# שיעור 2 שדות

## 2.1 מספרים מרוכבים

#### הגדרה 2.1 מספר מרוכב

מספר מחוכב. של מספרים ממשיים נקרא מספר מרוכב. z=(x,y) זוג סדור

אם מרוכבים בין מספרים מרוכבים: x=(x,0). נסמן y=0 אם y=0

### הגדרה 2.2 פעולות בינאריות של מספרים מרוכבים

 $z_1=(x_2,y_2)$  , $z_1=(x_1,y_1)$  נניח

1) חיבור

 $z_1 \oplus z_2 = (x_1 + x_2, y_1 + y_2)$ 

2) כפל

 $z_1 \odot z_2 = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$ 

קל לראות:

מתקיים 
$$z_1=(x_1,y_1)$$
 לכל מספר ממשי  $x=(x,0)$  ולכל  $x=(x,0)$  לכל מספר מספר לכל  $x\cdot z_1=(x\cdot x_1,x\cdot y_1)$ 

מתקיים ( $x_2,0$ ) -ו ( $x_1,0$ ) ממשיים (2

$$(x_1,0)\cdot(x_2,0)=(x_1x_2,0)=x_1x_2$$

## i 2.3 הגדרה

נסמן

$$i = (0,1)$$
.

היא i

$$i^2 = i \cdot i = (0,1) \cdot (0,1) = (0 \cdot 0 - 1 \cdot 1, \ 0 \cdot 1 + 1 \cdot 0) = (-1,0) = -1.$$

## משפט 2.1 הצגה אלגברית שך מספר מרוכב

תוך שימוש במספר i כל מספר מרוכב z=(x,y) ניתן לרשום

$$z = (x, y) = (x, 0) \oplus (0, y) = (x, 0) \oplus (y, 0) \cdot (0, 1) = x + iy.$$

מספר מרוכב. נקרא הצגה אלגברית של x+iy

 $x = \operatorname{Re}(z)$  מסמנים z הממשי של ל-  $x = \operatorname{Re}(z)$ 

 $y = \operatorname{Im}(z)$  מסמנים z ל- y קוראים החלק המדומה של

 $\dot{x}=-1$  ב- בהתחשב ב- רוכבים מספרים לחבר לחבר לחבר לחבר מאפשרת מאפשרת ב- ב- צורת הכתיבה ב- ולהכפיל

#### דוגמה 2.1

X

$$(x_1+iy_1)\odot(x_2+iy_2)=x_1x_2+ix_1y_2+iy_1x_2-y_1y_2=(x_1x_2-y_1y_2)+i(x_1y_2+y_1x_2)$$
.

#### דוגמה 2.2

$$(3-5i) \odot (2+3i) = 6+9i-10i+15=21-i$$
.

#### הגדרה 2.4 הצמוד

המספר הרוכב z=x+iy מסנים: x-iy מסנים:

$$\bar{z} = x - iy$$
.

#### משפט 2.2

$$z\odot \bar{z} = x^2 + y^2 .$$

 $oldsymbol{z}$  המספר הזה נקרא ה $oldsymbol{n}$ ער או הגודל של המספר מספר המרוכב

#### דוגמה 2.3

$$\frac{3+4i}{1-i} = \frac{(3+4i)(1+i)}{(1-i)(1+i)} = \frac{3+3i+4u-4}{2} = \frac{-1+7i}{2} = -\frac{1}{2} + \frac{7}{2}i$$

#### דוגמה 2.4

מצאו את המספר z המקיים את מצאו

$$\frac{1-iz}{1+iz} = -2i \ .$$

פתרון:

$$1 - iz = -2i(1 + iz) = 2z - 2i$$
  $\Rightarrow$   $z(2 + i) = 1 + 2i$ 

$$z = \frac{1+2i}{2+i} = \frac{(1+2i)(2-i)}{(2+i)(2-i)} = \frac{2-i+4i+2}{5} = \frac{4+3i}{5} = \frac{4}{5} + \frac{3}{5}i$$

 $\mathbb{C}$  -קבוצת המספרים המרוכבים מסומנת

אפשר לראות בקלות ש-  $\mathbb C$  יחד עם שתי הפעולות שהגדרנו בהגדרה 2.10 מקיימת את כל האקסיומות של שדה, כאשר

$$0 = (0,0)$$

$$1=(1,0)$$
 ועבור  $z^{-1}=rac{1}{x+iy}=rac{x-iy}{x^2+y^2}=rac{x}{x^2+y^2}-i\cdotrac{y}{x^2+y^2}$  .

## 2.2 הצגה פולרית של מספרים מרוכבים

#### הגדרה 2.5 הצגה פולרית

ניתן לרשום מספר מרוכב z=x+iy מספר מספר ניתן

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

כאשר

$$r = \sqrt{x^2 + y^2} = |z|$$
,  $\theta = \arctan\left(\frac{y}{x}\right)$ .

