שיעור 2
שדות

2.1 מספרים מרוכבים

"

הגדרה 2.1 מספר מרוכב

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

אם $y=0$ נקבל זוג $(x,0)$. נסמן $x=(x,0)$. נגדיר את הפעולות הבאות בין מספרים מרוכבים:

הגדרה 2.2 פעולות בינאריות של מספרים מרוכבים

נניח $z_1=(x_1,y_1)$, $z_2=(x_2,y_2)$. אז

1) <u>**חיבור**</u>

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

2) <u>**כפל**</u>

$$z_1\cdot z_2=(x_1x_2-y_1y_2,x_1y_2+x_2y_1)$$

קל לראות:

1) לכל מספר ממשי $x=(x,0)$ ולכל מספר מרוכב $z_1=(x_1,y_1)$ מתקיים

$$x\cdot z_1=(x\cdot x_1,x\cdot y_1)$$

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

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

הגדרה 2.3 i

נסמן

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

i היא

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

משפט 2.1 הצגה אלגברית שך מספר מרוכב

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

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

$x+iy$ נקרא הצגה אלגברית של מספר מרוכב.

ל- x קוראים החלק הממשי של z. מסמנים $x=\text{Re}(z)$.

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

צורת הכתיבה $x+iy$ מאפשרת לחבר ולהכפיל מספרים רוכבים בקלות בהתחשב ב- $i^2=-1$.

דוגמה 2.1

א

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

דוגמה 2.2

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

הגדרה 2.4 הצמוד

המספר הרוכב $x-iy$ נקרא צוד למפר $z=x+iy$. מסנים:

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

משפט 2.2

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

המספר הזה נקרא ה **הערך המוחלט** או **הגודל** של המספר מספר המרוכב z.

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 המשוואה

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

פתרון:

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

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

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

אפשר לראות בקלות ש- $\mathbb{C}$ יחד עם שתי הפעולות שהגדרנו בהגדרה 2.7 מקיימת את כל האקסיומות של שדה, כאשר

$$0=(0,0)$$
$$1=(1,0)$$

ועבור $z=x+iy\neq 0$,

$$z^{-1}=\frac{1}{x+iy}=\frac{x-iy}{x^2+y^2}=\frac{x}{x^2+y^2}-i\cdot\frac{y}{x^2+y^2}\ .$$

2.2 מערכות ליניאריות מעל $\mathbb{C}$

דוגמה 2.5

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

פתרון:

$$\left(\begin{array}{cc|c}1+i&1-i&3i\\3&2-i&4\end{array}\right)\xrightarrow{R_1\to(1-i)R_1}\left(\begin{array}{cc|c}2&-2i&3+3i\\3&2-i&4\end{array}\right)\xrightarrow{R_2\to 2R_2-3R_1}\left(\begin{array}{cc|c}2&-2i&3+3i\\0&4+4i&-1-9i\end{array}\right)$$

$$\xrightarrow{R_2\to(4-4i)R_2}\left(\begin{array}{cc|c}2&-2i&3+3i\\0&32&-40-32i\end{array}\right)\xrightarrow{R_1\to 16R_1+iR_2}\left(\begin{array}{cc|c}32&0&80+8i\\0&32&-40-32i\end{array}\right)$$

$$\xrightarrow{R_1\to\frac{1}{32}R_1}\left(\begin{array}{cc|c}1&0&\frac{5}{2}+\frac{1}{4}i\\0&1&-\frac{5}{4}-i\end{array}\right)$$

פתרון:

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

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

הגדרה 2.5 פונקציית שארית

עבור מספרים שלמים k,p הפונקצית השארית $\mathrm{rem}(k,p)$ מוגדרת להיות השארית של k בחילוק ב- p.

