① 31.10.05

המרצה: אליהו ריפס

זה קורס באלגברה לינארית. מה זה אלגברה ומה היא לינארית?
במהלך הקורס ננסה לענות על השאלות האלה.
בעצם פיתרון של משוואות מביא לאלגברה ואם הן לינאריות אז האלגברה לינארית. נקודת המוצא של הקורס היא פתרון מע' של משוואות לינאריות. בדרך יש כל מיני נושאים תיאורטיים שיש להתייחס אליהם וזה מה שמפתח את האלגברה הלינארית.
מתי משוואה נקראת לינארית? - כאשר כל הנעלמים הם בחזקה ראשונה ואין מכפלה של נעלמים.

> ספר לימוד: פרופ' עמיצור / אלגברה א'
> (יהיו סטיות ניכרות מה ספר, אם בתוכן ואם בסימונים, אבל
> סה"כ הספר משקף את החומר, כתוב בצורה טובה)

הערה

באלגברה אנחנו באים לפתור משוואות. למשל $2x+3y=5$
היא משוואה לינארית. המשתנים הם x,y.
המקדמים הם $2,3$
האיבר החופשי הוא 5

מה זה פתרון של משוואה? x ו-y שמקיימים את השוויון.
הנה דוגמא לכמה פתרונות: $x=1\ \ y=1$; $x=2\ \ y=\frac{1}{3}$ ויש עוד אינסוף..

נסתכל על מע' משוואות:
$$\begin{cases}2x+3y=5\\ x-y=0\end{cases}$$

למע' המשוואות הנוכחית קיים פתרון אחד והוא: $x=y=1$
במע' הנוכחית זה הפתרון היחיד ודי קל להראות את זה:
$$x-y=0 \Rightarrow x=y \Rightarrow 5x=5 \Rightarrow x=y=1$$
וזה שכבר מראה שיש רק פתרון אחד.

PDF processed with CutePDF evaluation edition www.CutePDF.com

עכשיו נסתכל על המע׳ הבאה:
$$\begin{cases} x+y=2 \\ 2x+2y=3 \end{cases}$$

כאן אין אף פתרון. למה? כמו קודם (נציב).

$$x+y=2 \Rightarrow x=2-y \Rightarrow 4-2y+2y=3 \Rightarrow 4=3$$

סתירה!

אז מה אנחנו רואים? ראינו 3 דוגמאות למשוואות:
- מצב שבו יש הרבה פתרונות.
- מצב שבו יש פתרון אחד בלבד.
- מצב שבו אין אף פתרון.

אז נניח שיש לנו מע׳ עם מלא מלא משוואות. איך נדע כמה בכלל פתרונות יש? איך נוכל לתאר את הפתרונות? אלה הבעיות הבסיסיות שאנחנו מנסים לפתור בא״ל של משוואות ליניאריות. יש פה עוד נושא. נושא לב שיש לנו מקדמים, לנעלמים וגם איברים חופשיים. אבל מאיפה הבאנו אותם? ומאיפה הערכים של הנעלמים? בדוגמאות לעיל כל השלושה היו מתוך המספרים הרציונליים. אבל אנחנו רוצים לעבור למצב הרבה יותר כללי. אנחנו רוצים למצוא איזה מושג מאיפה לקחת את כל אלה. מושג שיכלול כמקרה פרטי את המספרים הרציונליים אבל יביא גם הרבה אופציות אחרות. התשובה לכך היא <u>שדות</u>.

<u>דוגמה</u>: מספרים רציונליים (אנחנו יודעים על הנושא הזה לכן נסקור אותו בקצרה)

מדובר על מספרים שלמים ושברים והפעולות הידועות עליהם: חיבור וכפל.
לפעולות האלה יש מספר תכונות:

<u>חיבור</u>: א) סגירות - חיבור של רציונליים נותן מספר רציונלי.
עבור a,b רציונליים, המספר $a+b$ רציונלי.

ב) קומוטטיביות (חילופיות) - סדר החיבור לא מחליף את התוצאה.
לכל a,b רציונליים $a+b=b+a$

ג) אסוציאטיביות - רשמוספים סוגריים זה לא משנה

לכל a,b,c רציונליים $(a+b)+c = a+(b+c)$

ד) קיום 0. קיים איבר אפס רק שלכל a, $a+0=a$.

זה נקרא ניטרליות. האפס ניטרלי לפעולת החיבור.

ה) קיום איבר נגדי. לכל a רציונלי קיים איבר שנקרא $-a$ רק ש- $a+(-a)=0$.

<u>כפל</u>: א) סגירות. לכל a,b רציונליים מוגדר $a\cdot b$ רציונלי.

ב) קומוטטיביות. לכל a,b רציונליים $a\cdot b=b\cdot a$

ג) אסוציאטיביות. לכל a,b,c רציונליים $(a\cdot b)\cdot c = a\cdot(b\cdot c)$

ד) קיום 1. קיים איבר יחידה רק שלכל a: $a\cdot 1=a$

ה) קיום הופכי. לכל $a\neq 0$ רציונלי קיים איבר שנקרא $\frac{1}{a}$ ומתקיים $a\cdot\frac{1}{a}=1$.

> זה ההבדל בין כפל לחיבור. בחיבור קיים איבר (נגדי) לכל איבר רציונלי ואילו בכפל קיים איבר הופכי רק לאיברים שונים מאפס. זה מתאים לכלל שאסור לחלק באפס.

<u>חיבור וכפל</u>: חוק הפילוג (דיסטריביוטיביות):

לכל a,b,c רציונליים $a(b+c)=ab+ac$

ועוד הנחה: $0\neq 1$

חשוב לשים ♥ שכל התכונות האלה נתונות ללא הוכחה. זה נקרא אקסיומות של הרציונליים. אבל אנחנו לא נכנס לזה ונתייחס לזה כידוע מראש.

עכשיו נתקדם לעבר הגדרת מושג השדה.

מה אומרת לנו המילה "קבוצה"? - קבוצה זה אוסף של איברים. איזה איברים? לא משנה. העיקר שהם מאוגדים יחדיו.

נשים דגש: שדה עוברים שלושה שלבים.

שדה

(1) קבוצה F

(2) ב-F מוגדרות פעולות של חיבור וכפל

(3) הפעולות מקיימות את האקסיומות של השדה:

	חיבור:	כפל:
סגירות	$\forall a,b\in F\ \exists! a+b\in F$	$\forall a,b\in F\ \exists! a\cdot b\in F$
חילופיות	$\forall a,b\in F\ a+b=b+a$	$\forall a,b\in F\ a\cdot b=b\cdot a$
אסוציאטיביות	$\forall a,b,c\in F\ (a+b)+c=a+(b+c)$	$\forall a,b,c\in F\ (a\cdot b)\cdot c=a\cdot(b\cdot c)$
נייטרלי	$\exists 0_F: \forall a\in F\ a+0_F=a$	$\exists 1_F\ \forall a\in F\ 1_F\cdot a=a$
נגדי / הפכי	$\forall a\in F\ \exists -a\in F: a+(-a)=0_F$	הפכי: $\forall a\neq 0_F\in F\ \exists a^{-1}\in F: a\cdot a^{-1}=1_F$

דיסטריבוטיביות $\forall a,b,c\in F\quad a(b+c)=ab+ac$

הערה: נשים לב שהאקסיומה אומרת שיש נייטרלי לחיבור ולכפל ונגדי והפכי. היא לא אומרת שום דבר על יחידות האיברים האלה. אבל בהמשך נראה משפט על היחידות שלהם.

כמו כן נדרוש ש- $1_F \neq 0_F$.

אם כל הכתוב לעיל מתקיים אז F נקראת שדה (Field)

דוגמאות של שדות

(1) Q. שדה המספרים הרציונליים עם פעולות החיבור והכפל שאנחנו מכירים מחיי היומיום.

(2) R שדה המספרים הממשיים עם פעולות החיבור והכפל הרגילות.

מה זה מספר ממשי? האמת היא שזאת שאלה ממש קשה. אפשר לעשות את זה בצורה מדויקת בהמשך כחודש וחצי בעזרת חתכי דדקינד. אבל אנחנו לא נעשה את זה פה. אז נגיד משהו לסבר את האוזן. בשבילנו מספר ממשי זה כלשהו פיתוח עשרוני - סופי או אינסופי.

למשל $\pi=3.1415926...$ כאן הפיתוח העשרוני ממשיך בלי סוף.

איך משתלבים פה הרציונליים? אם הפיתוח הוא מחזורי המספר רציונלי. למשל $\frac{1}{3}=0.333...$ או $5.2171717...$

(3)

במספרים הרציונליים משתלבים בתוך המספרים הממשיים בתור פיתוחים עשרוניים <u>מחזוריים</u>: אם ניתן להציג את המספר בפיתוח סופי אפשר להציג אותו בשתי דרכים בפיתוח אינסופי. לפי הדוגמא הבאה: $1 = 1.0000\ldots = 0.9999\ldots = 1$

תשובה: $\left\{\begin{array}{l} 1.0 \neq 0.9 \\ 1.00 \neq 0.99 \\ 1.000 \neq 0.999 \end{array}\right.$ <u>אבל</u> באינסוף $1.000\ldots = 0.999\ldots$

כל שבר מחזורי $\frac{m}{n}$ ניתן להציג בפיתוח עשרוני מחזורי ולהפך.

⇐ מושג המספר הממשי בכלל לא פשוט בכלל, זה מבחינה לוגית וגם מבחינה פילוסופית. כרגע מה שעשינו מספיק לצורכינו, כך לא נתעמק בהגדרה המדויקת של כפל וחיבור בפיתוחים העשרוניים כמובן צריך זה להוכיח שמתקיימות אקסיומות השדה. במספרי אלינו יש הסברים מפורטים של כל זה.

(2) $F_2 = \{0, 1\}$ את הכפל נשאיר כמו שאנחנו מכירים אבל החיבור שונה מהחיבור הרגיל. - חיבור מודולו 2

(נסכם בטבלאות את פעולות החיבור והכפל)

$+_2$	$_{2}0$	$_{2}1$
$_{2}0$	$_{2}0$	$_{2}1$
$_{2}1$	$_{2}1$	$_{2}0$

$\cdot$	$_{2}0$	$_{2}1$
$_{2}0$	$_{2}0$	$_{2}0$
$_{2}1$	$_{2}0$	$_{2}1$

האם ב-F_2 עם הפעולות לעיל מתקיימות אקסיומות השדה?

- סגירות - ברור מעצם ההגדרה
- קומוטטיביות - רואים בקלות בטבלאות
- אסוציאטיביות - יש לבדוק $2^3 = 8$ מקרים

$0 = (\overset{0}{0+0})+0 = 0+(\overset{0}{0+0}) = 0$ ✓

$1 = (\overset{0}{0+0})+1 = 0+(\overset{1}{0+1}) = 1$ ✓

$1 = (\overset{1}{0+1})+0 = 0+(\overset{1}{1+0}) = 1$ ✓

$0 = (\overset{1}{0+1})+1 = 0+(\overset{0}{1+1}) = 0$ ✓

$1 = (\overset{1}{1+0})+0 = 1+(\overset{0}{0+0}) = 1$ ✓

$0 = (\overset{1}{1+0})+1 = 1+(\overset{1}{0+1}) = 0$ ✓

$0 = (\overset{0}{1+1})+0 = 1+(\overset{1}{1+0}) = 0$ ✓

$1 = (\overset{0}{1+1})+1 = 1+(\overset{0}{1+1}) = 1$ ✓

מה שלא נבדק בהמשך בדוק בבית!

הערה!!
אם היינו מגדירים את החיבור כך:

+	0	1
0	0	1
1	1	1

ברור שלא היה שדה כי אין פה איבר נגדי ל-1.

- איבר ניטרלי יש גם לחיבור (0_2) וגם לכפל (1_2) ו- $1_2 \neq 0_2$.

איבר נגדי ל- 0_2 : 0_2 - איבר הפכי ל- 1_2 - 1_2

נגדי של 1_2 הוא 1_2

- אסוציאטיביות הכפל ברורה כי זה כמו בטבעיים.

- את חוק הפילוג יש לבדוק, וזה אם באמת יתקיים.

המסקנה היא שקיבלנו שדה עם שני איברים - שהרי כל

אקסיומות השדה מתקיימות.

⇒ שדה עם פחות משני איברים לא קיים כי אמרנו שאיבר

האפס צריך להיות שונה מאיבר היחידה.

(4) 2.11.05

אנחנו מדברים כרגע על שדות - מה שהתחלנו בשיעור הראשון.

הגדרה: שדה F זאת קבוצה של איברים שמוגדרות בה פעולות של חיבור וכפל כך שמתקיימות האקסיומות של השדה:

כפל	חיבור
סגירות	סגירות
קומוטטיביות	קומוטטיביות
אסוציאטיביות	אסוציאטיביות
קיום היחידה	קיום האפס
קיום איבר הפכי לכל איבר שונה מאפס	קיום איבר נגדי

דיסטריביוטיביות

$1_F \neq 0_F$

הערות:
- (כדי לראות) שההבדל מהכפל ומהחיבור אקסיומות מלבד העובדה שלא קיים איבר הפכי לאפס.
- הדרישה ש- $0 \neq 1$ באה רק לשלול את המקרה של שדה בעל איבר אחד $F=\{0\}$.
- שדה הוא קבוצה של איברים, לאו דווקא מספרים.

דוגמאות:

(1) Q - המספרים הרציונליים עם הפעולות הידועות לנו

(2) - R - המספרים הממשיים. מספר ממשי הוא לא אוסף פשוט. אנחנו לקחנו כאן גרסה פשטנית למדי לאובייקט שמספר ממשי הוא פיתוח עשרוני אינסופי.

הרציונליים הם תת קבוצה של הממשיים, הם אלה שהפיתוח העשרוני שלהם מחזורי.

- ישנם ממשיים שיש להם שני פיתוחים עשרוניים שונים.

(3) - $F_2=\{0,1\}$ עם הכפל כמו שאנחנו מכירים וחיבור מודולו 2.

* חיבור מודולו n הוא לחלק מספר ב-n ולקחת את השארית.

בשיעור הקודם היה לנו קושי לבדוק אסוציאטיביות של חיבור. אפשר להוכיח באינדוקציה שכאשר מספר האחדים בסכום זוגי התוצאה היא אפס וכאשר הוא אי זוגי התוצאה היא אחד וזה היה חוסך לנו עבודה, משום שזה מראה שהתוצאה לא תלויה בסוגריים.

מה עם הדיסטריבוטיביות? $a(b+_2c) \overset{?}{=} ab+_2ac$

$a=0$ $\quad 0(b+_2c)=0 \;,\; 0\cdot b+_2 0\cdot c=0$

$a=1$ $\quad 1\cdot(b+_2c)=b+_2c \;,\; 1\cdot b+_2 1\cdot c=b+_2c$

} לפי לוח הכפל לכל $a\in F$ $a\cdot 0=0,\ a\cdot 1=a$

ברור כמובן לפי ההגדרה ש- $0\neq 1$. $\Leftarrow$ F_2 שדה.

- נניח שהיינו מגדירים את פעולות החיבור והכפל כך:

⊙	0 (1)	1 (0)
0 (1)	0 (1)	1 (0)
1 (0)	1 (0)	1 (0)

⊕	0 (1)	1 (0)
0 (1)	1 (0)	0 (1)
1 (0)	0 (1)	1 (0)

$G=\{0,1\}$

כאן פשוט התחלפו התפקידים של 0 ו- 1. אם נחליף כל 0 ב- 1 וכל 1 ב- 0 נקבל את לוחות החיבור והכפל הקודמים. (זה מראה לנו שלא משנה איך אנחנו קוראים לאיברים). רואים בבירור את לוחות הכפל והחיבור הקודמים שאנו יודעים כבר הוכחנו שזה שדה $\Leftarrow$ גם המקרה הזה הוא שדה. האפס של G הוא 1 והאחד של G הוא 0.

זה בא לסתור את האינטואיציה הראשונה שלנו לגבי איבר האפס והיחידה. מה שחשוב הן התכונות של האיברים, לא השמות שלהם.

- עוד תרגיל מסוג זה. $H=\{z,u\}$ ונגדיר לוח חיבור וכפל:

·	z	u
z	z	z
u	z	u

+	z	u
z	z	u
u	u	z

כמו קודם קל לראות שמתקיימות האקסיומות של השדה, כי אפשר להתאים ל- z אפס (zero) ול- u אחד (unit).

השדות האלה נקראים **שדות איזומורפיים** - אפשר לעשות ביניהם התאמה כך שלוחות החיבור והכפל מתלכדים.

הערה! תרגיל קל - מאמה: אם שתי קבוצות והפעולות בהן איזומורפיות - ואחת הקבוצות היא שדה, אז גם השנייה היא שדה.
אבל תרגיל זה לא חשוב עכשיו כי עוד לא ממש למדנו מה זה איזומורפיזם.

המשך דוגמאות:

(4) המספרים המרוכבים $\mathbb{C}=\{a+bi : a,b\in\mathbb{R}\}$ וברגע אנחנו מתייחסים ל-i כסתם אות בסוף לשין. הגדרנו קבוצה. עכשיו צריך להגדיר פעולות חיבור וכפל.

הגדרה: $x-y \equiv x+(-y)$

חיבור: $(a_1+b_1i)+(a_2+b_2i)=(a_1+a_2)+(b_1+b_2)i$

כפל: $(a_1+b_1i)(a_2+b_2i)=(a_1a_2-b_1b_2)+(a_1b_2+b_1a_2)i$

האם בקבוצה שהגדרנו תחת הפעולות שלנו מתקיימות אקסיומות השדה?

- סגירות: ברור גם בחיבור וגם בכפל כי $\mathbb{R}$ שדה $\Leftarrow$
$a_1b_2+b_1a_2,\ a_1a_2-b_1b_2,\ b_1+b_2,\ a_1+a_2\in\mathbb{R}$
התוצאות הן איברים במבנה האברים בקבוצה שהגדרנו.

- קומוטטיביות:

$$(a_1+b_1i)+(a_2+b_2i)\overset{(1)}{=}(a_1+a_2)+(b_1+b_2)i\overset{(2)}{=}(a_2+a_1)+(b_2+b_1)i\overset{(1)}{=}(a_2+b_2i)+(a_1+b_1i)$$

$$(a_1+b_1i)(a_2+b_2i)\overset{(1)}{=}(a_1a_2-b_1b_2)+(a_1b_2+b_1a_2)i\overset{(2)}{=}(a_2a_1-b_2b_1)+(b_2a_1+a_2b_1)i\overset{(2)}{=}(a_2a_1-b_2b_1)+(a_2b_1+b_2a_1)i\overset{(1)}{=}(a_2+b_2i)(a_1+b_1i)$$

1- הגדרה של הפעולות ב-$\mathbb{C}$
2 - קומוטטיביות ב-$\mathbb{R}$

- אסוציאטיביות של חיבור:

$$((a_1+b_1i)+(a_2+b_2i))+(a_3+b_3i)\overset{(1)}{=}((a_1+a_2)+(b_1+b_2)i)+(a_3+b_3i)\overset{(1)}{=}((a_1+a_2)+a_3)+((b_1+b_2)+b_3)i\overset{(3)}{=}$$
$$\overset{(3)}{=}(a_1+(a_2+a_3))+(b_1+(b_2+b_3))i\overset{(1)}{=}(a_1+b_1i)+((a_2+a_3)+(b_2+b_3)i)\overset{(1)}{=}(a_1+b_1i)+((a_2+b_2i)+(a_3+b_3i))$$

3 - אסוציאטיביות של חיבור ב-$\mathbb{R}$

- קיום האפס:

$$(a+bi)+(0+0i)\overset{(1)}{=}(a+0)+(b+0)i\overset{(4)}{=}a+bi \Rightarrow 0_{\mathbb{C}}=0+0i$$

4 - קיום האפס והגדרתו בממשיים.

- קיום איבר נגדי: נטען ש- $((-a)+(-b)i)$ - הוא הנגדי ל- $(a+bi)$

$$(a+bi)+((-a)+(-b)i) \overset{1}{=} (a+(-a))+(b+(-b))i \overset{5}{=} 0+0i = 0_c$$

5 - האיבר הנגדי ב- $\mathbb{R}$

- אסוציאטיביות של כפל (זה הולך להיות מייגע...)

$$((a_1+b_1i)(a_2+b_2i))(a_3+b_3i) \overset{?}{=} (a_1+b_1i)((a_2+b_2i)(a_3+b_3i))$$

$$((a_1a_2-b_1b_2)+(a_1b_2+b_1a_2)i)(a_3+b_3i) =$$

$$((a_1a_2-b_1b_2)a_3-(a_1b_2+b_1a_2)b_3)+((a_1a_2-b_1b_2)b_3+(a_1b_2+b_1a_2)a_3)i =$$

תזכורת: $(-b)c = -(bc)$

הערה: חוק הפילוג עובד גם עבור מינוס (-)

$$(a-b)c = (a+(-b))c = ac+(-b)c = ac+(-bc) = ac-bc$$

$$= ((a_1a_2)a_3-(b_1b_2)a_3-(a_1b_2)b_3-(b_1a_2)b_3)+((a_1a_2)b_3-(b_1b_2)b_3+(a_1b_2)a_3+(b_1a_2)a_3)i$$

$$(a_1+b_1i)((a_2a_3-b_2b_3)+(a_2b_3+b_2a_3)i) =$$

$$= (a_1(a_2a_3-b_2b_3)-b_1(a_2b_3+b_2a_3))+(a_1(a_2b_3+b_2a_3)+b_1(a_2a_3-b_2b_3))i =$$

$$= (a_1(a_2a_3)-a_1(b_2b_3)-b_1(a_2b_3)-b_1(b_2a_3))+(a_1(a_2b_3)+a_1(b_2a_3)+b_1(a_2a_3)-b_1(b_2b_3))i$$

בצבעים זהים נקבל את החלקים הזהים בשני הפיתוחים ולכן רואים שאכן מתקיימת אסוציאטיביות בכפל. (נובע מכפל קומוטטיבית ב $\mathbb{R}$)

- קיום היחידה: נראה ש- $1_c = 1+0\cdot i$

$$(a+bi)(1+0i) = (a\cdot1-b\cdot0)+(a\cdot0+b\cdot1)i = (a-0)+(0+b)i = a+bi$$

- דיסטריביוטיביות:

$$(a_1+b_1i)((a_2+b_2i)+(a_3+b_3i)) \overset{1}{=} (a_1+b_1i)((a_2+a_3)+(b_2+b_3)i) =$$

$$\overset{1}{=} (a_1(a_2+a_3)-b_1(b_2+b_3))+(a_1(b_2+b_3)+b_1(a_2+a_3))i =$$

$$\overset{6}{=} (a_1a_2+a_1a_3-b_1b_2-b_1b_3)+(a_1b_2+a_1b_3+b_1a_2+b_1a_3)i =$$

$$\overset{1}{=} ((a_1a_2-b_1b_2)+(a_1b_2+b_1a_2)i)+((a_1a_3-b_1b_3)+(a_1b_3+b_1a_3)i) =$$

$$\overset{1}{=} (a_1+b_1i)(a_2+b_2i)+(a_1+b_1i)(a_3+b_3i)$$

6 - פילוג בין מספרים ממשיים

- קיום הפכי :

קודם הגדרה: יהא המספר $a+bi$ ו-$a-bi$ נקרא הצמוד שלו.

נסתכל מה קורה כשכופלים מספר מרוכב בצמוד שלו:

$$(a+bi)(a-bi) = (a\cdot a - b(-b)) + (a(-b)+ba)i =$$
$$= (a^2+b^2) + 0\cdot i$$

⇐ מקבלים מהצורה : $\cdot i$ אפס + חלק ממשי

* לא באנו לבדוק את הממשיים כמרוכבים שהחלק המדומה שלהם אפס, אבל כדאי להקפיד לרשום את האפס. הדגש הוא שזה כן מספר מרוכב.

נניח כעת ש $\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i$ הוא ההפכי של $a+bi$.

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

זה כמובן כאשר $a^2+b^2\neq 0$ וזה שקול כאשר $a+bi \neq 0+0\cdot i$

כלומר זה נכון עבור כל המרוכבים ששונים מאפס.

⇓

$\mathbb{C}$ שדה.

Yey!

שיעור ביום רביעי הבא - בקפן.

כל שאר השיעורים החל מהיום יתקיימו באולם קפלן

שדה המספרים המרוכבים

שדה היא קבוצה שמוגדרות עליה פעולות חיבור וכפל שמקיימות את אקסיומות השדה. ראינו כמה דוגמאות לשדות: $\mathbb{Q}$, $\mathbb{R}$, $\{0,1\}$, $\mathbb{C}$.

על הקבוצה $\mathbb{C}=\{a+bi : a,b\in\mathbb{R}\}$ הגדרנו חיבור וכפל באופן הבא:

$$(a_1+b_1 i)+(a_2+b_2 i)=(a_1+a_2)+(b_1+b_2)i$$

$$(a_1+b_1 i)\cdot(a_2+b_2 i)=(a_1a_2-b_1b_2)+(a_1b_2+b_1a_2)i$$

נוסחת הכפל פחות מובנת מאליה. זאת מעורר הצורך להבין מה המשמעות של i. שהרי בשיעור הקודם אמרנו ש-i הוא רק סמל. אז מהו i בעצם?

$$(0+1i)(0+1i)=(0\cdot0-1\cdot1)+(0\cdot1+1\cdot0)i=-1+0i$$

אז i הוא מספר שהריבוע שלו הוא -1. בממשיים לא קיים שורש ל--1 ולשם כך בשדה יש לנו את המרוכבים. ב-$\mathbb{R}$ אין פתרון למשוואה $x^2+1=0$. ידוע שלכל $x\in\mathbb{R}$ $x^2\geq0 \Rightarrow x^2+1>0 \Rightarrow$ לא יכול להיות פיתרון. אבל אנחנו רוצים פיתרון וזאת הייתה המוטבציה שבניית שדה המספרים המרוכבים. במרוכבים יש למשוואה הזאת פיתרון: $x=0+1i$.

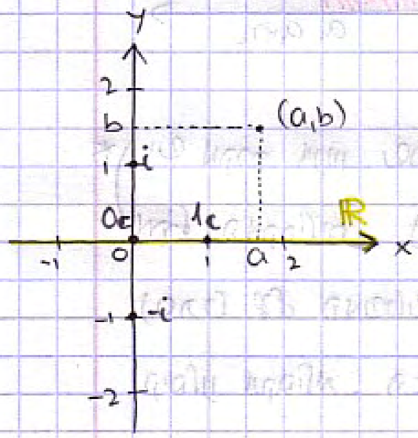
(נזהה את $\mathbb{R}$ כתת-קבוצה של $\mathbb{C}$ ע"י הזיהוי של $a\in\mathbb{R}$ עם $a+0\cdot i\in\mathbb{C}$)

את $0+1\cdot i$ נכתוב בד"כ כרק i. אז i הוא לא סתם סימן, הוא הפיתרון של $x^2+1=0$, והוא $i=\sqrt{-1}$. (שמו i זה בשביל imaginary)

כל הדיון לעיל מסביר את ה-$(-)$ בנוסחת הכפל - כי $b_1i\cdot b_2i=-b_1b_2$.

הצגה גאומטרית של המרוכבים

נסתכל על זוג צירים במישור. (אנחנו מניחים שאנחנו יודעים גאומטריה)



למספר מרוכב $a+bi$ נתאים נק' עם קואורדינטות (a,b). זה דורש הסבר.
לכל ציר יש קנה מידה. לכל נק' במישור אפשר לקחת היטלים על הצירים. ואז a הנו ההיטל על ציר ה-x ו-b הוא ההיטל על ציר ה-y.
וכך לכל מרוכב מתאים נקודה במישור.

ברור ש- $0_C = 0+0i$ מתאימה ראשית הצירים.
ו- $1_C = 1+0i$ מתאימה הנקודה $(1,0)$
ו- $i = 0+1\cdot i$ מתאימה הנקודה $(0,1)$
ו- $-i = 0-1i$ מתאימה הנקודה $(0,-1)$

את כל זה אפשר לראות בציור שבעמוד הקודם.

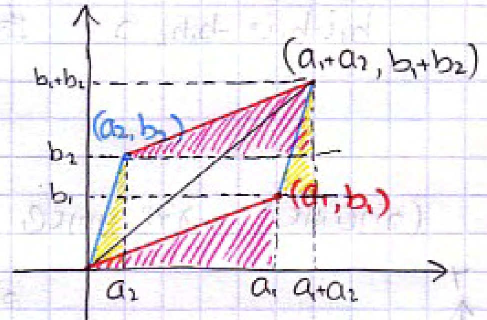
אז בשדה המספרים המרוכבים יש לנו שני פתרונות למשוואה $x^2+1=0$
$x_1 = 0+1\cdot i$ ו- $x_2 = 0-1\cdot i$.

המספרים המרוכבים מיוצגים ע"י מישור, והמספרים הממשיים מיוצגים ע"י ישר - הוא ציר ה-x.

מתברר שבשדה המספרים המרוכבים לכל משוואה לא טריוויאלית יש פיתרון.

לכל משוואה אלגברית מעל $\mathbb{C}$: $a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$, $a_0,\dots,a_n \in \mathbb{C}$, $a_n \neq 0$ ו- $n \geq 1$ יש שורש ב- $\mathbb{C}$. התכונה הזאת נקראת סגירות אלגברית.
זאת תכונה שאפשר להוכיח אבל אנחנו לא נעשה את זה במסגרת הזאת.
(שדה המספרים הממשיים $\mathbb{R}$ אינו סגור אלגברית - שם יש משוואה $x^2+1=0$ שאין לה פתרון בשדה $\mathbb{R}$.)
זה משפט כל כך חשוב שיש לו שם המשפט היסודי של האלגברה.

בתחום המרוכבים יש לנו פעולות חיבור וכפל. נרצה לעשות תיאור גאומטרי לפעולות האלה.
חיבור:



ציירנו את שני המספרים (נקודות) של המישור המרוכב. איך ניתן תיאור גאומטרי שמבטא את הנקודה שהיא הסכום של שני המספרים?
כלל המקבילית זאת התשובה.

*(יש מקרה מנוון שבו שתי הנקודות נמצאות על אותו ישר. ואז מיישמים את כלל המקבילית ע"י חיבור האורכים המכוונים.)

נסתכל על המשולשים שצבועים באותו צבע. קל לראות שהם חופפים ובאמת קיבלנו מקבילית. האלכסון שלה מייצג את הסכום של שני המספרים.

זה היה יחסית לא מסובך. ומה קורה עם הכפל? הנוסחה של הכפל הרבה יותר מסובכת. האם יש לכפל משמעות גאומטרית כמו שראינו לחיבור?

עקרונית, יכול להיות שלא, אבל שואלים בד"כ שאלה שיש לה תשובה. אז נראה כמה דוגמאות ואז ננסה להכליל.

- נניח שנסתכל רק על הממשיים - $a_1=a_1+0i$, $a_2=a_2+0i$

כשכופלים אותם בתור מרוכבים מקבלים $(a_1+0i)(a_2+0i)=(a_1a_2-0\cdot0)+(a_1 0+0a_2)i=a_1a_2$

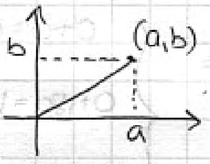
בחיבור זה כמובן עובד גם. אז החיבור והכפל בממשיים תואם את החיבור והכפל במרוכבים. אז כשכופלים מספרים ממשיים הם חייבים להיות על הציר הממשי.

- כשכופלים את הנקודה $(0,1)$ בעצמה מקבלים $(-1,0)$

- נסתכל על $(1+1i)$. נעלה אותו בריבוע: $(1+1i)^2=(1\cdot1-1\cdot1)+(1\cdot1+1\cdot1)i=0+2i$

- אנחנו יודעים מה קורה כאשר כופלים בצמוד: $(a+bi)(a-bi)=a^2+b^2+0i$

איך כל זה עוזר לנו? - טוב, לא ממש, אבל אם נתבונן נשים ♡ שאת המספר המרוכב לא מאפיינות רק הקואורדינטות שלו, אלא גם אורך הישר שמחבר את הראשית עם הנקודה והזווית בין ציר ה-x לבין אותו ישר.



לפי פיתגורס אורך הקטע הוא $\sqrt{a^2+b^2}$

מגדירים ערך מוחלט של $z=a+bi\in\mathbb{C}$ ע"י $|z|=\sqrt{a^2+b^2}$. וזה תואם לאורך שבהצגה הגאומטרית שלנו.

$$|a+bi|=\sqrt{a^2+b^2} \qquad |a-bi|=\sqrt{a^2+(-b)^2}=\sqrt{a^2+b^2}$$

למספרים מרוכבים צמודים יש אותו ערך מוחלט. ומה עם המכפלה?

$$|(a+bi)(a-bi)|=|(a^2+b^2)+0i|=\sqrt{(a^2+b^2)^2+0^2}=a^2+b^2$$

בממשיים ידוע ש- $|a_1a_2|=|a_1||a_2|$

ובמרוכבים עבור צמודים $|z\bar{z}|=|z||\bar{z}|$ (כאשר $\bar{z}$ הוא הצמוד של z)

אז מתבקש המשפט:

<u>משפט</u>: לכל $a_1+b_1i,\ a_2+b_2i\in\mathbb{C}$ $|(a_1+b_1i)(a_2+b_2i)|=|a_1+b_1i||a_2+b_2i|$

הוכחה:

$$|(a_1+b_1i)(a_2+b_2i)| = |(a_1a_2-b_1b_2)+(a_1b_2+a_2b_1)i| =$$
$$= \sqrt{(a_1a_2-b_1b_2)^2+(a_1b_2+b_1a_2)^2} =$$
$$= \sqrt{a_1^2a_2^2 - 2a_1a_2b_1b_2 + b_1^2b_2^2 + a_1^2b_2^2 + 2a_1a_2b_1b_2 + b_1^2a_2^2} =$$
$$= \sqrt{a_1^2a_2^2 + a_1^2b_2^2 + b_1^2b_2^2 + b_1^2a_2^2} =$$
$$= \sqrt{a_1^2(a_2^2+b_2^2)+b_1^2(b_2^2+a_2^2)} = \sqrt{(a_1^2+b_1^2)(a_2^2+b_2^2)} =$$
$$= \sqrt{a_1^2+b_1^2}\cdot\sqrt{a_2^2+b_2^2} = |a_1+b_1i||a_2+b_2i|$$

$\sqrt{ab}=\sqrt{a}\sqrt{b}$

אושר ☺

זאת תכונה מעניינת של המרוכבים. המשמעות הגאומטרית של זה היא המרחק של הנקודה מהראשית. מרחק המכפלה של שני מרוכבים מהראשית הוא מכפלת המרחקים של כל אחד מהם. זה מקרב אותנו לבעיה המקורית - ההצגה הגאומטרית של הכפל.

נותר לנו לטפל בזוויות. הזווית מוגדרת היטב עד כדי $360°$ (או 2π)

ברור שכל המספרים הממשיים הזווית היא 0 לחיוביים ו- π לשליליים:

- $\mathbb{P}\cdot\mathbb{P}=\mathbb{P}$ כמו ש- $0+0=0$
- $\mathbb{P}\cdot\mathbb{P}^-=\mathbb{P}^-$ כמו ש- $0+180=180$
- $\mathbb{P}^-\cdot\mathbb{P}^-=\mathbb{P}$ כמו ש $180+180=0$

$\Leftarrow$ מכפלה של מספרים ממשיים מתנהגת לפי סכום הזוויות.

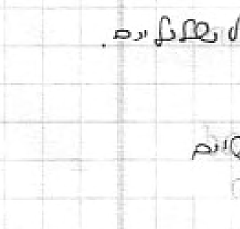
- $i^2=-1$ הזווית של i היא $\pi/2$ ואכן $\pi/2+\pi/2=\pi$

הזווית של $-i$ היא $3\pi/2$. $(-i)^2=-1$ ואכן $3\pi/2+3\pi/2=3\pi$

- נניח שהזווית של z היא α. הזווית של $\bar{z}$ היא $-\alpha$. המכפלה $z\cdot\bar{z}$ היא מספר ממשי שהזווית שלו 0 ואכן $\alpha+(-\alpha)=0$.

כל אלה מקרים פרטיים אבל זה מביא אותנו להשערה שזה נכון באופן כללי.

נסתכל על כל המספרים שמקיימים $|a+bi|=1$.



זה המקום הגאומטרי של כל הנקודות במרחק 1 מהראשית.

כלומר, זה מעגל היחידה. - $\{a+bi\in\mathbb{C} : |a+bi|=1\}$

מה הקואורדינטות של מספר שזוויתו α? $(\cos\alpha, \sin\alpha)$

β? $(\cos\beta, \sin\beta)$

באופן מסוים זאת ההגדרה של פונקציות sin ו- cos - היטל של מעגל היחידה!

