אלגברה לינארית 1

יובל קפלן

מחברת סיכום הרצאות ד״ר אלי בגנו בקורס ״אלגברה לינארית 1״ (80134) באוניברסיטה העברית, 2006–7. תוכן מחברת זו הוקלד ונערך על־ידי יובל קפלן. אין המרצה אחראי לכל טעות שנפלה בו. סודר באמצעות LaTeX 2_ε ב־4 בפברואר 2008.

עדכונים, תיקונים וסיכומים נוספים יימצאו ב־http://www.limsoup.net/. לתגובות, לתיקונים ובכל עניין אחר, אנא כתבו ל־yuvak@gmx.net.

תוכן עניינים

תוכן עניינים

1 שדות

1.1 $\mathbb{Z}$ ו־$\mathbb{Q}$ – המספרים השלמים והרציונאליים

22.10.2006 מוגדרת ב־$\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$ פעולת חיבור. מתקיימות התכונות:[1]

ח־1. לכל $a, b \in \mathbb{Z}$ קיים $c \in \mathbb{Z}$ יחיד כך ש־$a + b = c$ (סגירות)

ח־2. לכל $a, b \in \mathbb{Z}$, $\quad a + b = b + a$ (קומוטטיביות – חילוף)

ח־3. לכל $a, b, c \in \mathbb{Z}$, $\quad (a + b) + c = a + (b + c)$ (אסוציאטיביות – קיבוץ)

ח־4. קיים איבר $0 \in \mathbb{Z}$ כך שלכל $a \in \mathbb{Z}$, $\quad a + 0 = a$ (קיום איבר אפס)

ח־5. לכל $a \in \mathbb{Z}$ קיים $b \in \mathbb{Z}$ כך ש־$a + b = 0$ (קיום איברים נגדיים)

מוגדרת גם פעולת כפל. מתקיימות התכונות הבאות:

כ־1. לכל $a, b \in \mathbb{Z}$ קיים $c \in \mathbb{Z}$ יחיד כך ש־$a \cdot b = c$ (סגירות)

כ־2. לכל $a, b \in \mathbb{Z}$, $\quad a \cdot b = b \cdot a$ (קומוטטיביות)

כ־3. לכל $a, b, c \in \mathbb{Z}$, $\quad (a \cdot b)c = a(b \cdot c)$ (אסוציאטיביות)

כ־4. קיים איבר $1 \in \mathbb{Z}$ כך שלכל $a \in \mathbb{Z}$, $\quad a \cdot 1 = a$ (קיום איבר יחידה)

כ־ח. לכל $a, b, c \in \mathbb{Z}$, $\quad a(b + c) = ab + ac$ (דיסטריבוטיביות – פילוג)

תכונה מקבילה לח־5 אינה מתקיימת ב־$\mathbb{Z}$ עבור כפל.[2]

נגדיר $\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0\}$ – קבוצת המספרים הרציונאליים. $\mathbb{Z} \subseteq \mathbb{Q}$. מתקיימות כל התכונות הנ״ל, ובנוסף

כ־5. לכל $0 \neq a \in \mathbb{Q}$ קיים $b \in \mathbb{Q}$ כך ש־$a \cdot b = 1$ (קיום איברים הפכיים)

1.2 שדות

הגדרה. קבוצה $\mathbb{F}$ עליה מוגדרות פעולות ״חיבור״ ו״כפל״ נקראת **שדה** אם מתקיימות התכונות הבאות: שדה

ח־1. $\forall a, b \in \mathbb{F} \quad \exists! c \in \mathbb{F} \ : \ a + b = c$

ח־2. $\forall a, b \in \mathbb{F} \quad a + b = b + c$

ח־3. $\forall a, b, c \in \mathbb{F} \quad (a + b) + c = a + (b + c)$

ח־4. $\exists 0_{\mathbb{F}} \in \mathbb{F} \ : \ \forall a \in \mathbb{F} \quad a + 0_{\mathbb{F}} = a$

ח־5. $\forall a \in \mathbb{F} \quad \exists b \in \mathbb{F} \ : \ a + b = 0_{\mathbb{F}}$

כ־1. $\forall a, b \in \mathbb{F} \quad \exists! c \in \mathbb{F} \ : \ a \cdot b = c$

כ־2. $\forall a, b \in \mathbb{F} \quad a \cdot b = b \cdot a$

כ־3. $\forall a, b, c \in \mathbb{F} \quad (ab)c = a(bc)$

כ־4. $\exists 1_{\mathbb{F}} \in \mathbb{F} \ : \ \forall a \in \mathbb{F} \quad a \cdot 1_{\mathbb{F}} = a$

[1] קיום תכונות אלו ב־$\mathbb{Z}$ ניתן להוכחה; אלו אינן אקסיומות.

[2] קבוצה שמקיימת את התכונות דלעיל נקראת **חוג**.

כ־5. $\forall a \in \mathbb{F} \quad a \neq 0 \Longrightarrow \exists b \in \mathbb{F} \,:\, ab = 1_{\mathbb{F}}$

כ־ח. $\forall a, b, c \in \mathbb{F} \quad a(b+c) = ab + ac$

25.10.2006

דוגמה (שדה הדיאז והבמול). תהי קבוצה $\mathbb{F} = \{\sharp, \flat\}$. נגדיר פעולות:

$+$	$\sharp$	$\flat$
$\sharp$	$\sharp$	$\flat$
$\flat$	$\flat$	$\sharp$

$\cdot$	$\sharp$	$\flat$
$\sharp$	$\sharp$	$\sharp$
$\flat$	$\sharp$	$\flat$

זהו אכן שדה: סגירות (ח־1, כ־1) מתקיימת, לפי הגדרת הפעולות; קומוטטיביות (ח־2, כ־2) מתקיימת, לפי סימטריות הטבלאות; איבר האפס (ח־4) הוא $\sharp$ ואיבר היחידה (כ־4) הוא $\flat$, לפי הטבלאות; קיימים איברים נגדיים (ח־5) – $-\sharp = \sharp$, $-\flat = \flat$ – ואיבר הפכי (כ־5) – $\flat^{-1} = \flat$ ($\sharp$ הוא איבר האפס, לכן לא מוגדר לו הפכי). את קיום תכונות האסוציאטיביות (ח־3, כ־3) והדיסטריבוטיביות (כ־ח) ניתן להראות לפי בדיקת כל האפשרויות.

הגדרת שדה זו אינה רנדומאלית: ישנה רק דרך אחת להגדיר שדה בעל מספר שהוא חזקת־ראשוני של איברים, על־פי משפט מתורת השדות (ואין שדה בעל מספר איברים שאינו חזקת־ראשוני); ניתן לנסות ולראות שאם $\flat + \flat \neq \sharp$ לא יתקבל שדה.

משפט 1: איבר האפס ואיבר היחידה בשדה יחידים.

הוכחה (יחידות האפס). נניח ש־$0_{\mathbb{F}}$, $0'_{\mathbb{F}}$ האפסים של השדה $\mathbb{F}$. לכל $a \in \mathbb{F}$ מתקיים $a + 0_{\mathbb{F}} = a$ ו־$a + 0'_{\mathbb{F}} = a$; לכן בפרט, עבור $a = 0_{\mathbb{F}}$, מתקיים $0_{\mathbb{F}} = 0_{\mathbb{F}} + 0'_{\mathbb{F}} = 0'_{\mathbb{F}} + 0_{\mathbb{F}} = 0'_{\mathbb{F}}$ (בהסתמך על נייטרליות $0'_{\mathbb{F}}$ ו־$0_{\mathbb{F}}$) – כלומר, $0_{\mathbb{F}} = 0'_{\mathbb{F}}$.

משפט 2: לכל $a \in \mathbb{F}$ יש נגדי (איבר b המקיים $a + b = 0_{\mathbb{F}}$) יחיד ולכל $0 \neq a \in \mathbb{F}$ יש הפכי (איבר b המקיים $ab = 1_{\mathbb{F}}$) יחיד.

הוכחה (יחידות הנגדי). יהי $a \in \mathbb{F}$. נניח שיש שני איברים $b, b' \in \mathbb{F}$ כך שמתקיים $a + b = 0_{\mathbb{F}}$ ו־$a + b' = 0_{\mathbb{F}}$. נוסיף b[3] לשני האגפים: $b + (a+b) = b + (a+b')$. מהאסוציאטיביות, $(b+a)+b = (b+a)+b'$; מהקומוטטיביות, $(a+b)+b = (a+b)+b'$; מתכונת הנגדי, $0_{\mathbb{F}} + b = 0_{\mathbb{F}} + b'$, ומנייטרליות האפס, $b = b'$.

נוסיף לדרישות השדה את הדרישה $1_{\mathbb{F}} \neq 0_{\mathbb{F}}$. דרישה זו אינה בגדר חובה, אבל

טענה 3: אם בשדה $\mathbb{F}$ $1_{\mathbb{F}} = 0_{\mathbb{F}}$, אז לכל $a \in \mathbb{F}$, $a = 0$.

הוכחה. למה 1.3: יהי $\mathbb{F}$ שדה. אז לכל $a \in \mathbb{F}$, $a \cdot 0_{\mathbb{F}} = 0$.[4]

הוכחה. יהי $a \in \mathbb{F}$. מנייטרליות האפס ומהפילוג, $a \cdot 0_{\mathbb{F}} = a \cdot (0_{\mathbb{F}} + 0_{\mathbb{F}}) = a \cdot 0_{\mathbb{F}} + a \cdot 0_{\mathbb{F}}$. נחבר לשני האגפים $-a \cdot 0_{\mathbb{F}}$; נקבל $a \cdot 0_{\mathbb{F}} + (-(a \cdot 0_{\mathbb{F}})) = a \cdot 0_{\mathbb{F}} + a \cdot 0_{\mathbb{F}} + (-(a \cdot 0_{\mathbb{F}}))$.

[3] לא ניתן, בשלב זה, לכתוב $-a$ – סימון זה כרוך ביחידות, והרי זה מה שעלינו להוכיח.

[4] זו אינה טענה טריוויאלית – a לא חייב להיות מספר.

מהאסוציאטיביות, $a\cdot 0_{\mathbb{F}}+(-(a\cdot 0_{\mathbb{F}}))=a\cdot 0_{\mathbb{F}}+(a\cdot 0_{\mathbb{F}}+(-a\cdot 0_{\mathbb{F}}))$ ולכן, מתכונת הנגדי, $0_{\mathbb{F}}=a\cdot 0_{\mathbb{F}}$.

כעת, נניח שבשדה $\mathbb{F}$, $1_{\mathbb{F}}=0_{\mathbb{F}}$. יהי $a\in\mathbb{F}$. אז $a=a\cdot 1_{\mathbb{F}}=a\cdot 0_{\mathbb{F}}=0$, כנדרש.

1.3 תכונות שדה

יהי $\mathbb{F}$ שדה ויהיו $a,b,c\in\mathbb{F}$.

א. $a\cdot 0_{\mathbb{F}}=0_{\mathbb{F}}$

ב. $(-1_{\mathbb{F}})a=-a$

הוכחה. צריך להוכיח $(-1_{\mathbb{F}})a=-a$. על־פי יחידות הנגדי, כיוון ש־$-a$ הוא הנגדי של a, אם נוכיח ש־$(-1_{\mathbb{F}})a$ אף הוא נגדי של a נקבל שמתקיים $(-1_{\mathbb{F}})a=-a$. לכן מספיק להוכיח $a+(-1_{\mathbb{F}})a=0_{\mathbb{F}}$, כלומר $a+(-1_{\mathbb{F}})a=a(1_{\mathbb{F}}+(-1_{\mathbb{F}}))=a\cdot 0_{\mathbb{F}}=0_{\mathbb{F}}$.

ג. $a(-b)=(-a)b=-(ab)$

ד. $-(-a)=a$

ה. $(-a)(-b)=ab$

ו. $-(a+b)=-a-b$ [5]

ז. $a(b-c)=ab-ac$

ח. $(a^{-1})^{-1}=a$ ($a\neq 0_{\mathbb{F}}$) [6]

ט. $(ab)^{-1}=a^{-1}b^{-1}$ ($a,b\neq 0_{\mathbb{F}}$)

י. $a+c=b+c\Longrightarrow a=b$

יא. $ab=ac\Longrightarrow b=c$ ($a\neq 0_{\mathbb{F}}$)

יב. $ab=0_{\mathbb{F}}\Longrightarrow a=0_{\mathbb{F}}\vee b=0_{\mathbb{F}}$

1.4 $\mathbb{Z}_n$ – שדה השאריות מודולו n

29.10.2006 **משפט 4 (חילוק עם שארית):** יהי $1<n\in\mathbb{N}$. ניתן לחלק כל מספר טבעי m ב־n עם שארית: קיימים q, r יחיד כך ש־$m=qn+r\wedge 0\leq r<n$.

דוגמה. למשל,

m		q		n		r
13	=	4	·	3	+	1
14	=	4	·	3	+	2
15	=	5	·	3	+	0

[5] כאשר כותבים $a-b$, מתכוונים ל־$a+(-b)$.

[6] כאשר כותבים a^{-1}, מתכוונים להפכי של a, אם קיים.

נגדיר $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. אם נבחר שני מספרים מ־$\mathbb{Z}$, נחבר אותם, נחלק ב־$n$ וניקח את השארית, נקבל מספר ב־$\mathbb{Z}_n$. נגדיר חיבור מודולו n: אם $a, b \in \mathbb{Z}$, נכתוב $a + b = qn + r$ ונגדיר $a +_n b = r$. באופן דומה, נגדיר כפל ב־$\mathbb{Z}_n$: עבור $a, b \in \mathbb{Z}$, נכתוב $a \cdot b = qn + r$ ואז $a \cdot_n b = r$.

דוגמה. עבור $n = 2$,

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

אם נסמן $\sharp = 0$, $\flat = 1$ נקבל שוב את דוגמת הדיאז והבמול, בה כבר ראינו שמתקבל שדה.

דוגמה. עבור $n = 4$,

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

זהו אינו שדה – לא קיים 2^{-1}: נניח בשלילה ש־$0 \neq a \in \mathbb{Z}_4$ הוא ההפכי של 2. על־פי הטבלה, $2 \cdot_4 2 = 0$. נכפיל ב־a ונקבל $a \cdot_4 (2 \cdot_4 2) = a \cdot_4 0$; מחוק הקיבוץ, $a \cdot_4 0 = (a \cdot_4 2) \cdot_4 2$, ועל־פי ההנחה ש־$a$ ההפכי של 2, $1 \cdot_4 2 = 0$ – סתירה.

הגדרה. יהי $a \in \mathbb{N}$. נסמן ב־$[a]_n$ את השארית המתקבלת על־ידי חלוקה של a ב־n; כלומר, אם $a = qn + r$, $[a]_n = r$. אם a, a' נבדלים בכפולת n ($a - a' = qn$), נכתוב $a \equiv a' \pmod{n}$.

טענה 5: $a \equiv a' \pmod{n}$ אם"ם $[a]_n = [a']_n$.

דוגמה. $16 \pmod{5} \equiv 31$ כי $31 - 16 = 15 = 3 \cdot 5$. אפשר לראות זאת גם על־פי כך ש־$31 = 6 \cdot 5 + \mathbf{1}$ ו־$16 = 3 \cdot 5 + \mathbf{1}$.

הוכחה. נניח ש־$a \equiv a' \pmod{n}$. אז $a - a' = qn$ ולכן $a = a' + qn$. נחלק את a ב־n: $a' + qn = a = kn + [a]_n$. מכאן, $a' = (k - q)n + [a]_n$ – כלומר, שארית החלוקה של a' ב־n היא $[a]_n$, ולכן $[a]_n = [a']_n$. (הכיוון השני – כתרגיל.)

טענה 6: לכל $a \in \mathbb{N}$, $a \equiv [a]_n \pmod{n}$.

הוכחה. יהי $a \in \mathbb{N}$. נכתוב $a = qn + [a]_n$. אז $a - [a]_n = qn$, ולכן $a \equiv [a]_n \pmod{n}$.

טענה 7: אם $a \equiv a' \pmod{n}$ ו־$b \equiv b' \pmod{n}$, אז $(a + b) \equiv (a' + b') \pmod{n}$.

הוכחה. נניח $a \equiv a'$, $b \equiv b'$. לכן $a - a' = k_1 n$ ו־$b - b' = k_2 n$; נחבר את המשוואות ונקבל $(a+b) - (a'+b') = (k_1+k_2)n$. אז $(a+b) \equiv (a'+b') \pmod{n}$.

משפט 8: לכל $1 < n \in \mathbb{N}$, $\mathbb{Z}_n$ מקיים את כל תכונות השדה פרט (אולי) לקיום הפכי לכפל (כ־5). 1.11.2006

הוכחה. נבדוק את קיום התכונות:

ח־1. סגירות: אם $a, b \in \mathbb{Z}_n$, משפט החילוק עם שארית מבטיח ששארית החלוקה ב־n של $a+b$ היא מספר ב־$\mathbb{Z}_n$.

ח־2. קומוטטיביות: $a+b = b+a$, לכן $a +_n b = [a+b]_n = [b+a]_n = b +_n a$.

ח־3. אסוציאטיביות: צ״ל $(a +_n b) +_n c = a +_n (b +_n c)$.
מהגדרת הפעולה $+_n$ נקבל $(a +_n b) +_n c = [[a+b]_n + c]_n$. מטענות 7 ו־6, מתקיים $[a+b]_n + c \equiv (a+b) + c$, לכן על־פי טענה 5, $[[a+b]_n + c]_n = [(a+b)+c]_n$. מאסוציאטיביות $\mathbb{Z}$נקבל $[(a+b)+c]_n = [a+(b+c)]_n$, ועל־פי טענות 7 ו־6, $a + (b+c) \equiv a + [b+n]_n$ ולכן, מטענה 5, $[a+(b+c)]_n = [a + [b+c]_n]_n$. אז $(a +_n b) +_n c = a +_n (b +_n c)$.

ח־4. קיום איבר אפס: $a +_n 0 = [a+0]_n = [a]_n = a$

ח־5. קיום איברים נגדיים: יהי $0 \neq a \in \mathbb{Z}_n$; ניקח $-a = n - a$.[7] אז מתקיים $a +_n (n-a) = [a + (n-a)]_n = [n]_n = 0$. אם $a = 0$, ניקח $-a = 0$.

כ־1. סגירות: אם $a, b \in \mathbb{Z}_n$, משפט החילוק עם שארית מבטיח ששארית החלוקה ב־n של $a \cdot b$ היא מספר ב־$\mathbb{Z}_n$.

כ־2. קומוטטיביות: $a \cdot_n b = [ab]_n = [ba]_n = b \cdot_n a$

כ־3. אסוציאטיביות:

למה 1.8: יהיו $a, a', b, b' \in \mathbb{Z}_n$. אם $a \equiv a' \pmod{n}$ ו־$b \equiv b' \pmod{n}$ אז $ab \equiv a'b'$.

הוכחה. נניח $a \equiv a'$ ו־$b \equiv b'$. אז $a - a' = k_1 n$ ו־$b - b' = k_2 n$. אז –

$$\begin{aligned} ab - a'b' &= ab - a'b + a'b - a'b' \\ &= b(a-a') + a'(b-b') \\ &= b \cdot k_1 n + a' \cdot k_2 n \\ &= (b \cdot k_1 + a' \cdot k_2)n \end{aligned}$$

ולכן $ab \equiv a'b'$.

ממשיכים באופן דומה להוכחת אסוציאטיביות החיבור.

כ־4. קיום איבר יחידה: $a \cdot_n 1 = [a \cdot 1]_n = [a]_n = a \quad \forall a \in \mathbb{Z}_n$

כ־ח. דיסטריבוטיביות הכפל מעל החיבור: צ״ל $a \cdot_n 1 = [a \cdot 1]_n = [a]_n = a$. כתרגיל.

כ־5. קיום איברים הפכיים: לא תמיד מתקיימת

[7] אי־אפשר להגדיר $-a = [n-a]_n$ כי פעולה זו אינה מוגדרת מחוץ ל־$\mathbb{Z}_n$.

הגדרה. $1 < p \in \mathbb{N}$ נקרא **ראשוני** אם אין $1 < k, l < p$ ‏($k, l \in \mathbb{N}$) כך ש־$kl = p$. אחרת, p נקרא **פריק**.

משפט 9 (המשפט היסודי של האריתמטיקה): כל מספר $1 < n \in \mathbb{N}$ ניתן להצגה באופן יחיד (עד־כדי סדר הגורמים) כמכפלת גורמים ראשוניים.

טענה 10: יהי p מספר ראשוני, $m, n \in \mathbb{N}$. אם p גורם של mn אז p גורם של m או של n.

הוכחה. נניח ש־p גורם של mn. נציג את m ו־n כמכפלת ראשוניים: $m = p_1^{t_1} \dots p_k^{t_k}$, $n = q_1^{r_1} \dots q_l^{r_l}$. אז $mn = p_1^{t_1} \dots p_k^{t_k} q_1^{r_1} \dots q_l^{r_l}$. אם p גורם של mn, הוא מתלכד עם אחד המספרים הראשוניים ב־mn – כלומר, $p = p_i$ או $p = q_j$. במקרה הראשון, p גורם של m; בשני, של n.

טענה 11: אם $n \in \mathbb{N}$ אינו ראשוני, $\mathbb{Z}_n$ אינו שדה.

הוכחה. $n = kl$ כאשר $1 < k, l < n$. אז $k, l \in \mathbb{Z}_n$, ו־$l \cdot_n k = [lk]_n = [n]_n = 0$. נניח בשלילה כי x הוא ההפכי של k ב־$\mathbb{Z}_n$. אז $k \cdot_n x = 1$, ו־$l \cdot_n (k \cdot_n x) = l$. אבל לפי האסוציאטיביות $l \cdot_n (k \cdot_n x) = (l \cdot_n k) \cdot_n x = 0 \cdot_n x = 0$. קיבלנו ש־$l = 0$ – סתירה.[8]

טענה 12: אם $n \in \mathbb{N}$ ראשוני, $\mathbb{Z}_n$ שדה.