דוגמה 2.6

- השארית של 3 בחילוק ב- 2 היא 1. לכן

$$\text{rem}(3,2) = 1 \ .$$

- השארית של 7 בחילוק ב- 4 היא 3. לכן

$$\text{rem}(7,4) = 3 \ .$$

- השארית של 11 בחילוק ב- 8 היא 3. לכן

$$\text{rem}(11,8) = 3 \ .$$

הגדרה 2.6 $\mathbb{Z}_p$ - קבוצת השארית בחלוקה ב-p

נניח ש p מספר ראשוני. הקבוצה $\mathbb{Z}_p$ היא קבוצת הסימנים

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

הקבוצה מוגדרת לפי התנאים הבאים:

(1) כל איבר הוא מספר שלם וחיובי.

(2) מספרים עם אותה השאריות בחילוק ב- p שווים זה לזה.

(3) לכל מספר שלם k נתאים איבר ב- $\mathbb{Z}_p$ שנסמן $\bar{k}$ ונגדיר

$$\bar{k} = \overline{\text{rem}(k,p)} \ .$$

דוגמה 2.7

לקבוצה $\mathbb{Z}_3$ יש 3 איברים:

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

$$
\begin{aligned}
\bar{0} &= \overline{\text{rem}(0,3)} &&= \bar{0}\\
\bar{1} &= \overline{\text{rem}(1,3)} &&= \bar{1}\\
\bar{2} &= \overline{\text{rem}(2,3)} &&= \bar{2}\\
\\
\bar{3} &= \overline{\text{rem}(3,3)} &&= \bar{0}\\
\bar{4} &= \overline{\text{rem}(4,3)} &&= \bar{1}\\
\bar{5} &= \overline{\text{rem}(5,3)} &&= \bar{2}\\
\\
\bar{6} &= \overline{\text{rem}(6,3)} &&= \bar{0}\\
\bar{7} &= \overline{\text{rem}(7,3)} &&= \bar{1}\\
\bar{8} &= \overline{\text{rem}(8,3)} &&= \bar{2}\\
&\vdots\\
\overline{122} &= \overline{\text{rem}(122,3)} &&= \bar{2}\\
&\vdots
\end{aligned}
$$

ובן הלאה.

הגדרה 2.7　פעולות בינאריות של $\mathbb{Z}_p$ איברי

יהי $p\in\mathbb{N}$ מספר ראשוני ותהי $\mathbb{Z}_p=\{\bar{0},\bar{1},\ldots,\overline{p-1}\}$, קבוצת השאריות בחלוקה ב- p. לכל $\bar{a},\bar{b}\in\mathbb{Z}_p$ נגדיר את הפעולות חיבור וכפל כך:

1) <u>חיבור</u>

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

2) <u>כפל</u>

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

דוגמה 2.8

חשבו ב- $\mathbb{Z}_5$ את

א) $\bar{2}+\bar{4}$.

ב) $\bar{3}\cdot\bar{3}$.

פתרון:

א) $\bar{2}+\bar{4}=\overline{2+4}=\bar{6}=\bar{1}$.

ב) $\bar{3}\cdot\bar{3}=\overline{3\cdot 3}=\bar{9}=\bar{4}$.

דוגמה 2.9

חשבו ב- $\mathbb{Z}_{11}$ את

א) $\bar{3}\cdot\bar{7}$.

ב) $\bar{2}\cdot\bar{8}$.

פתרון:

א) $\bar{3}\cdot\bar{7}=\overline{3\cdot 7}=\overline{21}=\overline{10}$.

ב) $\bar{2}\cdot\bar{8}=\overline{16}=\bar{5}$.

דוגמה 2.10

לוח החיבור של איברים ב- $\mathbb{Z}_3$:

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

לוח הכפל של איברים ב- $\mathbb{Z}_3$:

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

דוגמה 2.11

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

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

לוח הכפל של איברים של $\mathbb{Z}_5$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

נחזור לממשיים. הנגדי של 7 הוא -7 כי $-7+7=0$.

ההופכי של 7 הוא 7^{-1}, (או $\frac{1}{7}$) כי $\frac{1}{7}\cdot 7=1$.

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

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

באופן דומה, $\bar{1}$ הוא הנגדי של $\bar{2}$. כלומר $-\bar{2}=\bar{1}$.