משפט והוכחה:

$$(\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta) =$$

$$= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\cos\alpha\sin\beta + \sin\alpha\cos\beta) =$$

$$= \cos(\alpha+\beta) + i\sin(\alpha+\beta)$$

לפי נוסחה ידועה

המשפט מדבר על מעגל היחידה. אזי $a+bi = \underbrace{|a+bi|}_{\text{אורך}}\underbrace{(\cos\alpha + i\sin\alpha)}_{\text{וקטור במעגל היחידה}}$

ראינו שבמכפלה של מרוכבים האורכים שלהם נכפלים אם לפי המשפט שאומר הזוויות מתחברות.

$$\Rightarrow (a+bi) = |a+bi|(\cos\alpha + i\sin\alpha)$$

$$(c+di) = |c+di|(\cos\beta + i\sin\beta)$$

$$\Rightarrow (a+bi)(c+di) = \left(|a+bi|(\cos\alpha + i\sin\alpha)\right)\left(|c+di|(\cos\beta + i\sin\beta)\right) =$$

$$= |a+bi||c+di|\left(\cos(\alpha+\beta) + i\sin(\alpha+\beta)\right)$$

בפרט

$$(a+bi)^n = |a+bi|^n(\cos n\alpha + i\sin n\alpha)$$

$$\sqrt[n]{a+bi} = \sqrt[n]{|a+bi|}\left(\cos\frac{n}{\alpha} + i\sin\frac{n}{\alpha}\right)$$

עכשיו יש פה נקודה יפה: פעולת השורש היא לא חד-ערכית. למעשה היא יכולה לתת n תשובות. משום שהזוית מוגדרת עד כדי 2π נקבל n זויות שונות $\frac{\alpha}{n}, \frac{\alpha}{n}+\frac{2\pi}{n}, \ldots, \frac{\alpha}{n}+(n-1)\frac{2\pi}{n}$

$\Leftarrow$ למשוואה $x^n=a+bi$ יש n פתרונות מרוכבים שונים!

(10) 9.11.05

לינארית

שדה שאריות מודולו p

פעם קודמת דיברנו על שדה המספרים המרוכבים. היום נדבר על סוג אחר של שדות - שאריות מודולו p.

יהי $0<n\in\mathbb{Z}$. נניח ש-$k,\ell\in\mathbb{Z}$. נאמר ש-$k\equiv \ell \pmod n$ כאשר קיים $u\in\mathbb{Z}$ רק ש-$k-\ell=u\cdot n$ - כלומר ההפרש בין המספרים הוא כפולה של n. או במילים אחרות - שני המספרים משאירים את אותה שארית בחלוקה ב-n.

למשל, שני מספרים חיוביים שקולים מודולו 10, כאשר יש להם אותה ספרה אחרונה. למעשה, זה נכון לכל שני מספרים שווי סימן. $2378\equiv 18 \pmod{10}$

כל שני מספרים זוגיים שקולים מודולו 2 וכל שני מספרים אי-זוגיים שקולים מודולו 2.

חילוק עם שארית

quotient → q, residue → r

יהי $0<n\in\mathbb{Z}$. לכל $m\in\mathbb{Z}$ קיימים $q,r\in\mathbb{Z}$, $0\le r\le n-1$ רק ש- $m=q\cdot n+r$. כלומר אפשר לחלק את m ב-n עם שארית r.

למשל: $28=2\cdot 13+2$. כאן $m=28$, $n=13$, $q=2$, $r=2$.

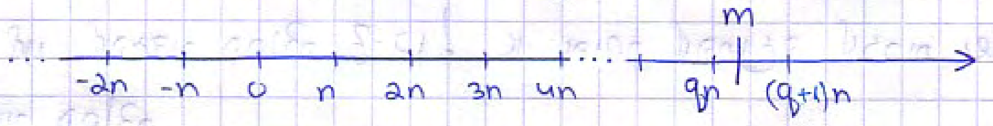
$-1=(-1)\cdot 10+9$, שהרי לא הרשנו לפי ההגדרה שארית שלילית.

$200=20\cdot 10+0$ - שארית $r=0$ - כלומר המספר אמנם מתחלק ללא שארית.

אחרי שסטודנט פעור אומר שהטענה ברורה אז) במתמטיקה צריך להוכיח כל דבר...

הוכחה:

נסתכל בכל הכפולות של מספר n: $\dots,-2n,-n,0,n,2n,3n,\dots$



קיים qn רק ש-$qn\le m$ ו-$(q+1)n>m$. $m-qn=r\in\mathbb{Z}$.

ברור ש- $n>m-qn=r\ge 0$. $r\in\mathbb{Z} \Rightarrow r\le n-1 \Rightarrow 0\le r\le n-1$

ו- $m=qn+r$. מש"ל

נרצה לקשר בין שני הנושאים שדיברנו עליהם.

טענה: עבור $m_1,m_2\in\mathbb{Z}$, $m_1\equiv m_2 \pmod n$ אמ"מ השארית של m_1 בחלוקה ב-n שווה לשארית של m_2 בחלוקה ב-n.

הוכחה: לפי הטענה הקודמת אפשר לרשום

$m_2=q_2n+r_2$, $m_1=q_1n+r_1$, $0\le r_1,r_2\le n-1$

($\Rightarrow$) נניח $r_1=r_2=r$. אזי $m_1-m_2=q_1n+r-(q_2n+r)=(q_1-q_2)n$

ולכן $m_1\equiv m_2 \pmod n$

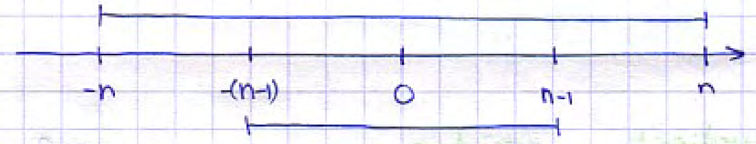
($\Leftarrow$) נניח ש-$m_1\equiv m_2 (\bmod 2)$ $\Leftarrow$ $m_1-m_2=u\cdot n$, $u\in\mathbb{Z}$ (לפי

הגדרה של שקילות מודולו n) $\Leftarrow$ $q_1n+r_1-(q_2n+r_2)=u\cdot n$

$\Leftarrow$ $r_1-r_2=(u-q_1+q_2)n$. אבל $0\le r_1,r_2\le n-1$ $\Leftarrow$

$-(n-1)\le r_1-r_2\le n-1$ $(*)$ מדוע?

$$-(n-1)=0-(n-1)\le 0-r_2\le r_1-r_2\le (n-1)-r_2\le (n-1)-0=n-1$$



$\Leftarrow$ $r_1-r_2=0$. 0 הוא היחיד שמקיים את אי השוויון $(*)$ והוא הכפלה של n. $\Leftarrow$ $r_1=r_2$ מש"ל ☺

סימון: אם $m=qn+r$ נסמן (באופן כללי, לא קיים סימון רשמי) $r=[m]_n$ - כלומר r היא השארית של m בחלוקה ב-n.

תחת הסימון החדש הוכחנו ש:

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

הגדרה: נסמן את כל השאריות מודולו n: $\mathbb{Z}_n=\{0,1,\dots,n-1\}$.

ב-$\mathbb{Z}_n$ יש n איברים.

מותר לנו להגדיר קבוצה זו-כן! אי אפשר להתנגד לזכות שלנו להגדיר קבוצה.

עכשיו נגדיר שתי פעולות על הקבוצה $\mathbb{Z}_n$: $+_n$ ו- $\cdot_n$ (האינדקס n מבדיל את הפעולות האלה מפעולות החיבור והכפל הרגילות ב-$\mathbb{Z}$).

נגדיר: לכל $a,b \in \mathbb{Z}_n$: $a +_n b = [a+b]_n$

$a \cdot_n b = [a \cdot b]_n$

ברור שאפשר להשתמש בפעולות האלה גם עבור כל $k,l \in \mathbb{Z}$:
$k +_n l = [k+l]_n$ ו- $k \cdot_n l = [k \cdot l]_n$. פשוט כרגע אנחנו מעוניינים
דווקא במקרה של $\mathbb{Z}_n$. לדוגמא $12 +_n 205 = [217]_{10} = 7$

$35 \cdot_n 14 = [490]_{10} = 0$

נתבונן עכשיו על $\mathbb{Z}_4 = \{0,1,2,3\}$. נשתמש בהגדרה של $+_n$
לפי נרשום את לוח החיבור:

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

באותו אופן, נרשום את לוח הכפל:

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

באופן טבעי, נרצה לדעת אם קיבלנו שדה. והנה, נשים ♡ של-2
אין איבר הפכי! אנחנו רואים את זה כי בשורה של 2 בלוח הכפל
לא קיים 1 $\Leftarrow$ אין אף איבר ב-$\mathbb{Z}_4$ שאם נכפול אותו ב-2 נקבל
את איבר היחידה.

משפט: לכל $1<n\in\mathbb{Z}$, $\mathbb{Z}_n$ עם הפעולות $+_n$, $\cdot_n$ מקיימת את כל אקסיומות השדה מלבד (אולי) קיום הופכי.

הכוונה כאן היא שבכלל לא נדון במשפט הזה בקיום הופכי. נדון בכל שאר האקסיומות מלבד קיום הופכי. בהמשך יהיה לנו דיון נפרד בנושא הזה ונראה שאם n ראשוני אז גם אקסיומת ההופכי מתקיימת.

טענת עזר 1: $m\equiv[m]_n(\mathrm{mod}\ n)$, $m\in\mathbb{Z}$.

הוכחה: $m=qn+r=qn+[m]_n$ כאשר $q,r\in\mathbb{Z}$ ו- $0\le r\le n-1$.

$\Leftarrow m-[m]_n=qn+r-r=qn \Leftarrow m\equiv[m]_n(\mathrm{mod}\ n)$. משל ☺

טענת עזר 2: אם $k_1\equiv k_2(\mathrm{mod}\ n)$ ו- $\ell_1\equiv\ell_2(\mathrm{mod}\ n)$ אז $\ell_1+k_2\equiv(\ell_2+k_2)(\mathrm{mod}\ n)$

הוכחה: $k_1-k_2=u_1n$ ו- $\ell_1-\ell_2=u_2n$ $\Leftarrow$

$$(k_1+\ell_1)-(k_2+\ell_2)=(k_1-k_2)+(\ell_1-\ell_2)=u_1n+u_2n=(u_1+u_2)n$$

$\Leftarrow k_1+\ell_1\equiv(k_2+\ell_2)(\mathrm{mod}\ n)$. משל ☺

דוגמאות:

טענת עזר 2 - $\ell_1=3$ $k_1=2$ $n=10$

$k_2=22$ $\ell_2=33$

$k_1+\ell_1=5$, $k_2+\ell_2=55$

טענת עזר 1 - $m=35$ $n=10$

$[m]_{10}=5$ $35\equiv5(\mathrm{mod}\ 10)$

אלה טענות די ברורות מאליהן, אבל צריך להוכיח אותן בכל אופן.

טענת עזר 3: אם $k_1\equiv k_2(\mathrm{mod}\ n)$ ו- $\ell_1\equiv\ell_2(\mathrm{mod}\ n)$ אז

$k_1\cdot\ell_1\equiv(k_2\cdot\ell_2)(\mathrm{mod}\ n)$

הוכחה: כמו בטענת עזר 2, $k_1-k_2=u_1n$ ו- $\ell_1-\ell_2=u_2n$, $u_1,u_2\in\mathbb{Z}$.

אנחנו רוצים להוכיח שההפרש בין המכפלות הוא כפולה של n.

$$k_1\ell_1-k_2\ell_2=(k_2+u_1n)(\ell_2+u_2n)-k_2\ell_2=$$

$$=k_2\ell_2+k_2u_2n+\ell_2u_1n+u_1u_2n^2-k_2\ell_2=$$

$$=(k_2u_2+\ell_2u_1+u_1u_2n)n \Rightarrow k_1\ell_1\equiv(k_2\ell_2)(\mathrm{mod}\ n)$$

משל ☺

<u>טענת עזר 4</u>: $k_1 \equiv k_2 \pmod n$ הוא יחס שקילות.

<u>הערה</u>: יחס שקילות הינו יחס שמקיים: רפלקסיביות
סימטריות
טרנזיטיביות.

<u>הוכחה:</u>

רפלקסיביות: $k_1 \equiv k_1 \pmod n$ כי $k_1 - k_1 = 0 \cdot n$

סימטריות: אם $k_1 \equiv k_2 \pmod n$ אז $k_2 \equiv k_1 \pmod n$ כי
אם $k_1 - k_2 = u n \Leftarrow k_2 - k_1 = (-u) n$.

טרנזיטיביות: אם $k_1 \equiv k_2 \pmod n$ ו-$k_2 \equiv k_3 \pmod n$ אזי

$k_1 - k_2 = u_1 n$ ו- $k_2 - k_3 = u_2 n$ $\Leftarrow$ $k_1 - k_3 = k_1 - k_2 + k_2 - k_3 =$

$= u_1 n + u_2 n = (u_1 + u_2) n$

$\Leftarrow k_1 \equiv k_3 \pmod n$

מש"ל ☺

<u>הוכחת המשפט:</u>

$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$. לפי הגדרה לכל $a, b \in \mathbb{Z}_n$: $a +_n b = [a+b]_n$

$a \cdot_n b = [a \cdot b]_n$

לפי הגדרה, $0 \le [m]_n \le n-1$ $\Leftarrow$ $[m]_n \in \mathbb{Z}_n$ $\Leftarrow$ הפעולות חיבור מודולו n
וכפל מודולו n מקיימות <u>סגירות</u>

החיבור והכפל של השלמים הם קומוטטיביים ולכן

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

$\Leftarrow$ חיבור וכפל מודולו n מקיימים <u>קומוטטיביות</u>

חיבור וכפל בשלמים הם אסוציאטיביים.

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

לפי $(a+b) \equiv [a+b]_n \pmod n$ ו- $c \equiv c \pmod n$ $\Leftarrow$ (לפי 2) $(a+b)+c \equiv ([a+b]_n + c) \pmod n$ $\Leftarrow$ (משפט קודם) $[(a+b)+c]_n = [[a+b]_n + c]_n$

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

Ⓑ 14.11.05
לינארית

שאריות מודולו p

אם $n \geq 1$ יחס שקילות מודולו n . $k, l \in \mathbb{Z}$ $k \equiv l (\mathrm{mod}\, n)$

כאשר $k - l = un$ ו- $u \in \mathbb{Z}$

זה יחס שקילות אם הוא מקיים רפלקסיביות, סימטריות וטרנזיטיביות.

ואכן $k \equiv k (\mathrm{mod}\, n)$

$k \equiv l (\mathrm{mod}\, n) \Rightarrow l \equiv k (\mathrm{mod}\, n)$

$k \equiv l (\mathrm{mod}\, n),\ l \equiv m (\mathrm{mod}\, n) \Rightarrow k \equiv m (\mathrm{mod}\, n)$.

אז מה זה חילוק מודולו n? לכל $m \in \mathbb{Z}$ אפשר למצוא $q, r \in \mathbb{Z}$
כאשר $0 \leq r \leq n-1$ וגם ש- $m = qn + r$.

<u>הגדרה:</u> $[m]_n = r$ - שארית של m מודולו n.

<u>טענה:</u> $k \equiv l (\mathrm{mod}\, n)$ אמ"מ $[k]_n = [l]_n$.

<u>טענת עזר 1:</u> $m = [m]_n (\mathrm{mod}\, n)$

הוכחה: אפשר לרשום $m = qn + r \Rightarrow m = qn + [m]_n \Rightarrow$
$m - [m]_n = qn \Rightarrow m = [m]_n (\mathrm{mod}\, n)$. מש"ל ☺

<u>טענת עזר 2:</u> אם $k_1 \equiv k_2 (\mathrm{mod}\, n)$ ו- $l_1 \equiv l_2 (\mathrm{mod}\, n)$ אז $k_1 + l_1 \equiv (k_2 + l_2)(\mathrm{mod}\, n)$

<u>טענת עזר 3:</u> אם $k_1 \equiv k_2 (\mathrm{mod}\, n)$ ו- $l_1 \equiv l_2 (\mathrm{mod}\, n)$ אז $k_1 l_1 \equiv (k_2 l_2)(\mathrm{mod}\, n)$

נסתכל על הקבוצה $\mathbb{Z}_n = \{0, \ldots, n-1\}$

נגדיר ב- $\mathbb{Z}_n$ חיבור מודולו n וכפל מודולו n.

יהיו $a, b \in \mathbb{Z}_n$ נגדיר <u>חיבור</u>: $a +_n b = [a+b]_n$

<u>כפל</u>: $a \cdot_n b = [ab]_n$

יש לנו קבוצה של איברים ומוגדרות עליה שתי פעולות. זה דורש...

משפט: אם $n>1$ אז $\mathbb{Z}_n$ עם הפעולות של חיבור מודולו n וכפל מודולו n מקיימת את כל האקסיומות של השדה, מלבד אולי קיום איבר הפכי.

* אולי - מה זה אומר? הכוונה היא שאנחנו בכלל לא מתחייבים על התכונה הזאת. לפעמים היא מתקיימת ולפעמים לא. בהמשך נראה שאם n ראשוני אז גם תכונת קיום איבר הפכי מתקיימת.

* $n>1$ - למה? אחת מאקסיומות השדה אומרת ש-$1_F \neq 0_F$ $\Leftarrow$ חייבים להיות לפחות שני איברים בשדה.

הוכחה:

- סגירות של חיבור וכפל מודולו n נובעת מההגדרה.
- קומוטטיביות של חיבור וכפל מודולו n נובעת מקומוטטיביות של חיבור וכפל ב-$\mathbb{Z}$.
- אסוציאטיביות גם נובעת מהאסוציאטיביות ב-$\mathbb{Z}$ אבל צריך לעבוד על זה קצת, בעזרת טענות העזר. ריפרש הראש בפעם הקודמת שזה הולך קצת קשה אז נעשה את זה שוב (עצה חמודה!)

יהיו $a,b,c \in \mathbb{Z}_n$:

$$(a+_n b)+_n c \overset{(1)}{=} [(a+_n b)+c]_n \overset{(1)}{=} [[a+b]_n + c]_n =$$

$$= [(a+b)+c]_n \overset{(2)}{=} [a+(b+c)]_n = [a+[b+c]_n]_n \overset{(1)}{=}$$

$a+b \equiv [a+b]_n \pmod n$	טענת עזר 1.
$c \equiv c \pmod n$	רפלקסיביות
$\Longrightarrow (a+b)+c \equiv ([a+b]_n + c) \pmod n$	טענת עזר 2
$\Longrightarrow [(a+b)+c]_n = [[a+b]_n + c]_n$	הטענה

$$\overset{(1)}{=} [a+(b+_n c)]_n \overset{(1)}{=} a+_n(b+_n c)$$

(1) - הגדרה של חיבור מודולו n

(2) - אסוציאטיביות של חיבור ב-$\mathbb{Z}$

בדיוק באותו האופן מוכיחים את האסוציאטיביות של כפל מודולו n.

① הגדרת הכפל מודולו n
② אסוציאטיביות הכפל ב- $\mathbb{Z}$.

$$(a\cdot_n b)\cdot_n c \overset{①}{=} [(a\cdot_n b)c]_n \overset{①}{=} [[ab]_n c]_n = [(ab)c]_n \overset{②}{=}$$

ab	$\equiv$	$[ab]_n \pmod{n}$	טע' 1
c	$\equiv$	$c \pmod{n}$	רפלקסיביות
$\Rightarrow (ab)c$	$\equiv$	$[ab]_n c \pmod{n}$	טע' 3
$\Rightarrow [(ab)c]_n$	$=$	$[[ab]_n c]_n$	המסקנה

$$\overset{②}{=} [a(bc)]_n = [a[bc]_n]_n \overset{①}{=} [a(b\cdot_n c)]_n \overset{①}{=} a\cdot_n (b\cdot_n c)$$

- חוק הפילוג:

$$a\cdot_n(b+_n c) = [a\cdot(b+_n c)]_n = [a[b+c]_n]_n \overset{\text{טע' 3}}{=} [a(b+c)]_n =$$
$$= [ab+ac]_n \overset{\text{טע' 2}}{=} [[ab]_n+[ac]_n]_n = [a\cdot_n b + a\cdot_n c]_n = (a\cdot_n b)+_n(a\cdot_n c)$$

- קיום איברים ניטרליים: $a+_n 0 = [a+0]_n = [a]_n = a$

$a\cdot_n 1 = [a\cdot 1]_n = [a]_n = a$

- קיום איבר נגדי: אם $a=0 \Leftarrow -_n 0 = 0$

אם $a\neq 0 \Leftarrow -_n a = n-a$

$$a -_n a = a +_n (n-a) = [a+(n-a)]_n = [n]_n = 0$$

מש"ל ☺

דנו בכל האקסיומות מלבד איבר הפכי. ואם ראינו עבור $\mathbb{Z}_4$ שלא היה איבר הפכי ל- 2.

<u>משפט</u>: אם $n>1$ לא ראשוני אז $\mathbb{Z}_n$ איננו שדה.

<u>הוכחה</u>: לפי ההנחה $n=kl$ כאשר $1<k$, $l\leq n-1$ (כי n פריק)

$\Leftarrow k,l\in\mathbb{Z}_n$ $k,l\neq 0,1$. $k\cdot_n l = [kl]_n = [n] = 0$

מצאנו שני איברים שונים מאפס שמכפלתם אפס. אבל בשדה אין מחלקי אפס* וזאת סתירה $\Leftarrow$ $\mathbb{Z}_n$ לא יכול להיות שדה.

מש"ל ☺

* <u>משפט</u>: בשדה F אין מחלקי האפס.

הוכחה: יהיו $a,b\in F$ (F שדה) ו- $a\cdot b=0_F$.

אם $b\neq 0_F$ אז $0_F=0_F\cdot b^{-1}=(ab)b^{-1}=a(bb^{-1})=a\cdot 1_F=a$

כלומר לא יתכן ש- $a\neq 0_F$ ו- $b\neq 0_F$ אבל $ab=0_F$ מש"ל ☺

משפט: אם p ראשוני אז $\mathbb{Z}_p$ שדה.

הוכחה 1: ניקח $0\neq a\in\mathbb{Z}_p$ ונראה כי ל- a יש הפכי ב- $\mathbb{Z}_p$.

לשם רק נתבונן בקבוצת האיברים $A=\{a\cdot_p 0, a\cdot_p 1, a\cdot_p 2,\dots,a\cdot_p(p-1)\}$

נראה כי עבור $k,\ell\in\mathbb{Z}_p$, $k\neq\ell$, $a\cdot_p k\neq a\cdot_p \ell$. נניח בשלילה שדווקא

כן מתקיים $a\cdot_p k=a\cdot_p \ell$. $\Leftarrow$ $[ak]_p=[a\ell]_p$ $\Leftarrow$

$ak\equiv(a\ell)(\text{mod}\,p)$ $\Leftarrow$ $ak-a\ell=u\cdot p$, $u\in\mathbb{Z}$ $\Leftarrow$ $a(k-\ell)=up$.

יש משפט שאומר שאם מספר ראשוני מחלק מכפלה של שני מספרים אז

הוא מחלק לפחות אחד מהם. $\Leftarrow$ p מחלק את $a(k-\ell)$ ולכן

או ש- p מחלק את a או ש- p מחלק את $k-\ell$.

אבל $1\leq k,\ell\leq p-1$ $\Leftarrow$ $-(p-1)\leq k-\ell\leq p-1$ ואם $k-\ell\neq 0$ $\Leftarrow$ $p\nmid k-\ell$.

ואם $1\leq a\leq p-1$ $\Leftarrow$ $p\nmid a$.

וזאת סתירה. $\Leftarrow$ כל האיברים בקבוצה A שונים ויש שם p איברים

$\Leftarrow$ אחד מהאיברים בדיוק הוא 1 $\Leftarrow$ יש הפכי ל- a.

מש"ל ☺

(15) 16.11.05
לינארית

שדה שאריות מודולו p

p מספר ראשוני. $\mathbb{Z}_p = \{0,1,\dots,p-1\}$ הוא שדה עם פעולות

$$a +_p b = [a+b]_p \qquad a \cdot_p b = [ab]_p \qquad a,b \in \mathbb{Z}_p$$

<u>משפט</u>: אם p ראשוני, אז ב-$\mathbb{Z}_p$ קיים הפכי לכל $0 \neq a \in \mathbb{Z}_p$
הוכחנו את המשפט בשיעור הקודם ועשינו שימוש ב-
<u>טענה</u>: אם p ראשוני מחלק את kl אז p מחלק את k או p מחלק את l.
עכשיו נראה הוכחה אחרת למשפט ונשתמש ב
<u>טענה</u>: אם m הוא המחלק המשותף המקסימלי של k ו-l אז קיימים $s,t \in \mathbb{Z}$ כך ש-$s\cdot k + t \cdot l = m$.
<u>הוכחה למשפט</u>: ניקח $0 \neq a \in \mathbb{Z}_p$, כלומר $1 \le a \le p-1$. המחלק המשותף המקסימלי של p ו-a הוא 1 (משום ש-p ראשוני).
לפי הטענה קיימים $s,t \in \mathbb{Z}$ כך ש-$as+pt=1$. כעת

$$a \cdot_p [s]_p = a \cdot_p s \underset{p}{=} [as]_p = [1-pt]_p = [1]_p = 1$$

$\Leftarrow$ $a^{-1} = [s]_p$ ב-$\mathbb{Z}_p$ מש"ל ☺

<u>הוכחת הטענה</u>: באינדוקציה על $k+l$
- בסיס האינדוקציה: עבור $1=k=l$ $\quad 1\cdot 1 + 0 \cdot 1 = 1$
- הנחת האינדוקציה: נעשה אינדוקציה שלמה ונניח לכל k',l' כך ש-$k'+l' < k+l$ קיימים s', t' כך ש-$s'k' + t'l' = m'$.
- שלב האינדוקציה: אם $k=l$ אז $m=k=l$ ואז $1\cdot k + 0 \cdot l = m$.

נניח ש-$k<l$. נשים לב שהמחלק המשותף המקסימלי של k ו-$l-k$ הוא m. קודם כל, m מחלק את k ואת l ולכן מחלק את $l-k$
לכן הוא מחלק משותף של k ו-$l-k$.
אם m' הוא מחלק כלשהו של k ו-$l-k$ אז m' מחלק גם את l
לכן הוא מחלק משותף של k ו-l ולכן $m' \le m$. $\Leftarrow$ m הוא מחלק משותף מקסימלי של k ו-$l-k$.

נשים לב ש $k+(l-k)=l<l+k$ ⇐ ניתן להשתמש
בהנחת האינדוקציה. ⇐ קיימים $s',t'\in\mathbb{Z}$ כך ש
$m = t'(l-k) + s'k = t'l + (s'-t')k$. ניקח $s=s'-t'$
ו- $t=t'$ ונקבל $sk+tl=m$.
אם $l<k$ מסתכלים על l ו- $k-l$ ופועלים באופן דומה.
⇐ לפי עיקרון האינדוקציה הטענה נכונה לכל k ו- l. מש"ל ☺

איזה שדות קיימים בכלל? זו לא שאלה לקורס שלנו.
לומדים על זה בתורת השדות וגם הם לא יודעים לענות
על השאלה. אבל בשדות סופיים דווקא יש משהו...
<u>משפט</u>: לכל p ראשוני ולכל $m\in\mathbb{N}$ יש שדה עם p^m איברים
<u>הוכחה</u>: ר' קורס בתורת השדות.

<u>משפט</u>: אם $1<n\in\mathbb{Z}$ איננו חזקת ראשוני, אין שדה עם n איברים.
<u>דוגמה</u>: אין שדה עם 6 איברים.
<u>הוכחה</u>: בשלב מאוחר יותר של הקורס. (אפשר לנסות בתור תרגיל קשה)

למעשה יש שדה יחיד כזה עד כדי איזומורפיזם.
אם F ו-F' שדות עם p^m איברים אזי קיימת העתקה
$f:F\to F'$ חח"ע ועל כך שלכל $a,b\in F$:

$$f(a)+f(b)=f(a+b)$$
$$f(a)\cdot f(b)=f(ab)$$

יהי F שדה. מגדירים כפל של 1_F ב $n\in\mathbb{N}$ ע"י

$$0\times 1_F=0_F,\ 1\times 1_F=1_F,\ 2\times 1_F=1_F+1_F,\ \ldots$$
$$(-n)\times 1_F=-(n\times 1_F)$$

<u>משפט</u>: כל שדה F קיימת אחת משתי אפשרויות:

(א) לכל $m,n\in\mathbb{Z}$ $m\neq n$ מתקיים $m\times 1_F\neq n\times 1_F$

(ב) קיים ראשוני p רק ש- $p\times 1_F=0_F$

<u>הוכחה</u>: אם (א) מתקיים אז סיימנו. אם לא, (נראה שמתקיים (ב))

קיימים $m,n\in\mathbb{Z}$, $m\neq n$ רק ש- $m\times 1_F=n\times 1_F$. הוכחנו בתרגיל

ש- $(k\times 1_F)+(\ell\times 1_F)=(k+\ell)\times 1_F$. $\Leftarrow$ נניח בה"כ $m<n$ ונקבל

$m\times 1_F+((n-m)\times 1_F)=n\times 1_F=m\times 1_F$ $\Leftarrow$ $(n-m)\times 1_F=0_F$.

נסמן ב- p את המספר החיובי הקטן ביותר רק $p\times 1_F=0_F$.

נוכיח ש- p ראשוני. אם לא אז $p=k\ell$ כאשר $1<k$, $\ell<p$.

ואז $(k\times 1_F)\cdot(\ell\times 1_F)=(k\ell)\times 1_F$ $\Leftarrow$ $(k\ell)\times 1_F=p\times 1_F=0$ אבל $k\times 1_F\neq 0_F$

ו- $\ell\times 1_F\neq 0_F$ בגלל המינימליות של p. וזאת סתירה כי בשדה F

אין מחלקי 0_F $\Leftarrow$ p ראשוני. מש"ל ☺

<u>הגדרה</u>: במקרה (א) כותבים $\text{char}F=0$ שדה עם אפיין 0

במקרה (ב) כותבים $\text{char}F=p$ שדה עם אפיין p

(17) 21.11.05
סנארית

מאפיין של שדה: (characteristic)

יהי F שדה, אז מתקיים אחד מהבאים:

(1) לכל $m,n \in \mathbb{Z}$ .. $m \neq n$ $\quad m\times 1_F \neq n\times 1_F$ (כאשר $m\times 1_F$ = חבור של 1_F עם עצמו m פעמים. אבל $m\cdot 1_F = ERROR$ לאת לא פעולה מוגדרת. x הוא לא כפל בשדה ולכן זה הסימון שלו אחר).

(2) קיים p ראשוני כך ש- $p\times 1_F = 0$.

במקרה (1) אומרים ש $char F = 0$ במקרה (2) $char F = p$

הערה (תרגיל): בשאלה 4 התבקשנו להראות ש $\mathbb{Q} \subseteq F$. לאות טעות חמורה שכן איבר f יכולים להיות לא מספרים בכלל. מה שצריך הוא להראות שקיים $S \subseteq F$ כך ש S איזומורפי ל- $\mathbb{Q}$.

<u>הגדרה</u>: יהיו F ו-S שדות. F ו-S איזומורפיים אם קיימת העתקה חח"ע ועל $f:F\to S$ כך שלכל $a,b\in F$ מתקיים

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

<u>דוגמה</u>: השדה $F=\{z,u\}$ איזומורפי לשדה $\mathbb{Z}_2$ שהפעולות בו מוגדרות ע"י הטבלאות

+	z	u
z	z	u
u	u	z

·	z	u
z	z	z
u	z	u

ברור ש- $char F = char \mathbb{Z}_2 = 2$.

<u>הגדרה</u>: יהי F שדה. ותהי תת קבוצה $K \subseteq F$. K תת שדה של F אם היא מקיימת את אקסיומות השדה ביחס לפעולות המוגדרות של F. כלומר, החבור והכפל של K זהים לחיבור והכפל של F.

<u>דוגמה</u>: $\mathbb{R}$ תת-שדה של $\mathbb{C}$ כאשר מזהים את $a\in\mathbb{R}$ עם $a+0\cdot i \in \mathbb{C}$ וכבר ראינו בעבר שהפעולות מתאימות. נו טוב, (ראה שוב):

$$(a+0\cdot i)+(b+0\cdot i) = (a+b)+(0+0)i = (a+b)+0\cdot i$$
$$(a+0i)\,(b+0i) = (ab-0\cdot 0)+(a\cdot 0+0\cdot b) = (ab)+0\cdot i$$

משפט: אם $charF=p>0$ אז קיים תת שדה K של F איזומורפי ל- $\mathbb{Z}_p$.

הוכחה: נגדיר $K=\{0\times 1_F, 1\times 1_F, \dots, (p-1)\times 1_F\} \subseteq F$ שהרי בעצם

$K=\{0_F, 1_F, 1_F+1_F, \dots, \underbrace{1_F+\dots+1_F}_{p-1 \text{ פעמים}}\}$ ו- F שדה ⇐ יש סגירות ולכן $K\subseteq F$.

נגדיר העתקה $f:\mathbb{Z}_p \to K$ ע"י לכל $a\in\mathbb{Z}_p$ $f(a)=a\times 1_F$.

ברור ש- f היא העתקה על. יהי $k\in K$ ⇐ $k=m\times 1_F$ כאשר $0\le m\le p-1$

⇐ $m\in\mathbb{Z}_p$ ⇐ $f(k)=m\times 1_F=k$. נראה כי f חח"ע. (נניח בשלילה

כי קיימים $0\le k,l\le p-1$, $k<l$ רק ש- $k\times 1_F=l\times 1_F$ ⇐ $k\times 1_F+((l-k)\times 1_F)=l\times 1_F=k\times 1_F$

⇐ $(l-k)\times 1_F=0_F$ (נסמן ב- m את המספר החיובי השלם הקטן ביותר

רק ש $m\times 1_F=0_F$. אז $0<m\le l-k<p$. (נחלק את p ב- m עם

שארית ונקבל $p=qm+r$ כאשר $0\le r<m$. $r\ne 0$ כי p

ראשוני. $charF=p$ ⇐ $p\times 1_F=0_F$. ומצד שני

$$p\times 1_F=(qm+r)\times 1_F=(q(m\times 1_F))+r\times 1_F=q\times 0_F+r\times 1_F=r\times 1_F$$

כי $m\times 1_F=0$ ⇐ $0=r\times 1_F$

וזאת סתירה למינימליות של m. ⇐ f חח"ע.

[* מראה בעצם נובע ש- p הוא המינימלי שמקיים את התכונה הנ"ל, כי לא קיים אחר רק ש- $m\times 1_F=0$.]

איך עושים פעולות על איברי K ? באותו אופן כמו על איברי F.

יהיו $a\times 1_F, b\times 1_F\in K$. ו- $0\le a,b\le p-1$ אזי

$$(a\times 1_F)+(b\times 1_F)=(a+b)\times 1_F=(qp+r)\times 1_F=(q\times(p\times 1_F))+r\times 1_F=$$

$a+b=qp+r$ חילוק עם שארית

$$=q\times 0_F+r\times 1_F=0_F+r\times 1_F=r\times 1_F=[a+b]_p\times 1_F=(a+_p b)\times 1_F$$

הוכחנו שלכל $a,b\in\mathbb{Z}_p$ $(a\times 1_F)+(b\times 1_F)=(a+_p b)\times 1_F$

כלומר, $f(a)+f(b)=f(a+b)$

$$(a\times 1_F)\cdot(b\times 1_F)\underset{\text{פילוג}}{=}a\times(1_F\cdot(b\times 1_F))=a\times(b\times 1_F))=(ab)\times 1_F=$$

$$=(q_1p+r_1)\times 1_F=q_1\times(p\times 1_F))+r_1\times 1_F=q_1\times 0_F+r_1\times 1_F=$$

$ab=q_1p+r_1$

$$=0_F+r\times 1_F=r\times 1_F=[a\cdot b]_p\times 1_F=(a\cdot_p b)\times 1_F$$

⇐ $(a\times 1_F)\cdot(b\times 1_F)=(a\cdot_p b)\times 1_F$ כלומר $f(a)\cdot f(b)=f(a\cdot b)$

⇐ ההעתקה $f:\mathbb{Z}_p\to K$ שומרת על הפעולות חיבור וכפל. ⇐ איזומורפיזם

⇐ מקיימת את אקסיומות השדה ⇐ תת שדה. מש"ל

<u>מסקנה</u>: אם F שדה ו- $\text{char}F=0$ אז קיים תת שדה K של F איזומורפי ל- $\mathbb{Q}$.

<u>הוכחה</u>: לא היום.

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

<u>הוכחה</u>: נגדיר העתקה $g:\mathbb{Q}\to F$ ע"י $g(\frac{m}{n})=(m\times 1_F)(n\times 1_F)^{-1}$

$n\neq 0$ ומשום ש- $charF=0$ מתקיים $n\times 1_F\neq 0_F$. נגדיר $K=g(\mathbb{Q})\subseteq F$

כלומר $a\in K$ אמ"מ קיימים $m,n\in\mathbb{Q}$ כך ש- $g(\frac{m}{n})=a$.

נראה שהעתקה g מוגדרת היטב. כלומר פעולת g על $\frac{m}{n}=\frac{m\ell}{n\ell}$, $n,\ell\neq 0$

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

כדי להראות ש- $g:\mathbb{Q}\to F$ אכן מוגדרת היטב, צריך לבדוק כי

$$(m\times 1_F)(n\times 1_F)^{-1}=((m\ell)\times 1_F)((n\ell)\times 1_F)^{-1}.$$

נשתמש בתכונה: לכל $k,\ell\in\mathbb{Z}$: $(k\ell)\times 1_F=k\times(\ell\times 1_F)$

עבור $k,\ell>0$:

$$(k\ell)\times 1_F=\underbrace{1_F+\dots+1_F}_{k\ell\text{ פעמים}}=\underbrace{\underbrace{1_F+\dots+1_F}_{\ell\text{ פעמים}}+\dots+\underbrace{1_F+\dots+1_F}_{\ell\text{ פעמים}}}_{k\text{ פעמים}}=k\times(\ell\times 1_F)$$

תרגיל: להשלים את הטענה עבור כל $k\ell\in\mathbb{Z}$.

