t = A$, ואם $\lambda\in\mathbb{R}$, אז מכיוון ש־ $(\lambda A)^t = \lambda A^t$,[3] הרי ש־ $(\lambda A)^t = \lambda A$. לכן גם λA היא מטריצה סימטרית מסדר $n\times n$, ולפיכך $S_{n\times n}^{\mathbb{R}}$ סגורה לכפל בסקלר.

מסקנה: $S_{n\times n}^{\mathbb{R}}$ היא תת־מרחב של $\mathbf{M}_{n\times n}^{\mathbb{R}}$.

ב. נראה כי $A_{n\times n}^{\mathbb{R}}$ היא תת־מרחב של $\mathbf{M}_{n\times n}^{\mathbb{R}}$:

1. $A_{n\times n}^{\mathbb{R}}$ אינה ריקה, כי, למשל, מטריצת האפס מסדר $n\times n$ שייכת ל־ $A_{n\times n}^{\mathbb{R}}$.
2. אם A,B הן מטריצות אנטי־סימטריות, אזי $A^t = -A$ ו־ $B^t = -B$
ולכן:

$$(A+B)^t = A^t + B^t = -A - B = -(A+B)$$

כלומר, גם $A+B$ היא מטריצה אנטי־סימטרית, ולכן $A_{n\times n}^{\mathbb{R}}$ סגורה לגבי החיבור.

3. אם A היא מטריצה אנטי־סימטרית, ואם $\lambda\in\mathbb{R}$ כלשהו, אז $(\lambda A)^t = \lambda A^t = \lambda(-A) = -(\lambda A)$. לכן גם λA היא מטריצה אנטי־סימטרית, ולכן $A_{n\times n}^{\mathbb{R}}$ סגורה ביחס לכפל בסקלר.

מסקנה: $A_{n\times n}^{\mathbb{R}}$ היא תת־מרחב של $\mathbf{M}_{n\times n}^{\mathbb{R}}$.

ג. תהי A מטריצה כלשהי ב־ $\mathbf{M}_{n\times n}^{\mathbb{R}}$, ותהיינה:

$$B = A + A^t$$

$$C = A - A^t$$

B היא מטריצה סימטרית, שכן:

$$B^t = (A+A^t)^t = A^t + (A^t)^t = A^t + A = B$$

C היא מטריצה אנטי־סימטרית, שכן:

$$C^t = (A-A^t)^t = A^t - (A^t)^t = A^t - A = -(A-A^t) = -C$$

3 בדקו!

ד. $$\frac{A+A^t}{2}+\frac{A-A^t}{2}=\frac{1}{2}(A+A^t+A-A^t)=\frac{1}{2}(2A)=A$$

כפי שרצינו להוכיח.

ה. עלינו להוכיח כי:

$$\mathbf{M}_{n\times n}^{\mathbb{R}}=S_{n\times n}^{\mathbb{R}}\oplus A_{n\times n}^{\mathbb{R}}$$

ראשית, בחלקים א ו־ב של השאלה ראינו כי $S_{n\times n}^{\mathbb{R}}$ ו־ $A_{n\times n}^{\mathbb{R}}$ הם תת־מרחבים של $\mathbf{M}_{n\times n}^{\mathbb{R}}$.

כמו כן, ראינו בחלק ג של השאלה כי לכל מטריצה $A\in\mathbf{M}_{n\times n}^{\mathbb{R}}$, $A+A^t$ היא מטריצה סימטרית ולכן גם $\frac{1}{2}(A+A^t)$ היא מטריצה סימטרית, כלומר:

$$\frac{A+A^t}{2}\in S_{n\times n}^{\mathbb{R}}$$

כמו כן, ראינו כי $A-A^t$ היא מטריצה אנטי־סימטרית ולכן גם $\frac{1}{2}(A+A^t)$ היא מטריצה אנטי־סימטרית, כלומר:

$$\frac{A-A^t}{2}\in A_{n\times n}^{\mathbb{R}}$$

תהי $A\in\mathbf{M}_{n\times n}^{\mathbb{R}}$ מטריצה כלשהי. לפי חלק ד נוכל לרשום:

$$A=\underset{\substack{\in\\ S_{n\times n}^{\mathbb{R}}}}{\frac{A+A^t}{2}}+\underset{\substack{\in\\ A_{n\times n}^{\mathbb{R}}}}{\frac{A-A^t}{2}}$$

בכך הוכחנו כי $\mathbf{M}_{n\times n}^{\mathbb{R}}\subseteq S_{n\times n}^{\mathbb{R}}+A_{n\times n}^{\mathbb{R}}$. ההכלה ההפוכה מתקיימת בבירור, ולכן הוכחנו כי $\mathbf{M}_{n\times n}^{\mathbb{R}}=S_{n\times n}^{\mathbb{R}}+A_{n\times n}^{\mathbb{R}}$.

כדי להוכיח כי הסכום דלעיל הוא סכום ישר, עלינו להראות כי:

$$S_{n\times n}^{\mathbb{R}}\cap A_{n\times n}^{\mathbb{R}}=\{O\}$$

תהי A מטריצה ב־ $S_{n\times n}^{\mathbb{R}}\cap A_{n\times n}^{\mathbb{R}}$, כלומר A סימטרית ואנטי־סימטרית גם יחד. כלומר $A^t=A$ וגם $A^t=-A$. לכן $A=-A$ ומכאן נובע בקלות ש־ $A=O$.

לכן:

$$S_{n\times n}^{\mathbb{R}}\cap A_{n\times n}^{\mathbb{R}}\subseteq\{O\}$$

ההכלה בכיוון ההפוך ברורה, ולכן

$$S_{n\times n}^{\mathbb{R}}\cap A_{n\times n}^{\mathbb{R}}=\{O\}$$

ומכאן:

$$\mathbf{M}_{n\times n}^{\mathbb{R}}=S_{n\times n}^{\mathbb{R}}\oplus A_{n\times n}^{\mathbb{R}}$$

תשובה 7.7.5 **השאלה בעמוד 190**

U ו־ W הם תת־מרחבים של V. נתון כי לוקטור האפס יש הצגה יחידה כסכום של וקטורים ב־ U וב־ W. כיוון ש־

$$0 = \underset{V}{\underset{\in}{0}} + \underset{W}{\underset{\in}{0}}$$

נובע כי זוהי ההצגה היחידה האפשרית.

(שימו לב: $0 \in U$ ו־ $0 \in W$ כי U ו־ W הם תת־מרחבים.)

מתוך $0 \in U$, $0 \in W$, נובע $0 \in U \cap W$. נוכיח כי $U \cap W = \{0\}$.

ואכן, נניח בשלילה כי קיים וקטור $0 \neq v$ המקיים $v \in U \cap W$.

$v \in W$, לכן $-v \in W$ (שכן W הוא תת־מרחב). לכן נוכל לרשום:

$$0 = \underset{U}{\underset{\in}{v}} + \underset{W}{\underset{\in}{(-v)}}$$

היות ש־ $v \neq 0$, זוהי הצגה של 0, השונה מההצגה $0 = 0 + 0$, וזאת בסתירה לנתון. לפיכך $U \cap W = \{0\}$. כעת, לפי הנתון $V = U + W$, ולכן נסיק ש־

$$V = U \oplus W$$

תשובה 7.7.6 **השאלה בעמוד 192**

א. נוכיח כי $V = U_1 \oplus \ldots \oplus U_n$ אם ורק אם מתקיימים שני התנאים:

1. $V = U_1 + \ldots + U_n$
2. לכל j $(1 \leq j \leq n)$, $\mathrm{U}_j \cap (U_1 + \ldots + \hat{U}_j + \ldots + U_n) = \{0\}$

נניח שמתקיימים התנאים 1 ו־2, ונוכיח כי הסכום הוא ישר.

די להוכיח כי לכל וקטור ב־ V יש הצגה יחידה כסכום של וקטורים מתוך המרחבים הללו.

נניח כי לוקטור מסוים $v \in V$ יש שתי הצגות.

$$u_1 + \ldots + u_n = v = v_1 + \ldots + v_n$$

כאשר לכל i $(1 \leq i \leq n)$:

$$u_i, v_i \in U_i$$

לכל i $(1 \leq i \leq n)$ נוכל לרשום:

$$v_i - u_i = (u_1 - v_1) + \ldots + (u_{i-1} - v_{i-1}) + (u_{i+1} - v_{i+1}) + \ldots + (u_n - v_n)$$

הוקטור שבאגף שמאל שייך ל־ U_i, ואילו הוקטור שבאגף ימין נמצא ב־

$$U_1 + \ldots + \hat{U}_i + \ldots + U_n$$

על פי תנאי 2, נסיק כי:

לכל i $(1 \leq i \leq n)$

$$v_i - u_i = 0$$

כלומר, לכל i $(1 \leq i \leq n)$

$$v_i = u_i$$

ומכאן ששתי ההצגות אינן אלא אחת, ולכן הסכום הוא ישר.

ובכיוון ההפוך – נניח עתה כי $V = U_1 \oplus \ldots \oplus U_n$. אז ברור כי מתקיים תנאי 1.
נוכיח כי מתקיים גם התנאי 2:

נניח בשלילה כי קיים j שעבורו:

$$U_j \cap (U_1 + \ldots + \hat{U}_j + \ldots + U_n) \neq \{0\}$$

לכן קיים v וקטור השונה מ־ 0 והשייך ל־

$$U_j \cap (U_1 + \ldots + \hat{U}_j + \ldots + U_n)$$

אז $v \in U_j$, ובנוסף לכך יש ל־ v הצגה כסכום של מחוברים מתוך יתר ה־ U_i $(i \neq j)$:

$$v = u_1 + \ldots + \hat{u}_j + \ldots + u_n$$

ומכאן נקבל שתי הצגות **שונות** של 0 כסכום של וקטורים מתוך ה־ U_i השונים, כך:

$$0 = v + (-u_1) + \ldots + (-\hat{u}_j) + \ldots + (-u_n) \qquad (1)$$

וכן

$$0 = 0 + 0 + \ldots + 0 \qquad (2)$$

וזאת בסתירה ליחידות ההצגה של וקטורים בסכום הישר $U_1 \oplus \ldots \oplus U_n$.
מכאן שמתקיים גם 2 כדרוש.

ב. נוכיח כי $V = U_1 \oplus \ldots \oplus U_n$ אם ורק אם מתקיימים שני התנאים:
1. $V = U_1 + \ldots + U_n$
2. ההצגה $\underset{U_1}{\underset{\in}{0}} + \ldots + \underset{U_n}{\underset{\in}{0}} = 0$ היא ההצגה היחידה של 0 כסכום של וקטורים מתוך $U_1, \ldots, U_n$.

נניח שמתקיימים התנאים 1 ו־2, ונוכיח כי הסכום הוא ישר.
כמו קודם, די להוכיח כי לכל וקטור ב־ V יש הצגה יחידה כסכום וקטורים מתוך המרחבים $U_1, \ldots, U_n$.

אכן, אם

$$u_1 + \ldots + u_n = v_1 + \ldots + v_n$$

אז:

$$(u_1 - v_1) + \ldots + (u_n - v_n) = 0$$

בשוויון זה מוצג 0 כסכום של וקטורים מתוך $U_1, \ldots, U_n$, ולכן על פי התנאי 2, לכל i $(1 \le i \le n)$,

$$u_i = v_i$$

ולכן לא תיתכנה שתי הצגות **שונות** של אותו וקטור.
את ההוכחה המיידית לכך שאם הסכום הוא ישר אז מתקיימים התנאים 1 ו־2, נשאיר לקוראים החרוצים.

תשובה 7.7.7 **השאלה בעמוד 192**

יהיו:

$$U_1 = \mathrm{Sp}\left(\{(1,0)\}\right) \ , \ U_2 = \mathrm{Sp}\left(\{(0,1)\}\right) \ , U_3 = \mathrm{Sp}\left(\{(1,1)\}\right)$$

אלה הם שלושה תת־מרחבים, וברור שהחיתוכים ההדדיים $U_1 \cap U_2$, $U_2 \cap U_3$, $U_1 \cap U_3$ מכילים את ראשית הצירים (הווקטור $(0,0)$) בלבד, כלומר:

$$U_1 \cap U_2 = U_1 \cap U_3 = U_2 \cap U_3 = \{0\}$$

כל וקטור (a,b) ניתן להצגה כסכום:

$$(a,b) = (a,0) + (0,b)$$

ובזה הוכחנו כי

$$\mathbb{R}^2 = U_1 + U_2$$

וממילא:

$$\mathbb{R}^2 = U_1 + U_2 + U_3$$

הסכום דלעיל אינו סכום ישר של U_1, U_2 ו־U_3. כי למשל, לוקטור $(1,1)$ יש הצגות שונות ב־$U_1 + U_2 + U_3$, למשל:

$$(1,1) = \underset{\substack{\in \\ U_1}}{(0,0)} + \underset{\substack{\in \\ U_2}}{(0,0)} + \underset{\substack{\in \\ U_3}}{(1,1)}$$

וכן

$$(1,1) = \underset{\substack{\in \\ U_1}}{(1,0)} + \underset{\substack{\in \\ U_2}}{(0,1)} + \underset{\substack{\in \\ U_3}}{(0,0)}$$

וישנן כמובן הצגות נוספות של $(1,1)$ כסכום של וקטורים מתוך U_1, U_2 ו־U_3.

הדוגמה איננה סותרת את משפט 7.7.5, שכן תנאי ב של המשפט אינו מתקיים.

למשל:

$$\mathbb{R}^2 = U_1 + U_2$$

ולכן:

$$U_3 \cap (U_1 + U_2) = U_3 \neq \{0\}$$

תשובה 7.7.8 **השאלה בעמוד 192**

$$\mathbf{e}_1 = (1,0,0,0) \ , \quad \mathbf{e}_2 = (0,1,0,0) \ , \quad \mathbf{e}_3 = (0,0,1,0) \ , \quad \mathbf{e}_4 = (0,0,0,1)$$

$$\mathbf{d}_1 = (1,1,0,0) \ , \quad \mathbf{d}_2 = (0,1,1,0) \ , \quad \mathbf{d}_3 = (0,0,1,1)$$

א. נוכיח כי:

$$\mathrm{Sp}(\{\mathbf{e}_1,\mathbf{e}_2\}) = \mathrm{Sp}(\{\mathbf{e}_1\}) \oplus \mathrm{Sp}(\{\mathbf{e}_2\})$$

קל לראות שמתקיים:

$$\mathrm{Sp}(\{\mathbf{e}_1,\mathbf{e}_2\}) = \left\{\lambda_1(1,0,0,0) + \lambda_2(1,0,0,0) \middle| \lambda_1,\lambda_2 \in \mathbb{R}\right\} = \mathrm{Sp}(\{\mathbf{e}_1\}) + \mathrm{Sp}(\{\mathbf{e}_2\})$$

עתה, אם $\mathbf{v} \in \mathrm{Sp}(\{\mathbf{e}_1\}) \cap \mathrm{Sp}(\{\mathbf{e}_2\})$, אז קיימים $a,b \in \mathbb{R}$ כך ש־

$$\mathbf{v} = (a,0,0,0)$$

$$\mathbf{v} = (0,b,0,0)$$

מכאן מתחייב ש־ $a = b = 0$ ולכן $\mathbf{v} = \mathbf{0}$.

הוכחנו, אם כן, כי

$$\mathrm{Sp}(\{\mathbf{e}_1\}) \cap \mathrm{Sp}(\{\mathbf{e}_2\}) = \{\mathbf{0}\}$$

ולכן:

$$\mathrm{Sp}(\{\mathbf{e}_1,\mathbf{e}_2\}) = \mathrm{Sp}(\{\mathbf{e}_1\}) \oplus \mathrm{Sp}(\{\mathbf{e}_2\})$$

ב. נבדוק אם מתקיים:

$$\left\{(a_1,2a_2,a_2,0) \middle| a_1,a_2 \in \mathbb{R}\right\} = \mathrm{Sp}(\{\mathbf{e}_1,\mathbf{e}_2\}) + \mathrm{Sp}(\{\mathbf{d}_2\}) \qquad (1)$$

$\mathrm{Sp}(\{\mathbf{d}_2\}) = \left\{(0,c,c,0) \middle| c \in \mathbb{R}\right\}$, ולכן:

$$\mathrm{Sp}(\{\mathbf{e}_1,\mathbf{e}_2\}) + \mathrm{Sp}(\{\mathbf{d}_2\}) = \left\{(a,b,0,0) + (0,c,c,0) \middle| a,b,c \in \mathbb{R}\right\}$$

$$= \left\{(a,b+c,c,0) \middle| a,b,c \in \mathbb{R}\right\} = \mathrm{Sp}(\{\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3\})$$

(ודאו לעצמכם את השוויון האחרון.)

לכן אגף ימין של (1) הוא $\mathrm{Sp}(\{\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3\})$, וקל לראות שקיימים וקטורים מן הקבוצה שבאגף ימין של (1) שאינם שייכים לאגף שמאל - כזה הוא, למשל, הוקטור $(0,1,0,0)$.

לכן:

$$\left\{(a_1,2a_2,a_2,0) \middle| a_1,a_2 \in \mathbb{R}\right\} \neq \mathrm{Sp}(\{\mathbf{e}_1,\mathbf{e}_2\}) + \mathrm{Sp}(\{\mathbf{d}_2\})$$

ג.

$$\mathrm{Sp}(\{\mathbf{d}_1\}) = \left\{(a,a,0,0) \middle| a \in \mathbb{R}\right\}$$

$$\mathrm{Sp}(\{\mathbf{d}_2\}) = \left\{(0,b,b,0) \middle| b \in \mathbb{R}\right\}$$

$$\mathrm{Sp}(\{\mathbf{d}_3\}) = \left\{(0,0,c,c) \middle| c \in \mathbb{R}\right\}$$

ולכן:

$$\mathrm{Sp}(\{\mathbf{d}_1\}) + \mathrm{Sp}(\{\mathbf{d}_2\}) + \mathrm{Sp}(\{\mathbf{d}_3\}) = \left\{(a,a+b,b+c,c) \middle| a,b,c \in \mathbb{R}\right\}$$

כדי לבדוק אם

$$\mathrm{Sp}(\{\mathbf{d}_1\}) + \mathrm{Sp}(\{\mathbf{d}_2\}) + \mathrm{Sp}(\{\mathbf{d}_3\})$$

הוא סכום ישר, נבחן אילו הצגות יש ל־ $\mathbf{0}$ כסכום של וקטורים מתוך שלושה תת־מרחבים אלה.

נניח

$$0 = (0,0,0,0) = (a,a,0,0) + (0,b,b,0) + (0,0,b,c)$$

$$= (a,a+b,b+c,c)$$

ומכאן:

$$a = 0$$

$$a + b = 0$$

$$b + c = 0$$

$$c = 0$$

הפתרון היחיד למערכת משוואות זו הוא $a = b = c = 0$, ולכן ההצגה היחידה של $\mathbf{0}$ היא

$$\mathbf{0} = \mathbf{0} + \mathbf{0} + \mathbf{0}$$

ולכן הסכום הוא ישר.

ד. יש להוכיח כי:

$$\mathbb{R}^4 = \mathrm{Sp}(\{\mathbf{e}_1\}) + \mathrm{Sp}(\{\mathbf{d}_1\}) + \mathrm{Sp}(\{\mathbf{d}_2\}) + \mathrm{Sp}(\{\mathbf{d}_3\})$$

ההכלה

$$\mathbb{R}^4 \supseteq \mathrm{Sp}(\{\mathbf{e}_1\}) + \mathrm{Sp}(\{\mathbf{d}_1\}) + \mathrm{Sp}(\{\mathbf{d}_2\}) + \mathrm{Sp}(\{\mathbf{d}_3\})$$

מובנת מאליה.

נוכיח את ההכלה ההפוכה:

$$\mathbb{R}^4 \subseteq \mathrm{Sp}(\{\mathbf{e}_1\}) + \mathrm{Sp}(\{\mathbf{d}_1\}) + \mathrm{Sp}(\{\mathbf{d}_2\}) + \mathrm{Sp}(\{\mathbf{d}_3\})$$

יהי (x_1, x_2, x_3, x_4) וקטור כלשהו ב-$\mathbb{R}^4$.

נראה שניתן להציג אותו כסכום של ארבעה וקטורים מתוך הקבוצות דלעיל כך:

$$(x_1, x_2, x_3, x_4) = (a, 0, 0, 0) + (b, b, 0, 0) + (0, c, c, 0) + (0, 0, d, d) \tag{2}$$

כלומר:

$$(x_1, x_2, x_3, x_4) = (a + b, b + c, c + d, d)$$

על הסקלרים a, b, c, d לקיים אם כן:

$$a + b = x_1$$

$$b + c = x_2$$

$$c + d = x_3$$

$$d = x_4$$

זוהי מערכת משוואות בנעלמים a, b, c, d. בהצבה לאחור מקבלים:

$$d = x_4$$

$$c = x_3 - x_4$$

$$b = x_2 - x_3 + x_4$$

$$a = x_1 - x_2 + x_3 - x_4$$

כלומר:

$$
\begin{aligned}
(x_1,x_2,x_3,x_4) &= (x_1-x_2+x_3-x_4,0,0,0) && (\in \mathrm{Sp}(\{\mathbf{e}_1\}))\\
&+(x_2-x_3+x_4,x_2-x_3+x_4,0,0) && (\in \mathrm{Sp}(\{\mathbf{d}_1\}))\\
&+(0,x_3-x_4,x_3-x_4,0) && (\in \mathrm{Sp}(\{\mathbf{d}_2\}))\\
&+(0,0,x_4,x_4)+ && (\in \mathrm{Sp}(\{\mathbf{d}_3\}))
\end{aligned}
$$

ובכן:

$$\mathbb{R}^4 = \mathrm{Sp}(\{\mathbf{e}_1\}) + \mathrm{Sp}(\{\mathbf{d}_1\}) + \mathrm{Sp}(\{\mathbf{d}_2\}) + \mathrm{Sp}(\{\mathbf{d}_3\})$$

במהלך הפתרון גילינו כבר שקיימת הצגה **יחידה** מהטיפוס (2), ולכן (על פי הגדרת סכום ישר):

$$\mathbb{R}^4 = \mathrm{Sp}(\{\mathbf{e}_1\}) \oplus \mathrm{Sp}(\{\mathbf{d}_1\}) \oplus \mathrm{Sp}(\{\mathbf{d}_2\}) \oplus \mathrm{Sp}(\{\mathbf{d}_3\})$$

ה.

$$\mathrm{Sp}(\{\mathbf{e}_3\}) = \{(0,0,a,0) \mid a \in R\}$$

$$\mathrm{Sp}(\{\mathbf{d}_3\}) = \{(0,0,b,b) \mid b \in R\}$$

נציג

$$\mathbf{0} = (0,0,0,0) = (0,0,a,0) + (0,0,b,b) = (0,0,a+b,b)$$

ומכאן:

$$a+b=0$$

$$b=0$$

כלומר $a=b=0$, ולכן ההצגה היחידה של $\mathbf{0}$ היא

$$\mathbf{0} = \mathbf{0} + \mathbf{0}$$

וממילא $\mathrm{Sp}(\{\mathbf{e}_3\}) + \mathrm{Sp}(\{\mathbf{d}_3\})$ הוא ישר.

ו.

$$\mathrm{Sp}(\{\mathbf{e}_3\}) = \{(0,0,a,0) \mid a \in \mathbb{R}\}$$

$$\mathrm{Sp}(\{\mathbf{e}_4\}) = \{(0,0,0,b) \mid b \in \mathbb{R}\}$$

יהי $\mathbf{v} \in \mathrm{Sp}(\{\mathbf{e}_3\}) \cap \mathrm{Sp}(\{\mathbf{e}_4\})$, אז $\mathbf{v} = (0,0,a,0)$ וכן $\mathbf{v} = (0,0,0,b)$.
מכאן

$$(0,0,a,0) = (0,0,0,b)$$

ולכן $a=b=0$, כלומר $\mathbf{v}=\mathbf{0}$. קיבלנו, אם כן

$$\mathrm{Sp}(\{\mathbf{e}_3\}) \cap \mathrm{Sp}(\{\mathbf{e}_4\}) = \{\mathbf{0}\}$$

ולכן הסכום $\mathrm{Sp}(\{\mathbf{e}_3\}) + \mathrm{Sp}(\{\mathbf{e}_4\})$ הוא **ישר**.

ז. נוכיח כי:

$$\mathrm{Sp}(\{\mathbf{e}_3\}) \oplus \mathrm{Sp}(\{\mathrm{d}_3\}) = \mathrm{Sp}(\{\mathbf{e}_3\}) \oplus \mathrm{Sp}(\{\mathbf{e}_4\}) \tag{1}$$

יהי $\mathbf{v}$ וקטור כלשהו באגף ימין של (1). אז

$$\mathbf{v} = (0,0,a,0) + (0,0,0,b) = (0,0,a,b)$$

כאשר a ו־b סקלרים מסוימים.

נרשום את הוקטור $\mathbf{v}$ בצורה אחרת:

$$\mathbf{v} = (0,0,a,b) = (0,0,\underset{\substack{\in \\ \mathrm{Sp}(\{\mathbf{e}_3\})}}{a-b},0) + (0,0,\underset{\substack{\in \\ \mathrm{Sp}(\{\mathbf{d}_3\})}}{b},b)$$

ולכן

$$\mathbf{v} \in \mathrm{Sp}(\{\mathbf{e}_3\}) \oplus \mathrm{Sp}(\{\mathbf{d}_3\})$$

כלומר:

$$\mathrm{Sp}(\{\mathbf{e}_3\}) \oplus \mathrm{Sp}(\{\mathbf{d}_3\}) \supseteq \mathrm{Sp}(\{\mathbf{e}_3\}) \oplus \mathrm{Sp}(\{\mathbf{e}_4\}) \tag{2}$$

להפך. יהי $\mathbf{v}$ וקטור כלשהו באגף שמאל של (1). אז

$$\mathbf{v} = (0,0,a,0) + (0,0,b,b) = (0,0,a+b,b)$$

כאשר a ו־b סקלרים מסוימים.

עתה נרשום:

$$\mathbf{v} = (0,0,a+b,b) = \underbrace{(0,0,a+b,0)}_{\in \mathrm{Sp}(\{\mathbf{e}_3\})} + \underbrace{(0,0,0,b)}_{\in \mathrm{Sp}(\{\mathbf{e}_4\})}$$

ולכן

$$\mathbf{v} \in \mathrm{Sp}(\{\mathbf{e}_3\}) \oplus \mathrm{Sp}(\{\mathbf{e}_4\})$$

כלומר:

$$\mathrm{Sp}(\{\mathbf{e}_3\}) \oplus \mathrm{Sp}(\{\mathbf{d}_3\}) \subseteq \mathrm{Sp}(\{\mathbf{e}_3\}) \oplus \mathrm{Sp}(\{\mathbf{e}_4\}) \tag{3}$$

מ־(2) ומ־(3) נובע השוויון המבוקש, (1).

תשובה 7.8.1 **השאלה בעמוד 194**

ההוכחה זהה להוכחה שנתנו במקרה הממשי, בתשובה 7.1.12.

תשובה 7.8.2 **השאלה בעמוד 196**

$$P(x) = 1 + 2x + x^3$$

כאשר $F = \mathbb{Z}_2$, מתקיים $f_P(0) = 1 + 2\cdot 0 + 0^3 = 1 + 0 + 0 = 1$, וכן:

$$f_P(1) = 1 + 2\cdot 1 + 1^3 = 1 + 2 + 1 = 0$$

כלומר, הפונקציה f_P "הופכת" את זוג ערכי התחום.

כאשר $F = \mathbb{Z}_3$, מתקיים $f_P(0) = 1 + 2\cdot 0 + 0^3 = 1 + 0 + 0 = 1$, וכן

$$f_P(1) = 1 + 2\cdot 1 + 1^3 = 1 + 2 + 1 = 0 + 1 = 1$$

ולבסוף:

$$f_P(2) = 1 + 2 \cdot 2 + 2^3 = 1 + 4 + 8 = 1 + 3 \cdot 4 = 1 + 0 = 1$$

כלומר, הפונקציה f_P היא הפונקציה הקבועה 1.

תשובה 7.8.3 **השאלה בעמוד 196**

אוסף כל הפונקציות הפולינומיאליות בוודאי אינו ריק, שכן פונקציית האפס היא, בוודאי, פולינומיאלית (היא מתאימה לפולינום האפס). קל לראות, ישירות מן ההגדרה, כי סכום של פונקציות פולינומיאליות וכן כפל פונקציה פולינומיאלית בסקלר, מניבים פונקציה פולינומיאלית. לכן אוסף זה הוא תת־מרחב.

תשובה 7.8.4 **השאלה בעמוד 197**

נעמוד על טיבה של הפונקציה הנתונה בשני המקרים.

א. כאשר $F = \mathbb{Z}_2$, $f(0) = 0$ וכן $f(1) = 1^{-1} = 1$. בזאת עברנו על כל איברי $\mathbb{Z}_2$! מכאן ש־ f היא פונקציית הזהות.

ב. כאשר $F = \mathbb{Z}_3$, $f(0) = 0$, $f(1) = 1^{-1} = 1$, וכן $f(2) = 2^{-1} = 2$, שהרי בשדה $\mathbb{Z}_3$ מתקיים $2 \cdot 2 = 1$. גם כאן, f היא פונקציית הזהות.

אך פונקציית הזהות היא תמיד פולינומיאלית (לכל שדה F), שהרי זוהי, לפי ההגדרה, הפונקציה הפולינומיאלית המתאימה לפולינום $P = x$.

תשובה 7.8.5 **השאלה בעמוד 197**

נניח ש־ f_P ו־ f_Q הן פונקציות פולינומיאליות, כאשר:

$$P = a_0 + a_1 x + \ldots + a_n x^n, \ Q = b_0 + b_1 x + \ldots + b_m x^m$$

נתבונן בפולינום הבא

$$R = c_0 + c_1 x + \ldots + c_{n+m} x^{n+m}$$

כאשר $c_i = a_0 b_i + a_1 b_{i-1} + \ldots + a_i b_0$ לכל i, ותהי f_R הפונקציה הפולינומיאלית המתאימה.

ודאו (על־ידי בדיקה ישירה) כי הפונקציה f_R מתלכדת עם הפונקציה $f_P \cdot f_Q$ על כל איברי F, וממילא האחרונה היא פונקציה פולינומיאלית.

פרק 8: בסיסים ותורת הממד

8.1 תלות לינארית

בפרק 2 הגדרנו מהו בסיס של המרחב F^n: קבוצת וקטורים ב־ F^n, שהיא בלתי תלויה לינארית ופורשת את F^n (הגדרה 2.7.6). תכונות האי־תלות הלינארית והפרישה ב־ F^n, שבאמצעותן מוגדר בסיס ב־ F^n, הוגדרו מצדן תוך הסתמכות על מושג הצירוף הלינארי ב־ F^n.

בפרק הקודם הכללנו את מושג הצירוף הלינארי ב־ F^n בכך שהגדרנו מהו צירוף לינארי במרחב לינארי כללי (הגדרה 7.4.1). כמו כן, הכללנו והגדרנו מתי תת־קבוצה K של מרחב לינארי כללי V פורשת את המרחב V (הגדרה 7.5.2).

ובכן, לצורך הכללת מושג הבסיס, דהיינו הגדרתו עבור מרחב לינארי כללי, חסרים אנו את מושגי התלות הלינארית והאי־תלות הלינארית במרחב כללי. מושגים אלה יוגדרו להלן.

יהי V מרחב לינארי מעל שדה F, ותהי K תת־קבוצה לא ריקה של V. וקטור האפס של V, 0, ניתן כמובן להצגה כצירוף לינארי של וקטורים מתוך K, שהרי אם $v_1,\ldots,v_n$ הם וקטורים כלשהם ב־ K, אז:

$$0 = 0v_1 + \ldots + 0v_n \qquad (*)$$

צירוף לינארי מעין זה הרשום באגף ימין של (*), דהיינו צירוף לינארי שכל מקדמיו הם אפסים, מכונה **צירוף טריוויאלי**. לעומתו – צירוף לינארי אשר לפחות אחד ממקדמיו **שונה מאפס**, מכונה **צירוף לא טריוויאלי**.

הגדרה 8.1.1

א. יהי V מרחב לינארי ותהי K תת־קבוצה של V. נאמר ש־ K **תלויה לינארית** אם קיימים ב־ K וקטורים שונים, $v_1,\ldots,v_n$, אשר וקטור האפס של V, 0, הוא צירוף לינארי לא טריוויאלי שלהם.

ב. קבוצה K המוכלת ב־ V, שאינה תלויה לינארית, מכונה **בלתי תלויה לינארית**.

הערות

א. מן ההגדרה ברור כי תת־קבוצה K של מרחב לינארי V היא בלתי תלויה לינארית אם ורק אם כל הצגה של וקטור האפס, 0, כצירוף לינארי של וקטורים שונים מתוך K, היא טריוויאלית.

לשון אחר: K היא בלתי תלויה לינארית אם ורק אם מתקיים לכל n וקטורים שונים, $v_1,\ldots,v_n \in K$, שאם $\lambda_1,\ldots,\lambda_n$ הם סקלרים שעבורם

$$\lambda_1 v_1 + \ldots + \lambda_n v_n = 0$$

אז בהכרח:

$$\lambda_1 = \lambda_n = \ldots = \lambda_n = 0$$

ב. אם $K=\{v_1,\ldots,v_k\}$ היא תת־קבוצה **סופית**, בת k וקטורים שונים, של מרחב לינארי V, אז K היא בלתי תלויה לינארית אם ורק אם מתוך השוויון

$$\lambda_1 v_1+\ldots+\lambda_k v_k=0$$

כאשר $\lambda_1,\ldots,\lambda_k$ הם סקלרים, נובע בהכרח כי:[1]

$$\lambda_1=\ldots=\lambda_k=0$$

שאלה 8.1.1

הוכיחו את הטענה שבהערה ב לעיל.

התשובה בעמוד 291

ג. בפרק 2 הגדרנו מתי תת־קבוצה סופית $\{\mathbf{a}_1,\ldots,\mathbf{a}_k\}$ של F^n, היא תלויה או בלתי תלויה לינארית (הגדרה 2.6.1). הגדרה 8.1.1 מכלילה את ההגדרה ההיא בשני מובנים. ראשית, שם נסב הדיון על תת־קבוצה **סופית**, וכאן – על תת־קבוצה כלשהי, סופית או אינסופית. שנית, כאן ההגדרה היא עבור תת־קבוצה של וקטורים במרחב לינארי כלשהו ,לאו דווקא F^n.

כדאי שתוודאו, שאם בהגדרה 8.1.1, בכל מקום שבו רשום V, תרשמו F^n, ובכל מקום שבו רשום K, תרשמו $\{\mathbf{a}_1,\ldots,\mathbf{a}_k\}$, כאשר $\mathbf{a}_1,\ldots,\mathbf{a}_k$ הם k וקטורים שונים ב־ F^n, תקבלו הגדרות של תלות ואי־תלות של קבוצה סופית ב־ F^n, המתלכדות עם אלה שניתנו בפרק 2.

שאלה 8.1.2

בכל אחד מחלקי השאלה מתוארת תת־קבוצה של מרחב לינארי. קבעו בכל מקרה אם הקבוצה הנדונה תלויה או בלתי תלויה.

א. קבוצת הפולינומים $\{1+x,1-x,1-x^2\}$ ב־ $\mathbb{R}[x]$.
ב. קבוצת המטריצות ההפיכות מסדר 2×2 מעל הממשיים.
ג. קבוצת הוקטורים $\{(1,-1,0,0),(0,2,-2,0),(0,0,3,-3),(-4,0,0,4)\}$ ב־ $\mathbb{R}^4$.
ד. קבוצת הוקטורים $\{(1,0,1),(0,1,1),(1,1,0)\}$ במרחב $\mathbb{Z}_2^3$.

התשובה בעמוד 291

בשאלות הבאות מסוכמות כמה תכונות בסיסיות של קבוצות תלויות ושל קבוצות בלתי תלויות לינארית.

שאלה 8.1.3

א. יהי V מרחב לינארי. הוכיחו שכל תת־קבוצה של V המכילה את וקטור האפס היא תלויה לינארית.
ב. הוכיחו שכל תת־קבוצה המכילה שני וקטורים פרופורציוניים[2] היא תלויה לינארית.

התשובה בעמוד 292

---

1 שימו לב, אם K היא סופית, אין צורך להתייחס לכל צירוף לינארי של איברים מתוך K. די לעסוק בצירופים הכוללים את **כל** איברי K.

2 נזכיר: שני וקטורים הם פרופורציוניים אם אחד מהם הוא מכפלה בסקלר של האחר.

שאלה 8.1.4

תהי K תת־קבוצה של מרחב לינארי V.

א. נניח ש־ K בלתי תלויה לינארית. הוכיחו שכל תת־קבוצה של K אף היא בלתי תלויה לינארית.

ב. הוכיחו כי אם $K \subseteq T$ ואם T תלויה לינארית, אז K תלויה לינארית.

