אלגברה לינארית 1 – המבחן...

נכתב ונערך ע"י ***דינה זליגר***

מבוסס על הרצאותיו של ***פרופ' איליה ריפס***

סמסטר א' תשס"ו

תוכן עניינים

1. אלגברה לינארית – הא?? 2
2. שדות 2
2.1. הגדרת השדה ותכונות בסיסיות 2
2.2. שדה המרוכבים 4
2.3. שדה השאריות מודולו n 5
2.4. המציין של שדה 8
2.5. תתי שדות 9
3. מרחבים וקטוריים 11
3.1. הגדרת המרחב הוקטורי 11
3.2. קוביות ב- $\mathbb{R}^n$ 13
3.3. בסיסים ומימד של מרחבים וקטוריים 14
3.4. תתי מרחבים 18
4. העתקות לינאריות 23
4.1. תכונות כלליות של העתקות 23
4.2. העתקות לינאריות של מרחבים וקטוריים 24
4.3. העתקות לינאריות ומטריצות 28
5. מערכות משוואות לינאריות 33

1. אלגברה לינארית – הא??

מהי אלגברה לינארית? ובכן, אלגברה היא תחום במתמטיקה שעוסק בפיתרון משוואות. אלגברה לינארית עוסקת בפיתרון משוואות לינאריות – כלומר משוואות שבהן הנעלמים מופיעים בחזקה ראשונה וגם לא מופיעה בהן מכפלה של נעלמים. בסוף הקורס אנחנו נראה אין פותרים מערכות משוואות. עד אז נפתח את הכלים שמאפשרים לנו לעשות זאת...*

נניח שיש לנו מערכת משוואות

$$\begin{aligned} &a_{1,1}x_1 + \ldots + a_{1,n}x_n = b_1 \\ &\vdots \\ &a_{m,1}x_1 + \ldots + a_{m,n}x_n = b_m \end{aligned}$$

מהם הפתרונות? הפתרונות הם $x_1,\ldots,x_n$ שמקיימים את המשוואת שרשומות למעלה (אם קיימים כאלה כלל). אבל מאיפה מביאים את המספרים האלה?

2. שדות

2.1. הגדרת השדה ותכונות בסיסיות

<u>הגדרה</u>: קבוצה F עם הפעולות הדו-מקומיות חיבור $(+_F)$ וכפל $(\cdot_F)$† תיקרא **שדה** אם מתקיימות התכונות הבאות אשר נקראות **אקסיומות השדה**:

1. *אקסיומות החיבור*:
   a. סגירות: לכל $a,b\in F$ $a+_F b\in F$
   b. קומוטטיביות: לכל $a,b\in F$ $a+_F b=b+_F a$
   c. אסוציאטיביות: לכל $a,b,c\in F$ $\left(a+_F b\right)+_F c=a+_F\left(b+_F c\right)$
   d. קיום איבר ניטרלי לחיבור: קיים $0_F\in F$ כך שלכל $a\in F$ $a+_F 0_F=a$‡
   e. קיום איבר נגדי לחיבור: לכל $a\in F$ קיים $-a\in F$ כך ש- $a+_F\left(-a\right)=0_F$
2. *אקסיומות הכפל*:
   a. סגירות: לכל $a,b\in F$ $a\cdot_F b\in F$§
   b. קומוטטיביות: לכל $a,b\in F$ $a\cdot_F b=b\cdot_F a$
   c. אסוציאטיביות: לכל $a,b,c\in F$ $\left(a\cdot_F b\right)\cdot_F c=a\cdot_F\left(b\cdot_F c\right)$
   d. קיום איבר ניטרלי לכפל: קיים $0_F\neq 1_F\in F$ כך שלכל $a\in F$ $a\cdot_F 1_F=a$**
   e. קיום איבר הופכי לכפל: לכל $a\in F$ אם $a\neq 0_F$ קיים $a^{-1}\in F$ כך ש- $a\cdot_F a^{-1}=1_F$
3. דיסטריביוטיביות: לכל $a,b,c\in F$ $a\cdot_F\left(b+_F c\right)=a\cdot_F c+_F b\cdot_F c$

נעיר רק שאם לא היינו דורשים ש- $0_F\neq 1_F$ היה יכול להיות קיים שדה עם איבר אחד בלבד $F=\{0\}$. זאת לא בעיה אבל זה גם לא מעניין ולכן מנענו מקרה זה מראש.

---

* כן, זה די עצוב ששיא הקורס הוא פתרון מערכת משוואות לינאריות...
† בד"כ נשמיט את סימן השדה ליד הפעולות. נרשום אותו רק לשם הדגשה.
‡ לפעמים נרשום רק 0 ולא 0_F ומההקשר תהיה ברורה הכוונה.
§ לפעמים נשמיט את סימן הכפל ואז $ab=a\cdot b$. בכל אופן הכוונה תהיה ברורה מן ההקשר.
** לפעמים נרשום רק 1 ולא 1_F ומההקשר תהיה ברורה הכוונה.

<u>דוגמאות</u>:

1. הרציונאליים $\mathbb{Q}$ עם הפעולות הרגילות (מושאר לקורא לוודא שאכן מתקיימות האקסיומות)
2. הממשיים $\mathbb{R}$ עם הפעולות הרגילות (כנ"ל)
3. $\mathbb{Z}_2=\{0,1\}$ ופעולות שמוגדרות ע"י הטבלאות הבאות:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

יש לבדוק שמתקיימות פה אקסיומות השדה. כמעט את כל האקסיומות ניתן להסיק מיידית מהטבלאות. נותר לבדוק אסוציאטיביות ודיסטריביוטיביות. הבדיקות האלה הן סופיות משום שיש מספר סופי של איברים. לא נעשה זאת כאן באופן מלא, אבל נראה שתי דוגמאות:

$$(0+1)+1=1+1=0=0+0=0+(1+1)$$
$$1\cdot(1+0)=1\cdot1=1=1+0=1\cdot1+1\cdot0$$

4. הקבוצה $\{z,u\}$ עם הפעולות שמוגדרות לפי הטבלאות:

$+$	z	u
z	z	u
u	u	z

$\cdot$	z	u
z	z	z
u	z	u

השדה הזה זהה ל-$\mathbb{Z}_2$ מלבד שלאיברים בקבוצה קוראים בשם אחד. שדות אלה נקראים שדות איזומורפיים[††]

5. המרוכבים $\mathbb{C}=\{a+bi:a,b\in\mathbb{R}\}$ עם הפעולות חיבור וכפל שמוגדרות באופן הבא:

$$(a+bi)+(c+di)=(a+c)+(b+d)i$$
$$(a+bi)\cdot(c+di)=(ac-bd)+(ad+bc)i$$

גם כאן הבדיקה של קיום האקסיומות הינה שגרתית. נציין רק כי $0_{\mathbb{C}}=0+0\cdot i$ ו-$1_{\mathbb{C}}=1+0\cdot i$.

בתרגיל מס' 1 הוכחנו כל מיני תכונות של שדות שנובעות ישירות מן ההגדרה. לא אוכיח אותן כאן מאחר שהדבר נעשה כבר:
אם F שדה אזי לכל $a,b,c\in F$ מתקיימות התכונות הבאות:

1. *תכונת הצמצום בחיבור*: $a+c=b+c\Rightarrow a=b$
2. *תכונת הצמצום בכפל*: אם $c\neq0$ מתקיים $ac=bc\Rightarrow a=b$
3. $0\cdot a=0$
4. אם $a\neq0$ מתקיים $\left(a^{-1}\right)^{-1}=a$
5. $-(-a)=a$
6. $(-1)a=-a$
7. $(-a)(-b)=ab$
8. $(-a)b=a(-b)=-(ab)$
9. $(ab)^{-1}=a^{-1}b^{-1}$
10. אם $ab=0$ אז $a=0$ או $b=0$

כמו כן ניתן להוכיח האיברים הניטרליים לפעולות הן יחידים ושהאיבר הנגדי לחיבור והאיבר ההופכי לכפל יחידים גם הם.
ההוכחה נעשית ע"י הנחה שקימים שניים אשר מקיימים את התכונה הנחוצה והוכחה שהשניים האלה חייבים להיות זהים (ע"י שימוש בתכונות הצמצום לחיבור ולכפל).

[††] נדבר על איזומורפיזמים עוד בהמשך

2.2. שדה המרוכבים

נדון באופן מפורט יותר בשדה המספרים המרוכבים. בהגדרה בסעיף הקודם לא נתנו משמעות ל- i. בעצם התייחסנו אליו כאל סמל בלבד. ננסה בכל זאת להבין מהו i זה. נשים לב ש-

$$(0+1\cdot i)(0+1\cdot i)=(0\cdot 0-1\cdot 1)+(0\cdot 1+1\cdot 0)i=-1+0\cdot i$$

כלומר $i^2=-1$. אהא! בממשיים למספרים שליליים לא קיים שורש ממעלה זוגית. מסתבר שבמרוכבים המצב הוא שונה. בעצם לשם כך הוגדר שדה מרוכבים. שדה המרוכבים הוא שדה סגור אלגברית – שדה שבו לכל פולינום יש שורש. למשל נסתכל על $x^2+1=0$. ב- $\mathbb{R}$ אין לפולינום זה שורש, שכן לכל x $x^2\geq 0$ ולכן $x^2+1\geq 1>0$. אבל ב- $\mathbb{C}$ דווקא יש שורש והוא i: $i^2+1=-1+1=0$...

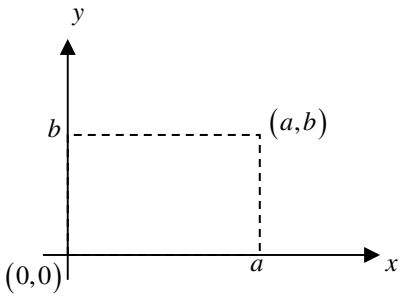
אגב, תכונה זו מסבירה את נוסחת הכפל. אם נכפול את המספרים המרוכבים כפי שאנחנו רגילים בממשיים נקבל:

$$(a+bi)\cdot(c+di)=ac+adi+bci+bdi^2=ac+adi+bci+bd(-1)=(ac-bd)+(ad+bc)i$$

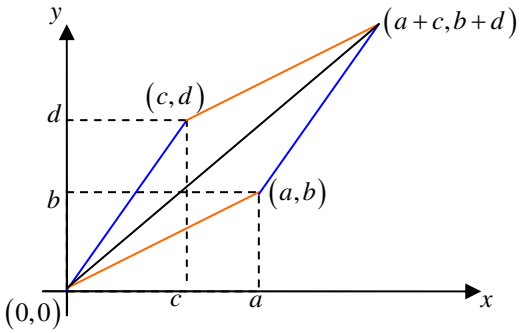
כמו כן נשים לב שניתן לזהות את הממשיים עם תת קבוצה של המרוכבים: $\mathbb{R}=\{a+bi\in\mathbb{C}:b=0\}$. נראה שגם הפעולות מתלכדות:

$$(a+0\cdot i)+(c+0\cdot i)=(a+c)+(0+0)i=(a+c)+0\cdot i$$
$$(a+0\cdot i)\cdot(c+0\cdot i)=(ac-0\cdot 0)+(a\cdot 0+0\cdot c)i=ac+0\cdot i$$

אפשר לחשוב על המרוכבים גם בצורה גאומטרית נסתכל על מערכת צירים במישור $[xy]$. למספר $a+bi$ נתאים את הנקודה (a,b). בתיאור זה המספרים הממשיים נמצאים רק על ציר ה- x.

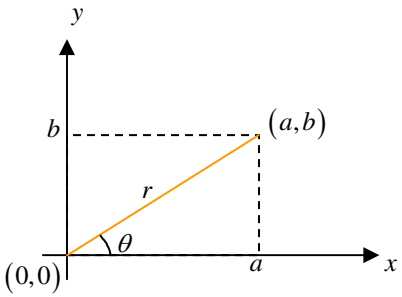


איך נחבר מרוכבים באופן גאומטרי? נשים לב שהנקודה המתאימה ל- $(a+bi)+(c+di)=(a+c)+(b+d)i$ היא $(a,b)+(c,d)=(a+c,b+d)$.



ומה עם הכפל? זה קצת מסובך יותר. לשם כך נגדיר את ההצגה הקוטבית של מספר מרוכב. זאת בעצם ההצגה הקוטבית של המישור $[xy]$. אם נסתכל של הציור נראה שכל נקודה אפשר גם לאפיין לפי המרחק שלה מהראשית יחד עם הזווית שנוצרת עם ציר ה- x.

החיבור מתבצע לפי כלל *המקבילית*:
הקודקוד הרביעי של המקבילית שנבנית ע"י נקודת הראשית ונקודות שני המחוברים היא הסכום.



לפי מה שלמדנו בתיכון בטריגו[‡‡] אנחנו יודעים שמתקיים היחס הבא:

$$r=\sqrt{a^2+b^2}$$
$$\tan\theta=\frac{b}{a}\Rightarrow\theta=\arctan\frac{b}{a}$$

ומצד שני $a=r\cos\theta, b=r\sin\theta$. לכן כל מספר מרוכב ניתן לרשום בשתי דרכים:

$$a+bi=r\cos\theta+r\sin\theta i=r(\cos\theta+i\sin\theta)\equiv r\,\mathrm{cis}\,\theta.$$

כעת אנחנו יכולים לכפול מספרים מרוכבים בהצגה הקוטבית שלהם.

$$(a+bi)(c+di)=r_1\,\mathrm{cis}\,\theta_1\cdot r_2\,\mathrm{cis}\,\theta_2=r_1r_2(\cos\theta_1+i\sin\theta_1)(\cos\theta_2+i\sin\theta_2)=$$
$$=r_1r_2\left((\cos\theta_1\cos\theta_2-\sin\theta_1\sin\theta_2)+(\cos\theta_1\sin\theta_2+\sin\theta_1\cos\theta_2)i\right)=r_1r_2\,\mathrm{cis}(\theta_1+\theta_2)$$

[‡‡] למעשה בתיכון גם למדנו את כל זה לגבי המספרים המרוכבים ואפילו יותר...

אז מה אנחנו רואים? כדי לכפול שני מרוכבים בהצגה הקוטבית שלהם יש לכפול את האורכים ולחבר את הזוויות. זה מאפשר לנו לכפול מספרים באופן גיאומטרי... (לא בא לי לשרטט את זה)

נגדיר **ערך מוחלט** של מספר מרוכב $|a+bi|=\sqrt{a^2+b^2}$ ו**צמוד** של מספר מרוכב $\overline{a+bi}=a-bi$.

נציין כמה תכונות של מספרים מרוכבים: לכל $z_1,z_2\in\mathbb{C}$ מתקיים:

1. $|z_1z_2|=|z_1||z_2|$
2. $|z_1|=|\overline{z_1}|$
3. $|z_1|^2=z_1\overline{z_1}$
4. אם $z_1=r\operatorname{cis}\theta$ $z_1^n=|\overline{z_1}|^n\operatorname{cis}n\alpha$
5. אי שיוויון המשולש: $|z_1+z_2|\le|z_1|+|z_2|$

ההוכחות הן ישירות. פשוט מביעים את המספרים בצורה קוטבית או קרטזית ומחשבים. את (4) מוכיחים באינדוקציה על n.

מה שיותר מעניין הוא שלמשוואה $\operatorname{cis}\alpha=x^n$ יש במרוכבים n פתרונות שונים...

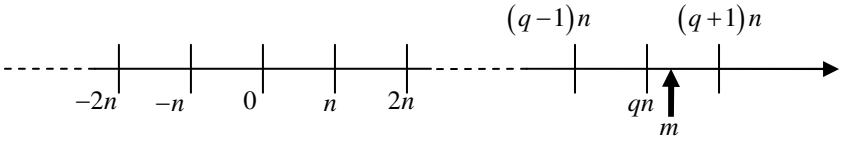
[§§] $x_i=\operatorname{cis}\left(\frac{\alpha+(i-1)2\pi}{n}\right),i=1,...,n$

2.3. שדה השאריות מודולו n

נזכור את השדה $\mathbb{Z}_2$. האם ניתן להגדיר שדה $\mathbb{Z}_n$ לכל n באופן דומה? התשובה היא שלא! לא לכל n מתקבל שדה. נראה עתה כמה משפטים בנושא...

יהי $n\in\mathbb{N}^+$ ויהיו $k,l\in\mathbb{Z}$. נאמר ש-$k\equiv l\pmod n$ אם קיים $u\in\mathbb{Z}$ כך ש-$k-1=un$. כלומר ההפרש בין המספרים k,l הוא כפולה שלמה של n. אומרים אז ש-k,l **שקולים מודולו** n. למשל שני מספרים חיוביים שקולים מודולו 10 כאשר הם נגמרים באותה הספרה. כל שני מספרים זוגיים וכל שני מספרים איזוגיים שקולים מודולו 2.

<u>טענה 1</u>: יהי $n\in\mathbb{N}^+$. לכל $m\in\mathbb{Z}$ קיימים $q,r\in\mathbb{Z}$ [***] כאשר $0\le r\le n-1$ כך ש-$m=qn+r$.
<u>הערה</u>: אם $r=0$ אז $n\mid m$ כלומר m מתחלק ב-n ללא שארית.
<u>הוכחה</u>: נסתכל בכפולות של המספר n: $...,-2n,-n,0,n,2n,3n,...$



קיים qn כך ש-$qn\le m<(q+1)n$. אז $m-qn=r\in\mathbb{Z}$. ברור ש-r זה מקיים את הדרוש. מש"ל ☺

<u>טענה 2</u>: יהיו $m_1,m_2\in\mathbb{Z}$. אזי $m_1\equiv m_2\pmod n$ אמ"מ השארית של m_1 בחלוקה ב-n שווה לשארית של m_2 בחלוקה ב-n.
<u>הוכחה</u>: לפי הטענה הקודמת אפשר לרשום $m_1=q_1n+r_1,m_2=q_2n+r_2$ כאשר $0\le r_1,r_2\le n-1$.
($\Leftarrow$) נניח $m_1\equiv m_2\pmod n$. אזי קיים $u\in\mathbb{Z}$ כך ש-$m_1-m_2=un$. כלומר
$(q_1n+r_1)-(q_2n+r_2)=(q_1-q_2)n+(r_1-r_2)=un$. אזי $r_1-r_2=(u-q_1+q_2)n$. כמו כן
$-(n-1)\le r_1-r_2\le n-1$. אבל $n\mid(r_1-r_2)$ ולכן $r_1-r_2=0$.

[§§] נדמה לי שבתיכון קוראים לזה משפט דה-מואבר
[***] q ל-quotient ו-r ל-residue

($\Rightarrow$) נניח ש- $r_1 = r_2 = r$. אזי $m_1 - m_2 = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n$. אבל $q_1 - q_2 \in \mathbb{Z}$. לכן $m_1 \equiv m_2 \pmod n$. מש"ל ☺

נסמן את השארית של m בחלוקה ב- n ע"י $[m]_n$. אז תחת סימון זה קיבלנו בטענה הקודמת ש-

$$[m_1]_n = [m_2]_n \Leftrightarrow m_1 \equiv m_2 \pmod n$$

נסמן את כל השאריות מודולו n: $\mathbb{Z}_n = \{0,1,...,n-1\}$. ברור ש- $|\mathbb{Z}_n| = n$ (כלומר בקבוצה זו יש n איברים - n שאריות אפשריות).

כמו כן נגדיר פעולות חיבור מודולו n ($+_n$) וכפל מודולו n ($\cdot_n$) באופן הבא:

לכל $a,b \in \mathbb{Z}_n$ $a +_n b = [a+b]_n$ ו- $a \cdot_n b = [ab]_n$[†††].

נשאלת אפוא השאלה, האם $\mathbb{Z}_n$ עם הפעולות הנ"ל הוא שדה?

<u>משפט 3</u>: לכל $1 < n \in \mathbb{N}$ ב- $\mathbb{Z}_n$ עם הפעולות $+_n, \cdot_n$ מתקיימות כל אקסיומות השדה מלבד אולי קיום הופכי.

<u>הוכחה</u>: לצורך ההוכחה נצטרך להיעזר במספר טענות עזר.

<u>טענת עזר 1</u>: $m \in \mathbb{Z}, m \equiv [m]_n \pmod n$

<u>הוכחה</u>: נניח ש- $m = qn + [m]_n$. אזי $m - [m]_n = qn$ ו- $q \in \mathbb{Z}$. מש"ל ☺

<u>טענת עזר 2</u>: אם $k_1 \equiv k_2 \pmod n$ ו- $l_1 \equiv l_2 \pmod n$ אז $k_1 + l_1 \equiv (k_2 + l_2) \pmod n$

<u>הוכחה</u>: $k_1 \equiv k_2 \pmod n$ לכן $k_1 - k_2 = u_k n$. $l_1 \equiv l_2 \pmod n$ לכן $l_1 - l_2 = u_l n$ כאשר $u_k, u_l \in \mathbb{Z}$. אזי

$(k_1 + l_1) - (k_2 + l_2) = (k_1 - k_2) + (l_1 - l_2) = u_k n + u_l n = (u_k + u_l)n$. מש"ל ☺

<u>טענת עזר 3</u>: אם $k_1 \equiv k_2 \pmod n$ ו- $l_1 \equiv l_2 \pmod n$ אז $k_1 \cdot l_1 \equiv (k_2 \cdot l_2) \pmod n$.

<u>הוכחה</u>: $k_1 \equiv k_2 \pmod n$ לכן $k_1 - k_2 = u_k n$. $l_1 \equiv l_2 \pmod n$ לכן $l_1 - l_2 = u_l n$. אזי

$k_1 l_1 - k_2 l_2 = (l_1 - l_2)k_1 + (k_1 - k_2)l_2 = u_l n k_1 + u_k n l_2 = (u_l k_1 + u_k l_2)n$. $u_l k_1 + u_k l_2 \in \mathbb{Z}$. מש"ל ☺

<u>טענת עזר 4</u>: היחס $\equiv$ הוא יחס שקילות.

<u>הוכחה</u>:

רפלקסיביות: ברור $k \equiv k \pmod n$ שהרי $k - k = 0 = 0 \cdot n$.

סימטריות: אם $k_1 \equiv k_2 \pmod n$ אז $k_1 - k_2 = un$. לכן $k_2 - k_1 = (-u)n$ ומכאן ש- $k_2 \equiv k_1 \pmod n$.

טרנזיטיביות: נניח $k_1 \equiv k_2 \pmod n$ ו- $k_2 \equiv k_3 \pmod n$. אזי $k_1 - k_2 = u_1 n$ ו- $k_2 - k_3 = u_2 n$. אזי

$k_1 - k_3 = (k_1 - k_2) + (k_2 - k_3) = u_1 n + u_2 n = (u_1 + u_2)n$. לכן $k_1 \equiv k_3 \pmod n$. מש"ל ☺

כעת נחזור להוכחת המשפט. נראה שמתקיימות כל האקסיומות פרט לקיום הופכי כפלי.

סגירות: ברור מהגדרת השארית - $0 \le [m]_n \le n-1$. לכן $\mathbb{Z}_n$ סגורה גם תחת חיבור מודלו n וגם תחת כפל מודולו n.

קומוטטיביות: נובע מהקומוטטיביות ב- $\mathbb{Z}$: יהיו $a,b \in \mathbb{Z}_n$. אזי

$$a +_n b = [a+b]_n = [b+a]_n = b +_n a$$
$$a \cdot_n b = [ab]_n = [ba]_n = b \cdot_n a$$

אסוציאטיביות: נובע מהאסוציאטיביות בשלמים ומטענות העזר: יהיו $a,b,c \in \mathbb{Z}_n$. אזי

$(a +_n b) +_n c = \left[(a +_n b) + c\right]_n = \left[[a+b]_n + c\right]_n$. אבל לפי ט"ע 1 $a + b \equiv [a+b]_n \pmod n$. לפי ט"ע 4

$(a+b) + c \equiv \left([a+b]_n + c\right) \pmod n$. כעת לפי ט"ע 2. לפי טענה (2)

$\left[[a+b]_n + c\right]_n = \left[(a+b) + c\right]_n$. כלומר $(a +_n b) +_n c = \left[(a+b)+c\right]_n$. כעת לפי האסוציאטיביות בשלמים

$(a +_n b) +_n c = \left[(a+b)+c\right]_n = \left[a+(b+c)\right]_n = a +_n (b +_n c)$ באותו אופן חוזרים לכך ש- $\left[a+(b+c)\right]_n$.

בדיוק באותו אופן מראים את האסוציאטיביות של הכפל רק שמקום בט"ע 2 משתמשים בט"ע 3.

קיום איברים ניטרליים: לכל $a \in \mathbb{Z}_n$ $a +_n 0 = [a+0]_n = [a]_n = a$ וכן $a \cdot_n 1 = [a \cdot 1]_n = [a]_n = a$.

קיום איבר נגדי לחיבור: אם $a = 0$ אז $-_n a = 0$ ואכן $0 +_n 0 = [0+0]_n = [0]_n = 0$. אם $a \ne 0$ אז

$-_n a = n - a \in \mathbb{Z}_n$ ואכן $a +_n (n-a) = \left[a + (n-a)\right]_n = [n]_n = 0$.