לכן:

$$(m\ell)\times 1_F=(\ell m)\times 1_F=\ell\times(m\times 1_F)=(\ell\times 1_F)(m\times 1_F)$$

$$(n\ell)\times 1_F=(\ell n)\times 1_F=\ell\times(n\times 1_F)=(\ell\times 1_F)(n\times 1_F)$$

$$\Rightarrow ((m\ell)\times 1_F)((n\ell)\times 1_F)^{-1}=\big((\ell\times 1_F)(m\times 1_F)\big)\big((\ell\times 1_F)(n\times 1_F)\big)^{-1}=$$

$$=\big((\ell\times 1_F)(m\times 1_F)\big)\big((\ell\times 1_F)^{-1}(n\times 1_F)^{-1}\big)=(\ell\times 1_F)(\ell\times 1_F)^{-1}(m\times 1_F)(n\times 1_F)=$$

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

⇐ g מוגדרת היטב.

נבדוק את g שומרת על הפעולות. יהיו $\frac{m}{n},\frac{s}{t}\in\mathbb{Q}$, $n,t\neq 0$

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

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

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

$$=((mt)\times 1_F+(ns)\times 1_F)((nt)\times 1_F)^{-1}=((mt)\times 1_F)((nt)\times 1_F)^{-1}+((ns)\times 1_F)((nt)\times 1_F)^{-1}=$$

$$=g\left(\frac{mt}{nt}\right)+g\left(\frac{ns}{nt}\right)=g\left(\frac{m}{n}\right)+g\left(\frac{s}{t}\right)$$

⇐ g שומרת על פעולות חיבור וכפל.

נראה ש-g הפיכה:

חח"ע: יהיו $\frac{m}{n}, \frac{s}{t} \in \mathbb{Q}$, $t,n \neq 0$ ונניח ש- $g(\frac{m}{n}) = g(\frac{s}{t})$. נראה ש- $\frac{m}{n} = \frac{s}{t}$. ואכן,

$$\left.\begin{aligned} g\left(\frac{m}{n}\right) &= g\left(\frac{mt}{nt}\right) = ((mt)\times 1_F)((nt)\times 1_F)^{-1} \\ g\left(\frac{s}{t}\right) &= g\left(\frac{ns}{nt}\right) = ((ns)\times 1_F)((nt)\times 1_F)^{-1} \end{aligned}\right\} \Rightarrow ((mt)\times 1_F) = ((ns)\times 1_F)$$

אבל $\mathrm{char}F = 0$ ⇐ $mt = ns$ ⇐ $\frac{m}{n} = \frac{s}{t}$. ⇐ g חח"ע

על: כל נכון לפי ההגדרה, שהרי הגדרנו $K = g(\mathbb{Q})$.

⇐ g שומרת על חיבור וכפל והיא חח"ע ועל. לכן K איזומורפי

ל-$\mathbb{Q}$ והוא תת שדה של F , כנדרש. מש"ל ☺

תם פרק "שדות" מקורס אלגברה לינארית

משוואות לינאריות

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{cases}$$

מע' של m משוואות לינאריות
ב-n נעלמים $x_1,\dots,x_n$
עם מקדמים a_{ij} ואיברים
חפשיים b_i.

אבל מאיפה הבאנו את המקדמים והאיברים החופשיים? הם שייכים לאיזשהו שדה F, כלומר $a_{ij}, b_i \in F$.
ואז גם את הפתרונות למשוואות נחפש גם כן ב-F נמצא $x_1,\dots,x_n \in F$ כך שאם נציב אותם במשוואות נקבל זהויות אמיתיות.
אבל לא תמיד יש פתרונות כאלה.

אז יש כמה אופציות:
א) אין פתרונות בכלל
ב) יש פתרון יחיד
ג) יש הרבה פתרונות

אפשר לפתור מע' משוואות גם ללא פיתוח של שיטות מתקדמות.
<u>חילוץ משתנים</u>: נשתמש באחת המשוואות כדי לבטא את אחד הנעלמים דרך שאר הנעלמים. נציב אותו בכל שאר המשוואות. מקבלים מע' עם פחות נעלמים וממשיכים בחילוץ משתנים. בסוף או שמגיעים למשוואה עם פתרון או למשוואה שאין לה פתרון, ואז זה אומר שמלכתחילה למע' המשוואות לא היה פתרון.

<u>דוגמה</u>: $F=\{u,z\}$

$$ux + zy + ut = u$$

(המשתנים: x,y,t; המקדמים: u,z,u)

+	z	u
z	z	u
u	u	z

$$ux = u - zy - ut = u + ut$$

$$\Rightarrow x = u^{-1}(u+ut) = u + ut$$

·	z	u
z	z	z
u	z	u

ולכן אפשר לתת ל-y,t ערכים שרירותיים, כי אין לנו מגבלות עליהם.

(1) $t=z \quad y=z \quad \Leftarrow \quad x=u$

(2) $t=u \quad y=z \quad \Leftarrow \quad x=z$

(3) $t=z \quad y=u \quad \Leftarrow \quad x=u$

(4) $t=u \quad y=u \quad \Leftarrow \quad x=z$

קיבלנו 4 פתרונות שונים.

(נבדוק למשל ש-(1) הוא פיתרון:

המשוואה $ux+zy+ut=u$

נציב (u,z,z)

$u\cdot u+z\cdot z+u\cdot z=$

$=u+z+z=u$

$\Leftarrow$ אכן (1) הוא פתרון.

באותו אופן אפשר לבדוק לגבי שאר הפתרונות.

מרחבים וקטוריים

הגדרה יהי שדה F. מרחב וקטורי V מעל שדה F הוא קבוצה של איברים (שנקרא להם וקטורים) שמוגדרות עליה פעולות של חיבור וקטורים ושל כפל של וקטור באיברי F (שנקרא להם סקלרים), כך שמתקיימות האקסיומות של מרחב וקטורי: לכל $u,v,w\in V$ ו-$a,b\in F$

<u>חיבור וקטורים</u>

(א) סגירות $u+v\in V$

(ב) קומוטטיביות $u+v=v+u$

(ג) אסוציאטיביות $(u+v)+w=u+(v+w)$

(ד) קיום איבר נטרלי לחיבור $v+0_v=v$

(ה) קיום איבר נגדי לחיבור $v+(-v)=0_v$

<u>כפל בסקלר</u>

(א) סגירות $av\in V$
(הכפל מוגדר תמיד מצד שמאל) $va=ERROR$

(ב) $1_F\cdot v=v$

(ג) $(ab)v=a(bv)$

(ד) $(a+b)v=av+bv$

(ה) $a(u+v)=au+av$

(21)

28.11.05
סמינריון

מרחבים וקטוריים ☺

F שדה. מרחב וקטורי V מעל שדה F (שאיבריו יקראו "סקלרים") הוא:
קבוצה (שאיבריה יקראו "וקטורים") שעליה
מוגדרת פעולה של חיבור וקטורים ושל כפל וקטור בסקלרים
כך שמתקיימות האקסיומות של מרחב וקטורי

אקסיומות המרחב הוקטורי: לכל $u,v,w\in V$ ו- $a,b\in F$:

חיבור	כפל בסקלר
$u+v\in V$	$av\in V$
$(u+v)+w=u+(v+w)$	$1_F v=v$
$u+v=v+u$	$(ab)v=a(bv)$
$\exists 0_v\in V\ \ 0_v+v=v$	$(a+b)v=av+bv$
$\exists -v\in V:\ v+(-v)=0_v$	$a(u+v)=au+av$

דוגמה מאוד יסודית של מרחב וקטורי (לא כל המרחבים הוקטוריים הם כאלה.
יש טיפוסים אחרים של מרחבים וקטוריים).
נקבע שדה F ונקבע $n\geq 1$ מספר שלם. נגדיר קבוצה:
$$F^n=\{(a_1,a_2,\dots,a_n): a_i\in F\ \ 1\leq i\leq n\}$$
כלומר F^n זו קבוצה של סדרות באורך n של איברי שדה F.
נגדיר חיבור של איברי F^n וכפל של איברי F^n באיברי F:
$$(a_1,\dots,a_n)+(b_1,\dots,b_n)\equiv(a_1+b_1,\dots,a_n+b_n)$$
$$c\in F \quad c(a_1,\dots,a_n)\equiv(ca_1,\dots,ca_n)$$
אם נראה שכל האקסיומות מתקיימות אז F^n הוא מ"ו מעל F.
<u>חיבור:</u>
סגירות - זה מובן כי קיבלנו n-יה ו F שדה אז $a_i+b_i\in F$
קומוטטיביות - $(a_1+\dots+a_n)+(b_1,\dots,b_n)=(a_1+b_1,\dots,a_n+b_n)=$
$$\underset{\text{קומוטטיביות } F}{=}(b_1+a_1,\dots,b_n+a_n)=(b_1,\dots,b_n)+(a_1,\dots,a_n)$$
אסוציאטיביות -
$$((a_1,\dots,a_n)+(b_1,\dots,b_n))+(c_1,\dots,c_n)=(a_1+b_1,\dots,a_n+b_n)+(c_1,\dots,c_n)=$$
$$=((a_1+b_1)+c_1,\dots,(a_n+b_n)+c_n)\underset{\text{אסוציאטיביות של } F}{=}(a_1+(b_1+c_1),\dots,a_n+(b_n+c_n))=$$
$$=(a_1,\dots,a_n)+(b_1+c_1,\dots,b_n+c_n)=(a_1,\dots,a_n)+((b_1,\dots,b_n)+(c_1,\dots,c_n))$$

קיום אפס 0_{F^n}. נסמן $0_{F^n}=(0_F,\dots,0_F)$ ואכן

$$(a_1,\dots,a_n)+(0_F,\dots,0_F)=(a_1+0_F,\dots,a_n+0_F)=(a_1,\dots,a_n)$$

קיום נגדי. נסמן $-(a_1,\dots,a_n)=(-a_1,\dots,-a_n)$ ואכן

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

<u>כפל בסקלר</u>

סגירות – טריוויאלי, קיבלנו n-יה ו- $ca_i\in F$ $\Leftarrow$ $(ca_1,\dots,ca_n)\in V$

קיום יחידה – $1_{F^n}=(1_F,\dots,1_F)$ ואכן $1_F(a_1,\dots,a_n)=(1_Fa_1,\dots,1_Fa_n)=(a_1,\dots,a_n)$

"אסוציאטיביות" – $(ab)(a_1,\dots,a_n)=((ab)a_1,\dots,(ab)a_n)=$
$$=(a(ba_1),\dots,a(ba_n))=a(ba_1,\dots,ba_n)=a(b(a_1,\dots,a_n))$$

"דיסטריבוטיביות" – $(a+b)(c_1,\dots,c_n)=((a+b)c_1,\dots,(a+b)c_n)=$
$$=(ac_1+bc_1,\dots,ac_n+bc_n)=(ac_1,\dots,ac_n)+(bc_1,\dots,bc_n)=$$
$$=a(c_1,\dots,c_n)+b(c_1,\dots,c_n)$$
$$a((b_1,\dots,b_n)+(c_1,\dots,c_n))=a(b_1+c_1,\dots,b_n+c_n)=$$
$$=(a(b_1+c_1),\dots,a(b_n+c_n))=(ab_1+ac_1,\dots,ab_n+ac_n)=$$
$$=(ab_1,\dots,ab_n)+(ac_1,\dots,ac_n)=a(b_1,\dots,b_n)+a(c_1,\dots,c_n)$$

ראינו שכל אקסיומות המרחב הוקטורי מתקיימות.

$\Leftarrow$ F^n מרחב וקטורי מעל F. ☺

מקרה פרטי שבו $n=2$ נקבל $F^2=\{(a_1,a_2): a_1,a_2\in F\}$

$$(a_1,a_2)+(b_1,b_2)=(a_1+b_1,a_2+b_2)$$
$$c(a_1,a_2)=(ca_1,ca_2)$$

מקרה פרטי שבו $n=1$ נקבל $F^1=\{(a): a\in F\}$

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

$F\neq F^1$!! F^1 הוא מרחב וקטורי של סדרות באורך 1!

מקרה פרטי שבו $n=0$ נקבל $F^0=\{()\}$

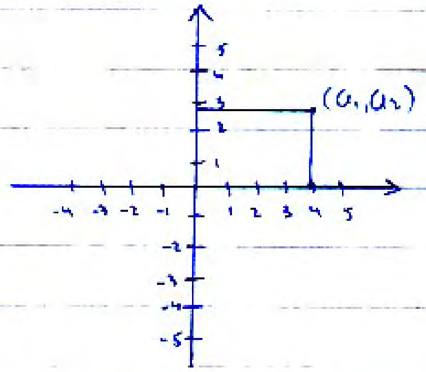
$0_{F^n}=()$ $\Leftarrow$ $()+()=()$

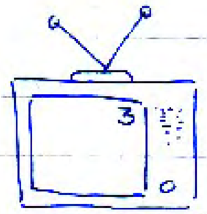
$$c()=()$$

רון ריפט נקרע מצחוק :)

נסתכל במקרה פרטי $n=2$ ו- $F=\mathbb{R}$, כלומר $V=\mathbb{R}^2$.
הוכחנו שזה מרחב וקטורי (אפיר מוד) גיאומטרי של $\mathbb{R}^2$:

לכל וקטור ב- $\mathbb{R}^2$ מתאימה נקודה אחת במישור עם קואורדינטות (a_1,a_2).

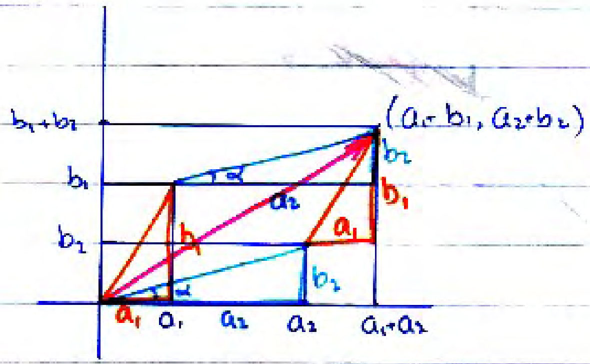




כיצד הפעולות ב $\mathbb{R}^2$ משתקפות במובן הגיאומטרי:
כל זאת ועוד אחרי הפרסומות...

חיבור $(a_1,a_2)+(b_1,b_2)=(a_1+b_1,\ a_2+b_2)$

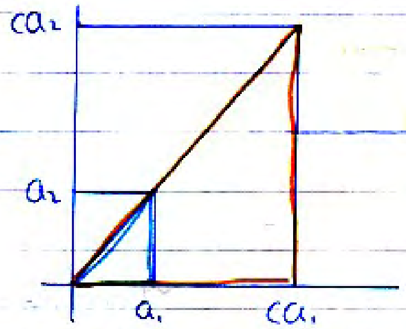
אפשר לחבר את הריבועים או להשתמש בכלל המקבילית.



כלל המקבילית: בונים מקבילית שקודקוד אחד שלה $(0,0)$ ושני הקודקודים האחרים הם (a_1,a_2) ו- (b_1,b_2) ואז הקודקוד הרביעי הוא (a_1+b_1,a_2+b_2) (זה מקור השם מקבילית הכוחות בפיסיקה).

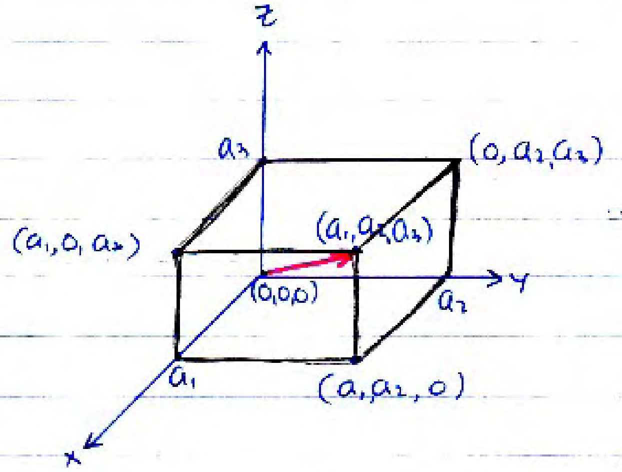
כפל: $c(a_1,a_2)=(ca_1,ca_2)$

קיבלנו משולשים דומים כי הזווית ישרה בשניהם והצלעות הן פרופורציוניות. על כן הזווית של השיפוע היא אותה זווית
$\Leftarrow$ (a_1,a_2) ו- (ca_1,ca_2) על אותו ישר עם ראשית הצירים $(0,0)$



לא דנו כאן בכל המקרים. לדוגמה יש מקרים מנוונים ש (a_1,a_2) ו- (b_1,b_2) על אותו ישר או ש- $c<0$. אבל כל המקרים נעשים בצורה דומה.

נסתכל ב- $\mathbb{R}^3$. ניקח מע' צירים במרחב.



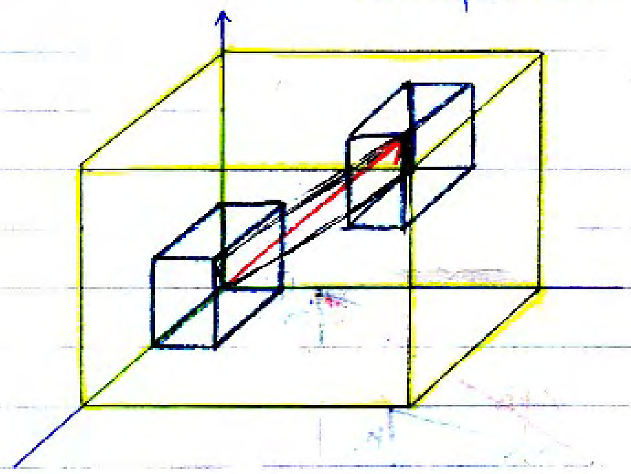
ל-(a_1,a_2,a_3) מתאימה נקודה במרחב עם קואורדינטות (a_1,a_2,a_3)

[xy] - מישור xy - המקום הגאומטרי של כל הנקודות שבהן הקואורדינטה השלישית היא 0. באותו אופן

[xz] - מישור xz איפה ש- $y=0$

[yz] - מישור yz איפה ש- $x=0$.

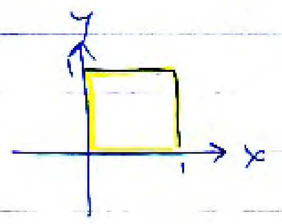
גם ב- $\mathbb{R}^3$ עושים חיבור ע"י כלל המקבילית.



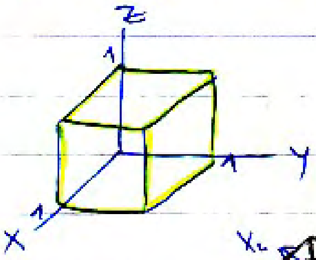
מעבירים את הקטעים כך שקודקודים שלהן יתלכדו ואז משתמשים בכלל המקבילית.

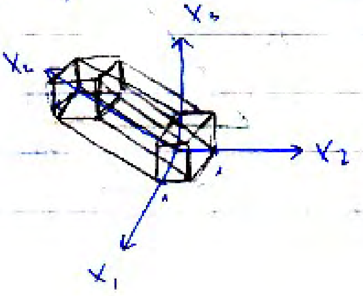
קטע היחידה ב- $\mathbb{R}^1$: $I_1=\{(a_1): 0\le a_1\le 1\}$

ריבוע היחידה ב- $\mathbb{R}^2$: $I_2=\{(a_1,a_2): 0\le a_1,a_2\le 1\}$



קוביית היחידה ב- $\mathbb{R}^3$: $I_3=\{(a_1,a_2,a_3): 0\le a_1,a_2,a_3\le 1\}$





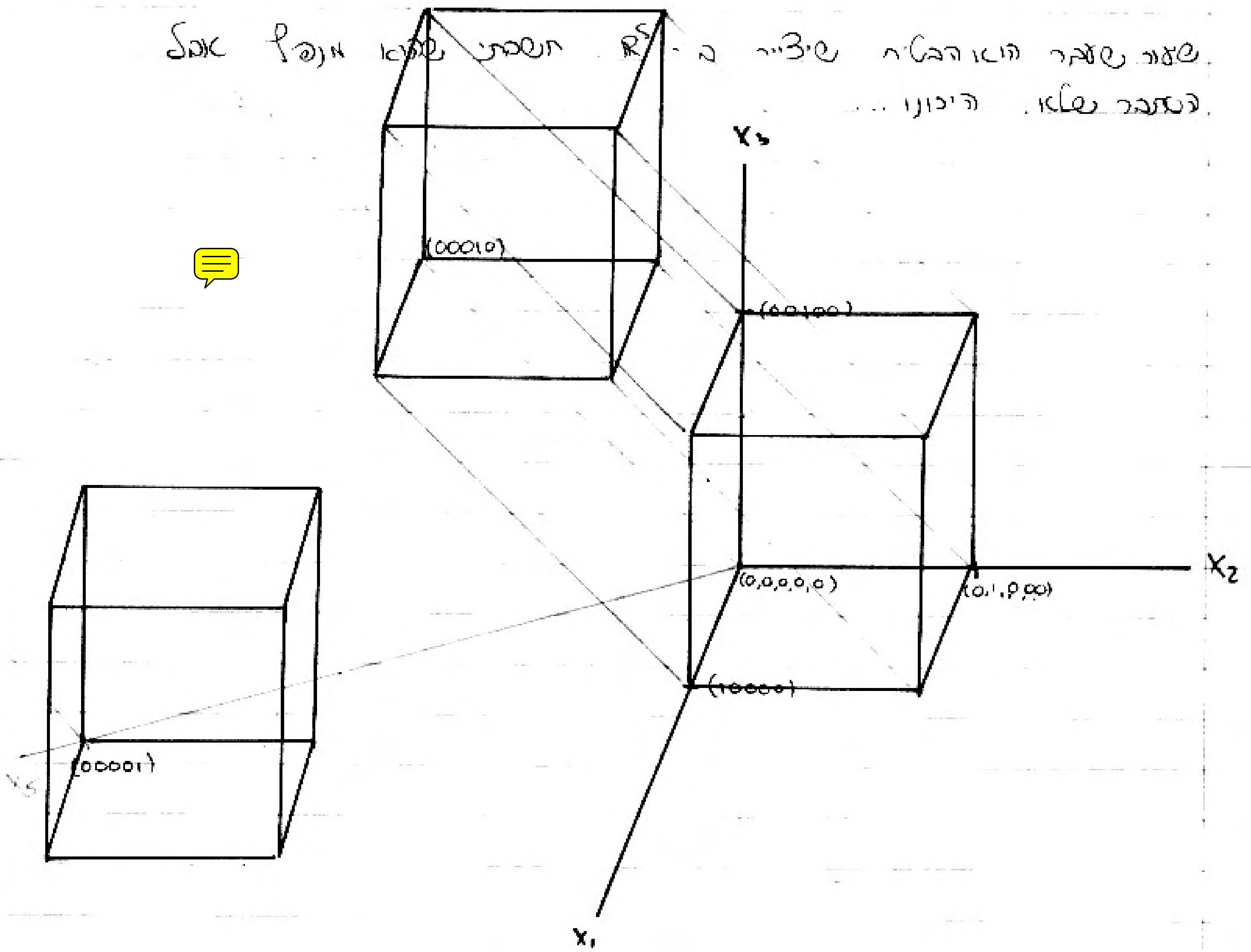
ב- $\mathbb{R}^4$ נגדיר $I_4=\{(a_1,a_2,a_3,a_4): 0\le a_i\le 1\}$:

פעם הבאה $\mathbb{R}^5$!

30.11.05

לינארית

שעור שעבר הובטח שיצייר ב- $\mathbb{R}^5$. חשבתי שהוא מגזים? אבל מסתבר שלא. הינהו...



כמה קודקודים יש לקוביה במימד n? - 2^n.

כמה פרטים (קודקודים, פאות, צלעות וקוביה) יש לקוביה ממימד n? - 3^n

למשל ב $\mathbb{R}^4$:

16	קודקודים
32	צלעות
24	פאות
8	קוביות תלת מימדיות
1	קוביה 4 - מימדית
$81=3^4$	פרטים

(ל-8 הקוביות התלת מימדיות:) 1 למעלה + 1 למטה. לכל 6 פאות של התחתונה הן מתחברות לפאות של העליונה ויוצרות 6 קוביות

למשל ב-$\mathbb{R}^5$:

32 קודקודים
80 צלעות
80 פאות
40 קוביות תלת מימדיות
10 קוביות 4-מימדיות
1 קוביה 5 מימדית

$243 = 3^5$ פרטים

אפשר לסדר את התוצאות ככה:

$$
\begin{array}{cccccc}
 & & & & & 1 \\
 & & & & 2 & 1 \\
 & & & 4 & 4 & 1 \\
 & & 8 & 12 & 6 & 1 \\
 & 16 & 32 & 24 & 8 & 1 \\
32 & 80 & 80 & 40 & 10 & 1
\end{array}
$$

32	80	80	40	10	1
↑	↑	↑	↑	↑	↑
קוביה ב $\mathbb{R}^0$	קוביה ב $\mathbb{R}^1$	קוביה ב $\mathbb{R}^2$	קוביה ב $\mathbb{R}^3$	קוביה ב $\mathbb{R}^4$	קוביה ב $\mathbb{R}^5$

נסמן ב (n,k) את האיבר שבשורה ה-n ובמקום ה-k (משמאל).
אפשר לרשום את החוקיות של המשולש הזה באופן הבא:

$$(n,k)+2(n,k+1) = (n+1,k+1)$$

את המשולש הזה אפשר לקבל בקלות ממשולש פסקל.

$1 = 1\cdot 1$

$2 = 2\cdot 1 \qquad 1 = 1\cdot 1$

$4 = 4\cdot 1 \qquad 4 = 2\cdot 2 \qquad 1 = 1\cdot 1$

$8 = 8\cdot 1 \qquad 12 = 4\cdot 3 \qquad 6 = 2\cdot 3 \qquad 1 = 1\cdot 1$

$16 = 16\cdot 1 \qquad 32 = 8\cdot 4 \qquad 24 = 4\cdot 6 \qquad 8 = 2\cdot 4 \qquad 1 = 1\cdot 1$

$32 = 32\cdot 1 \qquad 80 = 16\cdot 5 \qquad 80 = 8\cdot 10 \qquad 40 = 4\cdot 10 \qquad 10 = 2\cdot 5 \qquad 1$

המספרים בכחול הם המספרים ממשולש פסקל הרגיל
המספרים בורוד הם חזקות של 2

זה היה הקדמה קלה לגיאומטריה n-מימדית.

תלות לינארית של וקטורים

F שדה, V מרחב וקטורי מעל F ו- $v_1,\dots,v_n \in V$

<u>הגדרה</u>: הוקטורים $v_1,\dots,v_n \in V$ נקראים <u>תלויים לינארית</u> אם קיימים סקלרים $c_1,\dots,c_n \in F$ <u>לא כולם</u> 0_F כך ש- $\sum_{i=1}^{n} c_i v_i = 0_V$
אחרת, $v_1,\dots,v_n$ נקראים בלתי תלויים לינארית (בת"ל)

* הערה/הבהרה: <u>אסור</u> שכל ה- c_i יהיו 0_F. לפחות אחד שונה מ- 0_F.

עבור $n=1$ ו- $v_1 \in V$

אם $v_1 = 0_V$ אז $1_F \cdot v_1 = 0_V$, לכן יש תלות לינארית.

אם $v_1 \neq 0_V$ אז לכל $c_1 \in F$ $c_1 \neq 0_F$ מתקיים $c_1 v_1 \neq 0_V$.

למה זה נכון? אחרת $c_1 v_1 = 0_V$ ומכאן - $0_V = c_1^{-1} \cdot 0_V$
אז $v_1 = c_1^{-1}(c_1 v_1)$

ו- $c_1^{-1} \cdot 0_V = c_1^{-1} c_1 v_1 \Rightarrow 0_V = v_1$ וזאת סתירה.

$\Leftarrow$ אין תלות.

אז עבור וקטור אחד המצב מאוד פשוט: אם הוקטור הוא וקטור האפס אז יש תלות, אחרת הוקטור בת"ל.

עבור $n=2$ ו- $v_1,v_2 \in V$.

v_1,v_2 תלויים לינארית כאשר קיים $c_1,c_2 \in F$ לא כולם 0_F כך ש $c_1v_1+c_2v_2=0_V$. יש כמה מקרים:

א) אם $c_1 \neq 0_F$ אז $c_1v_1=-c_2v_2$ ⟸

$$v_1=1_F v_1=(c_1^{-1}c_1)v_1=c_1^{-1}(c_1v_1)=c_1^{-1}(-c_2v_2)=(-c_1^{-1}c_2)v_2$$

כלומר v_1 הוא כפולה סקלרית של v_2

ב) אם $c_2 \neq 0_F$ אז $c_2v_2=-c_1v_1$ ⟸

$$v_2=1_F v_2=(c_2^{-1}c_2)v_2=c_2^{-1}(c_2v_2)=c_2^{-1}(-c_1v_1)=(-c_2^{-1}c_1)v_1$$

כלומר v_2 הוא כפולה סקלרית של v_1

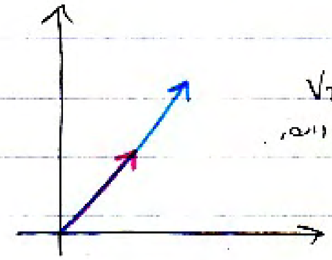
מסקנה: עבור $n=2$ שני וקטורים הם תלויים לינארית אם"ם אחד מהם הוא כפולה סקלרית של השני. כלומר כאשר v_1 הוא כפולה סקלרית של v_2 או v_2 הוא כפולה סקלרית של v_1.

אחרת, v_1, v_2 הם בת"ל.

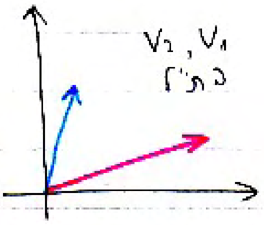
זה נכון לכל מרחב וקטורי בלי קשר לשדה.

מה המשמעות של ההגדרה הזאת באופן הגיאומטרי?

נסתכל על R^2:



אם v_1 ו- v_2 נמצאים על אותו ישר העובר דרך הראשית, אז הם תלויים לינארית. אחרת v_1, v_2 בת"ל.



ב- R^3 המצב דומה. אם הוקטורים נמצאים על אותו ישר אז הם תלויים. אחרת הם בת"ל.

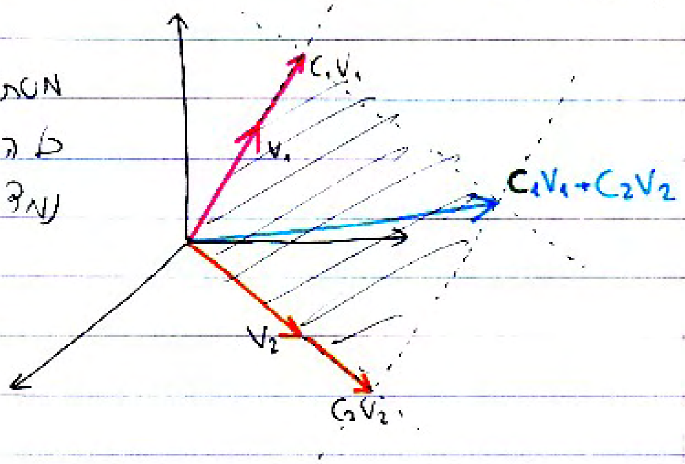
מה קורה כאשר יש 3 וקטורים? קיימים c_1,c_2,c_3 לא כולם אפס כך ש $\sum_{i=1}^{3} c_iv_i=0_V$

אם
- $c_1 \neq 0_F$: $v_1=(-c_1^{-1}c_2)v_2+(-c_1^{-1}c_3)v_3$
- $c_2 \neq 0_F$: $v_2=(-c_2^{-1}c_1)v_1+(-c_2^{-1}c_3)v_3$
- $c_3 \neq 0_F$: $v_3=(-c_3^{-1}c_1)v_1+(-c_3^{-1}c_2)v_2$

אחד מהוקטורים הוא צירוף לינארי של השניים האחרים. אחרת, v_1, v_2, v_3 הם בת"ל.

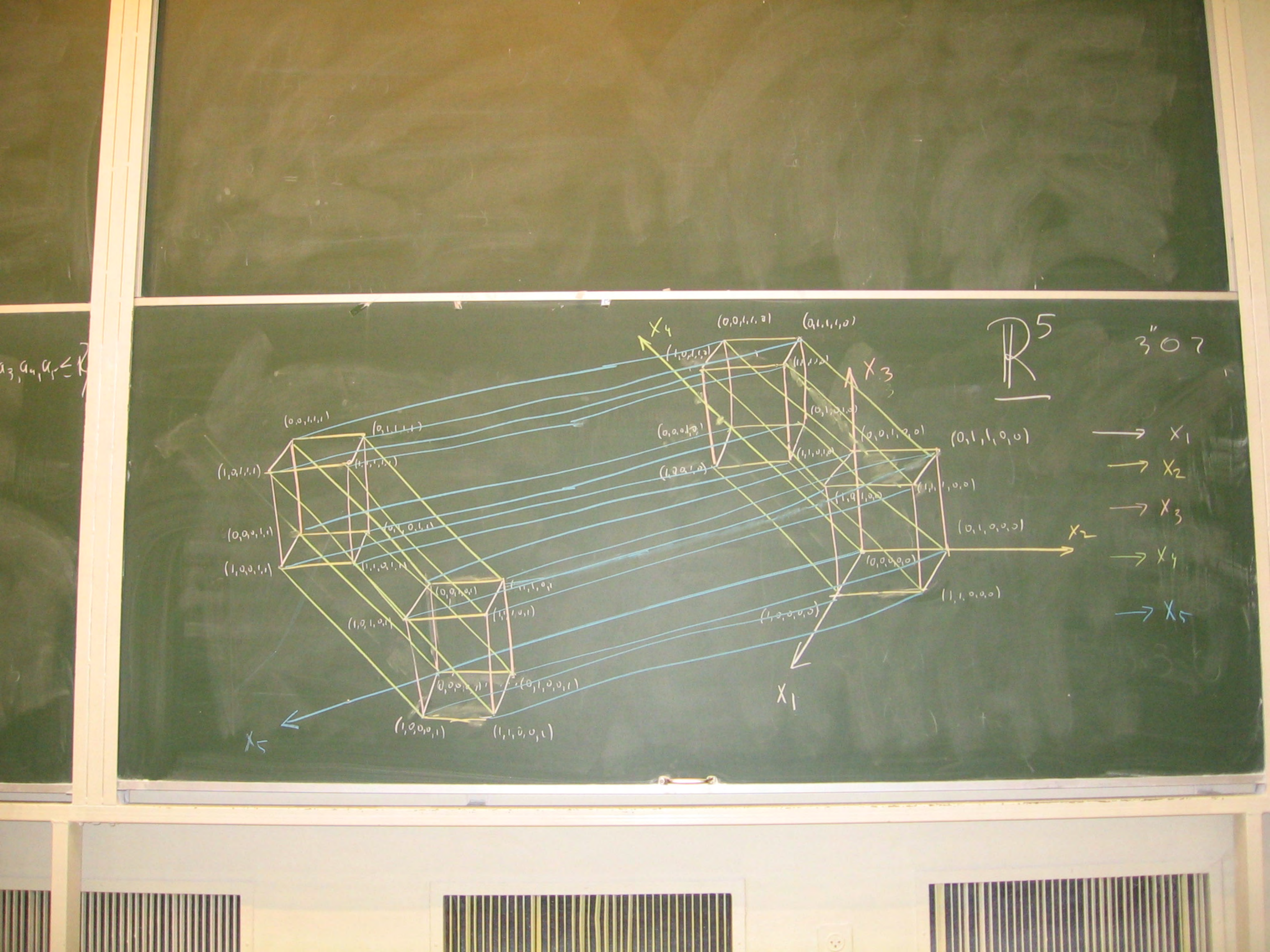
<u>הגדרה</u>: יהיו $u_1,\dots,u_k \in U$, U מרחב וקטורי מעל F ויהיו $F \ni a_1,\dots,a_k$. $\sum_{i=1}^{k} a_i u_i$ נקרא צירוף לינארי של $u_1,\dots,u_k$ עם מקדמים $a_1,\dots,a_k$.