התשובה בעמוד 292

שאלה 8.1.5

יהי V מרחב לינארי, ויהי v וקטור ב־ V. הוכיחו כי הקבוצה (בת איבר אחד) $\{v\}$ היא תלויה לינארית אם ורק אם $v = 0$.

התשובה בעמוד 293

שאלה 8.1.6

תהי $K = \{v_1,\ldots,v_n\}$ תת־קבוצה בת $n \geq 2$ וקטורים של מרחב לינארי V. הוכיחו כי K תלויה לינארית אם ורק אם לפחות אחד מן הוקטורים ב־ K הוא צירוף לינארי של יתר הוקטורים של K.
במונחי סעיף 7.4, פירוש הדבר שקבוצה היא תלויה לינארית אם ורק אם אחד הוקטורים שבה תלוי לינארית באחרים.[3]

התשובה בעמוד 293

את שהוכחתם במסגרת שאלה 8.1.6 עבור קבוצה סופית של וקטורים נכליל עכשיו לקבוצה כללית. המשפט שנקבל מתאר בוחן שימושי לבדיקת אי־תלותה הלינארית של קבוצת וקטורים נתונה.

משפט 8.1.2

תהי K תת־קבוצה של מרחב לינארי V המכילה לפחות שני איברים. K תלויה לינארית אם ורק אם לפחות אחד מהֶוקטורים שבה ניתן להצגה כצירוף לינארי של וקטורים אחרים מתוכה.[4]

הוכחה

כיוון ראשון:

נניח כי K תלויה לינארית. אם כך, קיימים n וקטורים שונים, $v_1,\ldots,v_n$, ב־ K, ו־ n סקלרים, $\lambda_1,\ldots,\lambda_n$, שלא כולם אפס, המקיימים את השוויון:

$$0 = \lambda_1 v_1 + \ldots + \lambda_n v_n \qquad (*)$$

בלי הגבלת הכלליות, נניח כי $\lambda_1 \neq 0$.[5]

אם $n = 1$, אז השוויון $(*)$ הוא:

$$0 = \lambda_1 v_1$$

---

3 נזכיר: וקטור הוא תלוי לינארית באוסף וקטורים אחרים אם ניתן להציגו כצירוף לינארי שלהם. שאלה 8.1.6 מסבירה את הקשר בין מונח התלות של וקטור בוקטורים אחרים ומונח התלות של קבוצת וקטורים.

4 כלומר, אם אחד הוקטורים תלוי לינארית באחרים.

5 תמיד נוכל לכנות בכינוי v_1 את אחד מאותם המחוברים שבאגף ימין של $(*)$, שמקדמו שונה מאפס.

מאחר ש־ $\lambda_1 \neq 0$, בהכרח $v_1 = 0$. במקרה זה, בוודאי v_1 ניתן להצגה כצירוף לינארי של וקטורים אחרים מתוך K (עם מקדמים שהם כולם אפס).

אם $n > 1$, נוכל להסיק מן השוויון (*) כי

$$\lambda_1 v_1 = (-\lambda_2)v_2 + (-\lambda_3)v_3 + \ldots + (-\lambda_n)v_n \qquad (**)$$

ומאחר ש־ $\lambda_1 \neq 0$, נוכל לכפול את שני אגפי (**) ב־ λ_1^{-1} ולקבל את v_1 כצירוף לינארי של הוקטורים $v_2, \ldots, v_n$.

כיוון שני:

נניח שיש ב־ K וקטור v שתלוי לינארית ביתר איברי הקבוצה K. אזי קיימים וקטורים $v_1, \ldots, v_n$ ב־ K השונים זה מזה ושונים כולם מ־ v, וסקלרים, $\lambda_1, \ldots, \lambda_n$, המקיימים את השוויון

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

ומכאן:

$$0 = (-1)v + \lambda_1 v_1 + \ldots + \lambda_n v_n$$

ניתן אפוא להציג את 0 כצירוף לא טריוויאלי של איברי K, ולכן K תלויה לינארית.[6]

מ.ש.ל.

שאלה 8.1.7

תהי $K \neq \{0\}$ תת־קבוצה של מרחב לינארי V. הוכיחו כי K תלויה לינארית אם ורק אם קיימת קבוצה T, שהיא חלקית ממש ל־ K, שעבורה:

$$\mathrm{Sp}(K) = \mathrm{Sp}(T)$$

התשובה בעמוד 294

שאלה 8.1.8

תהי K תת־קבוצה לא ריקה ובלתי תלויה לינארית במרחב לינארי V, ויהי v וקטור ב־ V שאינו ב־ K. הוכיחו כי v תלוי בקבוצה K אם ורק אם הקבוצה $K \cup \{v\}$ תלויה לינארית.

התשובה בעמוד 295

בפרק 2 הגדרנו מתי **סדרת** וקטורים תלויה לינארית (הגדרה 2.6.1'). לסיום הסעיף, נביא הגדרה מקבילה עבור סדרת וקטורים במרחב לינארי כללי.

הגדרה 8.1.3

תהי $(v_1, \ldots, v_n)$ **סדרת וקטורים** במרחב לינארי V מעל שדה F. נאמר שהסדרה $(v_1, \ldots, v_n)$ **תלויה לינארית** אם קיימים סקלרים $\lambda_1, \ldots, \lambda_n \in F$ שאינם כולם אפס כך ש־ $\lambda_1 v_1 + \ldots + \lambda_n v_n = 0$. אם הסדרה $(v_1, \ldots, v_n)$ אינה תלויה לינארית, נאמר שהיא **בלתי תלויה לינארית**.

---

6 שימו לב שהמקדם של v שונה מאפס!

הערה

לרוב נשמיט את הסוגריים ונאמר כי סדרת הוקטורים $v_1,\ldots,v_n$ תלויה (או בלתי תלויה לינארית), או אף נאמר בקצרה כי הוקטורים $v_1,\ldots,v_n$ תלויים או בלתי תלויים לינארית.

שאלה 8.1.9

תהי $(v_1,\ldots,v_n)$ סדרת וקטורים במרחב לינארי.

א. נניח ש־$(v_1,\ldots,v_n)$ בלתי תלויה לינארית. הראו שהוקטורים בסדרה בהכרח שונים זה מזה.

ב. נניח שהוקטורים $v_1,\ldots,v_n$ שונים זה מזה. הראו שהסדרה $(v_1,\ldots,v_n)$ בלתי תלויה לינארית אם ורק אם הקבוצה $\{v_1,\ldots,v_n\}$ בלתי תלויה לינארית.

התשובה בעמוד 295

לאור שאלה 8.1.9, בדיקת תלות או אי־תלות של סדרת וקטורים אינה קשה (או קלה) יותר מבדיקת תלות או אי־תלות של קבוצת וקטורים.

8.2 בסיסים

את הגדרת הבסיס עבור המרחב F^n כבר ראיתם בפרק 2 (הגדרה 2.7.6). לפני שניגש להכללת ההגדרה עבור מרחב לינארי כללי, נפתח בדיון בלתי פורמלי על אודות מושג זה. מאחר שכבר רכשתם ניסיון עם בסיסים (עבור F^n), אנו מקווים כי דיון זה יעזור לבסס את האינטואיציה שאותה התחלתם לגבש, וכן להכשיר את הקרקע לדיון במושג הכללי.

נניח כי בפנינו קבוצה סופית K של וקטורים במרחב **נוצר סופית** V. ייתכן שהקבוצה K פורשת את כל המרחב V (ולעיתים נאמר בקצרה - "K פורשת"), וייתכן שלא. נניח שאנו הולכים ומוסיפים "באקראי" וקטורים לקבוצה זו. אם הקבוצה כבר פורשת - הוספת וקטורים לא תשנה זאת, ואם אינה פורשת - ייתכן שהוספת וקטורים תהפוך את הקבוצה לקבוצה פורשת. באופן אינטואיטיבי (**ולא פורמלי**) נאמר כי ככל שהקבוצה גדולה יותר, כך "סביר יותר" שהיא פורשת. על דרך השלילה נוכל לומר, שככל שקבוצה קטנה יותר, כך "סביר פחות" שהיא פורשת את המרחב כולו.

מושג האי־תלות מתנהג באופן הפוך. אם $K=\{v_1,...,v_n\}$ קבוצה בת n וקטורים במרחב לינארי, אי־תלות הקבוצה פירושה שמתוך כלל האפשרויות לבחור סקלרים $\lambda_1,...,\lambda_n$, רק האפשרות $\lambda_1=...=\lambda_n=0$ הופכת את הצירוף $\lambda_1v_1+...+\lambda_nv_n$ לוקטור האפס. ככל שמספר האיברים n גדול יותר, כך יש "יותר" אפשרויות לבחירת המקדמים $\lambda_1,...,\lambda_n$, ולכן נהיה "סביר פחות" שהאפשרות היחידה (מתוך שלל האפשרויות השונות) לקבלת וקטור האפס היא האפשרות $\lambda_1=...=\lambda_n=0$. כלומר, ככל שהקבוצה K גדולה יותר, נהיה "סביר פחות" שהיא בלתי תלויה; על דרך השלילה - ככל שקבוצה קטנה יותר, כך "סביר יותר" שהיא בלתי תלויה.

את כל מה שאמרנו באופן בלתי פורמלי, נבסס בהמשך באופן מדויק. יתר על כן, אנו נראה כי הגודל שעבורו קבוצה היא "מספיק גדולה" כדי להיות פורשת, הוא בדיוק הגודל המְרַבִּי שעבורו היא יכולה להיות בלתי תלויה. מתברר כי קיימת נקודת שיווי משקל בין הפרישה והאי־תלות, והיא ייחודית עבור כל מרחב נוצר סופי - נקודת שיווי משקל זו היא מספר n, המתאר את הגודל המרבי של קבוצה בלתי תלויה במרחב, ובו בזמן את הגודל המזערי של קבוצה פורשת במרחב. קבוצה בת n איברים במרחב היא בלתי תלויה אם ורק אם היא פורשת, ובמקרה זה נאמר שהיא **בסיס** למרחב.

הגדרה 8.2.1

יהי V מרחב לינארי ותהי B תת־קבוצה של V.

B היא **בסיס** של[1] V אם מתקיימים שני התנאים:

א. B בלתי תלויה לינארית;

ב. B פורשת את V.

---

1 אפשר לומר גם בסיס **ל־** V.

דוגמאות

א. כבר פגשנו בפרק 2 את הבסיס הסטנדרטי למרחב F^n. יתרה מזו, ראינו שכל קבוצה בלתי תלויה בת n איברים ב־ F^n היא בסיס ל־ F^n (משפט 2.7.11).

ב. קבוצת הפולינומים $\{1, x, x^2, \ldots, x^{n-1}\}$ היא בסיס למרחב הפולינומים $F_n[x]$ מעל F (איברי המרחב $F_n[x]$ הם כל הפולינומים מעל F שמעלתם קטנה מ־ n).

ג. קבוצת הפולינומים $\{1, x, x^2, \ldots, x^n, \ldots\}$ היא בסיס למרחב הפולינומים $F[x]$ מעל F.

▸

שאלה 8.2.1

הוכיחו את הטענה שבדוגמה ב דלעיל.

התשובה בעמוד 295

שאלה 8.2.2

הוכיחו את הטענה שבדוגמה ג דלעיל.

התשובה בעמוד 296

הדוגמה הבאה והשאלה שאחריה הן בחזקת חומר רשות.

דוגמה

ד. נתבונן באוסף כל הסדרות האינסופיות של מספרים ממשיים. אוסף זה מהווה מרחב לינארי מעל שדה המספרים הממשיים – ראו דוגמה ז בסעיף 7.1. נסמן ב־ e_k את הסדרה האינסופית שכל איבריה פרט לאיבר ה־ k הם אפסים והאיבר ה־ k שלה הוא 1. למשל:

$$e_1 = (1, 0, 0, \ldots)$$

$$e_2 = (0, 1, 0, \ldots)$$

▸

שאלה 8.2.3

האם הקבוצה האינסופית, שאיבריה הם הסדרות $e_1, e_2, e_3, \ldots$, מהווה בסיס למרחב הסדרות הממשיות?

התשובה בעמוד 296

במשפט הבא נתונים שני תנאים הכרחיים ומספיקים לכך שתת־קבוצה B של מרחב לינארי V מהווה בסיס ל־ V – אלה התנאים שאליהם חתרנו במסגרת הדיון הבלתי פורמלי שבתחילת הסעיף.

משפט 8.2.2

תהי $B \neq \{0\}$ תת־קבוצה של מרחב לינארי V.

א. B היא בסיס של V אם ורק אם B בלתי תלויה לינארית וכל קבוצה המכילה ממש את B היא תלויה לינארית.[2]

ב. B היא בסיס של V אם ורק אם B פורשת את V, אך כל קבוצה המוכלת ממש ב־ B אינה פורשת את V.[3]

הוכחה

א. **כיוון ראשון:**

נניח כי B מהווה בסיס. אזי B בוודאי בלתי תלויה לינארית. נשאר להוכיח שכל קבוצה המכילה ממש את B היא תלויה לינארית.

אם T תת־קבוצה של V המכילה ממש את B, אז קיים ב־ T וקטור v שאינו שייך ל־ B. מאחר ש־ B היא בסיס, B בוודאי פורשת את V, ולכן v ניתן להצגה כצירוף לינארי של וקטורים מתוך B, ולכן על סמך משפט 8.1.2, הקבוצה $B \cup \{v\}$ היא תלויה לינארית.[4] הקבוצה $B \cup \{v\}$ בוודאי חלקית (או שווה) ל־ T, ולכן גם T תלויה לינארית (ראו שאלה 8.1.4).

הוכחנו, אם כן, כי כל קבוצה המכילה ממש את B היא תלויה לינארית.

כיוון שני:

נניח כי B היא בלתי תלויה לינארית, ושכל קבוצה המכילה ממש את B היא תלויה לינארית, ונוכיח כי B היא בסיס.

לשם כך, כל שעלינו להוכיח הוא כי $\mathrm{Sp}(B) = V$. ואמנם, אילו היה קיים ב־ V וקטור שאינו תלוי לינארית בקבוצה B, אז הקבוצה $B \cup \{v\}$, המכילה ממש את B, הייתה בלתי תלויה לינארית (ראו שאלה 8.1.8) – בסתירה להנחתנו ביחס ל־ B.

לכן B בהכרח פורשת את V וממילא B בסיס של V.

ב. **כיוון ראשון:**

נניח כי B היא בסיס. אז בפרט B פורשת את V.

נוכיח כי כל קבוצה המוכלת ממש ב־ B אינה פורשת את V.

אכן, אם T קבוצה המוכלת ממש ב־ B, אז קיים ב־ B וקטור v שאינו שייך ל־ T. אילו T הייתה פורשת את V, אז v היה צירוף לינארי של וקטורים מתוך T. הווי אומר, ב־ B היה

2 כלומר, B בסיס אם ורק אם B בלתי תלויה, אבל תוספת איברים ל־B הופכת אותה לקבוצה תלויה לינארית.

3 כלומר, B בסיס אם ורק אם B פורשת את V, אבל השמטת איברים מ־ B הופכת אותה לקבוצה שאינה פורשת את V.

4 שימו לב, הקבוצה B מכילה לפחות וקטור אחד, כי הקבוצה הריקה אינה פורשת שום מרחב לינארי. לכן הקבוצה $B \cup \{v\}$ מכילה לפחות שני איברים, ומכאן הרשות להשתמש במשפט.

קיים וקטור שהוא צירוף לינארי של וקטורים אחרים מתוך B, ומכאן נובע, על סמך משפט 8.1.2, כי B תלויה לינארית, בסתירה לכך ש־ B היא בסיס. לכן אין קבוצות חלקיות ממש ל־ B הפורשות את B.

כיוון שני:

נניח כי B פורשת את V, ושאין קבוצה חלקית ממש ל־ B הפורשת את V.

נוכיח כי B היא בסיס. לשם כך עלינו להוכיח כי B בלתי תלויה לינארית. אם יש ב־ B איבר אחד - ברור ש־ B בלתי תלויה לינארית, כי $B \neq \{0\}$ לפי הנתון. נוכל, אם כן, להניח כי יש ב־ B לפחות שני איברים. עתה, אילו B הייתה תלויה לינארית, היה בה וקטור כלשהו v שהוא צירוף לינארי של וקטורים אחרים מתוך B, ואז הקבוצה T, החלקית ממש ל־ B, המורכבת מכל איברי B פרט ל־ v, הייתה פורשת את V. נסביר:

הוקטור v ניתן להצגה בצורה $v = \lambda_1 v_1 + \ldots + \lambda_k v_k$, כאשר $v_1, \ldots, v_k \in T$ ו־ $\lambda_1, \ldots, \lambda_k$ סקלרים. בכל צירוף לינארי של וקטורים מ־ B שבו מופיע v, ניתן להחליף את v בצירוף $\lambda_1 v_1 + \ldots + \lambda_k v_k$. כך מתקבל צירוף לינארי של וקטורים מתוך T. לכן $\mathrm{Sp}T = \mathrm{Sp}B = V$, בסתירה להנחתנו ביחס ל־ B. לכן B בלתי תלויה לינארית, ומכאן ש־ B בסיס.

מ.ש.ל.

המשפט האחרון מלמדנו כי אם B הוא בסיס של מרחב לינארי V, אז אי־אפשר להוסיף איברים ל־ B או להשמיט איברים מ־ B ועם זאת להישאר עם בסיס: אם מוסיפים איברים ל־ B אז (על פי חלק א) מתקבלת קבוצה תלויה לינארית, ואם משמיטים איברים מ־ B אז (על פי חלק ב) מתקבלת קבוצה שאינה פורשת.

הווי אומר: כל בסיס הוא קבוצה **מרבית** מבחינת תכונת האי־תלות, ובאותה עת הוא קבוצה **מזערית** מבחינת הפרישה. בהתאם למשפט 8.2.2, תכונת המרביות ביחס לאי־תלות, וכמוה תכונת המזעריות ביחס לפרישה, **מאפיינות** את מושג הבסיס.

לאור האמור לעיל, משפט 8.2.2 שקול למשפט הבא:

משפט 8.2.3

תהי $B \neq \{0\}$ תת־קבוצה של מרחב לינארי V.

א. B היא בסיס אם ורק אם B היא קבוצה בלתי תלויה מרבית ב־ V.

ב. B היא בסיס אם ורק אם B היא קבוצה מזערית הפורשת את V.

השאלה הטבעית הנשאלת בשלב זה היא - האם לכל מרחב לינארי יש בסיס? עבור מרחבים נוצרים סופית, המשפט הבא נותן תשובה חיובית.

משפט 8.2.4

לכל מרחב לינארי נוצר סופית השונה מ־ $\{0\}$, יש בסיס (סופי).[5]

הערה

המרחב $\{0\}$ הוא בוודאי מרחב נוצר סופית, והוא עצמו סופי. אבל הקבוצה $\{0\}$ תלויה לינארית ולכן אינה בסיס. המרחב $\{0\}$ נהנה ממעמד מיוחד של מרחב נוצר סופית חסר בסיס.[6]

הוכחה

יהי $V \neq \{0\}$ מרחב נוצר סופית, ויהי n המספר הטבעי המזערי שעבורו קיימת ל־ V קבוצה בת n איברים הפורשת אותו. תהי B קבוצה פורשת של V בת n איברים. נוכל להניח ש־ $0 \notin B$, כי אם $0 \in B$ אז גם הקבוצה המתקבלת מ־ B לאחר השמטת 0 פורשת את V. (נמקו!), בסתירה למזעריות של n.

אם B היא בלתי תלויה, אז B היא בסיס וסיימנו. אם B תלויה לינארית, אז מובטח שיש בה לפחות שני איברים (מדוע?), ולכן על סמך משפט 8.1.2, יש ב־ B וקטור v התלוי לינארית ביתר $n-1$ איברי B.

נסמן ב־ B_1 את הקבוצה בת $n-1$ האיברים המתקבלת מ־ B לאחר השמטת v. הקשר בין B ל־ B_1 הוא:

$$B = B_1 \cup \{v\}$$

מאחר ש־ v תלוי לינארית ב־ B_1, נובע כי:

$$\mathrm{Sp}\left(B_1 \cup \{v\}\right) = \mathrm{Sp}(B_1)$$

אבל

$$\mathrm{Sp}\left(B_1 \cup \{v\}\right) = \mathrm{Sp}(B) = V$$

ולכן B_1 היא קבוצה בת $n-1$ איברים הפורשת את V, בסתירה למזעריות של n.

מ.ש.ל.

הערה

בהמשך הפרק, בכל עת שנכתוב קבוצת וקטורים כגון $\{v_1,\ldots,v_n\}$ במרחב לינארי, נניח במובלע שהוקטורים $v_1,\ldots,v_n$ כולם שונים זה מזה, כלומר שבקבוצה יש בדיוק n איברים.

5 כזכור, מרחב V הוא נוצר סופית אם מוכלת בו קבוצה **סופית** B שעבורה $\mathrm{Sp}(B) = V$.

6 יש הנוהגים לפי מוסכמה אחרת, שלפיה הקבוצה הריקה פורשת את המרחב $\{0\}$ ובשל כך היא אף בסיס שלו. בהתאם למוסכמה זו, לכל מרחב לינארי נוצר סופית יש בסיס.

משפט 8.2.5

יהי $V \neq \{0\}$ מרחב לינארי ותהי $B = \{v_1,\ldots,v_n\}$ תת־קבוצה של V בת n איברים. B היא בסיס של V אם ורק אם לכל וקטור $v \in V$ יש הצגה יחידה כצירוף לינארי של הוקטורים $v_1,\ldots,v_n$.

הערה

באומרנו "הצגה יחידה" הכוונה היא, כרגיל, ליחידות עד כדי סדר המחוברים. אין אנו מבחינים כאן בין הצירוף

$$\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_n v_n$$

לצירופים שבהם מופיעים בדיוק אותם מחוברים אך בסדר שונה.

הוכחה

כיוון ראשון:

נניח כי $B = \{v_1,\ldots,v_n\}$ היא בסיס. אז בפרט $\mathrm{Sp}(B) = V$, ולכן כל וקטור v ב־ V ניתן להצגה כצירוף לינארי של וקטורים מתוך B. אם בצירוף כזה לא מופיעים כל ה־ v_i ־ים $(1 \le i \le n)$, נוכל להוסיף את החסרים עם מקדם אפס. לכן, לכל $v \in V$ יש הצגה שצורתה:

$$\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_n v_n$$

נותר להוכיח שהצגתו של כל וקטור בצורה כזאת היא יחידה.

נניח שלוקטור V יש שתי הצגות:

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

וכן:

$$v = \mu_1 v_1 + \ldots + \mu_n v_n$$

אם כך, מתקיים:

$$\mu_1 v_1 + \ldots + \mu_n v_n = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

לאחר העברת אגפים וכינוס איברים נקבל:

$$(\mu_1 - \lambda_1)v_1 + \ldots + (\mu_n - \lambda_n)v_n = 0$$

מאחר ש־ $v_1,\ldots,v_n$ בלתי תלויים, נובע מהשוויון האחרון כי לכל i $(1 \le i \le n)$, $\mu_i - \lambda_i = 0$, כלומר:

$$\mu_i = \lambda_i$$

כיוון שני:

נניח שלכל $v \in V$ יש הצגה יחידה כצירוף לינארי

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

ונוכיח כי $B = \{v_1 \ldots v_n\}$ היא בסיס.

א. מן ההנחה נובע בפרט כי כל וקטור ב־ V תלוי לינארית ב־ B, כלומר B פורשת את V.

ב. מיחידות ההצגה של כל וקטור נובע, בפרט, כי ההצגה הטריוויאלית

$$0 = 0v_1 + \ldots + 0v_n$$

היא ההצגה **היחידה** של וקטור האפס כצירוף לינארי של $v_1,...,v_n$, ולכן B בלתי תלויה. B היא, אם כן, קבוצה פורשת (ראו א לעיל) ובלתי תלויה (ראו ב לעיל) ולכן B בסיס.

מ.ש.ל.

שאלה 8.2.4

תהי A המטריצה:

$$A = \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 2 & 1 & -2 \\ 2 & 3 & 2 & -3 \\ 2 & 3 & 2 & -3 \end{bmatrix}$$

מצאו בסיס למרחב הפתרונות של המערכת ההומוגנית $A\mathbf{x} = \mathbf{0}$.

התשובה בעמוד 297

משפט 8.2.4 קובע כי לכל מרחב לינארי נוצר סופית יש בסיס. אך מה לגבי מרחבים שאינם נוצרים סופית? בשאלה 8.2.1 ראיתם כי קבוצת הפולינומים $\{1, x, x^2, \ldots, x^n, \ldots\}$ (שהיא קבוצה אינסופית) מהווה בסיס למרחב הפולינומים $F[x]$ מעל שדה F – זוהי דוגמה לבסיס עבור מרחב שאינו נוצר סופית (ראו שאלה 7.5.14). באופן כללי, לא תמיד נוכל לתאר בצורה מפורשת בסיס לכל מרחב לינארי (רמזנו לכך בשאלה 8.2.3). למרות זאת, תחת ההנחות המקובלות על אודות אקסיומות היסוד של המתמטיקה, ניתן להוכיח כי לכל מרחב לינארי **קיים** בסיס, גם אם לא תמיד ניתן לתארו באופן מפורש. הוכחה זו חורגת מגבולות קורס זה, שבו אנו מתמקדים בעיקר במרחבים נוצרים סופית.[7]

כעת נביא שימוש מעניין נוסף למשפט 8.2.4. בפרק 5 ציינו, בלא הוכחה, כי מספר איבריו של שדה סופי הוא חזקה של מספר ראשוני. בעזרת משפט 8.2.4 נוכל עתה להוכיח זאת. ההוכחה היא בחזקת חומר רשות, אך נציין כי מדובר בהוכחה קלאסית ואלגנטית ביותר, ואנו ממליצים כי תעיינו בה.

משפט 8.2.6

יהי F שדה סופי. מספר איברי F הוא חזקה של מספר ראשוני.

הוכחה

לכל מספר טבעי n, נסמן ב־ n_F את האיבר הבא מתוך F,

$$\underbrace{1_F + 1_F + \ldots + 1_F}_{\text{פעמים } n}$$

כאשר 1_F הוא איבר היחידה של F.

7 עבור קוראים בעלי רקע בתורת הקבוצות, המכירים את הלמה של צורן (באופן שקול, את אקסיומת הבחירה), נתאר בקצרה את רעיון ההוכחה: אם V מרחב לינארי, נסמן ב־ B את אוסף התת־קבוצות הבלתי תלויות לינארית של V, הסדור חלקית לפי יחס ההכלה. לכל תת־קבוצה של B הסדורה באופן מלא, איחוד כל איבריה מהווה חסם עליון לקבוצה. לפי הלמה של צורן, ב־ B יש איבר מרבי. איבר זה הוא הבסיס המבוקש.

נתבונן בסדרת האיברים $1_F, 2_F, 3_F, \ldots$. מכיוון ש־ F סופי, סדרה זו כוללת מספר סופי בלבד של איברים מתוך F. לכן בהכרח קיימים שני מספרים טבעיים, $n < m$, כך ש־ $n_F = m_F$. קל לראות כי $m_F - n_F = (m-n)_F$, ולכן $k_F = 0_F$, כאשר $k = m - n$ הוא מספר טבעי מסוים. יהי p המספר הטבעי **המזערי** המקיים $p_F = 0_F$. נראה כי p הוא מספר ראשוני. תחילה נבחין כי בהכרח $p \neq 1$, שכן בכל שדה מתקיים $0_F \neq 1_F$. כעת נניח בשלילה ש־ p מספר פריק, ונרשום $p = mn$, כאשר m,n מספרים טבעיים הקטנים מ־ p. קל לראות כי $(mn)_F = m_F n_F$, ולכן $m_F n_F = 0_F$. מכך נובע ש־ $m_F = 0_F$ או $n_F = 0_F$, בסתירה למזעריות p.

נתבונן עתה בקבוצה $F_p = \{0_F, 1_F, \ldots, (p-1)_F\}$. תוכלו לבדוק ישירות, כי קבוצה זו מהווה תת־שדה של F, בעל p איברים (בדיקה זו דומה לבדיקה כי השדה $\mathbb{Z}_p$, אודותיו למדתם בפרק 5, הוא שדה ראשוני). אך כל שדה מהווה מרחב לינארי מעל כל תת־שדה שלו (עיינו בסעיף 7.1, דוגמה ב), ולכן F הוא מרחב לינארי מעל F_p. מאחר ש־ F סופי **כקבוצה**, הוא בוודאי נוצר סופית כמרחב לינארי - הוא נוצר על־ידי קבוצת כל איבריו, למשל. לכן, לפי משפט 8.2.4, קיים בסיס $\{v_1, \ldots, v_d\}$ ל־ F מעל F_p. כעת, כל איבר ב־ F ניתן לביטוי בצורה **אחת ויחידה** כ־ $t_1v_1 + \ldots + t_dv_d$, כאשר $t_1, \ldots, t_d$ סקלרים מתוך F_p. מאחר שב־ F_p ישנם p איברים, מספר האפשרויות לבחירת הסקלרים הללו הוא p^d, ולכן ב־ F ישנם בדיוק p^d איברים.

מ.ש.ל.

הערה

בפרק 5 ציינו שגם המשפט "ההפוך" למשפט 8.2.6 מתקיים - עבור כל מספר טבעי שהוא חזקה של ראשוני, קיים שדה סופי שזהו מספר איבריו. את המשפט הזה לא נוכיח במסגרת הקורס הנוכחי. הקוראים המעוניינים יוכלו ללמוד את הוכחת המשפט במסגרת הקורס "הרחבת שדות ותורת גלואה".

עד כה דנו במושג הבסיס באופן תיאורטי. כעת נדון בשאלה המעשית הבאה: נניח כי מרחב לינארי V נתון על־ידי קבוצה סופית $\{v_1, \ldots, v_k\}$ של וקטורים הפורשת אותו. כיצד נמצא בסיס למרחב?

השיטה היא פשוטה. תחילה נבדוק האם הקבוצה הנתונה בלתי תלויה לינארית. אם היא בלתי תלויה, אזי היא מהווה בסיס. אם היא תלויה, אז לפי משפט 8.1.2, אחד הוקטורים שבה תלוי לינארית באחרים, ונוכל להשמיטו מן הקבוצה. אם הקבוצה החדשה שהתקבלה היא בלתי תלויה לינארית, היא מהווה בסיס, ואם לא - נוכל להשמיט גם ממנה וקטור אחד, וחוזר חלילה.

שאלה 8.2.5

נתבונן בתת־מרחב

$$U = \operatorname{Sp}\left\{\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 2\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 1 & 1\end{pmatrix}, \begin{pmatrix}-1 & 2\\ 2 & 2\end{pmatrix}\right\}$$

של $\mathbf{M}_2(\mathbb{R})$. מצאו בסיס ל־ U.

התשובה בעמוד 298

8.3 הממד של מרחב לינארי נוצר סופית

בסעיף הקודם הוכחנו כי לכל מרחב נוצר סופית יש בסיס. דוגמה טיפוסית של מרחב נוצר סופית הוא המרחב F^n. ואמנם, זהו מרחב שיש לו בסיס; למשל הבסיס הסטנדרטי $\{\mathbf{e}_1,...,\mathbf{e}_n\}$.

שאלה 8.3.1

הוכיחו כי אם F הוא שדה אינסופי כלשהו, אז ל־ F^n יש אינסוף בסיסים שונים זה מזה.

התשובה בעמוד 298

לכל הבסיסים של F^n יש תכונה משותפת: בכולם יש אותו מספר איברים - בדיוק n. בסעיף זה נוכיח כי אם V הוא מרחב נוצר סופית כלשהו, אז לכל הבסיסים של V יש אותו מספר איברים. למספר זה נקרא **הממד של המרחב** V. להוכחת טענה זו ניעזר בלמה הבאה:

למה 8.3.1

יהי V מרחב לינארי מעל שדה F, הנפרש על־ידי k וקטורים $v_1,...,v_k$, ויהיו $u_1,...,u_m$ וקטורים ב־ V. אם $m > k$, אז הקבוצה $\{u_1,...,u_m\}$ תלויה לינארית.

הוכחה

כל אחד מ־ m הווקטורים $u_1,...,u_m$ ניתן להצגה כצירוף לינארי של $v_1,...,v_k$. הווי אומר, קיימים סקלרים λ_{ji} כך ש־

$$(1)\qquad \begin{aligned} &u_1 = \sum_{j=1}^{k}\lambda_{j1}v_j \ ; \ u_2 = \sum_{j=1}^{k}\lambda_{j2}v_j \ ; \ \dots \ ; \\ &u_i = \sum_{j=1}^{k}\lambda_{ji}v_j \ ; \ \dots \ ; \ u_m = \sum_{j=1}^{k}\lambda_{jm}v_j \end{aligned}$$

נתבונן בצירוף לינארי כלשהו של $u_1,...,u_m$,

$$\sum_{i=1}^{m}x_iu_i$$

כאשר $x_1,\dots,x_m \in F$. על־ידי הצבת הביטויים המתאימים עבור $u_1,...,u_m$ נקבל:

$$(2)\qquad \sum_{i=1}^{m}x_iu_i = \sum_{i=1}^{m}x_i\left[\sum_{j=1}^{k}\lambda_{ji}v_j\right]$$

ועל־ידי החלפת סדר הסכימה באגף ימין של (2) נקבל:

$$(3)\qquad \sum_{i=1}^{m}x_iu_i = \sum_{j=1}^{k}\left[\sum_{i=1}^{m}\lambda_{ji}x_i\right]v_j$$

המקדמים של $v_1,...,v_k$ בסכום שבאגף ימין של (3) תלויים בערכים של $x_1,...,x_m$.

נבדוק אילו ערכים נוכל לתת ל־ $x_1,\dots,x_m$ כך שהמקדמים של הוקטורים $v_1,\dots,v_k$ ישוו כולם ל־ 0.
לשם כך עלינו לבדוק מה הם הפתרונות האפשריים של המערכת הלינארית (בנעלמים $x_1,\dots,x_m$).

$$\begin{array}{ccccc} \lambda_{11}x_1 & +\dots+ & \lambda_{1m}x_m & = & 0 \\ \vdots & & \vdots & = & \vdots \\ \lambda_{k1}x_1 & +\dots+ & \lambda_{km}x_m & = & 0 \end{array} \qquad (4)$$

(הסכום שבאגף שמאל כאן הוא המקדם של v_1, ואותו השווינו לאפס. בדומה - ביחס למקדמים של יתר ה־ v_j $(1 \le j \le k)$.)

המערכת (4) היא מערכת הומוגנית של k משוואות לינאריות ב־ m נעלמים. מאחר ש־ $m > k$ זוהי מערכת משוואת הומוגנית שבה מספר המשתנים גדול ממספר המשוואות, וכפי שלמדתם בפרק 1, למערכת כזאת יש פתרון לא טריוויאלי.[1] הווי אומר, קיימת m־יה של סקלרים $(\mu_1,\dots,\mu_m)$ שלא כולם אפס, שהצבתם במקום ה־ m־יה $(x_1,\dots,x_m)$ באגף ימין של (3) תגרום להתאפסות המקדמים של כל v_j $(1 \le j \le k)$, וממילא להתאפסות אגף ימין של (3).

מן השוויון (3) נוכל אפוא להסיק כי קיימים סקלרים $\mu_1,\dots,\mu_m$, שלא כולם אפסים, שעבורם

$$\sum_{i=1}^{m} \mu_i u_i = 0$$

ולכן קבוצת הוקטורים $\{u_1,\dots,u_m\}$ תלויה לינארית, כפי שרצינו להוכיח.

מ.ש.ל.

מסקנות חשובות מלמה 8.3.1 מסוכמות במשפט שלפניכם:

משפט 8.3.2

יהי V מרחב לינארי. אם ל־ V יש בסיס בעל n וקטורים, אז:

א. כל קבוצה של וקטורים מתוך V, שיש בה יותר מ־ n וקטורים, היא תלויה לינארית.
ב. כל קבוצה של וקטורים מתוך V, שיש בה פחות מ־ n וקטורים, אינה פורשת את V.
ג. כל קבוצה בלתי תלויה לינארית של וקטורים מתוך V, המכילה בדיוק n וקטורים, היא בסיס של V.
ד. כל קבוצה הפורשת את V, ומכילה בדיוק n וקטורים, היא בסיס של V.
ה. בכל בסיס של V יש בדיוק n איברים.

שאלה 8.3.2

הוכיחו את משפט 8.3.2.

התשובה בעמוד 299

1 משפט 1.13.1.

לאור חלק ה של משפט 8.3.2, נוכל להגדיר:

הגדרה 8.3.3

יהי $V \neq \{0\}$ מרחב לינארי נוצר סופית. מספר האיברים בבסיס כלשהו של V מכונה **הממד של** V, וסימנו המקובל – $\dim V$.[2]

למען השלמות, נגדיר גם את ממד המרחב הכולל את וקטור האפס בלבד, כך:

$$\dim\{0\} \overset{\text{def}}{=} 0$$

הערה

אם $V \neq \{0\}$ אז כל בסיס של V כולל לפחות וקטור אחד (שבוודאי שונה מאפס), שכן $V \neq \{0\} = \operatorname{Sp}(\{0\})$, לכן בהכרח $\dim V \geq 1$.