מתקיים $\bar{2}\cdot\bar{2}=\bar{1}$ ולכן $\bar{2}$ הוא ההופכי של $\bar{2}$. כלומר $(\bar{2})^{-1}=\bar{2}$.

משפט 2.3 איבר ההופכי ואיבר הנגדי בקבוצה $\mathbb{Z}_p$

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

א) <u>איבר הנגדי</u>

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

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

האיבר $-a$ נקרא האיבר הנגדי של a.

ב) <u>איבר ההופכי</u>

לכל איבר $a\in\mathbb{Z}_p$ שונה מאפס (כלומר $a\neq\bar{0}$) קיים איבר יחיד $a^{-1}\in\mathbb{Z}_p$ כך ש-

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

האיבר a^{-1} נקרא האיבר ההופכי של a.

דוגמה 2.12

מצאו את האיבר הנגדי של $\bar{1}$ ב- $\mathbb{Z}_3$.

פתרון:

נשים לב ש-

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

ולכן

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

דוגמה 2.13

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

פתרון:

נשים לב ש-

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

ולכן

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

דוגמה 2.14

מצאו את האיבר הנגדי של $\bar{3}$ ב- $\mathbb{Z}_3$.

פתרון:

נשים לב ש-

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

ולכן

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

דוגמה 2.15

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

$$\begin{aligned}
-\bar{1} &= \bar{2}\\
-\bar{2} &= \bar{1}\\
\\
-\bar{3} &= \bar{0}\\
-\bar{4} &= \bar{2}\\
-\bar{5} &= \bar{1}\\
\\
-\bar{6} &= \bar{0}\\
-\bar{7} &= \bar{2}\\
-\bar{8} &= \bar{1}\\
&\vdots\\
-\bar{5}9 &= \bar{1}\ .
\end{aligned}$$

דוגמה 2.16

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

פתרון:

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

לכן $\bar{2}^{-1}=\bar{2}$.

דוגמה 2.17

מצאו את האיבר ההופכי של $\bar{1}$ ב- $\mathbb{Z}_3$.

פתרון:

$$\bar{1}\cdot\bar{1}=\bar{1}$$

לכן $\bar{1}^{-1} = \bar{1}$.

דוגמה 2.18

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

פתרון:

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

לכן $\bar{3}^{-1} = \bar{2}$.

דוגמה 2.19

חשבו את האיבר ההופכי של כל האיברים הבאים ב- $\mathbb{Z}_5$

(א) $\bar{1}$

(ב) $\bar{2}$

(ג) $\bar{3}$

(ד) $\bar{4}$

פתרון:

(א)

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

(ב)

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

(ג)

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

(ד)

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

דוגמה 2.20

חשבו ב- $\mathbb{Z}_{11}$:

(א) $\bar{3} \cdot \bar{7}$

(ב) $\bar{2} \cdot \bar{8}$

(ג) $-\bar{3}$

(ד) $(\bar{3})^{-1}$

פתרון:

(א) $\bar{3}\cdot\bar{7}=\overline{21}=\overline{10}$

(ב) $\bar{2}\cdot\bar{8}=\overline{16}=\bar{5}$

(ג) . $-\bar{3}=\bar{8} \quad \Rightarrow \quad \bar{3}+\bar{8}=\overline{11}=\bar{0}$

(ד) . $(\bar{3})^{-1}=\bar{4} \quad \Rightarrow \quad \bar{3}\cdot\bar{4}=\overline{12}=\bar{1}$

משפט 2.4

עבור $p\in\mathbb{N}$ ראשוני, לכל איבר השונה מאפס בקבוצה $\mathbb{Z}_p=\{\bar{0},\bar{1},\cdots\overline{p-1}\}$ יש הופכי.