[†††] ברור שניתן להשתמש בפעולות אלה לכל $k,l \in \mathbb{Z}$ אבל כרגע אנחנו מעוניינים רק במקרה של $\mathbb{Z}_n$.

דיסטריביוטיביות: יהיו $a,b,c\in\mathbb{Z}_n$. אזי

$$a\cdot_n\left(b+_n c\right)=\left[a\left(b+_n c\right)\right]_n=\left[a\left[b+c\right]_n\right]_n=\left[a\left(b+c\right)\right]_n=\left[ab+ac\right]_n$$
$$=\left[\left[ab\right]_n+\left[ac\right]_n\right]_n=\left[a\cdot_n b+a\cdot_n c\right]_n=a\cdot_n b+_n a\cdot_n c$$

ראינו שמתקיימות כל האקסיומות מלבד אולי קיום הופכי כפלי. מש"ל ☺

נסתכל על $\mathbb{Z}_4=\{0,1,2,3\}$ ונרשום את טבלאות החיבור והכפל לפי ההגדרה:

$+_n$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_n$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

מהטבלאות רואים בבירור שלא קיים הופכי כפלי ל- 2.
אז באמת לא בהכרח אקסיומה זו מתקיימת בכל $\mathbb{Z}_n$.

<u>משפט 4</u>: אם $n>1$ לא ראשוני אז $\mathbb{Z}_n$ אינו שדה.
<u>הוכחה</u>: $n>1$ פריק ולכן $n=kl$ כאשר $1<k,l<n$. לכן $k,l\in\mathbb{Z}_n$. אבל אז $k\cdot_n l=\left[kl\right]_n=\left[n\right]_n=0$. אבל זו סתירה כי בשדה אין מחלקי אפס. ☺

<u>משפט 5</u>: אם p ראשוני אז $\mathbb{Z}_p$ שדה.
<u>הוכחה 1</u>: ראינו שמתקיימות כל התכונות מלבד אולי קיום הופכי. נראה אם כן שאם p ראשוני אז לכל $0\neq a\in\mathbb{Z}_p$ קיים איבר הופכי. נסתכל בקבוצה האיברים $\left\{a\cdot_p 0,...,a\cdot_p\left(p-1\right)\right\}\subset\mathbb{Z}_p$. נטען שכל האיברים בקבוצה זו שונים. אם לא, אז קיימים $k\neq l\ \ k,l\in\mathbb{Z}_p$ כך ש- $a\cdot_p k=a\cdot_p l$. כלומר $\left[ak\right]_p=\left[al\right]_p$. אזי $ak\equiv al\left(\mathrm{mod}\ p\right)$ כלומר קיים $u\in\mathbb{Z}$ כך ש- $a\left(k-l\right)=ak-al=up$. לכן $p\mid a\left(k-l\right)$. לכן $p\mid a$ או $p\mid k-l$[‡‡‡]. אבל $0<a\leq p-1$ ולכן $p\nmid a$. כמו כן $0\leq k,l\leq p-1$ לכן $-\left(p-1\right)\leq k-l\leq p-1$. אבל $k\neq l$ ולכן $k-l\neq 0$. לכן $p\nmid\left(k-l\right)$. וזו סתירה. לכן לא קיימים k,l כאלה ולכן כל האיברים שונים. בקבוצה זו יש p איברים ולכן היא בעצם כל $\mathbb{Z}_p$. כלומר בתוכה יש גם האיבר 1. ולכן יש הופכי ל- a. מש"ל ☺
<u>הוכחה 2</u>: ראשית נוכיח טענת עזר.
<u>טענת עזר</u>: אם m הוא המחלק המשותף המקסימלי של $0<k,l$ אז קיימים $s,t\in\mathbb{Z}$ כך ש- $ks+lt=m$.
<u>הוכחה</u>: באינדוקציה שלמה[§§§] על הסכום $k+l$:
בסיס האינדוקציה: עבור $k=l=1$ המחלק המשותף המקסימלי שלהם הוא 1. ניקח $s=1,t=0$ ואז $1\cdot 1+1\cdot 0=1$.
הנחת האינדוקציה: נניח הטענה נכונה לכל k',l' שמקיימים $k'+l'<k+l$.
שלב האינדוקציה: אם $k=l$ אז המחלק המשותף המקסימלי הוא $m=k=l$ ואז $1\cdot k+0\cdot l=m$.
אחרת נניח בה"כ כי $k<l$. נטען ש- m הוא המחלק המשותף המקסימלי של k ו- $l-k$. m מחלק את k ואת l ולכן כמובן מחלק גם את $l-k$. ניח כעת ש- m' מחלק גם את k וגם את $l-k$. לכן הוא מחלק גם את l. כלומר m' הוא מחלק משותף של k ושל l. לכן $m'\leq m$. לכן m' הוא המחלק המשותף המקסימלי.
נשים לב ש- $k+\left(l-k\right)=k<l+k$. לכן ניתן להשתמש בהנחת האינדוקציה. אז קיימים $s',t'\in\mathbb{Z}$ כך ש- $\left(s'-t'\right)k+t'l=s'k+t'\left(l-k\right)=m$. ניקח $s=s'-t',t=t'$ ונקבל את הטענה עבור k,l.
לפי עיקרון האינדוקציה הטענה נכונה לכל סכום $k+l$, כלומר היא נכונה לכל k,l. מש"ל ☺
יהי $0\neq a\in\mathbb{Z}_p$. משום ש- p ראשוני המחלק המשותף שמקסימלי שלו ושל a הוא 1. לפי הטענה קיימים s,t כך ש- $a\cdot s+t\cdot p=1$. אזי $\left[1\right]_p=1$. $a\cdot_p\left[s\right]_p=a\cdot_p s=\left[as\right]_p=\left[1-pt\right]_p=\left[1\right]_p$. כלומר $\left[s\right]_p=a^{-1}$. ☺

<u>משפט 6</u>: לכל p ראשוני ולכל $m>0$ יש שדה עם p^m איברים. למעשה יש שדה יחיד כזה עד כדי איזומורפיזם.
<u>הוכחה</u>: ר' קורס בתורת השדות.

[‡‡‡] אם ראשוני מחלק מכפלה של מספרים אזי הוא מחלק אחד מהם (לפחות)
[§§§] עיקרון האינדוקציה השלמה: אם הטענה נכונה לכל $k<n$ ומוכיחים שהטענה נכונה ל- n אז היא נכונה לכל n.

נציין כמה תכונות מעניינות ב- $\mathbb{Z}_p$:

1. $p-1=p-1$. $(p-1)!=\prod_{i=1}^{p-1} i=1\cdot 2\cdot ....\cdot (p-1)$. מדוע? נשים לב שבמכפלה זו יש $p-1$ מוכפלים ולכל אחד מהם, חוץ משאר ל-1 ול-$p-1$ ההופכי שלו מופיע במכפלה. לכן הם כולם מתבטלים ואנחנו נשארים עם $1\cdot(p-1)=p-1$.
2. לכל $a\in\mathbb{Z}_p$ מתקיים $a^p=a$. מדוע? אם $a=0$ ברור שזה נכון. אחרת נסתכל בקבוצה $\{na:0\neq n\in\mathbb{Z}_p\}$. ברור ש- 0 אינו נמצא בקבוצה הזו וגם כל האיברים שונים, לכן יש בה $p-1$ איברים שונים מאפס, ולכן הקבוצה מכילה את כל איברי $\mathbb{Z}_p$ השונים מאפס. לפי תכונה (1) $(n_1a)(n_2a)...(n_{p-1}a)=a^{p-1}(p-1)!=a^{p-1}(p-1)$. אבל מאחר ששהם כבעצם כל איברי השדה אז גם $(n_1a)(n_2a)...(n_{p-1}a)=(p-1)!=p-1$. כלומר $a^{p-1}(p-1)=p-1$. אבל $p-1\neq 0$ ולכן $a^{p-1}=1$ *. כלומר $a^p=a$. נעיר רק שכל סימני השוויון שמופיעים כאן הם מודולו p . את (*) ניתן היה לרשום למעשה באופן הבא: לכל p ראשוני ולכל $a\neq 0$ $a^{p-1}\equiv 1(\bmod p)$.

2.4. המציין של שדה

נגדיר רישום מקוצר של חיבור איבר בשדה לעצמו מספר פעמים: יהי $a\in F$ ויהי $n\in\mathbb{Z}$. אזי נגדיר באופן רקורסיבי:

$$n\times a=\begin{cases}0 & n=0\\ (n-1)\times a+a & 1\le n\\ -((-n)\times a) & n<0\end{cases}$$

קל להוכיח את השיוויונים הבאים:

$$n\times a+m\times a=(n+m)\times a$$
$$(nm)\times a=n\times(m\times a)=(n\times a)(m\times a)$$

נעיר רק שיש להיזהר ולא להתבלבל בין $\cdot$ שהוא כפל בין איברים בשדה לבין $\times$ שהוא פעולה בין איברים בשדה לבין המספרים השלמים. אם $a,b\in F,n\in\mathbb{Z}$ הביטויים הבאים אינם מוגדרים: $a\times b,a\times n,a\cdot n,n\cdot a$.

<u>משפט 7</u>: יהי שדה F . אזי מתקיים אחד מהבאים:

1. לכל $m,n\in\mathbb{Z}$ כך ש- $m\neq n$ מתקיים $m\times 1_F\neq n\times 1_F$
2. קיים ראשוני p כך ש- $p\times 1_F=0_F$.

<u>הוכחה</u>: אם מתקיים (1) אז סיימנו. אחרת נראה שחייב להתקיים (2).
יהיו $m,n\in\mathbb{Z}$ כך ש- $m\times 1_F=n\times 1_F$. בה"כ נניח כי $m<n$. אזי $m\times 1_F+(n-m)\times 1_F=n\times 1_F=m\times 1_F$. לכן $(n-m)\times 1_F=0_F$. נסמן ב- p את המספר הקטן ביותר שמקיים $(n-m)\times 1_F=0_F$. נראה ש- p ראשוני. נניח בשלילה שקיימים $1<k,l<p$ כך ש- $kl=p$. לכן מתקיים $0_F=p\times 1_F=(kl)\times 1_F=(k\times 1_F)\cdot(l\times 1_F)$. לכן $k\times 1_F=0_F$ או $k\times 1_F=0_F$ בסתירה למינימליות של p . מש"ל ☺****

במקרה הראשון נאמר ש- $\operatorname{char}F=0$ והשדה הוא עם **מציין** 0 . ואילו אחרת נאמר ש- $\operatorname{char}F=p$ והמציין של השדה הוא p .

**** בהוכחה הראנו שהמינימליות של p גוררת את זה שהוא ראשוני. אבל גם הכיוון ההפוך נכון. לכן ניתן לומר באופן שקול שמציין של שדה הוא המספר המינימלי ששונה מאפס ומקיים $p\times 1_F=0_F$ (אם קיים כזה).

2.5. תתי שדות

<u>הגדרה</u>: יהיו F,S שדות. נאמר שהם **איזומורפיים** אם קיים ביניהם **איזומורפיזם**, כלומר העתקה $f:F\to S$ חח"ע ועל כך שלכל $a,b\in F$ היא שומרת על הפעולות:

$$f\left(a+_F b\right)=f\left(a\right)+_S f\left(b\right)$$
$$f\left(a\cdot_F b\right)=f\left(a\right)\cdot_S f\left(b\right)$$

חשוב לציין שאם שני מבנים איזומורפיים אז הם מקיימים אם אותן התכונות. למשל, אם הקבוצות F,S איזומורפיות ו- F שדה אזי גם S שדה. זה נובע בקלות מהגדרת האיזומורפיזם. זו תכונה חשובה מאוד של איזומורפיזמים ואנחנו נשתמש בה גם בהמשך כאשר נלמד על מרחבים וקטוריים.

<u>הגדרה</u>: יהי F שדה ותהי $K\subset F$ תת קבוצה. נאמר ש- K תת שדה אם היא מקיימת את כל אקסיומות השדה ביחס לפעולות שמוגדרות על F.

למשל, $\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$ והם תת שדות.

נעיר את תשומת ליבנו לתכונות הבאות:

1. לא קיים שדה F כך ש- $\mathbb{R}\subsetneq F\subsetneq\mathbb{C}$
2. קיימים שדות רבים F כך ש- $\mathbb{Q}\subsetneq F\subsetneq\mathbb{R}$. למשל $\mathbb{Q}\left[\sqrt{2}\right]=\left\{a+\sqrt{2}b:a,b\in\mathbb{Q}\right\}$ עם הפעולות כמו בממשיים.
3. שדה הרציונליים $\mathbb{Q}$ (או שדות איזומורפיים לו) הוא השדה המינימלי בעל מציין 0. מדוע? בכל שדה F חייבים להיות איבר היחידה 1. בגלל הסגירות תחת חיבור לכל $n\in\mathbb{N}$ מתקיים גם $n\times1\in F$. כך קיבלנו שכל הטבעיים חייבים להיות בשדה. בגלל קיום האיבר הנגדי נקבל שכל השלמים חייבים להיות בשדה. ובגלל קיום איבר הופכי וסגירות לכפל נקבל שכל מנה של שלמים חייבת להיות בשדב וזה הרי בדיוק שדה הרציונליים...

<u>משפט 8</u>: אם $\operatorname{char}F=p>0$ אז קיים תת שדה K של F איזומורפי ל- $\mathbb{Z}_p$.

<u>הוכחה</u>: נגדיר $K=\left\{n\times1_F:0\le n\le p-1\right\}$. בגלל הסגירות ב- F ברור ש- $K\subset F$.

נגדיר העתקה $f:\mathbb{Z}_p\to K$ באופן הבא $f\left(a\right)=a\times1_F$. נראה שזהו איזומורפיזם.

חח"ע: יהיו $a,b\in\mathbb{Z}_p$ כך ש- $a\times1_F=f\left(a\right)=f\left(b\right)=b\times1_F$. נניח ש- $a\ne b$. אזי $a-b\ne0$. כמו במשפט הקודם $0\le a,b\le p-1$ לכן $b\times1_F+\left(a-b\right)\times1_F=a\times1_F=b\times1_F$. לכן $\left(a-b\right)\times1_F=0_F$.

$-p<-\left(p-1\right)\le a-b\le p-1<p$ בסתירה למינימליות של p (בהיותו המציין). לכן $a=b$.

על: יהי $k\in K$ אזי ע"פ הגדרת K $k=m\times1_F$ כאשר $0\le m\le p-1$ כלומר $m\in\mathbb{Z}_p$. לכן $f\left(m\right)=k$.

שמירה על חיבור: יהיו $a,b\in\mathbb{Z}_p$. נניח ש- $a+b=qp+r$ (חילוק עם שארית). אזי

$$f\left(a\right)+_F f\left(b\right)=\left(a\times1_F\right)+\left(b\times1_F\right)=\left(a+b\right)\times1_F=\left(qp+r\right)\times1_F=\left(qp\right)\times1_F+r\times1_F=$$
$$=q\times\left(p\times1_F\right)+r\times1_F=q\times0_F+r\times1_F=0_F+r\times1_F=r\times1_F=\left[a+b\right]_p\times1_F=\left(a+_p b\right)\times1_F=f\left(a+_p b\right)$$

שמירה על כפל: יהיו $a,b\in\mathbb{Z}_p$. נניח ש- $ab=qp+r$ (חילוק עם שארית). אזי

$$f\left(a\right)\cdot_F f\left(b\right)=\left(a\times1_F\right)\cdot\left(b\times1_F\right)=\left(ab\right)\times1_F=\left(qp+r\right)\times1_F=\left(qp\right)\times1_F+r\times1_F=$$
$$=q\times\left(p\times1_F\right)+r\times1_F=q\times0_F+r\times1_F=0_F+r\times1_F=r\times1_F=\left[a\cdot b\right]_p\times1_F=\left(a\cdot_p b\right)\times1_F=f\left(a\cdot_p b\right)$$

מצאנו איזומורפיזם בין K ל- $\mathbb{Z}_p$. לפי משפט (5) $\mathbb{Z}_p$ שדה. לכן גם K שדה, והוא תת שדה של F כמובן. מש"ל ☺

<u>משפט 9</u>: אם F שדה ו- $\operatorname{char}F=0$ אז קיים תת שדה $K\subset F$ כך ש- K איזומורפי ל- $\mathbb{Q}$.

<u>הערה</u>: זה הניסוח הפורמלי של הערה (3) קודם לכן.

<u>הוכחה</u>: נגדיר העתקה $g:\mathbb{Q}\to F$ באופן הבא $g\left(\frac{m}{n}\right)=\left(m\times1_F\right)\left(n\times1_F\right)^{-1}$. נגדיר $K=g\left(\mathbb{Q}\right)\subset F$.

נראה שההעתקה מוגדרת היטב. $n \neq 0$ ומאחר ש-$charF = 0$ $n \times 1_F \neq 0_F$. לכן קיים $\left(n \times 1_F\right)^{-1}$ וההעתקה מוגדרת לכל מספר רציונלי m/n. כעת נראה שההעתקה פועלת באותו אופן לכל רציונלי ללא תלות בצורת ההצגה שלו. יהי $\frac{m}{n} \in \mathbb{Q}$ ויהי $l \neq 0$. נראה ש-$g\left(\frac{m}{n}\right) = g\left(\frac{ml}{nl}\right)$:

$$g\left(\frac{ml}{nl}\right) = \left((ml) \times 1_F\right)\left((nl) \times 1_F\right)^{-1} = \left(\left(m \times 1_F\right)\left(l \times 1_F\right)\right)\left(\left(n \times 1_F\right)\left(l \times 1_F\right)\right)^{-1} =$$

$$= \left(\left(m \times 1_F\right)\left(l \times 1_F\right)\right)\left(\left(l \times 1_F\right)\left(n \times 1_F\right)\right)^{-1} = \left(\left(m \times 1_F\right)\left(l \times 1_F\right)\right)\left(\left(l \times 1_F\right)\left(n \times 1_F\right)\right)^{-1} =$$

$$= \left(\left(m \times 1_F\right)\left(l \times 1_F\right)\right)\left(\left(l \times 1_F\right)^{-1}\left(n \times 1_F\right)^{-1}\right) = \left(m \times 1_F\right)\left(\left(l \times 1_F\right)\left(l \times 1_F\right)^{-1}\right)\left(n \times 1_F\right)^{-1} =$$

$$= \left(m \times 1_F\right)1_F\left(n \times 1_F\right)^{-1} = \left(m \times 1_F\right)\left(n \times 1_F\right)^{-1} = g\left(\frac{m}{n}\right)$$

כעת נסתכל על $f : Q \to g\left(\mathbb{Q}\right)$ אשר פועלת בצורה זהה ל-g אך הטווח שלה מצומצם לתמונה של g. בעצם כפינו על f להיות על. נראה שהיא חח"ע: יהיו $\frac{m}{n}, \frac{s}{t} \in \mathbb{Q}$ כך ש-$f\left(\frac{m}{n}\right) = f\left(\frac{s}{t}\right)$. כלומר $\left(m \times 1_F\right)\left(n \times 1_F\right)^{-1} = \left(s \times 1_F\right)\left(t \times 1_F\right)^{-1}$. אבל כמו כן מתקיים $f\left(\frac{mt}{nt}\right) = f\left(\frac{ns}{nt}\right)$ כלומר $\left((mt) \times 1_F\right)\left((nt) \times 1_F\right)^{-1} = \left((ns) \times 1_F\right)\left((nt) \times 1_F\right)^{-1}$. לכן $\left((mt) \times 1_F\right) = \left((ns) \times 1_F\right)$ כלומר $\left(mt - ns\right) \times 1_F = \left((mt) \times 1_F\right) - \left((ns) \times 1_F\right) = 0_F$. אבל $\text{char } F = 0$ ולכן $mt - ns = 0$. כלומר $mt = ns$ ומכאן ש-$\frac{m}{n} = \frac{s}{t}$. כלומר f חח"ע.

נראה ש-f שומרת על הפעולות. יהיו $\frac{m}{n}, \frac{s}{t} \in \mathbb{Q}$. אזי:

$$f\left(\frac{m}{n} + \frac{s}{t}\right) = f\left(\frac{mt + ns}{nt}\right) = \left((mt + ns) \times 1_F\right)\left((nt) \times 1_F\right)^{-1} = \left((mt) \times 1_F + (ns) \times 1_F\right)\left((nt) \times 1_F\right)^{-1} =$$

$$= \left((mt) \times 1_F\right)\left((nt) \times 1_F\right)^{-1} + \left((ns) \times 1_F\right)\left((nt) \times 1_F\right)^{-1} = f\left(\frac{mt}{nt}\right) + f\left(\frac{ns}{nt}\right) = f\left(\frac{m}{n}\right) + f\left(\frac{s}{t}\right)$$

ובאופן דומה לגבי הכפל:

$$f\left(\frac{m}{n} \cdot \frac{s}{t}\right) = f\left(\frac{ms}{nt}\right) = \left((ms) \times 1_F\right)\left((nt) \times 1_F\right)^{-1} = \left(\left(m \times 1_F\right)\left(s \times 1_F\right)\right)\left(\left(n \times 1_F\right)\left(t \times 1_F\right)\right)^{-1} =$$

$$= \left(\left(m \times 1_F\right)\left(s \times 1_F\right)\right)\left(\left(n \times 1_F\right)^{-1}\left(t \times 1_F\right)^{-1}\right) = \left(m \times 1_F\right)\left(s \times 1_F\right)\left(n \times 1_F\right)^{-1}\left(t \times 1_F\right)^{-1} =$$

$$\left(\left(m \times 1_F\right)\left(n \times 1_F\right)^{-1}\right)\left(\left(s \times 1_F\right)\left(t \times 1_F\right)^{-1}\right) = f\left(\frac{m}{n}\right) \cdot f\left(\frac{s}{t}\right)$$

אז $f : \mathbb{Q} \to g\left(\mathbb{Q}\right)$ היא איזומורפיזם. לכן $g\left(\mathbb{Q}\right)$ שדה. מש"ל ☺

3. מרחבים וקטוריים

3.1. הגדרת המרחב הוקטורי

<u>הגדרה</u>: יהי F שדה. **מרחב וקטורי מעל שדה** F הוא קבוצה של איברים (שנקרא להם **וקטורים**) שמוגדרות עליה פעולת חיבור של וקטורים ופעולת כפל באיברי השדה (שנקרא להם **סקלרים**), כך שמתקיימות האקסיומות הבאות: לכל $w,u,v \in V$ ו- $a,b \in F$:

1. *אקסיומות חיבור וקטורים*
   a. סגירות $u+v \in V$
   b. חילופיות $u+v=v+u$
   c. קיבוציות $(u+v)+w=u+(u+w)$
   d. קיום איבר ניטרלי לחיבור שנמסמנו 0_V כך ש- $v+0_V=v$
   e. קיום איבר נגדי לחיבור נסמנו $-v$ ומקיים $v+(-v)=0_V$
2. *אקסיומות כפל בסקלר*
   a. סגירות $a \cdot v \in V$
   b. $1_F \cdot v = v$
   c. $(ab)\cdot v = a\cdot(b\cdot v)$
   d. $(a+b).v = a\cdot v + b\cdot v$
      $a\cdot(v+w) = a\cdot v + a\cdot w$

נשים לב לכמה תכונות של מרחבים וקטוריים שנובעות ישירות מן האקסיומות:
יהי F שדה ויהי V מרחב וקטורי מעל F. אזי לכל $c \in F$ ולכל $u,v,s \in V$ מתקיימות התכונות הבאות:

1. $-(-u)=u$
2. $-(u+v)=-u-v$
3. $0_F \cdot u = 0_V$
4. $(-1_F)\cdot u = -u$
5. אם $cu=0_V$ אז $c=0_F$ או $u=0_V$
6. אם $u+s=v+s$ אז $u=v$

<u>דוגמה פונדמנטלית ביותר</u>:
יהי שדה F ויהי $0 \le n \in \mathbb{Z}$. נגדיר $F^n = \{(a_1,a_2,...,a_n) : a_i \in F, 1 \le i \le n\}$ (קבוצה של n-יות של איברי השדה).
נגדיר חיבור וכפל בסקלר:

$$(a_1,...,a_n)+(b_1,...,b_n)=(a_1+b_1,...,a_n+b_n)$$
$$c\cdot(a_1,...,a_n)=(c\cdot a_1,...,c\cdot a_n)$$

<u>טענה 10</u>: F^n מרחב וקטורי מעל F.
<u>הוכחה</u>: נראה את קיום כל אקסיומות השדה:
אקסיומות חיבור וקטורים:

1. *סגירות*: F שדה ולכן לכל $a,b \in F$ מתקיים $a+b \in F$. כמו כן, לפי הגדרת החיבור בחיבור של שתי n-יות מתקבלת n-יה. לכן אם $a=(a_1,...,a_n), b=(b_1,...,b_n) \in F^n$ אזי $a+b=(a_1+b_1,...,a_n+b_n) \in F^n$.
2. *חילופיות*: F שדה ולכן לכל $a,b \in F$ מתקיים $a+b=b+a$. לכן בהינתן $a,b \in F^n$

$$a+b=(a_1,...,a_n)+(b_1,...,b_n)=(a_1+b_1,...,a_n+b_n)=$$
$$=(b_1+a_1,...,b_n+a_n)=(b_1,...,b_n)+(a_1,...,a_n)=b+a$$

3. *קיבוציות*: יהיו $a,b,c\in F^n$. אזי לפי הגדרת החיבור ב- F^n ובגלל ש- F שדה מתקיים:

$$a+(b+c)=(a_1,...,a_n)+\left[(b_1,...,b_n)+(c_1,...,c_n)\right]=(a_1,...,a_n)+(b_1+c_1,...,b_n+c_n)=$$
$$=(a_1+(b_1+c_1),...,a_n+(b_n+c_n))=((a_1+b_1)+c_1,...,(a_n+b_n)+c_n)=$$
$$=(a_1+b_1,...,a_n+b_n)+(c_1,...,c_n)=\left[(a_1,...,a_n)+(b_1,...,b_n)\right]+(c_1,...,c_n)=(a+b)+c$$

4. *קיום איבר ניטרלי לחיבור*: נגדיר $0_{F^n}=\underbrace{(0_F,...,0_F)}_{\text{n times}}$ ונטען שלכל $a\in F^n$ מתקיים $a+0_{F^n}=a$. לפי הגדרת החיבור $a+0_{F^n}=(a_1,...,a_n)+(0_F,...,0_F)=(a_1+0_F,...,a_n+0_F)=(a_1,...,a_n)=a$. לכן 0_{F^n} כפי שהגדרנו אותו הוא איבר ניטרלי לחיבור.