הוכחה. הוכחנו את כל התכונות, פרט לקיום איברים הפיכים. יהי $0 \neq k \in \mathbb{Z}_n$; נוכיח ש־$k$ הפיך. נתבונן במספרים הבאים: $k \cdot_n 0,\ k \cdot_n 1,\ \dots,\ k \cdot_n (n-1)$. אם בקבוצה זו אין שני מספרים שווים, כל איברי $\mathbb{Z}_n$ בקבוצה, וביניהם 1 – כלומר, קיים l כך ש־$k \cdot_n l = 1$. נניח בשלילה שקיימים $0 \leq l_1 < l_2 \leq n-1$ כך ש־$k \cdot_n l_1 = k \cdot_n l_2$. אם כן, מתקיים $[kl_1]_n = [kl_2]_n$ ולכן $kl_1 \equiv kl_2$. לכן $k(l_2 - l_1) = kl_2 - kl_1 = qn$. כיוון ש־$n$ ראשוני, אם n גורם של $k(l_2 - l_1)$ אז n גורם של $l_2 - l_1$ או של k – סתירה, כי $0 < l_2 - l_1 < n$ ו־$0 < k < n$ (כלומר, n גדול משניהם).

1.5 המציין של שדה

יהי $\mathbb{F}$ שדה. אז $0_\mathbb{F}, 1_\mathbb{F} \in \mathbb{F}$. נתבונן באיברים $0_\mathbb{F},\ 1_\mathbb{F},\ 1_\mathbb{F} + 1_\mathbb{F},\ 1_\mathbb{F} + 1_\mathbb{F} + 1_\mathbb{F},\ \dots$. ישנן שתי אפשרויות: כל האיברים שונים זה מזה, או קיימים $m \neq n$ טבעיים שעבורם מתקיים 5.11.2006
$\underbrace{1_\mathbb{F} + \ldots + 1_\mathbb{F}}_{\text{פעמים } m} = \underbrace{1_\mathbb{F} + \ldots + 1_\mathbb{F}}_{\text{פעמים } n}$.

נתמקד במקרה השני. נניח $m > n$. נוסיף $-1_\mathbb{F}$ לשני צידי המשוואה:

$$\underbrace{1_\mathbb{F} + \ldots + 1_\mathbb{F}}_{\text{פעמים } m} + (-1_\mathbb{F}) = \underbrace{1_\mathbb{F} + \ldots + 1_\mathbb{F}}_{\text{פעמים } n} + (-1_\mathbb{F})$$

[8] אין זה אומר שכלל לא יהיו מספרים הפיכים: אם t זר ל־n, מתקיים $\forall s \in \mathbb{N} \quad [st]_n \neq 0$ ו־t הפיך. אולם מספיק שיש בלתי־הפיך אחד כדי ש־$\mathbb{Z}_n$ לא יהיה שדה, והראינו שלכל k שמחלק את n לא קיים הפכי.

כלומר, $\underbrace{1_{\mathbb{F}}+\ldots+1_{\mathbb{F}}}_{n-1 \text{ פעמים}} = \underbrace{1_{\mathbb{F}}+\ldots+1_{\mathbb{F}}}_{m-1 \text{ פעמים}}$. לאחר n חיסורים, נקבל $\underbrace{1_{\mathbb{F}}+\ldots+1_{\mathbb{F}}}_{m-n \text{ פעמים}} = 0_{\mathbb{F}}$.

מציין של שדה

הגדרה. המספר הטבעי המינימלי k עבורו $\underbrace{1_{\mathbb{F}}+\ldots+1_{\mathbb{F}}}_{k \text{ פעמים}} = 0_{\mathbb{F}}$ ייקרא **המציין** של השדה. מסמנים $\operatorname{char}\mathbb{F} = k$. אם לא קיים k כזה (כלומר, אם מתקיים המקרה הראשון), אומרים $\operatorname{char}\mathbb{F} = 0$.

דוגמה. $\operatorname{char}\mathbb{Q} = 0$; $\operatorname{char}\mathbb{Z}_n = n$[9].

משפט 13: אם $\operatorname{char}\mathbb{F} = n > 0$, n ראשוני.

הוכחה. נניח ש־n אינו ראשוני. אז יש $1 < k, l < n$ כך ש־$n = kl$. אז

$$\begin{aligned}
\underbrace{(1_{\mathbb{F}}+\ldots+1_{\mathbb{F}})}_{k \text{ פעמים}}\underbrace{(1_{\mathbb{F}}+\ldots+1_{\mathbb{F}})}_{l \text{ פעמים}} &= \overbrace{1_{\mathbb{F}}\underbrace{(1_{\mathbb{F}}+\ldots+1_{\mathbb{F}})}_{l \text{ פעמים}} + \ldots + 1_{\mathbb{F}}\underbrace{(1_{\mathbb{F}}+\ldots+1_{\mathbb{F}})}_{l \text{ פעמים}}}^{k \text{ פעמים}} \\
&= \underbrace{1_{\mathbb{F}}+\ldots+1_{\mathbb{F}}}_{kl = n \text{ פעמים}} = 0_{\mathbb{F}}
\end{aligned}$$

לפי תכונות השדה, אם $ab = 0_{\mathbb{F}}$ אז $a = 0_{\mathbb{F}}$ או $b = 0_{\mathbb{F}}$. אז $\underbrace{1_{\mathbb{F}}+\ldots+1_{\mathbb{F}}}_{k \text{ פעמים}} = 0_{\mathbb{F}}$ או $\underbrace{1_{\mathbb{F}}+\ldots+1_{\mathbb{F}}}_{l \text{ פעמים}} = 0_{\mathbb{F}}$, בסתירה למינימליות n.

1.6 $\mathbb{R}$ ו־$\mathbb{C}$ – המספרים הממשיים והמרוכבים

באופן לא־פורמאלי, נאמר שכל מספר ממשי x ניתן לייצוג כ־$x = n.d_1d_2\ldots$, כאשר $n \in \mathbb{N}$ ו־$d_i \in \{0,\ldots,9\}$. זה נקרא **פיתוח עשרוני**. ההצגה אינה יחידה – למשל, $0.\bar{9} = 1.\bar{0}$.

$(\mathbb{R},+,\cdot)$ שדה.

לא קיים מספר ממשי המקיים $x^2 = -1$. נניח שיש שדה שמכיל את $\mathbb{R}$ ובו יש מספר שהוא $\sqrt{-1}$; נקרא לאיבר זה i. שדה כזה יהיה חייב להיות סגור לכפל ולחיבור (אם $x, y \in \mathbb{R}$, גם $x+iy$ יהיה בשדה החדש). כמו־כן, החיבור חייב לקיים $(x+iy)+(x'+iy') = (x+x')+i(y+y')$ והכפל חייב לקיים $(x+iy)\cdot(x'+iy') = xx'+ixy'+ix'y+i^2yy' = (xx'-yy')+i(xy'+x'y)$.

הגדרה. $\mathbb{C} = \{(x,y) \mid x,y \in \mathbb{R}\}$, כך ש־$(x,y) = (x',y') \iff x = x', y = y'$.

נגדיר חיבור (רכיב־רכיב): $(x,y)\oplus(x',y') = (x+x', y+y')$

נגדיר כפל: $(x,y)\odot(x',y') = (xx'-yy', xy'+x'y)$.[10]

טענה 14: הקבוצה $\mathbb{C}$ עם פעולות הכפל והחיבור שהגדרנו מהווה שדה.

הוכחה. מתבססת על תכונות $\mathbb{R}$. כתרגיל. מספר נקודות חשובות:

[9] למעשה, המציין של כל שדה שמכיל את $\mathbb{Z}$ הוא 0.

[10] כפי שמיד נראה, $0_{\mathbb{C}} = (0,0)$; אילו היינו מגדירים כפל רכיב־רכיב, היינו מקבלים, גם אם $(x,0),(0,y) \neq (0,0)$, $(x,0)\odot(0,y) = (0,0)$.

ח־4. איבר אפס: $(x,y)+(0,0)=(x,y)$
ח־5. איברים נגדיים: $(x,y)+(-x,-y)=(0,0)$
כ־4. איבר יחידה: $(x,y)\cdot(1,0)=(x-0,0+y)=(x,y)$
כ־5. איברים הפכיים: אם $(x,y)\neq(0,0)$, נסמן $(x',y')=\left(\frac{x}{x^2+y^2},\frac{-y}{x^2+y^2}\right)$. קל לראות ש־$(x,y)\cdot(x',y')=(1,0)$.

נתבונן בקבוצה החלקית $\bar{\mathbb{R}}=\{(x,0)\mid x\in\mathbb{R}\}\subseteq\mathbb{C}$. ונגדיר העתקה $f:\mathbb{R}\to\bar{\mathbb{R}}$ על־ידי $f(x)=(x,0)$. f היא העתקה חד־חד ערכית (כלומר, לכל איבר ב־$\bar{\mathbb{R}}$ יש לכל היותר מקור אחד ב־$\mathbb{R}$). הפונקציה f שומרת על הפעולות ב־$\mathbb{R}$:

$$\begin{aligned} f(x+x') &= (x+x',0)=(x,0)\oplus(x',0)=f(x)\oplus f(x') \\ f(x\cdot x') &= (xx',0)=(x,0)\odot(x',0)=f(x)\odot f(x') \end{aligned}$$

8.11.2006

f היא **העתקת שיכון**; אז $\mathbb{R}$ משוכן ב־$\mathbb{C}$.[11]

טענה 15: האיבר $i=(0,1)\in\mathbb{C}$ הוא שורש של -1.[12] (כלומר, $i^2=(-1,0)$).

הוכחה. $i^2=(0,1)^2=(0,1)\odot(0,1)=(-1,0)$

יהי $(x,y)\in\mathbb{C}$. אז $(x,y)=(x,0)\oplus(0,y)=x\oplus((0,1)\odot(y,0))=x\oplus iy$. לכן כל מספר מרוכב ניתן להציג כ־$x\oplus iy$ כאשר $x,y\in\mathbb{R}$ – כלומר, נוכל לכתוב אחרת: $\mathbb{C}=\left\{x+iy\mid x,y\in\mathbb{R},\ i^2=-1\right\}$.

הגדרה. עבור $z=x+iy\in\mathbb{C}$, x נקרא **החלק הממשי** של z ($x=\operatorname{Re}z$); y נקרא **החלק המדומה** של z ($y=\operatorname{Im}z$).

לפי הכתיב החדש:

$$\begin{aligned} (x+iy)+(x'+iy') &= (x,y)+(x',y')=(x+x',y+y')= \\ &= (x+x')+i(y+y') \end{aligned}$$

$$\begin{aligned} (x+iy)\cdot(x'+iy') &= (x,y)\cdot(x',y')=(xx'-yy',xy'+x'y)= \\ &= (xx'-yy')+i(xy'+x'y) \end{aligned}$$

כפי שהיה ניתן לצפות, על־פי כללי החשבון הרגילים.[13]

[11] לא ניתן להגיד $\mathbb{R}\subseteq\mathbb{C}$ מכיוון של־$\mathbb{R}$ ול־$\mathbb{C}$ מבנים שונים.
[12] למעשה, יש עוד שורש – $(0,-1)$.
[13] אם i קבוע, $(x+iy)(x'+iy')=xx'+ixy'+iyx'+i^2yy'=(xx'-yy')+i(xy'+x'y)$.

2 מרחבים וקטוריים

2.1 הגדרת מרחב וקטורי

הגדרה. יהי $\mathbb{F}$ שדה. קבוצה[14] V נקראת **מרחב וקטורי** מעל $\mathbb{F}$ אם מרחב וקטורי

א. מוגדרת בתוך V פעולת "חיבור" (מסומנת $+$) המקיימת:

ח־1. לכל $v_1, v_2 \in V$ יש $v_3 \in V$ יחיד כך ש־$v_1 + v_2 = v_3$ (סגירות)

ח־2. לכל $v_1, v_2 \in V$, $v_1 + v_2 = v_2 + v_1$ (קומוטטיביות)

ח־3. לכל $v_1, v_2, v_3 \in V$, $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$ (אסוציאטיביות)

ח־4. קיים איבר $0_V \in V$ כך שלכל $v \in V$, $v + 0_V = v$ (קיום איבר אפס)

ח־5. לכל $v \in V$ קיים איבר שנסמנו $-v \in V$ כך ש־$v + (-v) = 0_V$ (קיום נגדיים)

ב. לכל $v \in V$ ולכל $\alpha \in \mathbb{F}$ מוגדר $a \cdot v \in V$. פעולה זו נקראת כפל בסקלר, ומתקיים, לכל $v_1, v_2 \in V$, $\alpha, \beta \in \mathbb{F}$:

כ־1. $\alpha v_1 \in V$ (סגירות)

כ־2. $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2$

כ־3. $(\alpha + \beta)v_1 = \alpha v_1 + \beta v_1$ (דיסטריבוטיביות)

כ־4. $1_{\mathbb{F}} \cdot v_1 = v_1$ (קיום סקלר יחידה)

כ־5. $(\alpha\beta) \cdot v_1 = \alpha(\beta \cdot v_1)$ (אסוציאטיביות)

דוגמה. ניקח $\mathbb{F} = \mathbb{R}$, $V = \mathbb{R}^n = \{(x_1, \ldots, x_n) \mid \forall i = 1 \ldots n \quad x_i \in \mathbb{R}\}$ (אוסף ה־n־יות).

נגדיר חיבור רכיב־רכיב. ניתן לראות שח־1, ח־2, ח־3 מתקיימות, על־פי קיומן ב־$\mathbb{R}$. איבר האפס: $(0, \ldots, 0)$. איבר נגדי: $-(x_1, \ldots, x_n) = (-x_1, \ldots, -x_n)$.

נגדיר כפל בסקלר רכיב־רכיב. נבדוק, למשל, את כ־2 (השאר כתרגיל): יהיו $\alpha \in \mathbb{R}$, $v_1 = (x_1, \ldots, x_n)$, $v_2 = (y_1, \ldots, y_n)$. אז

$$
\begin{aligned}
\alpha(v_1 + v_2) &= \alpha(x_1 + y_1, \ldots, x_n + y_n) \\
&= (\alpha(x_1 + y_1), \ldots, \alpha(x_n + y_n)) \\
&= (\alpha x_1 + \alpha y_1, \ldots, \alpha x_n + \alpha y_n) \\
&= (\alpha x_1, \ldots, \alpha x_n) + (\alpha y_1, \ldots, \alpha y_n) \\
&= \alpha(x_1, \ldots, x_n) + \alpha(y_1, \ldots, y_n) = \alpha v_1 + \alpha v_2
\end{aligned}
$$

ניתן להכליל דוגמה זו עבור $\mathbb{F}$ שדה כלשהו ו־$V = \mathbb{F}^n$, כאשר החיבור והכפל בסקלר מוגדרים רכיב־רכיב, בדיוק כמו ב־$\mathbb{R}^n$. בפרט, על כל שדה ניתן להסתכל כמרחב וקטורי מעל עצמו, כאשר החיבור הוקטורי הוא החיבור של השדה והכפל בסקלר הוא הכפל בשדה (למשל, $\mathbb{F} = V = \mathbb{R}$).

[14] לא בהכרח שדה.

דוגמה.

דוגמה. $\mathbb{C}$ הוא מרחב וקטורי מעל $\mathbb{R}$. החיבור – החיבור הרגיל ב־$\mathbb{C}$; הכפל בסקלר – כפל מתוך $\mathbb{R}$ ($\alpha(x+iy) = \alpha x + i\alpha y$).

דוגמה. $V = \{0, 1, a, a+1\}$, $\mathbb{F} = \mathbb{Z}_2 = \{0, 1\}$. ($\operatorname{char} V = 2$).

$+$	0	1	a	$a+1$
0	0	1	a	$a+1$
1	1	0	$a+1$	a
a	a	$a+1$	0	1
$a+1$	$a+1$	a	1	0

$\cdot$	0	1	a	$a+1$
0	0	0	0	0
1	0	1	a	$a+1$

12.11.2006

דוגמה. $V = \mathbb{R}^3 = \{(\alpha_1, \alpha_2, \alpha_3) \mid \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}\}$ עם פעולת חיבור חדשה $(\alpha_1, \alpha_2, \alpha_3) \oplus (\beta_1, \beta_2, \beta_3) = (\alpha_1\beta_1, \alpha_2\beta_2, \alpha_3\beta_3)$ ופעולת הכפל בסקלר $\lambda \odot (\alpha_1, \alpha_2, \alpha_3) = (\alpha_1^\lambda, \alpha_2^\lambda, \alpha_3^\lambda)$ ($\lambda \in \mathbb{R}$).

דוגמה. אוסף כל הפונקציות $L = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$ עם פעולת החיבור $(f_1 + f_2)(x) = f_1(x) + f_2(x)$ ופעולת הכפל בסקלר $(\lambda f)(x) = \lambda f(x)$ ($\lambda \in \mathbb{R}$).

2.2 תכונות מרחב וקטורי

תכונות מרחב וקטורי

יהי V מרחב וקטורי מעל שדה $\mathbb{F}$.

א. ב־V יש איבר אפס יחיד; סימונו 0_V או $\vec{0}$.

ב. לכל $\vec{v} \in V$ יש איבר נגדי יחיד.

ג. לכל $\lambda \in \mathbb{F}$, $\lambda \cdot \vec{0} = \vec{0}$.

ד. לכל $\vec{v} \in V$, $0 \cdot \vec{v} = \vec{0}$.

ה. לכל $\vec{v} \in V$, $-1 \cdot \vec{v} = -\vec{v}$.

ו. לכל $\vec{u}, \vec{v} \in V$, $-(\vec{u} + \vec{v}) = (-\vec{u}) + (-\vec{v})$.

ז. לכל $\vec{v} \in V$, $-(-\vec{v}) = \vec{v}$.

הוכחה (ג'). יהי $\lambda \in \mathbb{F}$.

$$\lambda\cdot\vec{0} = \lambda(\vec{0}+\vec{0}) = \lambda\cdot\vec{0}+\lambda\cdot\vec{0} \iff \lambda\cdot\vec{0}+(-\lambda\cdot\vec{0}) = \lambda\cdot\vec{0}+\lambda\cdot\vec{0}+(-\lambda\cdot\vec{0}) \iff \vec{0} = \lambda\cdot\vec{0}$$

פעולת החיסור במרחב וקטורי מוגדרת על־ידי $\vec{v} - \vec{u} = \vec{v} + (-\vec{u})$.

2.3 המודל הגיאומטרי של $\mathbb{R}^2$ ושל $\mathbb{R}^3$

את איברי $\mathbb{R}^2$ ניתן לזהות כאוסף הנקודות במישור אם נבחר מערכת צירים קרטזית, או אם נזהה כל נקודה $(x, y) \in \mathbb{R}^2$ עם החץ היוצא מהראשית ומסתיים באותה נקודה. חץ כזה נקרא **וקטור גיאומטרי**. באותו אופן, איברי $\mathbb{R}^3$ יותאמו לוקטורים גיאומטריים במרחב.

כפל בסקלר

יהי $\vec{a}=(\alpha_1,\alpha_2)$ וקטור גיאומטרי ב־$\mathbb{R}^2$. אם $\vec{a}\neq(0,0)$, $\vec{a}$ מגדיר ישר אחד ויחיד במישור – הישר שעובר דרך הראשית ודרך (α_1,α_2). ישר זה נקרא **הישר הנקבע על־ידי** $\vec{a}$.

טענה 16: יהי $\lambda\in\mathbb{R}$, $\vec{b}=\lambda\vec{a}$. הנקודה $\vec{b}$ נמצאת על הישר הנקבע על־ידי $\vec{a}$.

הוכחה. אם $\lambda=0$, $\vec{b}=0\cdot\vec{a}=\vec{0}$. כלומר, $\vec{b}$ היא הראשית ולכן נמצאת על הישר שקובע $\vec{a}$.

אם $\lambda\neq 0$, $\vec{b}\neq\vec{0}$. נכתוב $\vec{a}=(\alpha_1,\alpha_2)$, $\vec{b}=(\beta_1,\beta_2)$. נניח $\alpha_1\neq 0$. נסמן את הזווית בין $\vec{a}$ ל־$(1,0)$ θ ואת הזווית בין $\vec{b}$ ל־$(1,0)$ φ.

$\vec{b}=\lambda\vec{a}=(\lambda\alpha_1,\lambda\alpha_2)$ ולכן $\tan\theta=\frac{\alpha_2}{\alpha_1}=\frac{\lambda\alpha_2}{\lambda\alpha_1}=\frac{\beta_2}{\beta_1}=\tan\varphi$. מכאן, $\varphi=\theta$ או $\varphi=\theta+\pi$. במקרה הראשון, $\vec{a}$, $\vec{b}$ באותו צד של הראשית, על אותו ישר; במקרה השני, $\vec{a}$, $\vec{b}$ מצדדים שונים של הראשית, על אותו ישר. (אם $\lambda<0$, $\varphi=\theta+\pi$.)

במקרה ש־$\alpha_1=0$, $\vec{a}$ על ציר ה־y, ולכן $\vec{b}=\lambda\vec{a}$ גם־כן על ציר ה־y.

הראינו שכל נקודה מהצורה $\lambda\vec{a}$ נמצאת על הישר ש־$\vec{a}$ קובע. ניתן להראות שגם ההיפך נכון – כלומר, כל נקודה שנמצאת על הישר ש־$\vec{a}$ קובע היא מהצורה $\lambda\vec{a}$. $\{\lambda\vec{a}\mid\lambda\in\mathbb{R}\}$ היא **הצגה פרמטרית** של הישר הנקבע על־ידי $\vec{a}$.