משפט 8.3.4

אם V הוא מרחב לינארי נוצר סופית ו־ U הוא תת־מרחב של V, אז:

א. U הוא מרחב נוצר סופית, ומתקיים:

$$\dim U \leq \dim V$$

ב. השוויון $\dim U = \dim V$ מתקיים אם ורק אם $U = V$.

הוכחה

א. נסמן $\dim V = n$. בהתאם למשפט 8.3.2א, בכל קבוצה בלתי תלויה לינארית ב־ V יש לכל היותר n וקטורים.

יהי U תת־מרחב כלשהו של V. אם $U = \{0\}$, ברור כי U נוצר סופית, ומאחר ש־ $\dim\{0\} = 0$, ברור גם כי $\dim U \leq \dim V$. אם $U \neq \{0\}$, אז מוכלות ב־ U קבוצות בלתי תלויות לינארית (למשל: כל קבוצה המכילה וקטור אחד השונה מאפס מתוך U, היא בלתי תלויה לינארית).

כמו כן, ברור כי בכל קבוצה בלתי תלויה לינארית של וקטורים מתוך U יש לכל היותר n וקטורים, שכן קבוצה כזאת היא בפרט קבוצה בלתי תלויה של וקטורים מתוך V.

עתה, מאחר שמספר האיברים בקבוצות הבלתי תלויות של וקטורים מתוך U חסום על־ידי n,[3] ברור שבין הקבוצות הבלתי תלויות ב־ U קיימת קבוצה B שמספר האיברים בה הוא מרבי. בכל

2 dim היא ראש התיבה dimension, שפירושה ממד.

3 כלומר, אינו יכול לעלות על n.

תת־קבוצה של U המכילה ממש את B יש יותר איברים מאשר ב־ B,[4] ולכן כל תת־קבוצה כזאת היא תלויה לינארית. הווי אומר, B היא קבוצה בלתי תלויה מרבית, וממילא בסיס של U.
מצאנו, אם כן, כי לתת־מרחב U יש בסיס B שמספר איבריו קטן מ־ או שווה ל־ n. מכאן נובע הן כי U הוא נוצר סופית (למשל, הקבוצה B היא קבוצת יוצרים סופית של U) והן כי הממד של U מקיים:

$$\dim U \le \dim V$$

ב. ברור שאם $U = V$, אז $\dim U = \dim V$. נוכיח את הכיוון השני.
נניח כי $\dim U = \dim V$. יהי n הממד המשותף ל־ U ול־ V, ותהי הקבוצה $\{u_1,\ldots,u_n\}$ בסיס ל־ U. קבוצה זו מוכלת כמובן ב־ V, כי $U \subseteq V$. זוהי, אם כן, קבוצה בלתי תלויה בת n וקטורים במרחב ה־ n־ממדי V, ולכן היא בסיס למרחב V וממילא פורשת אותו.[5] הווי אומר:

$$U = \mathrm{Sp}\left(\{u_1,\ldots,u_n\}\right) = V$$

כלומר:

$$U = V$$

מ.ש.ל.

משפט 8.3.5

יהי $V \ne \{0\}$ מרחב לינארי n־ממדי, ותהי A קבוצה בלתי תלויה לינארית בת k וקטורים ב־ V.
אם $k < n$, אז קיימים וקטורים $v_{k+1},\ldots,v_n$, כך שהקבוצה $A \cup \{v_{k+1},\ldots,v_n\}$ היא בסיס ל־ V.

ובניסוח קצר המסבר את האוזן:
כל קבוצה בלתי תלויה לינארית במרחב נוצר סופית ניתנת ל**השלמה** לבסיס.

הוכחה

אם $k < n$, אז הקבוצה A בוודאי אינה בסיס (מדוע?).[6] לכן קיים וקטור $v_{k+1} \in V$ שאינו תלוי לינארית בקבוצה A, ולכן הקבוצה $A \cup \{v_{k+1}\}$ היא בלתי תלויה לינארית. עתה, אם $k+1 < n$, אז, כמו קודם, הקבוצה $A \cup \{v_{k+1}\}$ אינה בסיס וקיים וקטור v_{k+2} שאינו תלוי בה, כלומר הקבוצה $A \cup \{v_{k+1}, v_{k+2}\}$ היא בלתי תלויה לינארית. באופן זה אפשר להמשיך בהוספת וקטורים לקבוצה A, תוך שמירת האי־תלות עד שמגיעים לקבוצה בלתי תלויה בעלת n וקטורים, וקבוצה זו היא בהכרח בסיס (משפט 8.3.2ג).

מ.ש.ל.

4 כלומר, מוכלת ב־ U קבוצה בלתי תלויה B, בעלת התכונה שמספר האיברים של כל קבוצה בלתי תלויה אחרת אינו עולה על מספר איברי B.

5 משפט 8.3.2ג.

6 משפט 8.3.2ב.

משפט 8.3.6

יהיו U ו־ W שני תת־מרחבים של מרחב לינארי נוצר סופית V. אזי:

$$\dim(U+W) = \dim U + \dim W - \dim(U \cap W)$$ [7]

הוכחה

נניח כי $U \cap W \neq \{0\}$ (במקרה $U \cap W = \{0\}$ נטפל אחר־כך). נסמן $k = \dim(U \cap W)$, ויהי $\{v_1,...,v_k\}$ בסיס של המרחב $U \cap W$. נשלים בסיס זה לבסיס של U,[8]

$$\{v_1,...,v_k,\, u_1,...,u_m\}$$

ולבסיס של W

$$\{v_1,...,v_k,\, w_1,...,w_n\}$$

כך ש־

$$\dim U = k+m, \qquad \dim W = k+n$$

עלינו להוכיח כי:

$$\dim(U+W) = (k+m)+(k+n)-k = k+m+n$$

ראשית נשים לב לעובדה כי כל אחד מהוקטורים $u_1,\ldots,u_m$ הוא בלתי תלוי ב־ $\{v_1,...,v_k\}$ ולכן בוודאי אינו שייך ל־ $U \cap W$, וממילא אף אחד מבין $u_1,\ldots,u_m$ אינו שייך ל־ W. באותו אופן, אף אחד מבין הוקטורים $w_1,\ldots,w_n$ אינו שייך ל־ U. לפיכך, בפרט, כל אחד מן ה־ u_i $(1 \le i \le m)$ שונה מכל אחד מן ה־ w_j $(1 \le j \le m)$ ולכן בקבוצה

$$B = \{v_1,...,v_k,\, u_1,...,u_m,\, w_1,...,w_n\}$$

יש $k+m+n$ וקטורים.

אנו נראה כי קבוצה זו היא בסיס של $U+W$, ומכאן נסיק כי $\dim(U+W) = k+m+n$.
לשם כך נוכיח כי:

א. B בלתי תלויה;
ב. B פורשת את $U+W$.

א. נניח כי $\alpha_1,\ldots\alpha_k,\, \beta_1,\ldots,\beta_m,\, \gamma_1,\ldots,\gamma_n$ הם סקלרים כך ש־

$$\alpha_1 v_1 + \ldots + \alpha_k v_k + \beta_1 u_1 + \ldots + \beta_m u_m + \gamma_1 w_1 + \ldots + \gamma_n w_n = 0 \qquad (1)$$

ונוכיח כי:

$$\alpha_1 = \ldots = \alpha_k = \beta_1 = \ldots = \beta_m = \gamma_1 = \ldots = \gamma_n = 0$$

7 שימו לב, $U+W, U, W$ ו־ $U \cap W$ הם תת־מרחבים של V, ובשל כך הם נוצרים סופית ואפשר להתייחס לממדיהם.

8 תהליך ההשלמה לבסיס אפשרי, שכן $\{v_1,...,v_k\}$ בלתי תלויה לינארית (בהיותה בסיס של $U \cap W$) ולכן תנאי משפט 8.3.5 מתקיימים. שימו לב, אם $U = \{0\}$ או $W = \{0\}$, אז טענת המשפט מובנת מאליה, שכן במקרה זה $U \cap W = \{0\}$.

ואמנם, מ־(1) נובע כי:

$$\alpha_1 v_1 + \ldots + \alpha_k v_k + \beta_1 u_1 + \ldots + \beta_m u_m = (-\gamma_1)w_1 + \ldots + (-\gamma_n)w_n \qquad (5)$$

באגף שמאל של (2) רשום וקטור מתוך U (מדוע?), ובאגף ימין רשום וקטור מתוך W. מהשוויון בין האגפים נובע שבכל אחד מהם רשום וקטור מתוך $U \cap W$, נסמנו v. מאחר ש־ $\{v_1,\ldots,v_k\}$ הוא בסיס של $U \cap W$, הרי שקיימים סקלרים $\delta_1,\ldots,\delta_k$, שעבורם:

$$v = \delta_1 v_1 + \ldots + \delta_k v_k$$

נשווה הצגה זו של v להצגה הרשומה באגף ימין של (2), ונקבל:

$$(-\gamma_1)w_1 + \ldots + (-\gamma_n)w_n = \delta_1 v_1 + \ldots + \delta_k v_k \qquad (3)$$

נעביר אגפים ונקבל:

$$\delta_1 v_1 + \ldots + \delta_k v_k + \gamma_1 w_1 + \ldots + \gamma_n w_n = 0 \qquad (4)$$

מאחר ש־ $\{v_1,\ldots,v_k, w_1,\ldots,w_n\}$ בסיס של W, ובפרט קבוצה בלתי תלויה לינארית, נובע מ־(4) כי כל מקדמי הצירוף הם אפס, ובפרט:

$$\gamma_1 = \ldots = \gamma_n = 0 \qquad (5)$$

באופן דומה מוכיחים כי:

$$\beta_1 = \ldots = \beta_m = 0 \qquad (6)$$

נציב את התוצאות (5) ו־(6) ב־(1) ונזכור כי $\{v_1,\ldots,v_k\}$ בלתי תלויה (כבסיס של $U \cap W$), ונקבל:

$$\alpha_1 = \ldots = \alpha_k = 0 \qquad (7)$$

סיכום התוצאות (5) ו־(6) ו־(7) מראה כי

$$\alpha_1 = \ldots = \alpha_k = \beta_1 = \ldots = \beta_m = \gamma_1 = \ldots = \gamma_n = 0$$

ולכן הקבוצה $B = \{v_1,\ldots,v_k, u_1,\ldots,u_m, w_1,\ldots,w_n\}$ היא בלתי תלויה לינארית.

ב. כעת נראה (או, ליתר דיוק, אתם תראו בתשובה לשאלה הבאה) כי הקבוצה $B = \{v_1,\ldots,v_k, u_1,\ldots,u_m, w_1,\ldots,w_n\}$ פורשת את $U + W$.

לפיכך B בסיס של $U + W$ ומכאן ש־

$$\dim(U + W) = k + m + n$$

כלומר:

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$$

מ.ש.ל.

שאלה 8.3.3

השלימו את הוכחת משפט 8.3.6. כלומר:

א. הוכיחו כי הקבוצה $B = \{v_1,\ldots,v_k, u_1,\ldots,u_m, w_1,\ldots,w_n\}$ פורשת את $U + W$.

ב. אילו שינויים יש לעשות בהוכחה דלעיל כדי ש"תפעל" עבור המקרה $U \cap W = \{0\}$?

התשובה בעמוד 299

מסקנה 8.3.7

אם U ו־ W הם שני תת־מרחבים של מרחב נוצר סופית, ואם $V = U + W$, אז $V = U \oplus W$ אם ורק אם:

$$\dim V = \dim U + \dim W$$

שאלה 8.3.4

הוכיחו את מסקנה 8.3.7.

התשובה בעמוד 300

שאלה 8.3.5

הוכיחו כי קבוצת השורות השונות מאפס במטריצת המדרגות

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 2 & 1 & 4 \\ 0 & 0 & 0 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

מהווה בסיס למרחב השורות[9] של המטריצה.

התשובה בעמוד 300

שאלה 8.3.6

יהיו w_1 ו־ w_2 הוקטורים הבאים ב־ $\mathbb{R}^4$:

$$w_1 = (1,2,-1,4)$$

$$w_2 = (3,-1,-2,2)$$

א. הראו כי $\{w_1, w_2\}$ בלתי תלויה לינארית.

ב. השלימו קבוצה זו לבסיס של $\mathbb{R}^4$.

התשובה בעמוד 301

שאלה 8.3.7

נתבונן בוקטורים מתוך $\mathbb{R}^3$, $w_2 = (2,0,1)$, $w_1 = (1,1,0)$, $u_2 = (-1,1,0)$, $u_1 = (1,0,1)$.

נסמן:

$$W = \mathrm{Sp}\left(\{w_1, w_2\}\right)$$

$$U = \mathrm{Sp}\left(\{u_1, u_2\}\right)$$

א. הוכיחו כי הקבוצה $\{w_1, w_2, u_1\}$ היא בסיס של $\mathbb{R}^3$.

ב. הסיקו כי $W + U = \mathbb{R}^3$.

ג. חשבו את $\dim U$ ואת $\dim W$.

ד. בדקו אם $W \oplus U = \mathbb{R}^3$.

התשובה בעמוד 302

9 נזכיר כי מרחב השורות של מטריצה הוא המרחב הנפרש על־ידי שורותיה.

שאלה 8.3.8

חשבו את הממד של כל אחד ממרחבי המטריצות הבאים מעל הממשיים:

א. מרחב המטריצות מסדר $m \times n$.

ב. מרחב המטריצות הריבועיות מסדר $n \times n$.

ג. מרחב המטריצות האלכסוניות מסדר $n \times n$.

ד. מרחב המטריצות המשולשיות העיליות מסדר $n \times n$ (נמקו מדוע זהו תת־מרחב של מרחב המטריצות המתאים).

ה. מרחב המטריצות הסימטריות מסדר $n \times n$.

ו. מרחב המטריצות האנטי־סימטריות מסדר $n \times n$.

התשובה בעמוד 303

שאלה 8.3.9

מהו הממד של המרחב $F_n[x]$ מעל שדה F?

התשובה בעמוד 305

שאלה 8.3.10

כבר מצאנו כי אוסף הפולינומים ב־ $\mathbb{R}_n[x]$ המתאפסים ב־ $x = 0$ הוא תת־מרחב (ראו שאלה 7.1.11 בפרק הקודם). מהו הממד של תת־מרחב זה?

התשובה בעמוד 305

שאלה 8.3.11

א. מהו הממד של תת־המרחב U של $\mathbb{R}^n$ הנתון על־ידי:

$$U = \left\{ (a_1, \ldots, a_n) \,\middle|\, \sum_{i=1}^{n} a_i = 0 \right\}$$

ב. מצאו תת־מרחב $W \subseteq \mathbb{R}^n$ שעבורו:

$$W \oplus U = \mathbb{R}^n$$

(מהו הממד של W?)

התשובה בעמוד 305

8.4 קואורדינטות

בסעיף 8.2 הוכחנו שאם $v_1,\dots,v_n$ הם איבריו השונים של בסיס למרחב לינארי V מעל שדה F, אז לכל וקטור ב־V יש הצגה יחידה כצירוף לינארי של $v_1,\dots,v_n$ (משפט 8.2.5). במילים אחרות – בהצגתו של $v \in V$ כצירוף הלינארי

$$v = \lambda_1 v_1 + \dots + \lambda_n v_n \qquad (*)$$

המקדמים $\lambda_1,\dots,\lambda_n$ (שהם סקלרים מתוך F) נקבעים באופן **יחיד** על־ידי v.

יש כמובן חשיבות לכך שנייחס כל סקלר לוקטור הבסיס המתאים שאותו הוא כופל. דבר זה השגנו בכך ש"מִספרנו" את וקטורי הבסיס באינדקסים מ־1 עד n, וכן גם את הסקלרים, באופן שהסקלר λ_i הוא המקדם של v_i בהצגה (*). במילים אחרות, קבענו סדר מסוים בין איברי הבסיס, ובמקביל סידרנו גם את הסקלרים בסדר מתאים. דבר זה מוביל אותנו להגדרת מושג הבסיס הסדור.

הגדרה 8.4.1

יהי V מרחב לינארי נוצר סופית ממימד n. **סדרה** בת n וקטורים $(v_1,\dots,v_n)$ ב־V נקראת **בסיס סדור** ל־V, אם היא בלתי תלויה לינארית ופורשת את V.

הערות

א. הגדרה 8.4.1 מכלילה את הגדרת הבסיס הסדור למרחב F^n, שניתנה בפרק 2 (הגדרה 2.7.6).

ב. לאור שאלה 8.1.9, תנאי הכרחי (אך לאו דווקא מספיק) לכך שהסדרה $(v_1,\dots,v_n)$ תהווה בסיס ל־V הוא שהוקטורים בסדרה יהיו שונים זה מזה. יתר על כן, אם הוקטורים $v_1,\dots,v_n$ שונים זה מזה, אזי הסדרה $(v_1,\dots,v_n)$ היא בסיס סדור ל־V אם ורק אם הקבוצה $(v_1,\dots,v_n)$ היא בסיס ל־V.

ג. לעיתים נשמיט את המילה "סדור" ונאמר שסדרת וקטורים $(v_1,\dots,v_n)$ מהווה בסיס ל־V, או פשוט נאמר כי הוקטורים $v_1,\dots,v_n$ מהווים בסיס ל־V.

אם $v_1,\dots,v_n$ וקטורים שונים כך שהקבוצה $\{v_1,v_2,v_3,\dots,v_n\}$ מהווה בסיס למרחב, אז $B=(v_1,v_2,v_3,\dots,v_n)$ ו־$C=(v_2,v_1,v_3,\dots,v_n)$ מהווים בסיסים סדורים **שונים** למרחב, למרות שב־B וב־C מופיעים אותם האיברים. זאת משום שסדר הוקטורים ב־B שונה מסדרם ב־C.

את הסקלרים שבהצגה (*) נציג על־ידי וקטור עמודה:

$$\begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{bmatrix}$$

לוקטור זה נקרא **וקטור הקואורדינטות** של v לפי הבסיס $(v_1,\dots,v_n)$.

עבור $B=(v_1,v_2,v_3,...,v_n)$, נסמן את וקטור הקואורדינטות בקיצור על־ידי $[v]_B$. הסקלרים $\lambda_1,...,\lambda_n$ נקראים **הקואורדינטות של** v **לפי הבסיס הסדור** B.

וקטורי הקואורדינטות של v (הנתון במשוואה (*)) לפי בסיסים סדורים שונים יהיו שונים. למשל, אם $B=(v_1,v_2,v_3,...,v_n)$ אז:

$$[v]_B=\begin{bmatrix}\lambda_1\\ \lambda_2\\ \lambda_3\\ \vdots\\ \lambda_n\end{bmatrix}$$

ולעומת זאת, עבור $C=(v_2,v_1,v_3,...,v_n)$:

$$[v]_C=\begin{bmatrix}\lambda_2\\ \lambda_1\\ \lambda_3\\ \vdots\\ \lambda_n\end{bmatrix}$$

דוגמאות

א. נתבונן בבסיס הסדור $B=\left(1,x,x^2,x^3\right)$ של המרחב $\mathbb{R}_4[x]$. הצגתו של הפולינום $Q(x)=2-x+4x^3$ כצירוף לינארי של איברי B היא:

$$Q(x)=2(1)+(-1)x+0x^2+4x^3$$

ולכן וקטור הקואורדינטות המתאים הוא:

$$[Q(x)]_B=\begin{bmatrix}2\\ -1\\ 0\\ 4\end{bmatrix}$$

ב. נתבונן בשלושה בסיסים סדורים של $\mathbb{R}^2$:

$$B=\big((1,2),(3,4)\big)$$

$$D=\big((1,0),(1,1)\big)$$

$$E=\big((1,0),(0,1)\big)$$

נמצא את וקטורי הקואורדינטות של הוקטור $\mathbf{a}=(-1,2)$ על פי כל אחד מן הבסיסים הללו.

מהצגת $\mathbf{a}$ כצירוף לינארי של איברי B,

$\mathbf{a}=5\cdot(1,2)-2\cdot(3,4)$ [1]

1 את המקדמים 5 ו־ (-2) מצאנו על־ידי פתרון המשוואה הוקטורית $\begin{bmatrix}-1\\ 2\end{bmatrix}=x\begin{bmatrix}1\\ 2\end{bmatrix}+y\begin{bmatrix}3\\ 4\end{bmatrix}$, השקולה למערכת המשוואות

$$\begin{aligned}x+3y&=-1\\ 2x+4y&=\ \ 2\end{aligned}$$

נובע כי:

$$[\mathbf{a}]_B = \begin{bmatrix} 5 \\ -2 \end{bmatrix}$$

באופן דומה מוצאים כי:

$$\mathbf{a} = -3 \cdot (1,0) + 2 \cdot (1,1)$$

ולכן:

$$[\mathbf{a}]_D = \begin{bmatrix} -3 \\ 2 \end{bmatrix}$$

ולבסוף ודאו כי

$$\mathbf{a} = -1 \cdot (1,0) + 2 \cdot (0,1)$$

ולכן:

$$[\mathbf{a}]_E = \begin{bmatrix} -1 \\ 2 \end{bmatrix}$$

▸

שאלה 8.4.1

א. הוכיחו כי הסדרה B, הנתונה על־ידי

$$B = \left(\begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right)$$

מהווה בסיס (סדור) ל־ $\mathbf{M}_{2\times 2}^{\mathbb{R}}$.

ב. מצאו את וקטורי הקואורדינטות של המטריצות הבאות ביחס לבסיס הסדור B מחלק א.

1. $M_1 = \begin{bmatrix} 1 & 7 \\ 1 & -1 \end{bmatrix}$

2. $M_2 = \begin{bmatrix} 3 & 3 \\ 1 & -1 \end{bmatrix}$

התשובה בעמוד 307

שאלה 8.4.2

א. הוכיחו שסדרת הפולינומים $(1+x, x+x^2, x^2+x^3, 2x^3)$ מהווה בסיס למרחב הפולינומים $\mathbb{R}_4[x]$.

ב. מה הן הקואורדינטות של $P(x) = 3 + 2x + x^2 + 2x^3$ ביחס לבסיס זה?

התשובה בעמוד 309

שאלה 8.4.3

יהי E הבסיס הסטנדרטי הסדור של F^n, כאשר F שדה כלשהו,

$$E = (\mathbf{e}_1, \ldots, \mathbf{e}_n)$$

ויהי $\mathbf{a} = (a_1, \ldots, a_n)$ וקטור ב־ F^n. מהו $[\mathbf{a}]_E$?

התשובה בעמוד 310

עד כה הראינו כי בהינתן בסיס סדור $B = (v_1, \ldots, v_n)$ למרחב לינארי V מעל שדה F, אנו יכולים להתאים לכל וקטור v ב־ V וקטור $[v]_B$ ב־ F^n. התאמה זו היא בעלת חשיבות רבה - כפי שנראה בהמשך, היא מאפשרת לנו להמיר בעיות על אודות מרחב לינארי (נוצר סופית) כללי לבעיות במרחב מהצורה F^n, המוכר לנו היטב.

נעמוד מעט על טיבה של ההתאמה הנידונה.

ראשית, ההתאמה היא חד־חד־ערכית, שכן אם ל־ u_1 ול־ u_2 מותאם אותו וקטור

$$\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$$

אזי:

$$u_1 = \sum_{i=1}^{n} a_i v_i = u_2$$

לשני וקטורים **שונים** מותאמים אפוא וקטורי קואורדינטות **שונים**.

שנית, התאמה זו היא **על** F^n. שכן, אם $\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$ הוא איבר כלשהו ב־ F^n, נגדיר וקטור $v \in V$ על־ידי

$$v = \sum_{i=1}^{n} a_i v_i$$

ואז:

$$[v]_B = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$$

נתבונן עתה בשני וקטורים v ו־ w ב־ V ובסכומם $v + w$.

אם

$$v = \sum_{i=1}^{n} a_i v_i \qquad , \qquad w = \sum_{i=1}^{n} b_i v_i$$

אז:

$$v + w = \sum_{i=1}^{n} (a_i + b_i) v_i$$

לשלושת הוקטורים, v, w, $v+w$, מותאמים וקטורי הקואורדינטות שלהם לפי B:

$$[v]_B = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}, \ [w]_B = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}, \ [v+w]_B = \begin{bmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{bmatrix} \qquad (*)$$

אולם, על פי הגדרת החיבור ב־ F^n:

$$\begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} + \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{bmatrix}$$

שוויון אחרון זה פירושו (ראו (*)):

$$[v]_B + [w]_B = [v+w]_B$$

היחס שבין הוקטורים v, w ו־$v+w$ (השלישי הוא סכומם ב־ V של השניים הראשונים) נשמר אפוא גם בין הוקטורים $[v]_B$, $[w]_B$ ו־ $[v+w]_B$ (השלישי הוא שוב סכומם של השניים הראשונים ב־ F^n). כלומר, ההתאמה $v \to [v]_B$ **שומרת על החיבור**.

תכונה נוספת של ההתאמה שלנו עוסקת בכפל בסקלר:

עבור $v \in V$ ו־ $\lambda \in F$ כלשהם מתקיים:

$$[\lambda v]_B = \lambda [v]_B \qquad (**)$$

שאלה 8.4.4

הוכיחו טענה זו.

התשובה בעמוד 310

השוויון (*) פירושו כי ההתאמה $v \to [v]_B$ **שומרת על הכפל בסקלר**. קיבלנו שההתאמה $v \to [v]_B$ היא **העתקה**[2] **חד־חד־ערכית ועל, השומרת על החיבור והכפל בסקלר.**

נסכם את תכונותיה של ההתאמה $v \to [v]_B$ במשפט.

משפט 8.4.2

יהיו V מרחב לינארי n־ממדי מעל שדה F, ו־ B בסיס סדור ל־ V. ההתאמה $v \to [v]_B$ המתאימה לכל וקטור v ב־ V את וקטור הקואורדינטות שלו ב־ F^n, $[v]_B$, היא העתקה **חד־חד־ערכית** מ־ V **על** F^n, המקיימת:

א. לכל $v,w \in V$ מתקיים השוויון $[v]_B + [w]_B = [v+w]_B$.

ב. לכל $v \in V,\ \lambda \in F$ מתקיים השוויון $[\lambda v]_B + \lambda [v]_B$.

---

2 העתקה היא מילה חלופית להתאמה (כלומר, לפונקציה), המקובלת בהקשר זה.

העתקה חד־חד־ערכית ממרחב לינארי **על** מרחב לינארי, השומרת על החיבור והכפל בסקלר, נקראת **איזומורפיזם של מרחבים לינאריים**. נשוב ונעסוק באיזומורפיזמים כאלה בהמשך.

שאלה 8.4.5

יהי V מרחב לינארי n־ממדי, ו־ B בסיס סדור של V.

הוכיחו כי:

א. $[0]_B = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$

ב. לכל $v \in V$:

$$[-v]_B = -[v]_B$$

התשובה בעמוד 311

ממשפט 8.4.2 נובעת בנקל הלמה הבאה:

למה 8.4.3

יהיו V מרחב לינארי נוצר סופית מעל שדה F, ו־ B בסיס סדור של V.

אם $u_1,\ldots,u_m \in V$ ו־ $\lambda_1,\ldots,\lambda_m \in F$, אז:

$$[\lambda_1 u_1 + \ldots + \lambda_m u_m]_B = \lambda_1 [u_1]_B + \ldots + \lambda_m [u_m]_B$$ [3]

שאלה 8.4.6

הוכיחו את למה 8.4.3 (הוכיחו באינדוקציה על m).

התשובה בעמוד 311

המשפט השימושי הבא הוא מסקנה מיידית מהלמה האחרונה:

משפט 8.4.4

יהיו V מרחב לינארי ממֵמד n מעל שדה F, ו־ B בסיס סדור של V.

וקטורים $u_1,\ldots,u_m$ ב־ V הם תלויים לינארית אם ורק אם הוקטורים $[u_1]_B,\ldots,[u_m]_B$ ב־ F^n תלויים לינארית.[4]

שאלה 8.4.7

הוכיחו את משפט 8.4.4.

התשובה בעמוד 312

---

3 בניסוח מילולי עמוס במקצת: וקטור הקואורדינטות המתאים לצירוף לינארי של וקטורים הוא הצירוף הלינארי של וקטורי הקואורדינטות המתאימים עם אותם מקדמים.

4 וממילא $u_1,\ldots,u_n$ בלתי תלויים לינארית ב־ V אם ורק אם $[u_1]_B,\ldots,[u_n]_B$ בלתי תלויים לינארית ב־ F^n.

חשיבותו של המשפט האחרון בכך שהוא מאפשר להמיר בעיות של תלות ואי־תלות לינארית במרחב V מממד n מעל שדה F, בבעיות אנלוגיות ב־ F^n. את היכולת לבצע המרה זו, ננצל במשפט הבא:

משפט 8.4.5

יהי $B=(v_1,...,v_n)$ בסיס סדור של מרחב לינארי n־ממדי V מעל שדה F, ויהיו $u_1,...,u_n$ וקטורים ב־ V הנתונים על־ידי:

$$u_1 = a_{11}v_1 + a_{21}v_2 + ... + a_{n1}v_n$$

$$\vdots$$

$$u_n = a_{1n}v_1 + a_{2n}v_2 + ... + a_{nn}v_n$$

הסדרה $(u_1,\ldots,u_n)$ היא בסיס ל־ V אם ורק אם המטריצה

$$M=\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

הפיכה.

הערה

שימו לב, **העמודה** ה־ j $(1\le j\le n)$ של המטריצה M היא וקטור הקואורדינטות של u_j לפי הבסיס B.

הוכחה

כיוון ראשון:

אם הסדרה $(u_1,\ldots,u_n)$ היא בסיס של V, אז היא בלתי תלויה לינארית. לכן, על פי משפט 8.4.4, גם הסדרה $\left([u_1]_B,\ldots,[u_n]_B\right)$ בלתי תלויה לינארית. אך זו האחרונה אינה אלא סדרת העמודות של M (ראו הערה לעיל). כלומר, עמודות המטריצה M בלתי תלויות לינארית (כוקטורים ב־ F^n) ולכן M הפיכה (על איזה משפט הסתמכנו?).

כיוון שני:

אם המטריצה M הפיכה, עמודותיה בלתי תלויות לינארית. כלומר, סדרת הוקטורים $\left([u_1]_B,\ldots,[u_n]_B\right)$ בלתי תלויה לינארית, לכן, על פי משפט 8.4.4, גם הוקטורים $u_1,\ldots,u_n$ אינם תלויים לינארית. אך n וקטורים בלתי תלויים לינארית במרחב בעל ממד n מהווים בסיס.

מ.ש.ל.

דוגמה

נתבונן ב־ $\mathbb{R}_5[x]$ עם הבסיס (הסדור) $B=(1,x,x^2,x^3,x^4)$ ובסדרת הוקטורים:

$$C=(1+x,\ x+x^2,\ x^2+x^3,\ x^3+x^4,\ x^4)$$

נראה שהסדרה C היא בסיס ל־$\mathbb{R}_5[x]$. נבחין כי:

$$[1+x]_B = \begin{bmatrix}1\\1\\0\\0\\0\end{bmatrix},\ \left[x+x^2\right]_B = \begin{bmatrix}0\\1\\1\\0\\0\end{bmatrix},\ \left[x^2+x^3\right]_B = \begin{bmatrix}0\\0\\1\\1\\0\end{bmatrix}$$

$$\left[x^3+x^4\right]_B = \begin{bmatrix}0\\0\\0\\1\\1\end{bmatrix},\ \left[x^4\right]_B = \begin{bmatrix}0\\0\\0\\0\\1\end{bmatrix}$$

המטריצה M, שעמודותיה הם וקטורי הקואורדינטות הללו, היא:

$$M = \begin{bmatrix}1&0&0&0&0\\1&1&0&0&0\\0&1&1&0&0\\0&0&1&1&0\\0&0&0&1&1\end{bmatrix}$$

הדטרמיננטה של M שווה ל־1 (M היא מטריצה משולשית תחתית ולכן הדטרמיננטה שלה שווה למכפלת איברי האלכסון). מאחר שהדטרמיננטה שונה מאפס, המטריצה הפיכה. לכן, לפי המשפט האחרון, הסדרה C היא בסיס של $\mathbb{R}_5[x]$.

▸

כאשר הווקטורים $u_1,\ldots,u_n$ המופיעים במשפט 8.4.5 אכן מהווים בסיס, נודעת למטריצה M חשיבות רבה, ועל כן נעניק לה שם.

הגדרה 8.4.6

יהי $B=(v_1,\ldots,v_n)$ בסיס סדור של מרחב לינארי n־ממדי V מעל שדה F. אם $B'=(u_1,\ldots,u_n)$ הוא בסיס סדור אחר של אותו מרחב, ואם מתקיים

$$u_1 = a_{11}v_1 + .. + a_{n1}v_n$$

$$\vdots$$

$$u_n = a_{1n}v_1 + \ldots + a_{nn}v_n$$

אז המטריצה

$$M = \begin{bmatrix}a_{11} & \cdots & a_{1n}\\ \vdots & & \vdots\\ a_{n1} & \cdots & a_{nn}\end{bmatrix}$$

נקראת **מטריצת המעבר** מן הבסיס (הסדור) B לבסיס (הסדור) B'.

מעתה והלאה נשמיט לרוב את המלה "סדור", ונתייחס בפשטות אל מטריצת המעבר מבסיס מסוים לבסיס אחר. אך זכרו: מטריצת המעבר מוגדרת היטב רק לאחר שנקבע סדר לאיברי הבסיסים.

הערות

א. מטריצת מעבר היא מטריצה **ריבועית** מסדר n (כאשר n הוא הממד של V).

ב. מטריצת מעבר היא מטריצה הפיכה.[5]

שאלה 8.4.8

א. מהי מטריצת המעבר מן הבסיס $B=\big((1,1),(1,-1)\big)$ של $\mathbb{R}^2$ לבסיס $B'=\big((3,2),(0,1)\big)$?

ב. הוכיחו כי $B'=\big((1,2,1),(-1,0,1),(2,2,-1)\big)$ הוא בסיס ל־$\mathbb{R}^3$ ומצאו את מטריצת המעבר מן הבסיס $B=\big(\mathbf{e}_1,\mathbf{e}_2,\ldots,\mathbf{e}_n\big)$ ל־B'.

ג. מצאו את מטריצת המעבר מן הבסיס $B=\big((1,0),(0,1)\big)$ לבסיס $B'=\big((1,0),(0,1)\big)$.
מהי מטריצת המעבר מ־B' ל־B?

ד. רשמו את מטריצת המעבר מן הבסיס הסטנדרטי של $\mathbb{R}^n$, $B=(\mathbf{e}_1,\ldots,\mathbf{e}_n)$, לבסיס $B'=(\mathbf{e}_1+\mathbf{e}_2,\,\mathbf{e}_2+\mathbf{e}_3,\ldots,\mathbf{e}_{n-1}+\mathbf{e}_n,\,\mathbf{e}_n)$. (כיצד תוודאו כי B' הוא אכן בסיס?)

ה. הראו שאם B הוא הבסיס הסטנדרטי ב־$\mathbb{R}^n$ ו־$B'=(u_1,\ldots,u_n)$ גם הוא בסיס ל־$\mathbb{R}^n$, אז מטריצת המעבר מ־B ל־B' היא המטריצה שעמודותיה הן הוקטורים u_i הרשומים כעמודות.

התשובה בעמוד 313

ראינו שכל מטריצת מעבר מבסיס לבסיס היא הפיכה. אפשר להראות גם שכל מטריצה הפיכה עשויה לשמש כמטריצת מעבר. ביתר פירוט: אם B הוא בסיס במרחב לינארי n־ממדי V, ו־M היא מטריצה הפיכה כלשהי מסדר $n\times n$, אז קיים בסיס, B', למרחב V כך שהמטריצה M היא מטריצת המעבר מ־B ל־B'.

שאלה 8.4.9

א. הוכיחו את הטענה האחרונה.

ב. יהי $B=\big((1,0,0,0),(1,1,0,0),(1,1,1,0),(1,1,1,1)\big)$ בסיס ל־$\mathbb{R}^4$, ותהי M מטריצה מסדר 4×4 הנתונה על־ידי:

$$M=\begin{bmatrix}1&3&0&7\\0&4&0&8\\2&5&6&9\\0&0&0&10\end{bmatrix}$$

1. הראו כי M הפיכה.
2. מצאו בסיס B' ל־$\mathbb{R}^4$ באופן כזה שהמטריצה דלעיל תשמש מטריצת המעבר מ־B ל־B'.

התשובה בעמוד 314

אם $B=(v_1,\ldots,v_n)$ ו־$B'=(u_1,\ldots,u_n)$ הם שני בסיסים של המרחב V, אז לכל וקטור v ב־V מתאימים שני וקטורי קואורדינטות: $[v]_B$ לפי הבסיס B, ו־$[v]_{B'}$ לפי הבסיס B'.