5. *קיום איבר נגדי לחיבור*: לכל $a=(a_1,...,a_n)\in F^n$ נגדיר $-a=(-a_1,...,-a_n)$. נראה שזה איבר נגדי לחיבור:

$$a+(-a)=(a_1,...,a_n)+(-a_1,...,-a_n)=(a_1+(-a_1),...,a_n+(-a_n))=(0_F,...,0_F)=0_{F^n}$$

אקסיומות כפל בסקלר:

1. *סגירות*: F שדה ולכן לכל $c,a\in F$ מתקיים $c\cdot a\in F$. כמו כן, לפי הגדרת הכפל בסקלר בכפל של n-יה מתקבלת n-יה. לכן אם $a=(a_1,...,a_n)\in F^n, c\in F$ אזי $c\cdot a=(c\cdot a_1,...,c\cdot a_n)\in F^n$.

2. לפי הגדרת איבר היחידה בשדה נקבל שלכל $a\in F^n$ מתקיים

$$1_F\cdot a=1_F\cdot(a_1,...,a_n)=(1_F\cdot a_1,...,1_F\cdot a_n)=(a_1,...,a_n)=a$$

3. לפי הגדרת כפל בסקלר ב- F^n ובגלל האסוציאטיביות של F נקבל לכל $a,b\in F, v\in F^n$:

$$(a\cdot b)\cdot v=(a\cdot b)\cdot(v_1,...,v_n)=((a\cdot b)\cdot v_1,...,(a\cdot b)\cdot v_n)=$$
$$=(a\cdot(b\cdot v_1),...,a\cdot(b\cdot v_n))=a\cdot(b\cdot v_1,...,b\cdot v_n)=a\cdot(b\cdot(v_1,...,v_n))=a\cdot(b\cdot v)$$

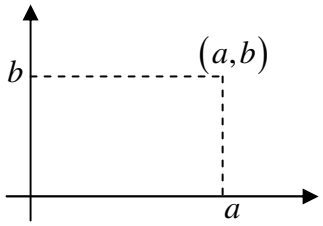
4. יהיו $a,b\in F$ ו- $u,v\in F^n$. אזי

$$(a+b)\cdot v=(a+b)\cdot(v_1,...,v_n)=((a+b)\cdot v_1,...,(a+b)\cdot v_n)=(a\cdot v_1+b\cdot v_1,...,a\cdot v_n+b\cdot v_n)=$$
$$=(a\cdot v_1,...,a\cdot v_n)+(b\cdot v_1,...,b\cdot v_n)=a\cdot(v_1,...,v_n)+b\cdot(v_1,...,v_n)=a\cdot v+b\cdot v$$
$$a\cdot(v+u)=a\cdot((v_1,...,v_n)+(u_1,...,u_n))=a\cdot(v_1+u_1,...,v_n+u_n)=(a\cdot(v_1+u_1),...,a\cdot(v_n+u_n))=$$
$$=(a\cdot v_1+a\cdot u_1,...,a\cdot v_n+a\cdot u_n)=(a\cdot v_1,...,a\cdot v_n)+(a\cdot u_1,...,a\cdot u_n)=$$
$$=a\cdot(v_1,...,v_n)+a\cdot(u_1,...,u_n)=a\cdot v+a\cdot u$$

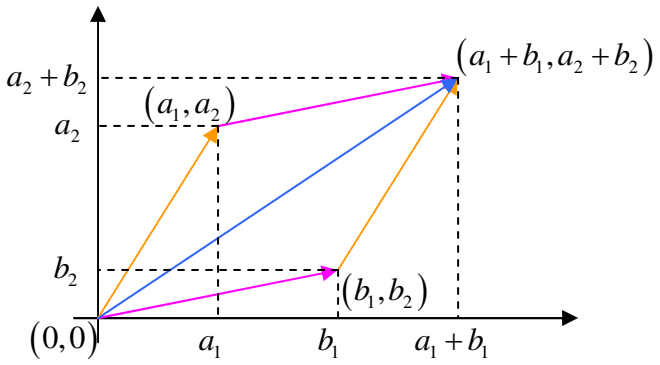
הראנו שכל אקסיומות המרחב הווקטורי מתקיימות. לכן F^n מרחב וקטורי מעל F. מש"ל ☺

<u>הערה</u>: המרחב הווקטורי מהדוגמה הוא מרחב חשוב מאוד אך לא כל המרחבים הווקטוריים הם מהצורה הזאת. יש מרחבים וקטוריים שונים ומשונים. אנחנו עוד נראה דוגמאות רבות בעתיד.

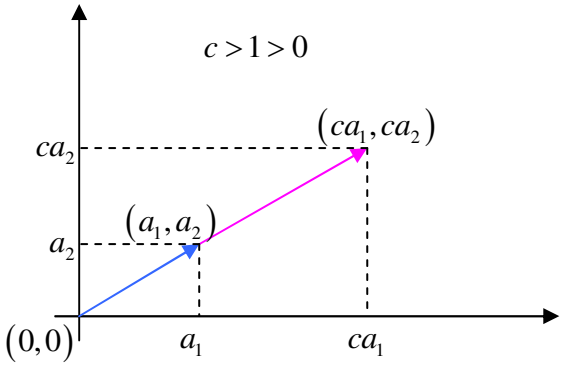
בפרט אם ניקח $F=\mathbb{R}$ ו- $n=2$ נקבל את $\mathbb{R}^2$. נגדיר לו <u>מודל גיאומטרי</u>:
לכל $(a,b)\in\mathbb{R}^2$ נתאים את הנקודה במישור שהקואורדינטות שלה הן (a,b):



כיצד משתקפות הפעולות שהגדרנו על $\mathbb{R}^2$ במודל הגיאומטרי?
חיבור ע"פ כלל המקבילית: עבור $(a_1,a_2),(b_1,b_2)\in\mathbb{R}^2$ בונים מקבילית שקודקוד אחד שלה הוא $(0,0)$ ושני הקודקודים האחרים הם (a_1,a_2) ו- (b_1,b_2). הקודקוד הרביעי הוא (a_1+b_1,a_2+b_2) - כלומר זה האלכסון של המקבילית:



כפל בסקלר ע"י הארכת (או קיצור) הווקטור באופן מכוון (אם הסקלר חיובי הווקטור מוארך באותו הכיוון ואם הוא שלילי בכיוון ההפוך).

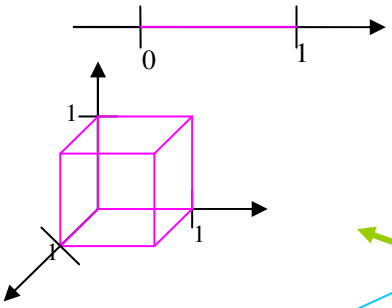


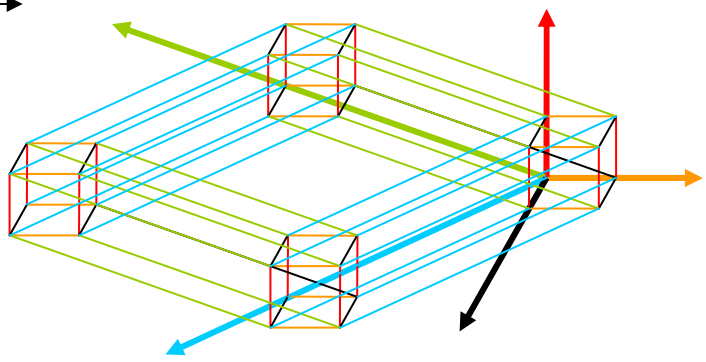
מודל גיאומטרי דומה אפשר להתאים למרחב הווקטורי $\mathbb{R}^3$ מעל $\mathbb{R}$. אזי לכל וקטור (a_1,a_2,a_3) תתאים נקודה במרחב שהקואורדינטות שלה הן (a_1,a_2,a_3).

3.2. קוביות ב- $\mathbb{R}^n$

זה לא ממש חשוב אבל זה די מגניב לצייר קוביה בחמישה ממדים אז נעשה את זה:

1. קטע היחידה ב- $\mathbb{R}^1$: $I_1=\{(a_1):0\le a_1\le 1\}$
2. רביע היחידה ב- $\mathbb{R}^2$: $I_2=\{(a_1,a_2):0\le a_1,a_2\le 1\}$
3. קוביית היחידה ב- $\mathbb{R}^3$: $I_3=\{(a_1,a_2,a_3):0\le a_1,a_2,a_3\le 1\}$
4. קובייה ב- $\mathbb{R}^5$:





3.3. בסיסים ומימד של מרחבים וקטוריים

<u>הגדרה</u>: יהי V מרחב וקטורי מעל שדה F. נאמר ש- $v_1,...,v_n \in V$ **תלויים לינארית** אם קיימים סקלרים $c_1,...,c_n \in F$ כך שקיים $1 \le i \le n$ שעבורו $c_i \neq 0_F$ (כלומר לא כולם אפס) ומתקיים $\sum_{i=1}^{n} c_i v_i = 0_V$. אחרת $v_1,...,v_n$ נקראים **בלתי תלויים לינארית** (להלן בת"ל).

<u>הגדרה</u>: יהי U מרחב וקטורי מעל שדה F. יהיו $u_1,...,u_k \in U$ ויהיו $a_1,...,a_k \in F$. הווקטור $\sum_{i=1}^{k} a_i u_i$ נקרא **צירוף לינארי** של $u_1,...,u_k$ עם מקדמים $a_1,...,a_k$. **צירוף לינארי טריוויאלי** הוא צירוף לינארי עם מקדמים שכולם אפס $a_1 = ... = a_k = 0_F$.

תחת הגדרה זו נאמר שהווקטורים $v_1,...,v_n \in V$ הם תלויים לינארית אם קיים צירוף לינארי לא טריוויאלי שמתאפס. אחרת נאמר שהם בלתי תלויים לינארית.

<u>דוגמאות</u>: יהי V מרחב וקטורי מעל F.

1. ויהי $v \in V$. אם $v = 0_V$ אזי $1_F v = 0_V$, כלומר קיים צירוף לינארי לא טריוויאלי של v אשר מתאפס ולכן v תלוי לינארית.
   אם $v \neq 0_V$ ו- $cv = 0_V$ אזי $c = 0_F$. אחרת קיים c^{-1} ולכן $v = 1_F v = c^{-1}(cv) = c^{-1}0_V = 0_V$ וזאת סתירה.
   כלומר קיבלנו שעבור וקטור אחד הוא תלוי לינארית אם הוא וקטור האפס, אחרת הוא בלתי תלוי לינארית.
2. יהיו $v_1, v_2 \in V$. הווקטורים תלויים לינארית אם קיימים סקלרים $c_1, c_2 \in F$ לא כולם 0_F כך ש- $c_1 v_1 + c_2 v_2 = 0_V$. אזי $c_1 v_1 = -c_2 v_2$.
   a. אם $c_1 \neq 0_F$ אזי קיים $c_1^{-1}1$ ואז נוכל לרשום
   $$v_1 = 1_F v_1 = \left(c_1^{-1}c_1\right)v_1 = c_1^{-1}\left(c_1 v_1\right) = c_1^{-1}\left(-c_2 v_2\right) = \left(-c_1^{-1}c_2\right)v_2$$
   כלומר v_1 הוא כפולה סקלרית של v_2.
   b. אם $c_2 \neq 0_F$ אזי קיים c_2^{-1} ואז נוכל לרשום
   $$v_2 = 1_F v_2 = \left(c_2^{-1}c_2\right)v_2 = c_2^{-1}\left(c_2 v_2\right) = c_2^{-1}\left(-c_1 v_1\right) = \left(-c_2^{-1}c_1\right)v_1$$
   כלומר v_2 הוא כפולה סקלרית של v_1.
   המסקנה: עבור שני וקטורים הם תלויים לינארית אם אחד מהם הוא כפולה סקלרית של השני.
3. יהיו $v_1, v_2, v_3 \in V$. באופן דומה למה שעשינו קודם ניתן לרשום שאם קיימים c_1, c_2, c_3 לא כולם 0_F כך ש- $\sum_{i=1}^{3} c_i v_i$ אזי מתקיים לפחות אחד מהבאים:
   a. אם $c_1 \neq 0_F$ אזי $v_1 = \left(-c_1^{-1}c_2\right)v_2 + \left(-c_1^{-1}c_3\right)v_3$
   b. אם $c_2 \neq 0_F$ אזי $v_2 = \left(-c_2^{-1}c_1\right)v_1 + \left(-c_2^{-1}c_3\right)v_3$
   c. אם $c_3 \neq 0_F$ אזי $v_3 = \left(-c_3^{-1}c_1\right)v_1 + \left(-c_3^{-1}c_2\right)v_2$
   כלומר, אם הווקטורים תלויים לינארית אזי אחד מהם הוא צירוף לינארי של השניים האחרים.

נחזור למודל הגיאומטרי של $\mathbb{R}^2$. איך תלות לינארית מתבטאת במודל הגיאומטרי?
עבור שני וקטורים, כפי שנאמר למעלה, הם תלויים אם אחד הוא כפולה סקלרית של השני. ולכן במודל הגיאומטרי אם שני וקטורים נמצאים על אותו הישר אזי הוא תלויים.
עבור שלושה וקטורים הם תלויים אם אחד מהם הוא צירוף לינארי של השניים האחרים. מכאן ניתן להסיק שכל שלושה וקטורים ב- $\mathbb{R}^2$ הוא תלויים.

<u>משפט 11</u>: יהי $0 \le m \in \mathbb{Z}$ ויהי F שדה. יהיו $v_1,...,v_n \in F^m$ כאשר $m < n$. אזי $v_1,...,v_n$ תלויים לינארית.
<u>הוכחה</u>: באינדוקציה על m.
בסיס האינדוקציה: $m = 0$. אזי $F^0 = \{()\}$, בפרט $() = 0_{F^0}$. יהי $0 < n$ ויהיו $v_1,...,v_n \in F^0$. ברור ש- $v_1 = ... = v_n = ()$. לכן $() = 0_{F^0} = \underbrace{() + ... + ()}_{\text{n times}} = \underbrace{1_F() + ... + 1_F()}_{\text{n times}} = ()$. קיבלנו צירוף לינארי לא טריוויאלי שמתאפס. לכן הווקטורים תלויים לינארית.

הנחת האינדוקציה: נניח שעבור m אם $v_1,...,v_n \in F^m$ ו- $m < n$ אזי $v_1,...,v_n$ תלויים לינארית.

שלב האינדוקציה: נוכיח את נכונות הטענה עבור $m+1$. יהיו $w_1,...,w_l \in F^{m+1}$ כאשר $m+1 < l$. נרצה להוכיח ש- $w_1,...,w_l$ תלויים לינארית.

נרשום את הווקטורים בצורה מפורשת:

$$w_1 = \left(a_{1,1},...,a_{1,m},a_{1,m+1}\right)$$
$$\vdots$$
$$w_{l-1} = \left(a_{l-1,1},...,a_{l-1,m},a_{l-1,m+1}\right)$$
$$w_l = \left(a_{l,1},...,a_{l,m},a_{l,m+1}\right)$$

נסתכל ראשית במקרה הפרטי שבו $a_{i,m+1} = 0_F$ לכל $1 \le i \le l$. נגדיר

$$w_1' = \left(a_{1,1},...,a_{1,m}\right) \in F^m$$
$$\vdots$$
$$w_l' = \left(a_{l,1},...,a_{l,m}\right) \in F^m$$

ולכן לפי הנחת האינדוקציה הווקטורים $w_1',...,w_l' \in F^m$ תלויים לינארית. לכן קיימים סקלרים $c_1,...,c_l \in F$ לא כולם 0_F כך ש- $\left(\sum_{i=1}^{l} c_i a_{i,1},...,\sum_{i=1}^{l} c_i a_{i,m}\right) = \sum_{i=1}^{l} c_i w_i' = 0_{F^m} = \left(0_F,...,0_F\right)$. אזי

$$\sum_{i=1}^{l} c_i w_i = \sum_{i=1}^{l} c_i \left(a_{i,1},...,a_{i,m},a_{i,m+1}\right) = \left(\sum_{i=1}^{l} c_i a_{i,1},...,\sum_{i=1}^{l} c_i a_{i,m},\sum_{i=1}^{l} c_i a_{i,m+1}\right) =$$
$$= \left(0_F,...,0_F,\sum_{i=1}^{l} c_i 0_F\right) = \left(0_F,...,0_F,0_F\right) = 0_{F^{m+1}}$$

כעת אם לא כל $a_{i,m+1}$ הם אפס אזי קיים $1 \le i \le l$ כך ש- $a_{i,m+1} \ne 0_F$. בה"כ $i = l$ (אחרת נשנה את סדר הווקטורים). נגדיר

$$u_1 = w_1 - a_{1,m+1}a_{l,m+1}^{-1}w_l$$
$$\vdots$$
$$u_{l-1} = w_{l-1} - a_{l-1,m+1}a_{l,m+1}^{-1}w_l$$

נשים לב שלכל $1 \le i \le l-1$ מתקיים $a_{i,m+1} - a_{i,m+1}a_{l,m+1}^{-1}a_{l,m+1} = a_{i,m+1} - a_{i,m+1}1_F = 0_F$. ולכן נוכל לרשום:

$$u_1 = \left(b_{1,1},...,b_{1,m},0_F\right)$$
$$\vdots$$
$$u_{l-1} = \left(b_{l-1,1},...,b_{l-1,m},0_F\right)$$

נגדיר וקטורים חדשים:

$$u_1' = \left(b_{1,1},...,b_{1,m}\right) \in F^m$$
$$\vdots$$
$$u_{l-1}' = \left(b_{l-1,1},...,b_{l-1,m}\right) \in F^m$$

$l-1 < m \Leftarrow l > m+1$ ולכן נוכל להשתמש בהנחת האינדוקציה. קיימים $d_1,...,d_{l-1} \in F$ לא כולם 0_F כך ש- $\sum_{i=1}^{l-1} d_i u_i' = 0_{F^m}$.

אזי כמו קודם

$$\sum_{i=1}^{l-1} d_i u_i = \left(\sum_{i=1}^{l-1} d_i\left(a_{i,1} - a_{i,m+1}a_{l,m+1}^{-1}a_{l,1}\right),...,\sum_{i=1}^{l-1} d_i\left(a_{i,m} - a_{i,m+1}a_{l,m+1}^{-1}a_{l,m}\right),\sum_{i=1}^{l-1} d_i\left(a_{i,m+1} - a_{i,m+1}a_{l,m+1}^{-1}a_{l,m+1}\right)\right) =$$
$$= \left(0_F,...,0_F,\sum_{i=1}^{l-1} d_i 0_F\right) = \left(0_F,...,0_F,0_F\right) = 0_{F^{m+1}}$$

נגדיר $d_l = -\sum_{i=1}^{l-1} d_i a_{i,m+1}a_{l,m+1}^{-1}$ ונקבל

$$\sum_{i=1}^{l} d_i w_i = \sum_{i=1}^{l-1} d_i w_i + d_l w_l = \sum_{i=1}^{l-1} d_i \left(u_i + a_{i,m+1} a_{l,m+1}^{-1} w_l \right) + \left(-\left(\sum_{i=1}^{l-1} d_i a_{i,m+1} a_{l,m+1}^{-1} \right) w_l \right) =$$

$$= \sum_{i=1}^{l-1} \left(d_i u_i + d_i a_{i,m+1} a_{l,m+1}^{-1} w_l - d_i a_{i,m+1} a_{l,m+1}^{-1} w_l \right) = \sum_{i=1}^{l-1} \left(d_i u_i + 0_V \right) = \sum_{i=1}^{l-1} d_i u_i = 0_{F^{m+1}}$$

קיבלנו צירוף לינארי של $w_1,...,w_l$ במקדמים לא טריויאליים. ולכן הם תלויים לינארית.
מכאן שלפי עיקרון האינדוקציה המשפט נכון לכל $0 \le m \in \mathbb{Z}$. מש"ל ☺

<u>הגדרה</u>: יהי V מרחב וקטורי מעל שדה F. נאמר שהווקטורים $v_1,...,v_n \in V$ **פורשים** (או **יוצרים**) את V כאשר כל וקטור ב- V ניתן להצגה כצירוף לינארי של $v_1,...,v_n$. במקרה כזה נאמר ש- V **נוצר סופית**.

<u>משפט 12</u>: יהי V מרחב וקטורי מעל שדה F. ויהיו $v_1,...,v_m \in V$ פורשים את V. אם $w_1,...,w_l \in V$ ו- $m < l$ אזי $w_1,...,w_l$ תלויים לינארית.
<u>הוכחה</u>: $v_1,...,v_n$ פורשים ולכן ניתן לרשום:

$$w_1 = a_{1,1} v_1 + ... + a_{1,m} v_m$$
$$\vdots$$
$$w_l = a_{l,1} + ... + a_{l,m} v_m$$

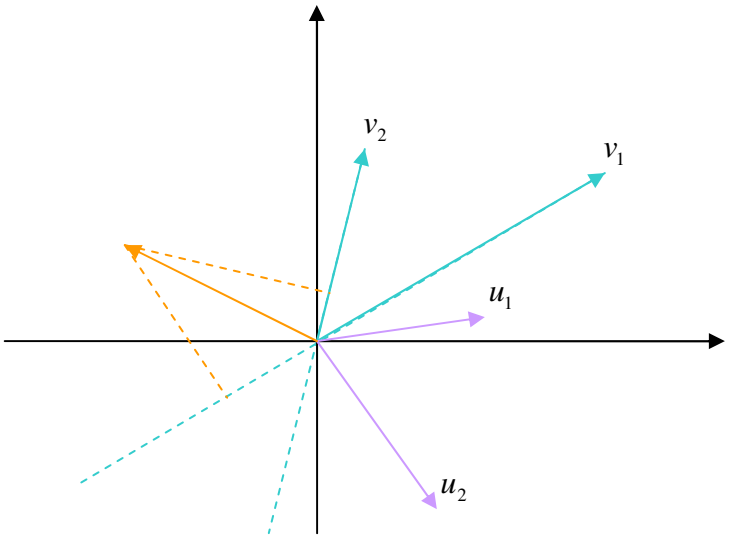
נגדיר לכל $1 \le i \le l$ $u_i = \left(a_{i,1},...,a_{i,m} \right) \in F^m$. מכיוון ש- $m < l$ ו- $u_1,...,u_l \in F^m$ נקבל לפי המשפט הקודם ש- $u_1,...,u_l$ תלויים לינארית. לכן קיימים $c_1,...,c_l \in F$ לא כולם 0_F כך ש- $\sum_{i=1}^{l} c_i u_i = 0_{F^m}$. אזי

$$\sum_{i=1}^{l} c_i w_i = \sum_{i=1}^{l} c_i \sum_{j=1}^{m} a_{i,j} v_j = \sum_{i=1}^{m} \left(\sum_{j=1}^{l} c_j a_{j,i} \right) v_i = \sum_{i=1}^{m} 0_F v_i = 0_V$$

ולכן $w_1,...,w_l$ תלויים לינארית. מש"ל ☺

<u>הגדרה</u>: יהי V מרחב וקטורי מעל שדה F. קבוצת הווקטורים $v = \{v_1,...,v_n\}$ תיקרא **בסיס** אם V נפרש ע"י v ו- v בלתי תלויה לינארית.