## דוגמה 2.5

רשמו את המספרים המרוכבים הבאים בהצכה פולרית:

$$z_1 = 3 + 4i$$
 (1

$$z_2 = -3 + 4i$$
 (2

$$z_3 = -3 - 4i$$
 (3

$$z_4 = 3 - 4i$$
 (4

## פתרון:

(2

(3

(4

$$r=|z_1|=\sqrt{3^2+4^2}=5 \; , \qquad heta=rctan\left(rac{4}{3}
ight)=53.1^\circ \; .$$

$$r = |z_2| = \sqrt{(-3)^2 + 4^2} = 5$$
,  $\theta = \arctan\left(\frac{4}{-3}\right) = 180^\circ - \arctan\left(\frac{4}{3}\right) = 126.9^\circ$ .

$$r=|z_3|=\sqrt{(-3)^2+(-4)^2}=5 \ , \qquad \theta=180^\circ+\arctan\left(rac{4}{3}
ight)=233.1^\circ \ .$$

$$r=|z_4|=\sqrt{(3)^2+(-4)^2}=5 \ , \qquad \theta=360^\circ-\arctan\left(rac{4}{3}
ight)=306.9^\circ \ .$$

#### 2.3 משפט

אם 
$$z_2=r_2\left(\cos\theta_2+i\sin\theta_2
ight)$$
 ואם  $z_1=r_1\left(\cos\theta_1+i\sin\theta_1
ight)$  אם  $z_1z_2=r_1r_2\left(\cos\left(\theta_1+\theta_2
ight)+i\sin\left(\theta_1+\theta_2
ight)
ight)$  .

$$\frac{z_1}{z_2} = \frac{r_1}{r_2} \left( \cos \left( \theta_1 - \theta_2 \right) + i \sin \left( \theta_1 - \theta_2 \right) \right) , \qquad (z_2 \neq 0) .$$

### משפט 2.4

אט 
$$z=r\left(\cos heta+i\sin heta
ight)$$
 אם

$$z^{n} = r^{n} \left( \cos \left( n\theta \right) + i \sin \left( n\theta \right) \right) .$$

# p קבוצת השאריות בחלוקה ב $\mathbb{Z}_p$ 2.3

### הגדרה 2.6

-יהיו q מספר שלם מספר אם מחלק את מחלק כי אומרים שלם. אומרים שלם מספר a,b יהיו

$$a = qb$$
.

q בלומר שלם שווה למספר שלם כלומר

a אומר כי b מחלק את  $b \mid a$  הסימון

#### דוגמה 2.6

- 6=3q -כך ש- q=2 כך שספר שלם 3 בגלל שקיים מספר 3 ( בגלל שקיים
- 42 = 7q -ע כך ש- q = 6 כל שקיים מספר 7 בגלל אקיים 7 א 7 בגלל 142 (ב
  - .8=5q -ע כך שלם שלם קיים מספר שלם בגלל שלא ל $5 \nmid 8$

## b -ל a יחס שקילות בין 2.7 הגדרה

נניח כי  $a,b\in\mathbb{Z}$  מספרים שלמים ו- מספר שלם חיובי. היחס

 $a \equiv b \mod m$ 

m|a-b אומר כי m מחלק את ההפרש ,a-b מחלק

a=qm+b כך ש- q כך שלם אם אם  $a\equiv b \mod m$  בנסוח שקול,

."m מודולו b - שקול ל- מודולו מיים אומרים כי

#### דוגמה 2.7

הוכיחו כי

- $5 \equiv 2 \mod 3$  (x
- $43 \equiv 23 \mod 10$  (ع
  - $7 \not\equiv 2 \mod 4$  (x

### פתרון:

(N

$$5-2=3=1\cdot 3 \quad \Rightarrow \quad 3\mid 5-2 \quad \Rightarrow \quad 5\equiv 2 \mod 3 \ .$$

(2

$$43-23=20=2\cdot 10\quad \Rightarrow\quad 10\mid 43-23\quad \Rightarrow\quad 43\equiv 23\mod 10\;.$$

.7 - 2 = 5 (x)

לא קיים שלם q כך ש- q-2 לכן q-7-7 לכן לא קיים שלם

 $7 \not\equiv 2 \mod 4$ .

## הגדרה 2.8 השארית

נתונים מספרים שלמים , $a,b\in\mathbb{Z}$  היחס

a % b

b -ב a מציין את השארית בחלוקת

#### דוגמה 2.8

43 % 10 = 3.

13 % 4 = 1.

8 % 2 = 0.

-10 % 3 = -1.

### דוגמה 2.9

 $\bullet$  השארית של 3 בחילוק ב- 2 היא 1. לכן

3 % 2 = 1.

לכן 3 היא 4 בחילוק ב- 4 היא השארית של

7 % 4 = 3.

השארית של 11 בחילוק ב-8 היא 3. לכן •

11 % 8 = 3.

## p-בחלוקה בחלוקה - $\mathbb{Z}_p$ 2.9 הגדרה

יהי מספר האשוני. הקבוצה  $\mathbb{Z}_p$  מספר ראשוני. הקבוצת

 $\{\overline{0},\overline{1},\overline{2},\ldots,\overline{p-1}\}$ .

הקבוצה מוגדרת לפי התנאים הבאים:

- . כל איבר שלם הוא מספר  $a\in\mathbb{Z}_p$  כל איבר (1)
- לפי  $\mathbb{Z}_p$  -ב a לכל מספר שלם n נתאים איבר (2)

 $n \equiv a \mod p$  .

## דוגמה 2.10

:לקבוצה  $\mathbb{Z}_3$  יש

$$\{\mathbb{Z}_3 = \bar{0}, \bar{1}, \bar{2}\}$$
.

$$3 = 0 \mod 3 \Rightarrow \bar{3} = \bar{0}$$

$$4 = 1 \mod 3 \Rightarrow \qquad \bar{4} = \bar{1}$$

$$5=2 \mod 3 \Rightarrow \qquad \bar{5}=\bar{2}$$

$$6 = 0 \mod 3 \Rightarrow \bar{6} = \bar{0}$$

$$7=1\mod 3 \Rightarrow \qquad \bar{7}=\bar{1}$$

$$8 = 2 \mod 3 \Rightarrow \bar{8} = \bar{2}$$

$$122 = 2 \mod 3 \Rightarrow \overline{122} = \overline{2} \ .$$

וכן הלאה.