5 על פי משפט 8.4.5.

על הקשר שבין שני וקטורי הקואורדינטות האלה נעמוד במשפט הבא.

משפט 8.4.7

יהי V מרחב לינארי ממֵמד n מעל שדה F, ויהיו $B=(v_1,\ldots,v_n),\ B'=(u_1,\ldots,u_n)$ שני בסיסים סדורים של V, ו־ M מטריצת המעבר מ־ B ל־ B'. לכל $v\in V$ מתקיים:

$$[v]_B = M\cdot [v]_{B'}$$ [6]

הוכחה

נראה תחילה שהשוויון הדרוש מתקיים עבור $v=u_j$, כלומר נראה כי לכל $1\le j\le n$:

$$[u_j]_B = M\cdot[u_j]_{B'} \tag{1}$$

נרשום:

$$u_j = 0\cdot u_1 + \ldots + 1\cdot u_j + \ldots + 0\cdot u_n$$

מכאן שוקטור הקואורדינטות של u_j לפי הבסיס B' הוא

$$[u_j]_{B'} = \begin{array}{c}\begin{bmatrix}0\\ \vdots\\ 1\\ \vdots\\ 0\end{bmatrix}\end{array}\begin{array}{l}\\ \\ \leftarrow j\ \text{קואורדינטה}\\ \\ \\ \end{array}$$

ולכן:

$$M\cdot[u_j]_{B'} = M\cdot \begin{array}{c}\begin{bmatrix}0\\ \vdots\\ 1\\ \vdots\\ 0\end{bmatrix}\end{array}\begin{array}{l}\\ \\ \leftarrow j\ \text{קואורדינטה}\\ \\ \\ \end{array}$$

$$= [M]_j^c = [u_j]_B$$

($[M]_j^c$ היא העמודה ה־ j של M, והיא - על פי הגדרתה של M - וקטור הקואורדינטות של u_j לפי הבסיס B).

נעבור למקרה הכללי. יהי $v\in V$ וקטור כלשהו. נציג אותו כצירוף לינארי של וקטור הבסיס B':

$$v = \sum_{j=1}^{n}\lambda_j u_j$$

6 שימו לב, מטריצת המעבר מ־ B ל־ B' משמשת ל"תרגום" וקטורי קואורדינטות לפי B' לוקטורי קואורדינטות לפי B!

לפי למה 8.4.3 מתקיים:

$$[v]_B = \sum_{j=1}^{n} \lambda_j [u_j]_B$$

וכן

$$[u_j]_{B'} = \sum_{j=1}^{n} \lambda_j [u_j]_{B'}$$

ומכאן:

$$M[v]_{B'} = M\left(\sum_{j=1}^{n} \lambda_j [u_j]_{B'}\right)$$

$$= \sum_{j=1}^{n} M\left(\lambda_j [u_j]_{B'}\right) = \sum_{j=1}^{n} \lambda_j M[u_j]_{B'}$$

$$\overset{7}{=} \sum_{j=1}^{n} \lambda_j [u_j]_B = \left[\sum_{j=1}^{n} \lambda_j u_j\right]_B = [v]_B$$

מ.ש.ל.

במשפט האחרון הראינו שמטריצת המעבר M משמשת ל"תרגום" של קואורדינטות מבסיס לבסיס. המשפט הבא מראה כי M היא המטריצה היחידה המבצעת "תרגום" זה.

משפט 8.4.8

יהי V מרחב לינארי מעל שדה F, ויהיו $B = (v_1,\dots,v_n)$ ו־ $B' = (u_1,\dots,u_n)$ זוג בסיסים סדורים של V. אם A היא מטריצה ריבועית מסדר n המקיימת

$$[v]_B = A \cdot [v]_{B'} \qquad (*)$$

לכל $v \in V$, אז A היא מטריצת המעבר מ־ B ל־ B'.

הוכחה

במהלך ההוכחה של משפט 8.4.7 ראינו כי לכל $1 \le j \le n$ מתקיים:

$$[u_j]_{B'} = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \begin{matrix} \\ \\ \leftarrow j \text{ קואורדינטה} \\ \\ \\ \end{matrix}$$

ומכאן

$$A[u_j]_{B'} = [A]_j^c$$

7 על פי (1) ועל פי למה 8.4.3.

ולכן נקבל על פי הנתון (*) כי:

$$[A]_j^c = [u_j]_B$$

כלומר, עמודותיה של המטריצה A הן וקטורי הקואורדינטות של הוקטורים u_j לפי הבסיס B. לכן A אינה אלא מטריצת המעבר מ־ B ל־ B'.

מ.ש.ל.

בעזרת המשפט האחרון נוכל למצוא בנקל את הקשר שבין מטריצת המעבר מהבסיס B לבסיס B' ובין מטריצת המעבר מהבסיס B' לבסיס B.

משפט 8.4.9

אם M היא מטריצת המעבר מבסיס B לבסיס B', אז M^{-1} היא מטריצת המעבר מהבסיס B' לבסיס B.

שאלה 8.4.10

הוכיחו את משפט 8.4.9.

התשובה בעמוד 315

דוגמה

בשאלה 8.4.8ג מצאנו כי מטריצת המעבר מהבסיס (הסדור) $B = ((1,0),(0,1))$ של $\mathbb{R}^2$ לבסיס $B' = ((2,0),(0,2))$ היא המטריצה:

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

ואילו מטריצת המעבר מ־ B ל־ B' היא:

$$\begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix}$$

קל לוודא שכל אחת מן המטריצות הללו היא אכן ההופכית של האחרת. ◀

שאלה 8.4.11

נתבונן בשני בסיסים סדורים ל־ $\mathbb{R}_n[x]$:

$$B = (1, x, x^2, \ldots, x^{n-1})$$

$$B' = (1, 1+x, 1+x+x^2, \ldots, 1+x+\ldots+x^{n-1}, 1+x+\ldots+x^{n-1})$$

א. רשמו את וקטורי B' כצירופים לינאריים של וקטורי B, ומצאו את מטריצת המעבר M מ־ B ל־ B'.

ב. רשמו את וקטורי B כצירופים לינאריים של איברי B'.

ג. מצאו את M^{-1} (ללא חישוב ישיר).

התשובה בעמוד 315

שאלה 8.4.12

יהי μ סקלר ממשי. נתבונן בסדרת הפולינומים:

$$B' = \left(1,\, x+\mu,\, (x+\mu)^2, \ldots, (x+\mu)^{n-1}\right)$$

הוכיחו כי B' הוא בסיס ל־ $\mathbb{R}_n[x]$.

הדרכה

רשמו את המטריצה שעמודותיה הן וקטורי הקואורדינטות של איברי B', לפי הבסיס $B = \left(1,\, x,\, x^2, \ldots, x^{n-1}\right)$.[8] הוכיחו שהדטרמיננטה של מטריצה זו שונה מאפס.

התשובה בעמוד 316

8 השתמשו בבינום של ניוטון.

8.5 הדרגה של מטריצה

תהי A מטריצה ב־$\mathbf{M}_{m\times n}^{F}$. שורותיה של מטריצה זו הן וקטורים ב־F^n. התת־מרחב של F^n, הנפרש על־ידי שורותיה של A, נקרא **מרחב השורות של** A. עמודותיה של A הן וקטורים ב־F^m. לתת־המרחב של F^m הנפרש על־ידי עמודותיה של A, נקרא **מרחב העמודות של** A.

בסעיף זה נעסוק בשתי שאלות.
האחת - כיצד לחשב את ממדיהם של מרחב השורות ומרחב העמודות. לממד של מרחב השורות של A נקרא **דרגת השורות של המטריצה** A, ולממד מרחב עמודותיה נקרא **דרגת העמודות של המטריצה** A. את הדרגות הללו נסמן בהתאמה $\rho_R(A)$ ו־$\rho_C(A)$.[1]
השאלה השנייה תעסוק בקשר שבין $\rho_R(A)$ לבין $\rho_C(A)$. במקרה טריוויאלי אחד נוכל לענות על שאלות אלה על נקלה.

שאלה 8.5.1
הוכיחו כי עבור מטריצת האפס $0_{m\times n}$ מתקיים:
א. מרחב שורותיה הוא $\{0\}$ (המרחב הכולל רק את וקטור האפס של F^n).
ב. מרחב עמודותיה הוא $\{0\}$ (המרחב הכולל רק את וקטור האפס של F^m).
ג. $\rho_R(0_{m\times n}) = \rho_C(0_{m\times n}) = 0$

התשובה בעמוד 317

בהמשך הדיון נניח אפוא כי A איננה מטריצת האפס.
תחילה נדון בחישוב דרגת השורות.

במרחב השורות של מטריצה עסקנו כבר בשאלה 7.5.12 בפרק הקודם. ראינו שם כי פעולות שורה אינן משנות את מרחב השורות, והסקנו כי לשתי מטריצות שקולות שורה יש אותו מרחב שורות.[2] מאחר שכל מטריצה היא שקולת שורות למטריצת מדרגות, די לנו אם נדע למצוא את מרחב שורותיה של מטריצת מדרגות.

למה 8.5.1
תהי $A = [a_{ij}] \in \mathbf{M}_{m\times n}^{F}$ מטריצת **מדרגות** ויהיו $v_1,\ldots,v_k$ שורותיה של A **שאינן שורות אפסים**.[3] אזי:
א. הקבוצה $\{v_1,\ldots,v_k\}$ היא בסיס למרחב השורות של A.
ב. דרגת השורות של A שווה למספר השורות של A שאינן שורות אפסים, דהיינו $\rho_R(A) = k$.

1 R היא ראש התיבה האנגלית Row (שורה), ו־ C היא ראש התיבה האנגלית Column (עמודה).
2 וממילא דרגות שורותיהן שוות זו לזו.
3 לאור שאלה 8.5.1 נוכל להניח ש־ A איננה מטריצת האפס ולכן $k \ge 1$ (וכמובן $k \le m$). זכרו כי במטריצת מדרגות, שורות אפסים נמצאות ב"תחתית" המטריצה. כמו כן, שימו לב שמכיוון שהמטריצה מדורגת, שורותיה השונות מאפס שונות זו מזו (האיבר הפותח בכל אחת מהן נמצא במקום שונה).

הוכחה

דרגת השורות של A הוגדרה כממד של מרחב שורותיה של A. לכן טענת סעיף ב נובעת ישירות מטענת סעיף א. נוכיח, אם כן, את סעיף א.

קבוצת השורות של A מכילה את k הוקטורים $v_1,...,v_k$ וכן את וקטור האפס 0 (אם $k < m$). אולם הוספתו או גריעתו של וקטור האפס לקבוצה כלשהי אינה משנה את המרחב הנפרש על־ידי קבוצה זו. נסיק כי השורות $v_1,...,v_k$ **פורשות** את מרחב השורות של A.

נותר להראות שהקבוצה $\{v_1,\ldots,v_k\}$ בלתי תלויה לינארית. אכן, לו הייתה קבוצה זו תלויה־לינארית, היה קיים צירוף לינארי לא טריוויאלי $\lambda_1 v_1 + \ldots + \lambda_k v_k$ המתאפס. נסמן ב־ t את האינדקס המזערי i שעבורו $\lambda_i \neq 0$. כלומר, $\lambda_1 = \ldots = \lambda_{t-1} = 0,\ \lambda_t \neq 0$. אזי:

$$(*) \qquad \lambda_t v_t + \lambda_{t+1} v_{t+1} + \ldots + \lambda_k v_k = 0$$

נניח שהאיבר הפותח בוקטור השורה v_t נמצא במקום ה־ p. מאחר שהמטריצה A מדורגת, הרכיב ה־ p של כל אחד מן הוקטורים $v_{t+1},\ldots,v_k$ מתאפס, ולכן הרכיב ה־ p של $\lambda_t v_t + \lambda_{t+1} v_{t+1} + \ldots + \lambda_k v_k$ שווה לרכיב ה־ p של $\lambda_t v_t$, והוא אינו מתאפס מאחר ש־ $\lambda_t \neq 0$. בזאת קיבלנו סתירה לשוויון (*). נסיק ש־ $\{v_1,\ldots,v_k\}$ בלתי תלויה.

מ.ש.ל.

כדי למצוא בסיס למרחב השורות של מטריצה נתונה כלשהי B, די אפוא לבצע פעולות אלמנטריות על שורותיה, על מנת להביא אותה למטריצת מדרגות A (לאו דווקא קנונית). השורות אשר אינן שורות האפס ב־ A יהיו בסיס למרחב השורות של A, ולכן גם בסיס למרחב השורות של B. מספר השורות האלה הוא דרגת השורות $\rho_R(B)$, ומתקיים $\rho_R(B) = \rho_R(A)$.

שאלה 8.5.2

מצאו בסיס למרחב השורות של המטריצה A שלפניכם, וקבעו את הדרגה $\rho_R(A)$.

$$A = \begin{bmatrix} 2 & -1 & 3 & -2 & 4 \\ 4 & -2 & 5 & 1 & 7 \\ 2 & -1 & 1 & 8 & 2 \end{bmatrix}$$

התשובה בעמוד 317

נעבור לדון בדרגת העמודות – כיצד נחשב את מרחב העמודות ואת ממדו? אפשר כמובן לעשות פעולות אלמנטריות על עמודות, פעולות שיביאו לדירוג של מטריצה בצורה "מעומדת". אולם מכיוון שכבר התרגלנו לעשות פעולות על שורות דווקא, נעדיף להסתכל במטריצה המשוחלפת ששורותיה הן עמודותיה של A. מרחב העמודות של A הוא מרחב השורות של A^t ובפרט –

$$\rho_C(B) = \rho_R(A^t)$$ [4]

לכן, כדי למצוא את מרחב העמודות של A יש לשחלפה ולהשתמש בשיטה שתוארה למציאת מרחב השורות של A^t.

4 דרגת העמודות של A שווה לדרגת השורות של A^t.

שאלה 8.5.3

מצאו את מרחב העמודות ואת דרגת העמודות $\rho_C(A)$ של המטריצה A משאלה 8.5.2.

התשובה בעמוד 317

עבור המטריצות שבשתי השאלות האחרונות ראינו שלמרות שמרחב השורות של A שונה ממרחב עמודותיה - ממדיהם **שווים**. גם עבור מטריצת האפס קיבלנו כי דרגת השורות שלה שווה לדרגת העמודות.[5] נוכיח שכך הדבר באופן כללי.

משפט 8.5.2

דרגת השורות של מטריצה שווה לדרגת העמודות שלה.

להוכחת המשפט ניעזר בלמה הבאה:

למה 8.5.3

אם P מטריצה מסדר $m \times k$ ו־ Q מטריצה מסדר $k \times n$ (שתיהן מעל שדה F), אז כל עמודה של מטריצת המכפלה PQ היא צירוף ליניארי של k עמודותיה של P.

הוכחה

בפרק 3 (ראו חלק א של למה 3.4.3) הוכחנו כי

$$[PQ]_j^c = P[Q]_j^c$$

לכל j $(1 \le j \le n)$. כלומר

$$[PQ]_j^c = \begin{bmatrix} p_{11} & \cdots & p_{1k} \\ \vdots & & \vdots \\ p_{m1} & \cdots & p_{mk} \end{bmatrix} \cdot \begin{bmatrix} q_{1j} \\ \vdots \\ q_{kj} \end{bmatrix} = \begin{bmatrix} p_{11}q_{1j} + & p_{12}q_{2j} + & \cdots & +p_{1k}q_{kj} \\ p_{21}q_{1j} + & p_{22}q_{2j} + & \cdots & +p_{2k}q_{kj} \\ \vdots & \vdots & & \vdots \\ p_{m1}q_{1j} + & p_{m2}q_{2j} + & \cdots & +p_{mk}q_{kj} \end{bmatrix}$$

$$= \begin{bmatrix} p_{11}q_{1j} \\ p_{21}q_{1j} \\ \vdots \\ p_{m1}q_{1j} \end{bmatrix} + \begin{bmatrix} p_{12}q_{2j} \\ p_{22}q_{2j} \\ \vdots \\ p_{m2}q_{2j} \end{bmatrix} + \ldots + \begin{bmatrix} p_{1k}q_{kj} \\ p_{2k}q_{kj} \\ \vdots \\ p_{mk}q_{kj} \end{bmatrix}$$

$$= q_{1j}\begin{bmatrix} p_{11} \\ \vdots \\ p_{m1} \end{bmatrix} + q_{2j}\begin{bmatrix} p_{12} \\ \vdots \\ p_{m2} \end{bmatrix} + \ldots + q_{kj}\begin{bmatrix} p_{1k} \\ \vdots \\ p_{mk} \end{bmatrix}$$

$$= q_{1j}[P]_1^c + q_{2j}[P]_2^c + \ldots + q_{kj}[P]_k^c$$

---

5 שתיהן שוות לאפס.

כלומר, העמודה $[PQ]_j^c$ היא אכן צירוף לינארי של העמודות של P כשמקדמי הצירוף הם הסקלרים $q_{1j},\dots,q_{kj}$.

מ.ש.ל.

הוכחת משפט 8.5.2

תהי $A=[a_{ij}]$ מטריצה מסדר $m\times n$ ונסמן $\rho_R(A)=k$. אז קיימים k וקטורים $v_1,\dots,v_k$ ב־ F^n הפורשים את מרחב השורות של A.

נסמן לכל $1\le i\le k$:

$$v_i=\left(b_{i1},\dots,b_{in}\right)$$

לכל $1\le i\le m$, השורה ה־ i של A היא צירוף לינארי של $v_1,\dots,v_k$.

נסמן ב־ c_{ij} מקדמי צירוף שכזה, כלומר:

$$[A]_i^r=c_{i1}v_1+\dots+c_{ik}v_k$$

מכאן:

$$\begin{aligned}\left(a_{i1},\dots,a_{in}\right)&=c_{i1}v_1+\dots+c_{ik}v_k\\&=c_{i1}\left(b_{11},\dots,b_{1n}\right)+\\&\quad\vdots\\&\quad+c_{ik}\left(b_{k1},\dots,b_{kn}\right)\end{aligned}$$

כלומר:

$$\begin{aligned}a_{i1}&=c_{i1}b_{11}+c_{i2}b_{21}+\dots+c_{ik}b_{k1}\\&\vdots\\a_{in}&=c_{i1}b_{1n}+c_{i2}b_{2n}+\dots+c_{ik}b_{kn}\end{aligned}$$

או, בכתיב מטריצות:[6]

$$[a_{i1},\dots,a_{in}]=[c_{i1},\dots,c_{ik}]\begin{bmatrix}b_{11}&\cdots&b_{1n}\\b_{21}&\cdots&b_{21}\\\vdots&\cdots&\vdots\\b_{k1}&\cdots&b_{k1}\end{bmatrix}$$

זאת לכל $1\le i\le m$. נסיק ש־ $A=CB$, כאשר $B=\left[b_{ij}\right]$, $C=\left[c_{ij}\right]$.

על פי למה 8.5.3, נסיק שעמודותיה של A הן צירופים לינאריים של k העמודות של המטריצה C. מכאן שמרחב העמודות של A נפרש על־ידי k עמודות המטריצה האחרונה, ולכן ממדו קטן מ־ k או שווה לו. כלומר $\rho_C(A)\le k$, ולכן:

(1) $$\rho_C(A)\le\rho_R(A)$$

(על פי הנחתנו, $\rho_R(A)=k$.)

---

6 בדקו!

אי־שוויון זה נכון עבור כל מטריצה, ובפרט עבור A^t:

$$\rho_C(A^t) \le \rho_R(A^t)$$

כלומר:

$$\rho_R(A) \le \rho_C(A) \quad (2)$$ [7]

מ־(1) ו־(2) נקבל:

$$\rho_R(A) = \rho_C(A)$$

מ.ש.ל.

הגדרה 8.5.4

ממד מרחב השורות של המטריצה A (שהוא גם ממד מרחב העמודות של A) נקרא **דרגת המטריצה**. את דרגת המטריצה A מסמנים $\rho(A)$.

שאלה 8.5.4

הוכיחו שלכל מטריצה מתקיים:

$$\rho(A) = \rho(A^t)$$

התשובה בעמוד 318

שאלה 8.5.5

תהי A מטריצה מסדר $m \times n$. הוכיחו כי:

$$\rho(A) \le \min\{m,n\}$$

התשובה בעמוד 318

שאלה 8.5.6

תהי C מכפלת שתי המטריצות A ו־B: $C = AB$ (כאשר המכפלה מוגדרת).

הוכיחו כי:

$$\rho(C) \le \min\{\rho(A), \rho(B)\}$$

או בניסוח מילולי:

דרגת המכפלה אינה עולה על דרגתו של אף גורם.

התשובה בעמוד 318

שאלה 8.5.7

א. תהי A מטריצה כלשהי מסדר $m \times n$, ותהי B מטריצה **הפיכה** מסדר $n \times n$.

הוכיחו כי:

$$\rho(AB) = \rho(A)$$

רמז: אם $AB = C$, אז $A = CB^{-1}$.

---

7 ראינו כבר שדרגת העמודות של A אינה אלא דרגת השורות של A^t, וכך גם דרגת השורות של A היא כדרגת העמודות של A^t.

ב. תהי A מסדר $m \times n$, ותהי C מטריצה **הפיכה** מסדר $m \times m$.

הוכיחו כי:

$$\rho(CA) = \rho(A)$$

התשובה בעמוד 319

שאלה 8.5.8

א. תהי A מטריצה **ריבועית** מסדר n.

הוכיחו כי

$$\rho(A) = n$$

אם ורק אם:

$$|A| \neq 0$$

ב. תהי A מטריצה מסדר $m \times n$.

1. הוכיחו כי

$$\rho(A) = m$$

אם ורק אם סדרת השורות של A בלתי תלויה לינארית.

מהו היחס בין m ו־ n במקרה זה?

2. הוכיחו כי

$$\rho(A) = n$$

אם ורק אם סדרת העמודות של A היא בלתי תלויה לינארית.

מהו היחס בין m ו־ n במקרה זה?

התשובה בעמוד 319

8.6 בחזרה למשוואות ליניאריות

עתה נשוב ונבחן מערכות של משוואות ליניאריות, הפעם לאור הידע שרכשנו בפרק זה. כבר ראינו (שאלה 7.1.7 בפרק הקודם) שקבוצת הפתרונות של מערכת משוואות ליניאריות **הומוגנית** ב־ n משתנים מעל שדה F היא **תת־מרחב** של F^n. בשאלת ממדו של תת־מרחב זה נעסוק בראשיתו של הסעיף, ואגב כך נציג את מרחב הפתרונות באמצעות בסיס למרחב זה.

דוגמה

במערכת המשוואות שלפניכם יש חמישה משתנים:

$$\begin{aligned} x_1 + 2x_2 - 2x_3 + 3x_4 + x_5 &= 0 \\ 2x_1 + 4x_2 - 3x_3 + 4x_4 + 2x_5 &= 0 \\ 5x_1 + 10x_2 - 8x_3 + 11x_4 + 5x_5 &= 0 \end{aligned}$$

נדרג את מטריצת המקדמים המצומצמת שלה:

$$\begin{bmatrix} 1 & 2 & -2 & 3 & 1 \\ 2 & 4 & -3 & 4 & 2 \\ 5 & 10 & -8 & 11 & 5 \end{bmatrix} \xrightarrow[R_3 \to R_3 - 5R_1]{R_2 \to R_2 - 2R_1} \begin{bmatrix} 1 & 2 & -2 & 3 & 1 \\ 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 2 & -4 & 0 \end{bmatrix}$$

$$\xrightarrow{R_3 \to R_3 - 2R_2} \begin{bmatrix} 1 & 2 & -2 & 3 & 1 \\ 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{R_1 \to R_1 + 2R_2} \begin{bmatrix} 1 & 2 & 0 & -1 & 1 \\ 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

כיוון שיש במטריצת המדרגות שתי שורות שאינן שורות אפס, הרי שדרגת מטריצת המקדמים המצומצמת של המערכת היא 2.

המערכת המדורגת נראית כך:

$$\begin{aligned} x_1 + 2x_2 \qquad - x_4 + x_5 &= 0 \\ x_3 - 2x_4 \qquad &= 0 \end{aligned}$$

המשתנים החופשיים הם x_2, x_4 ו־ x_5.

אם כן, הפתרון הכללי למערכת הוא:

$$v = (-2r + s - t, r, 2s, s, t)$$

נוכל לקבל שלושה פתרונות פרטיים אם נציב:

$$r = 1 \quad , \quad s = 0 \quad , \quad t = 0$$

או:

$$r = 0 \quad , \quad s = 1 \quad , \quad t = 0$$

או:

$$r = 0 \quad , \quad s = 0 \quad , \quad t = 1$$

הפתרונות שנקבל יהיו:

$$v_1 = (-2,1,0,0,0)$$

$$v_2 = (1,0,2,1,0)$$

$$v_3 = (-1,0,0,0,1)$$

שימו לב כי:

$$v = rv_1 + sv_2 + tv_3$$

כלומר, כל פתרון הוא צירוף לינארי של v_1, v_2, v_3.

נקל לוודא כי שלושת הוקטורים הללו הם בלתי תלויים,[1] ולכן ממדו של מרחב הפתרונות הוא 3. נשים לב שממד זה שווה למספר המשתנים החופשיים. מספר המשתנים החופשיים שווה גם למספר המשתנים פחות מספר האיברים הפותחים, ומספר האיברים הפותחים, שהוא כמספר השורות השונות מ־0, הוא בדיוק דרגת מטריצת המקדמים.[2] ◀

לפיכך גילינו בדוגמה שלפנינו כי (קראו משמאל לימין):

(ממד מרחב הפתרונות) = (דרגת מטריצת המקדמים המצומצמת) – (מספר המשתנים)

הנה דוגמה נוספת:

שאלה 8.6.1

תהי $A\mathbf{x} = 0$ מערכת משוואות הומוגנית ב־ n משתנים. נסמן ב־ P את מרחב הפתרונות של המערכת. הוכיחו את הנוסחה

$$n - \rho(A) = \dim P$$

במקרה שבו $\rho(A) = 0$.

התשובה בעמוד 320

עתה נוכיח שכך הדבר בכל מערכת משוואות הומוגנית.

משפט 8.6.1

אם $A\mathbf{x} = 0$ מערכת משוואות הומוגנית ב־ n משתנים ו־ P מרחב הפתרונות שלה, אז:

$$\dim P = n - \rho(A)$$

1 בדקו!

2 למה 8.5.1.

הוכחה

נסמן ב־ r את דרגת המטריצה A, כלומר:

$$r = \rho(A)$$

על־ידי תהליך הדירוג נביא את A למטריצת מדרגות. מספר האיברים הפותחים במטריצת מדרגות זו (שהוא כמספר שורותיה השונות מאפס) שווה ל־ r. מספר המשתנים החופשיים במערכת המדורגת הוא, אם כן, $n - r$.

שינוי סדר הופעת עמודות במטריצה אינו משנה את מרחב העמודות שלה, ולכן אנו רשאים להניח שהעמודות המתאימות למשתנים החופשיים מופיעות אחרונות, כלומר אנו מניחים שהמשתנים החופשיים הם $x_{r+1},\dots,x_n$. החלפת סדר המשתנים אינה משנה כמובן את ממד מרחב הפתרונות.

מטריצת המדרגות המתאימה נראית אפוא כך:

$$\begin{bmatrix} 1 & * & \dots & \dots & \dots & \dots & * \\ 0 & 1 & * & \dots & \dots & \dots & * \\ \vdots & & & \vdots & & & \vdots \\ 0 & \dots & \dots & 1 & * & \dots & * \\ 0 & \dots & \dots & 0 & \dots & \dots & 0 \\ \vdots & & & \vdots & & & \vdots \\ 0 & \dots & \dots & 0 & \dots & \dots & 0 \end{bmatrix}$$

בשיטת החילוץ, ניתן לבטא כל אחד מהמשתנים הקשורים המופיעים בפתרון הכללי $(x_1,\dots,x_r,x_{r+1},\dots,x_n)$ של המערכת באמצעות המשתנים החופשיים

$$\begin{aligned} x_1 &= c_{11}x_{r+1} + \dots + c_{1(n-r)}x_n \\ &\vdots \\ x_r &= c_{r1}x_{r+1} + \dots + c_{r(n-r)}x_n \end{aligned}$$

כאשר ה־ c_{ij} הם הסקלרים המתאימים המתקבלים באמצעות החילוץ.

את $(x_1,\dots,x_r,x_{r+1},\dots,x_n)$ נוכל לרשום כך:

$$(\underbrace{c_{11}x_{r+1} + \dots + c_{1(n-r)}x_n}_{x_1},\dots,\underbrace{c_{r1}x_{r+1} + \dots + c_{r(n-r)}x_n}_{x_r},x_{r+1},\dots,x_n)$$

$$\begin{aligned} &= x_{r+1}(c_{11},c_{21},\dots,c_{r1},1,0,0,\dots,0) + \\ &+x_{r+2}(c_{12},c_{22},\dots,c_{r2},0,1,0,\dots,0) + \\ &\qquad\vdots \\ &+x_n(c_{1(n-r)},c_{2(n-r)},\dots,c_{r(n-r)},0,0,0,\dots,0,1) \end{aligned} \tag{*}$$

בזאת הצגנו את הפתרון הכללי כצירוף לינארי של $n-r$ וקטורי הפתרונות הפרטיים:

$$v_1 = (c_{11}, c_{21}, \dots, c_{r1}, 1, 0, 0, \dots, 0)$$

$$v_2 = (c_{12}, c_{22}, \dots, c_{r2}, 0, 1, 0, \dots, 0)$$

$$\vdots$$

$$v_{n-r} = (c_{1(n-r)}, c_{2(n-r)}, \dots, c_{r(n-r)}, 0, 0, 0, \dots, 0, 1)$$

לכן מרחב הפתרונות P נפרש על־ידי וקטורים אלה. יתרה מזו, $n-r$ הוקטורים הללו הם **בלתי תלויים לינארית**.

שאלה 8.6.2

הוכיחו את הטענה האחרונה.

התשובה בעמוד 320

נסיק אם כן שקבוצת הוקטורים $\{v_1, \dots, v_{n-r}\}$ מהווה **בסיס** למרחב הפתרונות. לכן:

$$\dim P = n - r$$

כלומר:

$$\dim P = n - \rho(A)$$

מ.ש.ל.

שאלה 8.6.3

מצאו בסיסים למרחבי הפתרונות של מערכות המשוואות הבאות:

א.
$$\begin{aligned} x_1 - 3x_2 + x_3 &= 0 \\ 2x_1 + 2x_2 + 6x_3 &= 0 \\ x_1 + 5x_2 + 5x_3 &= 0 \end{aligned}$$

ב.
$$\begin{aligned} x_1 + 3x_2 + x_3 + 4x_4 &= 0 \\ 5x_1 + 4x_2 + 2x_3 + 3x_4 &= 0 \\ -7x_1 + x_2 - x_3 + 6x_4 &= 0 \end{aligned}$$

התשובה בעמוד 321

עד כה עסקנו במערכות משוואות לינאריות הומוגניות. לכל מערכת כזאת מובטח שיהיה פתרון. אין הדבר כך לגבי מערכות משוואות לינאריות לא הומוגניות. לא לכל מערכת כזאת יש פתרון. בפרק 1 מצאנו, שתנאי הכרחי ומספיק לקיום פתרון למערכת משוואות לינאריות נתונה הוא שלאחר דירוג מטריצת המקדמים שלה, לא תימצא במטריצה המדורגת שורה מהטיפוס $(0, \dots, 0, b)$ כאשר $b \neq 0$.
עתה ננסח תנאי נוסף, שגם הוא תנאי הכרחי ומספיק לקיום פתרון למערכת משוואות לינאריות.

משפט 8.6.2
למערכת משוואות לינאריות קיים פתרון אם ורק אם דרגת מטריצת המקדמים שלה שווה לדרגת מטריצת המקדמים המצומצמת.

הוכחה
נתבונן במערכת משוואות לינארית:

$$\begin{array}{lllll} a_{11}x_1 & +\ldots+ & a_{1n}x_n & = & b_1 \\ \vdots & & & & \\ a_{m1}x_1 & +\ldots+ & a_{mn}x_n & = & b_m \end{array}$$

נכתוב את המערכת בכתיב וקטורי:

$$x_1\begin{bmatrix} a_{11} \\ \vdots \\ a_{m1} \end{bmatrix} + \ldots + x_n\begin{bmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

לחלופין -

$$x_1\mathbf{a}_1 + \ldots + x_n\mathbf{a}_n = \mathbf{b}$$

כאשר $\mathbf{a}_1,\ldots,\mathbf{a}_n,\mathbf{b}$ הן עמודותיה של מטריצת המקדמים של המערכת.

מרחב העמודות של מטריצת המקדמים (הנפרש על־ידי $\mathbf{a}_1,\ldots,\mathbf{a}_n,\mathbf{b}$) בוודאי מכיל את מרחב העמודות של מטריצת המקדמים המצומצמת (הנפרש על־ידי $\mathbf{a}_1,\ldots,\mathbf{a}_n$). לפי משפט 8.3.4, שני המרחבים שווים זה לזה אם ורק אם ממדיהם שווים, כלומר אם ורק אם דרגת מטריצת המקדמים של המערכת שווה לדרגת מטריצת המקדמים המצומצמת.

מאידך גיסא, ברור ששני המרחבים שווים אם ורק אם הוקטור $\mathbf{b}$ שייך למרחב העמודות של מטריצת המקדמים המצומצמת, כלומר אם ורק אם $\mathbf{b} \in \mathrm{Sp}(\{\mathbf{a}_1,\ldots,\mathbf{a}_n\})$. תנאי זה שקול לקיום פתרון למערכת $x_1\mathbf{a}_1 + \ldots + x_n\mathbf{a}_n = \mathbf{b}$.

מ.ש.ל.

שאלה 8.6.4
נתבונן בקבוצת וקטורים בלתי תלויה לינארית במרחב F^n בת k וקטורים $(k < n)$. משפט 8.3.5 קובע שקבוצת וקטורים זו ניתנת להשלמה לבסיס של F^n. אולם הוכחת משפט זה אינה קונסטרוקטיבית. הוכחנו שקיימים $n-k$ וקטורים אשר משלימים את הקבוצה הנתונה לבסיס, אך לא הצבענו על דרך למציאתם! נסו לתאר תהליך שבעזרתו אפשר לבצע את ההשלמה לבסיס הלכה למעשה.

התשובה בעמוד 322

8.7 תלות הממד בשדה ההגדרה

בשאלה 7.1.2 בפרק 7, ראיתם כי אם V הוא מרחב לינארי מעל שדה F, ואם K הוא תת־שדה של F, אזי V מרחב לינארי גם מעל K ביחס לאותן הפעולות. כלומר, קבוצת איברי V, בצירוף אותה פעולת חיבור על V ואותה פעולת כפל בסקלר מ־ K (כאשר אנו "שוכחים" את האפשרות לכפול בסקלרים שאינם ב־ K), מהווה מרחב לינארי מעל K. כך למשל, המרחב $\mathbb{C}^3$ הוא מרחב לינארי מעל שדה המרוכבים $\mathbb{C}$, אך הוא גם מרחב לינארי מעל שדה המספרים הממשיים $\mathbb{C}$ (שהוא תת־שדה של $\mathbb{C}$).

שימו לב: כאשר אנו מסמנים מרחב לינארי, אנו משתמשים באותה האות (V, לרוב) כדי לציין הן את המרחב הלינארי והן את קבוצת איברי המרחב. בסעיף זה נעסוק באופן שבו אותה קבוצת איברים מהווה מרחב לינארי מעל שדות שונים, ולכן נקפיד לציין בכל עת מהו השדה המתאים - **שדה ההגדרה של המרחב**. אנו נתמקד במקרה שבו $F = \mathbb{C}$ ו־ $K = \mathbb{R}$, אך נציין כי ניתן להרחיב את התוצאות שנציג גם לשדות אחרים.

נפתח בשאלה הבאה, הממחישה את האופן שבו שינוי שדה ההגדרה משפיע על תכונות של וקטורים במרחב והקשרים שביניהם.

שאלה 8.7.1

א. יהי F שדה כלשהו, ונראה את F כמרחב לינארי מעל עצמו (עיינו בסעיף 7.1). יהיו $a,b \in F$ זוג איברים שונים, שאינם אפס. האם a,b תלויים לינארית? האם הקבוצה $\{a,b\}$ פורשת את F?

ב. נתבונן ב־ $\mathbb{C}$ כמרחב לינארי מעל עצמו. האם האיברים $1,i$ תלויים לינארית? האם הקבוצה $\{1,i\}$ פורשת את $\mathbb{C}$? האם היא בסיס?

ג. נתבונן ב־ $\mathbb{C}$ כמרחב לינארי מעל $\mathbb{R}$. האם האיברים $1,i$ תלויים לינארית? האם הם פורשים את $\mathbb{C}$? האם הקבוצה $\{1,i\}$ בסיס?