<u>דוגמה</u>: $F = \mathbb{R}$ ו- $V = \mathbb{R}^2$



ברור ש- v_1 ו- v_2 בלתי תלויים לינארית כי הם לא נמצאים על ישר אחד וגם כל וקטור אפשר להציג כצירוף לינארי שלהם (ע"י ההיטלים על v_1 ו- v_2). ולכן הם מהווים בסיס. בעצם, ב- $\mathbb{R}^2$ כל שני וקטורים שאינם נמצאים על ישר אחד הם בסיס.
מכאן נובע שלמרחב וקטורי יכולים להיות כמה בסיסים. כלומר, אין **ה**בסיס של המרחב. למשל, בציור גם $\{v_1, v_2\}$ וגם $\{u_1, u_2\}$ הם בסיסים ל- $\mathbb{R}^2$.

משפט 13: יהי V מרחב וקטורי מעל שדה F. אם $v_1,...,v_n \in V$ בסיס וגם $w_1,...,w_l \in V$ בסיס אזי $n = l$.
הסבר: המשפט לא מבטיח שלכל מרחב וקטורי קיים בסיס. אבל אם למרחב וקטורי יש בסיס אזי בכל בסיס יש אותו מספר איברים.
הוכחה: V נפרש ע"י $v_1,...,v_n$. נניח ש- $n < l$. אזי $w_1,...,w_l$ תלויים לינארית. בסתירה לכך שהם בסיס. באותו אופן, אם נניח ש- $l < n$ נקבל ש- $v_1,...,v_n$ תלויים לינארית שכן V נפרש ע"י $w_1,...,w_2$ בסתירה להיותם בסיס. האפשרות היחידה שנשארת היא $l = n$. מש"ל ☺

הגדרה: יהי V מרחב וקטורי נוצר סופית. מספר האיברים בבסיס של V נקרא **המימד** של V ומסומן $\dim_F V$.

דוגמה: נטען שלכל שדה F מתקיים $\dim_F F^n = n$
הוכחה: אם נמצא בסיס של F^n שבו n איברים נקבל את הטענה משום שלפי המשפט הקודם בכל בסיס של V יש אותו מספר איברים.
נסתכל, אם כן, על הווקטורים:

$$e_1 = (1_F, 0_F, ..., 0_F)$$
$$\vdots$$
$$e_i = \left(0_F, ..., \underbrace{1_F}_{\text{i-th place}}, ..., 0_F\right)$$
$$\vdots$$
$$e_n = (0_F, ..., 0_F, 1_F)$$

נוכיח כי $e_1,...,e_n \in F^n$ בסיס של F^n. לשם כך נראה שהוא פורשים ושהם בלתי תלויים לינארית.

פורשים: יהי $(a_1,...,a_n) \in F^n$. ברור ש- $(a_1,...,a_n) = \sum_{i=1}^{n} a_i e_i$. כלומר כל וקטור ב- F^n ניתן להצגה כצירוף לינארי של $e_1,...,e_n$. כלומר F^n נפרש ע"י $e_1,...,e_n$.

אי-*תלות*: נניח כי עבור סקלרים $a_1,...,a_n \in F$ מתקיים $\sum_{i=1}^{n} a_i e_i = 0_{F^n}$. ברור לפי הגדרת החיבור ש- $\sum_{i=1}^{n} a_i e_i = (a_1,...,a_n)$. ולכן $(a_1,...,a_n) = (0_F,...,0_F)$ ולכן $a_1 = ... = a_n = 0_F$. לכן $e_1,...,e_n$ בלתי תלויים לינארית.
הראנו שהווקטורים פורשים ובלתי תלויים לינארית. לכן הם בסיס. ומכאן ש- $\dim_F F^n = n$. מש"ל ☺

הגדרה: הבסיס $e_1,...,e_n$ ל- F^n כפי שהוגדר בדוגמה נקרא **הבסיס הסטנדרטי** של F^n.

משפט 14: יהי V מרחב וקטורי מעל שדה F. יהיו $v_1,...,v_n \in V$. התנאים הבאים שקולים:
1. $v_1,...,v_n$ בסיס של V
2. לכל וקטור $v \in V$ קיימת הצגה יחידה כצירוף לינארי של $v_1,...,v_n$

הוכחה:
$(1 \Leftarrow 2)$ $v_1,...,v_n$ בסיס. בפרט הם פורשים את V. לכן לכל וקטור $v \in V$ קיימת הצגה כצירוף לינארי שלהם. נוכיח שהיא יחידה. יהי $v \in V$ ויהיו $a_1,...,a_n \in F$ כך ש- $\sum_{i=1}^{m} a_i v_i = v$. נניח שקיימים גם $b_1,...,b_n \in F$ כך ש- $\sum_{i=1}^{n} b_i v_i = v$.
נסתכל על ההפרש ביניהם:

$$0_V = v - v = \sum_{i=1}^{n} a_i v_i - \sum_{i=1}^{n} b_i v_i = \sum_{i=1}^{n} (a_i - b_i) v_i$$

$v_1,...,v_n$ בסיס. בפרט הם בלתי תלויים לינארית ולכן אם השוויון למעלה נכון חייב להתקיים $a_i - b_i = 0_F$ לכל $1 \le i \le n$. ולכן $a_i = b_i$, כלומר ההצגה כצירוף לינארי של $v_1,...,v_n$ יחידה.

$(2 \Leftarrow 1)$ נניח שלכל $v \in V$ קיימת הצגה יחידה בצירוף לינארי של $v_1,...,v_n$. בפרט ברור שהם פורשים. נותר לנו להוכיח כי הם בלתי תלויים לינארית. ברור ש- $0_V = \sum_{i=1}^{n} 0_F v_i$. ההצגה הזאת היא יחידה ולכן לכל $a_1,...,a_n \in F$ אשר מקיימים $\sum_{i=1}^{n} a_i v_i = 0_V$ מתקיים $a_1 = ... = a_n = 0_F$, כלומר הווקטורים בלתי תלויים לינארית. לכן נקבל כי $v_1,...,v_n$ בסיס. ☺

3.4. תתי מרחבים

<u>הגדרה</u>: יהי V מרחב וקטורי מעל שדה F. תת-קבוצה $U \subset V$ נקראת **תת-מרחב** אם U מקיימת את כל אקסיומות המרחב הווקטורי ביחס לפעולות שמוגדרות על V.

<u>משפט 15</u>: יהי V מרחב וקטורי מעל שדה F. תהי $U \subset V$ תת קבוצה. U תת מרחב אם ורק אם:

1. U לא ריקה
2. U סגורה תחת חיבור של וקטורים
3. U סגורה תחת כפל בסקלר

<u>הוכחה</u>:

$(\Leftarrow)$ הכיוון הזה טריוויאלי ונובע מהגדרת תת מרחב כמרחב וקטורי.

$(\Rightarrow)$ נניח שמתקיימים התנאים לעיל ונוכיח כי U מקיימת את כל אקסיומות המרחב הווקטורי.

אקסיומות חיבור וקטורים:

1. סגירות: נתון בתנאי המשפט.
2. חילופיות: נובע מכך ש- $U \subset V$ ומוגדרות עליה אותן פעולות. V מרחב וקטורי ולכן לכל $u,v \in V$ מתקיים $u+v=v+u$. בפרט זה נכון לכל $v,u \in U \subset V$.
3. קיבוציות: מתקיימת מאותו שיקול כמו (2).
4. קיום איבר האפס: U לא ריקה ולכן קיים $v \in U$. U סגורה לכפל בסקלר ולכן $(-1_F)v \in U$. U סגורה תחת חיבור ולכן $0_F v = 0_V$. אגב, $v + (-1_F)v = 1_F v + (-1_F)v = (1_F + (-1_F))v = 0_F v = 0_V$. כלומר $0_W = 0_V$. נשים לב שנעשה כאן שימוש בדיסטריביוטיביות שאותה נוכיח תכף...
5. קיום איבר נגדי: כפי שראינו קודם לכל $v \in U$ $-v = (-1_F)v \in U$.

אקסיומות כפל בסקלר:

1. סגירות: נתון בנתאי המשפט.
2. שאר התכונות של כפל בסקלר נכונות לכל $u,v \in V$ ולכל $a,b \in F$. בפרט הן נכונות לגבי כל $u,v \in U \subset V$.

הראנו שמתקיימות כל אקסיומות המרחב הווקטורי. לכן U תת מרחב וקטורי של V. מש"ל ☺

<u>דוגמה</u>: נסתכל על המרחב הווקטורי $\mathbb{R}^3$ מעל $\mathbb{R}$. אזי תת המרחבים של $\mathbb{R}^3$ הם:

1. הראשית $\{(0,0)\}$
2. כל הישרים שעוברים דרך הראשית $l_t = \{(a,ta) : a \in \mathbb{R}\}$
3. כל המישורים שעוברים דרך הראשית $s_{t,p} = \{(a,ta,sa) : a \in \mathbb{R}\}$

קל לבדוק שכל אלה הם תת מרחבים. למעשה אלה הם כל תת המרחבים של $\mathbb{R}^3$ אבל לא נוכיח את זה כרגע.

<u>הגדרה</u>: יהי V מרחב וקטורי מעל שדה F. יהיו $u_1,...,u_k \in V$ כאשר $k \geq 1$. נגדיר: תת המרחב הנפרש ע"י $u_1,...,u_k$ הוא $\mathrm{Sp}(u_1,...,u_k) = \left\{ \sum_{i=1}^{k} c_i u_i : c_i \in F \right\}$. עבור $k=0$ נגדיר $\mathrm{Sp}(\ ) = \{0_V\}$. בכל מקרה ברור ש- $\mathrm{Sp}(u_1,...,u_k) \subset V$.

<u>משפט 16</u>: יהי V מרחב וקטורי מעל שדה F ויהיו $u_1,...,u_k \in V$. אזי $\mathrm{Sp}(u_1,...,u_n)$ תת מרחב וקטורי של V.

<u>הוכחה</u>: עבור $k=0$ ברור ש- $\mathrm{Sp}(\ ) = \{0_V\}$ תת מרחב וקטורי.

נסתכל במקרה שבו $k \geq 1$. נראה את קיום 3 התנאים מהמשפט הקודם:

1. ברור ש- $\mathrm{Sp}(u_1,...,u_k)$ לא ריקה, כי כל צירוף לינארי של $u_1,...,u_k$ נמצא בה.

2. יהיו $v,w\in \mathrm{Sp}\left(u_1,...,u_k\right)$. אזי קיימים סקלרים $c_1,...,c_k,d_1,...,d_k\in F$ כך ש- $v=\sum_{i=1}^{k}c_iu_i, w=\sum_{i=1}^{k}d_iu_i$.
אזי $u_1,...,u_k$ עם $v+w=\sum_{i=1}^{k}c_iu_i+\sum_{i=1}^{k}d_iu_i=\sum_{i=1}^{k}\left(c_i+d_i\right)u_i$ קיבלנו ש- $v+w$ הוא צירוף לינארי של
מקדמים $c_i+d_i\in F$ כאשר $1\le i\le k$. לכן $v+w\in \mathrm{Sp}\left(u_1,...,u_k\right)$. כלומר יש סגירות תחת חיבור.

3. יהי $v\in \mathrm{Sp}\left(u_1,...,u_k\right)$ ויהי $c\in F$. קיימים $a_1,...,a_k\in F$ כך ש- $v=\sum_{i=1}^{k}a_iu_i$. נסתכל על המכפלה:
$cv=c\sum_{i=1}^{k}a_iu_i=\sum_{i=1}^{k}\left(cb_i\right)u_i$ קיבלנו ש- cv הוא צירוף לינארי של $u_1,...,u_k$ עם מקדמים $cb_i\in F$ עבור
$1\le i\le k$. כלומר יש סגירות תחת כפל בסקלר.
לכן לפי משפט קודם $\mathrm{Sp}\left(u_1,...,u_k\right)$ תת מרחב וקטורי של V. מש"ל ☺

נעיר רק ש- $\mathrm{Sp}\left(u_1,...,u_k\right)$ וא תת המרחב המינימלי שמכיל את $u_1,...,u_k$. כלומר, אם $S\subset V$ תת מרחב שמקיים $u_1,...,u_k\in S$ אז בגלל הסגירות תחת חיבור ותחת כפל בסקלר כל קומבינציה לינארית של $u_1,...,u_k$ חייבת להיות גם היא ב- S. כלומר $\mathrm{Sp}\left(u_1,...,u_k\right)\subset S$.

<u>הערה</u>: עבור $u_1,...,u_k\in V$ $\mathrm{Sp}\left(u_1,...,u_k\right)=V$ אם ורק אם $u_1,...,u_k$ פורשים את V.

<u>הגדרה</u>: יהי F שדה ו- x משתנה. נגדיר $F\left[x\right]=\left\{\sum_{i=0}^{n}a_ix^i:a_i\in F,0\le n\right\}$ - קבוצת כל הפולינומים במשתנה x עם מקדמים משדה F. חיבור פולינומים וכפל בסקלר יתבצעו בצורה המוכרת לנו.

<u>טענה 17</u>: $F\left[x\right]$ מרחב וקטורי מעל F.
הטענה מובאת ללא הוכחה. ההוכחה פשוטה וישירה.

<u>משפט 18</u>: ב- $F\left[x\right]$ אין בסיס סופי.
<u>הוכחה</u>: נניח בשלילה ש- $F\left[x\right]$ בסיס של $v_1,...,v_n\in F\left[x\right]$. נניח שלכל $1\le i\le n$ v_i הוא פולינום ממעלה $0\le m_i$.
נגדיר $m=\max\left\{m_i\right\}_{i=1}^{n}$. אזי כל צירוף לינארי של $v_1,...,v_n$ הוא פולינום שמעלתו קטנה או שווה ל- m. בפרט $x^{m+1}\notin \mathrm{Sp}\left(v_1,...,v_n\right)$. כלומר, $v_1,...,v_n$ אינם פורשים את $F\left[x\right]$ ולכן אינם בסיס. זאת סתירה ולכן לא קיים בסיס סופי ל- $F\left[x\right]$. מש"ל ☺

<u>משפט 19</u>: יהי V מרחב וקטורי מעל שדה F שקיים לו בסיס $v_1,...,v_n$. יהי $U\subset V$ תת מרחב. אזי ל- U קיים בסיס.
הוכחה: לצורך הוכחת המשפט ניעזר בטענת עזר:
<u>טענת עזר</u>: התנאים הבאים שקולים:
1. $w_1,...,w_l\in V$ בלתי תלויים לינארית
2. $w_1\ne 0_V$ ו- $w_i\notin \mathrm{Sp}\left(w_1,...,w_{i-1}\right)$ לכל $2\le i\le l$

<u>הוכחת הטענה</u>:
$(1\Leftarrow 2)$ נניח ש- $w_1,...,w_l\in V$ בלתי תלויים לינארית. אם $w_1=0_V$ ניתן לרשום
$0_V=1_F0_V+0_Fw_2+...+0_Fw_l=1_Fw_1+0_Fw_2+...+0_Fw_l$. כלומר יש צירוף לינארי לא טריוויאלי של
$w_1,...,w_l$ שמתאפס. כלומר הווקטורים תלויים לינארית בסתירה לנתון. לכן $w_1\ne 0_V$.
כעת נניח שקיים $2\le i\le l$ כך שמתקיים $w_i\in \mathrm{Sp}\left(w_1,...,w_{i-1}\right)$. כלומר קיימים $a_1,...,a_{i-1}\in F$ לא כולם 0_F כך ש- $w_i=a_1w_1+...+a_{i-1}w_{i-1}$. אזי מתקיים
$0_V=w_i+\left(-a_1w_1\right)+...+\left(-a_{i-1}w_{i-1}\right)=\left(-a_1w_1\right)+...+\left(-a_{i-1}w_{i-1}\right)+w_i+0_Fw_{i+1}+...+0_Fw_l$ כלומר קיים צירוף לינארי לא טריוויאלי של הווקטורים שמתאפס. ולכן הם תלויים לינארית. בסתירה להנחה. לכן $w_i\notin \mathrm{Sp}\left(w_1,...,w_{i-1}\right)$ לכל $2\le i\le l$.

$(2\Leftarrow 1)$ נתון ש- $w_1\neq 0_V$ ו- $w_i\notin \mathrm{Sp}(w_1,...,w_{i-1})$ לכל $2\le i\le l$. נראה ש- $w_1,...,w_l$ בלתי תלויים לינארית.

נניח שקיים צירוף לינארי לא טריוויאלי שמקיים $\sum_{i=1}^{l}c_iw_i=0_V$. יהי k האינדקס המקסימלי שעבורו $c_k\neq 0_F$. אזי $c_{k+1},...,c_l=0_F$. לכן $0_V=\sum_{i=1}^{l}c_iw_i=\sum_{i=1}^{k}c_iw_i+\sum_{i=k+1}^{l}c_iw_i=\sum_{i=1}^{k}c_iw_i+\sum_{i=k+1}^{l}0_Fw_i=\sum_{i=1}^{k}c_iw_i$. נעביר אגפים ונקבל $c_kw_k=-c_1w_1-...-c_{k-1}w_{k-1}$. הנחנו ש- $c_k\neq 0_F$ לכן קיים c_k^{-1}. לכן $w_k=\left(-c_k^{-1}c_1\right)w_1+...+\left(-c_k^{-1}c_{k-1}\right)w_{k-1}\in\mathrm{Sp}(w_1,...,w_{k-1})$ בסתירה לנתון. לכן $w_1,...,w_l$ בלתי תלויים לינארית. מש"ל ☺

נחזור להוכחת המשפט. אם $V=\{0_V\}$ אזי קיים ל- V בסיס והוא הקבוצה הריקה.

אחרת קיים וקטור $0_V\neq w_1\in V$. לפי טענת העזר w_1 בלתי תלוי לינארית. אם $V=\mathrm{Sp}\{w_1\}$ אזי w_1 בסיס של V.

אחרת קיים $w_2\in V$ כך ש- $w_2\notin\mathrm{Sp}(w_1)$. לפי טענת העזר w_1,w_2 בלתי תלויים לינארית. אם $V=\mathrm{Sp}(w_1,w_2)$ אזי w_1,w_2 בסיס של V.

כעת נגדיר באינדוקציה: נניח שמצאנו $k<n$ וקטורים בת"ל ב- V $w_1,...,w_k$. אם הם פורשים את V אזי הם בסיס.

אחרת קיים $w_{k+1}\in V$ כך ש- $w_{k+1}\notin\mathrm{Sp}(w_1,...,w_k)$. לפי טענת העזר $w_1,...,w_{k+1}$ בלתי תלויים לינארית. כעת נחזור על התהליך עד שיתקיים אחד מהבאים:

1. נמצא בסיס של V
2. נקבל n וקטורים בלתי תלויים לינארית. במקרה זה הווקטורים יהיו חייבים להיות פורשים משום ש- $\dim_F V=n$.

בתהליך הזה מצאנו בסיס סופי ל- V. יתר על כן ברור שמתקיים $\dim_F U\le\dim_F V$. מש"ל ☺

<u>משפט 20</u>: יהי V מרחב וקטורי מעל שדה F ויהי $U\subset V$ תת מרחב. אם $\dim_F V=\dim_F U$ אז $U=V$.

<u>הוכחה</u>: נניח בשלילה ש- $U\neq V$. לפי המשפט הקודם ל- U קיים בסיס. נניח $v_1,...,v_n$ בסיס ל- V ו- $u_1,...,u_n$ בסיס ל- U. יהי $u_{n+1}\in V$ כך ש- $u_{n+1}\notin U$ (קיים כזה כי הנחנו ש- $U\neq V$). לפי טענת העזר $u_1,...,u_{n+1}$ בלתי תלויים לינארית. וזאת סתירה לכך ש- V נפרש ע"י $v_1,...,v_n$ (מאחר ש- $n<n+1$ הוכחנו שחייב להתקיים שכל $n+1$ וקטורים הם תלויים). לכן $U=V$. מש"ל ☺

<u>משפט 21</u>: יהי $V=\mathrm{Sp}(u_1,...,u_m)$. אזי הקבוצה $B=\{u_i:u_1\neq 0_V,1\le i\le m,u_i\notin\mathrm{Sp}(u_1,...,u_{i-1})\}$ היא בסיס ל- V.

<u>משמעות</u>: המשפט בעצם אומר שבהינתן קבוצה פורשת של וקטורים ניתן לדלל אותה עד כדי בסיס, כלומר ניתן להוציא ממנה איברים עד שנקבל קבוצה בלתי תלויה לינארית אך היא עדיין פורשת.

<u>הוכחה</u>: נוכיח ש- B קבוצה פורשת ובלתי תלויה לינארית. $u_1\neq 0_V$. נניח $|B|=n\le m$. לפי הגדרת B לכל $2\le i\le m$ מתקיים $u_i\notin\mathrm{Sp}(u_1,...,u_{i-1})$ ולכן לפי טענת העזר ממשפט (19) $u_1,...,u_n$ בלתי תלויים לינארית.

נראה שהם פורשים את V. נסמן ב- $\beta_{i_1},...,\beta_{i_{m-n}}$ את הווקטורים שהושמטו מבין $u_1,...,u_m$. לפי ההגדרה כל וקטור כזה הוא צירוף לינארי של $u_1,...,u_m$.

<u>למה</u>: יהי V מרחב וקטורי ויהיו $\alpha_1,...,\alpha_k\in V$. אם $\alpha_k\in\mathrm{Sp}(\alpha_1,...,\alpha_{k-1})$ אזי

$$\mathrm{Sp}(\alpha_1,...,\alpha_k)=\mathrm{Sp}(\alpha_1,...,\alpha_{k-1})$$

<u>הוכחה</u>: ברור ש- $\mathrm{Sp}(\alpha_1,...,\alpha_{k-1})\subset\mathrm{Sp}(\alpha_1,...,\alpha_k)$. אם $\alpha_k\in\mathrm{Sp}(\alpha_1,...,\alpha_{k-1})$ אזי $\alpha_k=\sum_{i=1}^{k-1}c_i\alpha_i$. יהי

$$v=\sum_{i=1}^{k}d_i\alpha_i\in\mathrm{Sp}(\alpha_1,...,a_k)$$ אזי

$$v=\sum_{i=1}^{k-1}d_i\alpha_i+d_k\sum_{i=1}^{k-1}c_i\alpha_i=\sum_{i=1}^{k-1}d_i\alpha_i+\sum_{i=1}^{k-1}(d_kc_i)\alpha_i=\sum_{i=1}^{k-1}(d_i+d_kc_i)\alpha_i\in\mathrm{Sp}(\alpha_1,...,\alpha_{k-1})$$

ולכן $\mathrm{Sp}(\alpha_1,...,\alpha_{k-1})\supset\mathrm{Sp}(\alpha_1,...,\alpha_k)$. לכן $\mathrm{Sp}(\alpha_1,...,\alpha_k)=\mathrm{Sp}(\alpha_1,...,\alpha_{k-1})$. מש"ל ☺

כעת נמספר מחדש את הווקטורים $u_1,...,u_m$ כך ש- $\beta_{i_1},...,\beta_{i_{m-n}}$ יופיעו בסוף הרשימה. ע"י שימוש בלמה $m-n$ פעמים נקבל ש- $V=\mathrm{Sp}(B)$. לכן B בסיס ל- V. מש"ל ☺

משפט 22: יהי $V=\mathrm{Sp}(u_1,...,u_m)$ ויהיו $v_1,...,v_k\in V$ בלתי תלויים לינארית. ניתן להשלים את $v_1,...,v_k$ לבסיס ע"י וקטורים מ- $\{u_1,...,u_m\}$.

משמעות: בהינתן קבוצת וקטורים בלתי תלויה לינארית במרחב נוצר סופית ניתן להרחיב אותה לבסיס של המרחב בשימוש בוקטורים היוצרים.

הוכחה: ברור ש- $V=\mathrm{Sp}(u_1,...,u_m)=\mathrm{Sp}(v_1,...,v_k,u_1,...,u_m)$. $v_1,...,v_k$ בלתי תלויים לינארית ולכן כל אחד מהם אינו צירוף לינארי של קודמיו. לכן על סמך המשפט הקודם נקבל בסיס של V מהצורה $v_1,...,v_k,u_{j_1},...,u_{j_l}$ שכן הוקטורים $v_1,...,v_k$ יעברו את תהליך הסינון שהצגנו. מש"ל ☺

טענה 23: יהי V מרחב וקטורי ותהי $B=\{v_1,...,v_n\}$ קבוצת וקטורים ב- V. אזי התנאים הבאים שקולים:

1. B בסיס של V
2. B קבוצה פורשת מינימלית
3. B קבוצה בלתי תלויה לינארית מקסימלית

הוכחה:

(א $\Leftarrow$ ב) אם B בסיס אזי היא קבוצה פורשת. נוכיח שהיא מינימלית. נניח בשלילה שהיא לא מינימלית. אזי קיים וקטור $v_i\in B$ שניתן להשמיט אותו מ- B ובכל זאת לקבל קבוצה פורשת. כלומר $B'=\{v_1,...,v_{i-1},v_{i+1},...,v_n\}$ פורשת את V. ברור ש- B' בלתי תלויה לינארית. ולכן B' בסיס. אבל $|B'|=n-1$ בסתירה לכך שבכל בסיס של V יש אותו מספר איברים.