## איברי $\mathbb{Z}_p$ איברי בינאריות של 2.10 הגדרה

 $ar a,ar b\in\mathbb Z_p$  לכל p -ב מסםר השאריות השאריות קבוצת  $\mathbb Z_p=\{ar 0,ar 1,\dots,\overline{p-1}\}$  לכל פלל מסםר הפעולות חיבור וכפל כך:

1) חיבור

$$\bar{a} \oplus \bar{b} = \overline{a+b}$$

<u>2) כפל</u>

$$\bar{a}\odot\bar{b}=\overline{a\cdot b}\ .$$

#### דוגמה 2.11

חשבו ב- $\mathbb{Z}_5$  את

$$.ar{2}\oplusar{4}$$
 (א

 $.ar{3}\odotar{3}$  (2

$$.ar{2}\oplusar{4}=\overline{2+4}=ar{6}=ar{1}$$
 (8

$$.ar{3}\odotar{3}=\overline{3\cdot3}=ar{9}=ar{4}$$
 (2

חשבו ב- תשבו את

$$.ar{3}\odotar{7}$$
 (x

$$ar{.2}\odotar{8}$$
 (2

## פתרון:

$$.ar{3}\odotar{7}=\overline{3\cdot7}=\overline{21}=\overline{10}$$
 (א

$$.ar{2}\cdotar{8}=\overline{16}=ar{5}$$
 (2

## דוגמה 2.13

$$: \mathbb{Z}_3$$
 -בור של איברים ב-

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$	

$$: \mathbb{Z}_3$$
 -ברים ב- לוח הכפל של

	, <u> </u>	-	/
$\odot$	$ \bar{0} $	1	$\bar{2}$
$\bar{0}$	Ō	$\bar{0}$	$\bar{0}$
$ar{1} \ ar{2}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

## דוגמה 2.14

 $\mathbb{Z}_5$  לוח החיבור של איברים של

J					—		1
	<u> </u>	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	
	$\bar{0}$	Ō	Ī	$\bar{2}$	3	<u>4</u>	
	$ar{1}$ $ar{2}$ $ar{3}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	
	$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	
	$\bar{3}$	$\begin{bmatrix} \bar{0} \\ \bar{0} \\ \bar{1} \\ \bar{2} \\ \bar{3} \\ \bar{4} \end{bmatrix}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	
	$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	

 $\mathbb{Z}_5$  לוח הכפל של איברים של

۰,	o	_	,			_,,,	,,,
	$\odot$	$\bar{0}$	Ī	$\bar{2}$	$\bar{3}$	$\bar{4}$	
	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	•
	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\ddot{\bar{3}}$	$\bar{4}$	
	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$	
	$ \begin{array}{c} \hline 0\\ \bar{1}\\ \bar{2}\\ \bar{3}\\ \bar{4} \end{array} $	$\begin{array}{c} \bar{0} \\ \bar{0} \\ \bar{0} \\ \bar{0} \\ \bar{0} \end{array}$	$ \begin{array}{c} \bar{0} \\ \bar{1} \\ \bar{2} \\ \bar{3} \\ \bar{4} \end{array} $	$ \begin{array}{c} \bar{2} \\ \bar{4} \\ \bar{1} \\ \bar{3} \end{array} $	$\frac{\bar{4}}{\bar{2}}$	$ \begin{array}{c} \bar{4} \\ \bar{3} \\ \bar{2} \\ \bar{1} \end{array} $	
	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	

 $rac{1}{7}\cdot 7=1$  כי ( $rac{1}{7}$ ) כי ההופכי של 7 הוא 7, ( או

: כלומר . $ar{1}$  הוא הנגדי של ל $ar{2}$  ולכן ל $ar{2}+ar{1}=ar{0}$  מתקיים , $\mathbb{Z}_3$  מתקיים

$$-\bar{1}=\bar{2} \ .$$

 $-ar{2}=ar{1}$  באופן דומה,  $ar{1}$  הוא הנגדי של

 $\bar{z}_{1}(\bar{z})^{-1}=\bar{z}$  כלומר הופכי של  $\bar{z}_{1}(\bar{z})^{-1}=\bar{z}_{2}$  מתקיים ליים ולכן ליים ולכן ליים ולכן

## $\mathbb{Z}_p$ משפט 2.5 איבר ההופכי ואיבר הנגדי בקבוצה

p -יהי p מספר ראשוני ותהי  $\mathbb{Z}_p$  הקבוצה השאריות בחלוקה בp

## א) איבר הנגדי

-כך ש- כך כך  $-a\in\mathbb{Z}_p$  לכל איבר  $a\in\mathbb{Z}_p$  קיים איבר יחיד

$$a \oplus (-a) = \bar{0} .$$

a נקרא האיבר הנגדי של -a

#### ב) איבר ההופכי

-לכל איבר  $\mathbb{Z}_p$  שונה מאפס (כלומר  $ar{0} 
eq ar{0}$  קיים איבר יחיד  $a \in \mathbb{Z}_p$  כך ש

$$a \odot a^{-1} = \bar{1}$$
.