ד. נתבונן ב־ $\mathbb{C}^2$ כמרחב לינארי מעל $\mathbb{C}$. מצאו בסיס ל־ $\mathbb{C}^2$ מעל $\mathbb{C}$.

ה. נתבונן ב־ $\mathbb{C}^2$ כמרחב לינארי מעל $\mathbb{R}$. מצאו בסיס ל־ $\mathbb{C}^2$ מעל $\mathbb{R}$.

ו. מהו הממד של $\mathbb{C}$ כמרחב לינארי מעל $\mathbb{C}$?

ז. מהו הממד של $\mathbb{C}$ כמרחב לינארי מעל $\mathbb{R}$?

ח. מהו הממד של $\mathbb{C}^2$ כמרחב לינארי מעל $\mathbb{C}$?

ט. מהו הממד של $\mathbb{C}^2$ כמרחב לינארי מעל $\mathbb{R}$?

התשובה בעמוד 325

את התוצאות שהצגנו בשאלה 8.7.1, נכליל עתה למרחבים לינאריים (נוצרים סופית) כלליים מעל שדה המספרים המרוכבים.

משפט 8.7.1

יהי V מרחב לינארי נוצר סופית מעל שדה המספרים המרוכבים $\mathbb{C}$, ונסמן את הממד של V מעל $\mathbb{C}$ ב- n.[1] אזי V נוצר סופית גם כמרחב לינארי מעל $\mathbb{R}$, וממדו מעל $\mathbb{R}$ הוא $2n$.

הוכחה

יהי $B = \{v_1, v_2, ..., v_n\}$ בסיס ל- V מעל $\mathbb{C}$, ונסמן $B' = \{v_1, v_2, ..., v_n, iv_1, iv_2, ..., iv_n\}$. תחילה נראה ש- B' פורשת את V מעל $\mathbb{R}$. אכן, יהי $v \in V$. מכיוון ש- B בסיס ל- V מעל $\mathbb{C}$, קיימים סקלרים מרוכבים $z_1 = a_1 + ib_1, z_2 = a_2 + ib_2, ..., z_n = a_n + ib_n$ כך ש-

$$v = z_1 v_1 + ... + z_n v_n$$

נוכל לרשום וקטור זה באופן שונה, כך:

$$v = a_1 v_1 + ib_1 v_1 + ... + a_n v_n + ib_n v_n = a_1 v_1 + ... + a_n v_n + b_1(iv_1) + ... + b_n(iv_n)$$

בזאת הצגנו את הוקטור v כצירוף לינארי של איברי B' (במקדמים ממשיים). נסיק ש-B' פורשת את V מעל $\mathbb{R}$. בפרט, V נוצר סופית כמרחב לינארי מעל $\mathbb{R}$.

כעת נראה שהקבוצה B' בלתי תלויה לינארית מעל $\mathbb{R}$. נניח כי $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n$ הם סקלרים ממשיים כך ש-

$$a_1 v_1 + a_2 v_2 + ... + a_n v_n + b_1(iv_1) + ... + b_n(iv_n) = 0$$

לאחר ארגון מחדש של המחוברים, נקבל

$$(a_1 + ib_1)v_1 + ... + (a_n + ib_n)v_n = 0$$

מכיוון שהקבוצה $B = \{v_1, v_2, ..., v_n\}$ בלתי תלויה לינארית מעל $\mathbb{C}$, כל אחד מן הסקלרים המרוכבים $a_1 + ib_1, ..., a_n + ib_n$ הוא אפס, ולכן החלק הממשי והמדומה של כל אחד מסקלרים אלה הוא אפס. כלומר, $a_1 = b_1 = ... = a_n = b_n = 0$. נסיק שהקבוצה B' בלתי תלויה לינארית מעל $\mathbb{R}$, ובעצם מהווה בסיס. מכיוון שבקבוצה זו $2n$ איברים, הוכחנו שהממד המבוקש הוא $2n$.

מ.ש.ל.

ייתכן שמשפט 8.7.1 נראה כסותר את האינטואיציה - **הקטנת** השדה שמעליו מוגדר המרחב מובילה ל**הגדלת** הממד. כדי לסבר את האוזן, ננסה לתת את הנימוק הבלתי פורמלי הבא: במובן מסוים, הממד של מרחב לינארי (נוצר סופית) V מעל שדה F קובע "כמה פעמים נכנס F ב- V". לכן, אם $\mathbb{R}$ "נכנס n פעמים" במרחב לינארי V, ואם $\mathbb{R}$ "נכנס פעמיים" ב- $\mathbb{C}$ (כפי שראיתם בחלק ז של שאלה 8.7.1), הרי ש- $\mathbb{R}$ "נכנס $2 \cdot n$ פעמים" ב- V.

1 מאחר שהמרחב נוצר סופית, בהכרח יש לו בסיס, ולכן אנו רשאים לדבר על ממדו.

תשובות לשאלות בפרק 8

תשובה 8.1.1 **השאלה בעמוד 244**

כיוון ראשון:

אם K בלתי תלויה לינארית, הרי שלפי האמור בהערה א, מתוך השוויון

$$a_1v_1 + \ldots + a_kv_k = 0$$

כאשר $a_1,\ldots,a_k$ סקלרים מתוך F, נובע בהכרח כי $a_1 = \ldots = a_k$.

כיוון שני:

נניח שההצגה היחידה של וקטור האפס כצירוף לינארי של **כל** איברי K היא ההצגה הטריוויאלית, ונוכיח כי K בלתי תלויה לינארית. לשם כך, לפי הערה א, די שנראה כי כל הצגה של וקטור האפס כצירוף לינארי של וקטורים שונים מתוך K (ולאו דווקא של **כל** איברי K) היא טריוויאלית; אכן, אילו הייתה ל־0 הצגה לא־טריוויאלית - כצירוף לינארי של וקטורים שונים מתוך K, יכולנו להוסיף לצירוף כל אחד מאיברי K שאינם מופיעים בו, עם מקדם 0, ולקבל הצגה לא־טריוויאלית של וקטור האפס כצירוף לינארי של כל איברי K.

תשובה 8.1.2 **השאלה בעמוד 244**

א. כדי לבדוק אם הקבוצה תלויה לינארית או לא, עלינו לבדוק האם קיימים סקלרים α,β,γ כך ש־

$$\alpha(1+x)+\beta(1-x)+\gamma(1-x^2) = 0$$

כלומר,

$$\alpha+\alpha x+\beta-\beta x+\gamma-\gamma x^2 = 0$$

או:

$$(\alpha+\beta+\gamma)+(\alpha-\beta)x-\gamma x^2 = 0$$

או באופן שקול:

$$\alpha+\beta+\gamma = 0$$

$$\alpha-\beta = 0$$

$$-\gamma = 0$$

למערכת לינארית זו יש פתרון יחיד והוא הפתרון הטריוויאלי $\alpha=\beta=\gamma=0$, ולכן הקבוצה $\{1+x,1-x,1-x^2\}$ בלתי תלויה לינארית.

ב. קבוצת המטריצות ההפיכות מסדר 2×2 מעל הממשיים היא תלויה לינארית, שכן איבר האפס (המטריצה $\begin{bmatrix}0&0\\0&0\end{bmatrix}$), ניתן להצגה כצירוף לא־טריוויאלי של איברי קבוצה זו, למשל באופן הבא:

$$4\begin{bmatrix}1&0\\0&1\end{bmatrix}+2\begin{bmatrix}-2&0\\0&-2\end{bmatrix}=\begin{bmatrix}0&0\\0&0\end{bmatrix}$$

(שימו ש־ $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ו־ $\begin{bmatrix} -2 & 0 \\ 0 & -2 \end{bmatrix}$ הן מטריצות הפיכות, למשל מכיוון שהדטרמיננטה של כל אחת מהן שונה מאפס.)

ג. עלינו לבדוק האם קיימים סקלרים $\alpha, \beta, \gamma, \delta$ כך ש־

$$\alpha(1,-1,0,0) + \beta(0,2,-2,0) + \gamma(0,0,3,-3) + \delta(-4,0,0,4) = (0,0,0,0)$$

או באופן שקול:

$$\alpha - 4\delta = 0$$

$$-\alpha + 2\beta = 0$$

$$-2\beta + 3\gamma = 0$$

$$-3\gamma + 4\delta = 0$$

למערכת הומוגנית זו יש פתרונות לא־טריוויאליים (כל הוקטורים $(\alpha, \beta, \gamma, \delta)$ שבהם α כלשהו ו־ $\beta = \frac{\alpha}{2}, \gamma = \frac{\alpha}{3}, \delta = \frac{\alpha}{4}$), ולכן הקבוצה

$$\{(1,-1,0,0), (0,2,-2,0), (0,0,3,-3), (-4,0,0,4)\}$$

תלויה לינארית.

ד. הקבוצה תלויה, שכן:

$$1 \cdot (1,0,1) + 1 \cdot (0,1,1) + 1 \cdot (1,1,0) = (1+0+1, 0+1+1, 1+1+0) = (0,0,0)$$

תשובה 8.1.3 **השאלה בעמוד 244**

א. אם K קבוצה המכילה את וקטור האפס, אז ההצגה $0 = 1 \cdot 0$ היא הצגה של וקטור האפס כצירוף לינארי לא־טריוויאלי של וקטורים מתוך K, ולכן K תלויה לינארית.

ב. נניח כי $v_1, v_2 \in K$ וכי קיים סקלר λ כך ש־ $v_1 = \lambda v_2$. אז:

$$(-1) \cdot v_1 + \lambda v_2 = (-1)(\lambda v_2) + \lambda v_2 = (-\lambda) v_2 + \lambda v_2 = 0 \cdot v_2 = 0$$

בכך הצגנו את וקטור האפס כצירוף לא־טריוויאלי של וקטורים מ־ K, ולכן K תלויה לינארית.

תשובה 8.1.4 **השאלה בעמוד 245**

א. K תת־קבוצה של V, שהיא בלתי תלויה לינארית.

תהי S תת־קבוצה לא ריקה של K, ונניח בשלילה כי S תלויה לינארית. במקרה זה וקטור האפס ניתן להצגה כצירוף לא־טריוויאלי של וקטורים מ־ S.

כיוון ש־ S חלקית ל־ K, כל וקטור ב־ S הוא גם וקטור ב־ K, ולכן וקטור האפס ניתן להצגה כצירוף לא־טריוויאלי של וקטורים ב־ K, ולכן K תלויה לינארית, בסתירה לנתון.

ב. הטענה שבחלק זה נובעת, כמובן, מן הטענה שבחלק הקודם: אם $T \subseteq K$ ו־ T תלויה לינארית, אז K תלויה לינארית, כי אילו K הייתה בלתי תלויה לינארית, אז T הייתה בלתי תלויה לינארית.

תשובה 8.1.5 **השאלה בעמוד 245**

כיוון ראשון:

אם $v = 0$, אז הקבוצה $\{v\}$, שהיא $\{0\}$, תלויה לינארית לפי שאלה 8.1.3.

כיוון שני:

נניח כי הקבוצה $\{v\}$ $(v \in V)$ תלויה לינארית. כל צירוף לינארי מתוך $\{v\}$ הוא מהצורה $\lambda \cdot v$ (λ סקלר). נניח כי וקטור האפס הוא צירוף לא־טריוויאלי של וקטורים מ־ $\{v\}$, אז קיים $\lambda \neq 0$ כך ש־ $0 = \lambda \cdot v$. מכך נובע כי $v = 0$.

מסקנה

$\{v\}$ תלויה לינארית אם ורק אם $v = 0$.

תשובה 8.1.6 **השאלה בעמוד 245**

תהי $K = \{v_1, \ldots, v_n\}$ תת־קבוצה של V, $(n \geq 2)$.

כיוון ראשון:

נניח כי K תלויה לינארית. במקרה זה וקטור האפס ניתן להצגה כצירוף לא־טריוויאלי של וקטורים מתוך K, ונוכל לרשום:

$$\lambda_1 v_1 + \ldots + \lambda_n v_n = 0$$

(אם הצירוף המקורי לא כלל את כל הוקטורים ב־ K, ניתן להוסיף לצירוף את שאר הוקטורים של K עם מקדם 0.)

כיוון שהצירוף לא־טריוויאלי, לפחות אחד ה־ λ_i־ים שונה מאפס. נוכל להניח בלי הגבלת הכלליות כי $\lambda_1 \neq 0$. כעת נרשום:

$$\lambda_1 v_1 = (-\lambda_2 v_2) + (-\lambda_3 v_3) + \ldots + (-\lambda_n v_n)$$

כיוון ש־ $\lambda_1 \neq 0$, נוכל לכפול את שני האגפים ב־ λ_1^{-1}, ונקבל:

$$v_1 = \lambda_1^{-1}(-\lambda_2)v_2 + \ldots + \lambda_1^{-1}(-\lambda_n)v_n$$

בכך הצגנו את v_1 כצירוף לינארי של שאר הוקטורים ב־ K.

כיוון שני:

נניח כי אחד הוקטורים ב־ K הוא צירוף לינארי של שאר איברי K. בלי הגבלת הכלליות יהא זה v_1, ואז מתקיים:

$$v_1 = \lambda_2 v_2 + \ldots + \lambda_n v_n$$

לכן נוכל לרשום:

$$0 = (-1)v_1 + \lambda_2 v_2 + \ldots + \lambda_n v_n$$

זוהי הצגה של וקטור האפס כצירוף לא־טריוויאלי של איברי K (הצירוף אינו טריוויאלי, כי המקדם של v_1 איננו אפס). לכן K תלויה לינארית.

תשובה 8.1.7 **השאלה בעמוד 246**

כיוון ראשון:

נניח כי K תלויה לינארית, ונמצא קבוצה $T \subset K$ שעבורה $\mathrm{Sp}(T) = \mathrm{Sp}(K)$. לפי שאלה 8.1.5, $\{v\}$ תלויה לינארית אם ורק אם $v = 0$. כיוון ש־ $K \neq \{0\}$ לפי הנתון, נובע כי יש ב־ K לפחות שני וקטורים.

לפי משפט 8.1.2, יש וקטור ב־ K הניתן להצגה כצירוף לינארי של וקטורים אחרים מ־ K. נניח, אם כן, כי

$$w = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

כאשר $\lambda_1, \ldots, \lambda_n$ סקלרים ו־ $w, v_1, \ldots, v_n$ איברים ב־ K, וכן $w \neq v_i$ לכל $1 \leq i \leq n$.

הקבוצה T, המכילה את כל איברי K פרט ל־ w, חלקית ממש ל־ K. כמו כן, ברור כי $\mathrm{Sp}(T) \subseteq \mathrm{Sp}(K)$ (צירוף לינארי של איברי T הוא בפרט צירוף לינארי של איברי K).

כעת נוכיח כי $\mathrm{Sp}(K) \subseteq \mathrm{Sp}(T)$.

יהי $\mu_1 u_1 + \ldots + \mu_m u_m \in \mathrm{Sp}(K)$ איבר כלשהו ב־ $\mathrm{Sp}(K)$ (כלומר, $u_i \in K$ ו־ μ_i סקלר, לכל $1 \leq i \leq m$). אם אף אחד מה־ u_i־ים אינו w, אז $u_i \in T$ לכל $1 \leq i \leq m$, ולכן:

$$\mu_1 u_1 + \ldots + \mu_m u_m \in \mathrm{Sp}(T)$$

כעת נניח כי אחד ה־ u_i־ים הוא w, ובלי הגבלת הכלליות יהא זה u_1. במקרה זה נוכל לרשום:

$$\begin{aligned}\mu_1 u_1 + \ldots + \mu_m u_m &= \mu_1 w + \mu_2 u_2 + \ldots + \mu_m u_m \\ &= \mu_1(\lambda_1 v_1 + \ldots + \lambda_n v_n) + \mu_2 u_2 + \ldots + \mu_m u_m \\ &= (\mu_1 \lambda_1) v_1 + \ldots + (\mu_1 \lambda_n) v_n + \mu_2 u_2 + \ldots + \mu_m u_m\end{aligned}$$

שימו לב ש־ $v_1 \ldots v_n, u_2 \ldots u_m$ הם איברים של T, לכן

$$\mu_1 u_1 + \ldots + \mu_m u_m \in \mathrm{Sp}(T)$$

ולכן:

$$\mathrm{Sp}(K) \subseteq \mathrm{Sp}(T)$$

מסקנה: $\mathrm{Sp}(T) = \mathrm{Sp}(K)$

כיוון שני:

נניח כי קיימת T חלקית ממש ל־ K שעבורה $\mathrm{Sp}(K) = \mathrm{Sp}(T)$.
נוכיח כי K תלויה לינארית.

T חלקית ממש ל־ K, לכן יש וקטור $v \in K$ שאינו ב־ T. $v \in K$, לכן בפרט $v \in \mathrm{Sp}(K)$. מאחר ש־ $\mathrm{Sp}(K) = \mathrm{Sp}(T)$, נובע כי ניתן להציג את v כצירוף לינארי של וקטורים מתוך T:

$$v = \lambda_1 t_1 + \ldots + \lambda_n t_n$$

אם כך, נוכל לרשום:

$$0 = (-1)v + \lambda_1 t_1 + \ldots + \lambda_n t_n$$

הצגה זו היא הצגה של 0 כצירוף לא־טריוויאלי של וקטורים מתוך K (הצירוף לא־טריוויאלי, כי המקדם של v שונה מאפס). לכן K תלויה לינארית.

תשובה 8.1.8 **השאלה בעמוד 246**

כיוון ראשון:

נניח כי $v \notin K$ וכי v תלוי בקבוצה K. במקרה זה ניתן להציג

$$v = \lambda_1 v_1 + \ldots + \lambda_k v_k$$

כאשר $v_i \in K$ ו־λ_i סקלר לכל $1 \le i \le k$.

לכן נוכל לרשום:

$$0 = (-1)v + \lambda_1 v_1 + \ldots + \lambda_k v_k$$

וקטור האפס הוצג כאן כצירוף לא־טריוויאלי של וקטורים מתוך $K \cup \{v\}$, ולכן $K \cup \{v\}$ תלויה לינארית.

כיוון שני:

נניח כי $K \cup \{v\}$ תלויה לינארית. אזי נוכל לרשום

$$0 = \lambda_1 v_1 + \ldots + \lambda_n v_n + \lambda v \qquad (1)$$

כאשר $v_i \in K$ לכל $1 \le i \le k$, וכאשר לפחות אחד מבין הסקלרים $\lambda, \lambda_n \ldots \lambda_1$ שונה מאפס.

אם $\lambda = 0$, אז

$$0 = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

כאשר לא כל ה־λ_i־ים הם אפסים, בסתירה לאי־תלות הקבוצה K.

לכן $\lambda \ne 0$, ונוכל לכפול את (1) ב־λ^{-1} ולקבל

$$0 = \lambda^{-1}\lambda_1 v_1 + \ldots + \lambda^{-1}\lambda_n v_n + v$$

או

$$v = -\lambda^{-1}\lambda_1 v_1 - \ldots - \lambda^{-1}\lambda_n v_n$$

ולכן v תלוי בקבוצה K.

תשובה 8.1.9 **השאלה בעמוד 247**

א. נניח בשלילה ש־$v_i = v_j$, עבור $1 \le i, j \le n$, $i \ne j$. אזי $1 \cdot v_i + (-1)v_j = 0$ הוא צירוף לינארי לא־טריוויאלי של איברי הסדרה (שאר הוקטורים הם עם מקדם אפס המתאפס, סתירה.

ב. הטענה מתקיימת ישירות על פי ההגדרה.

תשובה 8.2.1 **השאלה בעמוד 249**

כל פולינום $P(x)$ ב־$F_n[x]$ הוא פולינום ממעלה קטנה מ־n, ולכן ניתן להצגה בצורה

$$P(x) = a_0 x + a_1 x + \ldots + a_{n-1}x^{n-1} \qquad (1)$$

כאשר $a_0, \ldots, a_{n-1}$ סקלרים.

אבל הצגה זו היא הצגה של $P(x)$ כצירוף לינארי של איברי הקבוצה $\{1, x, \ldots, x^{n-1}\}$. לכן קבוצה זו פורשת את $F_n[x]$.

נוכיח כי קבוצה זו היא בלתי תלויה לינארית. ואמנם, אם צירוף לינארי של $1, x, \ldots, x^{n-1}$ עם מקדמים מתאימים $a_0, \ldots, a_{n-1}$,

$$a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$$

הוא פולינום האפס, אז המקדמים $a_0, \ldots, a_{n-1}$ כולם אפסים.

לפיכך – ההצגה היחידה של וקטור האפס של $F_n[x]$ כצירוף לינארי של איברי הקבוצה הנדונה היא הטריוויאלית, ולכן הקבוצה היא בלתי תלויה לינארית.

אם כן, הקבוצה $\{1, x, \ldots, x^{n-1}\}$ היא קבוצה פורשת ובלתי תלויה ב־ $F_n[x]$, ולכן מהווה בסיס של $F_n[x]$.

תשובה 8.2.2 **השאלה בעמוד 249**

1. הקבוצה $K = \{1, x, x^2, \ldots, x^n, \ldots\}$ פורשת את $F[x]$, כי לכל $P(x) \in F[x]$ קיים n וקיימים סקלרים $a_0, a_1, \ldots, a_n$ שעבורם:

$$P(x) = a_0 + a_1 x + \ldots + a_n x^n$$

זוהי הצגה של $P(x)$ כצירוף לינארי של איברי הקבוצה K, ולכן $\mathrm{Sp}(K) = F[x]$. (שימו לב, בכל פולינום יש מספר **סופי** של מונומים – מחוברים מהטיפוס $\alpha_k x^k$.)

2. נוכיח כי K בלתי תלויה לינארית:

נניח כי וקטור האפס של $F[x]$, כלומר פולינום האפס, ניתן להצגה כצירוף לינארי של איברים מתוך K. כיוון שצירוף לינארי כולל מספר סופי של מחוברים, נובע כי:

$$0 = a_0 + a_1 x + \ldots + a_n x^n$$

אולם

$$0 = 0 + 0x + \ldots + 0x^n$$

ולכן $a_0 = a_1 = \ldots = a_n = 0$.

כלומר, **לכל** הצגה מהטיפוס $0 = a_0 + a_1 x + \ldots + a_n x^n$ מתקיים:

$$a_0 = a_1 = \ldots = a_n = 0$$

אם כן, כל הצגה של וקטור האפס כצירוף לינארי של איברי K היא טריוויאלית, לכן K בלתי תלויה לינארית ו־ $\mathrm{Sp}(K) = F[x]$, ולכן K הינה בסיס ל־ $F[x]$.

תשובה 8.2.3 **השאלה בעמוד 249**

הקבוצה $K = \{e_1, e_2, e_3, \ldots\}$ אינה מהווה בסיס למרחב הסדרות. למשל, הסדרה $(a_n) = (1,1,1,\ldots)$ אינה ניתנת להצגה כצירוף לינארי של איברים מתוך K. בכל צירוף לינארי של איברים מ־ K מופיע

מספר **סופי** בלבד של מחוברים, ולכן כל צירוף לינארי של איברים מ־ K הוא סדרה שבה יש רק מספר סופי של איברים השונים מאפס, כלומר זו סדרה שהחל ממקום מסוים כל איבריה שווים לאפס. כיוון שכל איברי הסדרה (a_n) שהוגדרה למעלה שונים מאפס, ברור שסדרה זו איננה שייכת ל־ $\mathrm{Sp}(K)$, ולכן K אינה פורשת את מרחב הסדרות הממשיות ומשום כך אינה בסיס שלו. (בכל זאת, K בלתי תלויה, ותוכלו לבדוק כי היא מהווה בסיס למרחב לינארי הכולל את כל הסדרות שרק מספר סופי של איבריהן שונה מאפס.)

תשובה 8.2.4 **השאלה בעמוד 254**

נבצע פעולות אלמנטריות על שורות מטריצת המקדמים של המערכת הנתונה:

$$\begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 2 & 1 & -2 \\ 2 & 3 & 2 & -3 \\ 2 & 3 & 2 & -3 \end{bmatrix} \xrightarrow[\substack{R_3 \to R_3 - 2R_1 \\ R_4 \to R_4 - 2R_1}]{R_2 \to R_2 - R_1} \begin{bmatrix} 1 & 1 & 1 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & -1 \end{bmatrix} \xrightarrow[\substack{R_3 \to R_3 - R_2 \\ R_4 \to R_4 - R_2}]{R_1 \to R_1 - R_2} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

המטריצה האחרונה היא מטריצת המקדמים של מערכת המשוואות

$$\begin{aligned} x_1 + x_3 &= 0 \\ x_2 - x_4 &= 0 \end{aligned} \qquad (1)$$

וברור כי כל וקטור מהטיפוס $(\alpha,\beta,-\alpha,\beta)$, כאשר α,β ממשיים כלשהם, מהווה פתרון למערכת המשוואות (1) ולכן גם למערכת המשוואות המקורית.

כלומר, מרחב הפתרונות T הוא הקבוצה:

$$T = \{(\alpha,\beta,-\alpha,\beta) \mid \alpha,\beta \in R\}$$

נתבונן כעת בקבוצת הוקטורים

$$K = \{(1,0,-1,0),(0,1,0,1)\}$$

ונראה כי היא מהווה בסיס למרחב הפתרונות.

בהינתן וקטור כלשהו $(\alpha,\beta,-\alpha,\beta)$ ב־ T נוכל לרשום

$$(\alpha,\beta,-\alpha,\beta) = \alpha(1,0,-1,0) + \beta(0,1,0,1)$$

ולכן K פורשת את T.

כעת נשים לב כי K בלתי תלויה לינארית. ואכן, אם

$$\alpha(1,0,-1,0) + \beta(0,1,0,1) = (0,0,0,0)$$

אזי בהכרח $\alpha = \beta = 0$, ומכאן ש־ K בלתי תלויה לינארית.

ראינו, אם כן, כי הקבוצה

$$\{(1,0,-1,0),(0,1,0,1)\}$$

הינה קבוצה בלתי תלויה לינארית הפורשת את T, ולכן קבוצה זו מהווה בסיס ל־ T.

תשובה 8.2.5 **השאלה בעמוד 255**

נבדוק האם המטריצות הנתונות תלויות לינארית, כלומר האם קיימים סקלרים x, y, z, w שעבורם:

$$x\begin{pmatrix}1&0\\0&0\end{pmatrix}+y\begin{pmatrix}0&2\\0&0\end{pmatrix}+z\begin{pmatrix}0&0\\1&1\end{pmatrix}+w\begin{pmatrix}-1&2\\2&2\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

כלומר:

$$\begin{pmatrix}x-w&2y+2w\\z+2w&z+2w\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

כלומר:

$$x-w=0$$
$$2y+2w=0$$
$$z+2w=0$$
$$z+2w=0$$

זוהי מערכת משוואות בארבעה נעלמים. בדיקה ישירה, שאותה בוודאי תוכלו לבצע בעצמכם, מגלה שלמערכת זו יש פתרון לא־טריוויאלי, למשל, $x=-1, y=1, z=2, w=-1$. לכן:

$$(-1)\begin{pmatrix}1&0\\0&0\end{pmatrix}+1\begin{pmatrix}0&2\\0&0\end{pmatrix}+2\begin{pmatrix}0&0\\1&1\end{pmatrix}+(-1)\begin{pmatrix}-1&2\\2&2\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$

על־ידי העברת אגפים נוכל לבטא את אחת המטריצות כצירוף לינארי של האחרות, למשל כך:

$$(-1)\begin{pmatrix}1&0\\0&0\end{pmatrix}+1\begin{pmatrix}0&2\\0&0\end{pmatrix}+2\begin{pmatrix}0&0\\1&1\end{pmatrix}=\begin{pmatrix}-1&2\\2&2\end{pmatrix}$$

מכאן שהמרחב U נפרש על־ידי שלוש המטריצות:

$$\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&2\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&1\end{pmatrix}$$

בדיקה ישירה מעלה כי מטריצות אלה בלתי תלויות לינארית, ולכן מהוות בסיס ל־ U.

תשובה 8.3.1 **השאלה בעמוד 256**

אנו מכירים כבר בסיס אחד ל־ F^n - הבסיס הסטנדרטי. כמו כן ראינו כי כל n וקטורים הפורשים את F^n מהווים בסיס של F^n. אי לכך, להוכחת הטענה שבשאלה די שנוכיח, למשל, כי לכל $\lambda \in F$, $\lambda \neq 0$, הקבוצה

$$B=\{\lambda\mathbf{e}_1,\mathbf{e}_2,...,\mathbf{e}_n\}$$

פורשת את F^n.

ואמנם, כל וקטור ב־ F^n ניתן להצגה כצירוף לינארי של איברי הקבוצה B, שכן לכל וקטור $(a_1,...,a_n)\in F^n$, מתקיים:

$$(a_1,...,a_n)=\frac{a_1}{\lambda}(\lambda\mathbf{e}_1)+a_2\mathbf{e}_2+...+a_n\mathbf{e}_n$$

תשובה 8.3.2 **השאלה בעמוד 257**

יהי $B=\{v_1,\dots,v_n\}$ בסיס בעל n וקטורים למרחב V.

א. הקבוצה B בוודאי פורשת את V, ולכן על פי למה 8.3.1 - לכל $m>n$, כל m וקטורים ב־V הם תלויים לינארית.

ב. אילו הייתה קבוצה שבה פחות מ־n וקטורים, הפורשת את V, אז על פי הלמה, כל n וקטורים ב־V היו תלויים לינארית. אבל $v_1,\dots,v_n$ הם בלתי תלויים לינארית.

ג. נוכיח כי קבוצה בלתי תלויה לינארית K, שבה בדיוק n וקטורים, פורשת את V ולכן היא בסיס של V.

לכל $v\in V$, השונה מכל איברי K, הקבוצה $K\cup\{v\}$ היא קבוצה בעלת $n+1$ וקטורים ולכן היא תלויה לינארית (על פי חלק א). לכן קיימים $a_1,\dots,a_n,\lambda$ שלא כולם אפס כך ש־

$$0=a_1v_1+\ldots+a_nv_n+\lambda v \qquad (*)$$

ברור ש־$\lambda\neq 0$, כי אחרת היה 0 צירוף לא־טריוויאלי של איברי K שהיא בלתי תלויה, וזה לא ייתכן. על־ידי העברה מאגף לאגף ב־(*) וחילוק ב־λ, ניתן להציג את v כצירוף לינארי של $v_1,\dots,v_n$. בכך הוכחנו כי כל וקטור ב־V שייך ל־B', כלומר K פורשת את V.

ד. נוכיח שכל קבוצה K הפורשת את V ומכילה בדיוק n וקטורים, היא בלתי תלויה וממילא היא בסיס. אכן, אילו הייתה קבוצה K בת n וקטורים הפורשת את V ושהיא תלויה לינארית, הרי על פי שאלה 8.1.7 הייתה קיימת קבוצה T, חלקית ממש ל־K, המקיימת $B=\{v_1,\dots,v_n\}$. זו הייתה קבוצה בעלת פחות מ־n וקטורים הפורשת את V, בניגוד לחלק ב של המשפט.

ה. כל בסיס ל־V הוא קבוצה בלתי תלויה, ולכן לפי חלק א יש בו לכל היותר n איברים. אך כל בסיס פורש את המרחב, לכן לפי חלק ב יש בו לכל הפחות n איברים.

תשובה 8.3.3 **השאלה בעמוד 261**

א. יהי $u+w$ וקטור כלשהו ב־$U+W$ (כלומר $u\in W$ ו־$w\in W$).

כיוון ש־$\{v_1,\dots,v_k,u_1,\dots,u_m\}$ בסיס של U, יש סקלרים $\alpha_1,\dots,\alpha_k,\beta_1,\dots,\beta_m$ כך ש־

$$u=\alpha_1v_1+\ldots+\alpha_kv_k+\beta_1u_1+\ldots+\beta_mu_m$$

כיוון ש־$\{v_1,\dots,v_k,w_1,\dots,w_n\}$ בסיס של W, נובע שיש סקלרים $\gamma_1,\dots,\gamma_k,\varepsilon_1,\dots,\varepsilon_n$ כך ש־

$$w=\gamma_1v_1+\ldots+\gamma_kv_k+\varepsilon_1w_1+\ldots+\varepsilon_nw_n$$

ולכן נוכל לרשום:

$$\begin{aligned}u+w&=\alpha_1v_1+\ldots+\alpha_kv_k+\beta_1u_1+\ldots+\beta_mu_m\\&\quad+\gamma_1v_1+\ldots+\gamma_kv_k+\varepsilon_1w_1+\ldots+\varepsilon_nw_n\\&=(\alpha_1+\gamma_1)v_1+\ldots+(\alpha_k+\gamma_k)v_k\\&\quad+\beta_1u_1+\ldots+\beta_mu_m+\varepsilon_1w_1+\ldots+\varepsilon_nw_n\end{aligned}$$

בכך הצגנו את $u + w$ כצירוף לינארי של איברי

$$v_1,\dots,v_k\,,\, u_1,\dots,u_m\,,\, w_1,\dots,w_n$$

ולכן קבוצה זו פורשת את $U + W$.

ב. במקרה זה, $u_1,\dots,u_m$ ו־ $w_1,\dots,w_n$ יהיו בסיסים של U ו־ W בהתאמה.
את $v_1,\dots,v_k$ נשמיט לחלוטין - שאר ההוכחה "תפעל" באופן זהה.

תשובה 8.3.4 **השאלה בעמוד 262**

כיוון ראשון:

נניח כי $V = U \oplus W$. אז $U \cap W = \{0\}$

ולכן:

$$\dim(U \cap W) = 0$$

לפי משפט 8.3.6:

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

$$= \dim U + \dim W + 0 = \dim U + \dim V$$

כיוון שני:

נניח כעת כי $\dim V = \dim U + \dim W$

אז ממשפט 8.3.6 נובע כי:

$$\dim(U \cap W) = 0$$

אך רק למרחב הטריוויאלי יש ממד אפס, ולכן $U \cap W = \{0\}$.

היות שלפי הנתון $V = U + W$, נסיק כי $V = U \oplus W$ (על איזה משפט הסתמכנו?).

תשובה 8.3.5 **השאלה בעמוד 262**

עלינו להוכיח כי הקבוצה

$$K = \{(1,2,3,4,5),(0,0,2,1,4),(0,0,0,3,5)\}$$

מהווה בסיס למרחב:

$$M = \mathrm{Sp}\{(1,2,3,4,5),(0,0,2,1,4),(0,0,0,3,5),(0,0,0,0,0)\}$$

נוכיח ראשית כי K בלתי תלויה לינארית. אכן, אם

$$\alpha(1,2,3,4,5) + \beta(0,0,2,1,4) + \gamma(0,0,0,3,5) = (0,0,0,0,0)$$

אז α, β ו־ γ חייבים לקיים את מערכת המשוואות:

$$\begin{aligned}
\alpha &= 0\\
2\alpha &= 0\\
3\alpha + 2\beta &= 0\\
4\alpha + \beta + 3\gamma &= 0\\
5\alpha + 4\beta + 5\gamma &= 0
\end{aligned}$$

קל להיווכח כי הפתרון היחיד למערכת זו הוא $\alpha = \beta = \gamma = 0$.

לכן K בלתי תלויה לינארית.

כעת, מאחר שוקטור האפס הוא בוודאי צירוף לינארי (טריוויאלי) של איברי K, הרי ש־

$$M = \mathrm{Sp}\{K \cup \{0\}\} = \mathrm{Sp}(K)$$

ומכאן ש־ K פורשת את M.

K, אם כן, קבוצה בלתי תלויה לינארית הפורשת את מרחב השורות של המטריצה A, ולכן K היא בסיס למרחב זה.

תשובה 8.3.6 **השאלה בעמוד 262**

א. אם $\lambda_1 w_1 + \lambda_2 w_2 = 0$ היא הצגה של וקטור האפס כצירוף לא־טריוויאלי, אז $\lambda_1 \neq 0$ או $\lambda_2 \neq 0$.
לכן

$$w_1 = -\frac{\lambda_2}{\lambda_1} w_2$$

או:

$$w_2 = -\frac{\lambda_1}{\lambda_2} w_1$$

בכל מקרה, לפחות אחד הוקטורים הוא כפולה בסקלר של השני.
אך ברור כי שני הוקטורים $(3,-1,-2,2)$ ו־ $(1,2,-1,4)$ אינם פרופורציוניים, ולכן הקבוצה $\{w_1, w_2\}$ בלתי תלויה לינארית.

ב. נוסיף לקבוצה $\{w_1, w_2\}$ וקטורים מתוך הבסיס הסטנדרטי של $\mathbb{R}^4$, $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4\}$.

1. נוסיף את $\mathbf{e}_1$ ונראה אם הקבוצה $\{w_1, w_2, \mathbf{e}_1\}$ בלתי תלויה לינארית.
אם

$$\alpha(1,2,-1,4) + \beta(3,-1,-2,2) + \gamma(1,0,0,0) = (0,0,0,0)$$

אז:

$$\begin{aligned}
\alpha + 3\beta + \gamma &= 0 \\
2\alpha - \beta &= 0 \\
-\alpha - 2\beta &= 0 \\
4\alpha + 2\beta &= 0
\end{aligned}$$

קל לבדוק שהפתרון היחיד למערכת משוואות זו (במשתנים הממשיים α, β, γ) הוא הפתרון הטריוויאלי, ולכן הקבוצה $\{w_1, w_2, \mathbf{e}_1\}$ בלתי תלויה לינארית.