חיבור

יהיו $\vec{a},\vec{b}\in\mathbb{R}^2$. נניח ש־$\vec{b}$ אינו נמצא על הישר הנקבע על־ידי $\vec{a}$. נצייר מקבילית אשר שתיים מצלעותיה הן הקטעים המוגדרים על־ידי הוקטורים הגיאומטריים $\vec{a}$ ו־$\vec{b}$. נתבונן באלכסון מקבילית זו, שקצהו האחד בראשית ואת קצהו השני נסמן ב־$\vec{c}$.

טענה 17: $\vec{a}+\vec{b}=\vec{c}$.

הוכחה. נסמן $\vec{a}=(\alpha_1,\alpha_2)$, $\vec{b}=(\beta_1,\beta_2)$, $\vec{c}=(\gamma_1,\gamma_2)$. צ״ל $\gamma_1=\alpha_1+\beta_1$, $\gamma_2=\alpha_2+\beta_2$. נניח שכל הנקודות ברביע הראשון (הכללת ההוכחה – כתרגיל). כיוון ש־$\vec{0a}$ מקביל ל־$\vec{bc}$ ושווה לו, הרי גם היטליהם על ציר ה־x שווים. כלומר, $\alpha_1=\gamma_1-\beta_1$ ומכאן ש־$\gamma_1=\alpha_1+\beta_1$. באופן דומה נקבל $\gamma_2=\alpha_2+\beta_2$. לכן $\vec{c}=\vec{a}+\vec{b}$.

אם $\vec{a}$ ו־$\vec{b}$ קובעים אותו ישר, אז $\vec{b}=\lambda\vec{a}$ ולכן $\vec{a}+\vec{b}=\vec{a}+\lambda\vec{a}=(1+\lambda)\vec{a}$, ואז גם $\vec{c}=\vec{a}+\vec{b}$ נמצא על אותו ישר.

הצגה פרמטרית של $\mathbb{R}^2$

15.11.2006 יהיו $a_1,a_2\in\mathbb{R}^2$ שתי נקודות. נניח כי $\vec{a_2}$ אינה על הישר הנקבע על־ידי $\vec{a_1}$.

טענה 18: לכל $\vec{b}\in\mathbb{R}^2$ יש $\lambda_1,\lambda_2\in\mathbb{R}$ כך ש־$\vec{b}=\lambda_1\vec{a_1}+\lambda_2\vec{a_2}$.

הוכחה. תהי $\vec{b}$ נקודה במישור. נניח תחילה כי $\vec{b}$ אינה על הישרים הנקבעים על־ידי $\vec{a_1}$, $\vec{a_2}$. נעביר דרך $\vec{b}$ מקבילים לישרים הנקבעים על־ידי $\vec{a_1}$, $\vec{a_2}$. נסמן $\vec{a_1'}$, $\vec{a_2'}$ את נקודות החיתוך של

מקבילים אלה עם הישרים הנקבעים על־ידי $\vec{a_1}$, $\vec{a_2}$. כעת, על־פי כלל המקבילית, $\vec{b} = \vec{a_1'} + \vec{a_2'}$. $\vec{a_1'}$ נמצא על הישר הנקבע על־ידי $\vec{a_1}$; $\vec{a_2'}$ נמצא על הישר הנקבע על־ידי $\vec{a_2}$. לכן יש $\lambda_1, \lambda_2 \in \mathbb{R}$ כך ש־$\vec{a_1'} = \lambda_1 \vec{a_1}$, $\vec{a_2'} = \lambda_2 \vec{a_2}$. לכן $\vec{b} = \lambda_1 \vec{a_1} + \lambda_2 \vec{a_2}$.

אם $\vec{b}$ נמצאת על הישר שקובע $\vec{a_1}$, $\vec{b} = \lambda_1 \vec{a_1} + 0 \cdot \vec{a_2}$, ובאופן דומה אם $\vec{b}$ על הישר שקובע $\vec{a_2}$.

הצגה פרמטרית של $\mathbb{R}^3$

יהיו $a_1, a_2 \in \mathbb{R}^3$ כך ש־$\vec{a_1}$, $\vec{a_2}$ אינם קובעים אותו ישר; אז הישרים הנקבעים על־ידי $\vec{a_1}$, $\vec{a_2}$ קובעים מישור ב־$\mathbb{R}^3$ העובר דרך הראשית. ניתן להראות כי כל נקודה $\vec{c} \in \mathbb{R}^3$ הנמצאת במישור זה ניתנת להצגה כ־$\vec{c} = \lambda_1 \vec{a_1} + \lambda_2 \vec{a_2}$.

2.4 תת־מרחבים

2.4.1 הגדרת תת־מרחב

תת־מרחב

הגדרה. יהי V מרחב וקטורי מעל שדה $\mathbb{F}$. תהי $U \subseteq V$. U **תת־מרחב** של V ($U \leq V$) אם U מרחב וקטורי ביחס לפעולות של V.

דוגמה (תת־מרחבים טריוויאליים). $\{0_V\} \leq V$; $V \leq V$.

דוגמה. $u = \{(x_1, x_2, 0) \mid x_1, x_2 \in \mathbb{R}\}$, $V = \mathbb{R}^3 \Longleftarrow U \leq V$.

הוכחה. נראה את קיום התכונות.

1. ח־1. סגירות: צ״ל כי לכל $u_1, u_2 \in U$, $u_1 + u_2 \in U$. $u_1 = (x_1, x_2, 0)$, $u_2 = (y_1, y_2, 0)$, ואכן $u_1 + u_2 = (x_1 + y_1, x_2 + y_2, 0) \in U$.
2. ח־2. קומוטטיביות: נובעת בירושה מ־V.
3. ח־3. אסוציאטיביות: נובעת בירושה מ־V.
4. ח־4. קיום איבר אפס: $0 = (0,0,0) \in U$.
5. ח־5. קיום איברים נגדיים: $u = (x_1, x_2, 0) \in U \Leftarrow -u = (-x_1, -x_2, 0) \in U$.
6. כ־1. סגירות: אם $u = (x_1, x_2, 0) \in U$, $\lambda \in \mathbb{R}$, אז $\lambda u = (\lambda x_1, \lambda x_2, 0) \in U$.
7. כ־3,2. דיסטריבוטיביות: נובעת בירושה מ־V.
8. כ־4. קיום סקלר יחידה: $1_{\mathbb{F}} \cdot u = u$. נובע בירושה מ־$V$.
9. כ־5. אסוציאטיביות: $(\lambda\alpha)u = \lambda(\alpha u)$. נובעת בירושה מ־$V$.

2.4.2 קריטריון לקיום תת־מרחב

ניתן לראות, על־פי הדוגמה, שבהינתן מרחב וקטורי V מעל $\mathbb{F}$ וקבוצה $U \subseteq V$ מספיק שיתקיימו ארבעה תנאים בלבד על־מנת שיתקיים $U \leq V$:

ח־1. $\forall u_1, u_2 \in U\ u_1 + u_2 \in U$

כ־1. $\forall u \in U, \lambda \in \mathbb{F}\ \lambda u \in U$

ח־4. $0_V \in U$

ח־5. $\forall u \in U\ -u \in U$

נוכל לצמצם את הדרישות האלו אם נשים לב שאם תנאי כ־1 נתון, ח־5 נובע ממנו – יהי $u \in U$. אז $-u = -1_{\mathbb{F}} \cdot u \in U$. בנוסף, אם $U \neq \varnothing$ וכ־1 נתון, ח־4 מתקיים: יהי $u \in U$ (קיים, כי $U \neq \varnothing$). ניקח $\lambda = 0$ ונקבל $\lambda u = 0 \cdot u = 0 \in U$. נסכם:

יהי V מרחב וקטורי מעל $\mathbb{F}$. תהי $U \subseteq V$. אז $U \leq V$ אם קריטריון לקיום תת־מרחב

א. $U \neq \varnothing$

ב. $\forall u_1, u_2 \in U, u_1 + u_2 \in U$

ג. $\forall u \in U, \lambda \in \mathbb{F}\ \lambda u \in U$

דוגמה. $V = \mathbb{R}^n$, $U = \left\{ (x_1, \ldots, x_n) \mid \begin{smallmatrix} x_i \in \mathbb{R} \\ \sum x_i = 0 \end{smallmatrix} \right\}$.

דוגמה. $V = \mathbb{R}^3$, $v_0 \in V$, $U = \{\lambda v_0 \mid \lambda \in \mathbb{R}\}$.

דוגמה. $V = \mathbb{R}^3$, $v_0, v_1 \in \mathbb{R}^3$, $U = \{\alpha v_0 + \beta v_1 \mid \alpha, \beta \in \mathbb{R}\}$.

2.4.3 תת־מרחב הנפרש על־ידי קבוצה

19.11.2006 יהי V מרחב וקטורי מעל שדה $\mathbb{F}$. תהי $\varnothing \neq K \subseteq V$. K אינה בהכרח תת־מרחב: למשל, $V = \mathbb{R}^3$, $K = \{(1, 2, 3)\}$. אבל $K = \{\lambda(1, 2, 3) \mid \lambda \in \mathbb{R}\}$ תת־מרחב של $\mathbb{R}^3$.

הגדרה. יהי V מרחב וקטורי מעל $\mathbb{F}$, $V \supseteq K = \{v_1, \ldots, v_n\} \neq \varnothing$[15]. נגדיר $\operatorname{span} K = \{\lambda_1 v_1 + \ldots + \lambda_n v_n \mid \lambda_i \in \mathbb{F}\}$ – **הנפרש** של K. נפרש של קבוצה

מקובל להגדיר $\operatorname{span} \varnothing = \{0\}$.

דוגמה. $K = \{(1, 2), (2, 9)\}$.

$$\operatorname{span} K \begin{array}{|c|} \hline (1,2) = 1(1,2) + 0(2,9) \\ (2,9) = 0(1,2) + 1(2,9) \\ (7,24) = 3(1,2) + 2(2,9) \\ \ldots \\ \hline \end{array}$$

[15] הנחנו ש־K קבוצה סופית, לשם השפטות. זה לא הכרח.

משפט 19: יהי V מרחב וקטורי מעל $\mathbb{F}$. תהי $\varnothing \neq \{v_1, \dots, v_n\} = K \subseteq V$. אז:

א. $\operatorname{span} K \leq V$

ב. $K \subseteq \operatorname{span} K$

ג. אם $W \leq V$, $K \subseteq W$ אז $\operatorname{span} K \subseteq W$ (כלומר, $\operatorname{span} K$ הוא המינימלי המקיים את התכונות א' וב').

הוכחה. ב. אם $v \in K$, יש $i \in 1, \dots, n$ כך ש־$v = v_i$, ואז $v = 0 \cdot v_1 + \ldots + 0 \cdot v_{i-1} + 1 \cdot v_i + 0 \cdot v_{i+1} + \ldots + 0 \cdot v_n$.

א. $\operatorname{span} K \neq \varnothing$, כי $\operatorname{span} K \overset{\text{ב'}}{\supseteq} K \neq \varnothing$. סגירות לחיבור: יהיו $x_1, x_2 \in \operatorname{span} K$.

$x_1 \in \operatorname{span} K \Longleftarrow x_1 = \alpha_1 v_1 + \ldots + \alpha_n v_n$ ($\alpha_i, \beta_i \in \mathbb{F}$)

$x_2 \in \operatorname{span} K \Longleftarrow x_2 = \beta_1 v_1 + \ldots + \beta_n v_n$

לכן $x_1 + x_2 = (\alpha_1 + \beta_1) v_1 + \ldots + (\alpha_n + \beta_n) v_n \in \operatorname{span} K$.

סגירות לכפל בסקלר: יהי $x \in \operatorname{span} K$, $\lambda \in \mathbb{F}$. ניתן לכתוב $x = \sum_{i=1}^{n} \alpha_i v_i$. כעת,

$\lambda x = \lambda \sum_{i=1}^{n} \alpha_i v_i = \sum_{i=1}^{n} (\lambda \alpha_i) v_i \in \operatorname{span} K$

ג. יהי $W \leq V$, $K \subseteq W$. נוכיח $spnK \subseteq W$.

יהי $x \in \operatorname{span} K \Longleftarrow x = \alpha_1 v_1 + \ldots + \alpha_n v_n$ ($\alpha_i \in \mathbb{F}$). אבל הרי $v_1, \dots, v_n \in K \subseteq W$, ו־$W$ תת־מרחב – סגור לחיבור ולכפל בסקלר. מכאן, $x \in W$.

הגדרה. אם $V = \operatorname{span} K$, אומרים ש־$K$ **פורשת** את V.　קבוצה פורשת

דוגמה. כל קבוצה K פורשת את $\operatorname{span} K$.

דוגמה. עבור $K = \{e_1, e_2, e_3\}$, $\operatorname{span} K = \mathbb{R}^3$.

הוכחה. נראה הכלה הדדית. $\operatorname{span} K \subseteq \mathbb{R}^3$: $K \subseteq \mathbb{R}^3$. על־פי משפט קודם, כיוון ש־$\mathbb{R}^3$ מרחב וקטורי המכיל את K, הוא מכיל גם את $\operatorname{span} K$.

$\mathbb{R}^3 \subseteq \operatorname{span} K$: יהי $x = (\alpha_1, \alpha_2, \alpha_3) \in \mathbb{R}^3$. אז ניתן לכתוב

$x = \alpha_1 (1,0,0) + \alpha_2 (0,1,0) + \alpha_3 (0,0,1) = \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 \in \operatorname{span} K$.

2.5 צירופים לינאריים

הגדרה. יהי V מרחב וקטורי מעל שדה $\mathbb{F}$. יהיו $v_1, \dots, v_k \in V$. סכום מהטיפוס $\sum_{i=1}^{k} \alpha_i v_i = a_1 v_1 + \ldots + a_k v_k$ ($\forall i \in \mathbb{N}\ \alpha_i \in \mathbb{F}$) נקרא **צירוף לינארי** של הוקטורים $v_1, \dots, v_k$.　צירוף לינארי

דוגמה. $v_1 = (2,4), v_2 = (3,1) \in \mathbb{R}^2$. $7v_1 - \pi v_2 = (14 - 3\pi, 28 - \pi)$ צירוף לינארי של v_1 ו־v_2.

דוגמה. נסמן $e_1 = (1,0,0), e_2 = (0,1,0), e_3 = (0,0,1) \in \mathbb{R}^3$. כל וקטור ב־$\mathbb{R}^3$ הוא צירוף לינארי של e_1, e_2, e_3, כי אם $v = (\alpha_1, \alpha_2, \alpha_3)$ נקבל $v = \alpha_1 (1,0,0) + \alpha_2 (0,1,0) + \alpha_3 (0,0,1) = \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3$.

יש לשים לב שצירוף לינארי הוא צירוף של מספר סופי של וקטורים.

וקטור האפס הוא צירוף לינארי של כל k וקטורים מתוך V (ניתן לכתוב $0 = 0\cdot v_1 + \ldots + 0\cdot v_k$).

תלות לינארית

הגדרה. יהי V מרחב וקטורי מעל $\mathbb{F}$. אם $v \in V$ צירוף לינארי של $v_1, \ldots, v_k$, v **תלוי לינארית** ב־$v_1, \ldots, v_k$.

הגדרה. יהי V מרחב וקטורי מעל $\mathbb{F}$. $\varnothing \neq K = \{v_1, \ldots, v_k\}$ **תלויה לינארית** אם אחד מאיבריה תלוי לינארית בחבריו (כלומר, קיים $v_i \in K$ כך ש־$v_i = \alpha_1 v_1 + \ldots + \alpha_{i-1}v_{i-1} + \alpha_{i+1}v_{i+1} + \ldots + \alpha_k v_k$, $\alpha_i \in \mathbb{F}$).[16]

דוגמה. $K = \{(1,2),(3,4),(-5,-6)\}$ תלויה לינארית: $(-5,-6) = 1(1,2) + (-2)(3,4)$.

נשים לב שוקטור האפס הופך כל קבוצה שהוא בתוכה לתלויה.

צירופים לינאריים מתאפסים

הגדרה. הביטוי $\alpha_1 v_1 + \ldots + \alpha_k v_k = 0$ נקרא **צירוף לינארי מתאפס**. אם כל המקדמים הם 0, נאמר שזהו **צירוף מתאפס טריוויאלי**.

22.11.2006

תלות לינארית: הגדרה שקולה

משפט 20: קבוצה $B = \{v_1, \ldots, v_k\}$ תלויה לינארית אם ורק אם יש בה צירוף לינארי מתאפס שאינו טריוויאלי.

הוכחה. נניח ש־B תלויה לינארית. אז יש וקטור $v_i \in B$ שהוא צירוף לינארי של חבריו. כלומר, $v_i = \alpha_1 v_1 + \ldots + \alpha_{i-1}v_{i-1} + \alpha_{i+1}v_{i+1} + \ldots + \alpha_k v_k$. לכן $\alpha_1 v_1 + \ldots + \alpha_{i-1}v_{i-1} - 1v_i + \alpha_{i+1}v_{i+1} + \ldots + \alpha_k v_k = 0$. זהו צירוף לינארי מתאפס כאשר לא כל המקדמים הם 0. כלומר, זהו צירוף לינארי שאינו טריוויאלי.

מצד שני, נניח שיש צירוף לינארי מתאפס שאינו טריוויאלי $\alpha_1 v_1 + \ldots + \alpha_k v_k = 0$. בלי הגבלת הכלליות, נניח ש־$\alpha_1 \neq 0$, ואז $v_1 = -\frac{\alpha_2}{\alpha_1}v_2 - \ldots - \frac{\alpha_k}{\alpha_1}v_k$. v_1 ניתן להצגה כצירוף לינארי של חבריו, ולכן B תלויה.

אי־תלות לינארית

הגדרה. קבוצה B נקראת **בלתי־תלויה לינארית** אם היא אינה תלויה – כלומר, אם אין בה וקטור שתלוי לינארית בחבריו – כלומר, אם כל צירוף לינארי מתאפס של איברי הקבוצה הוא טריוויאלי ($\alpha_1 v_1 + \ldots + \alpha_k v_k = 0 \Longrightarrow \alpha_1 = \ldots = \alpha_k = 0$).

דוגמה. הוכח כי $B = \{(1,0,1,0),(0,1,0,0),(0,1,1,1),(0,0,0,1)\}$ בת״ל.

הוכחה. נסמן את הוקטורים ב־B ב־v_i לפי הסדר. כעת נניח שמתקיים $\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 + \alpha_4 v_4 = (0,0,0,0)$ ונוכיח $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = 0$.

ובכן, נניח $(0,0,0,0) = \alpha_1(1,0,1,0) + \alpha_2(0,1,0,0) + \alpha_3(0,1,1,1) + \alpha_4(0,0,0,1)$.

אז $(\alpha_1, \alpha_2+\alpha_3, \alpha_1 + = (\alpha_1,0,\alpha_1,0)+(0,\alpha_2,0,0)+(0,\alpha_3,\alpha_3,\alpha_3)+(0,0,0,\alpha_4)$

[16] מספיק שיהיה איבר אחד בקבוצה שתלוי בחבריו; לא תמיד כל איבר יהיה תלוי בחבריו.

$\alpha_3, \alpha_3+\alpha_4) = (0,0,0,0)$. לכן, כנדרש: $\alpha_4 = 0 \Longleftarrow \alpha_2 = 0 \Longleftarrow \alpha_3 = 0 \Longleftarrow \alpha_1 = 0$.
$\square$

דוגמה. $B = \{(1,0),(0,1),(1,1)\}$ תלויה לינארית.

הוכחה. $\alpha_1(1,0) + \alpha_2(0,1) + \alpha_3(1,1) = (0,0) \Longrightarrow \alpha_1 + \alpha_3 = 0 \wedge \alpha_2 + \alpha_3 = 0$.
נבחר $\alpha_3 = -1$; אז $\alpha_1 = \alpha_2 = -\alpha_3 = -1$, ו־$1(1,0) - 1(0,1) + 1(1,1) = (0,0)$.

דוגמה. $\varnothing$ בת״ל. (מתקיים, באופן ריק, שכל צירוף לינארי מתאפס של איברי $\varnothing$ טריוויאלי.)

למה 21 (סגירת הדלת[17]): יהי V מרחב וקטורי מעל $\mathbb{F}$. יהיו $v_1, \ldots, v_k \in V$ כך שהקבוצה $\{v_1, \ldots, v_{k-1}\}$ בלתי־תלויה לינארית. אז $\{v_1, \ldots, v_k\}$ תלויה לינארית אס״ם v_k הוא צירוף לינארי של $v_1, \ldots, v_{k-1}$.[18]

דוגמה. $v_1 = (1,0), v_2 = (0,1), v_3 = (1,1)$: הקבוצה $\{v_1, v_2\}$ בלתי־תלויה, אך $\{v_1, v_2, v_3\}$ כבר תלויה.

הוכחה. אם $k = 1$, $\{v_1, \ldots, v_{k-1}\} = \varnothing$. אם $v_k = v_1 = 0$, קיבלנו $\{0\}$ וזו קבוצה שתלויה לינארית באיברי $\varnothing$ על־פי הגדרה (כי $\operatorname{span}\varnothing = \{0\}$). אם $v_1 \neq 0$, $\{v_1\}$ אינה תלויה לינארית.

כעת נוכל להניח ש־$k \geq 2$. נניח ש־v_k צירוף לינארי של $v_1, \ldots, v_{k-1}$. אז הקבוצה $\{v_1, \ldots, v_k\}$ בוודאי תלויה לינארית.

מצד שני, אם הקבוצה $\{v_1, \ldots, v_k\}$ תלויה, יש $\alpha_1, \ldots, \alpha_k \in \mathbb{F}$ לא כולם אפסים כך ש־$\alpha_1 v_1 + \ldots + \alpha_k v_k = 0$. נטען שבהכרח $\alpha_k \neq 0$; אחרת, נקבל $\alpha_1 v_1 + \ldots + \alpha_{k-1} v_{k-1} = 0$ כשלא כל המקדמים אפסים, וזו סתירה לאי־תלות הוקטורים האלו. אז נוכל לכתוב $v_k = -\frac{\alpha_1}{\alpha_k} v_1 - \ldots - \frac{\alpha_{k-1}}{\alpha_k} v_{k-1}$ – כלומר, v_k צירוף לינארי של חבריו, ולכן הקבוצה תלויה.