(ב $\Leftarrow$ א) אם B קבוצה פורשת מינימלית בפרט היא פורשת. נראה שהיא בלתי תלויה לינארית. נניח שקיימת תלות לינארית. לפי טענת עזר קודמת קיים $1\le i\le n$ כך ש- $v_i\in\mathrm{Sp}(v_1,...,v_{i-1})$. אזי $V=\mathrm{Sp}(v_1,...,v_{i-1},v_{i+1},...,v_n)=\mathrm{Sp}(v_1,...,v_{i-1},v_i,v_{i+1},...,v_n)$ בסתירה למינימליות של B. לכן B בלתי תלויה לינארית ולכן היא בסיס.

(א $\Leftarrow$ ג) אם B בסיס אז היא בלתי תלויה לינארית ופורשת. לכן לכל $v_{n+1}\in V$ מתקיים $v_{n+1}\in\mathrm{Sp}(v_1,...,v_n)$. לכן $v_1,...,v_n,v_{n+1}$ תלויים לינארית. כלומר B קבוצה בלתי תלויה לינארית מקסימלית.

(ג $\Leftarrow$ א) אם B קבוצה בלתי תלויה לינארית מקסימלית אזי היא בפרט בלתי תלויה לינארית. נוכיח שהיא פורשת. נניח בשלילה ש- $V\ne\mathrm{Sp}(v_1,...,v_n)$. אזי קיים $v_{n+1}\in V$ כך ש- $v_{n+1}\notin\mathrm{Sp}(v_1,...,v_n)$. לכן לפי טענת העזר $v_1,...,v_{n+1}$ בלתי תלויה לינארית, בסתירה למקסימליות של B. מש"ל ☺

טענה 24: יהי V מרחב וקטורי מעל שדה F ויהיו $U,W\subset V$ תת מרחבים. אזי החיתוך $U\cap W$ גם כן תת מרחב של V.

הוכחה: $0_V\in W,0_V\in U$ משום שהם תת מרחבים ולכן $0_V\in U\cap W$ כלומר $U\cap W\ne\varnothing$.

יהיו $u,w\in U\cap W$. אזי $u,w\in W,u,w\in V$. לכן $u+w\in W,u+w\in V$ ומכאן ש- $u+w\in U\cap W$ כלומר יש סגירות תחת חיבור.

יהיו $v\in U\cap W$ ו- $c\in F$. אזי $v\in W,v\in U$ ולכן $cv\in W,cv\in U$. מכאן ש- $cv\in U\cap W$ כלומר יש סגירות תחת כפל בסקלר. לכן $U\cap W$ תת מרחב וקטורי של V. מש"ל ☺

הגדרה: יהי V מרחב וקטורי ויהיו $U,W\subset V$ תת מרחבים. נסמן

$$U+W=\{u+w:u\in U,w\in W\}$$

טענה 25: יהי V מרחב וקטורי ויהיו $U,W\subset V$ תת מרחבים. אזי $U+W$ תת מרחב וקטורי של V.

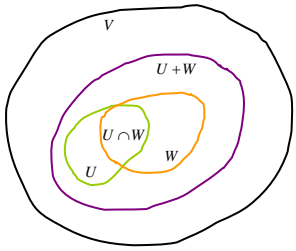
הוכחה: $0_V\in W,0_V\in U$ משום שהם תת מרחבים ולכן $0_V=0_V+0_V\in U+W$ כלומר $U+W\ne\varnothing$.

יהיו $v_1,v_2\in U+W$. אזי $v_1=u_1+w_1,v_2=u_2+w_2$ כאשר $u_1,u_2\in U,w_1,w_2\in W$. לכן $u_1+u_2\in U,w_1+w_2\in W$ ו- $v_1+v_2=(u_1+w_1)+(u_2+w_2)=(u_1+u_2)+(w_1+w_2)\in V+W$ ומכאן ש- $v_1+v_2\in U+W$ כלומר יש סגירות תחת חיבור.

יהיו $v\in U+W$ ו- $c\in F$. אזי $v=u+w$ כאשר $u\in U,w\in W$. אזי $cu\in U,cw\in W$ ולכן $cv=c(u+w)=cu+cw\in U+W$. מכאן ש- $cv\in U+W$ כלומר יש סגירות תחת כפל בסקלר. לכן $U+W$ תת מרחב וקטורי של V. מש"ל ☺

נעיר רק שאם $U,W\subset V$ תת מרחבים אזי $U\cup W$ אינו בהכרח תת מרחב. למשל אם נסתכל על $\mathbb{R}^3$ ועל תת המרחבים שלו – הציר האופקי והציר האנכי – ניווכח שהאיחוד שלהם אינו תת מרחב כמובן. למשל $(1,1)=(0,1)+(1,0)$ ונקודה זו אינה נמצאת על אף אחד מהצירים. כלומר בדוגמה זו אין סגירות תחת חיבור.
אבל, אם $W\cup U$ תת מרחב אזי בהכרח $W\subset U$ או $U\subset W$.

<u>משפט 26</u>: יהי V מרחב וקטורי נוצר סופית. יהיו $U,W\subset V$ תת מרחבים. אזי
$$\dim_F(U+W)=\dim_F U+\dim_F V-\dim_F(U\cap W)$$
<u>הוכחה</u>: ראשית נראה ציור סכמטי של המצב:



$U\cap W$ תת מרחב של מרחב וקטורי נוצר סופית V ולכן ניתן לבחור לו בסיס $v_1,...,v_m$. $U\cap W$ הוא גם תת מרחב של U ולכן ניתן להשלים את $v_1,...,v_m$ לבסיס של U כך: $v_1,...,v_m,u_1,...,u_k$. אבל $U\cap W$ הוא גם תת מרחב של W ולכן ניתן להשלים את $v_1,...,v_m$ לבסיס של W כך: $v_1,...,v_m,w_1,...,w_l$.
נטען שהווקטורים $v_1,...,v_m,u_1,...,u_k,w_1,...,w_l$ הם בסיס של $U+W$.
נראה שהקבוצה פורשת: יהי $v\in U+W$. אזי קיימים $u\in U,w\in W$ כך ש- $v=u+w$. ניתן לרשום אז
$u=\sum_{i=1}^{m}a_iv_i+\sum_{i=1}^{k}b_iu_i$ ו- $w=\sum_{i=1}^{m}c_iv_i+\sum_{i=1}^{l}d_iw_i$ ואז
$$v=u+w=\sum_{i=1}^{m}a_iv_i+\sum_{i=1}^{k}b_iu_i+\sum_{i=1}^{m}c_iv_i+\sum_{i=1}^{l}d_iw_i=$$
$$=\sum_{i=1}^{m}(a_i+c_i)v_i+\sum_{i=1}^{k}b_iu_i+\sum_{i=1}^{l}d_iw_i\in \mathrm{Sp}(v_1,...,v_m,u_1,...,u_k,w_1,...,w_l)$$
משום ש- $v_1,...,v_m,u_1,...,u_k,w_1,...,w_l\in U+W$ נקבל שהם פורשים את $U+W$.
נראה שהקבוצה בלתי תלויה לינארית: נניח ש- $\sum_{i=1}^{m}a_iv_i+\sum_{i=1}^{k}b_iu_i+\sum_{i=1}^{l}d_iw_i=0_V$ ונראה שכל המקדמים הם איבר האפס של השדה.
נסמן $z=\sum_{i=1}^{m}a_iv_i+\sum_{i=1}^{k}b_iu_i=-\sum_{i=1}^{l}d_iw_i$. לכן $z\in U$ וגם $z\in W$ ולכן $z\in U\cap W$. לכן נוכל לרשום $z=\sum_{i=1}^{m}c_iv_i=\sum_{i=1}^{m}c_iv_i+\sum_{i=1}^{k}0_Fu_i$ כלומר ל- z יש שתי הצגות כצירוף לינארי של הבסיס של U. בגלל יחידות ההצגה נקבל $1\le i\le k, b_i=0_F$. לכן $\sum_{i=1}^{m}a_iv_i+\sum_{i=1}^{l}d_iw_i=0_V$. אבל $v_1,...,v_m,w_1,...,w_l$ בסיס של W ולכן הם בלתי תלויים לינארית ולכן נקבל $d_1=...=d_l=a_1=...=a_m=0_F$. כלומר $v_1,...,v_m,u_1,...,u_k,w_1,...,w_l$ בלתי תלויים לינארית.
מכאן נובע ש- $v_1,...,v_m,u_1,...,u_k,w_1,...,w_l$ הם בסיס.
כעת נקבל:
$$\dim_F(U+W)=m+k+l=(m+k)+(m+l)-m=\dim_F U+\dim_F W-\dim_F(U\cap W)$$
כלומר $\dim_F(U+W)=\dim_F U+\dim_F W-\dim_F(U\cap W)$. מש"ל ☺

לסיכום, נציין <u>טענה מגניבה</u>: יהי F שדה בעל מציין $p>0$. אזי קיים n כך ש- $|F|=p^n$.
<u>הוכחה</u>: ראשית נשים לב שאם V מרחב וקטורי ממימד סופי מעל $\mathbb{Z}_p$, אזי קיים איזומורפיזם בין V לבין מרחב ה- n-יות $\{(a_1,...,a_n):a_i\in\mathbb{Z}_p\}$, שהרי כל וקטור ניתן להציג באופן יחיד כצירוף לינארי של איברי הבסיס, ואז $(a_1,...,a_n)$ היא ה- n-יה שמייצגת את המקדמים בהצגה זו. ברור ש- $|\{(a_1,...,a_n):a_i\in\mathbb{Z}_p\}|=p^n$ ולכן $|V|=p^n$.

כעת נחזור לבעיה שלנו. לפי משפט (8) קיים ל- F תת שדה K איזומורפי ל- $\mathbb{Z}_p$. כעת נסתכל על F כמרחב וקטורי מעל K. ברור אז ש- F נוצר סופית, שהרי F עצמו סופי. נניח שהמימד הוא n ואז לפי מה שאמרנו קודם $|F| = p^n$. מש"ל ☺

4. העתקות לינאריות

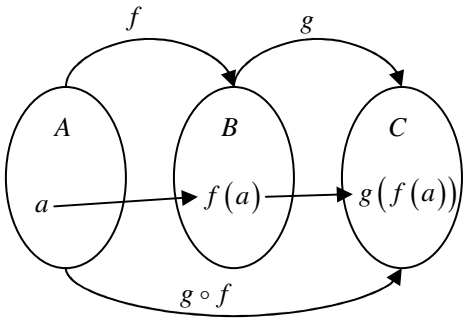
4.1. תכונות כלליות של העתקות

יהיו A, B קבוצות של איברים כלשהם. $f : A \to B$ **העתקה** מ- A ל- B היא התאמה של איבר אחד ויחיד מ- B לכל איבר של A. אם ל- $a \in A$ מותאם $b \in B$ מסמנים $f(a) = b$.

על כל קבוצה A ניתן להגדיר העתקה שלא עושה דבר, והיא נקראת **העתקת הזהות** $Id_A : A \to A$ ולכל $a \in A$ מתקיים $Id_A(a) = a$.

נאמר שההעתקה f היא **חד-חד-ערכית** (להלן חח"ע) כאשר לכל $a, b \in A$, אם $f(a) = f(b)$ אז $a = b$.
נאמר שההעתקה f היא **על** אם לכל $b \in B$ קיים $a \in A$ כך ש- $f(a) = b$.
נשים ♥ שמראש תנאים אלה לא נתונים לנו. ההעתקה מתאימה איבר אחד ויחיד $b \in B$ לכל איבר $a \in A$. כלומר לא יכול להיות "$f(a) = b', f(a) = b''$ אבל "$b' \neq b''$ וכן לא יכול להיות שקיים $a \in A$ שלא מותאם לו איבר ב- B. אבל יכול להיות ש- "$f(a') = f(a'')$ ו- "$a' \neq a''$ וכן יכול להיות שיש איזה $b \in B$ שלא קיים $a \in A$ כך ש- $f(a) = b$.
אם העתקה $f : A \to B$ היא חח"ע ועל קיימת העתקה שנקראת ההעתקה ה**הפכית** שנסמנה $f^{-1} : B \to A$ והיא מקיימת ש- $f(a) = b \Leftrightarrow f^{-1}(b) = a$ (לא נוכיח זאת במסגרת זו).

יהיו A, B, C קבוצות ויהיו $f : A \to B, g : B \to C$ העתקות. נגדיר את **ההרכבה** $g \circ f : A \to C$ באופן הבא: לכל $a \in A$ $(g \circ f)(a) = g(f(a))$[††††]. כלומר קודם מפעילים את f על a ולאחר מכן מפעילים את g על התוצאה.
באופן סכמטי:



אם $f : A \to B, f^{-1} : B \to A$ הופכיות אזי $f \circ f^{-1} = Id_B, f^{-1} \circ f = Id_A$.

נטען שפעולת הרכבת ההעתקות היא אסוציאטיבית. יהיו $f : A \to B, g : B \to C, h : C \to D$. אזי לכל $a \in A$ מתקיים $(hg)f = h(gf)$. כלומר $(h(gf))(a) = h((gf)(a)) = h(g(f(a))) = (hg)(f(a)) = ((hg)f)(a)$.

[††††] להבא נשמיט את הסימן $\circ$. מההקשר יהיה ברור למה הכוונה.

4.2. העתקות לינאריות של מרחבים וקטוריים

אם הקבוצות הן מרחבים וקטוריים אזי ההעתקה היא בין מרחבים וקטוריים (דה!). אנחנו נתעניין בסוג מסוים של העתקות: העתקות לינאריות. העתקות אלה מוגדרות על מרחבים וקטוריים רק במקרה ששניהם מוגדרים מעל אותו השדה.

יהי, אם כן שדה F ויהיו V,W מרחבים וקטוריים מעל F. ותהי $f:V\to W$ העתקה ביניהם. נאמר שההעתקה f היא **לינארית** כאשר מתקיימים שני התנאים הבאים:

$$\forall v_1,v_2\in V \qquad f\left(v_1+v_2\right)=f\left(v_1\right)+f\left(v_2\right)$$
$$\forall v\in V,\forall c\in F \qquad f\left(cv\right)=cf\left(v\right)$$

ההגדרה מסבירה לנו מדוע קבענו שהמרחבים צריכים להיות מעל אותו השדה. אחרת אין משמעות לביטוי $cf\left(v\right)$.

נשים ♥ שהעתקת הזהות על מרחב וקטורי היא לינארית: $Id_V:V\to V$. אזי לכל $v_1,v_2,v\in V,c\in F$ מתקיימים התנאים הנחוצים:

$$Id_V\left(v_1+v_2\right)=v_1+v_2=Id_V\left(v_1\right)+Id_V\left(v_2\right)$$
$$Id_V\left(cv\right)=cv=cId_V\left(v\right)$$

<u>טענה 27</u>: יהיו V,U,W מרחבים וקטוריים מעל שדה F. יהיו $f:V\to U$ ו- $g:U\to W$ העתקות לינאריות. אזי $g\circ f:V\to W$ לינארית.

<u>הוכחה</u>: נראה שמתקיימים שני התנאים של הגדרת העתקה לינארית. יהיו $v_1,v_2,v\in V,c\in F$. אזי:

$$\left(g\circ f\right)\left(v_1+v_2\right)=g\left(f\left(v_1+v_2\right)\right)=g\left(f\left(v_1\right)+f\left(v_2\right)\right)=g\left(f\left(v_1\right)\right)+g\left(f\left(v_2\right)\right)=\left(g\circ f\right)\left(v_1\right)+\left(g\circ f\right)\left(v_2\right)$$
$$\left(g\circ f\right)\left(cv\right)=g\left(f\left(cv\right)\right)=g\left(cf\left(v\right)\right)=cg\left(f\left(v\right)\right)=c\left(\left(g\circ f\right)\left(v\right)\right)$$

הראינו שמתקיימות שתי התכונות של העתקות לינאריות. לכן $g\circ f$ לינארית. מש"ל ☺

<u>טענה 28</u>: אם $f:V\to W$ העתקה לינארית חח"ע ועל אזי גם $f^{-1}:W\to V$ לינארית.

<u>הוכחה</u>: יהיו $w_1,w_2,w\in W,c\in F$. נראה שמתקיימים שני התנאים של ההגדרה של העתקה לינארית.

נסמן $v_1=f^{-1}\left(w_1\right),v_2=f^{-1}\left(w_2\right)\in V$ כלומר $f\left(v_1\right)=w_1,f\left(v_2\right)=w_2\in W$. כעת $f\left(v_1+v_2\right)=f\left(v_1\right)+f\left(v_2\right)=w_1+w_2$. נפעיל את f^{-1} משני האגפים ונקבל

$$f^{-1}\left(w_1\right)+f^{-1}\left(w_2\right)=v_1+v_2=Id_V\left(v_1+v_2\right)=\left(f^{-1}f\right)\left(v_1+v_2\right)=f^{-1}\left(f\left(v_1+v_2\right)\right)=f^{-1}\left(w_1+w_2\right)$$

באופן דומה נסמן $v=f^{-1}\left(w\right)$ כלומר $w=f\left(v\right)$. אזי $f\left(cv\right)=cf\left(v\right)=cw$. נפעיל את f^{-1} משני האגפים ונקבל $cf^{-1}\left(w\right)=cv=Id_V\left(cv\right)=\left(f^{-1}f\right)\left(cv\right)=f^{-1}\left(cw\right)$. מש"ל ☺

<u>טענה 29</u>: תהי $f:V\to W$ העתקה לינארית. אזי $f\left(0_V\right)=0_W$.

<u>הוכחה</u>: $f\left(0_v\right)=f\left(0_V+0_V\right)=f\left(0_V\right)+f\left(0_V\right)$. נחבר לשני האגפים $-f\left(0_V\right)$ ונקבל $f\left(0_V\right)=0_W$. מש"ל ☺

תהי $f:V\to W$ העתקה לינארית. נגדיר:

הגרעין של ההעתקה: $\operatorname{Ker}f=\left\{v\in V:f\left(v\right)=0\right\}$

התמונה של ההעתקה: $\operatorname{Im}f=\left\{w\in W:\exists v\in V\ f\left(v\right)=w\right\}$

<u>טענה 30</u>: יהיו V,W מרחבים וקטוריים מעל F ותהי העתקה לינארית $f:V\to W$. אזי

א. הגרעין של ההעתקה הוא תת מרחב של V

ב. התמונה של ההעתקה היא תת מרחב של W

<u>הוכחה</u>:

א. לפי טענה (29) $0_V\in\operatorname{Ker}f$. נראה סגירות לחיבור ולכפל בסקלר: יהיו $v_1,v_2,v\in\operatorname{Ker}f,c\in F$. אזי $f\left(v_1+v_2\right)=f\left(v_1\right)+f\left(v_2\right)=0_W+0_W=0_W$ וכן $f\left(cv\right)=cf\left(v\right)=c\cdot0_W=0_W$. קיבלנו ש- $v_1+v_2,cv\in\operatorname{Ker}f$. לפי משפט קודם $\operatorname{Ker}f$ תת מרחב וקטורי.

ב. לפי טענה (29) $0_W \in \operatorname{Im} f$. נראה סגירות לחיבור ולכפל בסקלר: יהיו $w_1, w_2, w \in \operatorname{Im} f, c \in F$. אזי קיימים $v_1, v_2, v \in V$ כך ש- $f(v_1) = w_1, f(v_2) = w_2, f(v) = w$. אזי $f(v_1 + v_2) = w_1 + w_2$ וכן $f(cv) = cw$ כלומר $w_1 + w_2, cw \in \operatorname{Im} f$. לפי משפט קודם $\operatorname{Im} f$ הוא תת מרחב וקטורי. מש"ל ☺

<u>טענה 31</u>: $f: V \to W$ חח"ע אמ"מ $\operatorname{Ker} f = \{0_V\}$

<u>הוכחה</u>:

($\Leftarrow$) לפי טענה (29) $f(0_V) = 0_W$. משום ש- f חח"ע לא קיים אף איבר אחר $v \neq 0_V$ שעבורו $f(v) = 0$ ולכן $\operatorname{Ker} f = \{0_V\}$.

($\Rightarrow$) יהיו v_1, v_2 כך ש- $f(v_1) = f(v_2)$. אזי $0_W = f(v_1) - f(v_2) = f(v_1 - v_2)$. כלומר $v_1 - v_2 \in \operatorname{Ker} f$ אבל $\operatorname{Ker} f = \{0_V\}$, כלומר $v_1 - v_2 = 0_V$ ולכן $v_1 = v_2$. כלומר f חח"ע. מש"ל ☺

נשים לב שהעתקה חח"ע מעבירה וקטורים בלתי תלויים לינארית לווקטורים בלתי תלויים לינארית. כלומר אם $v_1, \ldots, v_k$ בת"ל ו- $f: V \to W$ חח"ע אז $f(v_1), \ldots, f(v_k)$ בת"ל. מדוע? אם $v_1, \ldots, v_k$ בת"ל אז אם $\sum_{i=1}^{k} a_i v_i = 0_V$ אז $a_i = 0_F$. נניח ש- $\sum_{i=1}^{k} c_i f(v_i) = 0_W$. אבל בגלל הלינאריות של f כלומר $\sum_{i=1}^{k} c_i f(v_i) = f\left(\sum_{i=1}^{k} c_i v_i\right)$. $\sum_{i=1}^{k} c_i v_i \in \operatorname{Ker} f = \{0_V\}$ לכן $c_i = 0_F$. ולכן $f(v_1), \ldots, f(v_k)$ בת"ל.

<u>טענה 32</u>: יהיו $f: V \to W, g: W \to U$. אזי $\operatorname{Ker} f \subseteq \operatorname{Ker}(gf)$

<u>הוכחה</u>: יהי $v \in \operatorname{Ker} f$. אזי $(gf)(v) = g(f(v)) = g(0) = 0$. כלומר $v \in \operatorname{Ker}(gf)$. מכאן הטענה $\operatorname{Ker} f \subseteq \operatorname{Ker}(gf)$. מש"ל ☺

<u>משפט 32</u> (**משפט המימדים**): יהי V מרחב וקטורי נוצר סופית ותהי $f: V \to W$ העתקה לינארית. אזי

$$\dim_F \operatorname{Ker} f + \dim_F \operatorname{Im} f = \dim_F V$$

<u>הערה</u>: במשפט מובלעות בעצם עוד שתי טענות: שקיים בסיס לגרעין (אבל זה ברור כי הוא תת מרחב של מרחב וקטורי נוצר סופית ולכן לפי משפט קודם קיים לו בסיס) וקיים בסיס לתמונה (התמונה היא בכלל תת מרחב של W ואנחנו לא יודעים עליו דבר).

<u>הוכחה</u>:

<u>למה</u>: אם $V = \operatorname{Sp}(z_1, \ldots, z_m)$ אזי $\operatorname{Im} f = \operatorname{Sp}(f(z_1), \ldots, f(z_m))$.

<u>הערה</u>: הלמה מסבירה מדוע קיים בסיס לתמונה של f ולכן השוויון שלעיל מוגדר היטב.

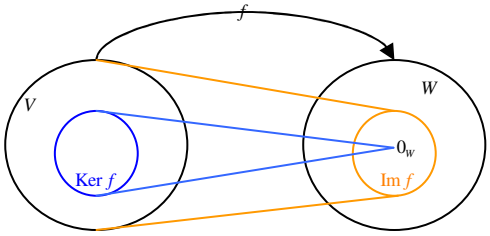
<u>הוכחה</u>: נוכיח הכלה בשני הכיוונים:

($\supseteq$) $f(z_1) \in \operatorname{Im} f$ שהרי $z_1 \in V$ הוא מקור שלו. באותו אופן $f(z_i) \in \operatorname{Im} f$ לכל $2 \leq i \leq m$. והוכחנו ש- $\operatorname{Im} f \subseteq W$ הוא תת מרחב. לכן הוא סגור לחיבור ולכפל בסקלר. לכן $\operatorname{Im} f \supseteq Sp(f(z_1), \ldots, f(z_m))$.

($\subseteq$) יהי $w \in \operatorname{Im} f$. אזי קיים $v \in V$ כך ש- $f(v) = w$. אבל $V = \operatorname{Sp}(z_1, \ldots, z_m)$ ולכן ניתן לרשום $v = \sum_{i=1}^{m} a_i z_i$ כאשר $a_i \in F$. אז $f(v) = f\left(\sum_{i=1}^{m} a_i z_i\right) = \sum_{i=1}^{m} a_i f(z_i) \in \operatorname{Sp}(f(z_1), \ldots, f(z_m))$. כלומר $\operatorname{Im} f \subseteq Sp(f(z_1), \ldots, f(z_m))$.

הראנו הכלה בשני היכוונים ומכאן ש- $\operatorname{Im} f = Sp(f(z_1), \ldots, f(z_m))$. ☺

נעשה ציור סכמטי של המצב:



נבחר בסיס $u_1,...,u_k$ ל- $\operatorname{Ker} f$ (זה אפשרי משום ש- V נוצר סופית והגרעין הוא תת מרחב שלו).
נבחר בסיס $w_1,...,w_l$ ל- $\operatorname{Im} f$ (זה אפשרי לפי הלמה). כלומר קיימים $v_1,...,v_l \in V$ כך ש- $f(v_i)=w_i$ לכל $1 \le i \le l$.
אם נראה ש- $u_1,...,u_k,v_1,...,v_l$ הם בסיס של V נקבל את השוויון הדרוש כי אז $\dim_F \operatorname{Ker} f + \dim_F \operatorname{Im} f = k+l = \dim_F V$.
נראה אם כן ש- $u_1,...,u_k,v_1,...,v_l$ פורשים את V ובת"ל.