2. נוסיף את $\mathbf{e}_2$ ונבדוק אם הקבוצה $\{w_1, w_2, \mathbf{e}_1, \mathbf{e}_2\}$ בלתי תלויה לינארית.
אם

$$\alpha(1,2,-1,4) + \beta(3,-1,-2,2) + \gamma(1,0,0,0) + \delta(0,1,0,0) = (0,0,0,0)$$

אז:

$$\begin{aligned} \alpha + 3\beta + \gamma &= 0 \\ 2\alpha - \beta + \delta &= 0 \\ -\alpha - 2\beta &= 0 \\ 4\alpha + 2\beta &= 0 \end{aligned}$$

שוב, קל להראות שהפתרון היחיד למערכת משוואות זו הוא הפתרון הטריוויאלי, ולכן הקבוצה $\{w_1, w_2, \mathbf{e}_1, \mathbf{e}_2\}$ בלתי תלויה לינארית. כיוון שזוהי קבוצה בת ארבעה איברים ב־ $\mathbb{R}^4$, הרי שהיא מהווה בסיס ל־ $\mathbb{R}^4$.

תשובה 8.3.7 **השאלה בעמוד 262**

א. נוכיח כי הקבוצה $\{w_1, w_2, u_1\}$ היא בלתי תלויה לינארית.

אם

$$\alpha(1,1,0) + \beta(2,0,1) + \gamma(1,0,1) = (0,0,0)$$

אז:

$$\begin{aligned} \alpha + 2\beta + \gamma &= 0 \\ \alpha &= 0 \\ \beta + \gamma &= 0 \end{aligned}$$

וקל להיווכח כי הפתרון היחיד למערכת משוואות זו הוא $\alpha = \beta = \gamma = 0$, ולכן הקבוצה $\{w_1, w_2, u_1\}$ בלתי תלויה לינארית.

קיבלנו קבוצה בלתי תלויה בת שלושה וקטורים ב־ $\mathbb{R}^3$, ולכן היא בסיס ל־ $\mathbb{R}^3$.

ב. המרחב $W + U$ מכיל בתוכו את הקבוצה $B = \{w_1, w_2, u_1\}$.

לכן גם $\mathrm{Sp}(\{w_1, w_2, u_1\}) \subseteq W + U$, אבל מאחר ש־ B הוא בסיס של $\mathbb{R}^3$, נסיק כי $\mathbb{R}^3 \subseteq W + U$. אך ברור גם כי $W + U \subseteq \mathbb{R}^3$ ולכן $W + U = \mathbb{R}^3$.

ג. קל לוודא כי הוקטורים $(1,1,0)$ ו־ $(2,0,1)$ אינם פרופורציוניים, ולכן הקבוצה $\{(1,1,0),(2,0,1)\}$ אינה תלויה לינארית, ולכן:

$$\dim W = \dim \mathrm{Sp}\{(1,1,0),(2,0,1)\} = 2$$

באופן דומה, נסיק כי הקבוצה $\{(1,0,1),(-1,1,0)\}$ בלתי תלויה לינארית, ולכן:

$$\dim U = \dim \mathrm{Sp}\{(1,0,1),(-1,1,0)\} = 2$$

ד. $\mathbb{R}^3 = W + U$

ולכן

$$\dim(W + U) = \dim \mathbb{R}^3 = 3$$

אבל

$$\dim W + \dim U = 2 + 2 = 4$$

ולכן, על פי מסקנה 8.3.7, הסכום $W + U$ אינו סכום ישר.

תשובה 8.3.8 **השאלה בעמוד 263**

א. קל לוודא שאוסף $m \cdot n$ המטריצות $E^{(i,j)}$ המוגדרות על־ידי

$$\begin{array}{cc} & \begin{array}{ccccc} & & \text{עמודה } j & & \\ & & \downarrow & & \end{array} \\ E^{(i,j)} = & \begin{bmatrix} 0 & \dots & 0 & \dots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \dots & 1 & \dots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & 0 \end{bmatrix} \begin{array}{l} \\ \\ \leftarrow i \text{ שורה} \\ \\ \\ \end{array} \end{array}$$

מהווה בסיס ל־ $\mathbf{M}_{m\times n}^{\mathbb{R}}$. כדי להראות זאת, נבחין כי נוכל להציג כל מטריצה $A = [a_{ij}]$ מסדר $m \times n$ כך:

$$A = a_{11}E^{(1,1)} + a_{12}E^{(1,2)} + \dots + a_{1n}E^{(1,n)} + a_{21}E^{(2,1)} + \dots +$$
$$+ a_{2n}E^{(2,n)} + \dots + a_{m1}E^{(m,1)} + \dots + a_{mn}E^{(m,n)}$$

ולכן קבוצת המטריצות $\{E^{(i,j)}\}$ פורשת את $\mathbf{M}_{m\times n}^{\mathbb{R}}$.

השוויון

$$a_{11}E^{(1,1)} + \dots + a_{1n}E^{(1,n)} + \dots + a_{2n}E^{(2,n)} + \dots + a_{m1}E^{(m,1)} + \dots + a_{mn}E^{(m,n)} = 0$$

כאשר a_{ij} סקלרים, שקול לאור האמור להתאפסות המטריצה $[a_{ij}]$. לכן השוויון מתקיים אם ורק אם כל הסקלרים a_{ij} מתאפסים. נסיק שהקבוצה $\{E^{(i,j)}\}$ בלתי תלויה לינארית, ולכן מהווה בסיס למרחב. לפיכך:

$$\dim \mathbf{M}_{m\times n}^{\mathbb{R}} = m \cdot n$$

ב. לפי סעיף א נקבל כי:

$$\dim \mathbf{M}_{n\times n}^{\mathbb{R}} = m \cdot n = n^2$$

ג. n המטריצות $E^{(i,i)}$, $1 \le i \le n$, מהוות בסיס למרחב המטריצות האלכסוניות מסדר $n \times n$, שכן

$$\begin{bmatrix} a_{11} & 0 \\ 0 & a_{nn} \end{bmatrix} = a_{11}E^{(1,1)} + a_{22}E^{(2,2)} + \dots + a_{nn}E^{(n,n)}$$

ולכן קבוצה זו פורשת את מרחב המטריצות האלכסוניות. הקבוצה $\{E^{(i,i)}\}$ בלתי תלויה לינארית משום שהיא מוכלת בקבוצה הבלתי תלויה לינארית $\{E^{(i,j)}\}$.

ד. אם $A = [a_{ij}]$ היא מטריצה משולשית עילית, צורתה היא:

$$\begin{bmatrix} a_{11} & a_{12} & a_{1n} \\ \vdots & a_{22} & \ddots \\ 0 & & a_{nn} \end{bmatrix}$$

כלומר, $a_{ij} = 0$ לכל $i > j$.

קל לבדוק כי מטריצת האפס הינה משולשית וכי הסכום והכפל בסקלר של מטריצות משולשיות היא מטריצה משולשית, ולכן בפנינו אכן תת־מרחב.

נימוק דומה לנימוקים שהופיעו בסעיפים הקודמים מראה כי אוסף כל המטריצות המשולשיות $E^{(i,j)}$, שעבורן $i \le j$, מהווה בסיס לתת־מרחב דלעיל.

נותר לחשב כמה מטריצות כאלה יש. בסך הכול יש n^2 מטריצות מטיפוס $E^{(i,j)}$, מתוכן n הן מהטיפוס $E^{(i,j)}$, והשאר - בחצי מהן $j < i$, ובחצי השני $j > i$. לכן יש $\frac{n^2 - n}{2}$ מטריצות מהטיפוס $E^{(i,j)}$ שעבורן $j < i$, ויש $\frac{n^2 - n}{2} + n = \frac{n^2 + n}{2}$ מטריצות מהטיפוס $E^{(i,j)}$ שעבורן $i \le j$, ולכן הממד של מרחב זה הוא $\frac{n^2 + n}{2}$.

(שימו לב ש־ $\frac{n(n+1)}{2} = \frac{n^2 + n}{2}$, וכיוון ש־ n ו־ $n+1$ הם מספרים עוקבים, אחד מהם הוא זוגי ולכן $\frac{n^2 + n}{2}$ הוא מספר שלם.)

ה. מטריצה $A \in \mathbf{M}_{n\times n}^{\mathbb{R}}$ היא סימטרית אם ורק אם $a_{ij} = a_{ji}$ לכל $1 \le i, j \le n$. נגדיר לכל i ו־ j מטריצה $C^{(i,j)}$ על־ידי:

$$\begin{array}{cccccccc} & & & \text{עמודה } i & \text{עמודה } j & & & \\ & & & \downarrow & \downarrow & & & \\ C^{(i,j)} = & \left[\begin{array}{c} \\ \\ \\ \\ \end{array} \right. & \begin{array}{c} 0 \\ \cdots \\ \cdots \\ \\ \end{array} & \begin{array}{c} \vdots \\ \vdots \\ 1 \\ \vdots \end{array} & \begin{array}{c} \vdots \\ 1 \\ \vdots \\ \vdots \end{array} & \begin{array}{c} \\ \cdots \\ \cdots \\ 0 \end{array} & \left. \begin{array}{c} \\ \\ \\ \\ \end{array} \right] & \begin{array}{c} \\ \leftarrow i \quad \text{שורה} \\ \leftarrow j \quad \text{שורה} \\ \\ \end{array} \end{array}$$

כלומר, $C^{(i_0,j_0)} = [c_{ij}]$ מוגדרת על־ידי:

$$c_{ij} = \begin{cases} 1 & \text{אם } (i,j) = (i_0, j_0) \text{ או } (i,j) = (j_0, i_0) \\ 0 & \text{אחרת} \end{cases}$$

שימו לב שעבור $i = j$ נקבל $C^{(i,i)} = E^{(i,i)}$, ועבור $i \ne j$ נקבל $C^{(i,j)} = E^{(i,j)} + E^{(j,i)}$.

קל להיווכח כי $C^{(i,j)} = C^{(j,i)}$, וכי אוסף כל המטריצות הסימטריות מהטיפוס $C^{(i,j)}$ כאשר $i \le j$, מהווה בסיס למרחב המטריצות הסימטריות $S^{\mathbb{R}}_{n\times n}$, ולכן ממד מרחב זה הוא $\frac{n^2+n}{2}$ (ראו חישוב בסעיף ד).

ו. מטריצה $A \in \mathbf{M}^{\mathbb{R}}_{n\times n}$ היא אנטי־סימטרית אם ורק אם $a_{ij} = -a_{ji}$ לכל $1 \le i,j \le n$.
כבר ראינו כי $A^{\mathbb{R}}_{n\times n}$ – אוסף המטריצות האנטי־סימטריות מסדר n – הוא תת־מרחב של $\mathbf{M}^{\mathbb{R}}_{n\times n}$, וכי

$$\mathbf{M}^{\mathbb{R}}_{n\times n} = S^{\mathbb{R}}_{n\times n} \oplus A^{\mathbb{R}}_{n\times n}$$

ולכן

$$\dim \mathbf{M}^{\mathbb{R}}_{n\times n} = \dim S^{\mathbb{R}}_{n\times n} + \dim A^{\mathbb{R}}_{n\times n}$$

(על איזו תוצאה הסתמכנו?), כלומר

$$n^2 = \frac{n^2+n}{2} + \dim A^{\mathbb{R}}_{n\times n}$$

ולכן:

$$\dim A^{\mathbb{R}}_{n\times n} = n^2 - \frac{n^2+n}{2} = \frac{n^2-n}{2}$$

תשובה 8.3.9 **השאלה בעמוד 263**

כבר ראינו (דוגמה ב לאחר הגדרה 8.2.1) כי הקבוצה $\{1,x,x^2,\dots,x^{n-1}\}$ מהווה בסיס ל־$F_n[x]$, ומכיוון שבקבוצה זו n איברים, נובע כי:

$$\dim F_n[x] = n$$

תשובה 8.3.10 **השאלה בעמוד 263**

לכל פולינום $P(x) = a_0 + \dots + a_k x^k$ ב־$\mathbb{R}_n[x]$, המתאפס ב־$x=0$, מתקיים $a_0 = 0$, שכן $P(0) = a_0$. לפיכך כל פולינום כזה הוא צירוף לינארי של איברי הקבוצה $\{x,x^2,\dots,x^{n-1}\}$, ולכן קבוצה זו פורשת את המרחב הנדון. מובן גם שהקבוצה היא בלתי תלויה (נמקו!), ולכן היא בסיס למרחב הנדון וממילא ממדו הוא $n-1$.

תשובה 8.3.11 **השאלה בעמוד 263**

א. נגדיר את הוקטורים $u_1,\dots,u_{n-1}$ כלהלן:

$$\begin{aligned}
u_1 &= (1,0,0,\dots,0,-1)\\
u_2 &= (0,1,0,\dots,0,-1)\\
&\vdots\\
u_{n-1} &= (0,0,0,\dots,0,1,-1)
\end{aligned}$$

יהי $u = (a_1,\dots,a_n)$ וקטור כלשהו ב־U.

אז

$$\sum_{i=1}^{n} a_i = 0$$

כלומר

$$a_n = -\sum_{i=1}^{n-1} a_i$$

ולכן נוכל להציג את u באופן הבא:

$$\begin{aligned} u &= (a_1,0,\dots,0,0) + (0,a_2,0,\dots,0,0) + \dots + (0,0,\dots,a_{n-1},0) + (0,0,\dots,-a_1 - \dots - a_{n-1}) \\ &= (a_1,0,\dots,0,-a_1) + (0,a_2,0,\dots,0,-a_2) + \dots + (0,0,\dots,a_{n-1},-a_{n-1}) \\ &= \sum_{i=1}^{n-1} a_i u_i \end{aligned}$$

ולכן $\{u_1,\dots,u_{n-1}\}$ פורשת את U.

נראה עתה שקבוצה זו היא בלתי תלויה לינארית.

אם

$$\sum_{i=1}^{n-1} \alpha_i u_i = 0$$

כאשר $a_1,\dots,a_{n-1}$ סקלרים, אז

$$\begin{array}{lllll} a_1 & & & & = 0 \\ & a_2 & & & = 0 \\ & & & a_{n-1} & = 0 \\ -a_1 & -a_2 & -\dots- & a_{n-1} & = 0 \end{array}$$

ומכאן קל לראות כי בהכרח $a_1 = \dots = a_{n-1} = 0$.

אם כן, הקבוצה $\{u_1,\dots,u_{n-1}\}$ היא בסיס למרחב U וממילא:

$$\dim U = n-1$$

ב. נבחר כ־ W את המרחב הנפרש על־ידי $\mathbf{e}_n$:

נראה כי:

$$\mathbb{R}^n = U \oplus W$$

יהי $\mathbf{b} = (b_1,\dots,b_n)$ וקטור כלשהו ב־ $\mathbb{R}^n$. נוכל להציג את $\mathbf{b}$ כך:

$$\begin{aligned} \mathbf{b} &= \left(b_1,\dots,b_{n-1},-\sum_{i=1}^{n-1} b_i\right) + \left(0,\dots,0,\sum_{i=1}^{n} b_i\right) \\ &= \sum_{i=1}^{n-1} b_i u_i + \left[\sum_{i=1}^{n} b_i\right] \cdot (0,0,\dots,0,1) = \\ &= b_1 u_1 + \dots + b_{n-1} u_{n-1} + \left(\sum_{i=1}^{n-1} b_i\right) \cdot \mathbf{e}_n \end{aligned}$$

שימו לב ש־ $b_1u_1+\ldots+b_{n-1}u_{n-1}$ הוא איבר של U, ו־ $\left(\sum_{i=1}^{n-1} b_i\right)\cdot e_n$ הוא איבר של $W=\mathrm{Sp}(\{\mathbf{e}_n\})$, כלומר הצגנו את $\mathbf{b}$ כסכום של וקטור ב־ U ווקטור ב־ W, ולכן $\mathbf{b}\in U+W$.
נסיק כי $\mathbb{R}^n\subseteq U+W$.

מאידך גיסא, ברור כי $U+W\subseteq\mathbb{R}^n$ ולכן:

$$\mathbb{R}^n=U+W$$

כדי להראות ש־ $\mathbb{R}^n=U\oplus W$, מספיק כעת שנראה כי $U\cap W=\{0\}$.
ברור כי $\{0\}\subseteq U\cap W$, ועלינו להראות רק כי החיתוך אינו מכיל שום וקטור פרט לוקטור האפס. ואמנם, אם

$$(a_1,\ldots,a_n)\in U\cap W$$

אז מכך ש־ $(a_1,\ldots,a_n)\in W$ נובע כי

$$a_1=\ldots=a_{n-1}=0$$

ומכך ש־ $(a_1,\ldots,a_n)\in U$ נובע כי

$$a_n=-a_1-a_2-\ldots-a_{n-1}=0$$

ולכן:

$$(a_1,\ldots,a_n)=(0,\ldots,0)$$

נסיק כי:

$$n=\dim\mathbb{R}^n=\dim U+\dim W$$

מאחר שראינו כי $\dim U=n-1$, נובע כי:

$$\dim W=1$$

(כמובן, אפשר להגיע למסקנה זו גם ישירות מהגדרת W.)

תשובה 8.4.1 **השאלה בעמוד 266**

א. ראשית נוכיח שקבוצת המטריצות הנתונה, B, היא בלתי תלויה ליניארית.
לשם כך נתבונן בצירוף ליניארי של איברי B ששווה למטריצת האפס:

$$\lambda_1\begin{bmatrix}1&2\\0&0\end{bmatrix}+\lambda_2\begin{bmatrix}1&0\\2&1\end{bmatrix}+\lambda_3\begin{bmatrix}0&1\\1&0\end{bmatrix}+\lambda_4\begin{bmatrix}0&0\\0&1\end{bmatrix}=\begin{bmatrix}0&0\\0&0\end{bmatrix}\qquad(*)$$

או:

$$\begin{bmatrix}\lambda_1+\lambda_2&2\lambda_1+\lambda_3\\2\lambda_2+\lambda_3&\lambda_2+\lambda_4\end{bmatrix}=\begin{bmatrix}0&0\\0&0\end{bmatrix}$$

השוויון האחרון שקול לארבע המשוואות:

$$\lambda_1 + \lambda_2 = 0$$

$$2\lambda_1 + \lambda_3 = 0$$

$$2\lambda_2 + \lambda_3 = 0$$

$$\lambda_2 + \lambda_4 = 0$$

למערכת זו פתרון יחיד והוא הפתרון הטריוויאלי (בדקו!).

הוכחנו אפוא שמן השוויון (*) נובע בהכרח כי

$$\lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = 0$$

ולכן B בלתי תלויה לינארית.

עתה, מכך ש־ B קבוצה בלתי תלויה במרחב שממדו 4, נובע כי B היא בסיס למרחב זה.

ב. 1. עלינו למצוא סקלרים $\lambda_1,\dots,\lambda_4 \in \mathbb{R}$ שעבורם יתקיים:

$$M_1 = \begin{bmatrix} 1 & 7 \\ 1 & -1 \end{bmatrix} = \lambda_1 \begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix} + \lambda_2 \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} + \lambda_3 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \lambda_4 \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} \lambda_1 + \lambda_2 & 2\lambda_1 + \lambda_3 \\ 2\lambda_2 + \lambda_3 & \lambda_2 + \lambda_4 \end{bmatrix}$$

שוויון זה יתקיים אם ורק אם:

$$\lambda_1 + \lambda_2 = 1$$

$$2\lambda_1 + \lambda_3 = 7$$

$$2\lambda_2 + \lambda_3 = 1$$

$$\lambda_2 + \lambda_4 = -1$$

הפתרון (היחיד) של המערכת הוא $(2,-1,3,0)$ ולכן:

$$[M_1]_B = \begin{bmatrix} 2 \\ -1 \\ 3 \\ 0 \end{bmatrix}$$

2. באופן דומה, בהציגנו את המטריצה M_2 כצירוף לינארי של איברי B, נגיע לשוויון

$$M_1 = \begin{bmatrix} 3 & 3 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} \lambda_1 + \lambda_2 & 2\lambda_1 + \lambda_3 \\ 2\lambda_2 + \lambda_3 & \lambda_2 + \lambda_4 \end{bmatrix}$$

או:

$$\lambda_1 + \lambda_2 = 3$$

$$2\lambda_1 + \lambda_3 = 3$$

$$2\lambda_2 + \lambda_3 = 1$$

$$\lambda_2 + \lambda_4 = -1$$

למערכת זו יש פתרון יחיד והוא $(2,1,-1,-2)$ ולכן:

$$[M_2]_B = \begin{bmatrix} 2 \\ 1 \\ -1 \\ -2 \end{bmatrix}$$

תשובה 8.4.2 **השאלה בעמוד 266**

א. הקבוצה מכילה ארבעה איברים והממד של $\mathbb{R}_4[x]$ אף הוא שווה ל־ 4. לכן די להראות שהקבוצה הנתונה בלתי תלויה לינארית.

השוויון

$$\lambda_1(1+x) + \lambda_2(x+x^2) + \lambda_3(x^2+x^3) + \lambda_4 2x^3 = 0$$

כאשר $\lambda_1,\ldots\lambda_4 \in \mathbb{R}$, שקול לשוויון:

$$\lambda_1 + (\lambda_1+\lambda_2)x + (\lambda_2+\lambda_3)x^2 + (\lambda_3+2\lambda_4)x^3 = 0$$

על־ידי השוואת מקדמים נקבל:

$$\lambda_1 = 0$$

$$\lambda_1 + \lambda_2 = 0$$

$$\lambda_2 + \lambda_3 = 0$$

$$\lambda_3 + 2\lambda_4 = 0$$

למערכת זו פתרון טריוויאלי בלבד (בדקו!), ולכן הקבוצה הנתונה בלתי תלויה לינארית ומהווה, אם כן, בסיס ל־ $\mathbb{R}_4[x]$.

ב. עלינו למצוא סקלרים $\lambda_1,\ldots\lambda_4 \in \mathbb{R}$ כך ש־

$$3 + 2x + x^2 + 2x^3 = \lambda_1(1+x) + \lambda_2(x+x^2) + \lambda_3(x^2+x^3) + (\lambda_3+2\lambda_4)x^3$$

כלומר:

$$3 + 2x + x^2 + 2x^3 = \lambda_1 + (\lambda_1+\lambda_2)x + (\lambda_2+\lambda_3)x^2 + (\lambda_3+2\lambda_4)x^3$$

או:

$$\lambda_1 = 3$$
$$\lambda_1 + \lambda_2 = 2$$
$$\lambda_2 + \lambda_3 = 1$$
$$\lambda_3 + 2\lambda_4 = 2$$

הפתרון (היחיד) למערכת זו הוא $(3,-1,2,0)$, ולכן וקטור הקואורדינטות של $P(x)$ לפי הבסיס הנתון הוא:

$$\begin{bmatrix} 3 \\ -1 \\ 2 \\ 0 \end{bmatrix}$$

תשובה 8.4.3 **השאלה בעמוד 267**

אם $\mathbf{a} = (a_1,\ldots,a_n)$ וקטור במרחב, אז

$$\mathbf{a} = a_0\mathbf{e}_1 + a_2\mathbf{e}_2 + \ldots + a_n\mathbf{e}_n$$

ולכן:

$$[\mathbf{a}]_E = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$$

מסקנה

וקטור הקואורדינטות של הוקטור $\mathbf{a}$ לפי הבסיס הסטנדרטי הוא $\mathbf{a}$ עצמו, כאשר רכיביו רשומים בעמודה.

תשובה 8.4.4 **השאלה בעמוד 268**

יהיו $v \in V$ ו־ $\lambda \in F$, ויהי $B = (v_1,\ldots,v_n)$ בסיס סדור של V.

אם

$$v = \sum_{i=1}^{n} a_i v_i$$

כאשר $a_1,\ldots,a_n \in F$, אז:

$$\lambda v = \lambda\sum_{i=1}^{n} a_i v_i = \sum_{i=1}^{n} (\lambda a_i) v_i$$

לפיכך

$$[v]_B = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$$

וכן

$$[\lambda v]_B = \begin{bmatrix} \lambda a_1 \\ \vdots \\ \lambda a_n \end{bmatrix} = \lambda \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$$

ולכן

$$[\lambda v]_B = \lambda [v]_B$$

כנדרש.

תשובה 8.4.5 **השאלה בעמוד 269**

א. יהי $B = (v_1, \ldots, v_n)$ בסיס סדור של V. אזי:

$$0 = 0v_1 + \ldots + 0v_n$$

ולכן:

$$[v]_B = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

ב. יהי $v \in V$.

אם

$$v = \sum_{i=1}^{n} \lambda_i v_i$$

אז

$$-v = (-1)v = (-1) \cdot \sum_{i=1}^{n} \lambda_i v_i = \sum_{i=1}^{n} (-\lambda_i) v_i$$

ומכאן:

$$[-v]_B = \begin{bmatrix} -\lambda_1 \\ \vdots \\ -\lambda_n \end{bmatrix} = (-1) \begin{bmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{bmatrix} = -[v]_B$$

תשובה 8.4.6 **השאלה בעמוד 269**

עבור $m = 1$, כבר ראינו בשאלה 8.4.4 כי לכל $u_1 \in V$ ולכל $\lambda_1 \in F$:

$$[\lambda_1 u_1]_B = \lambda_k [u_k]_B$$

נניח באינדוקציה שהלמה נכונה עבור $m = k$, כלומר נניח שלכל $u_1, \ldots, u_k \in V$ ולכל $\lambda_1, \ldots, \lambda_k \in F$ מתקיים:

$$[\lambda_1 u_1 + \ldots + \lambda_k u_k]_B = \lambda_1 [u_1]_B + \ldots + \lambda_k [u_k]_B$$

נוכיח כי עבור כל $k+1$ וקטורים $u_1, \ldots, u_{k+1}$ וכל $k+1$ סקלרים $\lambda_1, \ldots, \lambda_{k+1}$ ב־ F מתקיים:

$$[\lambda_1 u_1 + \ldots + \lambda_{k+1} u_{k+1}]_B = \lambda_1 [u_1]_B + \ldots + \lambda_{k+1} [u_{k+1}]_B$$

נסמן

$$u = \sum_{i=1}^{k} \lambda_i u_i$$

ואז נקבל (נמקו את כל המעברים!):

$$[\lambda_1 u_1 + \ldots + \lambda_{k+1} u_{k+1}]_B = [u + \lambda_{k+1} u_{k+1}]_B$$

$$= [u]_B + [\lambda_{k+1} u_{k+1}]_B = [u]_B + \lambda_{k+1} [u_{k+1}]_B$$

$$= \lambda_1 [u_1]_B + \ldots + \lambda_k [u_k]_B + \lambda_{k+1} [u_{k+1}]_B$$

בכך הוכחנו את הטענה.

תשובה 8.4.7 **השאלה בעמוד 269**

כיוון ראשון:

נניח כי הוקטורים $u_1,\ldots,u_m$ תלויים לינארית ב־ V.

פירוש הדבר שקיימים סקלרים $\lambda_1,\ldots,\lambda_m$ (שאינם כולם אפסים) כך ש־

$$\sum_{k=1}^{m} \lambda_k u_k = 0$$

מכאן נקבל על פי למה 8.4.3, כי:

$$\sum_{k=1}^{m} \lambda_k [u_k]_B = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

מאחר שלא כל מקדמי הצירוף שווים לאפס, נסיק מן השוויון האחרון תלות לינארית בין הוקטורים $[u_1]_B,\ldots,[u_m]_B$ ב־ F^n.

כיוון שני:

אם $[u_1]_B,\ldots,[u_m]_B$ תלויים לינארית ב־ F^n, אז קיים צירוף לא־טריוויאלי.

פירוש הדבר שקיימים סקלרים $\lambda_1,\ldots,\lambda_m$ שאינם כולם אפסים כך ש־

$$\sum_{k=1}^{m} \lambda_k [u_k]_B = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

ולכן, לפי למה 8.4.3

$$\left[\sum_{k=1}^{m} \lambda_k u_k\right]_B = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

ולכן כל הקואורדינטות של הוקטור $\sum \lambda_k u_k$ לפי הבסיס B הם אפסים.

נרשום $B=(v_1,\dots,v_m)$, ונקבל:

$$\sum_{k=1}^{m}\lambda_k u_k = 0v_1+\dots+0v_m = 0$$

מאחר שהצירוף איננו טריוויאלי, נובע מן השוויון האחרון כי הוקטורים $u_1,\dots,u_m$ תלויים לינארית ב־ V.

תשובה 8.4.8 **השאלה בעמוד 272**

א. נרשום את איברי הבסיס B' כצירופים לינאריים של איברי הבסיס B:

$$(3,2)=2.5(1,1)+0.5(1,-1)$$

$$(0,1)=0.5(1,1)+(-0.5)(1,-1)$$

(כיצד מצאנו את המקדמים?) לכן מטריצת המעבר מהבסיס B לבסיס B' היא:

$$\begin{bmatrix}2.5 & 0.5\\ 0.5 & -0.5\end{bmatrix}$$

ב. נתבונן במטריצה

$$M=\begin{bmatrix}1 & -1 & 2\\ 2 & 0 & 2\\ 1 & 1 & -1\end{bmatrix}$$

שעמודותיה הן וקטורי הקבוצה B'.

מאחר שהדטרמיננטה של M, $|M|$, אינה אפס:

$$|M|=-2\neq 0$$

(בדקו!) נקבל כי M הפיכה, ולכן קבוצת העמודות שלה היא בלתי תלויה לינארית ופורשת את $\mathbb{R}^3$, ומכאן ש־ B' בסיס ל־ $\mathbb{R}^3$.

מאחר שוקטור הקואורדינטות של וקטור מתוך $\mathbb{R}^3$ לפי הבסיס הסטנדרטי הוא הוקטור עצמו הרשום כעמודה, נקבל כי המטריצה M דלעיל היא מטריצת המעבר מ־ B ל־ B'.

ג. מטריצת המעבר M_1 מהבסיס B לבסיס B' היא, לפי ההגדרה:

$$M_1=\begin{bmatrix}2 & 0\\ 0 & 2\end{bmatrix}$$

נמצא עתה את מטריצת המעבר מ־ B' ל־ B.

נרשום את איברי הבסיס B כצירופים לינאריים של איברי הבסיס B':

$$(1,0)=0.5(2,0)+0(0,2)$$

$$(0,1)=0(2,0)+0.5(0,2)$$

ולכן מטריצת המעבר M_2, מ־ B' ל־ B, היא:

$$M_2 = \begin{bmatrix} 0.5 & 0 \\ 0 & 0.5 \end{bmatrix}$$

ד. מטריצת המעבר המבוקשת היא:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & 0 & \vdots \\ & & & & & 1 & 0 \\ 0 & 0 & 0 & & & 1 & 1 \end{bmatrix}$$

זוהי מטריצה משולשית תחתית ולכן הדטרמיננטה שלה שווה למכפלת איברי האלכסון הראשי, דהיינו שווה ל־1. מכאן נסיק שהמטריצה היא הפיכה ולכן הקבוצה B' היא אכן בסיס (על איזה משפט אנו מסתמכים?).

ה. הטענה נובעת משאלה 8.4.3.

תשובה 8.4.9 **השאלה בעמוד 272**

א. יהי $B = \{v_1,\dots,v_n\}$ הבסיס הנתון ותהי $M = [\mu_{ij}]_{n\times n}$ מטריצה הפיכה.
נתבונן ב־ n הוקטורים $u_1,\dots,u_n$ ב־ V המוגדרים על־ידי:

$$\begin{aligned} u_1 &= \mu_{11}v_1 + \mu_{21}v_2 + \dots + \mu_{n1}v_n \\ &\vdots \\ u_j &= \mu_{1j}v_1 + \mu_{2j}v_2 + \dots + \mu_{nj}v_n \\ &\vdots \\ u_n &= \mu_{1n}v_1 + \mu_{2n}v_2 + \dots + \mu_{nn}v_n \end{aligned}$$

הקבוצה $B' = (u_1,\dots,u_n)$ היא הבסיס המבוקש. עובדה זו נובעת ישירות מהגדרת מטריצת המעבר.

ב. 1. על־ידי חישוב ישיר מקבלים $|M| = 240 \neq 0$ (בדקו), ולכן M הפיכה.

2. אם $B' = (u_1,u_2,u_3,u_4)$ הוא הבסיס המבוקש, אז העמודה הראשונה של M היא וקטור הקואורדינטות $[u_1]_B$.
לכן:

$$u_1 = 1(1,0,0,0) + 0(1,1,0,0) + 2(1,1,1,0) + 0(1,1,1,1) = (3,2,2,0)$$

העמודה השנייה של M היא וקטור הקואורדינטות $[u_2]_B$.
לכן:

$$u_2 = 3(1,0,0,0) + 4(1,1,0,0) + 5(1,1,1,0) + 0(1,1,1,1) = (12,9,5,0)$$

באופן דומה נקבל כי:

$$u_3 = 0(1,0,0,0) + 0(1,1,0,0) + 6(1,1,1,0) + 0(1,1,1,1) = (6,6,6,0)$$

$$u_4 = 7(1,0,0,0) + 8(1,1,0,0) + 9(1,1,1,0) + 10(1,1,1,1) = (34,27,19,10)$$

ומכאן שהבסיס B' הוא:

$$B' = \big((3,2,2,0),(12,9,5,0),(6,6,6,0),(34,27,19,10)\big)$$

תשובה 8.4.10 **השאלה בעמוד 275**

אם M היא מטריצת המעבר מ־ B ל־ B', אז לכל $v \in V$ מתקיים:

$$[v]_B = M[v]_{B'}$$

B' הוא בסיס ולכן M היא מטריצה הפיכה.

נכפול אפוא את השוויון דלעיל במטריצה ההופכית M^{-1} ונקבל כי

$$[v]_{B'} = M^{-1}[v]_B$$

לכל $v \in V$. לכן נסיק ממשפט 8.4.8 כי M^{-1} היא מטריצת המעבר מ־ B' ל־ B.

תשובה 8.4.11 **השאלה בעמוד 275**

א. ישירות מן ההגדרה נקבל שמטריצת המעבר M מ־ B ל־ B' היא:

$$M = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 1 & \dots & 1 \\ 0 & 0 & 1 & \dots & 1 \\ \vdots & & 0 & \ddots & \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}$$ [1]

ב. נרשום את איברי B כצירופים ליניאריים של איברי B':

$$1 = 1 \cdot 1$$

$$x = (-1)1 + 1(1+x)$$

$$x^2 = (-1)(1+x) + (1+x+x^2)$$
$$\vdots$$
$$x^{n-1} = (-1)(1+x+\dots+x^{n-2}) + 1(1+x+\dots+x^{n-1})$$

1 שימו לב ש־ M היא מטריצה משולשית עילית, לכן הדטרמיננטה שלה שווה למכפלת איברי האלכסון וממילא שונה מאפס. לכן M הפיכה ו־ B' הוא אכן בסיס.

לכן מטריצת המעבר מ־ B' ל־ B היא:

$$\begin{bmatrix} 1 & -1 & 0 & 0 & \dots & 0 \\ 0 & 1 & -1 & 0 & \dots & \vdots \\ 0 & 0 & 1 & -1 & \dots & \\ \vdots & & & 1 & & \\ & & & & \ddots & -1 \\ 0 & & \dots & & 0 & 1 \end{bmatrix}$$

ג. ממשפט 8.4.2 נקבל שהמטריצה האחרונה היא המטריצה ההופכית M^{-1}.

תשובה 8.4.12 **השאלה בעמוד 276**

נרשום:

$$1 = 1 \cdot 1$$

$$x + \mu = \mu 1 + 1x$$

$$(x+\mu)^2 = \mu^2 1 + 2\mu x + 1x^2$$

$$\vdots$$

$$(x+\mu)^k = \mu^k + \binom{k}{1}\mu^{k-1}x + \binom{k}{2}\mu^{k-2}x^2 + \dots + 1x^k$$

$$\vdots$$

$$(x+\mu)^{n-1} = \mu^{n-1} + \binom{n-1}{1}\mu^{n-2}x + \dots + 1x^{n-1}$$

(השתמשנו בבינום של ניוטון.)

נתבונן במטריצה M שעמודותיה הן וקטורי הקואורדינטות של הפולינומים

$$1, x+\mu, \dots, (x+\mu)^{n-1}$$

לפי הבסיס הסדור:

$$B = (1, x, \dots, x^{n-1})$$

$$M = \begin{bmatrix} 1 & \mu & \mu^2 & \dots & \mu^k & \dots & \mu^{n-1} \\ 0 & 1 & 2\mu & \dots & \binom{k}{1}\mu^{k-1} & \dots & \binom{n-1}{1}\mu^{n-2} \\ 0 & 0 & 1 & & & & \\ & & 0 & & \ddots & & \vdots \\ \vdots & & & & & & \\ & & & & & \ddots & \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 \end{bmatrix}$$

M היא מטריצה משולשית עילית ולכן:

$$|M| = 1 \cdot 1 \dots 1 \neq 0$$

נסיק ש־ M הפיכה ולכן

$$B' = (1, x+\mu, \dots, (x+\mu)^{n-1})$$

בסיס.