26.11.2006

למה 22 (למת הקודמים): יהי V מרחב וקטורי וכן $v_1, \ldots, v_k \in V$. $v_1, \ldots, v_k$ תלויים לינארית אס״ם קיים $1 \leq j \leq k$ כך ש־v_j צ״ל של קודמיו.

הוכחה. נניח שקיים $1 \leq j \leq k$ כך ש־v_j צ״ל של קודמיו. אז, לפי ההגדרה, $v_1, \ldots, v_k$ ת״ל.

מצד שני, נניח ש־$v_1, \ldots, v_k$ תלויים לינארית. נסמן ב־j את האינדקס הקטן ביותר עבורו $v_1, \ldots, v_j$ ת״ל. (בוודאי קיים j כזה, שהרי הוקטורים תלויים.) כיוון ש־j מינימלי, הרי $v_1, \ldots, v_{j-1}$ בת״ל. לכן, לפי למת סגירת הדלת, כיוון ש־$v_1, \ldots, v_{j-1}$ בת״ל ו־$v_1, \ldots, v_j$ ת״ל, v_j צירוף לינארי של $v_1, \ldots, v_{j-1}$. $\square$

[18]כלומר, אם $k-1$ הוקטורים הראשונים בקבוצה בלתי־תלויים, כדי שהקבוצה תהיה תלויה הוקטור האחרון חייב להיות תלוי באחרים. (תלויות נוספות יכולות להיווצר במקרה זה, אבל זה לא רלוונטי.)

2.6 בסיסים

נתבונן בוקטורים $B=\{(1,2),(2,3),(3,5)\}$ ב־$\mathbb{R}^2$. כל וקטור במישור הוא צירוף לינארי של $(1,2)$, $(2,3)$, כיוון ששני אלה אינם על אותו ישר. אולם $(3,5)\in\operatorname{span}\{(1,2),(2,3)\}$, לכן גם $B\setminus\{(3,5)\}$ פורשת את $\mathbb{R}^2$. אם נוותר גם על $(2,3)$, למשל, ניוותר עם $(1,2)$, שפורש את הישר $\{t(1,2)\mid t\in\mathbb{R}\}$ ולא את $\mathbb{R}^2$ – על $(3,5)$ יכולנו לוותר כיוון שהוא צ״ל של איברי $B\setminus\{(3,5)\}$.

הגדרה. יהי V מרחב וקטורי. $B\subseteq V$ נקראת **בסיס** של V אם בסיס

א. B בת״ל;

ב. B פורשת את V ($\operatorname{span}B=V$).

משפט 23: V מרחב וקטורי; $B\subseteq V$ היא בסיס של V אס״ם לכל $v\in V$ יש הצגה יחידה כצ״ל של איברי B (כלומר, אם כאשר $B=\{v_1,\dots,v_n\}$ $v=\alpha_1v_1+\ldots+\alpha_nv_n$ ו־$v=\beta_1v_1+\ldots+\beta_nv_n$, בהכרח $\alpha_1=\beta_1,\dots,\alpha_n=\beta_n$).

דוגמה. $V=\mathbb{R}^3$. נבחר $B=\{e_1=(1,0,0),e_2=(0,1,0),e_3=(0,0,1)\}$. ניקח $v=(\alpha_1,\alpha_2,\alpha_3)\in\mathbb{R}^3$.

$$v=(\alpha_1,\alpha_2,\alpha_3)=(\alpha_1,0,0)+(0,\alpha_2,0)+(0,0,\alpha_3)=$$
$$=\alpha_1(1,0,0)+\alpha_2(0,1,0)+\alpha_3(0,0,1)=\alpha_1e_1+\alpha_2e_2+\alpha_3e_3$$

ההצגה יחידה:

$$(\alpha_1,\alpha_2,\alpha_3)=\beta_1e_1+\beta_2e_2+\beta_3e_3=$$
$$=\beta_1(1,0,0)+\beta_2(0,1,0)+\beta_3(0,0,1)=(\beta_1,0,0)+(0,\beta_2,0)+(0,0,\beta_3)=$$
$$=(\beta_1,\beta_2,\beta_3)\Longrightarrow\alpha_1=\beta_1,\alpha_2=\beta_2,\alpha_3=\beta_3\qquad\square$$

הוכחה. נניח ש־B בסיס. לכן B פורשת את V. מכאן, לכל וקטור $v\in V$ יש הצגה כצ״ל של איברי B. נוכיח כי ההצגה יחידה. ניקח $v\in V$ כך ש־$\alpha_1v_1+\ldots+\alpha_nv_n=v=\beta_1v_1+\ldots+\beta_nv_n$. לכן $(\alpha_1-\beta_1)v_1+\ldots+(\alpha_n-\beta_n)v_n=0$. זה צ״ל מתאפס של איברי B; כיוון ש־B בת״ל, הרי המקדמים מתאפסים – $\alpha_i-\beta_i=0\Longleftarrow\alpha_i=\beta_i$.

מצד שני, נניח שלכל וקטור יש הצגה יחידה ונוכיח כי B בסיס. על־פי ההנחה, לכל $v\in V$ יש הצגה כצ״ל של איברי B, ולכן B פורשת. נותר להראות ש־B בת״ל. יהי $\alpha_1v_1+\ldots+\alpha_nv_n=0$ צ״ל מתאפס של איברי B. נכתוב $\alpha_1v_1+\ldots+\alpha_nv_n=0v_1+\ldots+0v_n$. קיבלנו שתי הצגות של 0 כצ״ל של איברי B, ולכן על־פי ההנחה ההצגות שוות והמקדמים שווים – כלומר, $\alpha_1=\ldots=\alpha_n=0$. $\square$

משפט 24 (המשפט הכבד): יהיו $w_1,\dots,w_n\in\operatorname{span}\{v_1,\dots,v_m\}$. אם $n>m$, הקבוצה $\{w_1,\dots,w_n\}$ תלויה לינארית.

הוכחה. נוכיח באינדוקציה על m.

$m=0$: $\operatorname{span}\varnothing=\{0\}$ ולכן $w_1=\ldots=w_n=0$; $\{0\}$ תלויה לינארית.

$m>0$: נניח את נכונות המשפט עבור $m-1$ ונוכיח עבור m. אם $w_1,\dots,w_n\in\operatorname{span}\{v_1,\dots,v_{m-1}\}$, לפי הנחת האינדוקציה $w_1,\dots,w_n$ תלויים לינארית וגמרנו. לכן נניח

שלפחות את אחד מהוקטורים w_i לא ניתן להציג כצירוף לינארי של $v_1, \ldots, v_{m-1}$; בלי הגבלת הכלליות, נניח שזו w_n. נציג את הוקטורים כ־ $w_i = c_{i1}v_1 + \ldots + c_{im}v_m$ ($i = 1 \ldots n$) כאשר $c_{nm} \neq 0$ (אחרת $w_n \in \operatorname{span}\{v_1, \ldots, v_{m-1}\}$).

נגדיר וקטורי עזר: $u_i = w_i - \frac{1}{c_{nm}}c_{im}w_n$ ($i = 1 \ldots n-1$). אזי

$$\begin{aligned}
u_1 &= w_1 - \tfrac{1}{c_{nm}}c_{1m}w_n \\
&= c_{11}v_1 + \ldots + c_{1m}v_m - \tfrac{1}{c_{nm}}c_{1m}(c_{n1}v_1 + \ldots + c_{nm}v_m) \\
&= c_{11}v_1 + \ldots + c_{1m}v_m - \tfrac{1}{c_{nm}}c_{1m}c_{n1}v_1 - \ldots - \tfrac{1}{c_{nm}}c_{1m}c_{nm}v_m \\
&= (c_{11} - \tfrac{1}{c_{nm}}c_{1m}c_{n1})v_1 + \ldots + (c_{1m} - \tfrac{1}{c_{nm}}c_{1m}c_{nm})v_m \\
&= (c_{11} - \tfrac{1}{c_{nm}}c_{1m}c_{n1})v_1 + \ldots + (c_{1,m-1} - \tfrac{1}{c_{nm}}c_{1m}c_{n,m-1})v_{m_1} \\
&\in \operatorname{span}\{v_1, \ldots, v_{m-1}\}
\end{aligned}$$

זה נכון לכל u_i ($i = 1 \ldots n-1$). מכאן, הוקטורים $u_1, \ldots, u_{n-1}$ כולם ב־$\operatorname{span}\{v_1, \ldots, v_{m-1}\}$. כיוון ש־$n > m$, הרי $n-1 > m-1$ ועל־פי הנחת האינדוקציה $u_1, \ldots, u_{n-1}$ תלויים לינארית. לכן יש סקלרים $b_1, \ldots, b_{n-1}$ לא כולם אפסים כך ש־$b_1u_1 + \ldots + b_{n-1}u_{n-1} = 0$. נציב ונקבל

$$\begin{aligned}
0 &= b_1u_1 + \ldots + b_{n-1}u_{n-1} \\
&= b_1(w_1 - \tfrac{1}{c_{nm}}c_{1m}w_n) + \ldots + b_{n-1}(w_{n-1} - \tfrac{1}{c_{nm}}c_{n-1,m}w_n) \\
&= b_1w_1 + \ldots + b_{n-1}w_{n-1} - \tfrac{b_1}{c_{nm}}c_{1m}w_n - \ldots - \tfrac{b_{n-1}}{c_{nm}}c_{n-1,m}w_n \\
&= b_1w_1 + \ldots + b_{n-1}w_{n-1} + (-\tfrac{b_1}{c_{nm}}c_{1m} - \ldots - \tfrac{b_{n-1}}{c_{nm}}c_{n-1,m})w_n
\end{aligned}$$

זהו צירוף לינארי מתאפס של $w_1, \ldots, w_n$ שלא כל מקדמיו אפסים. מכאן, $\{w_1, \ldots, w_n\}$ תלויה לינארית. □

משפט 25: יהי V מרחב וקטורי. נניח של־V יש בסיס בעל n וקטורים. אז:

א. כל קבוצת וקטורים ב־V שבה יותר מ־n וקטורים תלויה לינארית.

ב. אין קבוצה בעלת פחות מ־n וקטורים מ־V הפורשת את V.

ג. כל קבוצה בלתי־תלויה המכילה n וקטורים מ־V היא בסיס של V.

ד. כל קבוצה פורשת של V המכילה בדיוק n איברים היא בסיס של V.

ה. בכל בסיס של V יש בדיוק n וקטורים.

הוכחה. א. אם ל־V בסיס בעל n וקטורים, ודאי ש־V נפרש על־ידי n וקטורים; לכן, על־פי המשפט הכבד, כל קבוצה גדולה יותר של וקטורים תלויה לינארית.

ב. נניח שיש קבוצה בעלת פחות מ־n וקטורים שפורשת את V. אז על־פי המשפט הכבד, קבוצה בעלת n איברים כבר תלויה לינארית ועל־כן אינה בסיס, בסתירה לנתון.

ג. תהי K קבוצה בלתי־תלויה המכילה n איברים. כדי לקבל ש־K בסיס, יש להראות ש־K פורשת. ניקח $v \in V$; צ״ל $v \in \operatorname{span} K$. אם $v \in K$ בוודאי $v \in \operatorname{span} K$ וגמרנו. אחרת, נוסיף אותו: $K \cup \{v\}$. זוהי קבוצה בעלת $n+1$ איברים, אבל ל־V יש בסיס בעל n איברים ולכן $K \cup \{v\}$ ת״ל. כיוון ש־K בת״ל, הרי על־ידי למת סגירת הדלת v צ״ל של איברי K – כלומר, $v \in \operatorname{span} K$.

ד. תהי K קבוצה פורשת של V המכילה בדיוק n וקטורים. נניח בשלילה ש־K ת״ל. אזי יש $v \in K$ כך ש־v צ״ל של חבריו. לכן $V = \operatorname{span} K = \operatorname{span}(K \setminus \{v\})$. קיבלנו קבוצה פורשת בת $n-1$ איברים, בסתירה לב׳.

ה. תהי $K = \{v_1, \ldots, v_m\}$ בסיס של V. אם $n > m$, על־פי א׳ כל קבוצה בעלת n וקטורים תלויה לינארית, וזאת בסתירה לנתון שקיימת עבור v קבוצת־בסיס בעלת n וקטורים. אם $n < m$, על־פי ב׳ קבוצה בעלת n איברים אינה פורשת. לכן $n = m$.

29.11.2006

משפט 26: יהי V מרחב וקטורי מעל $\mathbb{F}$. $B \subseteq V$ היא בסיס של V אס״ם B בת״ל מקסימלית.[19]

הוכחה. נניח כי B בסיס. צ״ל כי B בת״ל מקסימלית. ראשית, B בת״ל מתוקף היותה בסיס. נצטרך להוכיח שהיא בלתי־תלויה מקסימלית. תהי $B \subsetneq T \subseteq V$ – אזי ישנו $v \in T$ כך ש־$v \notin B$. כיוון ש־B בסיס, הרי היא פורשת, ולכן $v \in \operatorname{span} B$. לכן $B \cup \{v\}$ היא קבוצה תלויה לינארית. אבל $B \cup \{v\} \subseteq T$, ולכן T גם־כן תלויה לינארית.

מצד שני, נניח כי B בת״ל מקסימלית. צ״ל כי B בסיס. על־פי ההנחה, B כבר בת״ל; נותר להוכיח כי היא פורשת. נניח בשלילה כי ישנו v כך ש־$v \notin \operatorname{span} B$. הקבוצה $B \cup \{v\}$ מכילה ממש את B, ולכן היא תלויה לינארית (שהרי B בת״ל מקסימלית). כיוון ש־B בת״ל ו־$B \cup \{v\}$ כבר תלויה, v תלוי ב־B – משמע v שייך ל־$\operatorname{span} B$, בסתירה להנחה. לכן B פורשת ולכן מהווה בסיס.

משפט 27: יהי V מרחב וקטורי מעל $\mathbb{F}$. $B \subseteq V$ היא בסיס של V אס״ם B פורשת מינימלית.[20]

הוכחה. נניח כי B בסיס – אז בוודאי B פורשת. נרצה להראות שהיא פורשת מינימלית. תהי $T \subsetneq B$. יהי $v \in B \setminus T$. כלומר, v ב־B אך לא ב־T. אם T פורשת, בהכרח $v \in \operatorname{span} T$. אבל זה אומר שיש ב־$B$ וקטור שתלוי בחבריו, וזו סתירה לכך ש־B, בהיותה בסיס, בת״ל.

מצד שני, נניח כי B פורשת מינימלית. צ״ל כי B בסיס. נתון ש־B פורשת; לכן מספיק להראות ש־B בת״ל. אם B אינה בת״ל, יש בה וקטור v שהוא צ״ל של חבריו. נסמן $T = B \setminus \{v\}$. T בהכרח פורשת, כי כל וקטור פרט ל־v ניתן להציג בעזרת v, ו־v עצמו צ״ל של השאר. אבל על־פי הנתון B פורשת מינימלית, ולכן T שמוכלת בה ממש לא יכולה להיות פורשת – סתירה לכך ש־B תלויה.

3.12.2006

הגדרה. V מרחב וקטורי מעל $\mathbb{F}$ נקרא **נוצר סופית** אם יש $B \subseteq V$ סופית כך ש־$V = \operatorname{span} B$. מרחב וקטורי נוצר סופית

על־פי משפט 25ה, אם ל־V בסיס בעל n איברים, כל בסיס של V יכיל בדיוק n איברים. לכן נוכל להגדיר:

[19] B נקראת בת״ל מקסימלית אם כל $T \subseteq V$ שמכילה את B ממש כבר אינה בת״ל – כלומר, אם נוסיף עוד וקטור אחד ל־B, היא כבר תהיה תלויה.

[20] B נקראת פורשת מינימלית אם כל $T \subseteq V$ שמוכלת ב־B ממש כבר אינה פורשת – כלומר, אם נוריד וקטור מ־B, היא כבר לא תפרוש.

מימד **הגדרה.** V מרחב וקטורי מעל $\mathbb{F}$. נניח ש־V נוצר סופית. מספר האיברים בבסיס שלכהו של V נקרא ה**מימד** של V ‏($\dim \mathbb{F}$).

דוגמה. $V = \mathbb{R}^2$; $\dim V = 2$, כי $B = \{(1,0),(0,1)\}$ בסיס של V.

דוגמה. $V = \mathbb{R}^n$; $\dim V = n$, כי $B = \{e_1,\dots,e_n\}$ בסיס של V (כאשר $e_1 = (1,0,\dots,0),\dots,e_n = (0,\dots,0,1)$).

2.7 מרחב הפולינומים

פולינום **הגדרה. פולינום** מעל שדה $\mathbb{F}$ במשתנה x הוא ביטוי מהצורה ($a_i \in \mathbb{F}$) $P(x) = a_0 + a_1x + \dots + a_nx^n$.
מעלת פולינום **מעלת (דרגת) הפולינום** היא המספר הטבעי n הגדול ביותר כך ש־$a_n \neq 0$.[21]
שוויון פולינומים $a_0 + \dots + a_nx^n = b_0 + \dots + b_nx^n \iff a_0 = b_0,\dots,a_n = b_n$

נסמן ב־$F_n[x]$ את אוסף הפולינומים מדרגה $\leq n$:

$$F_n[x] = \{a_0 + a_1x + \dots + a_nx^n \mid a_0,\dots,a_n \in \mathbb{F}\}$$

נגדיר פעולת חיבור בין פולינומים:

$$(a_0 + \dots + a_nx^n) + (b_0 + \dots + b_nx^n) = (a_0+b_0) + \dots + (a_n+b_n)x^n$$

נגדיר פעולת כפל בסקלר: $\lambda \in \mathbb{F}$;

$$\lambda(a_0 + \dots + a_nx^n) = \lambda a_0 + \dots + \lambda a_nx^n$$

$F_n[x]$ מרחב וקטורי מעל $\mathbb{F}$. (הוכחה – כתרגיל.)
נתבונן ב־$\mathbb{R}_2[x]$.

טענה 28: הקבוצה $B = \left\{1, x, x^2\right\}$ בסיס ל־$\mathbb{R}_2[x]$.

הוכחה. מספיק להוכיח שלכל איבר ב־$Re_2[x]$ יש הצגה יחידה כצירוף לינארי של איברי B. ובכן, ניקח $P(x) = a_0 + a_1x + a_2x^2 = a_0 \cdot 1 + a_1 \cdot x + a_2 \cdot x^2$. זהו צירוף לינארי של איברי B.
נניח שיש שתי הצגות: $a_0 \cdot 1 + a_1 \cdot x + a_2 \cdot x^2 = b_0 \cdot 1 + b_1 \cdot x + b_2 \cdot x^2$. על־פי הגדרת שוויון פולינומים, $a_0 = b_0, a_1 = b_1, a_2 = b_2$.
לכן B בסיס של $\mathbb{R}_2[x]$, ולכן $\dim \mathbb{R}_2[x] = 3$.

באופן דומה, $B = \{1, x, \dots, x^n\}$ בסיס של $F_n[x]$, ולכן $\dim \mathbb{F}_n[x] = n+1$.

טענה 29: $C = \left\{1+x, 1-x, x^2\right\}$ בסיס של $\mathbb{R}_2[x]$.

[21] המעלה של $P(x) = 0$ מוגדרת להיות $-\infty$.

הוכחה. כיוון ש־$\dim \mathbb{R}_2[x] = 3$, מספיק לראות ש־C בלתי־תלויה לינארית. ניקח צ"ל מתאפס $\alpha_1(1+x) + \alpha_2(1-x) + \alpha_3 x^2 = 0$ ונוכיח ש־$\alpha_1 = \alpha_2 = \alpha_3 = 0$: $0 = \alpha_1(1+x) + \alpha_2(1-x) + \alpha_3 x^2 = (\alpha_1+\alpha_2)1 + (\alpha_1-\alpha_2)x + \alpha_3 x^2$. זהו צירוף לינארי מתאפס של וקטורי הבסיס B, לכן מקדמיו מתאפסים: $a_1 + a_2 = 0$, $\alpha_1 - \alpha_2 = 0$, $\alpha_3 = 0$ $\Longleftarrow$ $\alpha_1 = 0$ $\Longleftarrow$ $\alpha_2 = 0$.

משפט 30: יהי V מרחב וקטורי נוצר סופית מעל $\mathbb{F}$. יהי $U \le V$. אז

א. U נוצר סופית;

ב. $\dim U \le \dim V$;

ג. $\dim U = \dim V \iff U = V$.

הוכחה. א+ב. תהי $U \le V$. אם $U = \{0\}$, $U = \operatorname{span} \varnothing$ ולכן נוצר סופית ו־$0 = \dim U \le \dim V$. לכן נניח $U \ne \{0\}$. אז קיימת ב־U קבוצה בלתי־תלויה לינארית. כל קבוצה בת"ל ב־U גם בת"ל ב־V (כיוון שכל הוקטורים ב־U נמצאים גם ב־V). אם נסמן $\dim V = n$, ברור שבכל תת־קבוצה בת"ל של U יש לכל־היותר n איברים, לפי המשפט הכבד. מתוך כל תת־הקבוצות הבת"ל של U ניקח את B קבוצה שבה מספר מקסימלי של איברים (זה אפשרי כי n הוא חסם עליון למספר האיברים הבת"ל). כל קבוצת וקטורים מ־U המכילה ממש את B תלויה (אחרת B אינה בעלת מספר מקסימלי של וקטורים בת"ל), ולכן B בת"ל מקסימלית ב־U ולכן בסיס. ב־B יש מספר סופי של איברים, ולכן U נוצר סופית. $\dim U = |B| \le n = \dim V$.