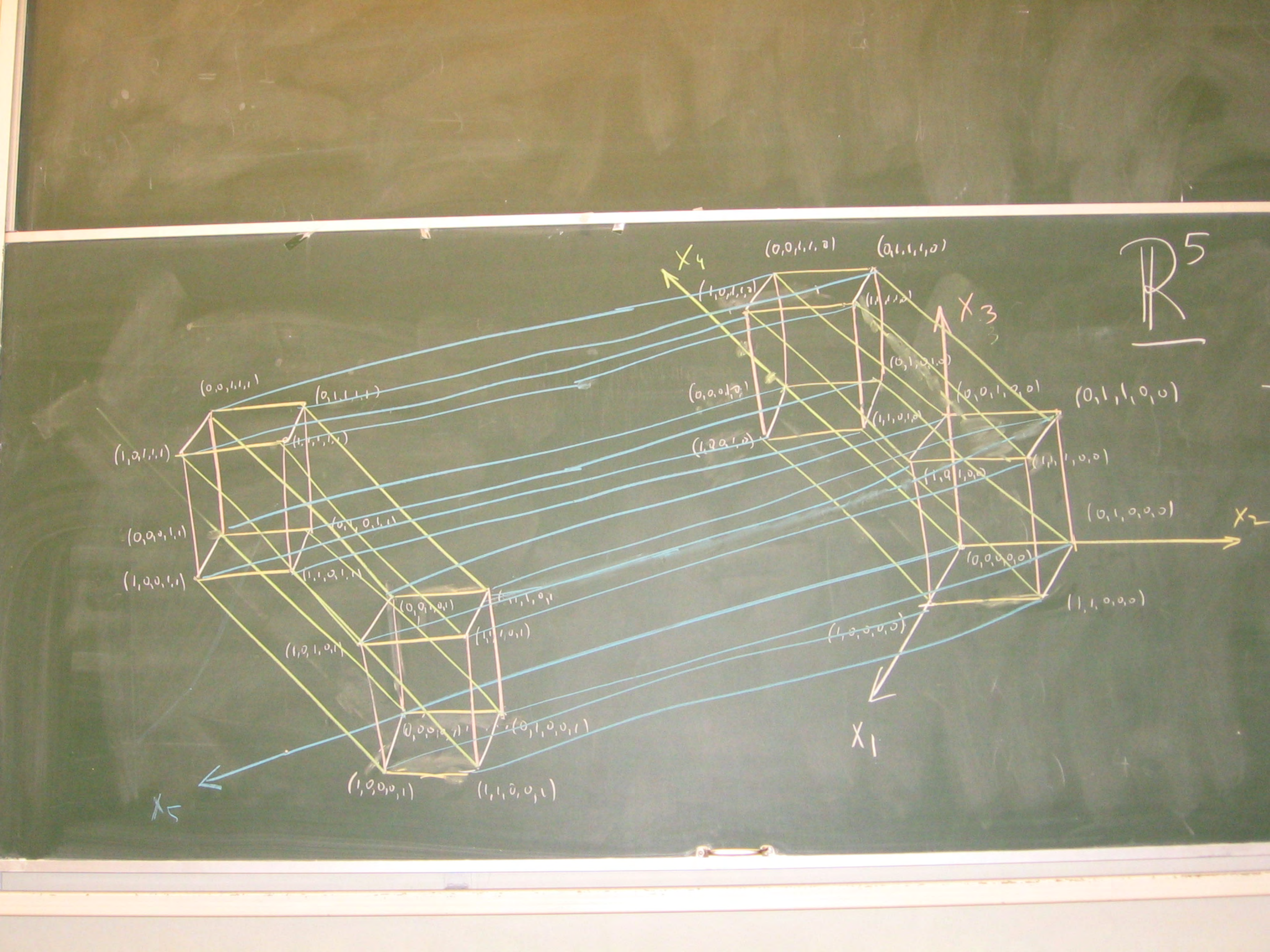
נסתכל על $\mathbb{R}^3$:



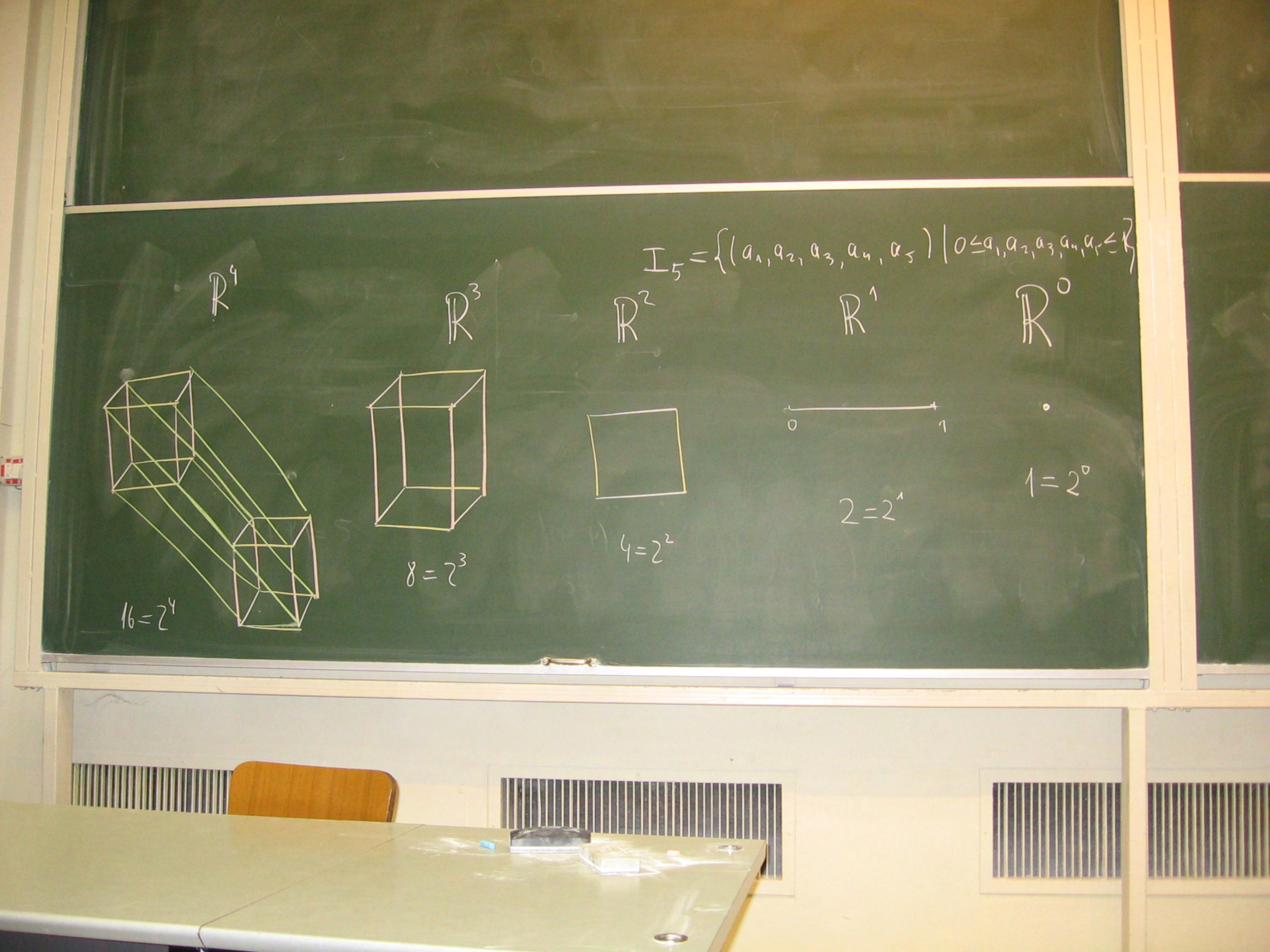
מסתכלים על המישור שנפרש ע"י v_1, v_2 וע"י כל הצירופים הלינאריים של v_1 ו-v_2 נמצאים על המישור הזה.

$\Leftarrow$ 3 וקטורים ב-$\mathbb{R}^3$ שלא נמצאים (הסבר בדף הראשון) באותו מישור הם בת"ל.


R5
3"07
X1
X2
X3
X4
X5
(0,1,1,0,0)
(0,1,0,0,0)
(1,1,0,0,0)
(1,0,0,0,1)
(1,1,0,0,1)
(0,1,0,0,1)
(0,0,1,1,1)
(1,0,0,1,1)



R5
X4
X3
X2
X1
X5
(0,0,1,1,0)
(0,1,1,1,0)
(0,0,1,1,1)
(0,1,1,1,1)
(1,0,1,1,1)
(0,0,0,1,1)
(1,0,0,1,1)
(0,0,1,0,0)
(0,1,1,0,0)
(1,1,1,0,0)
(0,1,0,0,0)
(0,0,0,0,0)
(1,1,0,0,0)
(1,0,0,0,0)
(1,0,1,0,1)
(0,1,0,0,1)
(1,0,0,0,1)
(1,1,0,0,1)



$I_5 = \{(a_1, a_2, a_3, a_4, a_5) \mid 0 \le a_1, a_2, a_3, a_4, a_5 \le 1\}$
$\mathbb{R}^4$
$\mathbb{R}^3$
$\mathbb{R}^2$
$\mathbb{R}^1$
$\mathbb{R}^0$
0
1
$16 = 2^4$
$8 = 2^3$
$4 = 2^2$
$2 = 2^1$
$1 = 2^0$

(26) 5.12.05

לינארית

תלות ואי תלות של וקטורים

באופן מפתיע אנחנו אמש מאחרים בחומר לעומת הקבוצה השניה אז מעכשיו נמהר קצת יותר (נקווה, מבטח).

נזכר מה זה תלות של וקטורים:

F שדה, V מ"ו מעל F. $v_1,\dots,v_n\in V$ נקראים __תלויים לינארית__ אמ"מ קיימים סקלרים $c_1,\dots,c_n\in F$ __לא כולם__ 0_F כך ש- $\sum_{i=1}^{n} c_iv_i=0_V$.

__משפט:__ $m\ge 0$ ו- $v_1,\dots,v_n\in F^m$, $n>m$ אז $v_1,\dots,v_n$ תלויים לינארית.

__הערה:__ באופן כללי זה לא נכון שוקטורים ב- F^m הם תלויים לינארית. לדוגמא $(0,1),(1,0)\in\mathbb{R}^2$ הם בת"ל. אבל אם לוקחים יותר מ- m וקטורים אז הם תמיד תלויים.

__תזכורת:__ $F^m=\{(a_1,\dots,a_m) : a_i\in F, 1\le i\le m\}$

$(a_1,\dots,a_m)+(b_1,\dots,b_m)=(a_1+b_1,\dots,a_m+b_m)$

$c\in F \quad c(a_1,\dots,a_m)=(ca_1,\dots,ca_m)$

__הסבר:__ המשפט אומר שלא משנה מה הוקטורים. אם יש יותר מ- m וקטורים אז הם חייבים להיות תלויים לינארית.

__הוכחה:__ באינדוקציה על m.

המקרה הראשון שיש להסתכל בו הוא $m=0$. $F^0=\{()\}$. יהי $n>0$ ו- $v_1,\dots,v_n\in F^0$. ברור ש- $v_1=\dots=v_n=()$ (כי יש רק איבר אחד בלבד ב- F) $\Leftarrow$ $1_Fv_1+\dots+1_Fv_n=()+\dots+()=()=0_{F^0}$ $\Leftarrow$ $v_1,\dots,v_n$ תלויים לינארית. כי קיבלנו צירוף לינארי עם מקדמים לא כולם (ובעצם אף אחד) אפס וזאת ההגדרה של תלות לינארית.

נניח שהטענה נכונה עבור m ונוכיח אותה עבור $m+1$.

ובכן, נתונים וקטורים $w_1,\dots,w_\ell \in F^{m+1}$ $\ell > m+1$

צריך להוכיח כי $w_1,\dots,w_\ell$ תלויים לינארית:

$$w_1 = (a_{11},\dots,a_{1m},a_{1\,m+1})$$
$$\vdots$$
$$w_{\ell-1} = (a_{\ell-1\,1},\dots,a_{\ell-1\,m},a_{\ell-1\,m+1})$$
$$w_\ell = (a_{\ell 1},\dots,a_{\ell m},a_{\ell\,m+1})$$

<u>מקרה פרטי</u>: $a_{1\,m+1}=\dots=a_{\ell\,m+1}=0_F$

נגדיר $w_1' = (a_{11},\dots,a_{1m})\in F^m$

$$\vdots$$

$$w_\ell' = (a_{\ell 1},\dots,a_{\ell m})\in F^m$$

$\ell>m+1>m \Rightarrow$ לפי הנחת האינדוקציה $w_1',\dots,w_\ell' \in F^m$ תלויים לינארית $\Rightarrow$ קיימים $c_1,\dots,c_\ell\in F$ לא כולם 0_F רק ש- $\sum_{i=1}^{\ell} c_i w_i' = 0_{F^m}$ אז במקרה הפרטי שאנו דנים בו $\sum_{i=1}^{\ell} c_i w_i = 0_{F^{m+1}}$

למה? תמיד המקום האחרון 0_F.

$$c_1\cdot w_1 = (a_{11},\dots,a_{1m},0_F)$$
$$\vdots$$
$$c_\ell\cdot w_\ell = (a_{\ell 1},\dots,a_{\ell m},0_F)$$

$$c_1w_1+\dots+c_\ell w_\ell + 0_F = 0_F$$

אז אם האיברים האחרונים שונים מ-0? נשאר לנו לבדוק במקרה בו לפחות אחד המקדמים $a_{1\,m+1},\dots,a_{\ell\,m+1}$ שונה מ-0_F. לצורך נוחות הכתיבה נניח $a_{\ell\,m+1}\neq 0_F$ (זה בסדר כי הסדר של הווקטורים לא משפיע עלינו יהיה נוח לחשוב שהווקטור האחרון הוא זה שבו האיבר האחרון מהצד שונה מאפס).

נגדיר:

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

צירופים לינאריים של w_i ו- w_ℓ.

נפתח קודם:

$$u_1 = w_1 - a_{1m+1} a^{-1}_{\ell m+1} w_\ell = (b_{11}, \ldots, b_{1m}, 0_F)$$

↑

$$a_{1m+1} - a_{1m+1} a^{-1}_{\ell m+1} a_{\ell m+1} = 0_F$$

⋮

$$u_{\ell-1} = w_{\ell-1} - a_{\ell-1\,m+1} a^{-1}_{\ell m+1} w_{\ell} = (b_{\ell-1\,1}, \ldots, b_{\ell-1\,m}, 0_F)$$

שוב נגדיר וקטורים חדשים: $u_1' = (b_{11}, \ldots, b_{1m}) \in F^m$

⋮

$$u_{\ell-1}' = (b_{\ell-1\,1}, \ldots, b_{\ell-1\,m}) \in F^m$$

$\ell > m+1 \Leftarrow \ell - 1 > m \Leftarrow$ לפי הנחת האינדוקציה קיימים סקלרים $d_1, \ldots, d_{\ell-1} \in F$ לא כולם רק 0_F ש- $\sum_{i=1}^{\ell-1} d_i u_i' = 0_{F^m}$

$\Leftarrow \sum_{i=1}^{\ell-1} d_i u_i = 0_{F^{m+1}}$. אבל

$$0_{F^{m+1}} = \sum_{i=1}^{\ell-1} d_i u_i = \sum_{i=1}^{\ell-1} d_i (w_i - \Sigma w_\ell) = \sum_{i=1}^{\ell} d_i w_i$$

משהו לא ברור. לא משנה

אז לא כרגע - זה יהיה משהו מאיברים של F

כאשר $d_\ell = \sum_{i=1}^{\ell-1} d_i \Sigma = -\sum_{i=1}^{\ell-1} d_i a_{im+1} a^{-1}_{\ell m+1}$

$\Leftarrow w_1, \ldots, w_\ell$ תלויים

משל ☺

הגדרה: יהיו F שדה ו- V מ"ו מעל F. הוקטורים $v_1, \ldots, v_n \in V$ פורשים (או יוצרים) את V כאשר כל וקטור ב- V הוא צירוף לינארי של $v_1, \ldots, v_m$.

משפט: נניח ש $v_1, \ldots, v_m \in V$ פורשים את V ונניח ש- $w_1, \ldots, w_\ell \in V$ ו- $\ell > m$ אז $w_1, \ldots, w_\ell$ תלויים לינארית.

הוכחה: אפשר לרשום $w_1 = a_{11} v_1 + \ldots + a_{1m} v_m$

⋮

$$w_\ell = a_{\ell 1} v_1 + \ldots + a_{\ell m} v_m$$

נגדיר $u_i = (a_{i1}, \ldots, a_{im}) \in F^m$. נזכיר ש- $\ell > m$ $u_1, \ldots, u_\ell \in F^m$ תלויים לינארית. $\Leftarrow$ קיימים $c_1, \ldots, c_\ell \in F$ לא כולם רק 0_F ש

$\sum_{i=1}^{\ell} c_i u_i = 0_{F^m}$. $\Leftarrow$

$$\sum_{i=1}^{l} c_i w_i = \sum_{i=1}^{l} c_i \sum_{j=1}^{m} a_{ij} v_j =$$ ⇐

$$= \sum_{i=1}^{m} \left(\sum_{j=1}^{l} c_j a_{ji} \right) v_i = \sum_{i=1}^{n} 0_F v_i = \sum 0_v = 0_v$$

⇐ $w_1, \dots, w_l$ תלויים לינארית.

אשף ☺

(28) 7.12.05
לינארית

בסיס של מרחב וקטורי

F שדה, V מרחב וקטורי מעל F.

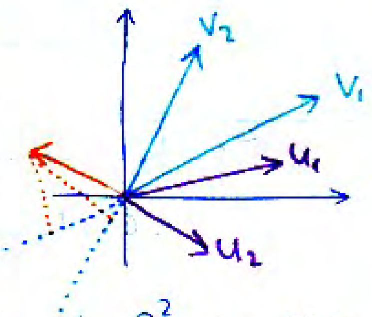
<u>הגדרה</u> קבוצת וקטורים $v_1,\dots,v_n \in V$ נקראת בסיס של V

אם (א) $v_1,\dots,v_n$ פורשים את V

(ב) $v_1,\dots,v_n$ בת"ל.

<u>דוגמה</u>

$F=\mathbb{R}$ $V=\mathbb{R}^2$



ברור ש v_1 ו- v_2 בת"ל כי הם לא נמצאים על אותו ישר ואם כל וקטור אחר אפשר להציג כצירוף לינארי שלהם (ע"י הטלה עליהם)

$\Leftarrow$ v_1 ו- v_2 בסיס ל-$\mathbb{R}^2$.

בעצם ב-$\mathbb{R}^2$ כל שני וקטורים שלא נמצאים על ישר אחד הם בסיס, כלומר יכולים להיות הרבה בסיסים. אין דבר כזה הבסיס. בציור v_1,v_2,u_1,u_2 פורשים את $\mathbb{R}^2$ אבל הם תלויים לינארית - גם כי ע"י v_1 ו- v_2 אפשר להגיע לכל וקטור אחר וגם לפי מה שהוכחנו בשיעור קודם - ב-$\mathbb{R}^2$ כל 3 ומעלה וקטורים הם תלויים ($3>2$)

<u>משפט</u> אם $v_1,\dots,v_n \in V$ בסיס של V ו- $w_1,\dots,w_\ell \in V$ בסיס של V אזי $\ell=n$.

<u>הוכחה</u> נניח $n<\ell$. לפי המשפט שהוכחנו בפעם הקודמת, V נפרש ע"י n וקטורים $v_1,\dots,v_n$ ועבור $n<\ell$ הווקטורים $w_1,\dots,w_\ell \in V$ תלויים לינארית בניגוד להגדרה של בסיס (אם אמרנו שהם בסיס הם חייבים להיות בת"ל). כמו כן, אם $\ell<n$ אזי היות ו- V נפרש ע"י ℓ וקטורים - $w_1,\dots,w_\ell$ אזי $v_1,\dots,v_n$ תלויים לינארית (כי $\ell<n$) בניגוד לכך ש- $v_1,\dots,v_n$ בסיס.

$\Leftarrow$ האפשרות היחידה שנשארת היא $n=\ell$ מש"ל ☺

המשפט הזה לא אומר שלכל מרחב וקטורי יש בסיס (סופי בכל אופן. יש מרחבים שאין להם בסיס סופי), אבל אם נבחר יש 2 בסיסים (או יותר) אז חייב להיות בהם אותו מספר איברים.

<u>הגדרה</u> מספר האיברים בבסיס של V נקרא המימד של V ומסומן $\dim_F V$ (dimension)

הנחנו במקרים שבהם קיים בסיס סופי.

<u>דוגמה:</u> $\dim_F F^n = n$

איך מוכיחים דבר כזה? אם נמצא בסיס כלשהו שיש בו n איברים, אז זה מספר האיברים בכל בסיס וזה המימד.

<u>הוכחה.</u> (אלו הווקטורים) $e_1 = (1_F, 0_F, \dots, 0_F)$

$e_2 = (0_F, 1_F, 0_F, \dots, 0_F)$

(מקום i)

$e_i = (0_F, \dots, 1_F, \dots, 0_F)$

$\vdots$

$e_n = (0_F, \dots, 0_F, 1_F)$

נוכיח כי $e_1, \dots, e_n \in F^n$ הם בסיס של F^n. לשם כך יש להוכיח כי הם פורשים וכי הם בת"ל:

פורשים: יהי $(a_1, \dots, a_n) \in F^n$. ברור ש-

$$(a_1, \dots, a_n) = \sum_{i=1}^n a_i e_i$$

⇐ כל וקטור ב-F^n ניתן להצגה כצירוף לינארי של $e_1, \dots, e_n$

⇐ $e_1, \dots, e_n$ פורשים את F^n.

בת"ל: נראה ש $e_1, \dots, e_n$ בת"ל. נניח שעבור סקלרים $a_1, \dots, a_n \in F$ מתקיים $\sum_{i=1}^n a_i e_i = 0_{F^n}$. צ"ל ש- $a_i = 0_F$ לכל i.

$$0_{F^n} = (0_F, \dots, 0_F) = a_1 e_1 + \dots + a_n e_n = a_1(1_F, 0_F, \dots, 0_F) + \dots + a_n(0_F, \dots, 0_F, 1_F) =$$

$$= (a_1, \dots, a_n) \Rightarrow a_1 = 0_F, \dots, a_n = 0_F$$

⇐ $e_1, \dots, e_n$ בת"ל. ⇐ $\dim_F F^n = n$ מש"ל ☺

למשל, ב-$\mathbb{R}^2$ כל בסיס יש 2 איברים!! (בדיוק)

והבסיס הסטנדרטי הזה $e_1,\dots,e_n$ נקרא
הבסיס הסטנדרטי של F^n. ל-F^n יש הרבה בסיסים
אבל $e_1,\dots,e_n$ הוא הכי פשוט ומאוד נוח לעבוד איתו
ולכן הוא זכה לשם משלו עם ה' הידיעה אפילו.

<u>משפט:</u> נניח ש $v_1,\dots,v_n\in V$ אזי התנאים הבאים שקולים.

א. $v_1,\dots,v_n$ בסיס של V

ב. לכל וקטור $v\in V$ קיימת הצגה יחידה כצירוף לינארי של $v_1,\dots,v_n$. כלומר הסקלרים $a_1,\dots,a_n\in F$ כך ש $v=\sum_{i=1}^{n}a_iv_i$ נקבעים בצורה חד-ערכית.

<u>הוכחה:</u>

(א ⇐ ב) $v_1,\dots,v_n$ בסיס, בפרט הם פורשים את V. ⇐ לכל $v\in V$ קיימים סקלרים $a_1,\dots,a_n\in F$ כך ש $v=\sum_{i=1}^{n}a_iv_i$.
נוכיח יחידות: לשם כך נניח שיש עוד הצגה $v=\sum_{i=1}^{n}b_iv_i$ כאשר $b_1,\dots,b_n\in F$ ⇐ $\sum_{i=1}^{n}a_iv_i=v=\sum_{i=1}^{n}b_iv_i$
נעביר אגף ונקבל $0_v=\sum_{i=1}^{n}(a_i-b_i)v_i$. $v_1,\dots,v_n$ בת"ל ⇐ $a_i-b_i=0_F$ ⇐ $a_i=b_i$.

(ב ⇐ א) לכל $v\in V$ קיימת הצגה $v=\sum_{i=1}^{n}a_iv_i$ ⇐ $v_1,\dots,v_n$ פורשים את המרחב ⇐ נותר להוכיח שהם בת"ל.
נניח שעבור $a_1,\dots,a_n\in F$ מתקיים $\sum_{i=1}^{n}a_iv_i=0_v$. ומכאן ⇐ ההצגה היחידה אבל זה נכון ש $\sum_{i=1}^{n}0_F\cdot v_i=0_v$ ⇐ $a_i=0_F$ לכל i.
⇐ $v_1,\dots,v_n$ בת"ל. ⇐ הם בסיס.

מש"ל ☺

הגדרה: יהי F שדה ו-V מ"ו מעל F. תת קבוצה $U \subseteq V$ נקראת תת-מרחב כאשר U מקיימת את האקסיומות של מרחב וקטורי ביחס לחיבור וקטורים וכפל בסקלר שמוגדרים ב-V.

משפט: $U \subseteq V$ הוא תת מרחב אם ורק אם

א. U לא ריקה

ב. U סגורה לגבי חיבור של וקטורים

ג. U סגורה לגבי כפל בסקלר

הוכחה:

($\Leftarrow$) אם U תת מרחב של V אז ברור שכל התכונות מתקיימות, פשוט כי זה מרחב וקטורי.

($\Rightarrow$) נניח שמתקיימים (א) (ב) ו-(ג) ונוכיח ש-U מקיים את כל האקסיומות של מרחב וקטורי.

(1) סגירות לגבי חיבור נובעת מתנאי ב'

(2) (3) קומוטטיביות ואסוציאטיביות של חבור וקטורים מתקיימים ב-V כי הוא מרחב וקטורי ולכן גם ב-U כי הפעולות זהות.

(4) קיום האפס: $U \neq \emptyset \Rightarrow$ קיים $u \in U$ לפי תנאי (ג) $(-1_F)u \in U$ ולפי תנאי ב'

$$U \ni u+(-1_F)u = 1_F\cdot u + (-1_F)u = (1_F+(-1_F))u = 0_F u = 0_V$$

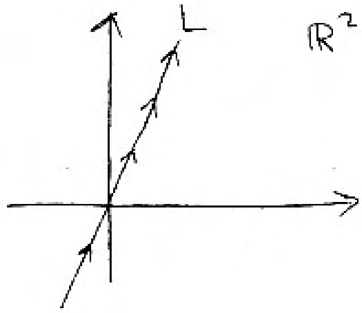
(5) קיום נגדי: אם $w \in U$ אז $(-1_F)w \in U$ ולפי שראינו קודם $w+(-1_F)w = 0_V$ כלומר $-w = (-1_F)w \in U$

(6) סגירות של כפל בסקלר היא תנאי (ג)

(7) $1_F \cdot u = u$, $(ab)u = a(bu)$, $(a+b)u = au+bu$, $a(u+v) = au+av$ — נכונים לכל $a,b \in F$ ו-$u,v \in V$ ובפרט ב-U.

מש"ל ☺

דוגמה:



$\{(0,0)\} \subseteq \mathbb{R}^2$ תת מרחב

ישר דרך הראשית $= L \subseteq \mathbb{R}^2$ תת מרחב כי גם חיבור וגם כפל בסקלר משאירים אותנו על אותו הישר

$\mathbb{R}^2 \subseteq \mathbb{R}^2$ תת-מרחב

האמת היא שזאת הרשימה המלאה של תת מרחבים של $\mathbb{R}^2$ אבל לא נוכיח את זה כרגע.

באופן דומה: ב-$\mathbb{R}^3$ תת המרחבים הם: כל המישורים שעוברים דרך הראשית, כל הישרים שעוברים דרך הראשית והראשית עצמה.

הגדרה: $u_1,\dots,u_k \in V$, $k \geq 1$ מגדירים

$$Sp(u_1,\dots,u_k) = \left\{ \sum_{i=1}^{k} c_i u_i : c_i \in F \right\} = \quad (\text{Span})$$

$= \{$אוסף הצירופים הליניאריים של $u_i\}$ עבור $k=0$: $Sp() = \{0_V\}$

משפט: $Sp(u_1,\dots,u_k)$ הוא תת מרחב של V.

הוכחה: אם $k=0$ ברור ש-$\{0\}$ תת מרחב.

כעת נניח $k>0$. ⇐

(א) $Sp(u_1,\dots,u_k)$ לא ריקה שהרי כל צירוף ליניארי שייך לה.

(ב) יהיו $\sum_{i=1}^{k} c_i u_i, \sum_{i=1}^{k} d_i u_i \in Sp(u_1,\dots,u_k)$. (נסתכל על) הסכום:

$$\sum_{i=1}^{k} d_i u_i + \sum_{i=1}^{k} c_i u_i = \sum_{i=1}^{k} (d_i + c_i) u_i \in Sp(u_1,\dots,u_k)$$

כי זה גם צירוף ליניארי.

(ג) יהי $\sum c_i u_i \in Sp(u_1,\dots,u_k)$ ויהי $b \in F$ אזי:

$$b \sum_{i=1}^{k} c_i u_i = \sum_{i=1}^{k} (b c_i) u_i \in Sp(u_1,\dots,u_k)$$

כי זה גם צירוף ליניארי.

⇐ על סמך המשפט הקודם $Sp(u_1,\dots,u_k)$ הוא תת מרחב של V.

אושר (☺)

הערה: עבור $u_1,\dots,u_k \in V$ אם $Sp(u_1,\dots,u_k) = V$ אז $u_1,\dots,u_k$ פורשים את V.

F שדה, x משתנה. נגדיר את המרחב F[x] של פולינומים במשתנה x עם המקדמים בשדה F.

באופן מפורש:

$$F[x]=\left\{\sum_{i=0}^{n} a_i x^i : a_i\in F,\ n\geq 0\right\}$$

איך מחברים פולינומים? כמו שאנחנו יודעים - לפי החזקות:

$$(3+x)+(2-x^2+x^3)=5+x-x^2+x^3$$

איך כופלים בסקלר? כמו שאנחנו יודעים:

$$10(3+x)=30+10x$$

הוכחת האקסיומות של מרחב וקטורי מושארת כתרגיל.

הערה: אנו מזהים פולינום $3+x$ עם הפולינום $3+x+0\cdot x^2+0\cdot x^3$

<u>משפט:</u> ב $F[x]$ אין בסיס סופי.

<u>הוכחה:</u> נניח בשלילה ש $v_1,\dots,v_n\in F[x]$ הוא בסיס של $F[x]$.

נניח ש v_1 פולינום ממעלה m_1, ו- v_2 פולינום ממעלה m_2, ..., v_n פולינום ממעלה m_n. ניקח $m=\max(m_1,\dots,m_n)$

אז כל צירוף ליניארי של $v_1,\dots,v_n$ הוא פולינום עד מעלה m

בפרט $x^{m+1}\notin Sp(v_1,\dots,v_n)$ ולכן $v_1,\dots,v_n$ אינם פורשים את $F[x]$ ולכן הם אינם בסיס של $F[x]$. סתירה

$\Rightarrow$ ל $F[x]$ אין בסיס סופי. כנדרש.

משפט :)

<u>משפט:</u> אם למרחב V יש בסיס ו- $U\subseteq V$ תת מרחב אז גם ל- U יש בסיס.

(31) 12.12.05
לינארית

בסיס ומימד

<u>הגדרה</u>: F שדה, V מ"ו מעל F. $v_1,\dots,v_n \in V$ נקראים בסיס של V אם:

(א) $v_1,\dots,v_n$ פורשים את V

(ב) $v_1,\dots,v_n$ בת"ל

<u>משפט</u>: לכל שני בסיסים של מ"ו יש אותו מספר איברים.

<u>הגדרה</u>: מספר האיברים של בסיס של V נקרא המימד של V ומסומן $\dim_F V$.

<u>הערה</u>: לא לכל מרחב וקטורי יש בסיס סופי. מצאנו דוגמה לכך - מרחב כל הפולינומים מהשאלה בשבת.

<u>משפט</u>: נניח ש-V מ"ו עם בסיס $v_1,\dots,v_n$ ו- $U \subseteq V$ תת"מ. אז ל-U יש בסיס.

<u>הערה</u>: האם הטענה מובנת? המשפט אומר שאפשר למצוא קבוצה פורשת סופית ב-U והווקטורים בה בת"ל.

המשפט נראה טריוויאלי אבל הוא קשה!

<u>טענת עזר</u>: התנאים הבאים שקולים:

(א) $w_1,\dots,w_l \in V$ בת"ל

(ב) $w_1 \neq 0_V$, $w_2 \notin Sp(w_1)$, ..., $w_l \notin Sp(w_1,\dots,w_{l-1})$

<u>הוכחה</u>:

(א ⇒ ב) נניח ש $w_1,\dots,w_l \in V$ בת"ל. אם $w_1 = 0_V$ אז יש תלות $0_V = 1\cdot w_1 + 0_F\cdot w_2 + \dots + 0_F\cdot w_l$ לא טריוויאלית ונקבל סתירה.

אם $w_2 \in Sp(w_1)$ אז $w_2 = c_1 w_1$ ואז $0_F w_l + \dots + 1_F w_2 + (-c_1)w_1 = 0_V$

⇐ $w_2 \notin Sp(w_1)$. כנ"ל השאר. באופן כללי אם

$w_k \in Sp(w_1,\dots,w_{k-1})$ אז $w_k = c_1 w_1 + \dots + c_{k-1} w_{k-1}$ ולכן

$0_F w_l + \dots + 0_F w_{k+1} + 1_F w_k + (-c_{k-1})w_{k-1} + \dots + (-c_1)w_1 = 0_V$ ⇐ $w_k \notin Sp(w_1,\dots,w_{k-1})$

(ב ⇐ א) נתון ש $w_1 \neq 0_V$ ו- $w_k \notin Sp(w_1,\dots,w_{k-1})$ לכל $2 \le k \le l$

נניח בשלילה שיש תלות $0_V = \sum_{i=1}^{l} c_i w_i$ ולא כל $c_i = 0_V$.

ניקח k הכי גדול רק ש $c_k \neq 0_F$. אולי $k=l$.

ואולי $k<l$ ואז, לפי ההגדרה של k, $c_{k+1}=0_F, \dots, c_l=0_F$

$$\Rightarrow 0_V = c_1w_1+\dots+c_kw_k+(c_{k+1}w_{k+1}+\dots+c_lw_l) = c_1w_1+\dots+c_kw_k$$

$$c_k \neq 0_F \Rightarrow \exists c_k^{-1} \Rightarrow c_kw_k = -c_1w_1 - c_2w_2 - \dots - c_{k-1}w_{k-1}$$

$$\Rightarrow w_k = -c_k^{-1}c_1w_1 - c_k^{-1}c_2w_2 - \dots - c_k^{-1}c_kw_{k-1} \in \dots$$

$$w_k \in Sp(w_1,\dots,w_{k-1})$$

קיבלנו סתירה להנחה ולכן $w_1,\dots,w_l$ בת"ל.

מש"ל ☺

הוכחת המשפט

אם $U \subseteq V$ ו- $U=\{0_V\}$ אז הקבוצה ריקה של וקטורים היא הבסיס של U. אם $U \neq \{0_V\}$ אז קיים וקטור $0_V \neq w_1 \in U$. לפי טענת עזר $\{w_1\}$ בת"ל.

אם $U = Sp(w_1)$ אז w_1 בסיס של U.

אם $U \neq Sp(w_1)$ אז קיים $U \ni w_2 \notin Sp(w_1)$. לפי ט"ע w_1, w_2 בת"ל.

אם $U = Sp(w_1,w_2)$ אז w_1,w_2 בסיס של U. אחרת יש $w_3 \notin Sp(w_1,w_2)$ ב- U. לפי ט"ע הם בת"ל וכן הלאה.

הוכחנו שבמרחב וקטורי שנפרש ע"י n וקטורים לא קיים $n+1$ וקטורים בת"ל. ⇐ התהליך חייב להיעצר לפני שלב $n+1$. לכן קיים $l \le n$ רק ש $U=Sp(w_1,\dots,w_l)$ כאשר $w_1,\dots,w_l$ בת"ל. כלומר קיבלנו בסיס של U כנדרש ובנוסף גם הוכחנו ש $\dim_F U \le \dim_F V$.

(נב)

<u>משפט</u>: אם $U \subseteq V$ ת"מ ו- $\dim_F U = \dim_F V$ אז $U = V$

<u>הוכחה</u>: נניח בדרך השלילה ש $U \neq V$. $w_1, \dots, w_n$ בסיס של U ו- $v_1, \dots, v_n$ בסיס של V. ניקח $w_{n+1} \notin U$, $w_{n+1} \in V$. לפי ט"ע $w_1, \dots, w_{n+1}$ בת"ל בסתירה לכך ש-V נפרש ע"י $v_1, \dots, v_n$. לכן $V = U$.

מש"ל ☺

<u>משפט</u>: נניח ש $V = Sp(u_1, \dots, u_m)$, אז קיימת תת קבוצה של $\{u_1, \dots, u_m\}$ שהיא בסיס של V. יתר על כן, הקבוצה $\{u_i : 1 \le i \le m, u_i \notin Sp(u_1, \dots, u_{i-1})\}$ בסיס ל-V.

<u>הוכחה</u>: נצבע את u_i בכתום כאשר $u_i \notin Sp(u_1, \dots, u_{i-1})$
ונצבע את u_i בכחול כאשר $u_i \in Sp(u_1, \dots, u_{i-1})$
נוכיח את אי התלות של הווקטורים ה~~כתומים~~ כתומים

$u_i \notin (\cdot\cdot \; \cdots \; \cdot\cdot)$ ⊇ $Sp(\cdot\cdot \; \cdot\cdot)$ ($u_1 \; \dots \; u_{i-1}$)

לכן הווקטורים הכתומים שלא שייכים ל Sp של קודמיהם ולכן הם בת"ל. $= Sp(\cdots \; \cdots \; \cdots) \overset{2}{\underset{\subseteq}{=}} V = Sp(\cdots \; \cdots \cdots \boxdot \cdot)$ ($u_1 \dots u_m$)
(כאשר השמטנו את הוקטור הכחול עם אינדקס הכי גדול.)