 $a^{-1}$  נקרא האיבר ההופכי של  $a^{-1}$ 

## דוגמה 2.15

 $\mathbb{Z}_3$  -ם  $ar{1}$  מצאו את האיבר הנגדי של

## פתרון:

נשים לב ש-

$$\bar{1}\oplus\bar{2}=\bar{3}=\bar{0}$$

ולכן

$$-\bar{1}=\bar{2}.$$

### דוגמה 2.16

 $\mathbb{Z}_3$  -ב  $\bar{2}$  מצאו את האיבר הנגדי של

#### פתרון:

נשים לב ש-

$$\bar{2}\oplus\bar{1}=\bar{3}=\bar{0}$$

ולכן

$$-\bar{2}=\bar{1}.$$

 $\mathbb{Z}_3$  -ם  $ar{3}$  של מצאו את האיבר הנגדי

## פתרון:

נשים לב ש-

$$\bar{3}\oplus\bar{0}=\bar{3}=\bar{0}$$

ולכן

$$-\bar{3}=\bar{3}.$$

## דוגמה 2.18

 $: \mathbb{Z}_3$  איברים של איברים של

$$-\bar{1} = \bar{2}$$

$$-\bar{2}=\bar{1}$$

$$-\bar{3} = \bar{0}$$

$$-\bar{4}=\bar{2}$$

$$-\bar{5}=\bar{1}$$

$$-\bar{6} = \bar{0}$$

$$-\bar{7}=\bar{2}$$

$$-\bar{8}=\bar{1}$$

:

$$-\bar{5}9 = \bar{1} .$$

## דוגמה 2.19

 $\mathbb{Z}_3$  -ב  $ar{2}$  של מצאו את האיבר ההופכי

### פתרון:

$$\bar{2}\odot\bar{2}=\bar{4}=\bar{1}$$

$$ar{2}^{-1}=ar{2}$$
 . לכן

## דוגמה 2.20

 $\mathbb{Z}_3$  -ב  $ar{1}$  בי של ל

$$\bar{1}\odot\bar{1}=\bar{1}$$

$$.ar{1}^{-1}=ar{1}$$
 לכן

 $\mathbb{Z}_5$  -ם  $\bar{3}$  של מצאו את האיבר ההופכי

## פתרון:

$$\bar{3}\odot\bar{2}=\bar{6}=\bar{1}$$

$$.ar{3}^{-1}=ar{2}$$
 לכן

## דוגמה 2.22

 $\mathbb{Z}_5$  -ם הבאים האיברים של כל החופכי ההופכי את חשבו את

- $\bar{1}$  (x)
- $\bar{2}$  (2)
- $\bar{3}$  (x)
- $\bar{4}$  (T)

## פתרון:

$$\bar{1} \odot \bar{1} = \bar{1} \quad \Rightarrow \quad \bar{1}^{-1} = \bar{1}$$

$$\bar{2}\odot\bar{3}=\bar{6}=\bar{1}$$
  $\Rightarrow$   $2^{-1}=\bar{1}$ 

$$\bar{3}\odot\bar{2}=\bar{6}=\bar{1}$$
  $\Rightarrow$   $\bar{3}^{-1}=\bar{1}$ 

$$\bar{4}\odot\bar{4}=\overline{16}=\bar{1}$$
  $\Rightarrow$   $\bar{4}^{-1}=\bar{1}$ 

## דוגמה 2.23

 $: \mathbb{Z}_{11}$  -חשבו ב

$$\bar{3}\odot \bar{7}$$
 (א)

$$ar{2}\odotar{8}$$
 (2)

$$-ar{3}$$
 (x)

$$(\bar{3})^{-1}$$
 (T)

$$ar{3}\odotar{7}=\overline{21}=\overline{10}$$
 (א)

$$ar{2}\odotar{8}=\overline{16}=ar{5}$$
 (2)

$$\bar{3}\oplus \bar{8}=\overline{11}=\bar{0}$$
  $\Rightarrow$   $-\bar{3}=\bar{8}$  . (a)

$$\bar{3}\odot \bar{4}=\overline{12}=\bar{1}$$
  $\Rightarrow$   $(\bar{3})^{-1}=\bar{4}$  . (7)

## 2.4 שדות

## הגדרה 2.11 שדה

קבוצה לא ריקה  $\mathbb{F}$ , שבה פעולת חיבור  $\oplus$  ופעולת כפל  $\odot$  מוגדרות על הקבוצה, מסומנת קבוצה לא ריקה קבוצה שדה שבה מתקיימים. לכל איברים  $a,b,c\in\mathbb{F}$ 

:סגורה תחת חיבור  $\mathbb{F}$  (1

 $a \oplus b \in \mathbb{F}$ .

:סגורה תחת כפל  $\mathbb{F}$  (2

 $a\odot b\in\mathbb{F}$ .

I: חוק החילוף (3

 $a \oplus b = b \oplus a$ 

II: חוק החילוף (4

 $a \odot b = b \odot a$ 

I: חוק הקיבוץ (**5** 

 $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ .

II: חוק הקיבוץ (6

 $a \odot (b \odot c) = (a \odot b) \odot c$ 

7) חוק הפילוג:

 $a \odot (b \oplus c) = a \odot b + a \odot c$ .

(8) קיום איבר ניוטרלי:

-קיים איבר  $0\in\mathbb{F}$  כך ש

 $a \oplus 0 = a$ .

(האיבר ניוטרל לגבי כפל: האיבר ניוטרל לגבי כפל):

-קיים איבר  $1\in\mathbb{F}$  כך ש

 $a\odot 1=a$  ,  $1\odot a=a$  .

(10) קיום איבר נגדי:

-לכל  $(-a)\in\mathbb{F}$  כך איבר נגדי  $a\in\mathbb{F}$  לכל

 $a \oplus (-a) = 0$ .

#### (11) קיום איבר הופכי:

לכל  $a^{-1} \in \mathbb{F}$  כך שa 
eq 0 קיים איבר  $a \in \mathbb{F}$  לכל

$$a \odot a^{-1} = 1$$
 ,  $a^{-1} \odot a = 1$  .