ג'. אם $U = V$, ודאי $\dim U = \dim V$. מצד שני, נניח $\dim U = \dim V = n$. יהי $B = \{u_1, \dots, u_n\}$ בסיס של U. $B \subseteq V$ קבוצה בלתי־תלויה בעלת n איברים; לכן היא בסיס של V. כלומר, $U = \operatorname{span} B = V$.

משפט 31: לכל מרחב וקטורי נוצר סופית V מעל $\mathbb{F}$ יש בסיס.

הוכחה. יהי V מרחב וקטורי נוצר סופית. אם $V = \{0\}$, $V = \operatorname{span} \varnothing$ ו־$\varnothing$ הוא הבסיס. לכן נניח ש־$v \ne \{0\}$. תהי B קבוצת וקטורים יוצרים סופית של V. נוכל להניח ש־$0 \ne B$; אחרת, כיוון שאינו תורם לפרישה, נגרשו לאלתר ("ילד מפה, יא אפס!"). נניח בנוסף $|B| = n$. אם B בלתי־תלויה, B בסיס וגמרנו. אחרת, קיים $u \in B$ שהוא צירוף לינארי של חבריו. נסמן $B_1 = B \setminus \{u\}$. כיוון ש־u ת"ל ב־B, הרי $\operatorname{span} B = \operatorname{span} B_1 = V$. אם B_1 בת"ל, כיוון ש־$\operatorname{span} B_1 = V$, B_1 בסיס וגמרנו. אחרת, קיים וקטור ב־B_1 שתלוי בחבריו. נזרוק אותו וכו'. אחרי לכל־היותר $n-1$ צעדים, ניוותר עם קבוצה בת"ל (שמכילה לפחות וקטור אחד שאינו 0), שמהווה בסיס.

6.12.2006

משפט 32: יהי $V \ne \{0\}$ מרחב וקטורי מעל $\mathbb{F}$. נניח ש־$\dim V = n$. תהי $\{v_1, \dots, v_k\} \subseteq V$ בלתי־תלויה לינארית. אז יש קבוצה $\{d_{k+1}, \dots, d_n\}$ כך ש־$\{v_1, \dots, v_k, d_{k+1}, \dots, d_n\}$ בסיס של V.

הוכחה. אם $k=n$, $\{v_1,\dots,v_k\}$ בסיס.

אם $k<n$, $\{v_1,\dots,v_k\}$ אינה פורשת ואינה בסיס. לכן יש $d_{k+1}\in V$ כך ש־$d_{k+1}\notin \operatorname{span}\{v_1,\dots,v_k\}$ – כלומר, d_{k+1} אינו ת״ל ב־$\{v_1,\dots,v_k\}$. על־פי למת סגירת הדלת, הקבוצה $\{v_1,\dots,v_k,d_{k+1}\}$ בלתי־תלויה לינארית (אחרת, בהכרח d_{k+1} ת״ל ב־$\{v_1,\dots,v_k\}$). אם $k+1=n$, $\{v_1,\dots,v_k,d_{k+1}\}$ מהווה בסיס. אחרת, קיים d_{k+2} שאינו ת״ל ב־$\{v_1,\dots,v_k,d_{k+1}\}$. נצרף אותו וכו'. בדרך זו, נוסיף וקטורים לקבוצה עד שנגיע ל־n וקטורים ונקבל בסיס.

דוגמה. נשלים את $\{w_1=(1,2,-1,4), w_2=(3,-1,-2,2)\}$ לבסיס של $\mathbb{R}^4$.

w_1 ו־w_2 אינם ת״ל. נוסיף לקבוצה את $w_3=e_3=(0,0,1,0)$. w_3 אינו תלוי בקודמיו. נוסיף גם את $w_4=e_4=(0,0,0,1)$. כעת, מכיוון ש־w_1,w_2,w_3,w_4 בת״ל, הקבוצה $\{w_1,w_2,w_3,w_4\}$ מהווה בסיס ל־$\mathbb{R}^4$.

2.8 סכום תת־מרחבים

משפט 33: אם $U,W\le V$ (V מרחב וקטורי), $U\cap W\le V$.

משפט 34: $U\cup W\le V$ אס״ם $U\subseteq W$ או $W\subseteq U$.

דוגמה. נחבר $V=\mathbb{R}^2$, $U=\operatorname{span}\{(1,0)\}$, $W=\operatorname{span}\{(0,1)\}$. אבל נקבל $\overset{\in U\subseteq U\cup W}{(1,0)} + \overset{\in W\subseteq U\cup W}{(0,1)} = (1,1)\notin U\cup W$.

סכום תת־מרחבים

הגדרה. יהיו $U,W\le V$. אז $U+W=\left\{u+w \mid \begin{smallmatrix} u\in U\\ w\in W\end{smallmatrix}\right\}$.

דוגמה.

$$U+W=\left\{u+w \mid \begin{smallmatrix} u\in \operatorname{span}\{(1,0)\}\\ w\in \operatorname{span}\{(0,1)\}\end{smallmatrix}\right\}=$$
$$=\{\lambda_1(1,0)+\lambda_2(0,1) \mid \lambda_1,\lambda_2\in\mathbb{R}\}=\operatorname{span}\{(1,0),(0,1)\}=\mathbb{R}^2$$

משפט 35: V מרחב וקטורי, $U,W\le V$; $U+W$ הוא תת־המרחב המינימלי המכיל את U ואת W.

הוכחה. נוכיח רק ש־$U+W$ הוא המינימלי המכיל את U,W. כלומר, נניח ש־$S\le V$ כך ש־$U\subseteq S$ ו־$W\subseteq S$, ונוכיח $U+W\subseteq S$. יהי $x=\overset{\in U}{u}+\overset{\in W}{w}\in U+W$. $u\in S \Longleftarrow U\subseteq S$ (שהרי $u\in U$); $w\in S\Longleftarrow W\subseteq S$ (שהרי $w\in W$). לכן, כיוון ש־S תת־מרחב, גם $x=u+w\in S$. (ההוכחה ש־$U+W$ תת־מרחב – כתרגיל.)

משפט המימדים 1

משפט 36 (משפט המימדים 1): יהי V מרחב וקטורי מעל $\mathbb{F}$, $U,W\le V$. אז $\dim(U+W)=\dim U+\dim W-\dim(U\cap W)$.

הוכחה. בשלב הראשון נניח כי $U\cap W\neq\{0\}$. נסמן $\dim(U\cap W)=k$, ויהי $\{d_1,\dots,d_k\}$ בסיס של $U\cap W$. נשלים לבסיסים: $\{d_1,\dots,d_k,u_1,\dots,u_m\}$ בסיס של U; $\{d_1,\dots,d_k,w_1,\dots,w_n\}$

בסיס של W. כעת,

$$\dim(U\cap W)=k \quad \dim(U)=k+m \quad \dim(W)=k+n$$

ויש להוכיח ש־$\dim(U+W)=(k+m)+(k+n)-k=k+m+n$.

כל אחד מהוקטורים $u_1,\dots,u_m$ בלתי־תלוי ב־$d_1,\dots,d_k$. לכן מתקיים $u_1,\dots,u_m\notin U\cap W=\operatorname{span}\{d_1,\dots,d_k\}$. עם זאת, $u_1,\dots,u_m\in U$, ולכן $u_1,\dots,u_m\notin W$. באותו אופן, $w_1,\dots,w_n\notin U$. בפרט, כל אחד מהוקטורים u_i ($i=1\dots m$) שונה מכל אחד מהוקטורים w_j ($j=1\dots n$). לכן בקבוצה $B=\{d_1,\dots,d_k,u_1,\dots,u_m,w_1,\dots,w_n\}$ יש $k+m+n$ וקטורים. נותר להוכיח כי B בסיס של $U+W$.

נוכיח תחילה כי B פורשת $U+W$. יהי $x=u+w\in U+W$. כיוון ש־$\{d_1,\dots,d_k,u_1,\dots,u_m\}$ פורשת את U, הרי יש מקדמים α_i, β_j ($i=1\dots k$, $j=1\dots m$) כך שניתן לכתוב $u=\alpha_1d_1+\dots+\alpha_kd_k+\beta_1u_1+\dots+\beta_nu_n$. באופן דומה, יש מקדמים δ_t, ε_r ($t=1\dots k$, $r=1\dots n$) כך שניתן לכתוב $w=\delta_1d_1+\dots+\delta_kd_k+\varepsilon_1w_1+\dots+\varepsilon_nw_n$. לכן $x=u+w=$ $=(\alpha_1d_1+\dots+\alpha_kd_k+\beta_1u_1+\dots+\beta_nu_n)+(\delta_1d_1+\dots+\delta_kd_k+\varepsilon_1w_1+\dots+\varepsilon_nw_n)=$ $=(\alpha_1+\delta_1)d_1+\dots+(\alpha_k+\delta_k)d_k+\beta_1u_1+\dots+\beta_nu_n+\varepsilon_1w_1+\dots+\varepsilon_nw_n$ צירוף לינארי של איברי B, ולכן B פורשת.

10.12.2006 כעת נוכיח אי־תלות לינארית. נניח ש־$\alpha_1d_1+\dots+\alpha_kd_k+\beta_1u_1+\dots+\beta_mu_m+\gamma_1w_1+\dots+\gamma_nw_n=0$. אז

$$U\ni\alpha_1d_1+\dots+\alpha_kd_k+\beta_1u_1+\dots+\beta_mu_m=-\gamma_1w_1-\dots-\gamma_nw_n\in W$$

כיוון שאגף שמאל הוא וקטור ב־U ואגף ימין הוא וקטור ב־W, לפנינו וקטור ב־$U\cap W$. נסמנו ב־v. כיוון ש־$\{d_1,\dots,d_k\}$ בסיס של $U\cap W$, הרי קיימים סקלרים $\delta_1,\dots,\delta_k\in\mathbb{F}$ כך ש־$v=\delta_1d_1+\dots+\delta_kd_k$.

נשווה הצגה זו לאגף ימין: $\delta_1d_1+\dots+\delta_kd_k=-\gamma_1w_1-\dots-\gamma_nw_n \iff \delta_1d_1+\dots+\delta_kd_k+\gamma_1w_1+\dots-\gamma_nw_n=0$ זהו צ״ל מתאפס של איברי הבסיס של W, שכבסיס היא קבוצה בלתי־תלויה – לכן כל המקדמים מתאפסים, ובפרט $\gamma_1=\dots=\gamma_n=0$. כעת, אם נתבונן ב־

$$W\ni\alpha_1d_1+\dots+\alpha_kd_k+\gamma_1w_1+\dots+\gamma_nw_n=-\beta_1u_1-\dots-\beta_mu_m\in U$$

נקבל באותו אופן ש־$\beta_1=\dots=\beta_m=0$. נציב ונקבל $\alpha_1d_1+\dots+\alpha_kd_k=0$. זהו צ״ל מתאפס של איברי הבסיס של $U\cap W$, ולכן $\alpha_1=\dots=\alpha_k=0$.

אם $U\cap W=\{0\}$, ההוכחה פועלת באותו אופן אחרי שמוציאים את $d_1,\dots,d_k$ מהתמונה.

3 העתקות לינאריות

3.1 הגדרת העתקה לינארית

העתקה לינארית

הגדרה. יהיו V ו־W מ"ו מעל אותו שדה $\mathbb{F}$. פונקציה $T:V\to W$ תיקרא **העתקה לינארית** אם T מקיימת –

א. $\forall v_1,v_2\in V\ T(v_1+v_2)=T(v_1)+T(v_2)$

ב. $\forall v\in V,\lambda\in\mathbb{F}\ T(\lambda v)=\lambda T(v)$

דוגמה. $T:\mathbb{R}^3\to\mathbb{R}^2$ מוגדרת על־ידי $T(x,y,z)=(x+y,y-z)$. לדוגמה, $T(1,2,4)=(1+2,2-4)=(3,-2)$. נבדוק שזו אכן העתקה לינארית:

$$\begin{aligned}T((x_1,y_1,z_1)+(x_2,y_2,z_2)) &= T(x_1+x_2,y_1+y_2,z_1+z_2)\\ &= (x_1+x_2+y_1+y_2,y_1+y_2-(z_1+z_2))\\ &= (x_1+y_1,y_1-z_1)+(x_2+y_2,y_2-z_2)\\ &= T(x_1,y_1,z_1)+T(x_2,y_2,z_2)\end{aligned}$$

$$\begin{aligned}T(\lambda(x,y,z)) &= T(\lambda x,\lambda y,\lambda z)\\ &= (\lambda x+\lambda y,\lambda y-\lambda z)\\ &= \lambda(x+y,y-z)\\ &= \lambda T(x,y,z)\end{aligned}$$

דוגמה. $T:\mathbb{R}\to\mathbb{R}$, $T(x)=\sin x$. $T(x+y)=\sin(x+y)$ לא תמיד שווה ל־$\sin x+\sin y$; T אינה העתקה לינארית.

13.12.2006

דוגמה (העתקה ששומרת רק על חיבור). $V=\mathbb{C}$ כמ"ו מעל עצמו. $T:V\to V$ מוגדרת על־ידי $T(\alpha+\beta i)=\alpha$.

חיבור: $T((\alpha_1+\beta_1 i)+(\alpha_2+\beta_2 i))=T((\alpha_1+\alpha_2)+(\beta_1+\beta_2)i)=\alpha_1+\alpha_2=T(\alpha_1+\beta_1 i)+T(\alpha_2+\beta_2 i)$

כפל בסקלר: $T(\overbrace{(a+bi)}^{\lambda}(\alpha+\beta i))=T((a\alpha-b\beta)+(a\beta+b\alpha)i)=a\alpha-b\beta\neq(a+bi)T(\alpha+\beta i)=a\alpha+b\alpha i$

משפט 37: תהי $T:V\to W$ העתקה לינארית. אז –

א. $T(0_V)=0_W$

ב. $\forall v\in V\ T(-v)=-T(v)$

הוכחה. א. $T(0_V)=T(0_V+0_V)=T(0_V)+T(0_V)$ נוסיף לשני האגפים $-T(0_V)$ ונקבל $0_W=T(0_V)+(-T(0_V))=T(0_V)$.

ב. יהי $v \in V$. אז $v + (-v) = 0_V$. מכיוון ש־T העתקה לינארית, נקבל $T(v) + T(-v) = T(v + (-v)) = T(0_V) = 0_W$. בשל יחידות האיבר הנגדי, כיוון ש־$T(-v)$ מתפקד כנגדי של $T(v)$, הרי הוא הנגדי של $T(v)$, ולכן נוכל לכתוב $T(-v) = -T(v)$.

3.2 קריטריון ללינאריות העתקה

משפט 38: V,W מ"ו מעל $\mathbb{F}$. אז $T : V \to W$ העתקה לינארית אס"ם $\forall v_1, v_2 \in V, \lambda_1, \lambda_2 \in \mathbb{F}$ $T(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 T(v_1) + \lambda_2 T(v_2)$. קריטריון ללינאריות העתקה

הוכחה. אם T העתקה לינארית, אז $T(\lambda_1 v_1 + \lambda_2 v_2) = T(\lambda_1 v_1) + T(\lambda_2 v_2) = \lambda_1 T(v_1) + \lambda_2 T(v_2)$.

להיפך, נניח שהקריטריון מתקיים. יהיו $v_1, v_2 \in V$. אז נקבל שמתקיים $T(v_1 + v_2) = T(1_{\mathbb{F}} v_1 + 1_{\mathbb{F}} v_2) = 1_{\mathbb{F}} T(v_1) + 1_{\mathbb{F}} T(v_2) = T(v_1) + T(v_2)$. כעת, יהיו $v \in V$, $\lambda \in \mathbb{F}$. אז $T(\lambda v) = T(\lambda v + 0_{\mathbb{F}} v) = \lambda T(v) + 0_{\mathbb{F}} T(v) = \lambda T(v)$. $\square$

מסקנה 39: יהיו $v_1, \ldots, v_n \in V$, $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$, $T : V \to W$ העתקה לינארית. אז $T(\sum_{i=1}^n \lambda_i v_i) = \sum_{i=1}^n \lambda_i T(v_i)$.

הוכחה. כתרגיל. (באינדוקציה.)

3.3 העתקות מיוחדות

3.3.1 העתקת האפס

V, W מ"ו מעל $\mathbb{F}$. נגדיר $0 : V \to W$ על־ידי $\forall v \in V$ $0(v) = 0_W$. העתקת האפס

למה זו ה"ל? $0(\lambda_1 v_1 + \lambda_2 v_2) = 0_W = \lambda_1 0(v_1) + \lambda_2 0(v_2)$.

3.3.2 העתקת הזהות

V מ"ו מעל $\mathbb{F}$. נגדיר $I : V \to V$ על־ידי $\forall v \in V$ $I(v) = v$. העתקת הזהות

למה זו ה"ל? $I(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 v_1 + \lambda_2 v_2 = \lambda_1 I(v_1) + \lambda_2 I(v_2)$.

3.4 מציאת העתקות לינאריות

משפט 40: יהיו V, W מ"ו מעל $\mathbb{F}$. יהי $B = \{v_1, \ldots, v_n\}$ בסיס של V. אם $S, T : V \to W$ כך שלכל $i = 1 \ldots n$ $S(v_i) = T(v_i)$ אז $S(v) = T(v)$ לכל $v \in V$; כלומר, $S = T$. יחידות העתקה לינארית

הוכחה. יהי $v \in V$. צ"ל $S(v) = T(v)$. כיוון ש־B בסיס, יש $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ (הנקבעים באופן יחיד) כך ש־$v = \alpha_1 v_1 + \ldots + \alpha_n v_n$. אז נקבל

$$\begin{aligned} S(v) &= S(\alpha_1 v_1 + \ldots + \alpha_n v_n) \\ &= \alpha_1 S(v_1) + \ldots + \alpha_n S(v_n) \\ &= \alpha_1 T(v_1) + \ldots + \alpha_n T(v_n) \\ &= T(\alpha_1 v_1 + \ldots + \alpha_n v_n) \qquad = \quad T(v) \end{aligned}$$

משפט 41: יהיו V, W מ"ו מעל $\mathbb{F}$. יהי $B = \{v_1, \ldots, v_n\}$ בסיס של V. יהיו $w_1, \ldots, w_n \in W$.
אז יש T אחת ויחידה שהיא העתקה לינארית מ־V ל־W ומקיימת $T(v_i) = w_i$ ($i = 1 \ldots n$).

דוגמה. כדי למצוא ה"ל $T : \mathbb{R}^3 \to \mathbb{R}^3$ שמקיימת $T(1,3,5) = (1,0,1)$, ניקח בסיס של $\mathbb{R}^3$ שמכיל את $(1,3,5)$ – למשל $\{(1,3,5),(0,1,0),(0,0,1)\}$ – ונגדיר $T(1,3,5) = (1,0,1)$, $T(0,1,0) = (0,0,0)$, $T(0,0,1) = (0,0,0)$. כעת נוכל להסתמך על לינאריות T לשם חישוב $T(1,4,6)$:
$T(1,4,6) = T((1,3,5)+(0,1,0)+(0,0,1)) = T(1,3,5)+T(0,1,0)+T(0,0,1)$.

הוכחה. לכל $v \in V$ יש הצגה יחידה כצירוף לינארי של איברי B - $v = \sum_{i=1}^{n} \alpha_i v_i$. נגדיר $T(v) = \sum_{i=1}^{n} \alpha_i w_i$. כיוון שמקדמי הצירוף הלינארי נקבעים באופן יחיד, הרי הנוסחה ל־$T(v)$ מתאימה לכל v $T(v)$ יחיד. $T(v_i) = w_i$, כנדרש, כי ניתן לכתוב $v_i = 0v_1 + \ldots + 0v_{i-1} + v_i + 0v_{i+1} + \ldots + 0v_n$, ואז, על־פי ההגדרה, $T(v_i) = 0w_1 + \ldots + 0w_{i-1} + w_i + 0w_{i+1} + \ldots + 0w_n = w_i$.

נותר להראות ש־T לינארית. יהיו $u_1, u_2 \in V$; צ"ל $T(u_1 + u_2) = T(u_1) + T(u_2)$. נכתוב $u_1 = \alpha_1 v_1 + \ldots + \alpha_n v_n$, $u_2 = \beta_1 v_1 + \ldots + \beta_n v_n$.

$$\begin{aligned} T(u_1 + u_2) &= T((\alpha_1 v_1 + \ldots + \alpha_n v_n) + (\beta_1 v_1 + \ldots + \beta_n v_n)) \\ &= T((\alpha_1 + \beta_1) v_1 + \ldots + (\alpha_n + \beta_n) v_n) \\ &\overset{\text{הגדרת } T}{=} (\alpha_1 + \beta_1) w_1 + \ldots + (\alpha_n + \beta_n) w_n \\ &= \alpha_1 w_1 + \ldots + \alpha_n w_n + \beta_1 w_1 + \ldots + \beta_n w_n \\ &= T(\alpha_1 v_1 + \ldots + \alpha_n v_n) + T(\beta_1 v_1 + \ldots + \beta_n v_n) \\ &= T(u_1) + T(u_2) \end{aligned}$$

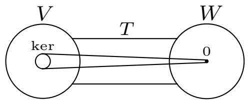
הוכחת שמירה על כפל בסקלר – כתרגיל.

יחידות T נובעת ממשפט 40.

לסיכום, אם $T : V \to W$ העתקה לינארית ו־B בסיס של V, מתוך הכרת ערכי T על וקטורי B נוכל לקבוע חד־משמעית מהו ערכה של T על כל $v \in V$.