תשובה 8.5.1 **השאלה בעמוד 277**

א. קבוצת שורותיה של המטריצה $0_{m\times n}$ מכילה את וקטור האפס בלבד.
לכן המרחב הנפרש על ידה הוא המרחב $\{0\}$.

ב. ההוכחה אנלוגית לסעיף א.

ג. לפי ההגדרה, $\dim\{0\} = 0$, ומכאן נכונות הטענה.

תשובה 8.5.2 **השאלה בעמוד 278**

$$A = \begin{bmatrix} 2 & -1 & 3 & -2 & 4 \\ 4 & -2 & 5 & 1 & 7 \\ 2 & -1 & 1 & 8 & 2 \end{bmatrix} \xrightarrow[R_2 \to R_2 - 2R_1]{R_3 \to R_3 - R_1} \begin{bmatrix} 2 & -1 & 3 & -2 & 4 \\ 0 & 0 & -1 & 5 & -1 \\ 0 & 0 & -2 & 10 & -2 \end{bmatrix}$$

$$(*) \qquad \xrightarrow{R_3 \to R_3 - 2R_2} \begin{bmatrix} 2 & -1 & 3 & -2 & 4 \\ 0 & 0 & -1 & 5 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

ממטריצת המדרגות $(*)$ אנו למדים שממד מרחב השורות הוא 2 ובסיס למרחב השורות הוא:

$$\{(2,-1,3,-2,4),(0,0,-1,5,-1)\}$$

נסיק שקבוצה זו היא בסיס גם למרחב השורות של A, ובפרט $\rho_R(A) = 2$.

תשובה 8.5.3 **השאלה בעמוד 279**

נדרג את המטריצה המשוחלפת:

$$A^t = \begin{bmatrix} 2 & 4 & 2 \\ -1 & -2 & -1 \\ 3 & 5 & 1 \\ -2 & 1 & 8 \\ 4 & 7 & 2 \end{bmatrix} \xrightarrow{R_1 \leftrightarrow R_2} \begin{bmatrix} -1 & -2 & -1 \\ 2 & 4 & 2 \\ 3 & 5 & 1 \\ -2 & 1 & 8 \\ 4 & 7 & 2 \end{bmatrix} \xrightarrow{\substack{R_2 \to R_2 + 2R_1 \\ R_3 \to R_3 + 3R_1 \\ R_4 \to R_4 - 2R_1 \\ R_5 \to R_5 + 4R_1}}$$

$$\begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 0 & -1 & -2 \\ 0 & 5 & 10 \\ 0 & -1 & -2 \end{bmatrix} \xrightarrow{R_2 \leftrightarrow R_5} \begin{bmatrix} -1 & -2 & -1 \\ 0 & -1 & -2 \\ 0 & -1 & -2 \\ 0 & 5 & 10 \\ 0 & 0 & 0 \end{bmatrix} \xrightarrow{\substack{R_3 \to R_3 - R_2 \\ R_4 \to R_4 + 5R_2}}$$

$$\begin{bmatrix} -1 & -2 & -1 \\ 0 & -1 & -2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

מהצורה המדורגת אנו רואים כי $\rho_R(A^t) = 2$, ומכאן שדרגת העמודות של A שווה ל־ 2,

$$\rho_C(A) = 2$$

ובסיס למרחב העמודות של A הוא:

$$\left\{\begin{bmatrix}-1\\-2\\-1\end{bmatrix},\begin{bmatrix}0\\-1\\-2\end{bmatrix}\right\}$$

תשובה 8.5.4 **השאלה בעמוד 281**

הטענה נובעת מכך שדרגת מטריצה היא דרגת שורותיה ואף דרגת עמודותיה:

$$\rho(A)=\rho_R(A)=\rho_C(A^t)=\rho(A^t)$$

תשובה 8.5.5 **השאלה בעמוד 281**

$$\rho(A)=\rho_R(A)$$

אולם הממד של מרחב השורות אינו עולה על מספר השורות ב־ A. כלומר:

$$\rho(A)=\rho_R(A)\le m$$

ובאופן דומה:

$$\rho(A)=\rho_C(A)\le n$$

ומכאן ש־ $\rho(A)$ אינו עולה לא על m ולא על n. כלומר:

$$\rho(A)\le \min\{m,n\}$$

תשובה 8.5.6 **השאלה בעמוד 281**

עמודותיה של AB הם צירופים לינאריים של עמודות A. לכן, לפי למה 8.5.3, עמודותיה של AB מוכלות במרחב העמודות של A, ומכאן שמרחב העמודות של AB מוכל במרחב העמודות של A. לפיכך דרגת העמודות של AB קטנה מ־ או שווה לדרגת העמודות של A:

$$\rho_C(AB)\le \rho_C(A)$$

אולם דרגת העמודות היא גם הדרגה של המטריצה AB, ולכן

$$\rho(AB)\le\rho(A) \tag{1}$$

וזאת לכל שתי מטריצות (שעבורן מוגדרת המכפלה). ובפרט, עבור המטריצות A^t, B^t נקבל:

$$\rho(B^tA^t)\le\rho(B^t) \tag{2}$$

אולם $B^tA^t=(AB)^t$, ולכן על פי שאלה 8.5.4:

וכן

$$\begin{cases}\rho(B^tA^t)=\rho((AB)^t)=\rho(AB)\\ \rho(B^t)=\rho(B)\end{cases} \tag{3}$$

אם נציב את (3) ב־(2) נקבל:

$$\rho(AB)\le\rho(B) \tag{4}$$

ועתה, מ־(1) ומ־(4) נובע כי:

$$\rho(AB) \le \min\{\rho(A), \rho(B)\}$$

תשובה 8.5.7 **השאלה בעמוד 281**

א. נניח כי

$$C = AB \qquad (1)$$

כאשר B היא מטריצה **הפיכה**. אזי מתקיים גם:

$$CB^{-1} = A \qquad (2)$$

מ־(1) נסיק כי[2]

$$\rho(AB) \le \min\{\rho(A), \rho(B)\}$$

ובפרט:

$$\rho(AB) \le \rho(A) \qquad (3)$$

מ־(2) נסיק כי

$$\rho(A) = \rho(CB^{-1}) \le \min\{\rho(C), \rho(B^{-1})\}$$

ובפרט:

$$\rho(A) \le \rho(C) = \rho(AB) \qquad (4)$$

ועתה, מ־(3) ומ־(4) נובע כי:

$$\rho(A) = \rho(AB)$$

ב. ההוכחה דומה.

תשובה 8.5.8 **השאלה בעמוד 282**

א. **כיוון ראשון:**

אם $\rho(A) = n$, הרי שהממד של מרחב השורות הוא n. אולם n השורות של A פורשות את מרחב שורותיה. לכן השורות של A פורשות את המרחב, ומספר שורותיה כממד המרחב. מכאן ששורות אלה בלתי תלויות לינארית. לכן המטריצה הפיכה, ובפרט:

$$|A| \ne 0$$

כיוון שני:

להפך, אם $|A| \ne 0$, אז A היא הפיכה ולכן שורותיה בלתי תלויות לינארית. כלומר, מרחב השורות של A נפרש על־ידי n וקטורים בלתי תלויים, ומכאן שממדו הוא n.

2 על פי שאלה 8.5.6.

מסקנה:

$$\rho(A) = n$$

ב. 1. אם $\rho(A) = m$, אז גם $\rho_R(A) = m$. כלומר, m השורות של A פורשות את מרחב השורות שממדו m. לכן הן בלתי תלויות לינארית.
להפך, אם שורות המטריצה הן בלתי תלויות לינארית, אז הן מהוות בסיס למרחב השורות (שכן הן גם פורשות אותו!) ומכאן שממדו הוא m. כלומר:

$$\rho(A) = m$$

השורות של A הן וקטורים ב־F^n (כאשר F השדה שמעליו מוגדרת המטריצה). לכן, אם הן בלתי תלויות, בהכרח מספרן m אינו עולה על n:

$$m \le n$$

2. ההוכחה דומה. הקשר בין m ו־n במקרה זה הוא:

$$m \ge n$$

תשובה 8.6.1 **השאלה בעמוד 284**

אם $\rho(A) = 0$, אז מרחב השורות של A הוא ממימד 0. כלומר, כל שורותיה של A הן שורות אפסים. או, במילים אחרות, A היא מטריצת האפס. כל n־יה $(x_1,\ldots,x_n)$ היא פתרון של המערכת

$$0\mathbf{x} = 0$$

ולכן מרחב הפתרונות הוא F^n כולו (כאשר F השדה שמעליו מוגדרת המטריצה). לכן, ממד מרחב הפתרונות הוא n. הוכחנו אפוא כי:

$$n - \underset{\overset{\|}{0}}{\rho(A)} = \underset{\overset{\|}{n}}{\dim P}$$

תשובה 8.6.2 **השאלה בעמוד 286**

יהיו

$$v_1 = (c_{11}, c_{21}, \ldots, c_{r1}, 1, 0, 0, \ldots, 0\}$$

$$v_2 = (c_{12}, c_{22}, \ldots, c_{r2}, 0, 1, 0, \ldots, 0\}$$

$$\vdots$$

$$v_{n-r} = (c_{1(n-r)}, \ldots, c_{r(n-r)}, 0, 0, 0, \ldots, 0, 1\}$$

$n-r$ הפתרונות הפרטיים. הצירוף הלינארי שלהם $\sum_{i=1}^{n-r} \lambda_i v_i$ ייראה כך:

$$\sum_{i=1}^{n-r} \lambda_i v_i = (*, *, \ldots, *, \lambda_1, \lambda_2, \ldots, \lambda_{n-r})$$ [3]

3 הכוכבים כאן מסמנים סקלרים כלשהם.

מכאן שאם

$$\sum_{i=1}^{n-r} \lambda_i v_i = (0,0,\ldots,0,0,0,\ldots,0)$$

אז בהכרח

$$\lambda_1 = \lambda_2 = \ldots = \lambda_{n-r} = 0$$

ולכן הוקטורים $v_1,\ldots,v_n$ בלתי תלויים לינארית.

תשובה 8.6.3 **השאלה בעמוד 286**

א. דירוג מראה כי המערכת הנתונה שקולה למערכת הבאה:

$$\begin{aligned} x_1 \quad + \frac{5}{2}x_3 &= 0 \\ x_2 + \frac{1}{2}x_3 &= 0 \end{aligned}$$

והפתרון הכללי שלה הוא:

$$v = \left(-\frac{5}{2}t, -\frac{1}{2}t, t\right)$$

או

$$v = t\left(-\frac{5}{2}, -\frac{1}{2}, 1\right)$$

כאשר t סקלר כלשהו. לכן מרחב הפתרונות הוא בעל ממד 1 ונפרש על־ידי $\left(-\frac{5}{2}, -\frac{1}{2}, 1\right)$:

(שימו לב שאכן מתקיים $\underset{3}{\underset{\|}{n}} - \underset{2}{\underset{\|}{\rho(A)}} = \underset{1}{\underset{\|}{\dim P}}$.)

$$P = \mathrm{Sp}\left\{\left(-\frac{5}{2}, -\frac{1}{2}, 1\right)\right\}$$

ב. דירוג מראה כי המערכת שקולה למערכת הבאה:

$$\begin{aligned} x_1 \quad + \frac{2}{11}x_3 - \frac{7}{11}x_4 &= 0 \\ x_2 + \frac{3}{11}x_3 + \frac{17}{11}x_4 &= 0 \end{aligned}$$

והפתרון הכללי שלה הוא:

$$v = \left(-\frac{2}{11}t + \frac{7}{11}s,\ -\frac{3}{11}t - \frac{17}{11}s,\ t,\ s\right)$$

נבחר $t = 1$, $s = 0$, ונקבל את הפתרון v_1:

$$v_1 = \left(-\frac{2}{11},\ \ -\frac{3}{11},\ \ 1,\ \ 0\right)$$

נבחר $t = 0$, $s = 1$, ונקבל את הפתרון v_2:

$$v_2 = \left(\frac{7}{11},\ \ -\frac{17}{11},\ \ 0,\ \ 1\right)$$

הוקטורים v_1, v_2 הם בסיס למרחב הפתרונות P. הם בלתי תלויים וכל פתרון v ניתן לכתיבה כך:[4]

$$v = tv_1 + sv_2$$

לכן:

$$P = \mathrm{Sp}\{v_1, v_2\}$$

תשובה 8.6.4 **השאלה בעמוד 287**

נחלק את התשובה לשלושה שלבים: בשלב א נדגים את התהליך במקרה פרטי; בשלב ב נתאר את התהליך במקרה הכללי, ולבסוף - בשלב ג - נוכיח שתהליך זה אכן משיג את המטרה.

א. יהיו נתונים ארבעה וקטורים ב- $\mathbb{R}^7$:

$$\mathbf{a}_1 = (0,5,-5,10,0,5,20)$$

$$\mathbf{a}_2 = (0,2,-2,5,4,7,10)$$

$$\mathbf{a}_3 = (0,2,-2,4,1,7,9)$$

$$\mathbf{a}_4 = (0,1,-1,2,0,1,5)$$

נערוך את השביעיות הללו במטריצה 4×7 ונדרג אותה.

$$\begin{bmatrix} 0 & 5 & -5 & 10 & 0 & 5 & 20 \\ 0 & 2 & -2 & 5 & 4 & 7 & 10 \\ 0 & 2 & -2 & 4 & 1 & 7 & 9 \\ 0 & 1 & -1 & 2 & 0 & 1 & 5 \end{bmatrix} \xrightarrow{R_1 \to \frac{1}{5}R_1}$$

$$\begin{bmatrix} 0 & 1 & -1 & 2 & 0 & 1 & 4 \\ 0 & 2 & -2 & 5 & 4 & 7 & 10 \\ 0 & 2 & -2 & 4 & 1 & 7 & 9 \\ 0 & 1 & -1 & 2 & 0 & 1 & 5 \end{bmatrix} \xrightarrow[R_4 \to R_4 - R_1]{\substack{R_2 \to R_2 - 2R_1 \\ R_3 \to R_3 - 2R_1}} \begin{bmatrix} 0 & 1 & -1 & 2 & 0 & 1 & 4 \\ 0 & 0 & 0 & 1 & 4 & 5 & 2 \\ 0 & 0 & 0 & 0 & 1 & 5 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

הגענו למטריצת מדרגות. האיברים הפותחים נמצאים בעמודות 2, 4, 5, 7. נוציא עתה מהבסיס הסטנדרטי של $\mathbb{R}^7$ את הוקטורים $\mathbf{e}_2, \mathbf{e}_4, \mathbf{e}_5, \mathbf{e}_7$ (ה"מתאימים" לעמודות המטריצה שבהן נמצאים האיברים הפותחים), ונתבונן ביתר וקטורי הבסיס הסטנדרטי שהם:

$$\mathbf{e}_1, \mathbf{e}_3, \mathbf{e}_6$$

4 ושוב נבדוק: $\underset{2}{\dim P} = \underset{4}{n} - \underset{2}{\rho(A)}$

טענה

הוקטורים $\mathbf{e}_1,\mathbf{e}_3,\mathbf{e}_6$ משלימים את הוקטורים הנתונים לבסיס של $\mathbb{R}^7$.

כדי לבדוק זאת נתבונן במטריצה ששורותיה הן:

$$\mathbf{e}_1,\mathbf{a}_1,\mathbf{e}_3,\mathbf{a}_2,\mathbf{a}_3,\mathbf{e}_6,\mathbf{a}_4 \qquad (*)$$

$$\begin{array}{c}\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & -5 & 10 & 0 & 5 & 20 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & -2 & 5 & 4 & 7 & 10 \\ 0 & 2 & -2 & 4 & 1 & 7 & 9 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & -1 & 2 & 0 & 1 & 5 \end{bmatrix}\end{array} \begin{array}{l} \leftarrow \mathbf{e}_1 \\ \leftarrow \mathbf{a}_1 \\ \leftarrow \mathbf{e}_3 \\ \leftarrow \mathbf{a}_2 \\ \leftarrow \mathbf{a}_3 \\ \leftarrow \mathbf{e}_6 \\ \leftarrow \mathbf{a}_4 \end{array}$$

על השורות 2, 4, 5 ו־7 של מטריצה זו (בשורות אלה רשומים הוקטורים הנתונים) נבצע את הפעולות האלמנטריות שביצענו על המטריצה המקורית ולא ניגע ביתר השורות. על־ידי כך נגיע למטריצה:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 2 & 0 & 1 & 4 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 4 & 5 & 2 \\ 0 & 0 & 0 & 0 & 1 & 5 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

המרחב הנפרש על־ידי וקטורי השורה הרשומים ב־$(*)$ הוא גם מרחב השורות של מטריצה זו, אולם מטריצה זו היא מטריצת מדרגות שאין בה שורת אפסים ולכן הממד של מרחב השורות שלה שווה ל־7. מכאן שקבוצת שורות המטריצה $(*)$ (המונה שבעה וקטורים) פורשת את $\mathbb{R}^7$ ולכן היא בסיס.

עתה נעבור לתיאור התהליך במקרה כללי.

ב. תהי

$$T=\{\mathbf{a}_1,\dots,\mathbf{a}_k\}$$

הקבוצה הנתונה.

נתבונן במטריצה A ששורותיה הן ה־ n ־יות $\mathbf{a}_1,\dots,\mathbf{a}_k$:

$$A=\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{k1} & \cdots & a_{kn} \end{bmatrix} \begin{array}{l} \leftarrow \mathbf{a}_1 \\ \quad \vdots \\ \leftarrow \mathbf{a}_k \end{array}$$

נשים לב שמן הנתון נובע כי $\rho(A)=k$.

נבצע עתה על שורותיה של A פעולות אלמנטריות ונביאה למטריצת מדרגות B.

מאחר ש־ $\rho(A)=k$, נובע כי גם $\rho(B)=k$, ולכן מספר האיברים הפותחים ב־ B שווה למספר שורותיה, k.

עתה, נוציא מן הבסיס הסטנדרטי של F^n את הוקטורים $\mathbf{e}_{j_1},\ldots,\mathbf{e}_{j_k}$ ה"מתאימים" לעמודות $j_1,\ldots,j_k$ שבהן נמצאים האיברים הפותחים $b_{1,j_1},\ldots,b_{k,j_k}$ של B, ונתבונן ביתר $n-k$ וקטורי הבסיס הסטנדרטי.

טענה

$n-k$ הוקטורים הנותרים הללו משלימים את הקבוצה $T=\{\mathbf{a}_1,\ldots,\mathbf{a}_k\}$ לבסיס.

ג. נוכיח את הטענה דלעיל.

$n-k$ הוקטורים הנותרים, שעליהם דובר לעיל, הם הוקטורים:

$$\mathbf{e}_1,\ldots,\mathbf{e}_{j_1-1} \;,\quad \mathbf{e}_{j_1+1},\ldots,\mathbf{e}_{j_2-1} \;,\quad \mathbf{e}_{j_2+1},\ldots,\mathbf{e}_{j_k-1} \;,\quad \mathbf{e}_{j_k+1},\ldots,\mathbf{e}_n$$

אנו טוענים שהקבוצה (1) דלהלן היא הבסיס המבוקש:

$$\left\{\mathbf{e}_1,\ldots,\mathbf{e}_{j_1-1},\mathbf{a}_1 \;,\quad \mathbf{e}_{j_1+1},\ldots,\mathbf{e}_{j_2-1},\mathbf{a}_2 \;,\quad \mathbf{e}_{j_2+1},\ldots,\mathbf{e}_{j_k-1},\mathbf{a}_k \;,\quad \mathbf{e}_{j_k+1},\ldots,\mathbf{e}_n\right\} \tag{1}$$

קבוצה זו מכילה n וקטורים. נרשום את רכיביהם בשורות מטריצה מסדר $n\times n$:

$$S=\begin{bmatrix} & & \\ & * & \\ & & \end{bmatrix}\begin{array}{l}\leftarrow \mathbf{e}_1\\ \vdots\\ \leftarrow \mathbf{e}_{j_1-1}\\ \leftarrow \mathbf{a}_1\\ \leftarrow \mathbf{e}_{j_1+1}\\ \vdots\\ \leftarrow \mathbf{e}_n\end{array}$$

השורות $j_1,\ldots,j_k$ של מטריצה זו יוצרות מטריצה A (שכן בשורות אלה רשומות ה־ k־יות $a_1,\ldots,a_k$). נבצע על שורות אלה את אותן הפעולות שבעזרתן הבאנו את A למטריצת המדרגות B. ביתר השורות לא ניגע. על־ידי כך נביא את המטריצה S לצורה:

$$\begin{bmatrix} 1 & & & & & & & & & & & & & & \\ & \ddots & & & & & & & & & & & & & \\ & & 1 & & & & & & & & & & & * & \\ & & & b_{1j_1} & & & & & & & & & & & \\ & & & & 1 & & & & & & & & & & \\ & & & & & \ddots & & & & & & & & & \\ & & & & & & 1 & & & & & & & & \\ & & & & & & & b_{2j_2} & & & & & & & \\ & & & & & & & & 1 & & & & & & \\ & & & & & & & & & \ddots & & & & & \\ & & & & & & & & & & 1 & & & & \\ & & 0 & & & & & & & & & b_{kj_k} & & & \\ & & & & & & & & & & & & 1 & & \\ & & & & & & & & & & & & & \ddots & \\ & & & & & & & & & & & & & & 1 \end{bmatrix}$$

מטריצה זו היא מטריצת מדרגות מסדר $n \times n$ שאין בה שורת אפסים, ולכן דרגתה היא n. לכן מתקיים גם:

$$\rho(S) = n$$

כלומר, n הוקטורים הרשומים ב־(1) הם $n \times n$ בלתי תלויים לינארית וממילא מהווים בסיס ל־ F^n.

תשובה 8.7.1 **השאלה בעמוד 288**

א. האיברים a,b תלויים לינארית - עדות לכך נותן הצירוף הלינארי הבא: $b \cdot a + (-a) \cdot b = ab - ab = 0$. כאן המקדמים הם (הסקלרים) $b,-a$, שאינם אפס. הקבוצה $\{a,b\}$ פורשת, שכן אפילו הקבוצה החלקית a פורשת. אכן, אם $\{c\}$ איבר שרירותי של F, אזי $c = a \cdot \frac{c}{a} \in Sp(\{a\})$.

ב. כאן הקבוצה $\{1,i\}$ אכן תלויה לינארית ופורשת, לאור הסעיף הקודם. מכיוון שהקבוצה תלויה לינארית, ממילא היא לא מהווה בסיס.

ג. הקבוצה $\{1,i\}$ בלתי תלויה לינארית מעל $\mathbb{R}$. אכן, אם a,b סקלרים ממשיים כך ש־ $a \cdot 1 + b \cdot i = a + ib = 0$, אזי $a = b = 0$. כמו כן, אם $z = a + bi$ מספר מרוכב שרירותי (כאשר a,b ממשיים), אזי $z = a + bi = a \cdot 1 + b \cdot i \in \mathrm{Sp}(\{1,i\})$, ולכן $\{1,i\}$ פורשת את כל $\mathbb{C}$. נסיק ש־ $\{1,i\}$ בסיס ל־ $\mathbb{C}$ כמרחב לינארי מעל $\mathbb{C}$.

ד. כידוע, לכל שדה F, הקבוצה $\{(1,0),(0,1)\}$ היא בסיס ל־ F^2 מעל F (זהו הבסיס הסטנדרטי), ובפרט נכון הדבר עבור $F = \mathbb{C}$.

ה. נתבונן בארבעת הוקטורים $\{(1,0),(0,1),(i,0),(0,i)\}$. תוכלו לוודא בנקל (בדומה לאופן שבו פעלנו בסעיף ג), שקבוצה זו פורשת את $\mathbb{C}^2$ ובלתי תלויה מעל $\mathbb{R}$, ולכן היא מהווה בסיס.

ו. לכל שדה F, הממד של F מעל F הוא 1, שכן כל איבר (שונה מאפס) של השדה מהווה בסיס. בפרט, הממד של $\mathbb{C}$ מעל $\mathbb{C}$ הוא 1.

ז. לאור סעיף ג, הממד הוא 2.

ח. לאור סעיף ג, הממד הוא 2.

ט. לאור סעיף ה, הממד הוא 4.

הגדרות ומשפטים בכרך ב

הגדרה 5.1.1 התחלקות

יהיו a,b מספרים שלמים.

אם קיים מספר שלם q כך ש־ $a = qb$, נאמר כי a **מתחלק ב־** b. על b נאמר במקרה זה שהוא **מחלק את** a, ונסמן $b|a$.

משפט 5.1.2 חילוק עם שארית

יהי a מספר **שלם** ויהי b מספר **טבעי**. קיים זוג יחיד (q,r) של מספרים שלמים, כך ש־

א. $a = qb + r$

ב. $0 \le r < b$

הגדרה 5.2.1

יהי n מספר טבעי, ויהיו a,b מספרים שלמים.

אם a ו־ b משאירים אותה שארית בחילוק ב־ n, נאמר כי a **קוֹנְגְרוּאֶנְטִי** (או **שקול**) **ל־** b **מודולו** n, ונרשום:

$$a \underset{\bmod n}{\equiv} b$$

כאשר a **אינו** שקול ל־ b מודולו n נרשום:

$$a \underset{\bmod n}{\not\equiv} b$$

טענה 5.2.2

יהי n מספר טבעי, ויהיו a,b מספרים שלמים.

$b \underset{\bmod n}{\equiv} a$ אם ורק אם $a-b$ מתחלק ב־ n.

משפט 5.2.3

יהי n מספר טבעי, ויהיו a,b,c,d מספרים שלמים.

אם

$$a \underset{\bmod n}{\equiv} c\ ,\quad b \underset{\bmod n}{\equiv} d$$

אז

$$(a+b) \underset{\bmod n}{\equiv} (c+d)$$

וכן:

$$ab \underset{\bmod n}{\equiv} cd$$

סימון 5.2.4

שארית החילוק של מספר שלם a במספר טבעי n תסומן $a_{\bmod n}$.

למה 5.2.5

אם b מתחלק ב־ n, אז $(a+b)_{\bmod n} = a_{\bmod n}$.

למה 5.2.6

יהיו: n מספר טבעי, a,b מספרים שלמים. אזי:

$$(a+b)_{\bmod n} = (a_{\bmod n} + b_{\bmod n})_{\bmod n}$$

וכן:

$$(a \cdot b)_{\bmod n} = (a_{\bmod n} \cdot b_{\bmod n})_{\bmod n}$$

הגדרה 5.2.7

יהי n מספר טבעי.

1. $(a+b)_{\bmod n}$ מכונה **הסכום מודולו** n **של** a **ו־** b;
   הפעולה על קבוצת המספרים השלמים $\mathbb{Z}$, המתאימה לכל $a,b \in \mathbb{Z}$ את סכומם מודולו n, נקראת **חיבור מודולו** n. היא תסומן $+_n$. אם כן:
   $$a +_n b := (a+b)_{\bmod n}$$
2. $(a \cdot b)_{\bmod n}$ מכונה **המכפלה מודולו** n **של** a **ו־** b;
   הפעולה על קבוצת המספרים השלמים $\mathbb{Z}$, המתאימה לכל $a,b \in \mathbb{Z}$ את מכפלתם מודולו n, נקראת **כפל מודולו** n. היא תסומן $\cdot_n$. אם כן:
   $$a \cdot_n b := (a \cdot b)_{\bmod n}$$

למה 5.2.8

יהי n מספר טבעי. פעולות החיבור והכפל מודולו n הן חילופיות וקיבוציות; כמו כן, הכפל מודולו n מתפלג מעל החיבור מודולו n.

מסקנה 5.2.9

הקבוצה $\mathbb{Z}_n$ **סגורה** ביחס לחיבור מודולו n וביחס לכפל מודולו n.

למה 5.2.10

בקבוצה $\mathbb{Z}_n$, המספר 0 הוא ניטרלי ביחס לחיבור מודולו n.

למה 5.2.11

יהי $n > 1$. ב־ $\mathbb{Z}_n$, המספר 1 הוא ניטרלי ביחס לכפל מודולו n.

למה 5.2.12

לכל איבר בקבוצה $\mathbb{Z}_n$ יש איבר נגדי ביחס לפעולת החיבור $+_n$.

הגדרה 5.3.1 מספר ראשוני

נאמר שמספר טבעי $n \geq 2$ הוא **ראשוני** אם המספרים הטבעיים היחידים המחלקים אותו הם 1 ו־ n. מספר טבעי $n \geq 2$ שאינו ראשוני (כלומר מספר שיש לו מחלק טבעי נוסף, פרט לעצמו ול־1), נקרא מספר **פריק**.

למה 5.3.2

כל מספר טבעי $n \geq 2$ מתחלק במספר ראשוני.

משפט 5.3.3

יש אינסוף מספרים ראשוניים.

למה 5.3.4

כל מספר טבעי $n \geq 2$ הוא ראשוני, או מכפלה של כמה מספרים ראשוניים.

משפט 5.3.5 המשפט היסודי של האריתמטיקה

כל מספר טבעי $n \geq 2$ ניתן להצגה **יחידה**, עד כדי סדר הגורמים, כמכפלה של מספרים ראשוניים.

מסקנה 5.3.6

יהי p מספר ראשוני. אם a,b מספרים טבעיים כך ש־$p|ab$, אזי בהכרח $p|a$ או $p|b$.

משפט 5.4.1

יהי $n \geq 2$ מספר טבעי. הקבוצה $\mathbb{Z}_n$, עם פעולות החיבור והכפל מודולו n, מהווה שדה אם ורק אם n הוא מספר ראשוני.

למה 5.4.2

תהי A קבוצה סופית, ותהי f פונקציה מ־A ל־A. אזי f חד־חד־ערכית אם ורק אם f על.

משפט 5.5.1

יהי $n \geq 2$ מספר טבעי. קיים שדה בן n איברים אם ורק אם n הוא **חזקה** של מספר ראשוני.

למה 5.6.1

לכל מספר שלם n השונה מאפס מתקיים:

א. $[n,1] = \{1\}$.

ב. $[n,n] = [n]$.

ג. $[n,m] = [m]$ לכל שלם m המחלק את n.

הגדרה 5.6.2 מחלק משותף מרבי

יהיו n,m מספרים שלמים שונים מאפס. למספר הגדול ביותר בקבוצה $[n,m]$ קוראים **המחלק המשותף המְרַבִּי** של n ו־m, ומסמנים אותו ב־$\gcd(n,m)$. כלומר, $\gcd(n,m)$ הוא המספר הטבעי הגדול ביותר המחלק גם את n וגם את m.

למה 5.6.3

לכל n שלם מתקיים:

א. $\gcd(n,1) = 1$.

ב. $\gcd(n,n) = n$.

ג. $\gcd(n,m) = |m|$ לכל שלם m המחלק את n.

טענה 5.6.4

יהי a מספר **שלם** ויהי b מספר **טבעי**. יהיו q,r זוג מספרים שלמים כך ש־ $a = bq + r$. אזי $\gcd(a,b) = \gcd(b,r)$.

טענה 5.6.5

יהיו a,b מספרים שלמים שונים מאפס. אז קיימים מספרים שלמים x,y כך ש־ $\gcd(a,b) = ax + by$. כלומר, ניתן להציג את המחלק המשותף המרבי $\gcd(a,b)$ כצירוף לינארי של a,b **במקדמים שלמים**.

הגדרה 6.1.1 תת־שדה

יהיו $(F,+_F,\cdot_F)$ ו־ $(K,+_K,\cdot_K)$ שדות. נאמר ש־ $(K,+_K,\cdot_K)$ הוא **תת־שדה** של $(F,+_F,\cdot_F)$, אם הקבוצה K היא תת־קבוצה של F, ואם הפעולות של השדות מתיישבות זו עם זו במובן הבא: לכל $x,y \in K$ מתקיים $x +_F y = x +_K y$ ו־ $x \cdot_F y = x \cdot_K y$.

הגדרה 6.1.2 שדה־הרחבה

נאמר ש־ F הוא **שדה־הרחבה** של K, אם K הוא תת־שדה של F.

טענה 6.1.3

יהי F שדה. אזי F הוא תת־שדה של F.

טענה 6.1.4

יהי F שדה ותהי K תת־קבוצה של F. אזי K תת־שדה של F אם ורק אם מתקיים:

א. K סגורה לגבי פעולות החיבור והכפל.

ב. K מכילה את 0, איבר האפס של F, ואת 1, איבר היחידה של F. יתר על כן, 0 הוא איבר האפס של K, ו־1 הוא איבר היחידה של K.

ג. לכל $x \in K$ מתקיים $-x \in K$.

ד. לכל $x \neq 0$ ב־ K מתקיים $x^{-1} \in K$.

משפט 6.1.5

לשדה המספרים הרציונליים $\mathbb{Q}$ אין תת־שדות פרט לעצמו.

משפט 6.1.6

יהי F שדה־הרחבה של $\mathbb{Q}$, ויהי K תת־שדה של F. אזי $\mathbb{Q} \subseteq K$.

טענה 6.1.7

נסמן ב־$\mathbb{Q}\left(\sqrt{2}\right)$ את אוסף המספרים הממשיים מהצורה $a + \sqrt{2}b$, כאשר $a,b \in \mathbb{Q}$. אזי $\mathbb{Q}\left(\sqrt{2}\right)$ הוא תת־שדה של $\mathbb{R}$.

טענה 6.2.1

יהי F שדה הרחבה של $\mathbb{R}$, ונניח כי קיים איבר $i \in F$ המקיים $i^2 = -1$. אזי $K = \{a + ib | a,b \in \mathbb{R}\}$ הוא תת־שדה של F.

הגדרה 6.2.2 שדה המספרים המרוכבים

נסמן ב־$\mathbb{C}$ את אוסף כל הביטויים מהצורה $a + ib$, כאשר a,b מספרים ממשיים. נגדיר על $\mathbb{C}$ פעולות חיבור $+_{\mathbb{C}}$ וכפל $\cdot_{\mathbb{C}}$, באופן הבא:

$$(a + ib) +_{\mathbb{C}} (c + id) = (a + c) + i(b + d)$$

$$(a + ib) \cdot_{\mathbb{C}} (c + id) = (ac - bd) + i(ad + bc)$$

לאיברי $\mathbb{C}$ נקרא **מספרים מרוכבים**.

טענה 6.2.3

הקבוצה $\mathbb{C}$, בצירוף זוג הפעולות שהגדרנו, מהווה שדה.

הגדרה 6.3.1

יהי $z = a + ib$ מספר מרוכב כלשהו, כאשר (a,b) מספרים ממשיים.

a נקרא **החלק הממשי** של z.

b נקרא **החלק המדומה** של z.

את החלק הממשי של z נסמן ב־$\operatorname{Re} z$.

את החלק המדומה של z נסמן ב־$\operatorname{Im} z$.

הגדרה 6.4.1

יהי $z = a + ib$ מספר מרוכב. **המספר הצמוד של** z, או בקיצור **הצמוד** של z, שסימונו $\bar{z}$, מוגדר על־ידי:

$$\bar{z} := a - ib$$

משפט 6.4.2 תכונות יסודיות של הצמוד

לכל $z, z_1, z_2 \in \mathbb{C}$ מתקיים:

א. $\bar{\bar{z}} = z$

ב. $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$

ג. $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$

ד. $z + \overline{z} = 2\operatorname{Re} z$

ה. $z - \overline{z} = 2i\operatorname{Im} z$

ו. $z = \overline{z}$ אם ורק אם z ממשי.

הגדרה 6.4.3

יהי $z = a + ib$ מספר מרוכב.

הערך המוחלט של z, שסימונו $|z|$, הוא המספר הממשי האי־שלילי המוגדר כך:

$$|z| \overset{\text{def}}{=} \sqrt{a^2 + b^2}$$

כלומר, $|z| = \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2}$.

משפט 6.4.4

לכל מספר מרוכב z מתקיים:

א. $|z| = |\overline{z}|$

ב. $z\overline{z} = |z|^2$

משפט 6.4.5 תכונות יסודיות של הערך המוחלט

יהיו z, z_1, z_2 מספרים מרוכבים. אזי:

א. $|z| \geq 0$

וכן, $|z| = 0$ אם ורק אם $z = 0$.

ב. $|z_1 z_2| = |z_1||z_2|$

ג. $|z_1 + z_2| \leq |z_1| + |z_2|$

ד. $|-z| = |z|$

טענה 6.4.6

לכל מספר מרוכב $z \neq 0$, מתקיים:

$$z^{-1} = \frac{\overline{z}}{|z|^2}$$

הגדרה 6.7.1 פולינום

יהי F שדה. פולינום מעל F במשתנה x (או בקצרה, **פולינום)** הוא **ביטוי** מהצורה

$$P(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

כאשר n הוא מספר שלם אי־שלילי, ו־ $a_0, \ldots, a_n$ הם סקלרים בשדה F. לסקלרים $a_0, \ldots, a_n$ קוראים **המקדמים** של הפולינום.