#### דוגמה 2.24

- א) הקבוצה  $\mathbb R$  של מספרים ממשיים שדה.
- בוצה  $\mathbb C$  של מספרים מרובכים שדה.

#### דוגמה 2.25

. שדה  $\mathbb{N}$  שדה קבעו אם הקבוצה

#### פתרון:

לא שדה. כדי להראות זאת די למצוא דוגמה נגדית לאחת התכונות.:  $a=3\in\mathbb{N}$  נבחור מבחור ...

$$-3 + 3 = 0$$

 $.-3 \notin \mathbb{N}$  אבל

## 2.6 משפט

. שדה  $(\mathbb{F},\oplus,\odot)$  יהי

- . עבור  $a\in\mathbb{F}$  האיבר הנגדי החיבורי,  $a\in\mathbb{F}$
- . עבור  $a^{-1}$  הוא יחיד. ( $a \neq 0$ ), האיבר ההפכי הכפלי ( $a \neq 0$ ) מ

#### 2.7 משפט

. יהי התיבור הנגדי האיבר הניוטרלי הכפלי ו- -1האיבר הנגדי החיבורי.  $a,b\in\mathbb{F}$ יהי יהי שדה, יהיו יהי

$$a \odot 0 = 0$$
 (1

$$a \odot (-1) = -a$$
 (2

$$.b=0$$
 אז  $a 
eq 0$  -ו $a \odot b = 0$  אז (3

הוכחה: תרגיל בית!

## ${\Bbb C}$ מערכות לינאריות מעל 2.5

.C מעל 
$$\begin{cases} (1+i)z_1 + (1-i)z_2 = 3i \\ 3z_1 + (2-i)z_2 = 4 \end{cases}$$
מעל

#### פתרון:

$$\begin{pmatrix}
1+i & 1-i & 3i \\
3 & 2-i & 4
\end{pmatrix}
\xrightarrow{R_1 \to (1-i)R_1}
\begin{pmatrix}
2 & -2i & 3+3i \\
3 & 2-i & 4
\end{pmatrix}
\xrightarrow{R_2 \to 2R_2 - 3R_1}
\begin{pmatrix}
2 & -2i & 3+3i \\
0 & 4+4i & -1-9i
\end{pmatrix}$$

$$\xrightarrow{R_2 \to (4-4i)R_2}
\begin{pmatrix}
2 & -2i & 3+3i \\
0 & 32 & -40-32i
\end{pmatrix}
\xrightarrow{R_1 \to 16R_1 + iR_2}
\begin{pmatrix}
32 & 0 & 80+8i \\
0 & 32 & -40-32i
\end{pmatrix}$$

$$\xrightarrow{R_1 \to \frac{1}{32}R_1}
\begin{pmatrix}
1 & 0 & \frac{5}{2} + \frac{1}{4}i \\
0 & 1 & -\frac{5}{4} - i
\end{pmatrix}$$

פתרון:

$$z_1 = \frac{5}{2} + \frac{1}{4}i$$
,  $z_2 = -\frac{5}{4} - i$ 

# $\mathbb{Z}_p$ מערכות לינאריות מעל 2.6

### דוגמה 2.27

 $\mathbb{Z}_3$  פתור את המערכת הבאה מעל

$$x_1 + x_2 + x_3 = \bar{0}$$

$$x_1 - x_2 - x_3 = \bar{0}$$

$$x_1 + \bar{2}x_2 + x_3 = \bar{1}$$

#### פתרון:

המטריצה המורחבת היא

$$\begin{pmatrix}
\bar{1} & \bar{1} & \bar{1} & \bar{0} \\
\bar{1} & -\bar{1} & -\bar{1} & \bar{0} \\
\bar{1} & \bar{2} & \bar{1} & \bar{1}
\end{pmatrix} = \begin{pmatrix}
\bar{1} & \bar{1} & \bar{1} & \bar{0} \\
\bar{1} & \bar{2} & \bar{2} & \bar{0} \\
\bar{1} & \bar{2} & \bar{1} & \bar{1}
\end{pmatrix}$$

נבצע שיטת גאוס:

$$\begin{pmatrix}
\bar{1} & \bar{1} & \bar{1} & \bar{0} \\
\bar{1} & \bar{2} & \bar{2} & \bar{0} \\
\bar{1} & \bar{2} & \bar{1} & \bar{1}
\end{pmatrix}
\xrightarrow{R_2 \to R_2 - R_1}
\begin{pmatrix}
\bar{1} & \bar{1} & \bar{1} & \bar{0} \\
\bar{0} & \bar{1} & \bar{1} & \bar{0} \\
\bar{1} & \bar{2} & \bar{1} & \bar{1}
\end{pmatrix}$$

$$\xrightarrow{R_3 \to R_3 - R_1}
\begin{pmatrix}
\bar{1} & \bar{1} & \bar{1} & \bar{0} \\
\bar{0} & \bar{1} & \bar{1} & \bar{0} \\
\bar{0} & \bar{1} & \bar{0} & \bar{1}
\end{pmatrix}$$

$$\xrightarrow{R_3 \to R_3 - R_2}
\begin{pmatrix}
\bar{1} & \bar{1} & \bar{1} & \bar{0} \\
\bar{0} & \bar{1} & \bar{1} & \bar{0} \\
\bar{0} & \bar{0} & -\bar{1} & \bar{1}
\end{pmatrix}
=
\begin{pmatrix}
\bar{1} & \bar{1} & \bar{1} & \bar{0} \\
\bar{0} & \bar{1} & \bar{1} & \bar{0} \\
\bar{0} & \bar{0} & \bar{2} & \bar{1}
\end{pmatrix}$$