פורשים: $V \in v$ יהי $v \in V$. נראה ש- $u_1,...,u_k,v_1,...,v_l \in V$ ולכן $\operatorname{Sp}(u_1,...,u_k,v_1,...,v_l) \subseteq V$. נראה הכלה בכיוון השני:
$v \in \operatorname{Sp}(u_1,...,u_k,v_1,...,v_l)$. נסתכל על $f(v) \in \operatorname{Im} f$. נפתח את $f(v)$ לפי הבסיס $w_1,...,w_l$:

$$f(v)=\sum_{i=1}^{l} a_i w_i = \sum_{i=1}^{l} a_i f(v_i) = f\left(\sum_{i=1}^{l} a_i v_i\right)$$

לכן $f(v)-f\left(\sum_{i=1}^{l} a_i v_i\right)=0$ כלומר $v-\sum_{i=1}^{l} a_i v_i \in \operatorname{Ker} f$. נפתח וקטור זה לפי הבסיס $u_1,...,u_k$: $v-\sum_{i=1}^{l} a_i v_i = \sum_{i=1}^{k} b_i u_i \in \operatorname{Ker} f$. נעביר אגפים ונקבל

$$v=\sum_{i=1}^{l} a_i v_i + \sum_{i=1}^{k} b_i u_i \in \operatorname{Sp}(v_1,...,v_l,u_1,...,u_k)$$

לכן $\operatorname{Sp}(u_1,...,u_k,v_1,...,v_l) \supseteq V$ לכן $\operatorname{Sp}(u_1,...,u_k,v_1,...,v_l)=V$.

אי תלות: נניח ש- $\sum_{i=1}^{l} a_i v_i + \sum_{i=1}^{k} b_i u_i = 0_V$. אזי:

$$0_W = f(0_V) = f\left(\sum_{i=1}^{l} a_i v_i + \sum_{i=1}^{k} b_i u_i\right) = \sum_{i=1}^{l} a_i f(v_i) + \sum_{i=1}^{k} b_i f(u_i) = \sum_{i=1}^{l} a_i w_i + \sum_{i=1}^{k} b_i \cdot 0_W = \sum_{i=1}^{l} a_i w_i + 0_W = \sum_{i=1}^{l} a_i w_i$$

אבל $w_1,...,w_l$ בסיס ובפרט בת"ל, לכן $a_i=0$. כלומר $0_V = \sum_{i=1}^{l} a_i v_i + \sum_{i=1}^{k} b_i u_i = 0_W + \sum_{i=1}^{k} b_i u_i = \sum_{i=1}^{k} b_i u_i$. אבל
$u_1,...,u_k$ בסיס ובפרט בת"ל ולכן $b_i=0$. קיבלנו שכל המקדמים הם 0. לכן $u_1,...,u_k,v_1,...,v_l$ בת"ל.
קיבלנו ש- $u_1,...,u_k,v_1,...,v_l$ פורשים ובת"ל ולכן הם בסיס ל- V וכפי שראינו כבר מכאן נובע המשפט. מש"ל ☺

משפט המימדים הוא יעיל מאוד ומשתמשים בו רבות. למשל, הוכחנו שהעתקה היא חח"ע ועל אמ"מ $\dim_F V = \dim_F \operatorname{Ker} f + \dim_F \operatorname{Im} f = 0 + \dim_F W = \dim_F W$. אז נקבל $\operatorname{Ker} f = \{0_V\}, \operatorname{Im} f = W$.

יהיו V,W מרחבים וקטוריים מעל F. נסמן $\operatorname{Hom}_F(V,W)=\{f:V\to W \mid f \text{ is linear}\}$. נגדיר על קבוצה זו
(קבוצת כל ההעתקות הלינאריות מ- V ל- W) מבנה של מרחב וקטורי מעל F.
חיבור: אם $f,g \in \operatorname{Hom}_F(V,W)$ אז נגדיר לכל $v \in V$ $(f+g)(v)=f(v)+g(v)$
כפל בסקלר: אם $f \in \operatorname{Hom}_F(V,W), c \in F$ נגדיר לכל $v \in V$ $(cf)(v)=cf(v)$.

<u>טענה 33</u>: $\operatorname{Hom}_F(V,W)$ עם הפעולות שהגדרנו למעלה הוא מרחב וקטורי מעל F.

<u>הוכחה</u>: נראה שמתקיימות כל אקסיומות המרחב הווקטורי:
אקסיומות החיבור:

1. סגירות: יהיו $f,g \in \operatorname{Hom}_F(V,W)$. נראה ש- $f+g \in \operatorname{Hom}_F(V,W)$:
   i. יהיו $v_1,v_2 \in V$. אזי:
$$(f+g)(v_1+v_2)=f(v_1+v_2)+g(v_1+v_2)=f(v_1)+f(v_2)+g(v_1)+g(v_2)=$$
$$=f(v_1)+g(v_1)+f(v_2)+g(v_2)=(f+g)(v_1)+(f+g)(v_2)$$
   ii. יהיו $v \in V, c \in F$. אזי:
$$(f+g)(cv)=f(cv)+g(cv)=cf(v)+cg(v)=c\big(f(v)+g(v)\big)=c\big((f+g)(v)\big)$$
   הראנו שמתקיימות התכונות של העתקה לינארית. לכן $f+g \in \operatorname{Hom}_F(V,W)$.
2. קומוטטיביות: לכל $v \in V$ מתקיים $(f+g)(v)=f(v)+g(v)=g(v)+f(v)=(g+f)(v)$. לכן
   $f+g=g+f$.
3. אסוציאטיביות: לכל $v \in V$ מתקיים
$$\big(f+(g+h)\big)(v)=f(v)+(g+h)(v)=f(v)+\big(g(v)+h(v)\big)=$$
$$=\big(f(v)+g(v)\big)+h(v)=(f+g)(v)+h(v)=\big((f+g)+h\big)(v)$$
   לכן $f+(g+h)=(f+g)+h$.

4. קיום אפס: נגדיר העתקה $0_{V,W}:V\to W$ באופן הבא: $0_{V,W}(v)=0_W$. ראשית נטען ש-$0_{V,W}\in \mathrm{Hom}_F(V,W)$. יהיו $v_1,v_2,v\in V, c\in F$. אזי

$$0_{V,W}(v_1+v_2)=0_W=0_W+0_W=0_{V,W}(v_1)+0_{V,W}(v_2)$$
$$0_{V,W}(cv)=0_W=c\cdot 0_W=c\cdot 0_{V,W}(v)$$

כעת נראה שהעתקה זו היא אכן איבר ניטרלי לחיבור ב-$\mathrm{Hom}_F(V,W)$. תהי $f\in \mathrm{Hom}_F(V,W)$. אזי $(f+0_{V,W})(v)=f(v)+0_{V,W}(v)=f(v)+0_W=f(v)$. לכן $f+0_{V,W}=f$, כלומר, העתקה זו ניטרלית לחיבור.

5. קיום איבר נגדי: לכל $f\in \mathrm{Hom}_F(V,W)$ נגדיר $-f:V\to W$ באופן הבא: $(-f)(v)=-f(v)$. ראשית נראה ש-$-f\in \mathrm{Hom}_F(V,W)$. יהיו $v_1,v_2,v\in V, c\in F$. אזי

$$(-f)(v_1+v_2)=-f(v_1+v_2)=-\big(f(v_1)+f(v_2)\big)=-f(v_1)+\big(-f(v_2)\big)=(-f)(v_1)+(-f)(v_2)$$
$$(-f)(cv)=-f(cv)=-\big(cf(v)\big)=c\big(-f(v)\big)=c\big((-f)(v)\big)$$

לכן $-f\in \mathrm{Hom}_F(V,W)$. נראה כעת שהיא נגדית ל-$f$. לכל $v\in V$ מתקיים

$$(f+(-f))(v)=f(v)+(-f)(v)=f(v)+\big(-(f(v))\big)=0_W,\ \text{כנדרש!}$$

אקסיומות כפל בסקלר:

1. סגירות: יהיו $f\in \mathrm{Hom}_F(V,W)$ ו-$c\in F$. נראה ש-$cf\in \mathrm{Hom}_F(V,W)$:
   i. יהיו $v_1,v_2\in V$. אזי:

$$(cf)(v_1+v_2)=cf(v_1+v_2)=c\big(f(v_1)+f(v_2)\big)=cf(v_1)+cf(v_2)=(cf)(v_1)+(cf)(v_2)$$

   ii. יהיו $v\in V, a\in F$. אזי:

$$(cf)(av)=cf(av)=c\big(af(v)\big)=(ca)f(v)=(ac)f(v)=a\big(cf(v)\big)=a\big((cf)(v)\big)$$

הראנו שמתקיימות התכונות של העתקה לינארית. לכן $cf\in \mathrm{Hom}_F(V,W)$.

2. לכל $f\in \mathrm{Hom}_F(V,W)$ מתקיים $(1_F f)(v)=1_F f(v)=f(v)$ ולכן $1_F f=f$.

3. לכל $f,g\in \mathrm{Hom}_F(V,W)$ ו-$a,b\in F$ מתקיים:

$((a+b)f)(v)=(a+b)f(v)=af(v)+bf(v)=(af)(v)+(bf)(v)$ כלומר $(a+b)f=af+bf$

$(a(f+g))(v)=a\big((f+g)(v)\big)+a\big(f(v)+g(v)\big)=af(v)+ag(v)=(af)(v)+(ag)(v)$ כלומר $a(f+g)=af+ag$.

הוכחנו שמתקיימות כל אקסיומות המרחב הווקטורי. לכן $\mathrm{Hom}_F(V,W)$ מרחב וקטורי ביחס לפעולות שהגדרנו. מש"ל ☺

<u>משפט 34</u>: יהי V,W מרחבים וקטוריים מעל אותו שדה. יהיו $v_1,\ldots,v_n\in V$ בסיס. אזי לכל $w_1,\ldots,w_n\in W$ קיימת העתקה לינארית יחידה $f:V\to W$ כך ש-$f(v_i)=w_i$ לכל $1\le i\le n$.

<u>הוכחה</u>: לכל $v\in V$ קיימת הצגה יחידה כצירוף לינארי של איברי הבסיס $v=\sum_{i=1}^{n}a_iv_i$. נגדיר $f:V\to W$ באופן הבא: $f(v)=\sum_{i=1}^{n}a_iw_i$. נראה שהעתקה זו מקיימת את התנאים הדרושים:

1. $f:V\to W$ לינארית:
   i. יהיו $v'=\sum_{i=1}^{n}c_i'v_i, v''=\sum_{i=1}^{n}c_i''v_i\in V$. אזי

$$f(v'+v'')=f\left(\sum_{i=1}^{n}c_i'v_i+\sum_{i=1}^{n}c_i''v_i\right)=f\left(\sum_{i=1}^{n}(c_i'+c_i'')v_i\right)=$$
$$=\sum_{i=1}^{n}(c_i'+c_i'')w_i=\sum_{i=1}^{n}c_i'w_i+\sum_{i=1}^{n}c_i''w_i=f(v')+f(v'')$$

   ii. יהיו $v=\sum_{i=1}^{n}c_iv_i\in V$ ו-$a\in F$. אזי

$$f(av)=f\left(a\sum_{i=1}^{n}c_iv_i\right)=f\left(\sum_{i=1}^{n}ac_iv_i\right)=\sum_{i=1}^{n}ac_iw_i=a\sum_{i=1}^{n}c_iw_i=af(w)$$

2. לכל $1\le i\le n$ $f(v_i)=w_i$: ברור ש- $v_i=\sum_{j\neq i}0\cdot v_j+1\cdot v_i$. לכן

$$f\left(\sum_{j\neq i}0\cdot v_j+1\cdot v_i\right)=\sum_{j\neq i}0\cdot w_j+1\cdot w_i=w_i$$

3. $f:V\to W$ עם תכונות אלה היא יחידה: תהי $g:V\to W$ העתקה לינארית שמקיימת $g(v_i)=w_i$. נראה שלכל $v\in V$ מתקיים $g(v)=f(v)$ ומכאן ינבע כי $f=g$. נניח כי $v=\sum_{i=1}^{n}a_iv_i$. מהלינאריות של g נקבל ש-

$$g(v)=g\left(\sum_{i=1}^{n}a_iv_i\right)=\sum_{i=1}^{n}a_ig(v_i)=\sum_{i=1}^{n}a_iw_i=f(v).$$

הראנו את הדרוש. מש"ל ☺

4.3. העתקות לינאריות ומטריצות

מטריצה היא טבלה של איברים בשדה מסוים. אם מספר השורות במטריצה הוא m ומספר העמודות הוא n אומרים שהמטריצה היא מ**סדר** $m\times n$. מסמנים:

$$A=(a_{i,j})=\begin{pmatrix}a_{1,1}&\cdots&a_{1,n}\\ \vdots&\ddots&\vdots\\ a_{m,1}&\cdots&a_{m,n}\end{pmatrix}$$

נסמן את האיבר של A שעומד בשורה i ובטור j ע"י $[A]_{i,j}$.

יהיו V,W מרחבים וקטוריים מעל שדה F ויהיו $\mathfrak{A}=\{v_1,\dots,v_n\}\subseteq V$ ו- $\mathfrak{B}=\{w_1,\dots,w_m\}\subseteq W$ בסיסים שלהם. כלומר $\dim_F V=n,\dim_F W=m$. תהי $f:V\to W$ העתקה לינארית. נבדוק איך היא פועלת על איברי הבסיס של V: נניח שלכל $1\le j\le n$ מתקיים $f(v_j)=\sum_{i=1}^{m}a_{i,j}w_i$ כאשר $a_{i,j}\in F$.

נוכל להתאים להעתקה הזו מטריצה שנסמנה ב- A_f (או ב- $[f]_{\mathfrak{B}}^{\mathfrak{A}}$) מסדר $m\times n$ כך: $A_f=(a_{i,j})$. כלומר בטור ה- j -י של המטריצה נרשום את המקדמים בפיתוח של $f(v_j)$ לפי הבסיס שבחרנו ל- W. ברור שאם היינו בוחרים בסיס אחר המטריצה הייתה אחרת, כלומר האיברים היו שונים, אבל הסדר של המטריצה היה נשאר אותו הסדר. נשים לב שיש משמעות לסדר הווקטורים בבסיס. כלומר כשאנחנו בוחרים כאן בסיס אנחנו בוחרים בסיס סדור!!! כמובן הדברים לא שונים בצורה מהותית לכל סדר שנבחר, אך יש להיות עקביים בחישובים שלנו. מטריצה כזאת כמובן מוגדרת באופן יחיד בהינתן שני בסיסים, שהרי כידוע שההצגה של וקטור כצירוף לינארי של בסיס היא יחידה!

<u>דוגמה</u>: נסתכל על $f:\mathbb{R}^3\to\mathbb{R}^2$ שמוגדרת כך: $f(x,y,z)=(3x-2y+5z,-x+2y-10z)$.
קל להיווכח שזו אכן העתקה לינארית.
כעת נסתכל על הבסיסים הסטנדרטיים של $\mathbb{R}^3,\mathbb{R}^2$: $E_3=((1,0,0),(0,1,0),(0,0,1)),E_2=((1,0),(0,1))$. נבדוק איך ההעתקה פועלת על הבסיס E_3 :

$$f(1,0,0)=(3,-1)=3(1,0)+(-1)(0,1)$$
$$f(0,1,0)=(-2,2)=-2(1,0)+2(0,1)$$
$$f(0,0,1)=(5,-10)=5(1,0)+(-10)(0,1)$$

לכן לפי מה שהגדרנו למעלה המטריצה המתאימה ל- f היא מסדר $2\times3=\dim_{\mathbb{R}}\mathbb{R}^2\times\dim_{\mathbb{R}}\mathbb{R}^3$ והיא

$$A_f=\begin{pmatrix}3&-2&5\\ -1&2&-10\end{pmatrix}$$

משפט 35: יהי V ויהי $w_1,...,w_m \in W$ בסיס של W. אזי לכל מטריצה A מסדר $m\times n$ קיימת העתקה לינארית $f:V\to W$ יחידה כך ש- $A_f = A$.

הוכחה: נתונה $A=\left(a_{i,j}\right)$ מסדר $m\times n$. נגדיר $u_j = \sum_{i=1}^{m} a_{i,j}w_i \in W$ לכל $1\le j\le n$. לפי משפט (9) קיימת העתקה לינארית $f:V\to W$ יחידה כך ש- $f\left(v_j\right)=u_j$ לכל $1\le j\le n$. כלומר $f\left(v_j\right)=\sum_{i=1}^{m} a_{i,j}w_i$. אבל לפי ההגדרה $A_f=\left(a_{i,j}\right)=A$. מש"ל ☺

נסמן את קבוצת כל המטריצות מסדר $m\times n$ שהאיברים שלהן ב- F ע"י $M_{m,n}\left(F\right)$. נגדיר חיבור של מטריצות: יהיו $A,B\in M_{n,m}\left(F\right)$. אם $A=\left(a_{i,j}\right),B=\left(b_{i,j}\right)$ נגדיר $A+B=\left(a_{i,j}+b_{i,j}\right)$ (כלומר מחברים את כל איברי המטריצה איבר-איבר).
נגדיר גם כפל של מטריצה בסקלר. אם $A=\left(a_{i,j}\right)\in M_{m,n}\left(F\right)$ ו- $c\in F$ נגדיר $cA=\left(ca_{i,j}\right)$ (כלומר כופלים כל איבר במטריצה בסקלר).

טענה 36: בהינתן $f,g\in \mathrm{Hom}_F\left(V,W\right), c\in F$ מתקיים $A_{f+g}=A_f+A_g, A_{cf}=cA_f$.
הוכחה: יהיו f,g,c כנ"ל. יהי V ויהי $v_1,...,v_n\in V$ בסיס של W בסיס של $w_1,...,w_m\in W$. אם $A_f=\left(a_{i,j}\right), A_g=\left(b_{i,j}\right)$ אז לפי הגדרה $f\left(v_j\right)=\sum_{i=1}^{m} a_{i,j}w_i, g\left(v_j\right)=\sum_{i=1}^{m} b_{i,j}w_i$ לכל v_j מתקיים $\left(f+g\right)\left(v_j\right)=f\left(v_j\right)+g\left(v_j\right)$. לכן $\left(f+g\right)\left(v_j\right)=\sum_{i=1}^{m} a_{i,j}w_i+\sum_{i=1}^{m} b_{i,j}w_i=\sum_{i=1}^{m}\left(a_{i,j}+b_{i,j}\right)w_i$ ואז לפי ההגדרה $A_{f+g}=\left(a_{i,j}+b_{i,j}\right)=A_f+A_g$.
כעת אם $\left(cf\right)\left(v_j\right)=cf\left(v_j\right)=c\sum_{i=1}^{m} a_{i,j}w_i=\sum_{i=1}^{m} ca_{i,j}w_i$ ולכן לפי ההגדרה $A_{cf}=\left(ca_{i,j}\right)=c\left(a_{i,j}\right)=cA_f$. מש"ל ☺

טענה 37: יהיו V,W מרחבים וקטוריים מעל F ממימד n,m בהתאמה. נגדיר $\varphi:\mathrm{Hom}_F\left(V,W\right)\to M_{m,n}\left(F\right)$ באופן הבא: $\varphi\left(f\right)=A_f$. אזי φ איזומורפיזם.
הוכחה: יש להראות שמתקיימות כל ההגדרות של איזומורפיזם. ההנחה היא כמובן שנתונים בסיסים לשני המרחבים.

1. $\varphi:\mathrm{Hom}_F\left(V,W\right)\to M_{m,n}\left(F\right)$ לינארית:
   i. יהיו $f,g\in\mathrm{Hom}_F\left(V,W\right)$. אזי לפי טענה (36) $\varphi\left(f+g\right)=A_{f+g}=A_f+A_g=\varphi\left(f\right)+\varphi\left(g\right)$
   ii. תהי $f\in\mathrm{Hom}_F\left(V,W\right)$ ויהי $c\in F$. אזי לפי טענה (36) $\varphi\left(cf\right)=A_{cf}=cA_f=c\varphi\left(f\right)$
2. $\varphi:\mathrm{Hom}_F\left(V,W\right)\to M_{m,n}\left(F\right)$ חח"ע: יהיו $f,g\in\mathrm{Hom}_F\left(V,W\right)$ כך ש- $\varphi\left(f\right)=\varphi\left(g\right)$, כלומר $A_f=A_g$. נראה שלכל v_j $f\left(v_j\right)=g\left(v_j\right)$ ומכאן ינבע כי $f=g$ שהרי אם העתקות פועלות באותו אופן על בסיס הן פועלות באותו אופן לכל וקטור. ובכן, לפי ההגדרה: $f\left(v_j\right)=\sum_{i=1}^{m} a_{i,j}w_i \overset{A_f=A_g}{=} \sum_{i=1}^{m} b_{i,j}w_i=g\left(v_j\right)$.
   כלומר $f=g$ ולכן φ חח"ע.
3. $\varphi:\mathrm{Hom}_F\left(V,W\right)\to M_{m,n}\left(F\right)$ על: לפי משפט (35) לכל $A\in M_{m,n}\left(F\right)$ קיימת $f\in\mathrm{Hom}_F\left(V,W\right)$ כך ש- $A=A_f$ כלומר $\varphi\left(f\right)=A_f=A$.

הראנו ש- φ לינארית, חח"ע ועל, ולכן היא איזומורפיזם. מש"ל ☺

מסקנה 38: $M_{m,n}\left(F\right)$ מרחב וקטורי מעל F.
הוכחה: הראנו איזומורפיזם בין הקבוצה $M_{m,n}\left(F\right)$ לבין המרחב הוקטורי $\mathrm{Hom}_F\left(V,W\right)$ ולכן גם הקבוצה $M_{m,n}\left(F\right)$ היא מרחב וקטורי. מש"ל ☺
הערה: ניתן כמובן גם להוכיח את המסקנה ע"י בדיקה ישירה של קיום אקסיומות המרחב הווקטורי, אבל אין שום סיבה לעשות את זה. כבר כשדיברנו על שדות ציינו שאיזומורפיזמים הם העתקות יעילות ביותר!

משפט 39: $\dim_F M_{m,n}(F) = m \cdot n$

הוכחה: לכל $1 \le i \le m, 1 \le j \le n$ נגדיר $E_{ij} = (e_{k,l}) \in M_{m,n}(F)$ כאשר $e_{k,l} = 0$ לכל $k \ne i, l \ne j$ ו-$e_{i,j} = 1$. כלומר כל איברי המטריצה עם אפסים מלבד השורה ה-i בטור ה-j ושם יש 1. ברור שיש $m \cdot n$ מטריצות כאלה. נטען ש-$\{E_{i,j}\}_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ בסיס של $M_{m,n}(F)$.

נראה שהקבוצה $\{E_{i,j}\}_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ פורשת: תהי $A = (a_{i,j}) \in M_{m,n}(F)$. ברור ש-$A = \sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} a_{i,j} E_{i,j} = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} E_{i,j}$.

נראה שהקבוצה $\{E_{i,j}\}_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ בת"ל: נניח ש-$\sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} E_{i,j} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$. אבל $\sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} E_{i,j} = (a_{i,j})$. לכן לכל $1 \le j \le n, 1 \le i \le m$ $a_{i,j} = 0$.

מצאנו בסיס של $M_{m,n}(F)$ ובו $m \cdot n$ איברים. מכאן $\dim_F M_{m,n}(F) = m \cdot n$. מש"ל ☺

משפט 40: יהי U מרחב וקטורי ממימד n. אזי אם $f : U \to U'$ איזומורפיזם של מרחבים וקטוריים אז $\dim_F U = \dim_F U'$.

הוכחה: f לינארית וחח"ע ולכן לפי טענה (31) $\operatorname{Ker} f = \{0_V\}$ כלומר $\dim_F \operatorname{Ker} f = 0$. f על ולכן $\operatorname{Im} f = U'$. לפי משפט המימדים $\dim_F V = \dim_F \operatorname{Ker} f + \dim_F \operatorname{Im} f$ כלומר $\dim_F U' = \dim_F V$. $n = 0 + \dim_F \operatorname{Im} f$. מש"ל ☺

מסקנה 41: $\dim_F \operatorname{Hom}_F(V,W) = \dim_F V \cdot \dim_F W$

הוכחה: נסמן $\dim_F V = n, \dim_F W = m$. לפי טענה (37) $M_{m,n}(F)$ איזומורפי ל-$\operatorname{Hom}_F(V,W)$. לכן לפי משפט (40) $\dim_F \operatorname{Hom}_F(V,W) = \dim_F M_{m,n}(F)$. לפי משפט (39) $\dim_F M_{m,n}(F) = m \cdot n$ ומכאן המסקנה. מש"ל ☺

ראינו שלסכום של העתקות מתאים סכום של מטריצות ולכפל של העתקה בסקלר מתאים כפל של מטריצה בסקלר. נשאלת אפוא השאלה מהי המטריצה של הרכבה של העתקות?