הגדרה 6.7.2 שוויון פולינומים

יהיו $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, $Q(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$ פולינומים מעל שדה F, ונניח ש־ $n \geq m$. נאמר שהפולינומים $P(x)$ ו־ $Q(x)$ **שווים**, ונסמן $P(x) = Q(x)$, אם מתקיים $a_i = b_i$ לכל $0 \leq i \leq n$, ו־ $b_i = 0$ לכל $n < i \leq m$.

אחרת נאמר שהפולינומים **שונים**. כלומר, שני פולינומים הם שווים אם כל המקדמים שלהם שווים (לפי הסדר), לאחר שהשמטנו אפסים "מיותרים".

הגדרה 6.7.3 מעלת פולינום

יהי $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ פולינום שאינו פולינום האפס.
לאינדקס המרבי k שעבורו $a_k \neq 0$ נקרא **מעלת הפולינום** (או **דרגת הפולינום**), ונסמנו $\deg P$. את מעלת פולינום האפס נגדיר להיות $\deg(0) \overset{\text{def}}{=} -\infty$.

סימון 6.7.4

נסמן את אוסף כל הפולינומים מעל שדה F במשתנה x ב־ $F[x]$.
אם n מספר טבעי, אז נסמן ב־ $F_n[x]$ את אוסף כל הפולינומים מעל F שמעלתם קטנה מ־n.

הגדרה 6.7.5 סכום פולינומים

יהיו $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, $Q(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m \in F[x]$, ונניח ש־ $m \geq n$ (תמיד נוכל להניח זאת, על־ידי הוספת מקדמי אפס, במידת הצורך). **הסכום** של $P(x)$ ו־ $Q(x)$ הוא הפולינום $(P+Q)(x)$ המוגדר על־ידי:

$$(P+Q)(x) \overset{\text{def}}{=} (a_0 + b_0) + (a_1 + b_1)x + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \ldots + b_mx^m$$

טענה 6.7.6

יהיו $P(x), Q(x)$ פולינומים מעל שדה F. אזי:

$$\deg(P+Q) \leq \max\{\deg P, \deg Q\}$$

הגדרה 6.7.7 כפל פולינומים

יהיו $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, $Q(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m \in F[x]$.
נגדיר את **המכפלה** $(P \cdot Q)(x)$ על־ידי:

$$(P \cdot Q)(x) = \sum_{\substack{0 \leq i \leq n \\ 0 \leq j \leq m}} a_i b_j x^{i+j}$$

טענה 6.7.8

א. כפל פולינומים הוא חילופי. כלומר, לכל זוג פולינומים P, Q מעל שדה נתון, $PQ = QP$.
ב. כפל פולינומים הוא קיבוצי. כלומר, לכל שלושה פולינומים P, Q, R מעל שדה נתון, $(PQ)R = P(QR)$.

ג. כפל פולינומים מתפלג מעל החיבור. כלומר, לכל שלושה פולינומים P, Q, R מעל שדה נתון, $P(Q+R) = PQ + PR$.

טענה 6.7.9

אם $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n,\ Q(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m \in F[x]$,
אז

$$(PQ)(x) = c_0 + c_1x + \ldots + c_{m+n}x^{m+n}$$

כאשר $c_k = \sum_{\substack{i+j=k \\ 0\le i\le n, 0\le j\le m}} a_ib_j$.

הגדרה 6.7.10 מקדם עליון; פולינום מתוקן

יהי $P(x) \in F[x]$ פולינום שונה מאפס, ונסמן $n = \deg P$.
במקרה זה נוכל לרשום $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, כאשר $a_n \neq 0$.
המקדם a_n נקרא **המקדם העליון** של $P(x)$, ונאמר ש־$P(x)$ הוא **פולינום מתוקן** אם המקדם העליון שלו הוא 1.

טענה 6.7.11

יהיו $P(x), Q(x)$ פולינומים מעל שדה F.

א. המקדם העליון של $P(x) \cdot Q(x)$ הוא מכפלת המקדמים העליונים של $P(x)$ ושל $Q(x)$.

ב. אם $P(x), Q(x)$ הם פולינומים מתוקנים, אזי גם $(PQ)(x)$ הוא מתוקן.

ג. מתקיים השוויון:

$$\deg(PQ) = \deg P + \deg Q$$

הגדרה 6.7.12 הצבה בפולינום

יהי $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in F[x]$ פולינום ויהי $\alpha \in F$ סקלר. נגדיר את **ההצבה** $P(\alpha)$ של a ב־P על־ידי:

$$P(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n$$

כלומר, $P(\alpha)$ הוא הסקלר המתקבל על־ידי החלפת כל מופע של x ב־$P(x)$ ב־α, וחישוב ערך הביטוי שהתקבל (בהתאם לפעולות בשדה).

טענה 6.7.13

יהיו $P(x), Q(x) \in F(x)$ פולינומים ויהי $\alpha \in F$ סקלר. אזי מתקיים:

א. $(P+Q)(\alpha) = P(\alpha) + Q(\alpha)$

ב. $(PQ)(\alpha) = P(\alpha)Q(\alpha)$

הגדרה 6.7.14 שורש של פולינום

יהי $P(x) \in F(x)$ פולינום ויהי $\alpha \in F$ סקלר. נאמר ש־α הוא **שורש** של P אם $P(\alpha) = 0$.

משפט 6.8.1 חילוק פולינומים עם שארית

יהיו $a(x),b(x)$ פולינומים מעל שדה F, כאשר $b(x)\neq 0$. קיים זוג יחיד $q(x),r(x)$ של פולינומים מעל F, כך ש־

א. $a(x)=q(x)b(x)+r(x)$

ב. $\deg(r(x))<\deg(b(x))$

למה 6.8.2

יהי $P(x)$ פולינום מעל שדה כלשהו F, ויהי $\alpha\in F$ סקלר. אזי α הוא שורש של $P(x)$ אם ורק אם $P(x)$ מתחלק בפולינום $x-\alpha$.

מסקנה 6.8.3

יהי $P(x)$ פולינום שונה מאפס ממעלה n, מעל שדה כלשהו F. אזי ל־ $P(x)$ יש לכל היותר n שורשים שונים ב־ F.

מסקנה 6.8.4

יהי F שדה אינסופי, ויהיו $P(x),Q(x)\in F[x]$ פולינומים כך ש־ $P(\alpha)=Q(\alpha)$ לכל $\alpha\in F$. אזי הפולינומים $P(x),Q(x)$ שווים זה לזה.

משפט 6.9.1 המשפט היסודי של האלגברה

יהי $P(x)$ פולינום ממשי/מרוכב ממעלה גדולה מאפס. אזי ל־ $P(x)$ יש שורש מרוכב.

למה 6.9.2

יהי $P(x)$ פולינום מעל שדה F ויהי k מספר טבעי. אזי $\deg(P^k(x))=k\deg(P(x))$.

למה 6.9.3

יהי $P(x)$ פולינום שונה מאפס מעל שדה F, ונניח ש־ $P(x)$ מתחלק בפולינום $Q(x)$. אזי $\deg\big(Q(x)\big)\leq\deg\big(P(x)\big)$.

למה 6.9.4

יהי $P(x)$ פולינום ממעלה חיובית מעל שדה F, ונניח ש־ $P(x)$ מתחלק בפולינום $(x-\alpha)^k$, כאשר $\alpha\in F$ סקלר ו־ k מספר טבעי. אזי $k\leq\deg\big(P(x)\big)$.

הגדרה 6.9.5 ריבוי של שורש של פולינום

יהי $P(x)$ פולינום ממעלה חיובית מעל שדה F, ויהי $\alpha\in F$ שורש של $P(x)$. **הריבוי** של השורש α בפולינום $P(x)$ הוא המספר הטבעי המרבי k שעבורו הפולינום $(x-\alpha)^k$ מחלק את $P(x)$.

למה 6.9.5

יהי $P(x)$ פולינום מעל שדה כלשהו F, ויהי $\alpha\in F$ שורש של $P(x)$. אזי הריבוי של α ב־ $P(x)$ הוא k אם ורק אם קיים פולינום $Q(x)$ כך ש־ $P(x)=(x-\alpha)^k Q(x)$ ו־ α אינו שורש של $Q(x)$.

טענה 6.9.6

יהי $P(x)$ פולינום שונה מאפס ממעלה n מעל שדה המספרים המרוכבים. אז ניתן לכתוב את $P(x)$ בצורה

$$P(x) = c(x-\alpha_1)\cdot(x-\alpha_2)\cdot\ldots\cdot(x-\alpha_n)$$

כאשר $\alpha_1, \alpha_2, \ldots, \alpha_n$ היא סדרת מספרים מרוכבים הכוללת את כל שורשי $P(x)$ (ייתכן שחלק מן השורשים מופיעים כמה פעמים), ו־c הוא המקדם העליון של $P(x)$ (אם $n=0$ אז לא מופיעים גורמים מהצורה $x-\alpha_i$ כלל).

משפט 6.9.7

יהי $P(x)$ פולינום שונה מאפס ממעלה n מעל שדה המספרים המרוכבים ויהיו $\alpha_1,\ldots,\alpha_m$ כל השורשים **השונים** של $P(x)$. אזי ניתן לכתוב את $P(x)$ בצורה הבאה

$$P(x) = c(x-\alpha_1)^{k_1}\cdot(x-\alpha_2)^{k_2}\cdot\ldots\cdot(x-\alpha_n)^{k_n}$$

כאשר c הוא המקדם העליון של $P(x)$, הריבוי של השורש α_i הוא k_i לכל $1 \le i \le m$, ומתקיים $n = k_1 + \ldots + k_m$.

טענה 6.10.1 הלמה של גאוס

יהי $P(x)$ פולינום מתוקן שכל מקדמיו הם מספרים שלמים. אם α שורש רציונלי של $P(x)$, אזי α הוא מספר שלם.

טענה 6.10.2

יהי $P(x)$ פולינום מתוקן שכל מקדמיו הם מספרים שלמים. אם α הוא שורש שלם של $P(x)$, אז α מחלק את המקדם החופשי של $P(x)$.

טענה 6.10.3

יהי $P(x)$ פולינום שמקדמיו שלמים. אם $\alpha = \frac{r}{s}$ הוא שורש של $P(x)$, כאשר r ו־s מספרים שלמים שונים מאפס וזרים, אזי r מחלק את המקדם החופשי של $P(x)$ ו־s מחלק את המקדם העליון של $P(x)$.

הגדרה 6.11.1 נגזרת של פולינום

יהי $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in F[x]$ פולינום מעל שדה F. **הנגזרת** של $P(x)$ היא הפולינום $a_1 + 2a_2x + 3a_3x^2 + \ldots + na_nx^{n-1}$. פולינום זה יסומן ב־$P'(x)$.

אפשר לרשום גם:

$$(a_0 + a_1x + a_2x^2 + \ldots + a_nx^n)' = a_1 + 2a_2x + 3a_3x^2 + \ldots + na_nx^{n-1}$$

טענה 6.11.2 נגזרת של סכום פולינומים

יהיו $P(x), Q(x)$ פולינומים. מתקיים השוויון: $\big(P(x)+Q(x)\big)' = P'(x) + Q'(x)$.

טענה 6.11.3

יהי $P(x) \in F[x]$ פולינום ויהי $c \in F$ סקלר. אזי $\left(cP(x)\right)' = cP'(x) \in F[x]$.

טענה 6.11.4

יהיו $P(x)Q(x)$ פולינומים כלשהם מעל שדה F. אזי:

$$\left(P(x)Q(x)\right)' = P'(x)Q(x) + P(x)Q'(x)$$

טענה 6.11.5

יהי $P(x) \in F[x]$ פולינום ויהי $\alpha \in F$ שורש של $P(x)$. אזי α הוא שורש פשוט של $P(x)$ אם ורק אם $P'(\alpha) \neq 0$, כלומר אם ורק אם α אינו שורש של $P'(x)$.

הגדרה 7.1.1 מרחב לינארי מעל שדה

יהי F שדה. קבוצה V, שעליה מוגדרת פעולת חיבור $+$ בין זוג איברים של V, וכן פעולת כפל בסקלר $\cdot$ בין איבר של V וסקלר מ־F, תיקרא **מרחב לינארי מעל** F, אם מתקיימות התכונות הבאות:

תכונות החיבור

א. **סגירות:** לכל $u,v \in V$, $\quad u + v \in V$

ב. **קיבוציות:** לכל $u,v,w \in V$, $\quad (u+v)+w = u+(v+w)$

ג. **חילופיות:** לכל $u,v \in V$, $\quad u+v = v+u$

ד. קיים ב־V **איבר ניטרלי** לגבי החיבור, שאותו נסמן ב־0. כלומר,
לכל $v \in V$, $\quad v + 0 = v$

ה. לכל $v \in V$ קיים ב־V איבר, שיסומן $-v$, המקיים:

$$v + (-v) = 0$$

$-v$ מכונה **איבר נגדי** ל־v.

תכונות הכפל בסקלר

א. **סגירות:** לכל $v \in V$ ולכל $\lambda \in F$, $\quad \lambda \cdot v \in F$

ב. **פילוג הכפל בסקלר מעל החיבור ב־V:**
לכל $u,v \in V$ ולכל $\lambda \in F$, $\quad \lambda(u+v) = \lambda u + \lambda v$

ג. **פילוג הכפל בסקלר מעל החיבור ב־F:**
לכל $v \in V$ ולכל $\lambda\mu \in F$, $\quad (\lambda+\mu)v = \lambda v + \mu v$

ד. **קיבוציות:**
לכל $v \in V$ ולכל $\lambda,\mu \in F$, $\quad (\lambda\mu)v = \lambda(\mu v)$

ה. **כפל באיבר היחידה:**
אם 1 הוא איבר היחידה של השדה F, אז לכל $v \in V$, $\quad 1 \cdot v = v$

משפט 7.2.1

יהי V מרחב לינארי מעל שדה F.

א. לכל $v \in V$ ו־ $\lambda_1,\dots,\lambda_n \in F$:

$$(\lambda_1 + \dots + \lambda_n)v = \lambda_1 v + \dots + \lambda_n v$$

ב. לכל $v_1,\dots,v_n \in V$ ו־ $\lambda \in F$:

$$\lambda(v_1 + \dots + v_n) = \lambda v_1 + \dots + \lambda v_n$$

משפט 7.2.2

יהי V מרחב לינארי (מעל שדה F).

א. ב־ V יש איבר ניטרלי **יחיד** (לגבי החיבור).

ב. לכל איבר ב־ V יש איבר נגדי **יחיד** (לגבי החיבור).

משפט 7.2.3

יהי V מרחב לינארי מעל שדה F.

א. אם וקטור $v \in V$ מקיים $v + v = v$, אז בהכרח $v = 0$.

ב. לכל $\lambda \in F$, $\lambda 0 = 0$.

ג. לכל $v \in V$, $0v = 0$.

ד. $\lambda v = 0$ אם ורק אם $\lambda = 0$ או $v = 0$.

ה. לכל $v \in V$, $(-1)v = -v$.

משפט 7.2.4

יהי V מרחב לינארי מעל שדה F, ויהיו $u, v \in V$. אז:

א. $-(-v) = v$

ב. $-(u + v) = (-u) + (-v)$

הגדרה 7.2.5

יהי V מרחב לינארי ויהיו $u, v \in V$ וקטורים כלשהם. **ההפרש** $u - v$ מוגדר על־ידי

$$u - v \overset{\text{def}}{=} u + (-v)$$

הגדרה 7.3.1

תת־קבוצה W של מרחב לינארי V מעל שדה F נקראת **תת־מרחב של** V, אם W עצמה היא מרחב לינארי מעל F לגבי פעולות החיבור והכפל בסקלר של המרחב V.

משפט 7.3.2

תהי W תת־קבוצה של מרחב לינארי V מעל שדה F.

אזי W היא תת־מרחב של V אם ורק אם:

א. $W \neq \phi$

ב. לכל $w_1, w_2 \in W$ גם $w_1 + w_2 \in W$

ג. לכל $w \in W$ ו־ $\lambda \in W$ גם $\lambda w \in W$

משפט 7.3.2′

תהי W תת־קבוצה של מרחב לינארי V מעל שדה F.

אזי W היא תת־מרחב של V אם ורק אם:

א. $W \neq \phi$

ב. לכל $w_1, w_2 \in W$ ולכל זוג סקלרים $\lambda_1, \lambda_2 \in W$,

$$\lambda_1 w_1 + \lambda_2 w_2 \in W$$

משפט 7.3.3 חיתוך של תת־מרחבים

אם W_1 ו־ W_2 הם תת־מרחבים של מרחב לינארי V (מעל שדה F), אזי החיתוך $W_1 \cap W_2$ אף הוא תת־מרחב של V.

הגדרה 7.4.1 צירוף לינארי

יהי V מרחב לינארי מעל שדה F, ויהיו $v_1, \ldots, v_n$ וקטורים כלשהם מתוך V.

סכום מהטיפוס

$$\lambda_1 v_1 + \ldots + \lambda_n v_n \quad \left(= \sum_{i=1}^{n} \lambda_i v_i \right)$$

שבו $\lambda_1, \ldots, \lambda_n$ הם סקלרים מתוך F, מכונה **צירוף לינארי של הוקטורים** $v_1, \ldots, v_n$ **עם המקדמים** $\lambda_1, \ldots, \lambda_n$.

משפט 7.5.1

תהי K קבוצה חלקית לא ריקה של מרחב לינארי V (מעל שדה F), ויהי $\mathrm{Sp}(K)$ אוסף כל הצירופים הלינאריים של וקטורים מתוך K. אזי:

א. $\mathrm{Sp}(K)$ הוא תת־מרחב של V המכיל את K.

ב. אם W הוא תת־מרחב של V המכיל את K, אז W מכיל גם את $\mathrm{Sp}(K)$.

הגדרה 7.5.2

יהי V מרחב לינארי (מעל שדה F) ותהי K תת־קבוצה לא ריקה של V.

התת־מרחב $\mathrm{Sp}(K)$, שאיבריו הם כל הצירופים הלינאריים של וקטורים מתוך K, נקרא **התת־מרחב הנפרש (או הנוצר)** על־ידי U.

על הקבוצה U אומרים שהיא **קבוצת יוצרים** של $\mathrm{Sp}(K)$ וגם שהיא **פורשת** את המרחב $\mathrm{Sp}(K)$.

בפרט, אם $\mathrm{Sp}(K) = V$, אומרים שהתת־קבוצה K **פורשת** את המרחב V.

הגדרה 7.5.2′

נאמר שסדרת וקטורים $(v_1, \ldots, v_n)$ במרחב לינארי V **פורשת** את V אם הקבוצה $\{v_1, \ldots, v_n\}$ פורשת את V.

הגדרה 7.5.3

יהי V מרחב לינארי. אומרים ש־ V **נוצר סופית** אם ורק אם קיימת קבוצה סופית היוצרת את V.

משפט 7.5.4

יהי V מרחב לינארי (מעל שדה F), ותהיינה K ו־ T תת־קבוצות לא ריקות של V. אז

$$\mathrm{Sp}(K) = \mathrm{Sp}(T)$$

אם ורק אם מתקיימים שני התנאים:

א. כל וקטור ב־ K הוא צירוף לינארי של וקטורים מתוך T (ובניסוח אחר: $K \subseteq \mathrm{Sp}(T)$).

ב. כל וקטור ב־ T הוא צירוף לינארי של וקטורים מתוך K (ובניסוח אחר: $T \subseteq \mathrm{Sp}(K)$).

הגדרה 7.6.1

יהי V מרחב לינארי מעל שדה F, ותהיינה S ו־ T שתי קבוצות חלקיות ל־ V. אוסף כל הוקטורים ב־ V שהם סכומים של וקטור מתוך S ווקטור מתוך T, מכונה **הסכום של הקבוצות** S ו־ T, וסימנו $S+T$.

הווי אומר:

$$S + T \overset{\text{def}}{=} \{s + t \mid s \in S,\, t \in T\}$$

משפט 7.6.2

יהיו U ו־ W שני תת־מרחבים של מרחב לינארי V מעל שדה F. אזי, הסכום $U+W$ הוא תת־מרחב של V המכיל את U ואת W. יתר על כן, $U+W$ הוא התת־מרחב הקטן ביותר של V בעל תכונה זו.

הגדרה 7.6.3

יהי V מרחב לינארי מעל שדה F, ותהיינה $T_1,\dots,T_n$ קבוצות חלקיות של V.

הסכום $T_1+\dots+T_n$ מוגדר כך:

$$T_1 + \dots + T_n \overset{\text{def}}{=} \{t_1 + \dots + t_n \mid t_i \in T_i, 1 \le i \le n \text{ לכל}\}$$

משפט 7.6.4

הסכום $U_1+\dots+U_n$ של מספר סופי כלשהו של תת־מרחבים, של מרחב לינארי V (מעל שדה F), הוא עצמו תת־מרחב של V.

מסקנה 7.6.5

הסכום $U_1+\dots+U_n$ של תת־מרחבים $U_1,\dots,U_n$ של מרחב לינארי V, הוא התת־מרחב הקטן ביותר של V המכיל את $U_1,U_2,\dots,U_n$.

הגדרה 7.7.1

יהיו U_1 ו־ U_2 שני תת־מרחבים של מרחב לינארי V מעל שדה F.

נאמר כי התת־מרחב W הוא **סכום ישר** של U_1 ו־ U_2 ונרשום

$$W = U_1 \oplus U_2$$

אם ורק אם מתקיימים שני תנאים:

א. $W = U_1 + U_2$

ב. לכל וקטור ב־ W יש הצגה **יחידה** כסכום של וקטור ב־U_1 ווקטור ב־ U_2.

משפט 7.7.2

יהי V מרחב לינארי, ויהיו U ו־ W תת־מרחבים של V.

$V = U \oplus W$ אם ורק אם מתקיימים שני התנאים:

א. $V = U + W$

ב. $U \cap W = \{0\}$

משפט 7.7.3

יהי V מרחב לינארי, ויהיו U ו־ W תת־מרחבים של V. אזי

$$V = U \oplus W$$

אם ורק אם מתקיימים שני התנאים:

א. $V = U + W$

ב. $0 = 0 + 0$ היא ההצגה היחידה של וקטור האפס, $0 \in V$, כסכום של וקטור מתוך U ווקטור מתוך W.

הגדרה 7.7.4

יהיו $U_1,\dots,U_n$ תת־מרחבים של מרחב לינארי V. אומרים על תת־מרחב W של V כי הוא **הסכום הישר** של $U_1,\dots,U_n$, ומסמנים

$$W = U_1 \oplus \dots \oplus U_n$$

אם ורק אם מתקיימים שני תנאים:

א. $W = U_1 + U_2 + \dots + U_n$

ב. לכל וקטור $W \ni w$ יש הצגה **יחידה** מהצורה

$$w = u_1 + \dots + u_n$$

כאשר $u_1 \in U_i$ לכל i $(1 \le i \le n)$.

משפט 7.7.5

יהי V מרחב לינארי, ויהיו $U_1,\dots,U_n$ תת־מרחבים של V.

נסמן את הסכום של כל התת־מרחבים U_i $(1 \le i \le n)$, **פרט** ל־ U_j, כך:

$$U_1 + \dots + \hat{U}_j + \dots + U_n$$

(שימו לב, התת־מרחב שמעליו מופיע הסימן $\wedge$ הוא זה **שאינו** משתתף בסכום).

אז

$$W = U_1 \oplus \ldots \oplus U_n$$

אם ורק אם מתקיימים שני התנאים:

א. $V = U_1 + \ldots + U_n$

ב. לכל j $(1 \le j \le n)$:

$$U_j \cap (U_1 + \ldots + \hat{U}_j + \ldots + U_n) = \{0\}$$

משפט 7.7.6

יהי V מרחב לינארי, ויהיו $U_1 \ldots U_n$ תת־מרחבים של V.

אז

$$V = U_1 \oplus \ldots \oplus U_n$$

אם ורק אם מתקיימים שני התנאים:

א. $V = U_1 + \ldots + U_n$

ב. ההצגה $\underset{U_1}{\underset{\in}{0}} + \ldots + \underset{U_n}{\underset{\in}{0}} = 0$ היא ההצגה היחידה של 0 כסכום של וקטורים מתוך $U_1,\ldots,U_n$.

הגדרה 7.8.1

יהי F שדה ויהי $P \in F[x]$.

הפונקציה $f_P : F \to F$, המוגדרת על־ידי

$$f_P(\alpha) = P(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n \qquad (\text{לכל } \alpha \in F),$$

נקראת **פונקציה פולינומיאלית**.

משפט 7.8.2

נניח כי $F = \mathbb{R}$ או $F = \mathbb{C}$. אם $P,Q \in F[x]$ הם זוג פולינומים שונים, אזי הפונקציות f_P ו־ f_Q הן פונקציות שונות.

משפט 7.8.3

אוסף כל הפונקציות הפולינומיאליות ב־ F^F הוא תת־מרחב של F^F.

למה 7.8.4

יהי F שדה. מכפלה של פונקציות פולינומיאליות ב־ F^F היא פונקציה פולינומיאלית.

למה 7.8.5

יהי F שדה סופי, ויהיו $a,b \in F$. אזי הפונקציה המוגדרת על־ידי $f(a) = b$ ו־ $f(a') = 0$ לכל $a' \ne a$ ב־ F היא פונקציה פולינומיאלית.

משפט 7.8.6

יהי F שדה סופי. כל הפונקציות ב־ F^F הן פולינומיאליות.

8.1.1 הגדרה

א. יהי V מרחב לינארי ותהי K תת־קבוצה של V. נאמר ש־ K **תלויה לינארית** אם קיימים ב־ K וקטורים שונים, $v_1,\dots,v_n$, אשר וקטור האפס של V, 0, הוא צירוף לינארי לא טריוויאלי שלהם.

ב. קבוצה K המוכלת ב־ V, שאינה תלויה לינארית, מכונה **בלתי תלויה לינארית**.

8.1.2 משפט

תהי K תת־קבוצה של מרחב לינארי V המכילה לפחות שני איברים. K תלויה לינארית אם ורק אם לפחות אחד מהוֶקטורים שבה ניתן להצגה כצירוף לינארי של וקטורים אחרים מתוכה.

8.1.3 הגדרה

תהי $(v_1,\dots,v_n)$ **סדרת וקטורים** במרחב לינארי V מעל שדה F. נאמר שהסדרה $(v_1,\dots,v_n)$ **תלויה לינארית** אם קיימים סקלרים $\lambda_1,\dots,\lambda_n \in F$ שאינם כולם אפס כך ש־ $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$. אם הסדרה $(v_1,\dots,v_n)$ אינה תלויה לינארית, נאמר שהיא **בלתי תלויה לינארית**.

8.2.1 הגדרה

יהי V מרחב לינארי ותהי B תת־קבוצה של V.

B היא **בסיס** של V אם מתקיימים שני התנאים:

א. B בלתי תלויה לינארית;

ב. B פורשת את V.

8.2.2 משפט

תהי $B \neq \{0\}$ תת־קבוצה של מרחב לינארי V.

א. B היא בסיס של V אם ורק אם B בלתי תלויה לינארית וכל קבוצה המכילה ממש את B היא תלויה לינארית.

ב. B היא בסיס של V אם ורק אם B פורשת את V, אך כל קבוצה המוכלת ממש ב־ B אינה פורשת את V.

8.2.3 משפט

תהי $B \neq \{0\}$ תת־קבוצה של מרחב לינארי V.

א. B היא בסיס אם ורק אם B היא קבוצה בלתי תלויה מרבית ב־ V.

ב. B היא בסיס אם ורק אם B היא קבוצה מזערית הפורשת את V.

8.2.4 משפט

לכל מרחב לינארי נוצר סופית השונה מ־ $\{0\}$, יש בסיס (סופי).

משפט 8.2.5

יהי $V \neq \{0\}$ מרחב לינארי ותהי $B = \{v_1,...,v_n\}$ תת־קבוצה של V בת n איברים. B היא בסיס של V אם ורק אם לכל וקטור $v \in V$ יש הצגה יחידה כצירוף לינארי של הוקטורים $v_1,...,v_n$.

משפט 8.2.6

יהי F שדה סופי. מספר איברי F הוא חזקה של מספר ראשוני.

למה 8.3.1

יהי V מרחב לינארי מעל שדה F, הנפרש על־ידי k וקטורים $v_1,...,v_k$, ויהיו $u_1,...,u_m$ וקטורים ב־ V. אם $m > k$, אז הקבוצה $\{u_1,...,u_m\}$ תלויה לינארית.

משפט 8.3.2

יהי V מרחב לינארי. אם ל־ V יש בסיס בעל n וקטורים, אז:

א. כל קבוצה של וקטורים מתוך V, שיש בה יותר מ־ n וקטורים, היא תלויה לינארית.

ב. כל קבוצה של וקטורים מתוך V, שיש בה פחות מ־ n וקטורים, אינה פורשת את V.

ג. כל קבוצה בלתי תלויה לינארית של וקטורים מתוך V, המכילה בדיוק n וקטורים, היא בסיס של V.

ד. כל קבוצה הפורשת את V, ומכילה בדיוק n וקטורים, היא בסיס של V.

ה. בכל בסיס של V יש בדיוק n איברים.

הגדרה 8.3.3

יהי $V \neq \{0\}$ מרחב לינארי נוצר סופית. מספר האיברים בבסיס כלשהו של V מכונה **הממד של** V, וסימנו המקובל – $\dim V$.

למען השלמות, נגדיר גם את ממד המרחב הכולל את וקטור האפס בלבד, כך:

$$\dim\{0\} \overset{\text{def}}{=} 0$$

משפט 8.3.4

אם V הוא מרחב לינארי נוצר סופית ו־ U הוא תת־מרחב של V, אז:

א. U הוא מרחב נוצר סופית, ומתקיים:

$$\dim U \leq \dim V$$

ב. השוויון $\dim U = \dim V$ מתקיים אם ורק אם $U = V$.

משפט 8.3.5

יהי $V \neq \{0\}$ מרחב לינארי n־ממדי, ותהי A קבוצה בלתי תלויה לינארית בת k וקטורים ב־ V. אם $k < n$, אז קיימים וקטורים $v_{k+1},\dots,v_n$, כך שהקבוצה $A \cup \{v_{k+1},\dots,v_n\}$ היא בסיס ל־ V.

ובניסוח קצר המסבר את האוזן:

כל קבוצה בלתי תלויה לינארית במרחב נוצר סופית ניתנת ל**השלמה** לבסיס.

משפט 8.3.6

יהיו U ו־ W שני תת־מרחבים של מרחב לינארי נוצר סופית V. אזי:

$$\dim(U+W)=\dim U+\dim W-\dim(U\cap W)$$

מסקנה 8.3.7

אם U ו־ W הם שני תת־מרחבים של מרחב נוצר סופית, ואם $V=U+W$, אז $V=U\oplus W$ אם ורק אם:

$$\dim V=\dim U+\dim W$$

הגדרה 8.4.1

יהי V מרחב לינארי נוצר סופית ממימד n. **סדרה** בת n וקטורים $(v_1,...,v_n)$ ב־ V נקראת **בסיס סדור** ל־ V, אם היא בלתי תלויה לינארית ופורשת את V.

משפט 8.4.2

יהיו V מרחב לינארי n־ממדי מעל שדה F, ו־ B בסיס סדור ל־ V. ההתאמה $v\to[v]_B$ המתאימה לכל וקטור v ב־ V את וקטור הקואורדינטות שלו ב־ F^n, $[v]_B$, היא העתקה **חד־חד־ערכית** מ־ V **על** F^n, המקיימת:

א. לכל $v,w\in V$ מתקיים השוויון $[v]_B+[w]_B=[v+w]_B$.

ב. לכל $\lambda\in F$,$v\in V$ מתקיים השוויון $[\lambda v]_B+\lambda[v]_B$.

למה 8.4.3

יהיו V מרחב לינארי נוצר סופית מעל שדה F, ו־ B בסיס סדור של V.

אם $u_1,\dots,u_m\in V$ ו־ $\lambda_1,\dots,\lambda_m\in F$, אז:

$$\left[\lambda_1u_1+\ldots+\lambda_mu_m\right]_B=\lambda_1\left[u_1\right]_B+\ldots+\lambda_m\left[u_m\right]_B$$

משפט 8.4.4

יהיו V מרחב לינארי ממימד n מעל שדה F, ו־ B בסיס סדור של V.

וקטורים $u_1,\dots,u_m$ ב־ V הם תלויים לינארית אם ורק אם הוקטורים $\left[u_1\right]_B,\dots,\left[u_m\right]_B$ ב־ F^n תלויים לינארית.

משפט 8.4.5

יהי $B=(v_1,...,v_n)$ בסיס סדור של מרחב לינארי n־ממדי V מעל שדה F, ויהיו $u_1,...,u_n$ וקטורים ב־ V הנתונים על־ידי:

$$\begin{aligned}u_1&=a_{11}v_1+a_{21}v_2+\ldots+a_{n1}v_n\\&\vdots\\u_n&=a_{1n}v_1+a_{2n}v_2+\ldots+a_{nn}v_n\end{aligned}$$

הסדרה $(u_1,\dots,u_n)$ היא בסיס ל־ V אם ורק אם המטריצה

$$M = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

הפיכה.

הגדרה 8.4.6

יהי $B=(v_1,\dots,v_n)$ בסיס סדור של מרחב לינארי n־ממדי V מעל שדה F. אם $B'=(u_1,\dots,u_n)$ הוא בסיס סדור אחר של אותו מרחב, ואם מתקיים

$$u_1 = a_{11}v_1 + .. + a_{n1}v_n$$

$$\vdots$$

$$u_n = a_{1n}v_1 + ... + a_{nn}v_n$$

אז המטריצה

$$M = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

נקראת **מטריצת המעבר** מן הבסיס (הסדור) B לבסיס (הסדור) B'.

משפט 8.4.7

יהי V מרחב לינארי מממד n מעל שדה F, ויהיו $B=\left(v_1,\dots,v_n\right)$, $B'=\left(u_1,\dots,u_n\right)$ שני בסיסים סדורים של V, ו־ M מטריצת המעבר מ־ B ל־ B'. לכל $v\in V$ מתקיים:

$$\left[v\right]_B = M\cdot\left[v\right]_{B'}$$

משפט 8.4.8

יהי V מרחב לינארי מעל שדה F, ויהיו $B=\left(v_1,\dots,v_n\right)$ ו־ $B'=\left(u_1,\dots,u_n\right)$ זוג בסיסים סדורים של V. אם A היא מטריצה ריבועית מסדר n המקיימת

$$\left[v\right]_B = A\cdot\left[v\right]_{B'} \qquad (*)$$

לכל $v\in V$, אז A היא מטריצת המעבר מ־ B ל־ B'.

משפט 8.4.9

אם M היא מטריצת המעבר מבסיס B לבסיס B', אז M^{-1} היא מטריצת המעבר מהבסיס B' לבסיס B.

למה 8.5.1

תהי $A=[a_{ij}]\in \mathbf{M}^F_{m\times n}$ מטריצת **מדרגות** ויהיו

$v_1,\dots,v_k$

שורותיה של A **שאינן שורות אפסים**. אזי:

א. הקבוצה $\{v_1,\ldots,v_k\}$ היא בסיס למרחב השורות של A.

ב. דרגת השורות של A שווה למספר השורות של A שאינן שורות אפסים, דהיינו $\rho_R(A) = k$.

משפט 8.5.2

דרגת השורות של מטריצה שווה לדרגת העמודות שלה.

למה 8.5.3

אם P מטריצה מסדר $m \times k$ ו־ Q מטריצה מסדר $k \times n$ (שתיהן מעל שדה F), אז כל עמודה של מטריצת המכפלה PQ היא צירוף לינארי של k עמודותיה של P.

הגדרה 8.5.4

ממד מרחב השורות של המטריצה A (שהוא גם ממד מרחב העמודות של A) נקרא **דרגת המטריצה**. את דרגת המטריצה A מסמנים $\rho(A)$.

משפט 8.6.1

אם $A\mathbf{x} = 0$ מערכת משוואות הומוגנית ב־ n משתנים ו־ P מרחב הפתרונות שלה, אז:

$$\dim P = n - \rho(A)$$

משפט 8.6.2

למערכת משוואות לינאריות קיים פתרון אם ורק אם דרגת מטריצת המקדמים שלה שווה לדרגת מטריצת המקדמים המצומצמת.

משפט 8.7.1

יהי V מרחב לינארי נוצר סופית מעל שדה המספרים המרוכבים $\mathbb{C}$, ונסמן את הממד של V מעל $\mathbb{C}$ ב־ n. אזי V נוצר סופית גם כמרחב לינארי מעל $\mathbb{R}$, וממדו מעל $\mathbb{R}$ הוא $2n$.

מהדורה פנימית
לא להפצה ולא למכירה
מק"ט 20109-5049