 $ar{z}^{-1} = ar{2}$  בכפיל את השורה השלישית בלכן נבצע את הפעולה הבאה:

$$\begin{pmatrix} \bar{1} & \bar{1} & \bar{1} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{2} & \bar{1} \end{pmatrix} \xrightarrow{R_3 \to \bar{2}R_3} \begin{pmatrix} \bar{1} & \bar{1} & \bar{1} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} & \bar{2} \end{pmatrix}$$

עכשיו נאפס כל איבר מעל ה $ar{1}$  המוביל בעזרת הפעולות הבאות:

$$\begin{pmatrix}
\bar{1} & \bar{1} & \bar{1} & | \bar{0} \\
\bar{0} & \bar{1} & \bar{1} & | \bar{0} \\
\bar{0} & \bar{0} & \bar{1} & | \bar{2}
\end{pmatrix}
\xrightarrow{R_2 \to R_2 - R_3}
\begin{pmatrix}
\bar{1} & \bar{1} & \bar{1} & | \bar{0} \\
\bar{0} & \bar{1} & \bar{0} & | -\bar{2} \\
\bar{0} & \bar{0} & \bar{1} & | \bar{2}
\end{pmatrix}
=
\begin{pmatrix}
\bar{1} & \bar{1} & \bar{1} & | \bar{0} \\
\bar{0} & \bar{1} & \bar{0} & | \bar{1} \\
\bar{0} & \bar{0} & \bar{1} & | \bar{2}
\end{pmatrix}$$

$$\xrightarrow{R_1 \to R_1 - R_2}
\begin{pmatrix}
\bar{1} & \bar{0} & \bar{1} & | -\bar{1} \\
\bar{0} & \bar{1} & \bar{0} & | \bar{1} \\
\bar{0} & \bar{0} & \bar{1} & | \bar{2}
\end{pmatrix}
=
\begin{pmatrix}
\bar{1} & \bar{0} & \bar{1} & | \bar{2} \\
\bar{0} & \bar{1} & \bar{0} & | \bar{1} \\
\bar{0} & \bar{0} & \bar{1} & | \bar{2}
\end{pmatrix}$$

$$\xrightarrow{R_1 \to R_1 - R_3}
\begin{pmatrix}
\bar{1} & \bar{0} & \bar{0} & | \bar{0} \\
\bar{0} & \bar{1} & \bar{0} & | \bar{1} \\
\bar{0} & \bar{0} & \bar{1} & | \bar{2}
\end{pmatrix}$$

לכן למערכת יש פתרון יחיד:

$$(x_1, x_2, x_3) = (\bar{0}, \bar{1}, \bar{2})$$
.

#### דוגמה 2.28

 $\mathbb{Z}_5$  פתור את המערכת הבאה מעל

$$x_1 + x_2 + x_3 = \bar{0}$$
,  
 $x_1 - x_2 - x_3 = \bar{1}$ .

#### פתרון:

המטריצה המורחבת היא

$$\left(\begin{array}{cc|c} \bar{1} & \bar{1} & \bar{1} & \bar{0} \\ \bar{1} & -\bar{1} & -\bar{1} & \bar{1} \end{array}\right) = \left(\begin{array}{cc|c} \bar{1} & \bar{1} & \bar{1} & \bar{0} \\ \bar{1} & \bar{4} & \bar{4} & \bar{1} \end{array}\right) \ .$$

:שיטת גאוס

$$\left(\begin{array}{cc|c} \overline{1} & \overline{1} & \overline{1} & \overline{0} \\ \overline{1} & \overline{4} & \overline{4} & \overline{1} \end{array}\right) \xrightarrow{R_2 \to R_2 - R_1} \left(\begin{array}{cc|c} \overline{1} & \overline{1} & \overline{1} & \overline{0} \\ \overline{0} & \overline{3} & \overline{3} & \overline{1} \end{array}\right) .$$

נכפיל את השורה השלישית באיבר ההופכי של  $ar{3}$  ב-  $\mathbb{Z}_5$ . נגלה כי

$$\bar{3} \cdot \bar{2} = \bar{6} = \bar{1} \quad \Rightarrow \quad (\bar{3})^{-1} = \bar{2} \; ,$$

ולכן

$$\begin{pmatrix}
\bar{1} & \bar{1} & \bar{1} & \bar{0} \\
\bar{0} & \bar{3} & \bar{3} & \bar{1}
\end{pmatrix}
\xrightarrow{R_3 \to \bar{2} \cdot R_3}
\begin{pmatrix}
\bar{1} & \bar{1} & \bar{1} & \bar{0} \\
\bar{0} & \bar{1} & \bar{1} & \bar{2}
\end{pmatrix}$$

$$\xrightarrow{R_1 \to R_1 - R_2}
\begin{pmatrix}
\bar{1} & \bar{0} & \bar{0} & -\bar{2} \\
\bar{0} & \bar{1} & \bar{1} & \bar{2}
\end{pmatrix}
=
\begin{pmatrix}
\bar{1} & \bar{0} & \bar{0} & \bar{3} \\
\bar{0} & \bar{1} & \bar{1} & \bar{2}
\end{pmatrix}$$