3.5 גרעין של העתקה לינארית

גרעין **הגדרה.** תהי $T : V \to W$ ה"ל. נסמן $\ker T = \{v \in V \mid T(v) = 0_W\}$. $\ker T$ הוא **הגרעין** של T. 20.12.2006



דוגמה. $T:\mathbb{R}^3\to\mathbb{R}^3$ מוגדרת על־ידי $T(x,y,z)=(x,y,0)$.

$$\begin{aligned}\ker T &= \left\{(x,y,z)\in\mathbb{R}^3 \mid T(x,y,z)=(0,0,0)\right\}\\ &= \left\{(x,y,z)\in\mathbb{R}^3 \mid (x,y,0)=(0,0,0)\right\}\\ &= \left\{(x,y,z)\in\mathbb{R}^3 \mid x=y=0\right\}\\ &= \left\{(0,0,z)\in\mathbb{R}^3\right\}=\left\{z(0,0,1)\mid z\in\mathbb{R}^3\right\}=\operatorname{span}\left\{(0,0,1)\right\}\end{aligned}$$

משפט 42: תהי $T:V\to W$ ה״ל. אז $\ker T\le V$.

הוכחה. תחילה, $0_v\in\ker T$, כי $T(0_V)=0_W$. יהיו $v_1,v_2\in\ker T$. $T(v_1)=0_W$, $T(v_2)=0_W$, ולכן $T(v_1+v_2)=T(v_1)+T(v_2)=0_W$ ו־$v_1+v_2\in\ker T$. כעת, יהיו $v\in\ker T$, $\lambda\in\mathbb{F}$. אז $T(\lambda v)=\lambda T(v)=\lambda 0_W=0_W$ ו־$\lambda v\in\ker T$. $\square$

3.6 תמונה של העתקה לינארית

תמונה של קבוצה

הגדרה. תהי $T:V\to W$ ה״ל. תהי $K\subseteq V$. נסמן $T(K)=\{T(v)\mid v\in K\}$. $T(K)$ נקראת **התמונה של** K.

דוגמה. $T:\mathbb{R}^2\to\mathbb{R}^2$ מוגדרת על־ידי $T(x,y)=x$. (הוכחה שזו ה״ל – כתרגיל.[22]) $K=\{(1,2),(1,3),(2,4)\}$. אז $T(K)=\{1,2\}$.

משפט 43: תהי $T:V\to W$ העתקה לינארית. אם $K\le V$, $T(K)\le W$.

הוכחה. תחילה, $T(K)\ni 0_W=T(0_V)$ ($0_V\in K$). לכן $T(K)\neq\varnothing$. יהיו $w_1,w_2\in T(K)$; צ״ל $w_1+w_2\in T(K)$.

$w_1\in T(K)\Longleftarrow \exists v_1\in KT(v_1)=w_1$

$w_2\in T(K)\Longleftarrow \exists v_2\in KT(v_2)=w_2$ ולכן $T(v_1+v_2)=T(v_1)+T(v_2)=w_1+w_2$.

אבל $v_1+v_2\in K$, שהרי $K\le V$. קיבלנו $w_1+w_2\in T(K)$. הוכחת סגירות לכפל בסקלר – כתרגיל.

תמונה

הגדרה. תהי $T:V\to W$ ה״ל. $\operatorname{im}T=\{T(v)\mid v\in V\}$ נקראת **התמונה** של T.

על־פי המשפט הקודם, $\operatorname{im}T\le W$.

דוגמה. נחשב את $\operatorname{im}T$ עבור T מהדוגמה הקודמת.

$$\begin{aligned}\operatorname{im}T &= \left\{T(x,y,z)\mid (x,y,z)\in\mathbb{R}^3\right\}\\ &= \{(x,y,0)\mid x,y\in\mathbb{R}\}\\ &= \{x(1,0,0)+y(0,1,0)\mid x,y\in\mathbb{R}\}\\ &= \operatorname{span}\{(1,0,0),(0,1,0)\}\end{aligned}$$

[22] בכל מקרה, זה לא משנה להגדרת התמונה.

נשים לב ש־$\dim\ker T + \dim\operatorname{im} T = \dim V \iff 1+2=3$.

איך מחשבים את $\operatorname{im} T$?

משפט 44: תהי $T : V \to W$ ה״ל. יהי $B = \{v_1, \dots, v_n\}$ בסיס של V. אז $\operatorname{im} T = \operatorname{span}\{T(v_1), \dots, T(v_n)\}$.

דוגמה. נחזור לדוגמה הקודמת. ניקח $B = \{(1,0,0),(0,1,0),(0,0,1)\}$ בסיס של $V = \mathbb{R}^3$. ואכן, $\operatorname{im} T = \operatorname{span}\{T(1,0,0), T(0,1,0), T(0,0,1)\} = \operatorname{span}\{(1,0,0),(0,1,0),(0,0,0)\} = \operatorname{span}\{(1,0,0),(0,1,0)\}$.

הוכחה. נראה הכלה הדדית. יהי $x \in \operatorname{span}\{T(v_1), \dots, T(v_n)\}$. אז

$$x = \sum_{i=1}^{n} \lambda_i T(v_i) = \sum_{i=1}^{n} T(\lambda_i v_i) = T(\sum_{i=1}^{n} \lambda_i v_i) \in \operatorname{im} T$$

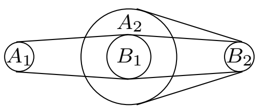
כעת, יהי $x \in \operatorname{im} T$. אז יש $v \in V$ כך ש־$x = T(v)$. כיוון ש־B בסיס, ניתן לכתוב $v = \sum_{i=1}^{n} \alpha_i v_i$, ואז

$$x = T(v) = T(\sum_{i=1}^{n} \alpha_i v_i) = \sum_{i=1}^{n} \alpha_i T(v_i) \in \operatorname{span}\{T(v_1), \dots, T(v_n)\}$$

$\square$

3.7 כמה מילים על פונקציות

נניח ש־$f_1 : A_1 \to B_1$, $f_2 : A_2 \to B_2$. רוצים להגדיר את הפונקציה המורכבת $f_2 \circ f_1$. אם התמונה של f_1 מוכלת בתחום של f_2, נוכל להגדיר את $f_2 \circ f_1$ כ־$(f_2 \circ f_1)(x) = f_2(f_1(x))$. 24.12.2006



הגדרה. פונקציה $f : A \to B$ נקראת **חד־חד ערכית** אם לכל $a_1, a_2 \in A$ $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$ או, באופן שקול, אם $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$. פונקציה חד־חד ערכית

הגדרה. פונקציה $f : A \to B$ נקראת **על** אם לכל $b \in B$ יש $a \in A$ כך ש־$f(a) = b$. פונקציה על

הגדרה. **פונקציית הזהות** $I_A : A \to A$ מוגדרת כך ש־$I_A(a) = a$ $\forall a \in A$. פונקציית הזהות

הגדרה. תהי $f : A \to B$ פונקציה. אם קיימת $g : B \to A$ כך ש־$f \circ g = I_A$ ו־$g \circ f = I_B$ נאמר ש־f **הפיכה**; g נקראת **הפונקציה ההופכית** של f. ניתן להראות שאם קיימת g כזו היא יחידה, ולכן ניתן לסמן $g = f^{-1}$. פונקציה הפיכה, פונקציה הופכית

משפט 45: $f : A \to B$ הפיכה $\iff$ f חח״ע ועל.

הגדרה. V, W מ״ו מעל $\mathbb{F}$. $T : V \to W$ ה״ל נקראת **מונומורפיזם** אם היא חח״ע; **אפימורפיזם** אם היא על; **איזומורפיזם** אם היא חח״ע ועל. (מונו|אפי|איזו)מורפיזם

משפט 46: V, W מ״ו מעל $\mathbb{F}$. $T : V \to W$ ה״ל. T חח״ע $\Leftrightarrow$ $\ker T = \{0_V\}$.

הוכחה. ($\Longleftarrow$) נניח T חח״ע. נניח בשלילה ש־$\ker T \neq \{0_V\}$. אז יש $0_V \neq v \in \ker T$. לכן $T(v) = T(0_V) = 0_W$, ומכאן T אינה חח״ע, בסתירה להנחה.

($\Longrightarrow$) נניח $\ker T = \{0_V\}$ ונוכיח ש־T חח״ע. נניח ש־$T(v_1) = T(v_2)$. מכאן, $T(v_1 - v_2) = T(v_1) - T(v_2) = 0_W$, ולכן $v_1 - v_2 \in \ker T$. אבל $\ker T = \{0_V\}$, ולכן $v_1 - v_2 = 0_V$. מכאן, $v_1 = v_2$.

($T : V \to W$ על $\iff$ $\operatorname{im} T = W$.)

3.8 הרכבת העתקות לינאריות

דוגמה. $T : \mathbb{R}^2 \to \mathbb{R}^2$, $T(x, y) = (x - y, 2x + y)$; $S : \mathbb{R}^2 \to \mathbb{R}^2$, $S(x, y) = (x + 2y, x + y)$. ההעתקה $T \circ S : \mathbb{R}^2 \to \mathbb{R}^2$ מוגדרת כך: $(T \circ S)(v) = T(S(v))$. עבור $v = (x, y)$,
$(T \circ S)(v) = T(S(x, y)) = T(x + 2y, x + y) =$
$= ((x + 2y) - (x + y), 2(x + 2y) + (x + y) = (y, 3x + 5y)$.
$S \circ T \neq T \circ S$ – כתרגיל.

משפט 47: יהיו V_1, W_1, V_2 ו־W_2 מ״ו מעל שדה $\mathbb{F}$. יהיו $S : V_1 \to W_1$, $T : V_2 \to W_2$ העתקות לינאריות. אז אם $\operatorname{im} S \subseteq V_2$, $T \circ S : V_1 \to W_2$ מוגדרת והיא העתקה לינארית.

הוכחה. נסמן $L = T \circ S$. צ״ל כי לכל $v_1, v_2 \in V_1$, $\lambda_1, \lambda_2 \in F$, $L(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 L(v_1) + \lambda_2 L(v_2)$. ואכן:

$$\begin{aligned} L(\lambda_1 v_1 + \lambda_2 v_2) &= (T \circ S)(\lambda_1 v_1 + \lambda_2 v_2) \\ &= T(S(\lambda_1 v_1 + \lambda_2 v_2)) \\ &= T(\lambda_1 S(v_1) + \lambda_2 S(v_2)) \\ &= \lambda_1 T(S(v_1)) + \lambda_2 T(S(v_2)) = \lambda_1 L(v_1) + \lambda_2 L(v_2) \end{aligned}$$

כפי שראינו, אם $T : V \to W$ ה״ל חח״ע ועל, יש $S : W \to V$ כך ש־$T \circ S = I_V$, $S \circ T = I_W$. כלומר, $S = T^{-1}$ היא ההופכית של T.

משפט 48: V, W מ״ו מעל $\mathbb{F}$. אם $T : V \to W$ ה״ל חח״ע ועל, אז $T^{-1} : W \to V$ אף היא ה״ל.

הוכחה. יהיו $w_1, w_2 \in W$, $\lambda_1, \lambda_2 \in \mathbb{F}$. צריך להוכיח כי

$$T^{-1}(\lambda_1 w_1 + \lambda_2 w_2) = \lambda_1 T^{-1}(w_1) + \lambda_2 T^{-1}(w_2)$$

נבחר $v_1, v_2 \in V$ כך ש־$T(v_1) = w_1$, $T(v_2) = w_2$ (נוכל לעשות זאת, כי T על). אז $T^{-1}(w_1) = v_1$, $T^{-1}(w_2) = v_2$. כעת, $T(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 T(v_1) + \lambda_2 T(v_2) = \lambda_1 w_1 + \lambda_2 w_2$, ולכן

$$T^{-1}(\lambda_1 w_1 + \lambda_2 w_2) = \lambda_1 v_1 + \lambda_2 v_2 = \lambda_1 T^{-1}(w_1) + \lambda_2 T^{-1}(w_2)$$

□

27.12.2006

משפט 49: V, W מ״ו מעל $\mathbb{F}$. $T : V \to W$ העתקה לינארית. $K \subseteq V$ קבוצת וקטורים בת״ל. אם T חח״ע, אז $T(K)$ בת״ל.

הוכחה. (לשם הפשטות, נניח $K = \{v_1, \ldots, v_n\}$ סופית.) ניקח צ״ל מתאפס של איברי $T(K)$ ונוכיח שהוא טריוויאלי. נניח $\alpha_1 T(v_1) + \ldots + \alpha_n T(v_n) = 0$. אז $T(\alpha_1 v_1) + \ldots + T(\alpha_n v_n) = 0$ ולכן $T(\alpha_1 v_1 + \ldots + \alpha_n v_n) = 0$. כיוון ש־$T$ חח״ע, הרי $\ker T = \{0\}$. מכאן, $\alpha_1 v_1 + \ldots + \alpha_n v_n = 0$. מכיוון שזהו צ״ל מתאפס של איברי הקבוצה הבת״ל K, $\alpha_1 = \ldots = \alpha_n = 0$. □

משפט המימדים: הקאמבק

משפט 50 (משפט המימדים 2): V, W מ״ו מעל שדה $\mathbb{F}$, $\dim \ker T = n$. $T : V \to W$ ה״ל. אז $\dim \ker T + \dim \operatorname{im} T = \dim V$.

דוגמה. כבר ראינו אחת כזאת (ב־21.02), כשדנו בגרעין ובתמונה.

הוכחה. נפריד לשלושה מקרים:

א. $\ker T = V$. כלומר, T העתקת האפס: $\forall v \in V\ T(v) = 0_W$. לכן $\operatorname{im} T = \{0_W\} \Longleftarrow$ $\dim \operatorname{im} T = 0$. $\ker T = V \Longleftarrow \dim \ker T = n$. כעת, $\dim \ker T + \dim \operatorname{im} T = n + 0 = n$.

ב. $\{0\} \subsetneq \ker T \subsetneq V$. נסמן $\dim \ker T = k$. ניקח בסיס ל־$\ker T$: $\{u_1, \ldots, u_k\}$. נשלים בסיס זה לבסיס של V: $\{u_1, \ldots, u_k, v_1, \ldots, v_{n-k}\}$. ראינו כבר כי $\operatorname{im} T$ נפרשת על־ידי $\{T(u_1), \ldots, T(u_k), T(v_1), \ldots, T(v_{n-k})\}$. אבל כיוון ש־$u_1, \ldots, u_k \in \ker T$, $T(u_1) = \ldots = T(u_k) = 0$, ולכן מספיק לכתוב $\operatorname{im} T = \operatorname{span}\{T(v_1), \ldots, T(v_{n-k})\}$. אם נראה ש־$\{T(v_1), \ldots, T(v_{n-k})\}$ בת״ל, נקבל $\dim \operatorname{im} T = n-k$, ואז $\dim \ker T + \dim \operatorname{im} T = k + (n-k) = n$ וגמרנו. אם כן, נוכיח אי־תלות. נניח $\alpha_1 T(v_1) + \ldots + \alpha_{n-k} T(v_{n-k}) = 0$. לכן $T(\alpha_1 v_1 + \ldots + \alpha_{n-k} v_{n-k}) = 0$ ו־$\alpha_1 v_1 + \ldots + \alpha_{n-k} v_{n-k} \in \ker T$. לכן יש $\beta_1, \ldots, \beta_k \in \mathbb{F}$ כך ש־$\alpha_1 v_1 + \ldots + \alpha_{n-k} v_{n-k} = \beta_1 u_1 + \ldots + \beta_k u_k$. לכן $-\beta_1 u_1 - \ldots - \beta_k u_k + \alpha_1 v_1 + \ldots + \alpha_{n-k} v_{n-k} = 0$. זהו צ״ל מתאפס של איברי בסיס של V, ולכן $\alpha_1 = \ldots = \alpha_{n-k} = 0$ וגמרנו.

ג. $\ker T = \{0\}$. יהי $\{v_1, \ldots, v_n\}$ בסיס של V. ראינו כבר ש־$\operatorname{im} T = \operatorname{span}\{T(v_1), \ldots, T(v_n)\}$. כיוון ש־$T$ חח״ע ו־$\{v_1, \ldots, v_n\}$ בת״ל, הרי גם $\{T(v_1), \ldots, T(v_n)\}$ בת״ל. לכן זהו בסיס

עבור $\operatorname{im} T$, ו־$\dim \operatorname{im} T = n$. בנוסף, $\dim \ker T = 0$, ולכן $\dim \ker T + \dim \operatorname{im} T = 0 + n = n$. $\square$

31.12.2006

מסקנה 51: יהיו V, W מ"ו נ"ס מעל שדה $\mathbb{F}$. אם $T : V \to W$ ה"ל ואם $\dim V = \dim W$, הבאים שקולים:

א. T איזומורפיזם (כלומר, T חח"ע ועל);

ב. $\ker T = \{0\}$ (כלומר, T חח"ע);

ג. $\operatorname{im} T = W$ (כלומר, T על).

הוכחה. (א'⇐ב') טריוויאלי: אם T איזומורפיזם, בפרט T חח"ע ו־$\ker T = \{0\}$.

(ב'⇐ג') אם $\ker T = \{0\}$ אז $\dim \ker T = 0$, ולכן, על־פי משפט המימדים, $\dim \operatorname{im} T = \dim V$. על־פי הנתון, $\dim V = \dim W$, ולכן $\dim \operatorname{im} T = \dim W$. כיוון ש־$\operatorname{im} T \leq W$, הרי $\operatorname{im} T = W$.

(ג'⇐א') נניח $\operatorname{im} T = W$. אז $\dim \operatorname{im} T = \dim W = \dim V$, ושוב, על־פי משפט המימדים, $\dim \ker T = 0$ ולכן $\ker T = \{0\}$ ו־T חח"ע; כיוון ש־T על, הרי T איזומורפיזם.

3.9 עוד אודות איזומורפיזמים

הגדרה. אם יש $T : V \to W$ איזומורפיזם, אזי V **איזומורפי** ל־W. מסמנים $V \approx W$. מרחבים איזומורפיים

משפט 52: אם $W \approx V$ אזי $V \approx W$.

הוכחה. אם $V \approx W$ אז יש איזומורפיזם $T : V \to W$ (ה"ל חח"ע ועל). לכן קיימת $T^{-1} : W \to V$. הוכחנו ש־T^{-1} לינארית. מדוע T^{-1} הפיכה? (כלומר, מדוע T^{-1} אף היא איזומורפיזם?) כיוון ש־T הפיכה, הרי $T^{-1} \circ T = I_V$, $T \circ T^{-1} = I_W$, ולכן T^{-1} הפיכה.

משפט 53: יהיו U, V, W מ"ו מעל $\mathbb{F}$. אם $V \approx W$ ו־$U \approx V$ אז $U \approx W$.

הוכחה. $U \approx V$ פירושו שיש $T : U \to V$ איזומורפיזם. $V \approx W$ פירושו יש $S : V \to W$ איזומורפיזם. $S \circ T : U \to W$ היא ה"ל. כדי להראות שהיא איזומורפיזם, מספיק להראות שהיא הפיכה. ואכן, S הפיכה $\Longleftarrow$ S^{-1} קיימת; T הפיכה $\Longleftarrow$ T^{-1} קיימת. נתבונן ב־$T^{-1} \circ S^{-1} : W \to U$. כעת, $(T^{-1} \circ S^{-1}) \circ (S \circ T) = T^{-1} \circ (S^{-1} \circ S) \circ T = T^{-1} \circ I_V \circ T = T^{-1} \circ T = I_V$,[23] ובאותו אופן, $(S \circ T) \circ (T^{-1} \circ S^{-1}) = I_W$; לכן $(S \circ T)^{-1} = T^{-1} \circ S^{-1}$.

3.10 וקטור הקואורדינטות

(הוכיחו, כתרגיל, כי $\mathbb{F}^n = \left\{ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \mid \alpha_1, \ldots, \alpha_n \in \mathbb{F} \right\}$ מ"ו ממימד n מעל $\mathbb{F}$.)

[23] יש לשים לב שהשתמשנו באסוציאטיביות העתקות לינאריות בלי להוכיח.

וקטור הקואורדינטות

הגדרה. יהי V מ"ו מעל $\mathbb{F}$, $\dim V = n$. יהי $B = \{v_1, \dots, v_n\}$ בסיס של V.[24] אז לכל $v \in V$ יש הצגה יחידה $v = \sum_{i=1}^n \alpha_i v_i$. **וקטור הקואורדינטות** של v לפי הבסיס B הוא הוקטור

$$[v]_B = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in \mathbb{F}^n$$

דוגמה. $V = \mathbb{R}^2$ מעל $\mathbb{R}$. $E = \{(1,0),(0,1)\}$. $v = (2,3) = 2(1,0) + 3(0,1) \Longleftarrow$ $[v]_E = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$.

משפט 54: יהי V מ"ו מעל $\mathbb{F}$, $\dim V = n$. יהי $B = \{v_1, \dots, v_n\}$ בסיס של V. נגדיר $T : V \to \mathbb{F}^n$ על־ידי $T(v) = [v]_B$. אז T איזומורפיזם מ־V ל־F^n.

הוכחה. מדוע T ה"ל? ניקח $u_1, u_2 \in V$. נכתוב $u_1 = \sum_{i=1}^n \alpha_i v_i$, $u_2 = \sum_{i=1}^n \beta_i v_i$. לכן $u_1 + u_2 = \sum_{i=1}^n \alpha_i v_i + \sum_{i=1}^n \beta_i v_i = \sum_{i=1}^n (\alpha_i + \beta_i) v_i$. כעת, $T(u_1 + u_2) = [u_1 + u_2]_B = \begin{pmatrix} \alpha_1 + \beta_1 \\ \vdots \\ \alpha_n + \beta_n \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} + \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = T(u_1) + T(u_2)$. הוכחת הסגירות לכפל בסקלר – כתרגיל.

כיוון ש־V ו־$\mathbb{F}^n$ בעלי מימד זהה, הרי כדי להוכיח ש־T איזומורפיזם מספיק להוכיח שהיא על. ניקח $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in \mathbb{F}^n$. נגדיר $v = \alpha_1 v_1 + \ldots + \alpha_n v_n$. אז $T(v) = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$, ולכן T על.

משפט 55: יהיו V, W מ"ו מעל $\mathbb{F}$. אם $\dim V = \dim W = n$, $V \approx W$.