$= Sp(\cdots \; \cdots) = \dots$ ▪

כי השמטנו את t הכחולים, t פעמים או זה עם האינדקס הכי גדול)

צ"ל שה הווקטורים הכתומים פורשים את V ולכן הם בסיס כנדרש.

(33) 14.12.05
לינארית

בסיסים וממד

בפעם הקודמת הוכחנו:

<u>משפט</u>: אם $V=Sp(u_1,\dots,u_m)$ אז קבוצת הווקטורים $\{u_i : 1\le i\le m,\ u_i\notin Sp(u_1,\dots,u_{i-1})\}$ היא בסיס של V.

<u>משמעות</u>: מה שהמשפט אומר הוא שאם יש לנו קבוצה של וקטורים שפורשת את המרחב אז אפשר למצוא בה תת קבוצה שהיא בסיס - כלומר שהיא גם פורשת וגם בת"ל.

<u>משפט</u>: אם $V=Sp(u_1,\dots,u_m)$ ו- $v_1,\dots,v_k\in V$ בת"ל, אז ניתן להשלים את $v_1,\dots,v_k$ לבסיס של V, כאשר משתמשים לצורך ההשלמה רק בווקטורים מהקבוצה $\{u_1,\dots,u_m\}$.

<u>משמעות</u>: בהינתן קבוצה בת"ל אפשר להוסיף לה וקטורים נוספים רק שכל הווקטורים ביחד יתנו בסיס של V. יתר על כן, לצורך ההשלמה אפשר להשתמש רק בווקטורים שפורשים את V.
ברור שמראש הקבוצה שהתחלנו לא חייבת כבר להיות פורשת. אם היא פורשת לא צריך להשלים אותה.

<u>הוכחה</u>: על סמך הנתון $V=Sp(u_1,\dots,u_m)=Sp(v_1,\dots,v_k,u_1,\dots,u_m)=V$
אם $u_1,\dots,u_m$ פרשו את V ברור שאם נוסיף להם וקטורים אז כל הקבוצה החדשה הגדולה עדיין תפרוש את V.
כעת נשתמש במשפט הקודם.
על סמך המשפט הקודם (נקבל בסיס של V מהצורה $v_1,\dots,v_k,u_{j_1},\dots,u_{j_s}$. לאחר שבמשפט הקודם מוצג תהליך סינון. כל וקטור חייב להיות בת"ל בווקטורים הקודמים לו. (נתון לנו ש $v_1,\dots,v_k$ בת"ל לכן הם עומדים בתנאי הסינון. לכן אם הצבנו את $v_1,\dots,v_k$ להיות הראשונים שעברו את התהליך).

מש"ל ☺

בעצם שני המשפטים הללו משלימים אחד את השני. מה שקורה כאן הוא שבעצם אם V נוצר סופית (נפרש ע"י קבוצה סופית של וקטורים) אז תמיד אפשר למצוא לו בסיס. אם הקבוצה גדולה מדי אפשר לדלל אותה, ואם יש לנו קבוצה בת"ל לא מספיק גדולה אז אפשר להרחיב אותה.

<u>טענה:</u> התנאים הבאים הם שקולים:

(א) $v_1,\dots,v_n \in V$ הם בסיס של V

(ב) $v_1,\dots,v_n \in V$ קבוצה פורשת מינימלית (כלומר אם משמיטים וקטור אחד הקבוצה כבר לא פורשת)

(ג) $v_1,\dots,v_n \in V$ קבוצת וקטורים בת"ל מקסימלית (כלומר אם מוסיפים אפילו וקטור אחד הקבוצה כבר לא בת"ל).

<u>הוכחה:</u>

(א ⇐ ב) אם $v_1,\dots,v_n$ בסיס ברור לפי ההגדרה שזו קבוצה פורשת. נראה שהיא מינימלית. נניח בשלילה שלא כך הדבר. אז ניתן להשמיט את אחד הוקטורים ונקבל $v_1,\dots,v_{i-1},v_{i+1},\dots,v_n$ קבוצה פורשת. קבוצה זו גם היא בת"ל (כי היא תת קבוצה של קבוצה בת"ל) ⇐ קיבלנו ש- $v_1,\dots,v_{i-1},v_{i+1},\dots,v_n$ בסיס ובו $n-1$ וקטורים, וזו סתירה לכך שבכל בסיס של V יש אותו מספר איברים.

(ב ⇐ א) נניח $v_1,\dots,v_n$ פורשת מינימלית. נראה שהיא בת"ל. נניח שיש תלות לינארית. לפי טענת העזר מהשיעור הקודם קיים $1 \le i \le n$ רק ש- $v_i \in Sp(v_1,\dots,v_{i-1})$. ואז

$$V = Sp(v_1,\dots,v_{i-1},v_i,v_{i+1},\dots,v_n) = Sp(v_1,\dots,v_{i-1},v_{i+1},\dots,v_n)$$

בסתירה למינימליות של $v_1,\dots,v_n$ ⇐ $v_1,\dots,v_n$ בת"ל ונתון שהם פורשים ⇐ $v_1,\dots,v_n$ בסיס של V.

הוכחנו את השקילות של (א) ו-(ב)

(א ⇐ ג) נתון ש $v_1,\dots,v_n\in V$ בסיס. אכן, לכל $v_{n+1}\in V$
מתקיים $v_{n+1}\in V=Sp(v_1,\dots,v_n)$ ולכן $v_1,\dots,v_n,v_{n+1}$
תלויים לינארית. כלומר כל וקטור שנוסיף יביא לכך שהקבוצה
תהיה לא בת"ל ⇐ $v_1,\dots,v_n$ בת"ל מקסימלית.

(ג ⇐ ב) נניח $v_1,\dots,v_n$ קבוצה בת"ל מקסימלית. (נראה שהיא
פורשת (טוב, האמת היא שזה די מיידי. מאחר שהיא מקסימלית
כל וקטור שנוסיף לה יהיה תלוי בקודמיו)
נניח ש- $Sp(v_1,\dots,v_n)\neq V$. אז קיים וקטור $v_{n+1}\in V$ כך
ש $v_{n+1}\notin Sp(v_1,\dots,v_n)$ ולכן

$v_1\neq 0_V,\ v_2\notin Sp(v_1),\ \dots,\ v_n\notin Sp(v_1,\dots,v_{n-1}),\ v_{n+1}\notin Sp(v_1,\dots,v_n)$

לכן $v_1,\dots,v_n,v_{n+1}$ בת"ל וזה בסתירה למקסימליות של $v_1,\dots,v_n$.
הוכחנו את השקילות של (ב) ו-(ג) ולכן 3 התנאים שקולים.
מש"ל ☺

<u>טענה</u>: אם V מ"ו מעל F, $U\subseteq V$, $W\subseteq V$ תת מרחבים
אז החיתוך $U\cap W$ הוא גם תת מרחב של V.

<u>הוכחה</u>: $0_V\in U$ ו $0_V\in W$ ⇐ $0_V\in U\cap W$ ולכן
$U\cap W\neq\emptyset$. נניח ש $v_1,v_2\in U\cap W$ ⇐ $v_1,v_2\in U$,
$v_1,v_2\in W$ ⇐ $v_1+v_2\in U$, $v_1+v_2\in W$ ⇐ $v_1+v_2\in U\cap W$
⇐ יש סגירות לחיבור.
נניח ש $v\in U\cap W$ ו $c\in F$ ⇐ $v\in U$, $v\in W$
⇐ $cv\in U$, $cv\in W$ ⇐ $cv\in U\cap W$ ⇐ יש סגירות
לכפל בסקלר. ⇐ $U\cap W$ תמ"ו.
מש"ל ☺

<u>הגדרה</u>: אם $U,W\subseteq V$ תמ"ו (סמן)
$U+W=\{u+w: u\in U, w\in W\}$

טענה: אם $U,W\subseteq V$ תמ"ו אז גם $U+W$ תמ"ו של V

הוכחה: $0_V\in U$, $0_V\in W$ ⇐ $0_V=0_V+0_V\in U+W$ ⇐

$U+W\neq\emptyset$.

נניח ש- $v_1,v_2\in U+W$. אז: $v_1=u_1+w_1$ כאשר $u_1\in U$ $w_1\in W$

ו- $v_2=u_2+w_2$ כאשר $u_2\in U$ $w_2\in W$. ⇐ $u_1+u_2\in U$

$w_1+w_2\in W$ ⇐ $(u_1+u_2)+(w_1+w_2)\in U+W$.

נניח ש $v\in U+W$ ו- $c\in F$ ⇐ $v=u+w$ כאשר

$u\in U$ $w\in W$ ⇐ $cu\in U$ $cw\in W$ ⇐

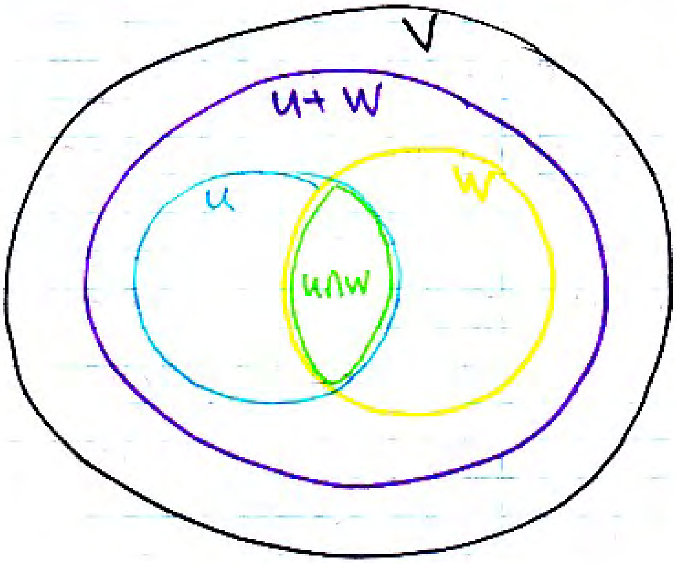
$cv=c(u+w)=cu+cw\in U+W$.

מש"ל ☺

משפט: נניח ש- V מ"ו נפרש סופית, $U,W\subseteq V$ תמ"ו

אז: $\dim_F(U+W)=\dim_F U+\dim_F V-\dim_F(U\cap W)$

הוכחה:



ל- $U\cap W$ אפשר לבחור בסיס $v_1,\dots,v_m$

$U\cap W$ הוא תמ"ו של U. לכן ניתן להשלים את $v_1,\dots,v_m$

עד לבסיס של U: $v_1,\dots,v_m,u_1,\dots,u_k$

כמו כן, $U\cap W$ הוא תמ"ו של W ולכן ניתן להשלים עד

לבסיס של W: $v_1,\dots,v_m,w_1,\dots,w_\ell$

טענה: הוקטורים $w_1,\dots,w_\ell$, $u_1,\dots,u_k$, $v_1,\dots,v_k$ הם בסיס של

$U+W$

הערה: אם לה נכון, הוכחנו את המשפט. שהרי אז:

$$\dim_F(U+W) = m+k+l = (m+k)+(m+l)-m =$$
$$= \dim_F U + \dim_F W - \dim_F(U\cap W)$$

<u>הוכחת הטענה:</u>

(א) נראה שהקבוצה פורשת. ניקח וקטור $v \in U+W$

אז קיימים וקטורים $u \in U$ ו- $w \in W$ כך ש- $v = u + w$

אז: $u = a_1 v_1 + \ldots + a_m v_m + b_1 u_1 + \ldots + b_k u_k$

ואז: $w = c_1 v_1 + \ldots + c_m v_m + d_1 w_1 + \ldots + d_l w_l$

$$v = u + w = (a_1+c_1)v_1 + \ldots + (a_m+c_m)v_m + b_1 u_1 + \ldots + b_k u_k + d_1 w_1 + \ldots + d_l w_l$$

$\Leftarrow$ $v \in Sp(v_1,\ldots,v_m, u_1,\ldots,u_k, w_1,\ldots,w_l)$

אנשים ש $w_1,\ldots,w_l$ $u_1,\ldots,u_k$ $v_1,\ldots,v_m \in U+W$ הם פורשים את $U+W$

(ב) אי תלות: נניח ש- $a_1 v_1 + \ldots + a_m v_m + b_1 u_1 + \ldots + b_k u_k + d_1 w_1 + \ldots + d_l w_l = 0_V$

צ"ל: $a_1 = \ldots = a_m = b_1 = \ldots = b_k = d_1 = \ldots = d_l = 0_F$. (סמן:

$$z = a_1 v_1 + \ldots + a_m v_m + b_1 u_1 + \ldots + b_k u_k =$$
$$= -d_1 w_1 - \ldots - d_l w_l$$

העברת אגף

לכן $z \in U$ וגם $z \in W$ לכן $z \in U\cap W$

$\Leftarrow$ $z = c_1 v_1 + \ldots + c_m v_m =$

$$= c_1 v_1 + \ldots + c_m v_m + 0_F \cdot u_1 + \ldots + 0_F u_k$$

לכן ל- z יש שתי הצגות לפי הבסיס של U

מכאן יחידות ההצגה $b_1 = \ldots = b_k = 0_F$

לכן $a_1 v_1 + \ldots + a_m v_m + d_1 w_1 + \ldots + d_l w_l = 0_V$

$v_1,\ldots,v_m\ w_1\ldots w_l$ הם בסיס של W לכן הם בת"ל

לכן $d_1 = \ldots = d_l = a_1 = \ldots = a_m = 0_F$

קיבלנו אי תלות של $v_1,\ldots,v_m\ u_1,\ldots,u_k\ w_1,\ldots,w_l$ לכן הם בסיס

של $U+W$

מש"ל ☺

(36) 19.12.05
לינארית

העתקות לינאריות של מרחבים וקטוריים

שמות נרדפים: טרנספורמציות לינאריות
הומומורפיזם של מרחבים וקטוריים
מורפיזמים של מרחבים וקטוריים
אופרטורים לינאריים

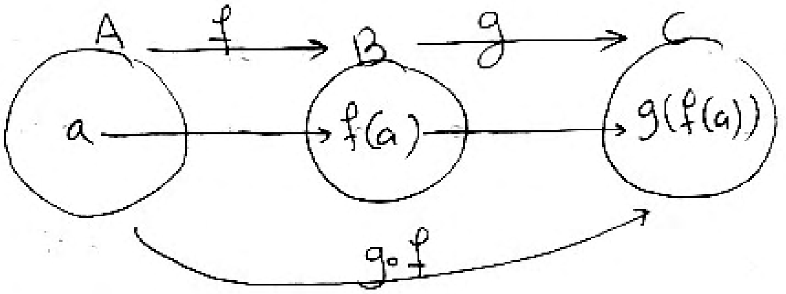
יהיו A,B קבוצות. $f:A\to B$ העתקה של קבוצות. כלומר לכל $a\in A$ f מתאימה איבר $f(a)\in B$.

יהי F שדה ויהיו V, W מ"ו מעל F.
$f:V\to W$ העתקה מ-V ל-W. כלומר לכל $v\in V$ $f(v)\in W$.

<u>הגדרה</u>: העתקה $f:V\to W$ נקראת העתקה <u>לינארית</u> כאשר
① לכל $v_1,v_2\in V$ $f(v_1+v_2)=f(v_1)+f(v_2)$ f שומרת חיבור
② לכל $v\in V$ $c\in F$ $f(cv)=cf(v)$ f שומרת כפל בסקלר

מההגדרה (סעיף 2) ברור שניתן להגדיר העתקה לינארית בין מ"ו רק כאשר הם מעל אותו השדה.

הדבר הטבעי שיש בקבוצות והעתקות הוא הרכבה של העתקות.



לכל $a\in A$ $(g\circ f)(a)=g(f(a))$
לפעמים משמיטים את ה $(\circ)$ ורושמים רק gf. $g\circ f=gf$.

טענה: יהיו V, W, U מ"ו מעל F ו- $f: V \to W$, $g: W \to U$ לינאריות. אזי $g \circ f: V \to U$ לינארית.

הוכחה: צריך לבדוק את קיום שני התנאים.

יהיו $v_1, v_2 \in V$:

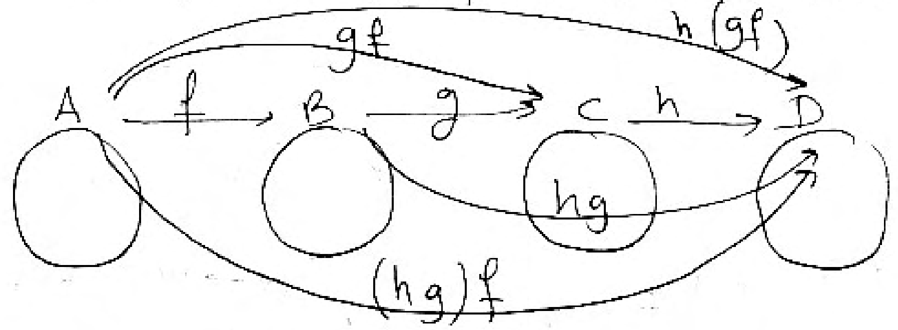
$$(g\circ f)(v_1+v_2) = g(f(v_1+v_2)) = g(f(v_1)+f(v_2)) =$$
$$= g(f(v_1)) + g(f(v_2)) = (g\circ f)(v_1) + (g\circ f)(v_2)$$

יהיו $v \in V$, $c \in F$:

$$(g\circ f)(cv) = g(f(cv)) = g(cf(v)) = cg(f(v)) = c(g\circ f)(v)$$

מש"ל ☺

פעולת ההרכבה של העתקות היא אסוציאטיבית.



לכל $a \in A$

$$(h(gf))(a) = h((gf)(a)) = h(g(f(a)))$$
$$((hg)f)(a) = (hg)(f(a)) = h(g(f(a)))$$
$$\Rightarrow h(gf) = (hg)f$$

היות וההרכבה של העתקות לינאריות מוגדרת כהרכבת העתקות, גם בשביל העתקות לינאריות נכונה <u>האסוציאטיביות</u>.

לכל קבוצה A יש העתקת הזהות $Id_A: A \to A$.

מה היא עושה? שום דבר! $Id_A(a) = a$.

העתקת הזהות של מרחב וקטורי היא לינארית: $Id_V: V \to V$

① לכל $v_1, v_2 \in V$ $\quad Id_V(v_1+v_2) = v_1+v_2 = Id_V(v_1)+Id_V(v_2)$

② לכל $v \in V$ $c \in F$ $\quad Id_V(cv) = cv = cId_V(v)$

(37) חח"ע ועל

אם $f:A\to B$ חח"ע ועל אז קיימת העתקה הפכית $f^{-1}:B\to A$.

f חח"ע כאשר $\forall a_1,a_2\in A$: $a_1\neq a_2 \Rightarrow f(a_1)\neq f(a_2)$

f על כאשר לכל $b\in B$ קיים $a\in A$ יחיד כך ש- $f(a)=b$.

לכל $a\in A$, $b\in B$ $f(a)=b$ אמ"מ $f^{-1}(b)=a$.

תנאי זה סימטרי ולכן $(f^{-1})^{-1}=f$

כמו כן $f^{-1}\circ f=Id_A$ ו- $f\circ f^{-1}=Id_B$.

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

<u>הוכחה:</u> יהיו $w_1,w_2\in W$ צ"ל: $f^{-1}(w_1+w_2)=f^{-1}(w_1)+f^{-1}(w_2)$

נסמן $v_1=f^{-1}(w_1)$ $v_2=f^{-1}(w_2)$ כאשר $v_1,v_2\in V$. לכן

לפי הגדרה של f^{-1}: $f(v_2)=w_2$ $f(v_1)=w_1$

f לינארית ולכן $f(v_1+v_2)=w_1+w_2=f(v_1)+f(v_2)$

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

כעת יהיו $w\in W$ ו- $c\in F$. צ"ל: $f^{-1}(cw)=cf^{-1}(w)$

נסמן $v=f^{-1}(w)$ $\Leftarrow$ $f(v)=w$ $\Leftarrow$

$f(cv)=cf(v)=cw$

$$\Rightarrow f^{-1}(cw)=f^{-1}(f(cv))=cv=cf^{-1}(w)$$

מש"ל ☺

נניח ש- $f:V\to W$ העתקה לינארית. נגדיר:

הגרעין של f: $Ker f=\{v: v\in V, f(v)=0_W\}$

התמונה של f: $Im f=\{w: w\in W, v\in V: f(v)=w\}$

<u>טענה:</u> $Ker f$ הוא תמ"ו של V.

<u>הוכחה:</u> $f(0_V)=f(0_F\cdot 0_V)=0_F\cdot f(0_V)=0_W$

ולכן $0_V\in Ker f$. כך $Ker f\neq\emptyset$.

יהיו $v_1,v_2\in Ker f$ אז: $f(v_1+v_2)=f(v_1)+f(v_2)=0_W+0_W=0_W$

$\Leftarrow$ $v_1+v_2\in Ker f$. יהיו $v\in Ker f$ ו- $c\in F$ אז: $f(cv)=cf(v)=c\cdot 0_W=0_W$

$\Leftarrow$ $cv\in Ker f$ $\Leftarrow$ $Ker f$ תמ"ו של V. מש"ל ☺

טענה: Imf הוא תמ"ו של W.

הוכחה: $0_W = f(0_V) \in Imf \Leftarrow Imf \neq \emptyset$

נניח ש $w_1, w_2 \in Imf$. צ"ל: $w_1+w_2 \in Imf$.

קיים $v_1 \in V$ כך ש $f(v_1) = w_1$ וקיים $v_2 \in V$ כך ש $f(v_2) = w_2$ אז $f(v_1+v_2) = f(v_1)+f(v_2) = w_1+w_2$

$\Leftarrow$ $w_1+w_2 \in Imf$ כי v_1+v_2 מקור שלו.

ניקח $w \in Imf$, $c \in F$. קיים $v \in V$ כך ש $f(v) = w$.

אז $f(cv) = cf(v) = cw$ לכן cv מקור של cw

לכן $cw \in Imf$ לכן Imf תמ"ו של w. מש"ל ☺

הערה: $f: V \to W$ הוא על אמ"מ $Imf = W$.

אין כאן מה להוכיח. זאת בדיוק ההגדרה של על.

טענה: $f: V \to W$ חח"ע אמ"מ $Ker f = \{0_V\}$.

הוכחה:

($\Leftarrow$) נניח ש- f חח"ע. כבר הוכחנו ש $0_V \in Kerf$

כי $f(0_V) = 0_W$. הוית ו- f חח"ע לכל $0_V \neq v \in V$

מתקיים $f(v) \neq f(0_V)$ לכן $v \notin Kerf \Leftarrow Kerf = \{0_V\}$.

($\Rightarrow$) נניח ש $Kerf = \{0\}$. נראה ש- f חח"ע.

יהיו $v_1, v_2 \in V$ $v_1 \neq v_2$. נראה ש $f(v_1) \neq f(v_2)$.

נניח בשלילה כי $f(v_1) = f(v_2)$ אז

$$f(v_1 - v_2) = f(v_1) - f(v_2) = 0_W$$

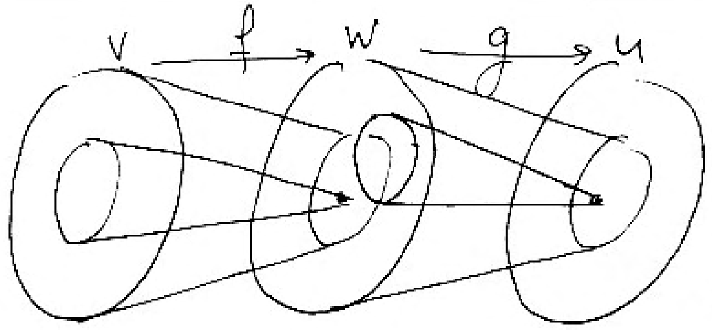
(כי $v_1 + (-1)v_2 = v_1 - v_2$)

אבל $Kerf = \{0_V\} \Leftarrow v_1 - v_2 = 0_V \Leftarrow v_1 = v_2$. סתירה!

$\Leftarrow$ f חח"ע

מש"ל ☺

38



טענה: $\ker f \subseteq \ker(gf)$

הוכחה: יהי $v \in \ker f \Leftarrow$

$$(gf)(v) = g(f(v)) = g(0_w) = 0_u$$

$\Leftarrow v \in \ker(gf)$.

$\Leftarrow \ker f \subseteq \ker(gf)$

מש"ל ☺

העתקות לינאריות

בפעם הקודמת הגדרנו את המושג העתקה לינארית בין מרחבים וקטוריים.

$f: V \to W$ העתקה לינארית של מרחבים וקטוריים V, W מעל אותו שדה F אם:

1 - לכל $v_1, v_2 \in V$ $\quad f(v_1 + v_2) = f(v_1) + f(v_2)$

2 - לכל $v \in V$ $c \in F$ $\quad f(cv) = cf(v)$

<u>הערה</u>: לנו יש מוסכמה שרושמים הסקלר משמאל - cv ולא vc.
אבל אם המוסכמה הייתה אחרת היינו רושמים $f(vc) = f(v)c$.
אבל בכל אופן אצלנו $vc = ERROR$!

כמו כן הגדרנו גרעין של העתקה = אותם הווקטורים של V שעוברים ל-0_W

$$Ker f = \{v \in V : f(v) = 0_W\}$$

התמונה של f היא הווקטורים ב-W שיש להם מקור ב-V

$$Im f = \{w \in W : \exists v \in V ,\ f(v) = w\}$$

הוכחנו ש-$Ker f$ תת מרחב של V
$Im f$ תת מרחב של W

<u>משפט</u>: נניח של-V יש בסיס (כלומר V נוצר סופית) אז:

$$\dim_F Ker f + \dim_F Im f = \dim_F V$$

<u>הערה</u>: בניסוח הזה יש בעייתיות מסוימת. אמרנו של-V יש בסיס והוכחנו שלכל תת מרחב שלו יש בסיס ולכן ל-$Ker f$ יש בסיס ולכן $\dim_F V$ ו-$\dim_F Ker f$ מוגדרים היטב. אבל $Im f$ הוא תת מרחב של W... מי אמר שבכלל יש לו בסיס?

<u>טענה</u>: אם $V = Sp(z_1, \dots, z_m)$ אז $Im f = Sp(f(z_1), \dots, f(z_m))$

<u>הוכחה</u>: נוכיח את ההכלה בשני הכיוונים:
$(\supseteq)$ הווקטור $f(z_i)$ שייך ל-$Im f$ כי יש לו מקור $z_i \in V$.

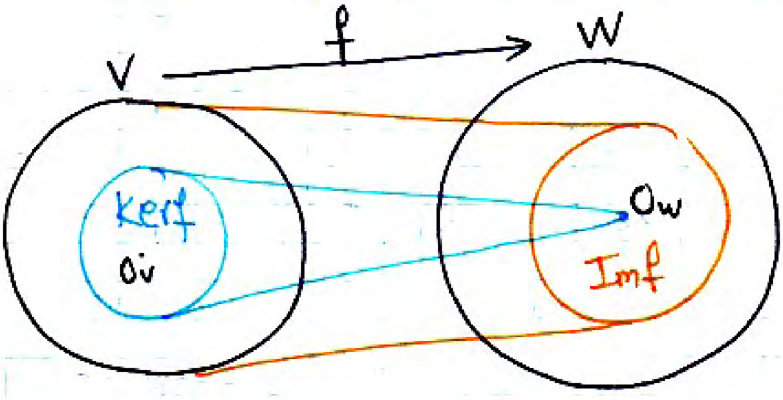
וכמו כן $f(z_1)\in Im f, \dots, f(z_m)\in Im f$. $Im f \subseteq W$ הוא
תת מרחב ולכן $Im f$ סגור לחיבור וכפל בסקלר.
$\Leftarrow$ $Sp(f(z_1),\dots,f(z_m)) \subseteq Im f$.

($\subseteq$) יהי $w\in Im f$ נראה ש- $w\in Sp(f(z_1),\dots,f(z_m))$
קיים מקור $v\in V$ כך ש- $f(v)=w$. לפי הנתון ש- $V=Sp(z_1,\dots,z_m)$
קיימים סקלרים $c_1,\dots,c_m\in F$ כך ש $v=c_1z_1+\dots+c_mz_m$.
f לינארית ולכן $w=f(v)=c_1f(z_1)+\dots+c_mf(z_m)$
כלומר $w\in Sp(f(z_1),\dots,f(z_m))$ $\Leftarrow$ $Im f\subseteq Sp(f(z_1),\dots,f(z_n))$
$\Leftarrow$ $Im f = Sp(f(z_1),\dots,f(z_n))$ מש"ל ☺

עכשיו הבעייתיות התיישבה. אם V מ"ו נוצר סופית ו- f העתקה לינארית בין V ל- W אז גם $Im f$ נוצר סופית. ולכן ניתן לדבר על המימד של $Im f$ ואפשר להתייחס למשפט. נרשום אותו שוב:

<u>משפט</u>: יהי V מרחב וקטורי נוצר סופית. ותהי $f:V\to W$ לינארית. אזי $\dim_F Ker f + \dim_F Im f = \dim_F V$

<u>הוכחה</u>:
קודם נעשה ציור סכמטי של המצב



נבחר בסיס $u_1,\dots,u_k$ של $Ker f$
נבחר בסיס $w_1,\dots,w_\ell$ של $Im f$
קיימים $v_1,\dots,v_\ell\in V$ כך ש $f(v_i)=w_i$ לכל $1\le i\le \ell$.
<u>טענה</u>: $u_1,\dots,u_k,v_1,\dots,v_\ell$ הם בסיס של V.
מכאן ינבע המשפט כי אז $\dim_F V = k+\ell = \dim_F Ker f + \dim_F Im f$

נראה שקבוצת הווקטורים הנ"ל היא בת"ל ופורשת.

א פורשת: $u_1,\dots,u_k,v_1,\dots,v_\ell\in V$ ולכן $Sp(u_1,\dots,u_k,v_1,\dots,v_\ell)\subseteq V$

יהי $v\in V$. נראה ש- $v\in Sp(u_1,\dots,u_k,v_1,\dots,v_\ell)$. נסתכל על $f(v)\in Imf$. נפתח את $f(v)$ לפי הבסיס $w_1,\dots,w_\ell$ של Imf. כלומר $f(v)=a_1w_1+\dots+a_\ell w_\ell$. נשים לב ש-

$$f(a_1v_1+\dots+a_\ell v_\ell)=a_1f(v_1)+\dots+a_\ell f(w_\ell)=$$

$$=a_1w_1+\dots+a_\ell w_\ell$$

לכן $f(a_1v_1+\dots+a_\ell v_\ell)=f(v)$ $\Leftarrow$

$$v-a_1v_1-\dots-a_\ell v_\ell\in Ker f$$

כי $f(v-a_1v_1-\dots-a_\ell v_\ell)=f(v)-f(a_1v_1+\dots+a_\ell v_\ell)=0_w$

לכן ניתן לפתח לפי הבסיס של הגרעין:

$$v-a_1v_1-\dots-a_\ell v_\ell=b_1u_1+\dots+b_ku_k\in Kerf$$

$\Leftarrow$ $v=b_1u_1+\dots+b_ku_k+a_1v_1+\dots+a_\ell v_\ell\in Sp(u_1,\dots,u_k,v_1,\dots,v_\ell)$

$\Leftarrow$ $Sp(u_1,\dots,u_k,v_1,\dots,v_\ell)=V$

ב אי תלות: נניח ש $b_1u_1+\dots+b_ku_k+a_1v_1+\dots+a_\ell v_\ell=0_v$

נראה ש- $b_1=\dots=b_k=a_1=\dots=a_\ell=0_F$.

$$0_w=f(0_v)=f(b_1u_1+\dots+b_ku_k+a_1v_1+\dots+a_\ell v_\ell)=$$

$$=b_1f(u_1)+\dots+b_kf(u_k)+a_1f(v_1)+\dots+a_\ell f(v_\ell)=$$

$$=0_w+a_1w_1+\dots+a_\ell w_\ell=0_w$$

$w_1,\dots,w_\ell$ בלתי תלויים ולכן $a_1=\dots=a_\ell=0_F$.

$\Leftarrow$ $b_1u_1+\dots+b_ku_k=0_v$

$u_1,\dots,u_k$ בת"ל ולכן $b_1=\dots=b_k=0_F$. קיבלנו אי תלות.

$\Leftarrow$ $v_1,\dots,v_\ell,u_1,\dots,u_k$ בסיס של V.

מש"ל ☺

אנחנו נראה בהמשך שהטענה הזאת יעילה בכל מיני מקרים.

דוגמא

$f:V\to W$ יש בסיס, V ו- W ...

f חח"ע ועל, כלומר $Ker f=\{0_V\}$ ו- $Im f = W$

ואז

$$dim_F V = dim_F Ker f + dim_F Im f = 0 + dim_F W = dim_F W$$

הגדרה: יהיו V,W מ"ו מעל שדה F. נגדיר

$$Hom_F(V,W) = \{f : f:V\to W \text{ לינארית}\}$$

כלומר $Hom_F(V,W)$ היא קבוצה של כל ההעתקות הלינאריות מ- V ל- W. נגדיר על קבוצה זו מבנה של מ"ו מעל F.

(1) נגדיר חיבור: נניח ש- $f:V\to W$ ו- $g:V\to W$ העתקות לינאריות. לכל $v\in V$ נגדיר

$$(f+g)(v) = f(v)+g(v)$$

קיבלנו $f+g: V\to W$

טענה: $f+g: V\to W$ היא העתקה לינארית.

הוכחה:

① נראה שהיא שומרת חיבור: יהיו $v_1,v_2\in V$ אז

$$(f+g)(v_1+v_2) = f(v_1+v_2)+g(v_1+v_2) =$$
$$= f(v_1)+f(v_2)+g(v_1)+g(v_2) =$$
$$= f(v_1)+g(v_1)+f(v_2)+g(v_2) = (f+g)(v_1)+(f+g)(v_2)$$

② נראה שהיא שומרת כפל בסקלר: יהיו $v\in V$ ו- $c\in F$

$$(f+g)(cv) = f(cv)+g(cv) = cf(v)+cg(v) =$$
$$= c(f(v)+g(v)) = c(f+g)(v)$$

כ"ל $f+g$ היא העתקה לינארית כלומר $f+g\in Hom_F(V,W)$

אושן ☺

(2) נגדיר כפל: עבור $f:V\to W$ העתקה לינארית

ו- $a\in F$ נגדיר $(af):V\to W$ לכל $v\in V$

$$(af)(v)=af(v)$$

__טענה:__ $af:V\to W$ היא העתקה לינארית

__הוכחה:__

א. שומרת חיבור: יהיו $v_1,v_2\in V$ אז:

$$(af)(v_1+v_2)=af(v_1+v_2)=a(f(v_1)+f(v_2))=$$
$$=af(v_1)+af(v_2)=(af)(v_1)+(af)(v_2)$$

ב. שומרת כפל בסקלר: יהיו $v\in V$ ו- $c\in F$

$$(af)(cv)=a(f(cv))=a(c(f(v)))=$$
$$=(ac)f(v)=(ca)f(v)=c(a(f(v)))=$$
$$=c(af(v))$$

$\Leftarrow$ $af\in Hom_F(V,W)$ מש"ל ☺

כדי להראות ש $Hom_F(V,W)$ מ"ו מעל F נשאר לבדוק

כי מתקיימות 8 האקסיומות של מרחב וקטורי:

העתקות לינאריות של מרחבים וקטוריים

F שדה V,W מרחבים וקטוריים מעל F. הגדרנו:

$$Hom_F(V,W) = \{ f : f:V\to W \text{ העתקה לינארית} \}$$

עבור $f:V\to W$, $g:V\to W$ הגדרנו $(f+g):V\to W$ כך:

$$(f+g)(v) = f(v)+g(v) \qquad \forall v\in V$$

עבור $f:V\to W$ ו- $a\in F$ הגדרנו $(af):V\to W$ כך:

$$(af)(v) = a(f(v)) \qquad \forall v\in V$$

ראינו שאם $f,g\in Hom_F(V,W)$ ו- $a\in F$ אז:

$$f+g,\ af \in Hom_F(V,W)$$

כלומר ב $Hom_F(V,W)$ יש סגירות לחיבור וכפל בסקלר.

> לשם הפורמליות דרוש להגדיר שוויון בין העתקות. נאמר ש $f=g$ אם לכל v $f(v)=g(v)$. עם הגדרה זו נעשה שימוש בכתיבה שלנו.

נבדוק את קיום שאר אקסיומות המרחב הוקטורי:

<u>חיבור</u> יהיו $h,f,g\in Hom_F(V,W)$ לכל $v\in V$

(1) סגירות V

(2) קומוטטיביות: $f+g=g+f$ כי:

$$(f+g)(v) = f(v)+g(v) = g(v)+f(v) = (g+f)(v)$$

(3) אסוציאטיביות: $(f+g)+h = f+(g+h)$ כי

$$((f+g)+h)(v) = (f+g)(v)+h(v) = (f(v)+g(v))+h(v) =$$
$$= f(v)+(g(v)+h(v)) = f(v)+(g+h)(v) = (f+(g+h))(v)$$

(4) קיום האפס. נגדיר $0_{V,W}:V\to W$ ע"י $0_{V,W}(v)=0_W$ לכל $v\in V$. נראה שזאת העתקה לינארית:

(1) שומרת חיבור: לכל $v,w\in V$

$$0_{V,W}(v+w) = 0_W = 0_W+0_W = 0_{V,W}(v)+0_{V,W}(w)$$

(2) שומרת כפל בסקלר: לכל $v\in V$ ו- $a\in F$:

$$0_{V,W}(av) = 0_W = a\cdot 0_W = a\cdot 0_{V,W}(v)$$

עכשיו נראה שהעתקת האפס ניטרלית לחיבור:

$$(f+0_{V,W})(v) = f(v)+0_{V,W}(v) = f(v)+0_W = f(v)$$

$\Leftarrow \quad f+0_{V,W} = f$.