המערכת המתאימה היא

$$x_1 = \bar{3} ,$$
  
$$x_2 + x_3 = \bar{2}$$

ולכן הפתרון הוא

$$x_1 = \bar{3} ,$$
  
$$x_2 = \bar{2} - x_3 .$$

כלומר,

$$(x_1, x_2, x_3) = (\bar{3}, \bar{2} - x_3, x_3), \quad x_3 \in \mathbb{Z}_5$$

נשים לב שלמערכת יש חמישה פתרונות:

$$x_3 = \bar{0} \Rightarrow (\bar{3}, \bar{2}, \bar{0})$$
 :1 פתרון  $x_3 = \bar{1} \Rightarrow (\bar{3}, \bar{1}, \bar{1})$  :2 פתרון  $x_3 = \bar{2} \Rightarrow (\bar{3}, \bar{0}, \bar{2})$  :3 פתרון  $x_3 = \bar{3} \Rightarrow (\bar{3}, -\bar{1}, \bar{3}) = (\bar{3}, \bar{4}, \bar{3})$  :4 פתרון  $x_3 = \bar{4} \Rightarrow (\bar{3}, -\bar{2}, \bar{4}) = (\bar{3}, \bar{3}, \bar{3})$  :5 פתרון :5

#### דוגמה 2.29

 $\mathbb{Z}_7$  פתור את המערכת הבאה מעל

$$x_1 + \bar{2}x_2 + \bar{4}x_3 = \bar{0} ,$$
  
$$\bar{2}x_1 - \bar{3}x_2 + x_3 = \bar{0} .$$

## פתרון:

$$\begin{pmatrix}
\bar{1} & \bar{2} & \bar{4} & \bar{0} \\
\bar{2} & -\bar{3} & \bar{1} & \bar{0}
\end{pmatrix} = \begin{pmatrix}
\bar{1} & \bar{2} & \bar{4} & \bar{0} \\
\bar{2} & \bar{4} & \bar{1} & \bar{0}
\end{pmatrix} \xrightarrow{R_2 \to R_2 - \bar{2} \cdot R_1} \begin{pmatrix}
\bar{1} & \bar{2} & \bar{4} & \bar{0} \\
\bar{0} & \bar{0} & -\bar{7} & \bar{0}
\end{pmatrix} = \begin{pmatrix}
\bar{1} & \bar{2} & \bar{4} & \bar{0} \\
\bar{0} & \bar{0} & \bar{0} & \bar{0}
\end{pmatrix}$$

המערכת המתאימה הינה

$$x_1 + \bar{2}x_2 + \bar{4}x_3 = \bar{0}$$
,  $x_2, x_3 \in \mathbb{Z}_7$ 

והפתרון הוא

$$x_1 = -\bar{2}x_2 - \bar{4}x_3 = \bar{5}x_2 + \bar{3}x_3$$
,  $x_2, x_3 \in \mathbb{Z}_7$ .

כלומר

$$(x_1, x_2, x_3) = (\bar{5}x_2 + \bar{3}x_3, x_2, x_3), \qquad x_2, x_3 \in \mathbb{Z}_7.$$

. נשים לב שלמערכת יש  $7^2 = 49$  פתרונות

#### דוגמה 2.30

תנו דוגמה למערכת לינארית בעלת 27 פתרונות.

מערכת : 1 המערכת

$$\bar{0}x = \bar{0}$$
.

 $\mathbb{Z}_{27}$  מעל

. מהווה פתרון של משוואה אחת במשתנה אחד, וכל איבר של מערכת של משוואה אחת הסבר:  $\underline{\mathbb{Z}_{27}}$ 

#### : 2 מערכת

$$x + y + z + w = \bar{0}$$

 $\mathbb{Z}_3$  מעל

 $3^3$  ולכן הסבר: זוהי מערכת של משוואה אחת בארבעה משתנים. למערכת יש שלושה משתני חופשיים ולכן פתרונות.

## דוגמה 2.31

 $\mathbb{Z}_5$  פתרו את המערכת הבאה מעל

$$\begin{aligned} x + \bar{3}y + \bar{2}z &= \bar{1} \ , \\ \bar{2}x + \bar{4}y + z &= \bar{3} \ , \\ \bar{3}x + \bar{3}z &= \bar{2} \ . \end{aligned}$$

### פתרון:

$$\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{2} & \bar{4} & \bar{1} & | & \bar{3} \\
\bar{3} & \bar{0} & \bar{3} & | & \bar{2}
\end{pmatrix}
\quad
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & -\bar{2} & -\bar{3} & | & \bar{1} \\
\bar{0} & -\bar{9} & -\bar{3} & | & -\bar{1}
\end{pmatrix}
=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{2} & | & \bar{4}
\end{pmatrix}$$

$$\xrightarrow{R_2 \to \bar{3}^{-1}R_2 = \bar{2}R_2}
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{4} & | & \bar{2} \\
\bar{0} & \bar{1} & \bar{4} & | & \bar{2}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{4} & | & \bar{2} \\
\bar{0} & \bar{1} & \bar{4} & | & \bar{2}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{4} & | & \bar{2} \\
\bar{0} & \bar{0} & \bar{3} & | & \bar{2}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{4} & | & \bar{2} \\
\bar{0} & \bar{0} & \bar{3} & | & \bar{2}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{4} & | & \bar{2} \\
\bar{0} & \bar{0} & \bar{3} & | & \bar{2}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{4} & | & \bar{2} \\
\bar{0} & \bar{0} & \bar{1} & | & \bar{4}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{4} & | & \bar{2} \\
\bar{0} & \bar{0} & \bar{1} & | & \bar{4}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{4} & | & \bar{2} \\
\bar{0} & \bar{0} & \bar{1} & | & \bar{4}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{4} & | & \bar{2} \\
\bar{0} & \bar{0} & \bar{1} & | & \bar{4}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{4} & | & \bar{2} \\
\bar{0} & \bar{0} & \bar{1} & | & \bar{4}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{4} & | & \bar{2} \\
\bar{0} & \bar{0} & \bar{1} & | & \bar{4}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{4} & | & \bar{2} \\
\bar{0} & \bar{0} & \bar{1} & | & \bar{4}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{1} & \bar{2} \\
\bar{0} & \bar{0} & \bar{1} & | & \bar{4}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{1} & \bar{2} \\
\bar{0} & \bar{0} & \bar{1} & | & \bar{4}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{1} & \bar{2} \\
\bar{0} & \bar{1} & \bar{1} & \bar{1}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{1} & \bar{1}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & | & \bar{1} \\
\bar{0} & \bar{1} & \bar{1} & \bar{1}
\end{pmatrix}$$