יהיו V, W, U מרחבים וקטוריים מעל F. יהיו $u_1, \ldots, u_l \in U, w_1, \ldots, w_m \in W, v_1, \ldots, v_n \in V$ בסיסים שלהם. יהיו $f : V \to W, g : W \to U$ העתקות לינאריות. אזי $(g \circ f) : V \to U$ לינארית גם היא. נניח ש-$A_f = (a_{i,j}) \in M_{m,n}(F), A_g = (b_{k,i}) \in M_{l,m}(F), A_{g \circ f} = (c_{k,j}) \in M_{l,n}(F)$ המטריצות המתאימות להעתקות. מה הקשר בין $A_{g \circ f}$ לבין A_g, A_f? נבדוק איך $g \circ f$ פועלת על איברי הבסיס $v_1, \ldots, v_n$. ראשית, לפי הגדרת המטריצות לכל $1 \le j \le n$ מתקיים $f(v_j) = \sum_{i=1}^{m} a_{i,j} w_i$ ולכל $1 \le i \le m$ מתקיים $g(w_i) = \sum_{k=1}^{l} b_{k,i} u_k$.

$$(g \circ f)(v_j) = g(f(v_j)) = g\left(\sum_{i=1}^{m} a_{i,j} w_i\right) = \sum_{i=1}^{m} a_{i,j} g(w_i) = \sum_{i=1}^{m} a_{i,j} \sum_{k=1}^{l} b_{k,i} u_k =$$

$$= \sum_{i=1}^{m} \sum_{k=1}^{l} a_{i,j} b_{k,i} u_k = \sum_{i=1}^{m} \sum_{k=1}^{l} b_{k,i} a_{i,j} u_k = \sum_{k=1}^{l} \sum_{i=1}^{m} b_{k,i} a_{i,j} u_k = \sum_{k=1}^{l} \left(\sum_{i=1}^{m} b_{k,i} a_{i,j} \right) u_k$$

לכן אם $(g \circ f)(v_j) = \sum_{k=1}^{l} c_{k,j} u_k$ אז $c_{k,j} = \sum_{i=1}^{m} b_{k,i} a_{i,j}$. זה הקשר שחיפשנו. על סמך קשר זה מגדירים **כפל של מטריצות**. אם $B = (b_{k,i}) \in M_{l,m}(F)$ ו-$A = (a_{i,j}) \in M_{m,n}(F)$ מגדירים את המכפלה $BA = (c_{k,j}) \in M_{l,n}(F)$ כאשר $c_{k,j} = \sum_{i=1}^{m} b_{k,i} a_{i,j}$. נשים לב שמספר העמודות של המטריצה הראשונה צריך להתאים למספר השורות של המטריצה השנייה.

משפט 42: $A_{gf} = A_g A_f$

הוכחה: פשוט ככה הגדרנו את כפל המטריצות – כדי שתהיה ההתאמה הזאת. ☺

דוגמה:

$$\begin{pmatrix}2&3&1\\1&-1&0\end{pmatrix}\begin{pmatrix}1&2&3&4\\5&6&7&8\\9&10&11&12\end{pmatrix}=$$

$$=\begin{pmatrix}2\cdot1+3\cdot5+1\cdot9&2\cdot2+3\cdot6+1\cdot10&2\cdot3+3\cdot7+1\cdot11&2\cdot4+3\cdot8+1\cdot12\\1\cdot1-1\cdot5+0\cdot9&1\cdot2-1\cdot6+0\cdot10&1\cdot3-1\cdot7+0\cdot11&1\cdot4-1\cdot8+0\cdot12\end{pmatrix}=$$

$$=\begin{pmatrix}26&32&38&44\\-4&-4&-4&-4\end{pmatrix}$$

משפט 43: כפל מטריצות, כאשר הוא מוגדר, הוא אסוציאטיבי.

הוכחה: יהיו $A\in M_{p,q}(F),B\in M_{q,r}(F),C\in M_{r,s}(F)$ מטריצות. נשים לב שגם $(AB)C$ וגם $A(BC)$ מוגדרות מבחינת התאמת הסדרים של המטריצות.

נראה ש- $\left[(AB)C\right]_{h,k}=\left[A(BC)\right]_{h,k}$ ומכאן ינבע המשפט.

$$\left[(AB)C\right]_{h,k}=\sum_{j=1}^{r}[AB]_{h,j}[C]_{j,k}=\sum_{j=1}^{r}\left(\sum_{i=1}^{q}[A]_{h,i}[B]_{i,j}\right)[C]_{j,k}=\sum_{j=1}^{r}\sum_{i=1}^{q}[A]_{h,i}[B]_{i,j}[C]_{j,k}$$

$$\left[A(BC)\right]_{h,k}=\sum_{i=1}^{q}[A]_{h,i}[BC]_{i,k}=\sum_{i=1}^{q}[A]_{h,i}\left(\sum_{j=1}^{r}[B]_{i,j}[C]_{j,k}\right)=\sum_{i=1}^{q}\sum_{j=1}^{r}[A]_{h,i}[B]_{i,j}[C]_{j,k}$$

אבל מאחר שמדובר בסכומים סופיים ניתן להחליף את סדר הסכימה ואז

$$\left[(AB)C\right]_{h,k}=\sum_{j=1}^{r}\sum_{i=1}^{q}[A]_{h,i}[B]_{i,j}[C]_{j,k}=\sum_{i=1}^{q}\sum_{j=1}^{r}[A]_{h,i}[B]_{i,j}[C]_{j,k}=\left[A(BC)\right]_{h,k}$$. מש"ל ☺

טענה 44: כאשר כפל המטריצות מוגדר,

$$P(Q_1+Q_2)=PQ_1+PQ_2$$
$$(P_1+P_2)Q=P_1Q+P_2Q$$

הוכחה: נניח $P_1,P_2,P\in M_{p,q}(F)$ ו- $Q_1,Q_2,Q\in M_{q,r}(F)$. אז הכפל מוגדר. כעת נחשב את המטריצות:

$$\left[P(Q_1+Q_2)\right]_{i,j}=\sum_{k=1}^{q}[P]_{i,k}[Q_1+Q_2]_{k,j}=\sum_{k=1}^{q}\left([P]_{i,k}[Q_1]_{k,j}+[P]_{i,k}[Q_2]_{j,j}\right)=$$

$$=\sum_{k=1}^{q}[P]_{i,k}[Q_1]_{k,j}+\sum_{k=1}^{q}[P]_{i,k}[Q_1]_{k,j}=[PQ_1]_{i,j}+[PQ_2]_{i,j}$$

ובאופן דומה

$$\left[(P_1+P_2)Q\right]_{i,j}=\sum_{k=1}^{q}[P_1+P_2]_{i,k}[Q]_{k,j}=\sum_{k=1}^{q}\left([P_1]_{i,k}[Q]_{k,j}+[P_2]_{i,k}[Q]_{j,j}\right)=$$

$$=\sum_{k=1}^{q}[P_1]_{i,k}[Q]_{k,j}+\sum_{k=1}^{q}[P_2]_{i,k}[Q]_{k,j}=[P_1Q]_{i,j}+[P_2Q]_{i,j}$$

מכאן שמתקיים הדרוש. מש"ל ☺

טענה 45: יהיו $P\in M_{p,q}(F),Q\in M_{q,r}(F)$ ויהי $a\in F$. אזי $(aP)Q=P(aQ)=a(PQ)$.

הוכחה: באופן דומה להוכחת הטנות הקודמות.

יהיו V,W מרחבים וקטוריים מעל F ויהיו $\mathfrak{A}=\{v_1,...,v_n\}\subseteq V,\mathfrak{B}=\{w_1,...,w_m\}\subseteq W$ בסיסים. יהיו $\mathfrak{A}'=\{v_1',...,v_n'\}\subseteq V,\mathfrak{B}'=\{w_1',...,w_m'\}\subseteq W$ זוג בסיסים נוסף. תהי $f\in\mathrm{Hom}_F(V,W)$. נניח ש- $\left[f\right]_{\mathfrak{B}}^{\mathfrak{A}}=A_f=\left(a_{i,j}\right)$ המטריצה המתאימה ל- f לפי זוג הבסיסים הראשון ואילו $\left[f\right]_{\mathfrak{B}'}^{\mathfrak{A}'}=A_f'=\left(a_{i,j}'\right)$ המטריצה לפי זוג הבסיסים השני.

ברור ש- $f=Id_W\circ f\circ Id_V$. הוכחנו שהרכבה של העתקות היא פעולה אסוציאטיבית ושהיא מתאימה לכפל של מטריצות.

לכן $A_f'=PA_fQ$ כאשר $P=\left[Id_W\right]_{\mathfrak{B}'}^{\mathfrak{B}}$ ו- $Q=\left[Id_V\right]_{\mathfrak{A}}^{\mathfrak{A}'}$. P,Q אינן תלויות ב- f אלא רק בבסיסים שבחרנו ולכן הקשר $A_f'=PA_fQ$ נכון לכל העתקה. המטריצות P,Q נקראת **מטריצות מעבר בסיס**.

<u>משפט 46</u>: אם P מטריצת מעבר בסיס מ- $\mathfrak{A}$ ל- $\mathfrak{A}'$ ו- Q מטריצת מעבר בסיס מ- $\mathfrak{A}'$ ל- $\mathfrak{A}$ אזי $PQ = I = QP$.

<u>הוכחה</u>: נסתכל על ההעתקה הלינארית $V \xrightarrow[\mathfrak{A}]{Id_V} V \xrightarrow[\mathfrak{A}']{Id_V} V$: Id_V. ראינו קודם ש- $QP = \left[Id_V\right]_{\mathfrak{A}}^{\mathfrak{A}'}\left[Id_V\right]_{\mathfrak{A}'}^{\mathfrak{A}} = \left[Id_V\right]_{\mathfrak{A}}^{\mathfrak{A}}$. אבל לכל $1 \le j \le n$ $Id_V\left(v_j\right) = v_j = \sum_{i \ne j} 0 \cdot v_i + 1 \cdot v_j$ כאשר $v_j \in \mathfrak{A}$. ולכן

$$QP = \left[Id_V\right]_{\mathfrak{A}}^{\mathfrak{A}} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

באותו אופן, אם נסתכל על $V \xrightarrow[\mathfrak{A}']{Id_V} V \xrightarrow[\mathfrak{A}']{Id_V} V$: Id_V נקבל $PQ = \left[Id_V\right]_{\mathfrak{A}'}^{\mathfrak{A}'} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$. כלומר $PQ = I = QP$. ☺

אם שתי מטריצות A, B מקיימות ש- $AB = I = BA$ אומרים שהן **הופכיות** אחת לשנייה ומסמנים $A = B^{-1}, B = A^{-1}$.

נסתכל במקרה הפרטי שבו $W = V$ כלומר $f : V \to V$. נבחר שני בסיסים $\mathfrak{A}, \mathfrak{A}'$ ל- V ונסתכל על ההעתקה $V \xrightarrow[\mathfrak{A}']{Id_V} V \xrightarrow{f} V \xrightarrow[\mathfrak{A}]{Id_V} V$: f. לפי המשפט שכרגע הוכחנו $Q = P^{-1}$ ואז $A_f{}' = PA_fP^{-1}$.

כעת, נניח שיש לנו מטריצה A_f של העתקה לינארית $f : \underset{v_1,\ldots,v_n}{V} \to \underset{w_1,\ldots,w_m}{W}$ בהתאם לבסיסים כלשהם. איך נדע איך ההעתקה פועלת על וקטור? ראשית נציג את הווקטור כצירוף לינארי של איברי הבסיס של התחום $v = \sum_{j=1}^{n} c_j v_j$. נסתכל על

$C_v = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \in F^n$ - טור המקדמים של v בפיתוח שלו ביחס לבסיס $v_1,\ldots,v_n$. נניח ש- $f\left(v\right) = w = \sum_{i=1}^{m} d_i w_i$ ונסתכל על

$C_{f(v)} = \begin{pmatrix} d_1 \\ \vdots \\ d_m \end{pmatrix} \in F^m$ - טור המקדמים של $f\left(v\right) = w$ בפיתוח שלו לפי הבסיס $w_1,\ldots,w_m$.

<u>משפט 47</u>: $C_{f(v)} = A_f C_v$

<u>הוכחה</u>: יהי $v = \sum_{j=1}^{n} c_j v_j$. וננית $f\left(v\right) = w = \sum_{i=1}^{m} d_i w_i$. אז $C_v = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ ו- $C_{f(v)} = \begin{pmatrix} d_1 \\ \vdots \\ d_m \end{pmatrix}$. אבל

$$f\left(v\right) = f\left(\sum_{j=1}^{n} c_j v_j\right) = \sum_{j=1}^{n} c_j f\left(v_j\right) = \sum_{j=1}^{n} c_j \sum_{i=1}^{m} a_{i,j} w_i = \sum_{i=1}^{n}\left(\sum_{j=1}^{n} c_j a_{i,j}\right) w_i$$

כלומר $d_i = \sum_{j=1}^{n} a_{i,j} c_j$.

אז לפי הגדרה של כפל מטריצות נקבל:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{n} a_{1,j} c_j \\ \vdots \\ \sum_{j=1}^{n} a_{n,j} c_j \end{pmatrix} = \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}$$

כלומר $C_{f(v)} = A_f C_v$. מש"ל ☺

5. מערכות משוואות לינאריות

נזכור שכשרק התחלנו לדבר על מרחבים וקטוריים דיברנו על דוגמה פונדמנטלית ביותר - F^n. אז היה זה מרחב וקטורי של שורות של איברים של השדה F. כעת נעשה העמסה לסימון הזה ומעתה F^n יסמן טורים בגובה n. אז בעצם $M_{n,1}(F)$ זה כמו F^n.

בהינתן מטריצה $A \in M_{m,n}(F)$ נגדיר העתקה $f_A : F^n \to F^m$ שפועלת באופן הבא: לכל $c \in F^n$ $f_A(c) = Ac$. האם זו העתקה לינארית? ברור שכן, אחרת לא היינו מדברים עליה בכלל.
יהיו $c', c'' \in F^n$ ויהי $a \in F$. לפי חוק הפילוג שהוכחנו קודם

$$f_A(c'+c'') = A(c'+c'') = Ac'+Ac'' = f_A(c') + f_A(c'').$$

ולפי טענה אחרת שלא הוכחנו אבל ההוכחה שלה זהה להוכחה של חוק הפילוג

$$f_A(ac') = A(ac') = a(Ac') = af_A(c')$$

אז f_A משמרת חיבור וכפל בסקלר ולכן היא העתקה לינארית. אם היא העתקה לינארית אפשר לדבר על המטריצה שלה.

<u>טענה 48</u>: המטריצה של f_A ביחס לבסיסים הסטנדרטיים של F^m, F^n : $e_1,...,e_n \in F^n$, $d_1,...,d_m \in F^m$ ‡‡‡‡ היא A :
<u>הוכחה</u>: פשוט נחשב איך ההעתקה פועלת על איברי הבסיס של F^n :

$$f_A(e_1) = Ae_1 = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1,1} \\ \vdots \\ a_{m,1} \end{pmatrix} = a_{1,1} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + ... + a_{m,1} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

$$\vdots$$

$$f_A(e_n) = Ae_n = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{m,n} \end{pmatrix} = a_{1,n} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + ... + a_{m,n} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

או באופן כללי $f_A(e_j) = Ae_j = \sum_{i=1}^{m} a_{i,j} d_i$ עבור $1 \le j \le n$. כעת נרשום את המקדמים במטריצה ונקבל

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} = [f_A]_{\{d_i\}}^{\{e_i\}}.$$ ראו איזה פלא! מש"ל. ☺

נסמן ב- I_k את המטריצה $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in M_k(F)$.

<u>משפט 49</u>: תהי $A \in M_{m,n}(F)$ ותהי $B \in M_{n,m}(F)$ כך ש- $AB = I_m, BA = I_n$. אזי $m = n$.
<u>הוכחה</u>: נסתכל על ההעתקות הלינאריות $f_A : F^n \to F^m$ ו- $f_B : F^m \to F^n$. כמו כן שים לב שמתקיים

$$Id_{F^m} : \underset{d}{F^m} \xrightarrow{f_B} \underset{Bd}{F^n} \xrightarrow{f_A} \underset{\substack{A(Bd)= \\ =(AB)d= \\ =I_m d=d}}{F^m}$$ ו- $$Id_{F^n} : \underset{c}{F^n} \xrightarrow{f_A} \underset{AC}{F^m} \xrightarrow{f_B} \underset{\substack{B(Ac)= \\ =(BA)c= \\ =I_n c=c}}{F^n}$$

כלומר f_A, f_B הופכיות זו לזו. אזי הן איזומופרפיזמים של מרחבים וקטוריים. ז"א F^n איזומורפי ל- F^m. כבר ראינו שאם שני מרחבים נוצרים סופית איזומורפיים אז יש להם אותו מימד. ולכן

$$n = \dim_F F^n = \dim_F F^m = m$$

שזה מה שרצינו. ☺
המסקנה מהמשפט הזה היא שרק למטריצות ריבועיות יכולה להיות מטריצה הופכית.

---

‡‡‡‡ d זה בשביל Dina וחשוב מאוד לזכור את זה אחרת יורדות נקודות במבחן... ☺

עכשיו נשתמש בכל מה שאנחנו יודעים כדי לפתור מערכות של משוואות לינאריות. תכינו את עצמכם, זה הולך להיות מרתק. או שלא...

נניח שיש לנו מערכת של משוואות לינאריות - m משוואת ב- n נעלמים:

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + ... + a_{1,n}x_n = b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + ... + a_{2,n}x_n = b_2 \\ \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + ... + a_{m,n}x_n = b_m \end{cases}$$

הנעלמים הם $x_1,...,x_n$ והמקדמים הם $a_{i,j} \in F$ באיזשהו שדה. האיברים החופשיים הם $b_1,...,b_m \in F$. כשאנחנו אומרים שמצאנו פיתרון למערכת משוואת, למה אנחנו מתכוונים? ובכן האיברים $\alpha_1,...,\alpha_n \in F$ הם פיתרון של מערכת המשוואות למעלה אם כאשר נרשום אותם במקום הנעלמים $x_1,...,x_n$ בהתאמה נקבל שכל השוויונים הם נכונים. כלומר אכן מתקיים:

$$\begin{gathered} a_{1,1}\alpha_1 + a_{1,2}\alpha_2 + ... + a_{1,n}\alpha_n = b_1 \\ a_{2,1}\alpha_1 + a_{2,2}\alpha_2 + ... + a_{2,n}\alpha_n = b_2 \\ \vdots \\ a_{m,1}\alpha_1 + a_{m,2}\alpha_2 + ... + a_{m,n}\alpha_n = b_m \end{gathered}$$

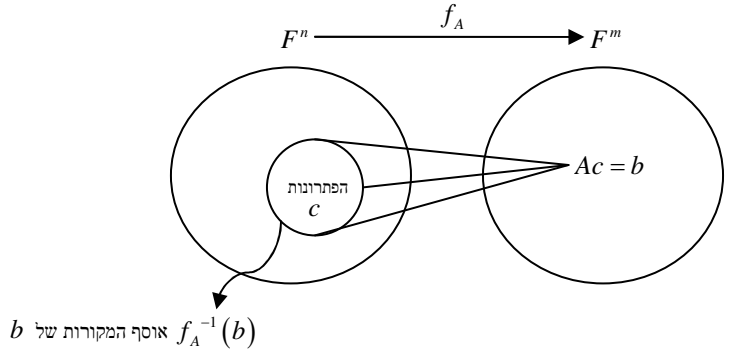
באופן טבעי נשאלות כל מיני שאלות: האם תמיד יש פיתרון למערכת משוואות? אם יש, האם הוא יחיד? האם יש דרך לדעת אם קיים פיתרון מבלי ממש למצוא אותו? ועוד...
לכל אלה ננסה לתת תשובה במהלך הדיון הבא.

את מערכת המשוואת אפשר לרשום בצורת מטריציונית באופן הבא:

$$\underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}}_{\text{מטריצת המקדמים}} \underbrace{\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}}_{\substack{\text{עמודת} \\ \text{הנעלמים}}} = \underbrace{\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}}_{\substack{\text{עמודת} \\ \text{האיברים} \\ \text{החופשיים}}}$$

או בקיצור $Ax = b$ כאשר A מטריצת המקדמים, b עמודת האיברים החופשיים ו- x עמודת הנעלמים.
לפני שאנחנו ונכנסים לנושא במלואו נדון במקרה פרטי שבו $m = n$ ולמטריצה A יש מטריצה הופכית A^{-1}. במקרה זה אם נכפיל משמאל את שני האגפים של $Ax = b$ ב- A^{-1} נקבל $x = Ix = \left(A^{-1}A\right)x = A^{-1}\left(Ax\right) = A^{-1}b$. כלומר קיים פיתרון למערכת המשוואת ויתר על כן הוא יחיד!!

נחזור כעת למקרה הכללי. נניח יש לנו מערכת משוואות $Ax = b$ כאשר $A \in M_{m,n}\left(F\right), x \in F^n, b \in F^m$.
$c \in F^n$ הוא פיתרון אם מתקיים $Ac = b$. אז מציאת פיתרון של המערכת הזו בעצם שקולה למציאת מקור של b תחת ההעתקה הלינאריות f_A שכזכור הייתה מוגדרת ע"י $f_A\left(x\right) = Ax$.



ברור גם שלמערכת $Ax = b$ יש פיתרון אמ"מ $b \in \mathrm{Im}\left(f_A\right)$ שהרי אחרת לא נוכל למצוא x -ים כך ש- $Ax = b$.
ראינו שהעתקה לינארית f היא חח"ע אמ"מ $\mathrm{Ker}\, f = \{0\}$. זה אומר שלכל איבר בתמונה יש מקור יחיד. אז מפה נובע שלמערת $Ax = b$ יש פיתרון יחיד אמ"מ יש פיתרון וגם $\mathrm{Ker}\, f_A = \{0\}$.

משפט 50: אם $f:V\to W$ העתקה לינארית ו- $f(c)=b$ אז $f^{-1}(b)=c+\operatorname{Ker} f$

הוכחה: כרגיל כאשר יש להוכיח שיוויון בין שתי קבוצות נוכיח הכלה בשני הכיוונים:

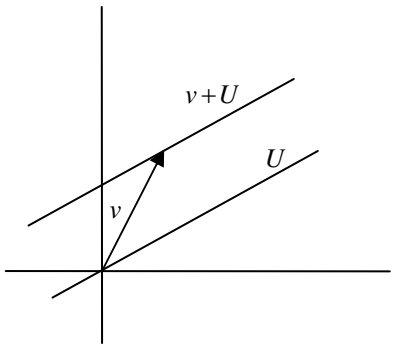
$(\subset)$ יהי $a\in f^{-1}(b)$. אזי $f(a)=b$. נרצה להציג את a בצורה $c+c'$ כאשר $c'\in\operatorname{Ker} f$. ברור ש- $a=c+(a-c)$. נראה ש- $a-c\in\operatorname{Ker} f$: $f(a-c)=f(a)-f(c)=b-b=0_W$. לכן $a\in c+\operatorname{Ker} f$.

$(\supset)$ יהי $c'\in\operatorname{Ker} f$. אזי $f(c+c')=f(c)+f(c')=b+0_W=b$. כלומר $c+c'\in f^{-1}(b)$. מש"ל ☺

אם נשתמש במשפט הזה כדי לנתח את המצב שלנו נראה שאם מערכת המשוואת שלנו היא $Ax=b$ אז $f_A^{-1}(b)=c+\operatorname{Ker} f_A$ כאשר c הוא פיתרון כלשהו של המערכת. זוהי טענה מאוד חשובה משום שהיא אומרת בעצם שאם אנחנו יודעים פיתרון יחיד כלשהו של המערכת אז אנחנו יכולים לבטא באמצעותו את **כל** הפתרונות. זה לא עוזר לנו למצוא את הפיתרון הזה. אבל אם בטעות מצאנו את הפיתרון אז מצאנו את כולם.
נשים לב רק, שאם ההעתקה f_A היא חח"ע, כלומר $\operatorname{Ker} f_A=\{0\}$ אז הפיתרון הוא יחיד!

הגדרה: יהי $U\subset V$ תת מרחב. ויהי $v\in V$. הקבוצה $v+U=\{v+u:u\in U\}$ נקראת **ישרייה**. U נקרא **תת המרחב המכוון** של הישרייה.

דוגמה: $V=\mathbb{R}^2$ וניקח תת מרחב שהוא איזה ישר העובר דרך הראשית. ניקח $v\in V$. אז הישרייה $v+U$ היא ישר מקביל ל- U שעובר דרך v.



אזהרה: $v+U$ בכלל לא חייב להיות תת מרחב.

טענה 51: $v+U$ הוא תת מרחב של V אמ"מ $v\in U$ ואז $v+U=U$.