ה) איבר נגדי. לכל $f \in Hom_F(V,W)$ נגדיר $-f: V \to W$

ע"י $(-f)(v) = -f(v)$. נראה שזאת העתקה לינארית:

1) שומרת חיבור: לכל $v,w \in V$

$(-f)(v+w) = -f(v+w) = -(f(v)+f(w)) = -f(v) + (-f(w)) = (-f)(v) + (-f)(w)$

2) שומרת כפל בסקלר: לכל $v \in V$ ו- $a \in F$

$(-f)(av) = -f(av) = -af(v) = ((-1_F)a)f(v) = \ldots$

$= c(-1_F)f(v) = c((-1_F)f(v)) = c(-f(v)) = c((-f)(v))$

קיבלנו ש $-f$ היא לינארית.

$(f+(-f))(v) = f(v) + (-f)(v) = f(v) + (-f(v)) = 0_W = f_{0,W}(v)$

$\Leftarrow$ $-f$ נגדי ל- f.

<u>כפל בסקלר</u>

א) סגירות. ✓

ב) לכל $f \in Hom_F(V,W)$ כי $1_F f = f$:

$(1_F f)(v) = 1_F(f(v)) = f(v)$

ג) לכל $f \in Hom_F(V,W)$ ו- $a,b \in F$

$((a \cdot b)f)(v) = (ab)(f(v)) = a(bf(v)) =$

$= a((bf)(v)) = (a(bf))(v)$

ד) לכל $f,g \in Hom_F(V,W)$ ו- $a,b \in F$

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

$= (af)(v) + (bf)(v) = (af+bf)(v)$

$(a(f+g))(v) = a((f+g)(v)) = a(f(v)+g(v)) =$

$= af(v) + ag(v) = (af)(v) + (ag)(v) =$

$= (af+ag)(v)$

סיימנו את בדיקת קיום כל אקסיומות המרחב הנקטורי:

<u>מסקנה</u> $Hom_F(V,W)$ מ"ו מעל F עם הפעולות כפי שהגדרנו.

<u>משפט</u>: אם ל-V ול-W יש בסיסים אז

$$\dim_F Hom(V,W) = \dim_F V \cdot \dim_F W$$

<u>הוכחה</u>: בשלב מאוחר יותר. אבל תחשבו על זה.

<u>משפט</u>: נניח ש- $v_1,\dots,v_n \in V$ בסיס של V. אז לכל בחירה שרירותית של איברים $u_1,\dots,u_n \in W$ קיימת העתקה לינארית יחידה $f:V\to W$ רק ש $f(v_i)=u_i$ לכל $1\le i\le n$.

(נדגיש שאין הווקטורים $u_1,\dots,u_n \in W$ חייבים להיות בסיס של W).

<u>הוכחה</u>: לכל וקטור $v\in V$ קיימת הצגה יחידה $v=\sum_{i=1}^n c_i v_i$

נגדיר את $f:V\to W$ ע"י $f(v)=\sum_{i=1}^n c_i u_i$ (אותם ה-c-ים כמו קודם). צריך לבדוק:

(א) ההעתקה $f:V\to W$ לינארית.

(ב) $f(v_i)=u_i$ לכל $1\le i\le n$

(ג) f עם התכונות הנ"ל היא יחידה.

נראה שכל הדברים האלה נכונים.

(א) יהיו $v,v'\in V$ רק ש $v=\sum c_i v_i$ ו- $v'=\sum c_i' v_i$: $v+v'=\sum(c_i+c_i')v_i$

$f(v)=\sum c_i u_i$ ו- $f(v')=\sum c_i' u_i$

$$f(v+v') = \sum(c_i+c_i')u_i = \sum c_i u_i + \sum c_i' u_i = f(v)+f(v')$$

$\Leftarrow$ f שומרת חיבור.

יהי $v\in V$, $v=\sum c_i v_i$ ויהי $a\in F$ אז $av=\sum(ac_i)v_i$

$$f(av)=\sum(ac_i)u_i = \sum a(c_iu_i) = a\sum c_iu_i = af(v)$$

$\Leftarrow$ f שומרת כפל בסקלר $\Leftarrow$ f לינארית.

(ב) $v_i = 0_F\cdot v_1 + \dots + 1_F\cdot v_i + \dots + 0_F\cdot v_n$

$\Leftarrow$ $f(v_i) = 0_F\cdot u_1+\dots+1_F u_i+\dots+0_F u_n = 1_F u_i = u_i$

(ג) יחידות: נניח כי העתקה לינארית $g:V\to W$ שגם היא מקיימת $g(v_i)=u_i$ לכל $1\le i\le n$

עבור $v=\sum c_iv_i \in V$ בגלל הלינאריות של g

$g(v)=\sum c_i g(v_i) = \sum c_i u_i = f(v)$ $\Leftarrow$ $f=g$ מש"ל ☺

$v_1,\dots,v_n \in V$ בסיס של V

$w_1,\dots,w_m \in W$ בסיס של W

אז לכל העתקה לינארית $f: V \to W$ נוכל להתאים מטריצה מסדר $m\times n$ באופן הבא:

$$f(v_1) = a_{11} w_1 + a_{21} w_2 + \dots + a_{m1} w_m$$
$$f(v_2) = a_{12} w_1 + a_{22} w_2 + \dots + a_{m2} w_m$$
$$\vdots$$
$$f(v_n) = a_{1n} w_1 + a_{2n} w_2 + \dots + a_{mn} w_m$$

קיבלנו $n\cdot m$ סקלרים (a_{ij}) שנבנה מהם מטריצה:

$$A_f = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mm} \end{pmatrix}$$

במטריצה זו יש m שורות ו-n עמודות ואומרים שהסדר שלה $m\times n$. זאת המטריצה של ההעתקה הלינארית $f: V\to W$ כאשר נתונים בסיסים למרחבים.

נשים לב ש $m=\dim W$; $n=\dim V$.

לפי ההגדרה שלנו, מספר השורות של המטריצה A_f שווה ל $\dim_F W = m$ - המימד של הטווח, ומספר העמודות של A_f שווה ל $\dim_F V$ - המימד של התחום.

דוגמה:

$F=\mathbb{R}$, $V=\mathbb{R}^3$, $W=\mathbb{R}^2$ $\quad f:\mathbb{R}^3 \to \mathbb{R}^2$

$$f(a_1,a_2,a_3) = (3a_1-2a_2+5a_3, -a_1+2a_2-10a_3)$$

תרגיל: להוכיח כי f היא העתקה לינארית.

ניקח את הבסיסים הסטנדרטיים של $\mathbb{R}^3$ ושל $\mathbb{R}^2$

$d_1=(1,0)$ $d_2=(0,1)$ $e_1=(1,0,0)$ $e_2=(0,1,0)$ $e_3=(0,0,1)$

~~$f(e_1)=f(1,0,0)=(3,-1)=3d_1+(-1)d_2$~~

$f(e_2$

מה המטריצה של ההעתקה f ?

נחשב את הפעולת ההעתקה של איברי הבסיס:

$$f(e_1) = f(1,0,0) = (+3,-1) = 3(1,0) - 1(0,1) = 3d_1 + (-1)d_2$$
$$f(e_2) = f(0,1,0) = (-2,2) = -2(1,0) + 2(0,1) = (-2)d_1 + 2d_2$$
$$f(e_3) = f(0,0,1) = (5,-10) = 5(1,0) + (-10)(0,1) = 5d_1 + (-10)d_2$$

$\Leftarrow$ המטריצה תהיה מדרגה 2×3 (ונקבל)

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

$$n = \dim \mathbb{R}^3 = 3 \qquad m = \dim \mathbb{R}^2 = 2$$

<u>משפט</u>: אם ל-V בסיס $v_1,\dots,v_n$ ול-W בסיס $w_1,\dots,w_m$ אז לכל מטריצה A מסדר $m\times n$ עם מקדמים בשדה F קיימת העתקה לינארית יחידה $f: V \to W$ רק ש $A_f = A$

<u>הוכחה</u>: נתונה מטריצה $A = (a_{ij})$ מסדר $m\times n$.
נגדיר $u_j = \sum_{i=1}^{m} a_{ij} w_i \in W$
לפי המשפט הקודם קיימת העתקה לינארית יחידה $f: V \to W$ רק ש $f(v_j) = u_j$ לכל $1 \le j \le n$.
לפי ההגדרה $A_f = A$.

מש"ל ☺

לבין השאר הודעה על הלוח:
" חג שמח שהדהר לא שבלוע ε אגבו ! "

העתקות לינאריות ומטריצות

F שדה V,W מ"ו מעל F.

$v_1,\dots,v_n\in V$ בסיס ל-V ו-$w_1,\dots,w_m\in W$ בסיס ל-W.

לכל העתקה לינארית $f:V\to W$ הגדרנו מטריצה A_f

מסדר $m\times n$ (m שורות ו-n עמודות) באופן הבא:

מסתכלים איך f פועלת על איברי הבסיס של V

$$f(v_j)=\sum_{i=1}^{m}a_{ij}w_i \qquad 1\le j\le n$$

נכתוב במפורש למי שלא מבין

$$f(v_1)=a_{11}w_1+a_{21}w_2+\dots+a_{m1}w_m$$
$$f(v_2)=a_{12}w_1+a_{22}w_2+\dots+a_{m2}w_m$$
$$\vdots$$
$$f(v_n)=a_{1n}w_1+a_{2n}w_2+\dots+a_{mn}w_m$$

אזי $A_f=(a_{ij})$ כלומר

$$A_f=\begin{pmatrix} a_{11} & a_{21} & & a_{m1}\\ a_{21} & a_{22} & & a_{m2}\\ a_{m1} & a_{2n} & & a_{mn}\end{pmatrix}$$

המטריצה הזאת מוגדרת באופן יחיד בהינתן בסיסים קבועים של V ושל W. בהמשך נראה איך המטריצה משתנה כאשר הבסיסים משתנים.

ראינו גם שבהינתן מטריצה כזאת היא מגדירה העתקה לינארית באופן יחיד!

נניח שיש לנו עוד העתקה לינארית $g : V \to W$

רק ש-g פועלת על איברי הבסיס באופן הבא:

$g(v_j) = \sum_{i=1}^{m} b_{ij} w_i \quad 1 \le j \le n$

אז המטריצה המתאימה ל-g היא $A_g = (b_{ij})$.

וגם היא כמובן מטריצה מסדר $m \times n$.

שוב, למי שלא מבין את הכתיב המקוצר:

$$g(v_1) = b_{11} w_1 + b_{21} w_2 + \dots + b_{m1} w_m$$
$$g(v_2) = b_{12} w_1 + b_{22} w_2 + \dots + b_{m2} w_m$$
$$\vdots$$
$$g(v_n) = b_{1n} w_1 + b_{2n} w_2 + \dots + b_{mn} w_m$$

$$\Rightarrow A_g = \begin{pmatrix} b_{11} & b_{21} & \dots & b_{m1} \\ b_{12} & b_{22} & \dots & b_{m2} \\ \vdots & & & \\ b_{1n} & b_{2n} & \dots & b_{mn} \end{pmatrix}$$

הגדרנו את ההעתקה הלינארית $(f+g) : V \to W$

ע"י $(f+g)(v) = f(v) + g(v)$ לכל $v \in V$

מהי המטריצה המתאימה ל-$f+g$? האינטואיציה אומרת ש $A_{f+g} = A_f + A_g$.

יש לנו הגדרה, אז נבדוק את זה:

$$1 \le j \le n \quad (f+g)(v_j) = f(v_j) + g(v_j) = \sum_{i=1}^{m} a_{ij} w_i + \sum_{i=1}^{m} b_{ij} w_i$$
$$= \sum_{i=1}^{m} (a_{ij} + b_{ij}) w_i$$

$$\Rightarrow A_{f+g} = (a_{ij} + b_{ij}) =$$
$$= (a_{ij}) + (b_{ij}) = A_f + A_g$$

* נמאס לי לרשום כל פעם את הפיתוח. אני מרגישה שאנחנו בשלב מספיק לעבור לכתיב המקוצר

רק סכום של מטריצות. ניתן לחבר מטריצות אם ורק אם הן מאותו הסדר וגם המטריצה של הסכום היא מאותו סדר.

$$\begin{pmatrix} 2 & 3 & 1 \\ 4 & 4 & 8 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \text{ERROR}$$

לכל סקלר $c \in F$ הגדרנו העתקה לינארית $(cf): V \to W$

ע"י $(cf)(v) = cf(v)$ לכל $v \in V$ נשאלת אפוא

השאלה: מהי המטריצה המתאימה ל- cf ?

באופן דומה למה שעשינו קודם נבדוק איך cf פועלת

על איברי הבסיס.

$$(cf)(v_j) = cf(v_j) = c \cdot \sum_{i=1}^{m} a_{ij} w_i = \quad 1 \le j \le n$$
$$= \sum_{i=1}^{m} c a_{ij} w_i$$

$$\Rightarrow A_{cf} = (ca_{ij}) = cA_f$$

נסמן ב- $M_{m,n}(F)$ קבוצת כל המטריצות מסדר

$m \times n$ עם מקדמים בשדה F. הגדרנו ב- $M_{m,n}(F)$

חיבור (של מטריצות) וכפל (של מטריצה בסקלר).

נשאלת אפוא השאלה: האם קיבלנו ב- $M_{m,n}(F)$ מבנה

של מרחב וקטורי מעל F ?

תשובה: כן! בדיקת האקסיומות הוא תרגיל שגרתי,

אם להיזכר איך הוכחנו ש- F^n הוא מרחב וקטורי מעל F.

מצד שני, אפשר לפשט את זה מאוד: אנחנו יודעים

שמרחב העתקות הוא מרחב וקטורי. ואנחנו יודעים שלכל

מטריצה מתאימה העתקה לינארית יחידה ולהפך. כמו כן,

ראינו שחיבור העתקות מביא לחיבור מטריצות וכפל

העתקה בסקלר מביא לכפל מטריצה בסקלר. כלומר

מרחב העתקות הלינאריות איזומורפי לקבוצת המטריצות

ולכן גם $M_{m,n}(F)$ מ"ו מעל F.

עתה, כשמסתכלים גם על $Hom_F(V,W)$ וגם על $M_{m,n}(F)$ כמרחבים

וקטוריים מעל F, נמצא שההעתקה $\varphi: Hom_F(V,W) \to M_{m,n}(F)$

הנ"ל: $f \longmapsto A_f$ היא שומרת חיבור כי $A_{f+g} = A_f + A_g$

ושומרת כפל בסקלר כי $A_{cf} = cA_f$.

כלומר φ העתקה לינארית חח"ע ועל!

האמת היא שעוד לא הוכחנו ש-φ חח"ע (נראה זאת כעת:

ובכן, ניקח $f: V \to W$, $g: V \to W$ העתקות לינאריות.

ונניח כי $A_f = A_g$. נראה ש- $f = g$. ואכן,

$$f(v_j) = \sum_{i=1}^{m} a_{ij} w_i = \sum_{i=1}^{m} b_{ij} w_i = g(v_j) \qquad 1 \le j \le n$$

↓ אם המטריצות שוות המקדמים שווים

כלומר f ו- g פועלות באותו אופן על איברי הבסיס.

והיה לנו משפט שאומר שאם שתי העתקות פועלות באותו אופן על איברי הבסיס אזי הן שוות. $f = g$.

$\Leftarrow$ φ חח"ע.

כלומר φ איזומורפיזם בין מרחב ההעתקות למרחב המטריצות המתאימות! לסיכום:

<u>משפט</u>: $Hom_F(V,W) \longrightarrow M_{m,n}(F)$, $f \longmapsto A_f$ הוא איזומורפיזם של מרחבים וקטוריים מעל F.

<u>משפט</u>: $\dim_F M_{m,n}(F) = m \cdot n$

<u>הוכחה</u>: נסתכל מבסיס הסטנדרטי של $M_{m,n}(F)$:

$$E_{ij} = \begin{pmatrix} 0_F & \vdots & 0_F \\ \cdots & 1_F & \cdots \\ 0_F & \vdots & 0_F \end{pmatrix}$$

(כלומר $e_{ij} = 1_F$ וכל שאר המקדמים במטריצה הם 0_F)

טענה: $\{E_{ij}\}$, $1 \le i \le m$, $1 \le j \le n$ הם בסיס של $M_{m,n}(F)$.

אם הטענה הזאת נכונה אזי $\dim_F M_{m,n}(F) = m \cdot n$.

נוכיח את הטענה:

(א) $\{E_{ij}\}$ קבוצה פורשת: נניח ש- $A = (a_{ij}) \in M_{m,n}(F)$

$$\Rightarrow \quad A = \sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} a_{ij} E_{ij} = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} E_{ij}$$

(ב) $\{E_{ij}\}$ בת"ל: נניח $\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} E_{ij} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$. נראה ש- $a_{ij} = 0_F$. אכן

$$\sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} E_{ij} = (a_{ij}) \Rightarrow (a_{ij}) = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \Rightarrow a_{ij} = 0_F$$

מש"ל ☺

משפט: אם ל-U יש בסיס ו- $f: U \to U'$ איזומורפיזם של מרחבים וקטוריים (כלומר, f העתקה לינארית חח"ע ועל) אז $\dim_F U = \dim_F U'$.

הוכחה: f חח"ע ולכן $\mathrm{Ker} f = \{0_U\}$. f על ולכן $\mathrm{Im} f = U'$. הוכחנו ש-

$$\dim_F \mathrm{Ker} f + \dim_F \mathrm{Im} f = \dim_F U$$

$$\Rightarrow \quad 0 + \dim_F U' = \dim_F U$$

מש"ל ☺

משפט: $\dim \mathrm{Hom}_F(V,W) = \dim_F V \cdot \dim_F W$ כאשר ל-V ול-W יש בסיסים.

הוכחה: נניח ש $\dim_F V = n$, $\dim_F W = m$

⇐ ראינו ש $\mathrm{Hom}_F(V,W)$ איזומורפי ל- $M_{mn}(F)$

ולכן $\dim_F M_{mn}(F) = \dim_F \mathrm{Hom}_F(V,W)$

והוכחנו ש $\dim_F M_{m,n}(F) = m \cdot n$

⇐ $\dim_F \mathrm{Hom}_F(V,W) = m \cdot n = \dim_F W \cdot \dim_F V$

מש"ל ☺

דוגמה שלא ברור למה היא קשורה:

$\dim_{\mathbb{C}} \mathbb{C} = 1$ אבל $\dim_{\mathbb{R}} \mathbb{C} = 2$

כאן $\{1\}$ הוא בסיס. כאן $\{1, i\}$ הם בסיס.

ברור ש $a+bi = a \cdot 1 + b \cdot i$

1 ו- i בת"ל כי אם

$0 + 0i = a1 + bi$

אז $a=0$, $b=0$

אה, הבנתי למה זה חשוב. השכותבים מאיפה, אם ברור מעל איזה שדה לא רושמים אותו. אבל זה כן משפיע!!!

נניח ש V, W, U מ"ו מעל שדה F.

$v_1,\dots,v_n \in V$ בסיס ל- V.

$w_1,\dots,w_m \in W$ בסיס ל- W.

$u_1,\dots,u_l \in U$ בסיס ל- U.

נניח שיש העתקות f, g רק $\underbrace{V \xrightarrow{f} W \xrightarrow{g} U}_{gf}$

ל-f מתאימה מטריצה A_f מסדר $m\times n$

ל-g מתאימה מטריצה A_g מסדר $l\times m$.

נשאלת אפוא השאלה, איזו מטריצה מתאימה ל- $g\circ f$

ל- $g\circ f$ מתאימה מטריצה A_{gf} מסדר $l\times n$.

מה הקשר בין A_f, A_g ו- A_{gf} ???

מהי מטריצת ההרכבה של הרכבה של העתקות?

ט לאור ועוד בפעם הבאה...

העתקות לינאריות ומטריצות

V, W, U מ"ו מעל שדה F.

$v_1, \ldots, v_n \in V$ בסיס ל- V $f: V \to W$ לינארית

$w_1, \ldots, w_m \in W$ בסיס ל- W $g: W \to U$ לינארית

$u_1, \ldots, u_\ell \in U$ בסיס ל- U $(g \cdot f): V \to U$ לינארית

לכל אחת מההעתקות יש מטריצה (כמו שראינו בשיעורים הקודמים):

$f(v_j) = \sum_{i=1}^{m} a_{ij} w_i \qquad A_f = (a_{ij})$ מסדר $m \times n$

$g(w_i) = \sum_{k=1}^{\ell} b_{ki} u_k \qquad A_g = (b_{ki})$ מסדר $\ell \times m$

$(gf)(v_j) = \sum_{k=1}^{\ell} c_{kj} u_k \qquad A_{g \cdot f} = (c_{kj})$ מסדר $\ell \times n$

אנחנו רוצים לדעת מה הקשר בין A_g, A_f ו- A_{gf}.

יהיו לנו הרבה אינדקסים אז נעשה הסכמה.

$i = 1, \ldots, m$

$j = 1, \ldots, n$

$k = 1, \ldots, \ell$

$$\sum_{k=1}^{\ell} c_{kj} u_k = (gf)(v_j) = g(f(v_j)) \overset{\text{הגדרה של } f}{=} g\left(\sum_{i=1}^{m} a_{ij} w_i\right) =$$

$$\overset{g \text{ לינארית}}{=} \sum_{i=1}^{m} a_{ij} g(w_i) = \sum_{i=1}^{m} a_{ij} \left(\sum_{k=1}^{\ell} b_{ki} u_k\right) =$$

$$= \sum_{i=1}^{m} \sum_{k=1}^{\ell} a_{ij} b_{ki} u_k = \sum_{i=1}^{m} \sum_{k=1}^{\ell} b_{ki} a_{ij} u_k =$$

$$\overset{\text{החלפת סדר סכמה}}{=} \sum_{k=1}^{\ell} \sum_{i=1}^{m} b_{ki} a_{ij} u_k = \sum_{k=1}^{\ell} \left(\sum_{i=1}^{m} b_{ki} a_{ij}\right) u_k$$

קיבלנו שתי הצגות לווקטור $(gf)(v_j)$ באמצעות אותו הבסיס.

$$\Rightarrow c_{kj} = \sum_{i=1}^{m} b_{ki} a_{ij}$$

וזה הקשר בין המטריצות!

אם $l \neq n$
אז
AB=ERROR

<u>הגדרה</u>: תהי $B=(b_{ki})$ מטריצה מסדר $l\times m$
ותהי $A=(a_{ij})$ מטריצה מסדר $m\times n$
נגדיר את המכפלה BA באופן הבא:
BA מטריצה מסדר $l\times n$ $BA=(c_{kj})$ ומתקיים
$c_{kj}=\sum_{i=1}^{m} b_{ki}a_{ij}$, $k=1,\dots,l$, $j=1,\dots,n$.

<u>משפט</u>: $A_{gf}=A_gA_f$
המשפט הזה נכון מעצם הגדרת כפל מטריצות. כלומר, הגדרנו כפל מטריצות רק שיתאים למשפט הזה.

<u>דוגמה</u>:

$$\underset{A}{\begin{pmatrix} 2 & 3 & 1 \\ 1 & -1 & 0 \end{pmatrix}}\underset{B}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix}}=\underset{AB}{\begin{pmatrix} 26 & 32 & 38 & 44 \\ -4 & -4 & -4 & -4 \end{pmatrix}}$$

סדר: 2×3 3×4 2×4

בקיצור מה שכתוב בנוסחה הוא בעצם שעושים כפל איבר איבר של כל שורה ב-A עם טור ב-B ואז מסכמים. (למשל: $2\cdot 1+3\cdot 5+1\cdot 9=2+15+9=26$)
ושמים במקום המתאים ב-AB

<u>משפט</u>: כפל מטריצות הוא אסוציאטיבי, כאשר הוא מוגדר.
<u>הוכחה</u> (נורמלית): ראינו שיש איזומורפיזם בין מרחב ההעתקות למרחב המטריצות. ראינו שהרכבה של העתקות היא אסוציאטיבית ולכן כפל מטריצות הוא אסוציאטיבי ☺
<u>סימון</u>: עבור מטריצה A נסמן $[A]_{ij}$ את האיבר של A העומד בשורה מספר i ועמודה מספר j.
<u>הוכחה</u> (ראש בקיר)
יהיו A,B,C מטריצות מסדר $p\times q$, $q\times r$, $r\times s$ בהתאמה.
נוכיח כי $(AB)C=A(BC)$

נשים לב שממדיות הסדרים של המטריצות הכל מסתדר:

$$\underbrace{(AB)}_{p\times r}\ \underbrace{C}_{r\times s} = \underbrace{A}_{p\times q}\ \underbrace{(BC)}_{q\times s}$$

$$p\times s \qquad\qquad p\times s$$

כעת נעשה קצת חישובים:

$$[(AB)C]_{hk} = \sum_{j=1}^{r} [AB]_{hj}[C]_{jk} =$$

$$= \sum_{j=1}^{r}\left(\sum_{i=1}^{q}[A]_{hi}[B]_{ij}\right)[C]_{jk} = \sum_{j=1}^{r}\sum_{i=1}^{q}[A]_{hi}[B]_{ij}[C]_{jk}$$

$$[A(BC)]_{hk} = \sum_{i=1}^{q}[A]_{hi}[BC]_{ik} =$$

$$= \sum_{i=1}^{q}[A]_{hi}\left(\sum_{j=1}^{r}[B]_{ij}[C]_{jk}\right) = \sum_{i=1}^{q}\sum_{j=1}^{r}[A]_{hi}[B]_{ij}[C]_{jk}$$

אבל אלה סכומים סופיים לכן ניתן להחליף את סדר הסכימה

$$\Leftarrow \quad [(AB)C]_{hk} = [A(BC)]_{hk}$$

$$\Leftarrow \quad (AB)C = A(BC)$$

מש"ל ☺

נוסחת שינוי בסיס ☺-☺

V,W מ"ו מעל F. $v_1,\dots,v_n\in V$ בסיס של V.

$w_1,\dots,w_m\in W$ בסיס של W.

$v_1',\dots,v_n'\in V$ עוד בסיס של V. $w_1',\dots,w_m'\in W$ עוד בסיס של W.

$f:V\to W$ העתקה לינארית.

$A_f=(a_{ij})$ - המטריצה לפי הבסיסים הראשונים.

$A_f'=(a_{ij}')$ - המטריצה לפי הבסיסים הנוספים.

מה הקשר בין (a_{ij}) ו- (a_{ij}') ?

לצורך כך נסתכל על ההרכבה של ההעתקות:

$$f = Id_W\circ f\circ Id_V \qquad f: V\xrightarrow{Id_V} V\xrightarrow{f} W\xrightarrow{Id_W} W$$

$$v\longmapsto v\longmapsto f(w)\longrightarrow f(w)$$

$$v_1',\dots,v_n' \qquad v_1,\dots,v_n \qquad w_1,\dots,w_m \qquad w_1',\dots,w_m'$$

הוכחנו שהרכבה של העתקות מתאימה לכפלה של מטריצות והיא פעולה אסוציאטיבית. ונקבל

$$A'_f = P A_f Q$$

כאשר P - המטריצה המתאימה ל-Id_W ביחס לבסיסים

Q - המטריצה המתאימה ל-Id_V ביחס לבסיסים

כלומר ב-P יש $w_1,\dots,w_m$ בתחום ו-$w'_1,\dots,w'_m$ בטווח

ב-Q יש $v'_1,\dots,v'_n$ בתחום ו-$v_1,\dots,v_n$ מטווח.

נשים לב ש-P ו-Q אינן תלויות ב-f, אלא רק בבסיסים שבחרנו. כלומר הנוסחה הזאת נכונה לכל העתקה לינארית f, בהינתן שבחרנו בסיסים קבועים.

P היא מטריצה מסדר $m\times m$ ו-Q היא מטריצה מסדר $n\times n$.

נחשב את המטריצות:

$$P=(p_{ij}) \qquad Id_W(w_j)=w_j=\sum_{i=1}^{m} p_{ij}w'_i \qquad 1\le j\le m$$

P נקראת מטריצת מעבר בסיסים - מבסיס $w_1,\dots,w_m$ לבסיס $w'_1,\dots,w'_m$.

מה עם Q? בדיוק אותו הדבר אבל הפוך:

$$Q=(q_{lk}) \qquad Id_V(v'_k)=v'_k=\sum_{l=1}^{n} q_{lk}v_l \qquad 1\le k\le n$$

זה באופן כללי. נסתכל על מקרה פרטי. מה קורה כאשר

$f:V\to V$ אז $A_f=(a_{ij})$ מסדר $n\times n$ (התחום והטווח באותו בסיס)

$A'_f=(a'_{ij})$ מסדר $n\times n$. (התחום והטווח באותו בסיס חדש)

כמו קודם יש לנו:

$$\underset{v'_1\dots v'_n}{V} \xrightarrow{Id_V} \underset{v_1\dots v_n}{V} \xrightarrow{f} \underset{v_1\dots v_n}{V} \xrightarrow{Id_V} \underset{v'_1\dots v'_n}{V}$$

$$A'_f = P A_f Q$$

P - מטריצת מעבר בסיס מ-$v_1\dots v_n$ ל-$v'_1\dots v'_n$

Q - מטריצת מעבר בסיס מ-$v'_1\dots v'_n$ ל-$v_1\dots v_n$

משפט: אם P היא מטריצת מעבר בסיסים מ- $v_1 \dots v_n$ ל- $v'_1, \dots, v'_n$ ו- Q היא מטריצת מעבר בסיסים בכיוון ההפוך: מ- $v'_1 \dots v'_n$ ל- $v_1, \dots, v_n$ אז

$QP = PQ = I$ כאשר

$$I = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$ (1-ים באלכסון הראשי והשאר אפסים)

הוכחה:

נסתכל בהעתקות לינאריות $Id_V : \underset{v_1 \dots v_n}{V} \xrightarrow{Id_V} \underset{v'_1 \dots v'_n}{V} \xrightarrow{Id_V} \underset{v_1 \dots v_n}{V}$

$$Id_V(v_1) = 1_F v_1 + 0_F v_2 + \dots + 0_F v_n$$
$$\vdots$$
$$Id_V(v_j) = 0_F v_1 + \dots + 1_F v_j + \dots + 0_F v_n$$
$$\vdots$$
$$Id_V(v_n) = 0_F v_1 + \dots + 0_F v_{n-1} + 1_F v_n$$

$$\Rightarrow QP = I = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

באותו אופן אפשר להסתכל על $Id_V : \underset{v'_1 \dots v'_n}{V} \xrightarrow{Id_V} \underset{v_1 \dots v_n}{V} \xrightarrow{Id_V} \underset{v'_1 \dots v'_n}{V}$

ואז נקבל $PQ = I = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$.

מש"ל ☺

הגדרה: אם $I = QP = PQ$ אז מגדירים

$$P^{-1} = Q, \quad Q^{-1} = P$$

מטריצות הופכיות אחת לשנייה, כמובן זה נכון רק למטריצות ריבועיות.

תחת הגדרה זו נקבל נוסחת שינוי בסיס $A_{f'} = PA_fP^{-1}$ או
$A_{f'} = Q^{-1}A_fQ$

כאשר $f: V \to V$.

(51) 4.1.06
ליניארית

העתקות ליניאריות ומטריצות

יש עוד נקודה יסודית שיש לדון בה. נזכיר שאנחנו דנים במצב הבא:

V,W מ"ו מעל F. $v_1,\dots,v_n\in V$ בסיס של V

$w_1,\dots,w_m\in W$ בסיס של W

$f:V\to W$ העתקה ליניארית ו- $A_f=(a_{ij})$ המטריצה שלה ביחס לבסיסים הנ"ל. לכל $1\le j\le n$ $f(v_j)=\sum_{i=1}^m a_{ij}w_i$

יהי $v\in V$. מטריצה מבטאת איך ההעתקה הליניארית f פועלת על איברי הבסיס והיה לנו משפט שאומר שאם יודעים איך f פועלת על איברי הבסיס אז אנחנו יודעים איך היא פועלת על כל וקטור.

פשוט נפתח את v לפי הבסיס הנתון ונשתמש בליניאריות של f:

אם $v=\sum_{j=1}^n c_jv_j$ הפיתוח של v לפי הבסיס $v_1,\dots,v_n$ אז

$$f(v)=f\left(\sum_{j=1}^n c_jv_j\right)=\sum_{j=1}^n c_jf(v_j)=$$

$$=\sum_{j=1}^n c_j\left(\sum_{i=1}^m a_{ij}w_i\right)=\sum_{j=1}^n\sum_{i=1}^m c_ja_{ij}w_i=$$

$$=\sum_{i=1}^m\sum_{j=1}^n c_ja_{ij}w_i=\sum_{i=1}^m\sum_{j=1}^n a_{ij}c_jw_i=\sum_{i=1}^m\left(\sum_{j=1}^n a_{ij}c_j\right)w_i$$

קיבלנו את $f(v)$ כצירוף ליניארי של איברי הבסיס של W.
כלומר אם $W\ni f(v)=\sum_{i=1}^m d_iw_i$ אז מיחידות הפירוק

$$d_i=\sum_{j=1}^n a_{ij}c_j \qquad 1\le i\le m$$

ומה המשמעות המעמיקה של זה? זה בעצם נותן לנו דרך לחשב פעולה של העתקה על וקטור באמצעות המטריצה שלה - זאת מכפלה של מטריצה בוקטור: (נשים לב שהוקטור הוא גם מטריצה - עם עמודה אחת!)

$$\underset{m\times n}{\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n}\\ a_{21} & a_{22} & \dots & a_{2n}\\ \vdots & & & \\ a_{m1} & a_{m2} & \dots & a_{mn}\end{pmatrix}}\underset{n\times 1}{\begin{pmatrix} c_1\\ c_2\\ \vdots\\ c_n\end{pmatrix}}=\underset{m\times 1}{\begin{pmatrix} a_{11}c_1+a_{12}c_2+\dots+a_{1n}c_n\\ a_{21}c_1+a_{22}c_2+\dots+a_{2n}c_n\\ \vdots\\ a_{m1}c_1+a_{m2}c_2+\dots+a_{mn}c_n\end{pmatrix}}$$

נסמן $C_v = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ - המקדמים בפירוק של v לפי הבסיס של V

C-בשביל column

$C_{f(v)} = \begin{pmatrix} d_1 \\ \vdots \\ d_m \end{pmatrix}$ - המקדמים בפירוק של $f(v)$ לפי הבסיס של W

<u>משפט:</u> $C_{f(v)} = A_f \cdot C_v$

כלומר בשביל להפעיל f על וקטור יש לכפול את המטריצה בווקטור המקדמים.

מערכות של משוואות לינאריות

נניח שיש לנו מע' משוואות לינאריות:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_n \end{cases}$$

זאת מע' של m משוואות לינאריות בנעלמים $x_1,\dots,x_n$ עם מקדמים $a_{ij} \in F$ ואיברים חפשיים $b_i \in F$.

לפתור מע' משוואות פירושו למצוא איברים $\alpha_1,\dots,\alpha_n$ ב-F, לרשום אותם במקום $x_1,\dots,x_n$ בהתאמה ולקבל שכל השוויונים מתקבלים.

נשאלות כל מיני שאלות: האם יש פתרון? האם הוא יחיד? ועוד...

את מע' המשוואות אפשר לרשום בצורה מטריציונית:

$$\underbrace{\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}}_{\text{מטריצת המקדמים } A} \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}}_{\text{עמודת הנעלמים } X} = \underbrace{\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}}_{\text{עמודת האיברים החפשיים } b}$$

עם הסימונים האלה נחסכה לנו הכתיבה בצורה נרחבת ואפשר לרשום $Ax=b$.

לפני שאנחנו נכנסים לנושא במלואו נדון במקרה פרטי:

<u>מקרה פרטי</u>: נניח ש- $m=n$ ונניח של- A יש מטריצה הפכית A^{-1}. אז נסתכל על $Ax=b$. נכפיל את שני האגפים משמאל במטריצה A^{-1} ונקבל

(אסוציאטיביות; תרגיל לבדוק זה)

$$x = Ix = (A^{-1}A)x = A^{-1}(Ax) = A^{-1}b$$

כלומר קיבלנו פיתרון למע' המשוואות! ולא רק שיש פתרון - הוא יחיד!

<u>מסקנה</u>: במקרה פרטי זה, הפתרון קיים והוא יחיד!

<u>הערה</u>: מובלעת פה העובדה שאם מטריצה היא לא ריבועית אז אין לה הפכית.

<u>משפט</u>: נניח שעבור מטריצה A מסדר $m\times n$ קיימת מטריצה B מסדר $n\times m$ כך ש $AB=I_m$ ו- $BA=I_n$. אז $m=n$.
(I_k - מטריצת יחידה מסדר $k\times k$)

נכניס סימונים חדשים. $M_{m,n}(F)$ קבוצת המטריצות מסדר $m\times n$ עם מקדמים בשדה F. $M_{n,1}(F)$ - קבוצת העמודות בגובה n. במקום לרשום $M_{n,1}(F)$ נרשום F^n. (לזכור שקודם F^n היה שורות של איברי F. אנחנו עושים העמסה של המונח.

$$f_A : F^n \longrightarrow F^m$$
$$\underset{(n\times 1)}{c} \longmapsto \underset{(m\times n)\cdot(n\times 1)=(m\times 1)}{Ac}$$

<u>טענה</u>: $(P_1+P_2)Q = P_1Q+P_2Q$, $P(Q_1+Q_2)=PQ_1+PQ_2$
כאשר החיבור והכפל של המטריצות מוגדר.