2.4 מערכות ליניאריות מעל $\mathbb{Z}_p$

דוגמה 2.21

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

$$\begin{aligned}x_1+x_2+x_3&=\bar{0}\\x_1-x_2-x_3&=\bar{0}\\x_1+\bar{2}x_2+x_3&=\bar{1}\end{aligned}$$

פתרון:

המטריצה המורחבת היא

$$\left(\begin{array}{ccc|c}\bar{1}&\bar{1}&\bar{1}&\bar{0}\\\bar{1}&-\bar{1}&-\bar{1}&\bar{0}\\\bar{1}&\bar{2}&\bar{1}&\bar{1}\end{array}\right)=\left(\begin{array}{ccc|c}\bar{1}&\bar{1}&\bar{1}&\bar{0}\\\bar{1}&\bar{2}&\bar{2}&\bar{0}\\\bar{1}&\bar{2}&\bar{1}&\bar{1}\end{array}\right)$$

נבצע שיטת גאוס:

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

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

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

נכפיל את השורה השלישית ב $\bar{2}$ מכיוון ש $\bar{2}^{-1}=\bar{2}$: לכן נבצע את הפעולה הבאה:

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

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

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

לכן למערכת יש פתרון יחיד:
$$(x_1,x_2,x_3)=(\bar{0},\bar{1},\bar{2}) \ .$$

דוגמה 2.22

פתור את המערכת הבאה מעל $\mathbb{Z}_5$:
$$\begin{aligned} x_1+x_2+x_3 =& \bar{0} \ , \\ x_1-x_2-x_3 =& \bar{1} \ . \end{aligned}$$

פתרון:

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

שיטת גאוס:
$$\left(\begin{array}{ccc|c} \bar{1} & \bar{1} & \bar{1} & \bar{0} \\ \bar{1} & \bar{4} & \bar{4} & \bar{1} \end{array}\right) \xrightarrow{R_2\to R_2-R_1} \left(\begin{array}{ccc|c} \bar{1} & \bar{1} & \bar{1} & \bar{0} \\ \bar{0} & \bar{3} & \bar{3} & \bar{1} \end{array}\right) \ .$$

נכפיל את השורה השלישית באיבר ההופכי של $\bar{3}$ ב- $\mathbb{Z}_5$. נגלה כי
$$\bar{3}\cdot\bar{2}=\bar{6}=\bar{1} \quad \Rightarrow \quad (\bar{3})^{-1}=\bar{2} \ ,$$

ולכן
$$\left(\begin{array}{ccc|c} \bar{1} & \bar{1} & \bar{1} & \bar{0} \\ \bar{0} & \bar{3} & \bar{3} & \bar{1} \end{array}\right) \xrightarrow{R_3\to \bar{2}\cdot R_3} \left(\begin{array}{ccc|c} \bar{1} & \bar{1} & \bar{1} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} & \bar{2} \end{array}\right)$$
$$\xrightarrow{R_1\to R_1-R_2} \left(\begin{array}{ccc|c} \bar{1} & \bar{0} & \bar{0} & -\bar{2} \\ \bar{0} & \bar{1} & \bar{1} & \bar{2} \end{array}\right) = \left(\begin{array}{ccc|c} \bar{1} & \bar{0} & \bar{0} & \bar{3} \\ \bar{0} & \bar{1} & \bar{1} & \bar{2} \end{array}\right) \ .$$

המערכת המתאימה היא
$$\begin{aligned} x_1 =& \bar{3} \ , \\ x_2+x_3 =& \bar{2} \end{aligned}$$

ולכן הפתרון הוא
$$\begin{aligned} x_1 =& \bar{3} \ , \\ x_2 =& \bar{2}-x_3 \ . \end{aligned}$$

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

נשים לב שלמערכת יש חמישה פתרונות:

$$\begin{array}{lllll}
\text{פתרון 1:} & & (\bar{3},\bar{2},\bar{0}) & \Rightarrow & x_3=\bar{0} \\
\text{פתרון 2:} & & (\bar{3},\bar{1},\bar{1}) & \Rightarrow & x_3=\bar{1} \\
\text{פתרון 3:} & & (\bar{3},\bar{0},\bar{2}) & \Rightarrow & x_3=\bar{2} \\
\text{פתרון 4:} & (\bar{3},\bar{4},\bar{3}) = & (\bar{3},-\bar{1},\bar{3}) & \Rightarrow & x_3=\bar{3} \\
\text{פתרון 5:} & (\bar{3},\bar{3},\bar{3}) = & (\bar{3},-\bar{2},\bar{4}) & \Rightarrow & x_3=\bar{4}
\end{array}$$