הוכחה. על־פי המשפט הקודם, $V \approx \mathbb{F}^n$ ו־$W \approx \mathbb{F}^n \Longleftarrow \mathbb{F}^n \approx W$. מכך ש־$V \approx \mathbb{F}^n$ ו־$\mathbb{F}^n \approx W$ נובע, על־פי משפט 53, ש־$V \approx W$.

3.11 מרחב ההעתקות

7.1.2007

מרחב ההעתקות

הגדרה. יהיו V, W מ"ו מעל $\mathbb{F}$. נגדיר $\hom(V,W) = \{T : V \to W \mid T \text{ ה"ל}\}$.

חיבור העתקות

הגדרה. אם $T, S \in \hom(V,W)$, נגדיר את סכומן $T + S : V \to W$ על־ידי $(T+S)(v) = T(v) + S(v)$.

משפט 56: אם $T, S \in \hom(V,W)$ אז $T + S \in \hom(V+W)$ ($T + S$ ה"ל).

הוכחה. נסמן $K = T + S$. יהיו $u_1, u_2 \in V$, $\alpha_1, \alpha_2 \in \mathbb{F}$.

[24] נתייחס לבסיס כאל קבוצה סדורה. כלומר, הבסיס $\{(1,0),(0,1)\}$ של $\mathbb{R}^2$ שונה מהבסיס $\{(0,1),(1,0)\}$ של $\mathbb{R}^2$.

$$\begin{aligned} K(\alpha_1 v_1 + \alpha_2 v_2) &= (T+S)(\alpha_1 v_1 + \alpha_2 v_2) \\ &= T(\alpha_1 v_1 + \alpha_2 v_2) + S(\alpha_1 v_1 + \alpha_2 v_2) \\ &= \alpha_1 T(v_1) + \alpha_2 T(v_2) + \alpha_1 S(v_1) + \alpha_2 S(v_2) \\ &= \alpha_1 \left(T(v_1) + S(v_1)\right) + \alpha_2 \left(T(v_2) + S(v_2)\right) \\ &= \alpha_1 (T+S)(v_1) + \alpha_2 (T+S)(v_2) \\ &= \alpha_1 K(v_1) + \alpha_2 K(v_2) \end{aligned} \quad \square$$

הגדרה. $T \in \hom(V,W)$, $\lambda \in \mathbb{F}$. נגדיר $\lambda T : V \to W$ על־ידי $(\lambda T)(v) = \lambda T(v)$. כפל העתקות בסקלר

משפט 57: אם $T \in \hom(V,W)$, $\lambda \in \mathbb{F}$ אז $\lambda T \in \hom(V,W)$.

הוכחה. נסמן $K = \lambda T$.

$$\begin{aligned} K(\alpha_1 v_1 + \alpha_2 v_2) &= (\lambda T)(\alpha_1 v_1 + \alpha_2 v_2) \\ &= \lambda T(\alpha_1 v_1 + \alpha_2 v_2) \\ &= \lambda \left(\alpha_1 T(v_1) + \alpha_2 T(v_2)\right) \\ &= \alpha_1 \lambda T(v_1) + \alpha_2 \lambda T(v_2) \\ &= \alpha_1 (\lambda T)(v_1) + \alpha_2 (\lambda T)(v_2) \\ &= \alpha_1 K(v_1) + \alpha_2 K(v_2) \end{aligned} \quad \square$$

משפט 58: V, W מ״ו מעל $\mathbb{F}$ (לא בהכרח נ״ס). אז $\hom(V,W)$ הוא מ״ו מעל $\mathbb{F}$.

הוכחה. כתרגיל. רק נעיר שאיבר האפס ב־$\hom(V,W)$ הוא העתקת האפס ואיבר נגדי ל־T ב־$\hom(V,W)$ הוא העתקה המוגדרת $(-T)(v) = -T(v)$.

3.12 מרחב המטריצות

3.12.1 פעולות על מטריצות

יהיו V, W מ״ו מעל $\mathbb{F}$, $B = \{v_1, \dots, v_n\}$ בסיס של V, $C = \{w_1, \dots, w_m\}$ בסיס של W, $T, S : V \to W$ העתקות לינאריות. חיבור מטריצות

$$[T]_C^B = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \quad [S]_C^B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix}$$

נמצא את $[T+S]_C^B$. כדי לעשות זאת, נחשב את העמודה הראשונה של $[T+S]_C^B$. נסמן $T(v_1) = \sum_{k=1}^m a_{k1} w_k$, $S(v_1) = \sum_{k=1}^m b_{k1} w_k$ $\Longleftarrow$

$$(T+S)(v_1) = T(v_1) + S(v_1) = \sum_{k=1}^m (a_{k1} b_{k1}) w_k$$

כלומר, $\begin{pmatrix} a_{11}+b_{11} \\ \vdots \\ a_{m1}+b_{m1} \end{pmatrix} = [(T+S)(v_1)]_C$. לכן העמודה הראשונה של $[T+S]_C^B$ היא סכום העמודות הראשונות של $[T]_C^B$ ו־$[S]_C^B$, ועבור העמודה ה־i נקבל אותו דבר באמצעות אותו חישוב. לכן המטריצה $[T+S]_C^B$ מתקבלת כסכום של $[T]_C^B$ ו־$[S]_C^B$ רכיב־רכיב. נוכל להגדיר, לכל מטריצות כלשהן:

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \quad B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} \quad A+B = \begin{pmatrix} a_{11}+b_{11} & \dots & a_{1n}+b_{1n} \\ \vdots & & \vdots \\ a_{m1}+b_{m1} & \dots & a_{mn}+b_{mn} \end{pmatrix}$$

יהיו V, W מ״ו מעל $\mathbb{F}$. תהי $T : V \to W$ ה״ל. הגדרנו עבור $\lambda \in \mathbb{F}$ את $\lambda T : V \to W$ על־ידי $(\lambda T)(v) = \lambda(T(v))$. אם 10.1.2007

$$[T]_C^B = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

כפל מטריצה בסקלר

מטריצת הייצוג של T, אז מטריצת הייצוג של λT היא

$$[\lambda T]_C^B = \begin{pmatrix} \lambda a_{11} & \dots & \lambda a_{1n} \\ \vdots & & \vdots \\ \lambda a_{m1} & \dots & \lambda a_{mn} \end{pmatrix}$$

מכאן, מגדירים עבור מטריצה כלשהי כפל בסקלר רכיב־רכיב.

3.12.2 הגדרת מרחב המטריצות

מרחב המטריצות

נסמן ב־$M_{m\times n}(\mathbb{F})$ את קבוצת המטריצות בעלות m שורות ו־n עמודות עם רכיבים מהשדה $\mathbb{F}$.

משפט 59: $M_{m\times n}(\mathbb{F})$ מ״ו ביחס לפעולות חיבור מטריצות וכפל מטריצה בסקלר.

משפט 60: $\hom(V,W) \approx M_{m\times n}(\mathbb{F})$, כאשר V, W מ״ו מעל $\mathbb{F}$, $\dim V = n$, $\dim W = m$.

הוכחה. נבחר בסיסים: $B = \{v_1,\dots,v_n\}$ עבור V, $C = \{w_1,\dots,w_m\}$ עבור W. נגדיר $\varphi : \hom(V,W) \to M_{m\times n}(\mathbb{F})$ על־ידי $\varphi(T) = [T]_C^B$.

מדוע φ לינארית? יהיו $T,S \in \hom(V,W)$; לפי הגדרת חיבור מטריצות, $\varphi(T+S) = [T+S]_C^B = [T]_C^B + [S]_C^B = \varphi(T)+\varphi(S)$. יהיו $T \in \hom(V,W)$, $\alpha \in \mathbb{F}$; לפי הגדרת כפל מטריצה בסקלר, $\varphi(\alpha T) = [\alpha T]_C^B = \alpha[T]_C^B$.

מדוע φ חח״ע? נניח ש־$\varphi(T_1) = \varphi(T_2)$. אז $[T_1]_C^B = [T_2]_C^B$. לכל j העמודה ה־j של $[T_1]_C^B$ שווה לעמודה ה־j של $[T_2]_C^B$: $\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} = \begin{pmatrix} b_{1j} \\ \vdots \\ b_{mj} \end{pmatrix}$. $T_1(v_j) = \sum_{i=1}^m a_{ij}w_i$, $T_2(v_j) = \sum_{i=1}^m b_{ij}w_i$. מכיוון ש־$a_{ij} = b_{ij}$ ($i = 1\dots m$, $j = 1\dots n$), T_1 ו־T_2 משתוות על הבסיס, ולכן, לפי משפט 40, $T_1 = T_2$.

מדוע φ על? ניקח $A \in M_{m\times n}(\mathbb{F}) = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$. נגדיר בעזרתה $T: V \to W$. לכל j, $T(v_j) = \sum_{i=1}^m a_{ij} w_i$. זו הגדרת T על הבסיס. נרחיב אותה לה"ל על כל המרחב, ולפי ההגדרה, $\varphi(T) = A$.

3.12.3 מטריצות ייצוג של הרכבת העתקות

יהיו U, V, W מ"ו מעל $\mathbb{F}$, $B = \{u_1, \dots, u_n\}$ בסיס של U, $C = \{v_1, \dots, v_m\}$ בסיס של V, $D = \{w_1, \dots, w_k\}$ בסיס של W, $S: U \to V$, $T: V \to W$.

ל־S יש מטריצת ייצוג: $[S]_C^B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix}$. לכל j, $S(u_j) = \sum_{l=1}^m b_{lj} v_l$ ($1 \le j \le n$).

ל־T יש מטריצת ייצוג: $[T]_D^C = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & & \vdots \\ a_{k1} & \dots & a_{km} \end{pmatrix}$. לכל l, $T(v_l) = \sum_{i=1}^k a_{il} w_i$ ($1 \le l \le k$).

נסמן $[T \circ S]_D^B = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & & \vdots \\ c_{k1} & \dots & c_{kn} \end{pmatrix}$. ניקח $1 \le j \le n$. נחשב:

$$(T \circ S)(u_j) = T(S(u_j)) = T(\sum_{l=1}^m b_{lj} v_l) = \sum_{l=1}^m b_{lj} T(v_l) = \sum_{l=1}^m b_{lj} \sum_{i_1}^k a_{il} w_i =$$

$$= \sum_{l=1}^m \sum_{i=1}^k a_{il} b_{lj} w_i = \sum_{i=1}^k (\sum_{l=1}^m a_{il} b_{lj}) w_i$$

קיבלנו, לכל $j = 1 \dots n$, $(T \circ S)(u_j) = \sum_{i=1}^k \sum_{l=1}^m (a_{il} b_{lj}) w_i$. לכן העמודה ה־$j$ של $[T \circ S]_D^B$ היא $[(T \circ S)(u_j)]_D = \begin{pmatrix} \sum_{l=1}^m a_{1l} b_{lj} \\ \vdots \\ \sum_{l=1}^m a_{kl} b_{lj} \end{pmatrix}$. מכאן, המקום ה־$(i,j)$ ב־$[T \circ S]_D^B$ הוא $c_{ij} = \sum_{l=1}^m a_{il} b_{lj}$.

כעת, בהינתן שתי מטריצות כלשהן $A_{k\times m}$, $B_{m\times n}$, נגדיר $AB = C$ כאשר האיבר ה־(i,j) ב־C מוגדר על־ידי $c_{ij} = \sum_{l=1}^m a_{il} b_{lj}$. (ובפרט, נקבל שמתקיים $[T \circ S]_D^B = [T]_D^C [S]_C^B$.) כפל מטריצות

דוגמה. $A = \begin{pmatrix} 2 & 3 & 1 \\ 4 & 2 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 5 & 1 \\ 0 & 0 \\ 1 & 2 \end{pmatrix}$. נקבל $AB = \begin{pmatrix} 11 & 4 \\ 20 & 4 \end{pmatrix}$, לפי החישובים $c_{11} = \sum_{l=1}^3 a_{1l} bl1 = a_{11} b_{11} + a_{12} b_{21} + a_{13} b_{31}$ וכו'.

בהינתן שורה $a = \begin{pmatrix} a_1 & \dots & a_n \end{pmatrix}$ ועמודה $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$, נגדיר פעולה חדשה $a \cdot b = a_1 b_1 + \dots + a_n b_n$. כעת, אם A ו־B מטריצות, איברי $C = AB$ יהיו $c_{ij} =$ שורה i של A $\cdot$ עמודה j של B.

נשים לב שמכפלת המטריצות $B_{n\times k}$, $A_{m\times p}$ מוגדרת רק כאשר $p = n$, ואז המכפלה תהיה מסדר $m \times k$.

14.1.2007

משפט 61: V, W מ״ו מעל $\mathbb{F}$, $T : V \to W$, $B = \{v_1, \dots, v_n\}$ בסיס של V, $C = \{w_1, \dots, w_m\}$ בסיס של W. אז $[T(v)]_C = [T]_C^B [v]_B$.

דוגמה. $V = \mathbb{R}_2[x]$, $B = \left\{1, x, x^2\right\}$, $W = \mathbb{R}_1[x]$, $C = \{1, x\}$. נגדיר העתקה $D : \mathbb{R}_2[x] \to \mathbb{R}_1[x]$ על־ידי $D\left(P(x)\right) = P'(x)$. קל לראות ש־$D$ ה״ל. נמצא את $[D]_C^B$.

$$\begin{array}{lcl} D(1) = 0 & \text{ולכן} & [D(1)]_C = \binom{0}{0} \\ D(x) = 1 & & [D(x)]_C = \binom{1}{0} \\ D(x^2) = 2x & & [D(x^2)]_C = \binom{0}{2} \end{array} \quad \Longleftarrow \quad [D]_C^B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

לפני שנזרוק את הסיכומים באינפי, נבדוק שזה אכן עובד: נבחר $P(x) = 3 + x + 7x^2$, $[P(x)]_B = \begin{pmatrix} 3 \\ 1 \\ 7 \end{pmatrix}$. אזי $P'(x) = 1 + 14x$, $[P'(x)]_B = \binom{1}{14}$. ואכן:

$$[D(P(x))]_C = [D]_C^B [P(x)]_B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \\ 7 \end{pmatrix} = \begin{pmatrix} 1 \\ 14 \end{pmatrix}$$

הוכחה. נסמן $[T]_C^B = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$. אז לכל j מתקיים $T(v_j) = \sum_{i=1}^m a_{ij} w_i$. יהי $v \in V$.
נסמן $[v]_B = \begin{pmatrix} \gamma_1 1 \\ \vdots \\ \gamma_n 1 \end{pmatrix}$; אז $v = \sum_{j=1}^n \gamma_{j1} v_j$.

$$T(v) = T(\sum_{j=1}^n \gamma_{j1} v_j) = \sum_{j=1}^n \gamma_{j1} T(v_j) = \sum_{j=1}^n \gamma_{j1} \sum_{i=1}^m a_{ij} w_i = \sum_{i=1}^m (\sum_{j=1}^n a_{ij} \gamma_{j1}) w_i$$

לכן וקטור הקואורדינטות של $T(v)$ הוא $[T(v)]_C = \begin{pmatrix} \sum_{j=1}^n a_{1j}\gamma_{j1} \\ \vdots \\ \sum_{j=1}^n a_{mj}\gamma_{j1} \end{pmatrix}$, והאיבר בשורה ה־$i$ של $[T(v)]_C$ הוא $\sum_{j=1}^n a_{ij}\gamma_{j1}$. כעת נחשב את האיבר בשורה ה־i של $[T]_C^B[v]_B$. על־פי הנוסחה של כפל מטריצות, $[T]_C^B[v]_B$ וקטור עמודה; האיבר במיקום ה־$(i,1)$ הוא $\sum_{j=1}^n a_{ij}\gamma_{j1}$. □

3.13 תכונות של כפל מטריצות

תכונות כפל מטריצות

אסוציאטיביות

טענה 62: כפל מטריצות אסוציאטיבי. כלומר, אם $A \in M_{m\times n}(\mathbb{F})$, $B \in M_{n\times p}(\mathbb{F})$, $C \in M_{p\times q}(\mathbb{F})$, $(AB)C = A(BC)$.

הוכחה. נבחר בסיסים סטנדרטיים E_m, E_n, E_p, E_q למרחבים $\mathbb{F}^m, \mathbb{F}^n, \mathbb{F}^p, \mathbb{F}^q$. נגדיר $T_C : \mathbb{F}^q \to \mathbb{F}^p$ על־ידי $T(e_j) = \text{עמודה } j \text{ של } C$. נקבל $[T_C]_{E_p}^{E_q} = c$. באופן דומה, נגדיר $T_B : \mathbb{F}^p \to \mathbb{F}^n$, $T_A : \mathbb{F}^n \to \mathbb{F}^m$, ו־$[T_B]_{E_n}^{E_p} = B$, $[T_A]_{E_m}^{E_n} = A$. מכאן, $[T_B \circ T_C] = [T_B][T_C] = BC$, $[T_A \circ T_B] = [T_A][T_B] = AB$. כעת,

$$[T_A \circ (T_B \circ T_C)] = [T_A][T_B \circ T_C] = A(BC)$$

$$[(T_A \circ T_B) \circ T_C] = [T_A \circ T_B][T_C] = (AB)C$$

ובשל אסוציאטיביות הרכבת העתקות נקבל שוויון.

למה 63: אם $T, S : V \to W$ ה"ל ו־$K : W \to U$ ה"ל, אז $K \circ (T+S) = K \circ T + K \circ S$. דיסטריבוטיביות

הוכחה. כתרגיל.

התכונה נובעת מיידית מהלמה.

נניח V מ"ו מעל $\mathbb{F}$, $B = \{v_1, \ldots, v_n\}$ **בסיס** של V. $I_V : V \to V$ **העתקת הזהות**: $\forall v \in V \; I_V(v) = v$ מטריצת היחידה

$$I_V(v_1) = v_1 = 1v_1 + 0v_2 + \ldots + 0v_n \Longleftarrow [I_V(v_1)]_B = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

לכן המטריצה $\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} = [I_V]_B^B = I_n$ היא מטריצת היחידה.

$[T]_B^B$ מטריצת הייצוג של T. $T = I_V \circ T : V \to V$, $T = T \circ I_V : V \to V$. לכן $[T]_B^B = [I_V \circ T]_B^B = I_n [T]_B^B$, $[T]_B^B = [T \circ I_V]_B^B = [T]_B^B I_n$. בהינתן מטריצה $n \times n$ כלשהי A, נוכל לראותה כמטריצת ייצוג של העתקה כלשהי $T_A : \mathbb{F}^n \to \mathbb{F}^n$ המוגדרת על־ידי עמודה i של A · $T_A(e_i)$, ונקבל $AI_V = I_V A = A$.

תהי A מטריצה מסדר $n \times n$. נגדיר העתקה $T_A : \mathbb{F}^n \to \mathbb{F}^n$ על־ידי עמודה i של A $= T_A(e_i)$. אם T_A העתקה הפיכה – כלומר, אם קיימת העתקה $T_A^{-1} : V \to V$ כך ש־$T_A \circ T_A^{-1} = I_V$, $T_A^{-1} \circ T_A = I_V$ – אז מתקיימים התנאים $[T_A][T_A^{-1}] = I_n$, $[T_A^{-1}][T_A] = I_n$. למטריצה $[T_A^{-1}]$ קוראים **המטריצה ההופכית** של A; מסמנים A^{-1}, ו־$[T_A]^{-1} = A^{-1} = [T_A^{-1}]$. מטריצות הפיכות

דוגמה. תהי $A = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$. נראה ש־$A^{-1} = \frac{1}{3}\left(\begin{smallmatrix} 2 & -1 \\ -1 & 2 \end{smallmatrix}\right)$:

$$AA^{-1} = \frac{1}{3}\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} = \frac{1}{3}\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} = I_2$$

כמו־כן, $A^{-1}A = I_2$.

לא כל מטריצה היא הפיכה. מכאן, המטריצות הן חוג, לא שדה.

3.14 מטריצות מעבר

הגדרה. יהי V מ"ו מעל $\mathbb{F}$, ויהיו $B = \{v_1, \ldots, v_n\}$, $C = \{v'_1, \ldots, v'_n\}$ שני בסיסים עבור V. נתבונן במטריצת הייצוג $[I_V]_C^B$ של העתקת הזהות $I_V : V \to V$. יהי $v \in V$. אז על־פי משפט 61, $[v]_C = [I_V(v)]_C = [I_V]_C^B [v]_B$. $[I_V]_C^B$ נקראת **מטריצת המעבר** מהבסיס B לבסיס C. מטריצת מעבר

העמודה ה־j של מטריצת המעבר: $[I(v_j)]_C = [v_j]_C$.

דוגמה. $V=\mathbb{R}^2$, $B=\{v_1=\binom{3}{5}, v_2=\binom{-1}{-1}\}$, $C=\{v_1'=\binom{1}{2}, v_2'=\binom{2}{3}\}$. נמצא את $[I]_C^B$.

$$\left.\begin{array}{lll} v_1=\binom{3}{5}=v_1'+v_2' & \Rightarrow & [v_1]_C=\binom{1}{1} \\ v_2=\binom{-1}{-1}=v_1'-v_2' & \Rightarrow & [v_2]_C=\binom{1}{-1} \end{array}\right\} \Longrightarrow \quad [I]_C^B=\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

ניקח $v=\binom{3}{5}=1v_1+0v_2$. אז $[v]_B=\binom{1}{0}$. כדי למצוא את $[v]_C$, צריך לפתור $\binom{3}{5}=\alpha_1\binom{1}{2}+\alpha_2\binom{2}{3}$ ולקבל $[\binom{3}{5}]_C=\binom{\alpha_1}{\alpha_2}$ – או, בעזרת מטריצת המעבר, ניתן פשוט לחשב $[v]_C=[I]_C^B[v]_B=\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\binom{1}{0}=\binom{1}{1}$.