הוכחה:

$(\Leftarrow)$ נניח ש- $v+U$ תת מרחב של V ונראה ש- $v\in U$. נניח בשלילה כי $v\notin U$. $v+U$ תת מרחב ולכן $0_V\in v+U$. כלומר קיים $u\in U$ כך ש- $0_V=v+u$. אבל חייב להתקיים אז $u=-v$. אבל מכאן ש- $v\in U$. בסתירה להנחה. לכן $v\in U$.

$(\Rightarrow)$ נניח כי $v\in U$ ונראה כי $v+U=U$. ברור ש- $v+U\subset U$ כי U סגור לחיבור. מצד שני, יהי $u\in U$. ברור ש- $u=v+(u-v)$. אבל מאחר ש- $v\in U$ גם $-v\in U$ ולכן $u-v\in U$. לכן $v+U\supset U$. כלומר $v+U=U$.
בפרט $v+U$ תת מרחב. מש"ל ☺

תחת הגדרה זו ברור שאוסף כל הפתרונות של מערכת משוואות לינארית הוא ישרייה שהמרחב המכוון שלה הוא הגרעין של ההעתקה שנקבעת ע"י המטריצה של המקדמים של המערכת.

טענה 52: יהיו $U_1,U_2\subset V$ תתי מרחבים ו- $v_1,v_2\in V$ כך ש- $v_1+U_1=v_2+U_2$. אזי $U_1=U_2$.
משמעות: הטענה הזאת בעצם אומרת שהמימד המכוון של ישרייה הוא יחיד.
הוכחה: משום ש- $0_V\in U_1$ נקבל $v_1=v_1+0_V\in v_1+U_1=v_2+U_2$. כלומר קיים $u_2\in U_2$ כך ש- $v_1=v_2+u_2$. ולכן $v_2-v_1=-u_2\in U_2$. מהשוויון $v_1+U_1=v_2+U_2$ נובע

$$U_1=(-v_1)+(v_1+U_1)=(-v_1)+(v_2+U_2)=(v_2-v_1)+U_2=(-u_2)+U_2\underset{u_2\in U_2}{=}U_2$$ ☺

הגדרה: נאמר שהמימד של הישרייה $v+U$ הוא $\dim_F(v+U)=\dim_F U$. בגלל הטענה הקודמת המימד מוגדר היטב.

אם ישריית הפתרונות של $Ax=b$ היא $c+\operatorname{Ker} f_A$ נוכל לכתוב $\dim_F(c+\operatorname{Ker} f_A)=\dim_F\operatorname{Ker} f_A$. כמו כן לפי משפט המימדים $n=\dim_F F^n=\dim_F\operatorname{Im} f_A+\dim_F\operatorname{Ker} f_A$ לכן $\dim_F(c+\operatorname{Ker} f_A)=n-\dim_F\operatorname{Im} f$.

נגדיר כמה סימונים חדשים. תהי $A=\left(a_{i,j}\right)\in M_{m,n}\left(F\right)$. נסמן:

$$a_{1*}=\begin{pmatrix}a_{1,1} & \dots & a_{1,n}\end{pmatrix}$$
$$\vdots \qquad \text{השורות של } A:$$
$$a_{m*}=\begin{pmatrix}a_{m,1} & \dots & a_{m,n}\end{pmatrix}$$
$$a_{*1}=\begin{pmatrix}a_{1,1}\\ \vdots \\ a_{m,1}\end{pmatrix},...,a_{*n}=\begin{pmatrix}a_{1,n}\\ \vdots \\ a_{m,n}\end{pmatrix} \qquad \text{העמודות של } A:$$

<u>משפט 53</u>: אם $f_A:F^n\to F^m$ מוגדרת ע"י $f_A\left(c\right)=Ac$ אז $\operatorname{Im}f_A=\operatorname{Sp}\left(a_{*1},...,a_{*n}\right)\subset F^m$

<u>הערה</u>: $\dim_F \operatorname{Sp}\left(a_{*1},...,a_{*n}\right)$ הוא המספר המקסימלי של עמודות בלתי תלויות של המטריצה A. זה נובע מהמשפט שהוכחנו שאם $V=Sp\left(u_1,...,u_m\right)$. אזי הקבוצה $\left\{u_i:1\le i\le m,u_i\notin Sp\left(u_1,...,u_{i-1}\right)\right\}$ היא בסיס ל- V.

<u>הוכחה</u>: הוכחנו כבר שאם $f:V\to W$ העתקה לינארית ו- $V=\operatorname{Sp}\left(v_1,...,v_n\right)$ אז $\operatorname{Im}f=\operatorname{Sp}\left(f\left(v_1\right),...,f\left(v_n\right)\right)$.

נסתכל על העמדודות הסטנדרטיות ב- F^n. ברור שהן פורשות אותו. נבדוק איך f_A פועלת עליהן:

$$f_A\begin{pmatrix}1\\0\\ \vdots \\0\end{pmatrix}=A\begin{pmatrix}1\\0\\ \vdots \\0\end{pmatrix}=\begin{pmatrix}a_{1,1} & \dots & a_{1,n}\\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n}\end{pmatrix}\begin{pmatrix}1\\0\\ \vdots \\0\end{pmatrix}=\begin{pmatrix}a_{1,1}\\ \vdots \\ a_{m,1}\end{pmatrix}=a_{*1}$$
$$\vdots$$
$$f_A\begin{pmatrix}0\\ \vdots \\0\\1\end{pmatrix}=A\begin{pmatrix}0\\ \vdots \\0\\1\end{pmatrix}=\begin{pmatrix}a_{1,1} & \dots & a_{1,n}\\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n}\end{pmatrix}\begin{pmatrix}0\\ \vdots \\0\\1\end{pmatrix}=\begin{pmatrix}a_{1,n}\\ \vdots \\ a_{m,n}\end{pmatrix}=a_{*n}$$

לכן $\operatorname{Im}f_A=\operatorname{Sp}\left(f_A\begin{pmatrix}1\\0\\ \vdots \\0\end{pmatrix},...,f_A\begin{pmatrix}0\\ \vdots \\0\\1\end{pmatrix}\right)=\operatorname{Sp}\left(a_{*1},...,a_{*n}\right)$. מש"ל ☺

<u>הגדרה</u>: הדרגה של מטריצה $A\in M_{m,n}\left(F\right)$ לפי העמודות היא $\operatorname{rank}_c A=\dim_F Sp\left(a_{*1},...,a_{*n}\right)$

הדרגה של מטריצה $A\in M_{m,n}\left(F\right)$ לפי השורות היא $\operatorname{rank}_r A=\dim_F Sp\left(a_{1*},...,a_{m*}\right)$

<u>משפט 54</u>: לכל מטריצה $C\in M_{n,p}\left(F\right)$ $\operatorname{rank}_c C=\operatorname{rank}_r C$

<u>הוכחה</u>: תהי $B=\left(b_{i,j}\right)\in M_{n,p}\left(F\right)$. אזי מוגדרת המכפלה $AB\in M_{m,p}\left(F\right)$. נרשום אותה באופן מפורש:

$$AB=\begin{pmatrix}a_{1,1} & \dots & a_{1,n}\\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n}\end{pmatrix}\begin{pmatrix}b_{1,1} & \dots & b_{1,p}\\ \vdots & \ddots & \vdots \\ b_{n,1} & \cdots & b_{n,p}\end{pmatrix}=$$
$$=\begin{pmatrix}a_{1,1}b_{1,1}+...+a_{1,n}b_{n,1} & \dots & a_{1,1}b_{1,p}+...+a_{1,n}b_{n,p}\\ \vdots & \ddots & \vdots \\ a_{m,1}b_{1,1}+...+a_{m,n}b_{n,1} & \cdots & a_{m,1}b_{1,p}+...+a_{m,n}b_{n,p}\end{pmatrix}=\begin{pmatrix}a_{1,1}b_{1*}+...+a_{1,n}b_{n*}\\ \vdots \\ a_{m,1}b_{1*}+...+a_{m,n}b_{n*}\end{pmatrix}$$

כלומר השורות של AB הן צירופים לינאריים של השורות של B עם מקדמים מ- A.
אבל אפשר גם לרשום

$$AB=\begin{pmatrix}a_{1,1}&\cdots&a_{1,n}\\ \vdots&\ddots&\vdots\\ a_{m,1}&\cdots&a_{m,n}\end{pmatrix}\begin{pmatrix}b_{1,1}&\cdots&b_{1,p}\\ \vdots&\ddots&\vdots\\ b_{n,1}&\cdots&b_{n,p}\end{pmatrix}=\begin{pmatrix}a_{1,1}b_{1,1}+...+a_{1,n}b_{n,1}&\cdots&a_{1,1}b_{1,p}+...+a_{1,n}b_{n,p}\\ \vdots&\ddots&\vdots\\ a_{m,1}b_{1,1}+...+a_{m,n}b_{n,1}&\cdots&a_{m,1}b_{1,p}+...+a_{m,n}b_{n,p}\end{pmatrix}=$$

$$=\begin{pmatrix}b_{1,1}a_{*1}+...+b_{n,1}a_{*n}&\cdots&b_{1,p}a_{*1}+...+b_{n,p}a_{*n}\end{pmatrix}$$

כלומר העמודות של AB הן צירופים לינאריים של העמודות של A עם מקדמים מ- B.

נסמן $C=AB$. אזי

$$\mathrm{Sp}\left(c_{*1},...,c_{*p}\right)\subset\mathrm{Sp}\left(a_{*1},...,a_{*n}\right)$$

$$\mathrm{Sp}\left(c_{1^*},...,c_{m^*}\right)\subset\mathrm{Sp}\left(b_{1^*},...,b_{n^*}\right)$$

תהי $C\in M_{n,p}\left(F\right)$. נראה ש- $\dim_F\mathrm{Sp}\left(c_{*1},...,c_{*p}\right)=\dim_F\mathrm{Sp}\left(c_{1^*},...,c_{m^*}\right)$. נניח ש- $\dim_F\mathrm{Sp}\left(c_{1^*},...,c_{m^*}\right)=n$.

נבנה פירוק של C למכפלה AB כאשר $A\in M_{m,n}\left(F\right)$ ו- $B\in M_{n,p}\left(F\right)$.

לפי ההנחה ל- $\mathrm{Sp}\left(c_{1^*},...,c_{m^*}\right)$ יש בסיס ובו n וקטורים, כלומר n שורות באורך p. נסמן

$$\begin{pmatrix}b_{1,1}&\cdots&b_{1,p}\end{pmatrix}=b_{1^*}$$

$$\vdots$$

$$\begin{pmatrix}b_{n,1}&\cdots&b_{n,p}\end{pmatrix}=b_{n^*}$$

נגדיר $B=\left(b_{i,j}\right)\in M_{n,p}\left(F\right)$. בגלל שזה בסיס $\mathrm{Sp}\left(c_{1^*},...,c_{m^*}\right)=\mathrm{Sp}\left(b_{1^*},...,b_{n^*}\right)$. כמו כן ניתן להציג את $c_{1^*},...,c_{m^*}$ כצירוף לינארי של איברי הבסיס:

$$c_{1^*}=a_{1,1}b_{1^*}+...+a_{1,n}b_{n^*}$$

$$\vdots$$

$$c_{m^*}=a_{m,1}b_{1^*}+...+a_{m,n}b_{n^*}$$

נגדיר $A=\left(a_{i,j}\right)\in M_{m,n}\left(F\right)$. ברור ש- $C=AB$. כעת לפי מה שעשינו קודם $\mathrm{Sp}\left(c_{*1},...,c_{*p}\right)\subset\mathrm{Sp}\left(a_{*1},...,a_{*n}\right)$.

ואז $\mathrm{rank}_c\,C=\dim_F\mathrm{Sp}\left(c_{*1},...,c_{*p}\right)\le\dim_F\mathrm{Sp}\left(a_{1^*},...,a_{n^*}\right)\le n=\mathrm{rank}_r\,C$!!

כעת נניח ש- $\dim_F\mathrm{Sp}\left(c_{*1},...,c_{*p}\right)=n$. אזי נסתכל על הבסיס של $\mathrm{Sp}\left(c_{*1},...,c_{*p}\right)$:

$$a_{*1}=\begin{pmatrix}a_{1,1}\\ \vdots\\ a_{m,1}\end{pmatrix},...,a_{*n}=\begin{pmatrix}a_{1,n}\\ \vdots\\ a_{m,n}\end{pmatrix}$$

נגדיר $A=\left(a_{i,j}\right)\in M_{m,n}\left(F\right)$.

נבטא את $c_{*1},...,c_{*p}$ ע"י איברי הבסיס:

$$c_{*1}=b_{1,1}a_{*1}+...+b_{n,1}a_{*n}$$

$$\vdots$$

$$c_{*p}=b_{1,p}a_{*1}+...+b_{n,p}a_{*n}$$

ונגדיר $B=\left(b_{i,j}\right)\in M_{n,p}\left(F\right)$. אזי $C=AB$ וכמו קודם

$$\mathrm{rank}_r\,C=\dim_F\mathrm{Sp}\left(c_{1^*},...,c_{m^*}\right)\le\dim_F\mathrm{Sp}\left(b_{1^*},...,b_{n^*}\right)\le n=\mathrm{rank}_c\,C\ \text{!!}$$

מכאן ש- $\mathrm{rank}_r\,C=\mathrm{rank}_c\,C$. מש"ל ☺

נשים לב לשתי תכונות מעניינות. אם A מייצגת טרנספורמציה לינארית חח"ע אז $\mathrm{rank}_c\,A=n$, כלומר דרגת העמודות היא המקסימלית שיכולה להיות. ואם A מייצגת טרנספורמציה לינארית על אז $\mathrm{rank}_r\,A=m$, כלומר דרגת השורות היא המקסימלית שיכולה להיות. אבל דרגת השורות שווה לדרגת העמודות. לכן מפה נובע שאם מטריצה היא הפיכה (כלומר ההעתקה שהיא מייצגת היא גם חח"ע וגם על) אז היא חייבת להיות ריבועית!

נגדיר $\mathrm{rank}\,A=\mathrm{rank}_c\,A=\mathrm{rank}_r\,A$

למערכת המשוואות $Ax=b$ קיים פיתרון אמ"מ $b\in\mathrm{Im}\,f_A$. אמרנו ש- $\mathrm{Im}\,f_A=\mathrm{sp}\left(a_{*1},...,a_{*n}\right)$. אז למערכת יש פיתרון אמ"מ $b\in\mathrm{sp}\left(a_{*1},...,a_{*n}\right)$. ואפשר לנסח זאת גם כך: יש פיתרון אמ"מ $\mathrm{sp}\left(a_{*1},...,a_{*n},b\right)=\mathrm{sp}\left(a_{*1},...,a_{*n}\right)$.

נגדיר את מטריצת המקדמים המורחבת של המערכת: $A^*=\left(a_{*1},...,a_{*n},b\right)=\left(A\ b\right)$. אז נוכל לסכם את מה שהגענו אליו:

משפט 55: למערכת המשוואת $Ax=b$ יש פיתרון אמ"מ $\operatorname{rank} A^* = \operatorname{rank} A$.

אז עשכיו אנחנו יודעים מתי יש פיתרון למערכת משוואות. אבל איך מוצאים אותו? באופן כללי השיטה די דומה למה שלמדנו בתיכון על צמצום משתנים. אנחנו נפתח את זה בצורה פורמלית יותר.

הגדרה: שתי מערכות משוואות $Ax=b$ ו- $A'x=b'$ נקראות **שקולות** אם יש להן בדיוק אותם הפיתרונות.

משפט 56: תהי C מטריצה הפיכה מסדר $m\times m$. אזי המערכת $Ax=b$ שקולה למערכת $(CA)x=Cb$.

הוכחה: תהי $B=C^{-1}$. אם $Ac=b$ אזי $(CA)c=C(Ac)=Cb$. להפך אם $(CA)c=Cb$ אזי

$Ac=(BC)(Ac)=B((CA)c)=B(Cb)=(BC)b=b$. ☺

המוטיבציה שלנו תהיה להפוך את $Ax=b$ למערכת משוואות שקולה לה שקל לנו יותר לפתור. זה ייעשה ע"י סדרה של הכפלות במטריצות הפיכות.

נגדיר כמה מטריצות:

לכל $0\neq a\in F$ נגדיר $D_i(a)=\begin{pmatrix}0&\cdots&0\\ \vdots&a&\vdots\\ 0&\cdots&0\end{pmatrix}$ כך ש- $\left[D_i(a)\right]_{i,i}=a$ ובכל מקום אחר 0.

לכל $a\in F$ עבור $i\neq j$ נסמן $E_{i,j}(a)=\begin{pmatrix}1&&&0\\ &\ddots&a&\\ &&\ddots&\\ 0&&&1\end{pmatrix}$ כך ש- $\left[E_{ij}(a)\right]_{i,j}=a$, $\left[E_{ij}(a)\right]_{k,k}=1$ ובכל מקום אחר 0.

עבור $i\neq j$ נסמן $P_{i,j}=\begin{pmatrix}1&&&&0\\ &0&&1&\\ &&1&&\\ &1&&0&\\ 0&&&&1\end{pmatrix}$ כלומר מטריצת היחידה שבה הוחלפו במקומן שורות i ו- j.

קל לראות שלכל מטריצה A מתקיים:

$$D_i(a)A=\begin{pmatrix}a_{1*}\\ \vdots\\ a\cdot a_{i*}\\ \vdots\\ a_{m*}\end{pmatrix}\qquad E_{i,j}(a)A=\begin{pmatrix}a_{1*}\\ \vdots\\ a_{i*}+a\cdot a_{j*}\\ \vdots\\ a_{m*}\end{pmatrix}\qquad P_{i,j}A=\begin{pmatrix}a_{1*}\\ \vdots\\ a_{j*}\\ \vdots\\ a_{i*}\\ \vdots\\ a_{m*}\end{pmatrix}$$

כמו כן מאותה הסיבה ברור ש

$$D_i(a)^{-1}=D_i\left(a^{-1}\right)$$
$$E_{i,j}(a)^{-1}=E_{i,j}(-a)$$
$$P_{i,j}{}^{-1}=P_{i,j}$$

הגדרה: מטריצה D נקראת מדורגת כאשר צורתה כלהלן:

1. יש בה עמודות סטנדרטיות לפי הסדר שלהן.
2. ניתן להעביר קו מדרגות כאשר כל עמודה סטנדרטית קובעת מדרגה.
3. מתחת לקו המדרגות יש רק אפסים.

<u>משפט 57</u>: לכל מטריצה $A\in M_{m,n}\left(F\right)$ קיימת מטריצה הפיכה $B\in M_m\left(F\right)$ כך ש- BA היא מדורגת.

<u>הוכחה</u>: ההוכחה נעשית באינדוקציה על n ובעצם מה שקורה שם זה שכופלים את המטריצה בכל שלב באחת מהמטריצות שהגדרנו למעלה וככה לאט לאט מאפסים את כל מה שצריך. בגלל שכל המטריצות האלה הן הפיכות אז גם המכפלה שלהן הפיכה.

שלב ראשון: התבונן בעמודה הראשונה של המטריצה A אשר אינה כולה אפסים. לשם נוחיות נניח כי זו העמודה הראשונה. הבא איבר שונה מאפס לראש העמודה ע"י החלפת שורות (מטריצה $P_{i,j}$) וכפול לאחר מכן את השורה הראשונה בהפכי של איבר זה (מטריצה D_i). ע"י כך תתקבל מטריצה חדשה $B=\left(b_{i,j}\right)$ אשר בה $b_{1,1}=1$. כעת אפס כל איבר $b_{i,1}\neq 0$ (פרט ל- $b_{1,1}$) שעוד נותר בעמודה הראשונה ע"י הוספת השורה הראשונה כפולה ב- $-b_{i,1}$ לשורה ה- i (מטריצה $E_{i,j}$). ע"י כך תתקבל מטריצה חדשה מהצורה:

$$\begin{pmatrix} c_{2,2} & \cdots & c_{2,n} \\ \vdots & \ddots & \vdots \\ c_{m,2} & \cdots & c_{m,n} \end{pmatrix}=C\in M_{m-1,n-1}\left(F\right) \text{ כאשר } C'=\begin{pmatrix} 1 & c_{1,2} & \cdots & c_{1,n} \\ 0 & c_{2,2} & \cdots & c_{2,n} \\ \vdots & & & \\ 0 & c_{m,2} & \cdots & c_{m,n} \end{pmatrix}=\begin{pmatrix} 1 & c_{1,2} & \cdots & c_{1,n} \\ 0 & & & \\ \vdots & & C & \\ 0 & & & \end{pmatrix}$$

נשים לב שכל הפעולות שבוצעו הן פעולות אלמנטריות על שורות המטריצה.

שלב שני: המשך בפעולות אלמנטריות על השורות $2,...,m$ של C' על מנת לאפס איברים בעמודתה השנייה. היות והאפסים בעמודה הראשונה של C' לא "יתקלקלו" ע"י פעולות אלה, ניתן להעלם מהם, ולבצע את הפעולות רק על שורות המטריצה החלקית C. חזור על התהליך של השלב הראשון לגבי העמודה הראשונה של C.

השלבים הבאים: ממשיכים כבשלבים הקודמים, כאשר בשלב ה- $k+1$ מבצעים פעולות אלמנטריות על $n-k$ השורות האחרונות בלבד, עד שמגיעים למספר r שעבורו $n-r$ השורות האחרונות מכילות אפסים בלבד (ייתכן גם $r=n$ ואז אין שורות שמכילות אפסים בלבד). נתאר את המטריצה $D=D_{i,j}$ שהתקבלה בשלב זה: עבור $i=1,...,r$ קיימים מספרים טבעיים $1\le t_1<...<t_r\le n$ כך ש- $d_{i,1}=...=d_{i,t_i-1}=0,d_{i,t_i}=1$ ואילו $n-r$ השורות האחרונות מכילות אפסים בלבד:

$$D=\begin{pmatrix} 0 & \cdots & 0 & 1 & * & & & & * \\ 0 & & & 0 & 1 & * & & & * \\ \vdots & & & & & & & & \\ 0 & & & & & 0 & 1 & * & * \\ 0 & & & & & & & & 0 \\ \vdots & & & & & & & & \\ 0 & & & & & & & & 0 \end{pmatrix}\begin{matrix} \\ \\ \\ \leftarrow \text{row } r \\ \\ \\ \end{matrix}$$

$$\begin{matrix} & & & t_1 & t_2 & & & t_r & \\ & & & \downarrow & \downarrow & & & \downarrow & \end{matrix}$$

וזואת צורה מדורגת. מש"ל ☺

אז למה זה עזר לנו? מאוד קל לפתור מערכת משוואות שרשומה בצורה מדורגת וחוץ מזה זה גם נותן לנו מידע לגבי מספר הפתרונות.

נסתכל במטריצת המקדמים המורחבת של מערכת המשוואת $Ax=b$ - $A^*=\left(A\ b\right)$. קיימת B כך ש- $B*A^*$ מדורגת. כעת, אם העמודה האחרונה היא סטנדרטית אז אין פיתרון למערכת המשוואת כי אז בעצם נקבל שאחת מהמשוואות היא מהצורה $0\cdot x_1+...+0\cdot x_n=1$ וזה כמובן בלתי אפשרי.

אם העמודה האחרונה אינה עמודה סטנדרטית אזי יש פתרונות. נניח ש- $\left\{j_k\right\}_{k=1}^r$ הן העמודות ב- $B*A^*$ שבהן יש עמודה סטנדרטית. נחלק את המשתנים לשתי קבוצות. הראשונה, $\left\{x_{j_1},...,x_{j_r}\right\}$ והשנייה $\left\{x_1,...,x_n\right\}\setminus\left\{x_{j_1},...,x_{j_r}\right\}$. כל נעלם מהקבוצ הראשונה מופיע במערכת המשוואות פעם אחת בלבד. לכן נוכל לרשום:

$$\begin{aligned} x_{j_1}&=c_1-(\ )\Leftarrow x_{j_1}+\left(\text{variables from second set}\right)=c_1 \\ x_{j_2}&=c_2-(\ )\Leftarrow x_{j_2}+\left(\text{variables from second set}\right)=c_2 \\ &\vdots \\ x_{j_r}&=c_r-(\ )\Leftarrow x_{j_r}+\left(\text{variables from second set}\right)=c_r \end{aligned}$$

לנעלמים מהקבוצה השנייה ניתן לתת ערכים שרירותיים והנעלמים מהקבוצה הראשונה נקבעים באופן חד ערכי ע"י ערכים אלה.

משפט 58: אם $D_1 = B_1 A, D_2 = B_2 A$ כאשר B_1, B_2 הפיכות ו- D_1, D_2 מדורגות אז $D_1 = D_2$.
הוכחה: גם כאן צריך לרשום מלא מטריצות ולא ממש בא לי.

המשפט הזה חשוב כי הוא אומר שהצורה המדורגת של מטריצה היא יחידה. לכן זה לא משנה בפועל באיזה סדר פעולות ננקוט, תמיד נגיע לאותה התוצאה! אם זה לא היה כך, היינו בצרות...

בזאת נגמר החומר למבחן. בהצלחה לכולם.