דוגמה 2.23

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

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

פתרון:

$$\left(\begin{array}{ccc|c} \bar{1} & \bar{2} & \bar{4} & \bar{0} \\ \bar{2} & -\bar{3} & \bar{1} & \bar{0} \end{array}\right) = \left(\begin{array}{ccc|c} \bar{1} & \bar{2} & \bar{4} & \bar{0} \\ \bar{2} & \bar{4} & \bar{1} & \bar{0} \end{array}\right) \xrightarrow{R_2\to R_2-\bar{2}\cdot R_1} \left(\begin{array}{ccc|c} \bar{1} & \bar{2} & \bar{4} & \bar{0} \\ \bar{0} & \bar{0} & -\bar{7} & \bar{0} \end{array}\right) = \left(\begin{array}{ccc|c} \bar{1} & \bar{2} & \bar{4} & \bar{0} \\ \bar{0} & \bar{0} & \bar{0} & \bar{0} \end{array}\right)$$

המערכת המתאימה הינה

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

והפתרון הוא

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

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 2.24

תנו דוגמה למערכת לינארית בעלת 27 פתרונות.

פתרון:

מערכת 1 : המערכת

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

מעל $\mathbb{Z}_{27}$.

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

מערכת 2 :

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

מעל $\mathbb{Z}_3$.

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

דוגמה 2.25

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

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

פתרון:

$$\left(\begin{array}{ccc|c} \bar{1} & \bar{3} & \bar{2} & \bar{1} \\ \bar{2} & \bar{4} & \bar{1} & \bar{3} \\ \bar{3} & \bar{0} & \bar{3} & \bar{2} \end{array}\right) \xrightarrow[R_3\to R_3-\bar{3}\cdot R_1]{R_2\to \bar{R}_2-\bar{2}\cdot R_1} \left(\begin{array}{ccc|c} \bar{1} & \bar{3} & \bar{2} & \bar{1} \\ \bar{0} & -\bar{2} & -\bar{3} & \bar{1} \\ \bar{0} & -\bar{9} & -\bar{3} & -\bar{1} \end{array}\right) = \left(\begin{array}{ccc|c} \bar{1} & \bar{3} & \bar{2} & \bar{1} \\ \bar{0} & \bar{3} & \bar{2} & \bar{1} \\ \bar{0} & \bar{1} & \bar{2} & \bar{4} \end{array}\right)$$

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

$$= \left(\begin{array}{ccc|c} \bar{1} & \bar{3} & \bar{2} & \bar{1} \\ \bar{0} & \bar{1} & \bar{4} & \bar{2} \\ \bar{0} & \bar{0} & \bar{3} & \bar{2} \end{array}\right) \xrightarrow{R_3\to \bar{3}^{-1}R_3=\bar{2}R_3} \left(\begin{array}{ccc|c} \bar{1} & \bar{3} & \bar{2} & \bar{1} \\ \bar{0} & \bar{1} & \bar{4} & \bar{2} \\ \bar{0} & \bar{0} & \bar{1} & \bar{4} \end{array}\right)$$

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

$$\xrightarrow{R_1\to R_1-\bar{3}R_2-\bar{2}R_3} \left(\begin{array}{ccc|c} \bar{1} & \bar{0} & \bar{0} & -\overline{10} \\ \bar{0} & \bar{1} & \bar{0} & \bar{1} \\ \bar{0} & \bar{0} & \bar{1} & \bar{4} \end{array}\right) = \left(\begin{array}{ccc|c} \bar{1} & \bar{0} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} & \bar{1} \\ \bar{0} & \bar{0} & \bar{1} & \bar{4} \end{array}\right)$$

לפיכך $(x_1,x_2,x_3)=(\bar{0},\bar{1},\bar{4})$.