<u>הוכחה</u>: P_1,P_2,P מסדר $p\times q$ ו- Q_1,Q_2,Q מסדר $q\times r$.

$$[(P_1+P_2)Q]_{ij} = \sum_{k=1}^{q}[P_1+P_2]_{ik}[Q]_{kj} = \sum_{k=1}^{q}([P_1]_{ik}+[P_2]_{ik})[Q]_{kj} =$$

$$= \sum_{k=1}^{q}([P_1]_{ik}[Q]_{kj}+[P_2]_{ik}[Q]_{kj}) = \sum_{k=1}^{q}[P_1]_{ik}[Q]_{kj}+\sum_{k=1}^{q}[P_2]_{ik}[Q]_{kj} =$$

$$= [P_1Q]_{ij}+[P_2Q]_{ij} = [P_1Q+P_2Q]_{ij} \Rightarrow (P_1+P_2)Q = P_1Q+P_2Q$$

$$[P(Q_1+Q_2)]_{ij}=\sum_{k=1}^{q}[P]_{ik}[Q_1+Q_2]_{kj}=\sum_{k=1}^{q}[P]_{ik}\left([Q_1]_{kj}+[Q_2]_{kj}\right)=$$

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

$$=[PQ_1]_{ij}+[PQ_2]_{ij}=[PQ_1+PQ_2]_{ij}\Rightarrow P(Q_1+Q_2)=PQ_1+PQ_2$$

מש"ל ☺

$$f_A: F^n\to F^m,\quad c\mapsto Ac$$

כעת ע"פ חוק הפילוג f_A שומרת חבור.

אכן, ניקח $c,c'\in F^n$. אז:

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

מה עם כפל בסקלר? תרגיל:

לכל $a\in F$ לכל מטריצות P, Q ($p\times q$, $q\times r$) מתקיים

$$(aP)Q=P(aQ)=a(PQ)$$

$\Leftarrow$ f_A שומרת כפל בסקלר. $f_A(ac)=A(ac)=a(Ac)=af_A(c)$.

$\Leftarrow$ f_A העתקה לינארית.

נסתכל על הבסיסים הסטנדרטיים של F^n ו- F^m:

$e_1,\dots,e_n\in F^n$ ו- $d_1,\dots,d_m\in F^m$ (d בשביל dina)

אז ל- f_A יש מטריצה. איך נמצא אותה? (נסתכל על הבסיס)

$1\le j\le n$ $\quad f_A(e_j)=Ae_j=\sum_{i=1}^{m}a_{ij}d_i$ לכן:

$$f_A(e_1)=Ae_1=\begin{pmatrix}a_{11}&\cdots&a_{1n}\\ \vdots&&\\ a_{m1}&\cdots&a_{mn}\end{pmatrix}\begin{pmatrix}1\\0\\ \vdots\\0\end{pmatrix}=\begin{pmatrix}a_{11}\\ \vdots\\ a_{m1}\end{pmatrix}=a_{11}\begin{pmatrix}1\\0\\ \vdots\\0\end{pmatrix}+\dots+a_{m1}\begin{pmatrix}0\\ \vdots\\0\\1\end{pmatrix}$$

$$\vdots$$

$$f_A(e_n)=Ae_n=\begin{pmatrix}a_{11}&\cdots&a_{1n}\\ \vdots&&\\ a_{m1}&\cdots&a_{mn}\end{pmatrix}\begin{pmatrix}0\\ \vdots\\0\\1\end{pmatrix}=\begin{pmatrix}a_{1n}\\ \vdots\\ a_{mn}\end{pmatrix}=a_{1n}\begin{pmatrix}1\\0\\ \vdots\\0\end{pmatrix}+\dots+a_{mn}\begin{pmatrix}0\\ \vdots\\0\\1\end{pmatrix}$$

אז מה המטריצה? שמים את המקדמים בעמודות:

$$A_{f_A}=\begin{pmatrix}a_{11}&\cdots&a_{1n}\\ \vdots&&\vdots\\ a_{m1}&&a_{mn}\end{pmatrix}=A$$

אז!

<u>מסקנה:</u> $A_{f_A}=A$.

(53) 9.1.06
לינארית

מט' של משוואות לינאריות, מטריצות והעתקות לינאריות

F שדה, F^n, F^m מ"ו של עמודות באורך n, m בהתאמה.

$$\underset{m\times n}{A} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \qquad f_A : F^n \longrightarrow F^m,\quad c \longmapsto Ac$$

הוכחנו כי f_A היא העתקה לינארית. כמו כן, הוכחנו שאם ניקח את הבסיסים הסטנדרטיים ב-F^n וב-F^m אז המטריצה של ההעתקה הלינארית f_A ביחס לבסיסים אלה היא $A = A_{f_A}$.

<u>משפט</u>: נניח ש-A ו-B שתי מטריצות, A מסדר $m\times n$ ו-B מסדר $n\times m$, כך ש-$BA = I_n$ ו-$AB = I_m$, אז $m=n$.

<u>הוכחה</u>: נסתכל בהעתקות לינאריות $f_A : F^n \to F^m$ ו-$f_B : F^m \to F^n$.

(נסתכל על ההרכבה)

$$Id_{F^m} : F^m \xrightarrow{f_B} F^n \xrightarrow{f_A} F^m,\quad d \longrightarrow Bd \longrightarrow A(Bd) = (AB)d = I_m d = d$$

באותו אופן

$$Id_{F^n} : F^n \xrightarrow{f_A} F^m \xrightarrow{f_B} F^n,\quad c \longmapsto Ac \longrightarrow B(Ac) = (BA)c = I_n c = c$$

$\Leftarrow$ f_A ו-f_B הפיכות זו לזו. לכן הן חח"ע ועל ולכן הן איזומורפיזמים של מ"ו. (נאמר ש-F^m איזומורפי ל-F^n.)
הוכחנו קודם שמרחבים וקטוריים איזומורפיים יש אותו מימד.

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

מש"ל ☺

<u>מסקנה</u>: <u>רק</u> למטריצה ריבועית יכולה להיות מטריצה הפכית.

עכשיו נחזור למשוואות לינאריות.

הצגנו מע' משוואות בצורה מטריציונית.

$$Ax = b$$

מקדמים: (a_{ij}) ; נעלמים: $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$; איברים חופשיים: $\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$

במע' משוואות נתונים A ו-b ואנחנו מחפשים עמוד X רק שהשוויון יתקיים.

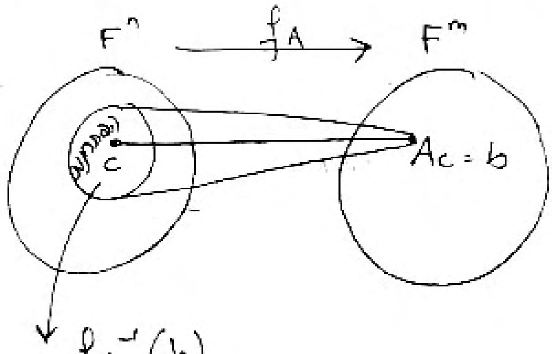
אמרנו שאם A מסדר $n\times n$ ויש לה הפכית אז

$$x = (A^{-1}A)x = A^{-1}(Ax) = A^{-1}\cdot b$$

באופן כללי אם $A_{m\times n}$, $b=\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ ו- $x=\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

נסתכל על $f_A : F^n \to F^m$, $c \mapsto Ac$

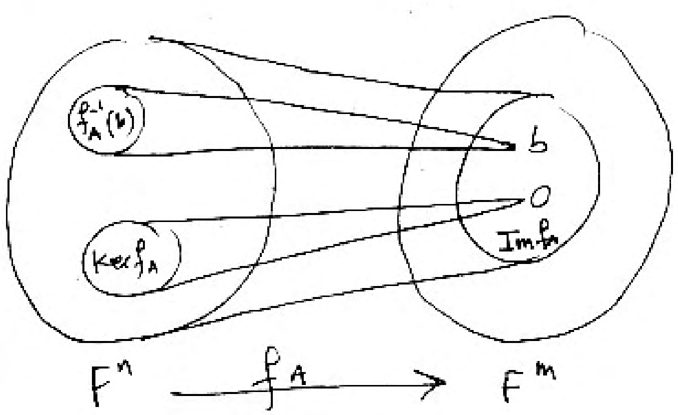
למצוא פיתרון של המע' $Ax=b$ הנ"ל זה בעצם, למצוא מקור של b תחת ההעתקה הלינארית f_A.



$f_A^{-1}(b)$ - אוסף כל המקורות של b

<u>הערה</u>: למע' $Ax=b$ יש פתרון אמ"מ $b\in Im(f_A)$ (כי אחרת הרי לא נוכל למצוא x-ים רק ש $Ax=b$)

<u>הערה</u>: למע' $Ax=b$ יש פתרון <u>יחיד</u> אמ"מ $b\in Im(f_A)$ ואם $ker(f_A)=\{0\}$ (כלומר ההעתקה חח"ע ולכן יש רק מקור אחד)



<u>משפט:</u> אם $f: V \to W$ העתקה לינארית, $c \in V$
ו- $f(c) = b \in W$ אז $f^{-1}(b) = c + \ker f$

<u>הוכחה:</u>

א) נוכיח כי $c + \ker f \subseteq f^{-1}(b)$. אכן, לכל $v \in \ker f$
$f(c+v) = f(c) + f(v) = b + 0_W = b$ ז"א $c + v \in f^{-1}(b)$

ב) נוכיח כי $f^{-1}(b) \subseteq c + \ker f$. ניקח $c' \in f^{-1}(b)$, ז"א
$f(c') = b$. $f(c-c') = f(c) - f(c') = b - b = 0_W$ ז"א $c - c' \in \ker f$
לכן $v = c' - c \in \ker f \Rightarrow c' = c + (c'-c) = c + v \in c + \ker f$
ז"א $f^{-1}(b) \subseteq c + \ker f$.

$\Rightarrow f^{-1}(b) = c + \ker f$ מש"ל ☺

<u>הגדרה:</u> $U \leq V$ תמ"ו. $v \in V \Rightarrow v + U = \{v + u : u \in U\}$
נקראת <u>ישריה</u> (יריעה + ישר) (affine subspace)
U נקרא <u>תת-מרחב המכוון</u> של הישריה $v + U$.

נשים ♡ שהישריה היא לא בהכרח תת מרחב של V.
הישריה היא תמ"ו אמ"מ $v \in U$.

<u>טענה:</u> אם $U_1, U_2 \leq V$ תמ"ו $v_1, v_2 \in V$. אם $v_1 + U_1 = v_2 + U_2$
אז $U_1 = U_2$

<u>הוכחה:</u> היות ו- $0_V \in U_1$ נקבל $v_1 = v_1 + 0_V \in v_1 + U_1 = v_2 + U_2$
ז"א קיים $u_2 \in U_2$ כך ש- $v_1 = v_2 + u_2$. ז"א $v_1 - v_2 = u_2 \in U_2$
או $v_2 - v_1 = -u_2 \in U_2$.

באותו אופן, היות ו- $0_V \in U_2$ $v_2 = v_2 + 0_V \in v_2 + U_2 = v_1 + U_2$

קיים $u_1 \in U_1$ כך ש $v_2 = v_1 + u_1$. לכן $v_2 - v_1 = u_1 \in U_1$

ו- $v_1 - v_2 = -u_1 \in U_1$. מהשוויון $v_1 + U_1 = v_2 + U_2$ נובע

$$U_1 = (-v_1) + (v_1 + U_1) = (-v_1) + (v_2 + U_2) = (v_2 - v_1) + U_2 = U_2$$

כי $v_2 - v_1 \in U_2$

מש"ל ☺

<u>הגדרה:</u> $\dim_F (v + U) = \dim_F U$

משום שהוכחנו שלכל ישריה יש תת מרחב מכוון יחיד,

זה מוגדר היטב.

<u>מסקנה:</u> אוסף של כל הפתרונות של מע' לינארית הוא ישריה.

(55) 11.1.06

לינארית

מע' של משוואות לינאריות, מטריצות והעתקות לינאריות

יש לנו מע' משוואות - m משוואות ב-n נעלמים

$$a_{11}x_1 + \dots + a_{1n}x_n = b_1$$
$$\vdots$$
$$a_{m1}x_1 + \dots + a_{mn}x_n = b_m$$

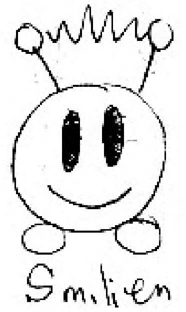
אפשר לרשום את המע' בצורה מטריציונית וזה בדיוק אותו הדבר:

$$Ax = b$$

$A = (a_{ij})$ המקדמים

$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ הנעלמים

$\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ מקדמים חופשיים



נסתכל על ההעתקה הלינארית שמוגדרת ע"י A: $f_A : F^n \to F^m$, $c \mapsto Ac$

כדי לפתור את מע' המשוואות פירושו למצוא את המקורות של b: $f_A^{-1}(b)$*. למה? מה זה מקור? מקור זה משהו שאם מפעילים עליו את ההעתקה מקבלים את b. אם $d \in F^n$ מקור של b, כלומר $d \in f_A^{-1}(b)$ אזי $f_A(d) = b$, כלומר $b = Ad$ וזה בדיוק אומר ש-d פותר את מע' המשוואות.

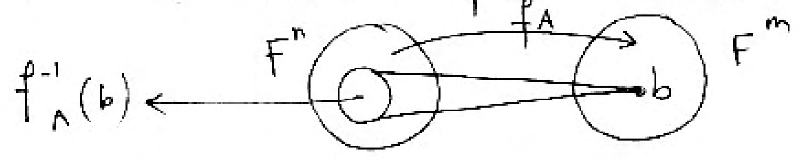
אם יש הרבה d-ים אזי יש הרבה פתרונות.

אם יש d אחד בלבד יש פתרון אחד בלבד.

אם אי אפשר למצוא d כזה אז אין למע' המשוואות פתרון.

* הערה: הסימון $f_A^{-1}(b)$ קצת מטעה. כאן לא הכוונה היא לפונקציה ההפוכה, אלא הכוונה היא לקבוצת המקורות:

$$f_A^{-1}(b) = \{c \in F^n : f_A(c) = b\}$$

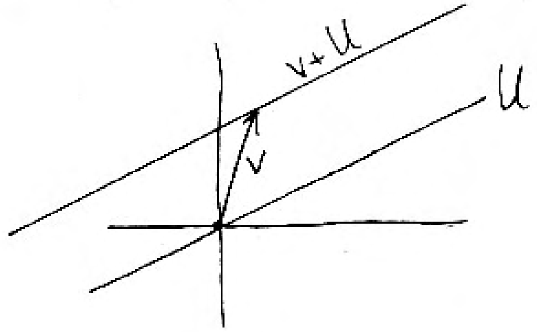


הוכחנו בשיעור הקודם טענה: $f: V \to W$ לינארית.
$w \in W$. אם קיים מקור $v \in V$ של w, כלומר $f(v) = w$
אז $f^{-1}(w) = v + \operatorname{Ker} f$
זאת טענה כללית.

במקרה שלנו אנחנו מטפלים של ההעתקה $f_A : F^n \to F^m$.
אז אם $f_A(c) = b$ אז נקבל $f_A^{-1}(b) = c + \operatorname{Ker} f_A$.
כלומר, אם אנחנו מצליחים למצוא פתרון אחד של המע',
אז אנחנו יודעים מהי קבוצת הפתרונות.
נשים לב, אם ההעתקה חח"ע, כלומר $\operatorname{Ker} f_A$ טרי' אז
למע' המשוואות יש רק פתרון אחד (אם בכלל) כי
$c + 0 = c$.

<u>הגדרה</u>: אם $U \subseteq V$ ת"מ. יהי $v \in V$ אז $v + U$ נקרא <u>ישריה</u> (זה כמו סכום של קבוצות רק שכאן אחת מהקבוצות הינו איבר אחד בלבד).

<u>דוגמה</u>: $V = \mathbb{R}^2$ וניקח $U \le V$ ת"מ שהוא איזה ישר שעובר דרך האפס. ניקח $v \in V$. ישריה כאן תהיה ישר מקביל ל-U ועובר דרך v:



<u>הגדרה</u>: $\dim_F(v + U) = \dim_F U$.

אזהרה! $v + U$ בכלל <u>לא</u> חייבת להיות תת מרחב. למשל, כמו בדוגמה למעלה.

<u>טענה:</u> $v+U$ הוא תת מרחב של V אם ורק אם $v\in U$ ואז $v+U=U$.

<u>הוכחה:</u>

(א) אם $v\notin U$ אז $0_V\notin v+U$. למה? (נניח בשלילה כי $0_V\in v+U$.
⇐ קיים $u\in U$ כך ש $0_V=v+u$ ⇐ $v=-u\in U$.
⇐ סתירה). לכן $0_V\notin v+U$, לכן... זה לא תת מרחב.

(ב) אם $v\in U$, נוכיח כי $v+U=U$. ברור שלכל $u\in U$ $v+u\in U$ כי U סגור לגבי חיבור לכן $v+U\subseteq U$. מצד שני, ניקח $u'\in U$ ונראה כי $u'\in v+U$. אכן, $u'=v+(u'-v)$ ומכיון ש $u',v\in U$ גם $u'-v\in U$. לכן $u'\in v+U$. קיבלנו ש- $U\subseteq v+U$, לכן $v+U=U$.

מש"ל ☺

משפט המימדים: אם $f:V\to W$ העתקה לינארית אז:

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

(כמובן, אם $\dim_F V<\infty$)

נעביר אגפים (כן לא תרומה גדולה) ונקבל:

$$\dim_F \mathrm{Ker} f=\dim_F V-\dim_F \mathrm{Im} f$$

ובמקרה הפרטי שאנחנו מדברים עליו כבר כל השעור

$$\dim_F \mathrm{Ker} f_A=\dim_F F^n-\dim_F \mathrm{Im} f_A=$$
$$=n-\dim_F \mathrm{Im} f_A$$

למה זה מעניין אותנו בכלל? אמרנו שאם c פתרון של מע' המשוואות אז קבוצת כל הפתרונות היא $c+\mathrm{Ker}_F f_A$ וראינו ישירות. אמרנו ש- $\dim_F(c+\mathrm{Ker}_F f_A)=\dim_F \mathrm{Ker} f_A$ לכן זה מעניין אותנו.

נכניס כמה סימונים חדשים.

נניח ש $A=(a_{ij})$. אזי

השורות של A
$$\begin{cases} A_{1*} = (a_{11}\ a_{12} \dots a_{1n}) \\ \vdots \\ A_{m*} = (a_{m1}\ a_{m2} \dots a_{mn}) \end{cases}$$

$$A_{*1} = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} \quad \dots\dots \quad A_{*n} = \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix}$$

העמודות של A

<u>משפט</u>: עבור $f_A : F^n \to F^m$, $f_A : c \mapsto Ac$

$$\mathrm{Im} f_A = Sp(a_{*1}, \dots, a_{*n}) \subseteq F^m$$

<u>הוכחה</u>: הוכחנו כבר שאם $f : V \to W$ העתקה לינארית

ו- $V = Sp(v_1, \dots, v_k)$ אז $\mathrm{Im} f = Sp(f(v_1), \dots, f(v_k))$

ניקח מתוך הוקטורים הפורשים את F^n את העמודות הסטנדרטיות.

$$f_A\begin{pmatrix}1\\0\\ \vdots\\0\end{pmatrix} = A\begin{pmatrix}1\\0\\ \vdots\\0\end{pmatrix} = \begin{pmatrix} a_{11} \dots a_{1n} \\ \vdots \\ a_{m1} \dots a_{mn}\end{pmatrix}\begin{pmatrix}1\\0\\ \vdots\\0\end{pmatrix} = \begin{pmatrix}a_{11}\\ \vdots \\ a_{m1}\end{pmatrix} = a_{*1}$$

$\vdots$

$$f_A\begin{pmatrix}0\\ \vdots\\0\\1\end{pmatrix} = A\begin{pmatrix}0\\ \vdots\\0\\1\end{pmatrix} = \begin{pmatrix} a_{11} \dots a_{1n} \\ \vdots \\ a_{m1} \dots a_{mn}\end{pmatrix}\begin{pmatrix}0\\ \vdots\\0\\1\end{pmatrix} = \begin{pmatrix}a_{1n}\\ \vdots \\ a_{mn}\end{pmatrix} = a_{*n}$$

$$\Rightarrow \mathrm{Im} f_A = Sp\left(f_A\begin{pmatrix}1\\ \vdots\\0\end{pmatrix}, \dots, f_A\begin{pmatrix}0\\ \vdots\\1\end{pmatrix}\right) = Sp(a_{*1}, \dots, a_{*n})$$

מש"ל ☺

(57)

<u>הערה:</u> $\dim_F Sp(a_{*1},\dots,a_{*n})$ הוא המספר המקסימלי של עמודות בלתי תלויות של המטריצה A.

זה טריויאלי ונובע מהגדרה של בסיס. אם מרחב וקטורי נוצר סופית אז יש תת קבוצה של הווקטורים הפורשים שהיא בסיס:

<u>משפט:</u> אם $V=Sp(v_1,\dots,v_k)$ אז $\{v_i : 1\le i\le k, v_i \notin Sp(v_1,\dots,v_{i-1})\}$ בסיס של V.

<u>הגדרה</u> דרגה של מטריצה A לפי העמודות היא
$rank_c(A) = \dim_F Sp(a_{*1},\dots,a_{*n})$ (c בשביל column)

<u>הגדרה:</u> דרגה של מטריצה A לפי השורות היא
$rank_r(A) = \dim_F Sp(a_{1*},\dots,a_{n*})$ (r בשביל row)
והינו שווה למספר המקסימלי של שורות בלתי תלויות של מטריצה A

בינתיים הוכחנו: $\dim_F Ker f_A = n - rank_c(A)$

<u>משפט</u> לכל מטריצה A $rank_c(A) = rank_r(A)$

(58) 16/01/06
לינארית

הדרגה של מטריצה

F שדה, $A\in M_{m,n}(F)$ - מטריצה מסדר $m\times n$ עם מקדמים בשדה F.

$$A=\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{m1} & \cdots & a_{mn}\end{pmatrix} = \begin{pmatrix} a_{1*} \\ \vdots \\ a_{m*}\end{pmatrix} = \begin{pmatrix} a_{*1} & \cdots & a_{*n}\end{pmatrix}$$

טבלה מלבנית — עמודה של שורות — שורה של עמודות

משפט. $\dim_F Sp(a_{1*}\dots a_{m*}) = \dim_F Sp(a_{*1},\dots,a_{*n})$

נניח ש $\underset{n\times p}{B}=(b_{ij})$. אז מוגדרת המכפלה AB

והיא מטריצה מסדר $m\times p$. מה זה AB?

$$AB=\begin{pmatrix} a_{11}b_{11}+a_{12}b_{21}+\dots+a_{1n}b_{n1} & a_{11}b_{12}+a_{12}b_{22}+\dots+a_{1n}b_{n2} & \dots & a_{11}b_{1p}+\dots+a_{1n}b_{np} \\ a_{21}b_{11}+a_{22}b_{21}+\dots+a_{2n}b_{n1} & a_{21}b_{12}+a_{22}b_{22}+\dots+a_{2n}b_{n2} & \dots & a_{21}b_{1p}+\dots+a_{2n}b_{np} \\ \vdots & & & \\ a_{m1}b_{11}+a_{m2}b_{21}+\dots+a_{mn}b_{n1} & a_{m1}b_{12}+a_{m2}b_{22}+\dots+a_{mn}b_{n2} & \dots & a_{m1}b_{1p}+\dots+a_{mn}b_{np}\end{pmatrix} =$$

$$=\begin{pmatrix} a_{11}b_{1*}+a_{12}b_{2*}+\dots+a_{1n}b_{n*} \\ a_{21}b_{1*}+a_{22}b_{2*}+\dots+a_{2n}b_{n*} \\ \vdots \\ a_{m1}b_{1*}+a_{m2}b_{2*}+\dots+a_{mn}b_{n*}\end{pmatrix} \qquad B=\begin{pmatrix} b_{11} & \dots & b_{1p} \\ b_{21} & \dots & b_{2p} \\ b_{n1} & \dots & b_{np}\end{pmatrix}$$

AB - שורותיה הן צירופים לינאריים של שורות מטריצה B עם מקדמים ממטריצה A.

באותו אופן אפשר גם לרשום:

$$(**)\quad AB = \left(b_{11}a_{*1} + b_{21}a_{*2} + \dots + b_{n1}a_{*n} \ \dots \ b_{1p}a_{*1} + b_{2p}a_{*2} + \dots + b_{np}a_{*n}\right)$$

כלומר AB עמודותיה הן צירופים לינאריים של עמודות מטריצה A כאשר בתור מקדמים משמשים איברי מטריצה B.

נסמן $AB = C = \begin{pmatrix} c_{11} & \dots & c_{1p} \\ \vdots & & \\ c_{m1} & \dots & c_{mp} \end{pmatrix}$

$$\Rightarrow Sp(c_{*1}, \dots, c_{*p}) \subseteq Sp(a_{*1}, \dots, a_{*n})$$

$$Sp(c_{1*}, \dots, c_{m*}) \subseteq Sp(b_{1*}, \dots, b_{n*})$$

$$Sp\{v_1, \dots, v_m\} = \{a_1v_1 + \dots + a_mv_m \mid a_i \in F\}$$

$v_1, \dots, v_m \in V \Rightarrow Sp(v_1 \dots v_m) \subseteq V$ ת"מ של V

אם $w_1 \dots w_k \in Sp(v_1 \dots v_m)$ אז $Sp(w_1 \dots w_k) \subseteq Sp(v_1 \dots v_m)$

ניקח מטריצה C מסדר $n \times p$ צ"ל:

$$\dim_F Sp(c_{1*}, \dots, c_{m*}) = \dim_F Sp(c_{*1}, \dots, c_{*p})$$

נניח ש $n = \dim_F Sp(c_{1*}, \dots, c_{m*})$. נרצה לבנות פירוק של C למכפלה $C = AB$ כאשר A מסדר $m \times n$ ו- B מסדר $n \times p$.

ל- $Sp(c_{1*} \dots c_{m*})$ יש בסיס שיש בו n וקטורים, כלומר n שורות באורך p. נסמן:

$$(b_{11}\ b_{12} \ \dots \ b_{1p}) = b_{1*}$$

$$(b_{21}\ b_{22} \ \dots \ b_{2p}) = b_{2*}$$

$$\vdots$$

$$(b_{n1}\ b_{n2} \ \dots \ b_{np}) = b_{n*}$$

נגדיר $\underset{n \times p}{B} = (b_{ij})$

(59)

בגלל שזה בסיס $Sp(C_{1*},\dots,C_{m*}) = Sp(b_{1*},\dots,b_{n*})$

כמו כן

קיימים a_{ij}:

$C_{1*} = a_{11}b_{1*} + \dots + a_{1n}b_{n*}$

$\vdots$

$C_{m*} = a_{m1}b_{1*} + \dots + a_{mn}b_{n*}$

נגדיר $\underset{m\times n}{A} = (a_{ij})$

הצלחנו לפרק את C כפי שרצינו $C = AB$.

ועכשיו לפי מה שעשינו קודם

$Sp(C_{*1},\dots,C_{*p}) \subseteq Sp(a_{*1},\dots,a_{*n})$

~~[crossed out]~~

לכן

$rank_c C = \dim_F Sp(C_{*1},\dots,C_{*p}) \le \dim_F Sp(a_{*1},\dots,a_{*n}) \le n = rank_r C$

כלומר $rank_c C \le rank_r C$

בדיוק באותו אופן (רק הפוך) אפשר להראות ש

$rank_r C \le rank_c C$

$\Rightarrow rank_r C = rank_c C$

נעשה את זה: נסמן $n = \dim_F Sp(C_{*1},\dots,C_{*p})$ (לא לבלבל אותו עם ה-n כמו קודם)

נסמן את הבסיס של $Sp(C_{*1},\dots,C_{*p})$ באופן הבא:

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix} \dots \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix}$$

$$a_{*1} \quad a_{*2} \quad\quad a_{*n}$$

נגדיר A מסדר $m\times n$ כך: $A = (a_{ij})$

נבטא את $C_{*1},\dots,C_{*p}$ ע"י הבסיס $a_{*1},\dots,a_{*n}$

$C_{*1} = b_{11}a_{*1} + \dots + b_{n1}a_{*n}$

$\vdots$

$C_{*p} = b_{1p}a_{*1} + \dots + b_{np}a_{*n}$

וקיבלנו $C = AB$ כאשר $B = (b_{ij})$

$AB = (**) = (C_{*1} \dots C_{*p})$

$$\Leftarrow \quad Sp(c_{1*},\dots,c_{m*}) \subseteq Sp(b_{1*},\dots,b_{n*})$$

$$\Rightarrow \dim_F Sp(c_{1*}\dots c_{m*}) \le \dim_F Sp(b_{1*},\dots,b_{n*}) \le n$$

$$\Rightarrow \operatorname{rank}_r C \le \operatorname{rank}_r C$$

ולכן הוכחנו $\operatorname{rank}_r C = \operatorname{rank}_c C$

[illegible] (☺)

<u>הערה</u> $\operatorname{rank} C = \operatorname{rank}_c C = \operatorname{rank}_r C$

(60) 18.1.06
לינאריות

מערכות של משוואות לינאריות

F שדה, A מטריצה מסדר $m\times n$. $b\in F^m$ עמודה של איברים
תפשים $x=\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}$ עמודה של נעלמים. $f_A: F^n \to F^m$, $c \mapsto Ac$
מע' המשוואות היא $Ax=b$. אוסף כל הפתרונות
של המשוואה $Ax=b$ זהה לאוסף של כל המקורות של b
ביחס ל-f_A, כ"א $f_A^{-1}(b)$ (ראינו לא הכוונה היא
להעתקה הפכית, שהרי f_A לא מהכרח חח"ע, אלא
למקור של b) ראינו שאם $f_A(c)=b$, כלומר c
מקור של b, אזי אוסף כל הפתרונות הוא $f_A^{-1}(b)=c+\ker f_A$
כלומר יריעת הפתרונות של המערכת. הגדרנו ש-
$\dim_F f_A^{-1}(b)=\dim_F \ker f_A$ (מימד של יריעה הוא מימד
המרחב המכוון). לפי משפט המימדים

$$\dim_F f_A^{-1}(b)=\dim_F \ker f_A=\dim_F F^n-\dim_F \operatorname{Im} f_A=$$
$$=n-\dim_F Sp(a_{*1},\dots,a_{*n})=$$
$$=n-\operatorname{rank}_c A=n-\operatorname{rank}_r A$$

$$\dim_F f_A^{-1}(b)=n-\operatorname{rank} A$$

<u>משפט</u> (סיכום של מה שעשינו)
אם למע' משוואות יש פתרון אזי מימד יריעת הפתרונות
שווה למספר הנעלמים פחות הדרגה של מטריצת המקדמים.

אם $b\in \operatorname{Im} f_A$ למע' יש פתרון.
אם $b\notin \operatorname{Im} f_A$ למע' אין פתרון } ראה הגדרה של $\operatorname{Im} f_A$.

אמרנו ש $\operatorname{Im} f_A=Sp(a_{*1},\dots,a_{*n})$
כלומר אם $b\in Sp(a_{*1},\dots,a_{*n})$ יש פתרון
אם $b\notin Sp(a_{*1},\dots,a_{*n})$ אין פתרון.

את התנאי הזה אפשר לנסח גם כך:

אם $Sp(a_{*1},\dots,a_{*n},b)=Sp(a_{*1},\dots,a_{*n})$ יש פתרון

אם $Sp(a_{*1},\dots,a_{*n},b)\neq Sp(a_{*1},\dots,a_{*n})$ אין פתרון

נגדיר מטריצת מקדמים המורחבת:

$$\underset{m\times(n+1)}{A^*}=(a_{*1},\dots,a_{*n},b)=(A\ b)$$

זאת לא חיבור אלא שרשור.

אז אם $\text{rank}A^*=\text{rank}A$ יש פתרון

אם $\text{rank}A^*\neq\text{rank}A$ אין פתרון.

<u>משפט</u>: למע"ל $Ax=b$ יש פתרון אמ"מ $\text{rank}A^*=\text{rank}A$.

כל זה טוב ויפה, <u>אבל</u> איך בכל הרוחות פותרים מערכת משוואות???

חילוץ המשתנים של גאוס ☺

<u>הגדרה</u>: שתי מע"ל של משוואות $Ax=b$ ו- $A'x=b'$ נקראות <u>שקולות</u> כאשר יש להן בדיוק אותם הפתרונות.

<u>משפט</u>: נניח ש- B,C מטריצות הפיכות מסדר $m\times m$, כלומר $B=C^{-1}$ ו- $C=B^{-1}$. אז המערכת $Ax=b$ שקולה למע"ל $(CA)x=Cb$.

<u>הערה</u>: הדרישה ש- C תהיה הפיכה היא חשובה. אחרת יכולנו לקחת $C=\tilde{0}$ (מטריצת האפס) ואז כמובן המשפט לא נכון. למשל $2x=4$ ויהי l:

$$2lx=4l$$

אם $l\neq0$ קיבלנו אותם הפתרונות, <u>אבל</u> אם $l=0$ כל סקלר הוא פתרון והמע' לא שקולה!

הוכחה: אם $Ac=b$ אז $(CA)c=C(Ac)=Cb$
ז"א אם $c=\begin{pmatrix}c_1\\ \vdots\\ c_m\end{pmatrix}$ פתרון של $Ax=b$ הוא גם פתרון של $(CA)x=Cb$.

להפך, נניח ש $(CA)c=Cb$. נכפול את שני האגפים ב- B ונקבל

$$Ac=I_m(Ac)=(I_mA)c=((BC)A)c=(B(CA))c=$$
$$=B((CA)c)=B(Cb)=(BC)b=I_mb=b$$

ז"א אם c פתרון של $(CA)x=Cb$ אז הוא גם פתרון של $Ax=b$ מש"ל ☺

המוטיבציה היא אישהו להפוך את $Ax=b$ למע' משוואות שהרבה יותר קל לפתור אותה.

<u>הגדרה:</u>

(א) נסמן $D_i(a)=\begin{pmatrix}1 & & & \\ & \ddots & & \\ & & a & \\ & & & \ddots \\ & & & & 1\end{pmatrix}$ (שורה i), $a\in F$ — diagonal

(ב) עבור $i\neq j$ נסמן $E_{ij}(a)=\begin{pmatrix}1 & & & \\ & \ddots & a & \\ & & \ddots & \\ & & & 1\end{pmatrix}$ (a בשורה i, עמודה j) — elementary

(ג) עבור $i\neq j$ נסמן $P_{ij}=\begin{pmatrix}1 & & & & \\ & 0 & & 1 & \\ & & 1 & & \\ & 1 & & 0 & \\ & & & & 1\end{pmatrix}$ (שורות i, j) — permutation
(במטריצת היחידה הוחלפו שורות i ו- j)

<u>טענה 1:</u> $D_i(a)A=\begin{pmatrix}a_{1*}\\ \vdots\\ a\cdot a_{i*}\\ \vdots\\ a_{m*}\end{pmatrix}$

<u>טענה 2:</u> $E_{ij}(a)A=\begin{pmatrix}a_{1*}\\ \vdots\\ a_{i-1*}\\ a_{i*}+a\,a_{j*}\\ \vdots\\ a_{j*}\\ \vdots\\ a_{m*}\end{pmatrix}$

<u>טענה 3:</u> $P_{ij}A=\begin{pmatrix}a_{1*}\\ \vdots\\ a_{j*}\\ a_{i*}\\ \vdots\\ a_{m*}\end{pmatrix}$ (a_{j*} ← שורה i, a_{i*} ← שורה j)

(ההוכחות טריוויאליות, פשוט עושים את החישוב ורואים שזה נכון)

אנחנו היינו מעוניינים במטריצות הפיכות.

טענה: (א) אם $a \neq 0_F$ אז $D_i(a)^{-1} = D_i(a^{-1})$.