4 מערכות משוואות לינאריות

4.1 מערכות משוואות

נתבונן במערכת המשוואות הבאה: 17.1.2007

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \dots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \dots & + & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots \\ a_{n1}x_1 & + & a_{n2}x_2 & + & \dots & + & a_{nn}x_n & = & b_n \end{array}$$

או, בכתיב אחר: עלינו לפתור $Ax = b$, כאשר

$$b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \qquad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \qquad \begin{array}{c} a_{ij} \in \mathbb{F} \\ 1 \le i \le m \\ 1 \le j \le n \end{array}$$

וקטור המקדמים החופשיים   וקטור הנעלמים   מטריצת המקדמים

הגדרה. אם $b = 0_{\mathbb{F}^m}$ המערכת נקראת **הומוגנית**. אחרת, המערכת נקראת **אי־הומוגנית**. מערכת (אי־)הומוגנית

הגדרה. וקטור $c \in \mathbb{F}^n$ שאם נציב אותו במקום x ישמור על השוויון נקרא **וקטור פתרון**. מתקיים $Ac = b$. וקטור פתרון

מקרה פרטי: $m = n$

אם $m = n$ – כלומר, A ריבועית – ו־A הפיכה, נקבל $c = A^{-1}b$ פתרון:

$$A^{-1}(AX) = A^{-1}b \iff (A^{-1}A)x = A^{-1}b \iff x = A^{-1}b$$

בהינתן המערכת $Ax = b$, נתאים למטריצה A העתקה $T_a : \mathbb{F}^n \to \mathbb{F}^m$ המוגדרת על־ידי $T_A(x) = Ax$. T_A היא העתקה לינארית: היא שומרת על חיבור – $T_A(x+y) = A(x+y) = Ax + Ay = T_A(x) + T_A(y)$ – ועל כפל בסקלר – $T_A(\lambda x) = A(\lambda x) = \lambda(Ax) = \lambda T_A(x)$.

אם c פתרון של המערכת, מתקיים $T_A(c) = Ac = b$.

נעיר ש־$A = [T_A]_{E_n}^{E_m}$: $Ae_i = T_A(e_i) = [T_A(e_i)]_{E_m}$ זו העמודה ה־i של A.

עבור כל פונקציה $f : K \to L$, $b \in L$ נגדיר את **קבוצת המקור** של $\{b\}$: $f^{-1}(\{b\}) = \{a \in K \mid f(a) = b\}$. אם $T : V \to W$ העתקה לינארית, $\ker T = T^{-1}(\{0\})$. מכאן נוכל לומר ש־$T_A^{-1}\{b\}$ היא **קבוצת הפתרונות** של המערכת $A_x = b$.

למה 64: למערכת $A_x = b$ יש פתרון אס"ם $b \in \operatorname{im} T_A$.

הוכחה. יש פתרון c למערכת $\iff Ac = b \iff T_A(c) = b \iff b \in \operatorname{im} T_A$

נניח ש־A מערכת הומוגנית. כלומר, $Ax=0$. קבוצת הפתרונות של המערכת היא $\ker T_A$.
במקרה זה, 0 תמיד פתרון; זהו פתרון יחיד אס״ם T_A חח״ע ($\ker T_A=\{0\}$).

דוגמה. $T_A\binom{x_1}{x_2}=A\binom{x_1}{x_2}=\binom{2x_1+3x_2}{4x_1+6x_2}$ $\quad A=\begin{pmatrix}2&3\\4&6\end{pmatrix}$ $\quad \begin{cases}2x_1+3x_2=0\\4x_1+6x_2=0\end{cases}$

$$\ker T_A=\left\{\binom{x_1}{x_2}\mid T_A\binom{x_1}{x_2}=\binom{0}{0}\right\}=\left\{\binom{x_1}{x_2}\mid \begin{matrix}2x_1+3x_2=0\\4x_1+6x_2=0\end{matrix}\right\}$$

נפתור את המערכת: $2x_1+3x_2=0\implies x_1=\frac{-3x_2}{2}$. נסמן $x_2=t$ ונקבל $x_1=\frac{-3t}{2}$.
לכן וקטור מהצורה $\begin{pmatrix}-\frac{3t}{2}\\t\end{pmatrix}$ פותר את המערכת. ואכן, $\ker T_A=\left\{t\begin{pmatrix}-\frac{3}{2}\\1\end{pmatrix}\mid t\in\mathbb{R}\right\}=\operatorname{span}\left\{\begin{pmatrix}-\frac{3}{2}\\1\end{pmatrix}\right\}$.

קבוצת הפתרונות של מערכת הומוגנית $A_x=0$ היא מ״ו.[25] מצד שני, קבוצת הפתרונות של מערכת אי־הומוגנית אינה מרחב וקטורי: אם קבוצת הפתרונות היא מרחב וקטורי, 0 נמצא בה – אולם אז נקבל $A0=b\neq 0$, בסתירה לאי־הומוגניות המערכת.

דוגמה. $A=\begin{pmatrix}1&1\\1&-1\end{pmatrix}$ $\quad \begin{cases}x_1+x_2=1\\x_1-x_2=0\end{cases}$. נפתור ונקבל $x_1=x_2=\frac{1}{2}$.

ישרייה

הגדרה. יהיו $W\leq V$ ו־$v\in V$. אז $v+W=\{v+w\mid w\in W\}$ נקראת **ישרייה**. W נקרא **תת־המרחב המכוון** של הישרייה. מימד הישרייה $v+W$ מוגדר להיות המימד של W.

משפט 65: תהי $Ax=b$ מערכת משוואות לינאריות. נניח כי $b\in\operatorname{im}T_A$ (כלומר, ישנו פתרון למערכת). יהי $s\in\mathbb{F}^n$ פתרון. קבוצת כל הפתרונות תהיה הישרייה $T_A^{-1}(b)=s+\ker T_A$.

דוגמה.

מערכת הומוגנית	מערכת אי־הומוגנית
$\begin{cases}2x_1+x_2=0\\4x_1+2x_2=0\end{cases}$	$\begin{cases}2x_1+x_2=2\\4x_1+2x_2=4\end{cases}$
$\begin{cases}2x_1+x_2=0\\0+0=0\end{cases}$	$\begin{cases}2x_1+x_2=2\\0+0=0\end{cases}$
$x_2=t$	$x_2=t$
$2x_1=-t\implies x_1=-\frac{t}{2}$	$x_1=\frac{2-t}{2}=1-\frac{t}{2}$
$T_A^{-1}\{b\}=\left\{\begin{pmatrix}-\frac{t}{2}\\t\end{pmatrix}\mid t\in\mathbb{R}\right\}=\ker T_A$	$T_A^{-1}\{b\}=\left\{\begin{pmatrix}1-\frac{t}{2}\\t\end{pmatrix}\mid t\in\mathbb{R}\right\}=\ker T_A+\binom{1}{0}$

הוכחה. יהי $v\in\ker T_A$. צ״ל ש־$s+v\in T_A^{-1}\{b\}$. ואכן, $T_A(s+v)=T_A(s)+T_A(v)=b+0=b$ ו־$s+v\in T_A^{-1}\{b\}$ פתרון.
מצד שני, נניח כי $c\in T_A^{-1}\{b\}$. נתבונן בוקטור $c-s$: $T_A(c-s)=T_A(c)-T_A(s)=b-b=0$, ולכן $c-s\in\ker T_A$. נסמן $v=c-s$, ואז $c=\overset{\text{פתרון}}{s}+\overset{\in\ker T_A}{v}$.

[25] ניזכר שהגרעין הוא מ״ו.

משפט 66: למערכת $Ax+b$ יש פתרון (יחיד) אס"ם $b\in \operatorname{im} T_A$ ו־$\ker T_A=\{0\}$. 21.1.2007

הוכחה. נניח שהתנאים מתקיימים. כיוון ש־$b\in\operatorname{im}T_A$, קיים $v\in\mathbb{F}^n$ כך ש־$Av=T_A(v)=b$. מכאן, v פתרון. כעת, יהיו v_1,v_2 שני פתרונות. אז $T_A(v_1)=T_A(v_2)$. לכן $T_A(v_1-v_2)=0$, ומכאן $v_1-v_2=\ker T_A=\{0\}$. מכאן, $v_1=v_2 \iff v_1-v_2=0$.

מצד שני, נניח שיש פתרון יחיד v. $Av=T_A(v)=b$, ולכן $b\in\operatorname{im}T_A$. כעת ניקח $u\in\ker T_A$. אז $T_A(u+v)=T_A(u)+T_A(v)=0+b=b$. לכן $T_A(u+v)=b$, ומכאן $u+v$ אף הוא פתרון של המערכת. אולם הנחנו שהפתרון יחיד, ולכן $u=0 \iff u+v=v$. מכאן $\ker T_A\subseteq\{0\}$. ודאי מתקיים $\{0\}\subseteq\ker T_A$, ולכן $\ker T_A=\{0\}$. □

אם $Ax=b$ מערכת משוואות ($A\in M_{m\times n}(\mathbb{F})$), מוגדרת העתקה לינארית $T_A:\mathbb{F}^n\to\mathbb{F}^m$. על־פי משפט המימדים, $n=\dim\ker T_A+\dim\operatorname{im}T_A$. כלומר, $\dim_{\text{מרחב הפתרונות}}=n-\dim\operatorname{im}T_A$. אך מהו $\dim\operatorname{im}T_A$? איך מחשבים את $\operatorname{im}T_A$?

נסמן, עבור מטריצה $A=\begin{pmatrix}a_{11}&\cdots&a_{1n}\\ \vdots&&\vdots\\ a_{m1}&\cdots&a_{mn}\end{pmatrix}$, $\vec{a_i}$ השורה ה־i של A ו־$a_i\downarrow$ העמודה ה־i של A.

אז $\begin{pmatrix}a_1\downarrow&\cdots&a_n\downarrow\end{pmatrix}=\begin{pmatrix}\vec{a_1}\\ \vdots\\ \vec{a_n}\end{pmatrix}=A$.

טענה 67: $\operatorname{im}T_A=\operatorname{span}\{a_1\downarrow,\dots,a_n\downarrow\}$

הוכחה. נשים לב ש־A היא מטריצת הייצוג של ההעתקה T_A לפי הבסיסים הסטנדרטיים של $\mathbb{F}^n$, $\mathbb{F}^m$ - כלומר,

$$T_A(\overset{\text{מ־}E_n}{e_1})=[T_A(e_1)]_{E_m}=T_A\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}=$$

$$=A\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}=\begin{pmatrix}a_{11}&\cdots&a_{1n}\\ \vdots&&\vdots\\ a_{m1}&\cdots&a_{mn}\end{pmatrix}\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}=\begin{pmatrix}a_{11}\\\vdots\\a_{m1}\end{pmatrix}=a_1\downarrow$$

. זה נכון לכל $i=1\dots n$; כלומר, $\forall i=1\dots n T_A(e_i)=a_i\downarrow$.

מכאן, $\operatorname{im}T_A=\operatorname{span}\{T_A(e_1),\dots,T_A(e_n)\}=\operatorname{span}\{a_1\downarrow,\dots,a_n\downarrow\}$.

הגדרה. $\operatorname{span}\{a_1\downarrow,\dots,a_n\downarrow\}$ נקרא **מרחב העמודות** של A. המימד שלו, **דרגת העמודות** של A, מסומן $r_c(A)$. דרגת העמודות, מרחב העמודות

4.2 דירוג מטריצות – פתרון משוואות

דוגמה.

$$\begin{array}{ccccccccccc}
3x_1 & + & 3x_2 & + & 2x_3 & + & 5x_4 & + & 2x_5 & = & 2\\
 & & & & 2x_3 & + & 2x_4 & + & 4x_5 & = & 4\\
x_1 & + & x_2 & & & + & x_4 & - & x_5 & = & 2\\
3x_1 & + & 3x_2 & + & 4x_3 & + & 7x_4 & + & 6x_5 & = & 6
\end{array}$$

נכתוב את המערכת כמטריצת מקדמים:

$$\begin{matrix} 3 & 3 & 2 & 5 & 2 & 2 \\ 0 & 0 & 2 & 2 & 4 & 4 \\ 1 & 1 & 0 & 1 & -1 & 2 \\ 3 & 3 & 4 & 7 & 6 & 6 \end{matrix}$$

בשלב א׳, נרצה לחלץ את x_1 מכל המשוואות פרט לראשונה. לשם כך, נחליף בין שורה 1 ו־3: $R_1 \leftrightarrow R_3$

$$\begin{matrix} 1 & 1 & 0 & 1 & -1 & 2 \\ 0 & 0 & 2 & 2 & 4 & 4 \\ 3 & 3 & 2 & 5 & 2 & 2 \\ 3 & 3 & 4 & 7 & 6 & 6 \end{matrix}$$

$R_4 \to R_4 - 3R_1$,$R_3 \to R_3 - 3R_1$

$$\begin{matrix} 1 & 1 & 0 & 1 & -1 & 2 \\ 0 & 0 & 2 & 2 & 4 & 4 \\ 0 & 0 & 2 & 2 & 5 & 5 \\ 0 & 0 & 4 & 4 & 9 & 9 \end{matrix}$$

בשלב ב׳, נרצה לחלץ את x_2 מכל המשוואות פרט לשנייה. לא נוכל לעשות זאת מבלי לפגוע בהישגים הקודמים, לכן נעבור לשלב ג׳.

בשלב ג׳, נרצה לחלץ את x_3 מכל המשוואות פרט לשנייה (כי שלב ב׳ נכשל). $R_2 \to \frac{1}{2}R_2$

$R_4 \to R_4 - 3R_1$,$R_3 \to R_3 - 3R_1$

$$\begin{matrix} 1 & 1 & 0 & 1 & -1 & 2 \\ 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 0 & 2 & 2 & 5 & 5 \\ 0 & 0 & 4 & 4 & 9 & 9 \end{matrix}$$

$R_4 \to R_4 - 4R_2$,$R_3 \to R_3 - 2R_2$

$$\begin{matrix} 1 & 1 & 0 & 1 & -1 & 2 \\ 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{matrix}$$

בשלב ד׳, נרצה לחלץ את x_3 מכל המשוואות פרט לשלישית. לא נוכל לעשות זאת מבלי לפגוע בהישגים הקודמים, לכן נעבור לשלב ה׳.

בשלב ה׳, נרצה לחלץ את x_4 מכל המשוואות פרט לשלישית (כי שלב ד׳ נכשל). $R_1 \to R_1 + R_3$, $R_2 \to R_2 - 2R_3$, $R_4 \to R_4 - R_3$

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

כעת נפתור: $x_5 = 1$; לגבי x_4 אין מספיק נתונים, וכל בחירה שלו תשפיע על המשתנים האחרים. לכן נסמן $x_4 = t$. כנ״ל לגבי $x_2 = s$. בסוף נקבל שפתרון המערכת הוא $(-t-s, s, -t, t, 1)$. כלומר, קבוצת הפתרונות היא הישרייה

$$\left\{ \begin{pmatrix} -t-s \\ s \\ -t \\ t \\ 1 \end{pmatrix} \mid t, s \in \mathbb{R} \right\} = \operatorname{span}\left\{ \begin{pmatrix} -1 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

x_2, x_4 נקראים **משתנים חופשיים**. x_1, x_3, x_5 נקראים **משתנים מובילים (פותחים)**. מימד מרחב הפתרונות זהה למספר המשתנים החופשיים; כזכור, $\dim_{\text{מרחב הפתרונות}} = n - r_c$, וכיוון שמספר המשתנים בסך־הכל הוא n, הרי $r_c = n - \text{מספר המשתנים החופשיים} = \text{מספר המשתנים המובילים}$.

4.3 מטריצת מדרגות קנונית

24.1.2007

הגדרה. מטריצה B מסדר $m \times n$ נקראת **מטריצת מדרגות קנונית** אם $B = 0$ או $k \leq n$ כך ש־   מטריצת מדרגות קנונית

א. העמודות הסטנדרטיות $e_1, \ldots, e_k$ מופיעות לפי הסדר, אך לא בהכרח ברצף, כעמודות B;

ב. אם ניצור קו מדרגות – כלומר, קו שמתחיל מעל האיבר הראשון של B ומתקדם ימינה עד שפוגש את האיבר 1 של העמודה הסטנדרטית הראשונה, אז הוא יורד שורה למטה, וכן הלאה עד שעבר על כל העמודות.

בניסוח אחר: מטריצה B נקראת **מטריצת מדרגות קנונית** אם –

א. כל שורות האפס נמצאות מתחת לשורות שאינן אפס;

ב. האיבר הפותח של כל שורה נמצא מימין לאיבר הפותח של השורה שלפניה;

ג. האיבר הפותח של כל שורה שאינה אפס הוא 1, ויתר האיברים בעמודתו הם אפסים.

כל איבר פותח מתאים למשתנה פותח (משתנה שנקבע על־ידי משתנים אחרים).

משפט 68: נתבונן במערכת $Ax=b$. ניתן לדרג את A כך שבסיום הדירוג נקבל מטריצת מדרגות קנונית במקום A. c פתרון של $Ax=b \iff c$ פתרון של המערכת המדורגת.

4.4 מטריצות אלמנטריות

1. נסמן ב־$E_{ij}(\alpha)$ ($i\neq j$, $\alpha\neq 0$) את המטריצה מסדר $m\times m$ שבאלכסון שלה 1־ים, במקום ה־(i,j) מופיע α וכל השאר אפסים.

   המטריצה $E_{ij}(\alpha)A$ מתקבלת מ־A על־ידי הפעולת $R_i\to R_i+\alpha R_j$.

   דוגמה. $\begin{pmatrix}1&0&0\\0&1&\alpha\\0&0&1\end{pmatrix}\begin{pmatrix}a_{11}&a_{12}&a_{13}\\a_{21}&a_{22}&a_{23}\\a_{31}&a_{32}&a_{33}\end{pmatrix}=\begin{pmatrix}a_{11}&a_{12}&a_{13}\\a_{21}+\alpha a_{31}&a_{22}+\alpha a_{32}&a_{23}+\alpha a_{33}\\a_{31}&a_{32}&a_{33}\end{pmatrix}$

2. נסמן ב־$E_i(\alpha)$ ($\alpha\neq 0$) את המטריצה מסדר $m\times m$ שבאלכסון שלה 1־ים פרט למקום ה־(i,i) בו מופיע α וכל השאר אפסים.

   המטריצה $E_i(\alpha)$ מתקבלת מ־A על־ידי הפעולה $R_i\to\alpha R_i$.

   דוגמה. $\begin{pmatrix}1&0&0\\0&\alpha&0\\0&0&1\end{pmatrix}\begin{pmatrix}a_{11}&a_{12}&a_{13}\\a_{21}&a_{22}&a_{23}\\a_{31}&a_{32}&a_{33}\end{pmatrix}=\begin{pmatrix}a_{11}&a_{12}&a_{13}\\\alpha a_{21}&\alpha a_{22}&\alpha a_{23}\\a_{31}&a_{32}&a_{33}\end{pmatrix}$

3. נסמן ב־P_{ij} ($i\neq j$) את מטריצת היחידה מסדר $m\times m$ שהפכו בה שורה i עם שורה j.

   המטריצה $P_{ij}A$ מתקבלת מ־A על־ידי הפעולה $R_i\leftrightarrow R_j$.

   דוגמה. $\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}\begin{pmatrix}a_{11}&a_{12}&a_{13}\\a_{21}&a_{22}&a_{23}\\a_{31}&a_{32}&a_{33}\end{pmatrix}=\begin{pmatrix}a_{21}&a_{22}&a_{23}\\a_{11}&a_{12}&a_{13}\\a_{31}&a_{32}&a_{33}\end{pmatrix}$

כעת, אם במקום לדרג את המטריצה A נכפיל בכל פעם במטריצה אלמנטרית, נקבל $K=E_t\dots E_1A$ כאשר K מטריצת מדרגות $E_1,\dots,E_t$ מטריצות אלמנטריות מהסוגים שהוגדרו לעיל.

נשים לב כי $E_{ij}^{-1}(\alpha)=E_{ij}(\alpha^{-1})$, $E_i^{-1}(\alpha)=E_i(\alpha^{-1})$, $P_{ij}^{-1}=P_{ij}$. (הוכחה - כתרגיל.)

ניתן להוכיח כי מכפלה של מטריצות הפיכות היא מטריצה הפיכה ($(AB)^{-1}=B^{-1}A^{-1}$).
לכן $E_t\dots E_1=C$ היא מטריצה הפיכה. כדי להגיע מ־A למטריצת המדרגות K, הכפלנו את A במטריצה ההפיכה C: $K=CA$.

משפט 69: תהי $Ax=b$ מערכת לינארית, $A\in M_{m\times n}(\mathbb{F})$. תהי C מטריצה הפיכה מסדר m. אז למערכת $(CA)x=Cb$ ולמערכת $Ax=b$ אותם פתרונות.

הוכחה. יהי d פתרון של המערכת $Ax=b$. אז $Ad=b$. לכן $C(Ad)=Cb \iff (CA)d=Cb$, ומכאן d פתרון של המערכת $(CA)x=Cb$.

כעת, נניח ש־d הוא פתרון של המערכת $(CA)x=Cb$. אז d מקיים $(CA)d=Cb$. לכן $((C^{-1}C)A)d=(C^{-1}C)b \iff C^{-1}((CA)d)=C^{-1}(Cb)$, ומכאן d פתרון של $Ax=b$.

מסקנה 70: אם $Ax = b$ ו־K מטריצה שהתקבלה מ־A על־ידי פעולות דירוג, אז ל־A ול־K אותם פתרונות.

4.5 טיפ לחיים

נעיר כי דירוג שומר על מרחב השורות. לכן, אם רוצים למצוא בסיס למרחב וקטורי כלשהו, מסדרים וקטורים מקבוצה פורשת, כותבים כשורות מטריצה ומדרגים. מרחב השורות האלו זהה למרחב הוקטורים המקוריים, ושורות אלו בת״ל. הקץ לבדיקות מייגעות! בהצלחה במבחן!