$$=
\begin{pmatrix}
\bar{1} & \bar{3} & \bar{2} & |$$

#### דוגמה 2.32

 $:\!\mathbb{Z}_5$  פתרו את המערכת הבאה מעל

$$x + \bar{4}y + z = \bar{1} ,$$
  
$$\bar{3}x + \bar{2}y + \bar{3}z = \bar{2} ,$$
  
$$\bar{4}x + y + \bar{4}z = \bar{3} .$$

$$\begin{pmatrix} \bar{1} & \bar{4} & \bar{1} & | & \bar{1} \\ \bar{3} & \bar{2} & \bar{3} & | & \bar{2} \\ \bar{4} & \bar{1} & \bar{4} & | & \bar{3} \end{pmatrix} \xrightarrow{R_2 \to R_2 - \bar{3}R_1 \atop R_3 \to R_3 - \bar{4}R_1} \begin{pmatrix} \bar{1} & \bar{4} & \bar{1} & | & \bar{1} \\ \bar{0} & -\bar{10} & \bar{0} & | & -\bar{1} \\ \bar{0} & -\bar{15} & \bar{0} & | & -\bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{4} & \bar{1} & | & \bar{1} \\ \bar{0} & \bar{0} & \bar{0} & | & \bar{4} \\ \bar{0} & \bar{0} & \bar{0} & | & \bar{4} \end{pmatrix}$$

קיבלנו שורת סתירה לכן למערכת אין פתרון.

#### דוגמה 2.33

 $\mathbb{Z}_5$  פתרו את המערכת הבאה מעל

$$\begin{split} \bar{2}x + \bar{3}y + \bar{4}z = &\bar{1} \ , \\ x + \bar{2}y + \bar{3}z = &\bar{0} \ , \\ \bar{3}x + \bar{2}z = &\bar{1} \ . \end{split}$$

#### פתרון:

$$\begin{pmatrix} \bar{2} & \bar{3} & \bar{4} & | & \bar{1} \\ \bar{1} & \bar{2} & \bar{3} & | & \bar{0} \\ \bar{3} & \bar{0} & \bar{2} & | & \bar{1} \end{pmatrix} \qquad \frac{R_1 \leftrightarrow R_2}{2} \qquad \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & | & \bar{0} \\ \bar{2} & \bar{3} & \bar{4} & | & \bar{1} \\ \bar{3} & \bar{0} & \bar{2} & | & \bar{1} \end{pmatrix} \qquad \frac{R_2 \to R_2 - \bar{2} \cdot R_1}{2} \qquad \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & | & \bar{0} \\ \bar{0} & -\bar{1} & -\bar{2} & | & \bar{1} \\ \bar{0} & -\bar{6} & -\bar{7} & | & \bar{1} \end{pmatrix} \qquad = \qquad \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & | & \bar{0} \\ \bar{0} & \bar{4} & \bar{3} & | & \bar{1} \\ \bar{0} & \bar{4} & \bar{3} & | & \bar{1} \end{pmatrix}$$

$$\xrightarrow{R_3 \to R_3 - R_2} \qquad \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & | & \bar{0} \\ \bar{0} & \bar{4} & \bar{3} & | & \bar{1} \\ \bar{0} & \bar{0} & \bar{0} & | & \bar{0} \end{pmatrix} \qquad \xrightarrow{R_2 \to \bar{4}^{-1}R_2} \qquad \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & | & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} & \bar{2} & | & \bar{4} \\ \bar{0} & \bar{0} & \bar{0} & | & \bar{0} \end{pmatrix} \qquad = \qquad \begin{pmatrix} \bar{1} & \bar{2} & \bar{3} & | & \bar{0} \\ \bar{0} & \bar{1} & \bar{2} & | & \bar{4} \\ \bar{0} & \bar{0} & \bar{0} & | & \bar{0} \end{pmatrix}$$

$$\xrightarrow{R_1 \to R_1 - \bar{2}R_2} \qquad \begin{pmatrix} \bar{1} & \bar{0} & -\bar{1} & | -\bar{8} \\ \bar{0} & \bar{1} & \bar{2} & | & \bar{4} \\ \bar{0} & \bar{0} & \bar{0} & | & \bar{0} \end{pmatrix} \qquad = \qquad \begin{pmatrix} \bar{1} & \bar{0} & \bar{4} & | & \bar{2} \\ \bar{0} & \bar{1} & \bar{2} & | & \bar{4} \\ \bar{0} & \bar{0} & \bar{0} & | & \bar{0} \end{pmatrix}$$

$$\Rightarrow \qquad x = -\bar{4}z + \bar{2} = z + \bar{2} \\ y = -\bar{2}z + \bar{4} = \bar{3}z + \bar{4} \end{pmatrix}$$

$$(x, y, z) = (z + \bar{2}, \bar{4} + \bar{3}z, z) \qquad , z \in \mathbb{Z}_5 .$$

ישנם 5 פתרונות.