(ב) $E_{ij}(a)^{-1} = E_{ij}(-a) \quad i \neq j$

(ג) $P_{ij}^{-1} = P_{ij} \quad i \neq j$

הוכחה: טריוויאלי - זה נובע מהטענות הקודמות.

$$D_i(a)\,D_i(a^{-1}) = D_i(1) = I$$

$$E_{ij}(a)\,E_{ij}(-a) = E_{ij}(0) = I$$

$$P_{ij}P_{ij} = I$$

דוגמה

$$\begin{pmatrix} 1 & 5 & 3 & 2 & 2 \\ 2 & 6 & 4 & 3 & 3 \\ -1 & 2 & 7 & 1 & 1 \end{pmatrix} \xrightarrow[E_{21}(-2)]{} \begin{pmatrix} 1 & 5 & 3 & 2 & 2 \\ 0 & -4 & -2 & -1 & -1 \\ -1 & 2 & 7 & 1 & 1 \end{pmatrix} \xrightarrow[E_{31}(1)]{} \begin{pmatrix} 1 & 5 & 3 & 2 & 2 \\ 0 & -4 & -2 & -1 & -1 \\ 0 & 7 & 10 & 3 & 3 \end{pmatrix}$$

$E_{21}(-2)$: $L_1 \to L_1$, $L_2 \to L_2 - 2L_1$, $L_3 \to L_3$

$E_{31}(1)$: $L_1 \to L_1$, $L_2 \to L_2$, $L_3 \to L_3 + L_1$

$$\xrightarrow[D_2(-\frac{1}{4})]{} \begin{pmatrix} 1 & 5 & 3 & 2 & 2 \\ 0 & 1 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ 0 & 7 & 10 & 3 & 3 \end{pmatrix} \xrightarrow[E_{32}(-7)]{} \begin{pmatrix} 1 & 5 & 3 & 2 & 2 \\ 0 & 1 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ 0 & 0 & 6\frac{1}{2} & 1\frac{1}{4} & 1\frac{1}{4} \end{pmatrix}$$

$D_2(-\frac{1}{4})$: $L_1 \to L_1$, $L_2 \to -\frac{1}{4}L_2$, $L_3 \to L_3$

$E_{32}(-7)$: $L_1 \to L_1$, $L_2 \to L_2$, $L_3 \to L_3 - 7L_2$

$$\xrightarrow[E_{12}(5)]{} \begin{pmatrix} 1 & 0 & \frac{1}{2} & \frac{3}{4} & \frac{3}{4} \\ 0 & 1 & \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ 0 & 0 & 6\frac{1}{2} & 1\frac{1}{4} & 1\frac{1}{4} \end{pmatrix}$$

$E_{12}(5)$: $L_1 \to L_3 - 5L_2$, $L_2 \to L_2$, $L_3 \to L_3$

23.1.06
Algebra linear

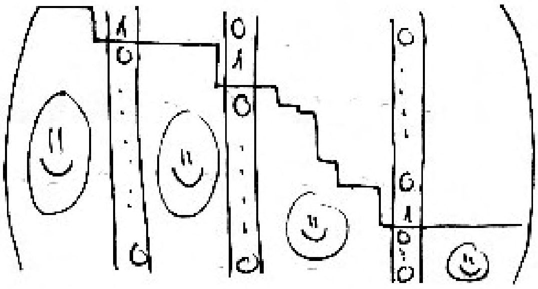
חילוץ המשתנים של גאוס

הגדרה: מטריצה D מסדר $m \times n$ נקראת **מדורגת** כאשר צורתה כפי שנסביר:

(1) יש בה עמודות סטנדרטיות לפי הסדר שלהן

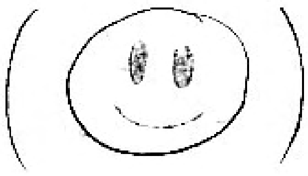
(2) ניתן להעביר קו המדרגות כאשר כל עמודה סטנדרטית קובעת מדרגה.

(3) מתחת לקו המדרגות יש רק אפסים.

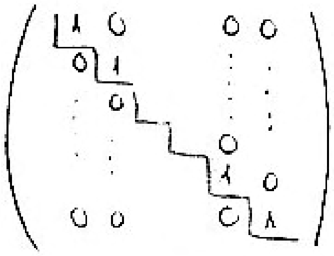


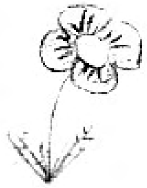
לא כל העמודות הסטנדרטיות חייבות להופיע אבל אם העמודה ה-i-ית מופיעה אז כל מה שלפניה צריך להופיע.

דוגמה למטריצה שאין בה עמודות סטנדרטיות:



דוגמה למטריצה מדורגת: מטריצת היחידה





ראינו כל העמודות הן סטנדרטיות. הנה עוד דוגמה:

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

לא נחשבות

משפט: לכל מטריצה $A_{m\times n}$ קיימת מטריצה הפיכה $B_{m\times m}$
כך ש BA היא מדורגת

הוכחה: באינדוקציה על m:

$m=1$ אז A הוא שורה $A=(a_{11}\, a_{12} \dots a_{1n})$. אם A היא
כולה אפסים אז היא כולה מדורגת וניקח $B=(1)$ ואז
$BA=(0 \dots 0)$. אם לא, יש ב-A איברים
שאינם 0_F. נניח ש j_1 הוא האינדקס הקטן ביותר כך
ש $a_{1j_1} \neq 0_F$. ניקח $B=(a_{1j_1}^{-1})$. אז
$BA=(0 \dots 0 | 1 | * \dots *)$ מדורגת.

נניח ש- $m>1$ ונניח שהטענה נכונה עבור $m-1$
אם $A=0$ אז היא כבר מדורגת. ניקח $B=I$
ואז $A=BA=0$ מדורגת.
נניח שיש ב-A איברים שונים מ- 0_F. ניקח j_1
האינדקס הקטן ביותר כך שקיים $a_{ij_1} \neq 0_F$.

$$\left(0 \;\middle|\; \overset{j_1}{a_{ij_1}} \;\middle|\; * \right)$$

אם $i=1$, הרי טוב. ואם לא, נכפיל משמאל במטריצה
P_{1i} (מהשיעור הקודם). כפל זה מחליף את השורות
1 ו- i ואז במטריצה $P_{1i}A$ איבר זה ששונה מאפס הוא
בשורה הראשונה

$$\left(0 \;\middle|\; \begin{matrix} \neq 0 \\ \vdots \end{matrix} \;\middle|\; \right) \quad \text{טור } j_1$$

בשלב הבא נכפיל ב- $D_1(a_{ij_1}^{-1}) = \begin{pmatrix} a_{ij_1}^{-1} & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix}$

ואז נקבל

$$D_1(a_{ij_1}^{-1}) P_{1i} A = \left(0 \;\middle|\; \begin{matrix} 1 \\ c_2 \\ \vdots \\ c_m \end{matrix} \;\middle|\; * \right)$$

נסתכל במטריצה $E_{m1}(-c_m)\dots E_{21}(-c_1)D_1(a_{ij_1}^{-1})P_{1i}A$

כפל ב- $E_{21}(-c_2)$ כופל שורה ראשונה ב- c_2 -

ומוסיף לשורה השנייה.

$$\Rightarrow E_{m1}(-c_m)\dots E_{21}(-c_2)D_1(a_{ij_1}^{-1})P_{1i}A =$$

$$= \left(0 \;\middle|\; \begin{matrix}1\\0\\ \vdots\\0\end{matrix} \;\middle|\; * \right)$$

במטריצה זו j_1 היא העמודה הסטנדרטית הראשונה.

נסתכל במטריצה A_1 מסדר $(m-1)\times(n-j_1)$

$$A' = \left(0 \;\middle|\; \begin{matrix}1\\ \\ \\ \end{matrix} \;\middle|\; \begin{matrix}* & \dots & * \\ & \boxed{A_1} & \end{matrix} \right)$$

לפי הנחת האינדוקציה קיימת מטריצה B_1 הפיכה מסדר $(m-1)\times(m-1)$ כך ש- B_1A_1 היא מדורגת.

נגדיר $C_1 = B_1^{-1}$.

$$\underset{m\times m}{B_1'} = \begin{pmatrix} 1 & 0 \dots 0 \\ 0 & \\ \vdots & \boxed{B_1} \\ 0 & \end{pmatrix}$$

אז $B_1'^{-1} = \begin{pmatrix} 1 & 0 \dots 0 \\ 0 & \\ \vdots & \boxed{C_1} \\ 0 & \end{pmatrix}$ (תרגיל)

נסתכל ב-

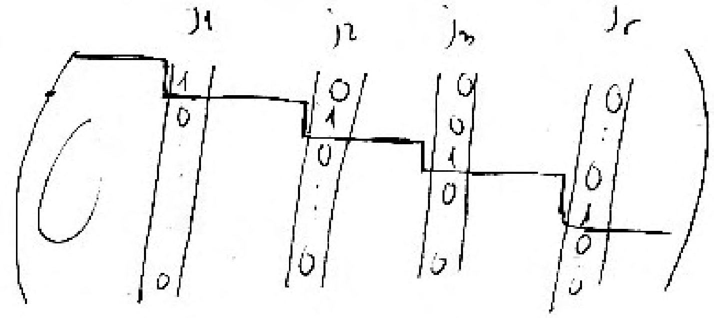
$$B_1'A' = \left(0 \;\middle|\; \begin{matrix}1\\0\\ \vdots\\0\end{matrix} \;\middle|\; \begin{matrix} * \; h_2 \; \dots \; h_3 \; h_r \; * \\ \boxed{0 \; \begin{matrix}1\\0\\ \vdots\\0\end{matrix} \; 0 \; \begin{matrix}0\\1\\ \vdots\\0\end{matrix} \dots 0 \; \begin{matrix}0\\ \vdots\\1\\0\end{matrix} \; 0} \end{matrix} \right)$$

מדורגת

אבל עכשיו צריך לאפס את האיברים בשורה הראשונה של העמודות הסטנדרטיות.

אז נסתכל על

$$E_{1r}(-h_r)\cdots E_{12}(-h_2)B_1' A' =$$

$=$ 

קיבלנו ש-

$$E_{1r}(-h_r)\cdots E_{12}(-h_2)B_1' E_{m1}(-c_m)\cdots E_{21}(-c_2)D_1(a_{1j_1}^{-1})P_{1i}A$$

היא מטריצה מדורגת

כעת כל המטריצות לפני A במכפלה הן הפיכות

לכן המכפלה היא הפיכה.

באופן כללי: $(B_k\cdots B_1)^{-1}=B_1^{-1}\cdots B_k^{-1}$

מש"ל ☺

בשביל מה כל זה? אנחנו מדברים על מע' משוואות.

הייתה לנו מע' משוואות $Ax=b$.

אם נכפול אותה ב-B הפיכה נקבל מע' משוואות

שקולה $(BA)x=Bb$.

נסתכל על $A^*=(A|b)$ מטריצת המקדמים המורחבת.

בעזרת התהליך שמצאנו ניתן להפוך אותה למדורגת

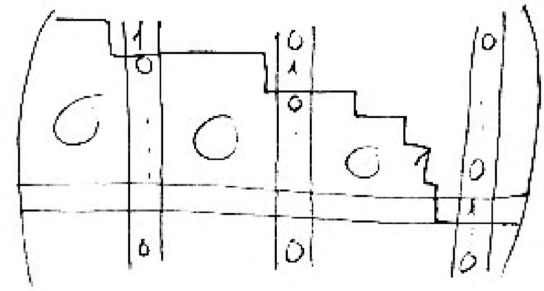
ע"י B^*: B^*A^*. כעת נבין מה קורה למע' המשוואות.

במטריצה המדורגת B^*A^*, האם העמודה האחרונה

היא סטנדרטית?

אם כן, אז אין למע' אף פתרון.

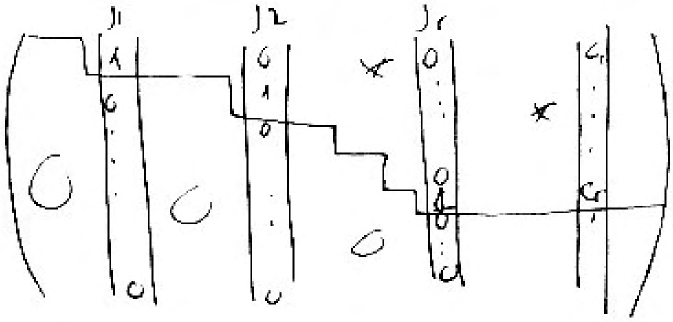
למה?



למשוואה $0x_1 + 0\cdot x_2 + \ldots + 0\cdot x_n = 1$ אין פתרונות

וממילא אין פתרונות של המערכת.

אם העמודה האחרונה איננה בכלל העמודות הנ"ל, יש פתרונות.



אז המע' משוואות היא כזאת

$$x_{j_1} + (\qquad) = c_1$$
$$x_{j_2} + (\qquad) = c_2$$
$$\vdots$$
$$x_{j_r} + (\qquad) = c_r$$

והמשתנים שנמצאים בתוך הסוגריים שונים מ- $x_{j_1}, \ldots, x_{j_r}$

ולהם אפשר לתת ערכים שרירותיים.

(65) 25.1.06

[redacted]

אתר ובו סיכומים באינפי ובלינארית - www.cs.huji.ac.il/~shuaavi

(הם מקוצרים, אז מהבחינה הזאת הם צדיקים של שלי)

* * *

מע' של משוואות ליניאריות ומטריצות מדורגות

יש לנו מע' משוואות $A_{m\times n}x = b_{m\times 1}$

$A^*_{m\times(n+1)} = (A,b)$ מטריצת המקדמים המורחבת.

בשיעור הקודם הוכחנו שקיימת B^* מסדר $m\times m$ הפיכה

רק ש B^*A^* היא מטריצה מדורגת.

באינדוקציה אפשר להראות שיש דרך בסה"כ לכל היותר $m(m+1)$

פעולות כדי לבצע את הדירוג.

$$D = [(E_{1r}(-h_r)\dots E_{13}(-h_3)E_{12}(-h_2))B_1(E_{m1}(-c_m)\dots E_{21}(-c_2)D_1(a)P_{1i})]A$$

$r-1$ פעולות, אבל $r\le m$; $m+1$ פעולות

המטריצה שמשמשת לדירוג לפי הנחת האינדוקציה וזה לכל היותר $m(m-1)$ פעולות

סה"כ $m-1 + m+1 + (m-1)m = m^2+m = m(m+1)$

<u>משפט</u>: לכל מטריצה A מסדר $m\times n$ קיימת מטריצה B הפיכה מסדר $m\times m$ רק ש $D=BA$ היא מטריצה מדורגת. יתר על כן, ניתן להציג את B כמכפלה של לא יותר מ- $m(m+1)$ גורמים, של אחד מהם מצורה P_{ij}, $D_i(a)$ $a\neq 0$, $E_{ij}(c)$ $i\neq j$

נשים לב שאם $A^*=(A;b)$ אז $B^*A^* = (B^*A; B^*b)$

כלומר B^*A^* היא מטריצת המקדמים המורחבת

של מע' המשוואות $B^*Ax = B^*b$. הוכחנו שאם כופלים

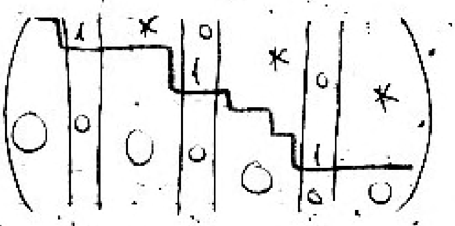
מע' משוואות משמאל במטריצה הפיכה, מקבלים מע' משוואות

שקולה. כלומר $B^*Ax=B^*b$ שקולה ל- $Ax=b$.

למה זה טוב? יותר קל לפתור מע' משוואות שמוצגת בצורה מדורגת...

מסקנה: כל מע' משוואות לינאריות שקולה למע' שמטריצת המקדמים המורחבת שלה היא מטריצה מדורגת.
וראינו גם דרך מעשית איך להגיע למע' מדורגת רצות
וראינו שזה נעשה בסיבוכיות $O(n^2)$ [רק שיש לזכור שפעולות השורה הן $O(n)$ ולכן סה"כ $O(n^3)$]

איך נדע אם יש למע' משוואות פתרון?



האם $\boxed{j_r = n+1}$? אז נקבל שאחת המשוואות (המשוואה האחרונה) היא
$$0x_1+\dots+0x_n=1$$
אז אין פתרונות!

אם $\boxed{j_r < n+1}$ נוכל לתאר את הפתרונות, והתיאור הזה ממילא מראה שיש פתרונות.
אנו מחלקים את המשתנים $x_1,\dots,x_n$ לשתי קבוצות:

I. $\{x_{j_1}, x_{j_2},\dots,x_{j_r}\}$

II. כל השאר $= \{x_1,\dots,x_n\}\setminus\{x_{j_1},\dots,x_{j_r}\}$

כל נעלם מקבוצה I מופיע במע' המשוואות פעם אחת בלבד.

$$x_{j_1} + (\text{משתנים מ-II}) = c_1 \Rightarrow x_{j_1} = c_1 - (\quad)$$
$$x_{j_2} + (\text{משתנים מ-II}) = c_2 \qquad x_{j_2} = c_2 - (\quad)$$
$$\vdots$$
$$x_{j_r} + (\text{משתנים מ-II}) = c_r \qquad x_{j_r} = c_r - (\quad)$$

(אחרי הטור האחרון)

לנעלמים מהקבוצה II ניתן לתת ערכים שרירותיים ואז הנעלמים מ-I נקבעים באופן חד ערכי.

ניתן להתייחס לנעלמים מקבוצה II כפרמטרים חופשיים
וערך הנעלמים מקבוצה I נקבע באופן חד-ערכי
כאשר נתונים הערכים של הנעלמים מקבוצה II,
כלומר של הפרמטרים החופשיים.

אם F שדה סופי ובו p^k איברים, כאשר p ראשוני
כמובן, אז יש $(p^k)^{n-r}$ אפשרויות לנתינת ערכים
לפרמטרים החופשיים. כלומר יש $(p^k)^{n-r}$ פתרונות.

<u>דוגמה</u>

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 0 & 4 & 5 & 8 \\ 0 & 0 & 0 & 0 & 1 & 6 & 7 & 9 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad I = \{x_2, x_5\}$$

$j_1 = 2 \quad j_2 = 5 \qquad II = \{x_1, x_3, x_4, x_6, x_7\}$

$n = 7$

$$x_2 + (2x_3 + 3x_4 + 4x_6 + 5x_7) = 8$$
$$x_5 + (6x_6 + 7x_7) = 9$$

$$\Longrightarrow \quad x_2 = 8 - (2x_3 + 3x_4 + 4x_6 + 5x_7)$$
$$x_5 = 9 - (6x_6 + 7x_7)$$

ניתן ערכים שרירותיים ל- II:

$x_1 = a_1 \quad x_3 = a_3 \quad x_4 = a_4 \quad x_6 = a_6 \quad x_7 = a_7$

אז וקטור הפתרונות הוא

$$= \begin{pmatrix} a_1 \\ 8 - (2a_3 + 3a_4 + 4a_6 + 5a_7) \\ a_3 \\ a_4 \\ 9 - (6a_6 + 7a_7) \\ a_6 \\ a_7 \end{pmatrix}$$

אפשר לרשום גם רק:

$$\begin{pmatrix}0\\8\\0\\0\\9\\0\\0\end{pmatrix} + a_1\begin{pmatrix}1\\0\\0\\0\\0\\0\\0\end{pmatrix} + a_3\begin{pmatrix}0\\-2\\1\\0\\0\\0\\0\end{pmatrix} + a_4\begin{pmatrix}0\\-3\\0\\1\\0\\0\\0\end{pmatrix} + a_6\begin{pmatrix}0\\-4\\0\\0\\-6\\0\\1\end{pmatrix} + a_7\begin{pmatrix}0\\-5\\0\\0\\-7\\0\\1\end{pmatrix}$$

או

$$\begin{pmatrix}0\\8\\0\\0\\9\\0\\0\end{pmatrix} + Sp\left(\begin{pmatrix}1\\0\\0\\0\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\-2\\1\\0\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\-3\\0\\1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\-4\\0\\0\\-6\\0\\1\end{pmatrix}, \begin{pmatrix}0\\-5\\0\\0\\-7\\0\\1\end{pmatrix}\right)$$

וכן יריעה שהמימד שלה הוא: $n-r=5$

(67) 301.06
סמינרים

עוד משפט אחד קטן

הוכחנו שלכל מטריצה A מסדר $m\times n$ אפשר למצוא מטריצה B ריבועית הפיכה מסדר $m\times m$ כך ש $D=BA$ היא מטריצה מדורגת.

<u>משפט</u>: אם $D_1=B_1A$, $D_2=B_2A$ כאשר B_1,B_2 הפיכות ו- D_1, D_2 מדורגות אז $D_1=D_2$.

בטרם ניגש להוכחה, (חזרה) ונושא.

V מ"ו מעל F. $v_1,\dots,v_n\in V$ $Sp(v_1\dots v_n)=U\subseteq V$ ת"מ.

$\dim_F U=r$. הוכחנו שניתן למצוא בסיס של U שהוא תת קבוצה של $\{v_1\dots v_n\}$, באופן מסוים (ניקח

$$\{v_j : 1\le j\le n \quad v_j\notin Sp(v_1\dots v_{j-1})\}$$

נקבל בסיס $v_{j_1},\dots,v_{j_r}$ של $Sp(v_1\dots v_n)=U$

כאשר $1\le j_1<j_2<\dots<j_r\le n$.

1) אם $j_1>1$ אז $v_1=0_V,\dots,v_{j_1-1}=0_V$

2) אם $j_2>j_1+1$ אז: $v_{j_1+1}=a_{1j_1+1}v_{j_1},\dots,v_{j_2-1}=a_{1j_2-1}v_{j_1}$

3) אם $j_3>j_2+1$ אז: באותו אופן

$$v_{j_2+1}=a_{1j_2+1}v_{j_1}+a_{2j_2+1}v_{j_2},\dots,v_{j_3-1}=a_{1j_3-1}v_{j_1}+a_{2j_3-1}v_{j_2}$$

⋮

r) אם $j_r>j_{r-1}+1$ אז:

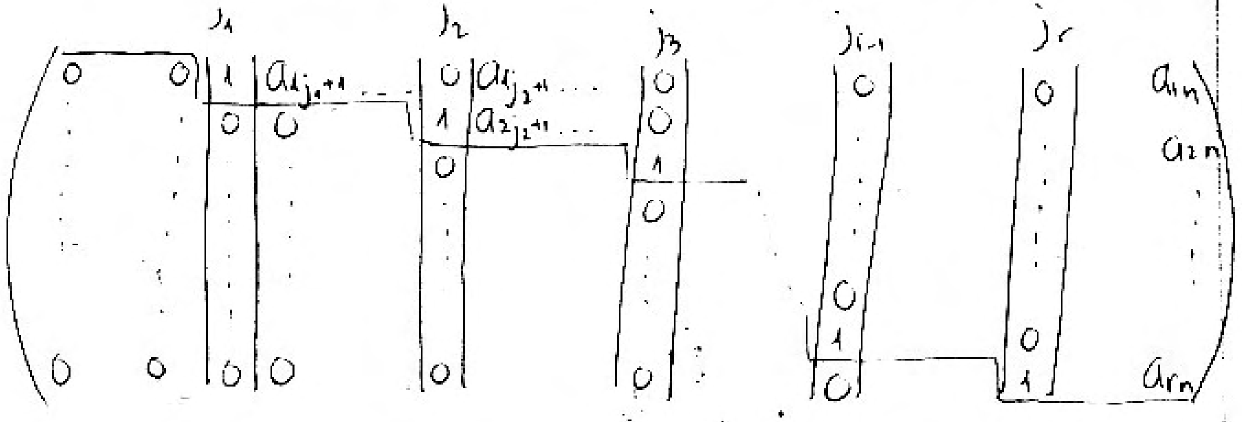
$$v_{j_{r-1}+1}=a_{1j_{r-1}+1}v_{j_1}+\dots+a_{r-1,j_{r-1}+1}v_{j_{r-1}},\dots,v_{j_r-1}=a_{1j_r-1}v_{j_1}+\dots+a_{r-1,j_r-1}v_{j_{r-1}}$$

r+1) אם $j_r<n$ אז:

$$v_{j_r+1}=a_{1j_r+1}v_{j_1}+\dots+a_{rj_r+1}v_{j_r},\dots,v_n=a_{1n}v_{j_1}+\dots+a_{rn}v_{j_r}$$

$v_{j_1},\dots,v_{j_r}$ בסיס של U.

נשווה את המקדמים במטריצה $r\times n$



קנונית = מטריצה מדורגת רק שקו המדרגות מגיע עד הרצפה

תזכורת למשפט:

נסמן ב את העמודות של A

$a_{*1},\dots,a_{*n}\in F^m$

וקטורים בגובה m

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

$$U := Sp(a_{*1},\dots,a_{*n})$$

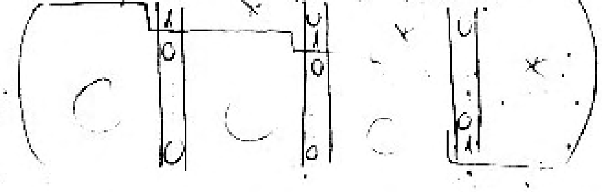
$$\dim_F U = \operatorname{rank} A =: r$$

נסמן ב $\{a_{*j}: 1\le j\le n,\ a_{*j}\notin Sp(a_{*1},\dots,a_{*j-1})\}$

קיבלנו בסיס $a_{*j_1},\dots,a_{*j_r}$ של U

נציג את כל a_{*j} ע"י הבסיס $a_{*j_1},\dots,a_{*j_r}$

קיבלנו מטריצה מדורגת מסדר $r\times n$

$D=$ 

נניח ש B מטריצה הפיכה (סתם) אז

$$BA = B(a_{*1}\dots a_{*n}) = (Ba_{*1},\dots,Ba_{*n}) =$$

$$= (f_B(a_{*1}),\dots,f_B(a_{*n}))$$

$f_B: F^m \to F^m$, $c \mapsto Bc$

B הפיכה. אז $C = B^{-1}$ $f_C : F^m \to F^m$

אז $f_C = f_B^{-1}$.

אם $D_1 = B_1 A$ ו- $C_1 = B_1^{-1}$ אז $A = C_1 D_1$

<u>טענה:</u> אם B מטריצה הפיכה, אז עבור A ועבור BA מקבלים אותה מטריצה מדורגת מסדר חצי.

עמודות של A: $(a_{*1} \dots a_{*n})$; עמודות של BA: $(Ba_{*1} \dots Ba_{*n}) =$

$= (f_B(a_{*1}) \dots f_B(a_{*n}))$ ⟵ $f_B : F^m \to F^m$, $c \mapsto Bc$

כי העתקה לינארית הפיכה וזה כי B הפיכה $C = B^{-1}$

ו- $f_C = f_B^{-1}$!

לכן צורת המטריצה דומה היות כמו: ההעתקה מעבירה וקטורים בת"ל לוקטורים בת"ל אז העמודות המובילות יראו אותו דבר.

התהליך של בניית מטריצה מדורגת (כמתואר קודם) נותן תוצאה זהה עבור ~~הוקטורים~~: הוקטורים $a_{*1}, \dots, a_{*n}$ ועבור הוקטורים $f_B(a_{*1}) \dots f_B(a_{*n})$ כי $f_B : F^m \to F^m$ העתקה לינארית הפיכה וזה.

כלומר: ל- A יש אותה תוצאה כמו $B_1 A$

ול- A יש אותה תוצאה כמו $B_2 A$

אז ל- $B_1 A$ ול- $B_2 A$ יש אותה תוצאה.

$\Leftarrow D_1 = D_2$. מש"ל ☺

יהיו $A,B\in M_n(F)$ אזי $A+B\in M_n(F)$, $A\cdot B$

האם זה שדה? נבדוק, אילו אקסיומות מתקיימות:

כפל		חיבור	
סגירות	מתקיים	סגירות	מתקיים
קיבוציות	מתקיים	חילופיות	מתקיים
קיום יחידה	מתקיים	קיבוציות	מתקיים
חילופיות	לא בהכרח	אפס	מתקיים
קיום הפכי	לא בהכרח	קיום נגדי	מתקיים

פילוג מתקיים
$$A(B+C)=AB+AC$$
$$(A+B)C=AC+BC.$$

$M_n(F)$ אינו שדה. אבל זה חוג (ring).

יש תיאוריה נרחבת של חוגים ובפרט של חוגים קומוטטיביים.

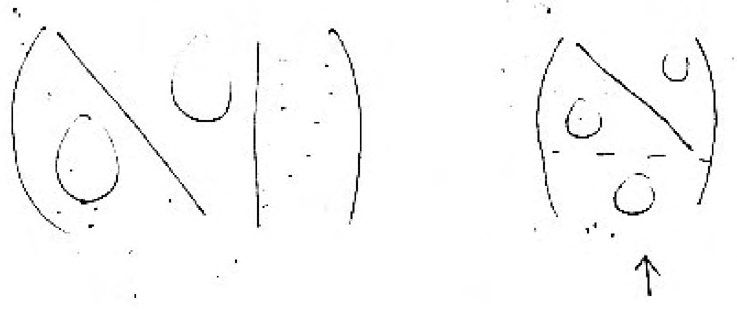
באותו אופן $End_F(V)=Hom_F(V,V)$ חוג עם יחידה.

ויש ביניהם איזומורפיזם של חוגים.

בשיעור הבא נעשה חזרה.

שאלה: פיתרון של מע' משוואות לינאריות כאשר צריך לדרג את המערכת.

תשובה: בונים מטריצת המקדמים המורחבת ומדרגים כך, שיש מתחת לאלכסון ואם מעליו יש אפסים.



פה אין פתרונות

(69) 1/2/06
לינארית

תרגיל (כל הבודדים שביקשו את זה...)

ריפס התבקש לפתור מע' משוואות ב-4 נעלמים

$$\begin{cases} 4x + 3y + z = -2 \\ 3x + 2y + 5z - m = 0 \\ 3y - 2z + 3m = 5 \\ x + 2y + \frac{1}{2}z + 5m = 3 \end{cases}$$

נבנה מטריצת המקדמים המורחבת:

$$\begin{pmatrix} 4 & 3 & 1 & 0 & -2 \\ 3 & 2 & 5 & -1 & 0 \\ 0 & 3 & -2 & 3 & 5 \\ 1 & 2 & \frac{1}{2} & 5 & 3 \end{pmatrix} \xrightarrow{L_1 \to L_1 - L_2} \begin{pmatrix} 1 & 1 & -4 & 1 & -2 \\ 3 & 2 & 5 & -1 & 0 \\ 0 & 3 & -2 & 3 & 5 \\ 1 & 2 & \frac{1}{2} & 5 & 3 \end{pmatrix} \xrightarrow{L_2 \to L_2 - 3L_1}$$

הערה: הוכחנו את משפט היחידות. לכן לא משנה באיזו דרך נבחר: אנחנו אמורים להגיע לאותה התוצאה הסופית. למשל היה יותר קל פה להחליף את שורה 1 בשורה 4 ואת שורה 2 בשורה 3.

$$\begin{pmatrix} 1 & 1 & -4 & 1 & -2 \\ 0 & -1 & 17 & -4 & 6 \\ 0 & 3 & -2 & 3 & 5 \\ 1 & 2 & \frac{1}{2} & 5 & 3 \end{pmatrix} \xrightarrow{L_4 \to L_4 - L_1} \begin{pmatrix} 1 & 1 & -4 & 1 & -2 \\ 0 & -1 & 17 & -4 & 6 \\ 0 & 3 & -2 & 3 & 5 \\ 0 & 1 & 4\frac{1}{2} & 4 & 5 \end{pmatrix} \xrightarrow{L_2 \to -L_2}$$

$$\begin{pmatrix} 1 & 1 & -4 & 1 & -2 \\ 0 & 1 & -17 & 4 & -6 \\ 0 & 3 & -2 & 3 & 5 \\ 0 & 1 & 4\frac{1}{2} & 4 & 5 \end{pmatrix} \xrightarrow[\substack{L_3 \to L_3 - 3L_2 \\ L_4 \to L_4 - L_2}]{L_1 \to L_1 - L_2} \begin{pmatrix} 1 & 0 & 13 & -3 & 4 \\ 0 & 1 & -17 & 4 & -6 \\ 0 & 0 & 49 & -9 & 23 \\ 0 & 0 & 21\frac{1}{2} & 0 & 11 \end{pmatrix} \xrightarrow{L_4 \to 2L_4}$$

$$\begin{pmatrix} 1 & 0 & 13 & -3 & 4 \\ 0 & 1 & -17 & 4 & -6 \\ 0 & 0 & 49 & -9 & 23 \\ 0 & 0 & 43 & 0 & 22 \end{pmatrix} \xrightarrow[L_3 \to L_3 - L_4]{} \begin{pmatrix} 1 & 0 & 13 & -3 & 4 \\ 0 & 1 & -17 & 4 & -6 \\ 0 & 0 & 6 & -9 & 1 \\ 0 & 0 & 43 & 0 & 22 \end{pmatrix} \xrightarrow[L_4 \to L_4 - 7L_3]{}$$

$$\begin{pmatrix} 1 & 0 & 13 & -3 & 4 \\ 0 & 1 & -17 & 4 & -6 \\ 0 & 0 & 6 & -9 & 1 \\ 0 & 0 & 1 & 63 & 15 \end{pmatrix} \xrightarrow[\substack{L_3 \to L_4 \\ L_4 \to L_3}]{} \begin{pmatrix} 1 & 0 & 13 & -3 & 4 \\ 0 & 1 & -17 & 4 & -6 \\ 0 & 0 & 1 & 63 & 15 \\ 0 & 0 & 6 & -9 & 1 \end{pmatrix} \xrightarrow[\substack{L_2 \to L_2 + 17L_3 \\ L_4 \to L_4 - 6L_3}]{}$$

$$\begin{pmatrix} 1 & 0 & 0 & -822 & -191 \\ 0 & 1 & 0 & 1075 & 249 \\ 0 & 0 & 1 & 63 & 15 \\ 0 & 0 & 0 & -387 & -89 \end{pmatrix} \xrightarrow[L_4 \to \frac{L_4}{-387}]{} \begin{pmatrix} 1 & 0 & 0 & -822 & -191 \\ 0 & 1 & 0 & 1075 & 249 \\ 0 & 0 & 1 & 63 & 15 \\ 0 & 0 & 0 & 1 & \frac{89}{387} \end{pmatrix}$$

$$\xrightarrow[\substack{L_3 \to L_3 - 63L_4 \\ L_2 \to L_2 - 1075L_4 \\ L_1 \to L_1 + 822L_4}]{} \begin{pmatrix} 1 & 0 & 0 & 0 & -\frac{759}{387} \\ 0 & 1 & 0 & 0 & \frac{688}{387} \\ 0 & 0 & 1 & 0 & \frac{198}{387} \\ 0 & 0 & 0 & 1 & \frac{89}{387} \end{pmatrix}$$

Wuhu!

אז אנו פתרון יחיד!

$x = -\frac{759}{387}$

$y = \frac{688}{387}$

$z = \frac{198}{387}$

$m = \frac{89}{387}$

במקרה הזה היינו זקוקים בעיקר לאורך רוח...

הסימן שיש פתרון יחיד למע' משוואות הוא שאחרי הדירוג קיבלנו חוץ מהעמודה האחרונה (שמביא בעצם הפתרונות) את מטריצת היחידה.

$$\begin{pmatrix} 1 & 0 & 0 & c & x \\ 0 & 1 & 0 & 0 & y \\ 0 & 0 & 1 & 0 & z \end{pmatrix}$$

אם שורה אחת מתאפסת לגמרי אז יש אינסוף פתרונות ולחלק מהמשתנים אפשר פשוט להתייחס אליהם כפרמטרים שיכולים לקבל כל ערך

$$\begin{matrix} 0 & 1 & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{matrix}$$

$$x_2 + 2x_3 + 3x_5 = 1$$
$$x_4 = 2$$
$$x_5 = 2$$

כאן x_1, x_3 הוא פרמטר נניח $x_3 = b,\ x_1 = a$

$$\Rightarrow x_5 = 2$$
$$x_4 = 2$$
$$x_2 + 2b + 3a = 1 \Rightarrow x_2 = 1 - 2b - 3a$$

הפתרונות: הם $\begin{pmatrix} a \\ 1-2b-3a \\ b \\ 2 \\ 2 \end{pmatrix}$ ואפשר לרשום

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 2 \\ 2 \end{pmatrix} + a \begin{pmatrix} 1 \\ 0 \\ -3 \\ 0 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ -2 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 2 \\ 2 \end{pmatrix} + Sp\left\{ \begin{pmatrix} 0 \\ -2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -3 \\ 0 \\ 0 \end{pmatrix} \right\}$$

וכו' ישרייה!

איך הופכים מטריצה $A_{n\times n}$?

נסתכל על $(A|I)$ - שתי המטריצות הרשומות זו ליד זו.

אז $B(A|I) = (BA|BI)$

ואם $B=A^{-1}$ אז

$$B(A|I) = (A^{-1}A|A^{-1}I) = (I|A^{-1})$$

אז מה שצריך לעשות הוא להשתמש בפעולות גאוס כדי לצמצם את A ואת אותן הפעולות לעשות על I.

מה שיוצא מ-I הוא A^{-1}.

למשל נהפוך את $\begin{pmatrix}1&2\\3&4\end{pmatrix}$

$$\left(\begin{array}{cc|cc}1&2&1&0\\3&4&0&1\end{array}\right)\rightarrow\left(\begin{array}{cc|cc}1&2&1&0\\0&-2&-3&1\end{array}\right)$$

$$\rightarrow\left(\begin{array}{cc|cc}1&0&-2&1\\0&-2&-3&1\end{array}\right)\rightarrow\left(\begin{array}{cc|cc}1&0&-2&1\\0&1&\frac{3}{2}&-\frac{1}{2}\end{array}\right)$$

איך יודעים את מטריצה היא הפיכה?

מנסים להפוך אותה. אם יוצא אז סבבה!

אם A מדרגה $n\times n$ ו-$rankA=n$! אז היא הפיכה.

חוץ מזה אם הדטרמיננטה שונה מ-0 המטריצה הפיכה (את זה נלמד בסמסטר הבא)