דוגמה 2.26

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

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

פתרון:

$$\left(\begin{array}{ccc|c} \bar{1} & \bar{4} & \bar{1} & \bar{1} \\ \bar{3} & \bar{2} & \bar{3} & \bar{2} \\ \bar{4} & \bar{1} & \bar{4} & \bar{3} \end{array}\right) \xrightarrow[R_3\to R_3-\bar{4}R_1]{R_2\to R_2-\bar{3}R_1} \left(\begin{array}{ccc|c} \bar{1} & \bar{4} & \bar{1} & \bar{1} \\ \bar{0} & -\overline{10} & \bar{0} & -\bar{1} \\ \bar{0} & -\overline{15} & \bar{0} & -\bar{1} \end{array}\right) = \left(\begin{array}{ccc|c} \bar{1} & \bar{4} & \bar{1} & \bar{1} \\ \bar{0} & \bar{0} & \bar{0} & \bar{4} \\ \bar{0} & \bar{0} & \bar{0} & \bar{4} \end{array}\right)$$

קיבלנו שורת סתירה לכן למערכת אין פתרון.

דוגמה 2.27

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

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

פתרון:

$$\left(\begin{array}{ccc|c} \bar{2} & \bar{3} & \bar{4} & \bar{1} \\ \bar{1} & \bar{2} & \bar{3} & \bar{0} \\ \bar{3} & \bar{0} & \bar{2} & \bar{1} \end{array}\right) \xrightarrow{R_1\leftrightarrow R_2} \left(\begin{array}{ccc|c} \bar{1} & \bar{2} & \bar{3} & \bar{0} \\ \bar{2} & \bar{3} & \bar{4} & \bar{1} \\ \bar{3} & \bar{0} & \bar{2} & \bar{1} \end{array}\right) \xrightarrow[R_3\to R_3-\bar{3}\cdot R_1]{R_2\to R_2-\bar{2}\cdot R_1} \left(\begin{array}{ccc|c} \bar{1} & \bar{2} & \bar{3} & \bar{0} \\ \bar{0} & -\bar{1} & -\bar{2} & \bar{1} \\ \bar{0} & -\bar{6} & -\bar{7} & \bar{1} \end{array}\right) = \left(\begin{array}{ccc|c} \bar{1} & \bar{2} & \bar{3} & \bar{0} \\ \bar{0} & \bar{4} & \bar{3} & \bar{1} \\ \bar{0} & \bar{4} & \bar{3} & \bar{1} \end{array}\right)$$

$$\xrightarrow{R_3\to R_3-R_2} \left(\begin{array}{ccc|c} \bar{1} & \bar{2} & \bar{3} & \bar{0} \\ \bar{0} & \bar{4} & \bar{3} & \bar{1} \\ \bar{0} & \bar{0} & \bar{0} & \bar{0} \end{array}\right) \xrightarrow[=\bar{4}\cdot R_2]{R_2\to\bar{4}^{-1}R_2} \left(\begin{array}{ccc|c} \bar{1} & \bar{2} & \bar{3} & \bar{0} \\ \bar{0} & \bar{1} & \overline{12} & \bar{4} \\ \bar{0} & \bar{0} & \bar{0} & \bar{0} \end{array}\right) = \left(\begin{array}{ccc|c} \bar{1} & \bar{2} & \bar{3} & \bar{0} \\ \bar{0} & \bar{1} & \bar{2} & \bar{4} \\ \bar{0} & \bar{0} & \bar{0} & \bar{0} \end{array}\right)$$

$$\xrightarrow{R_1\to R_1-\bar{2}R_2} \left(\begin{array}{ccc|c} \bar{1} & \bar{0} & -\bar{1} & -\bar{8} \\ \bar{0} & \bar{1} & \bar{2} & \bar{4} \\ \bar{0} & \bar{0} & \bar{0} & \bar{0} \end{array}\right) = \left(\begin{array}{ccc|c} \bar{1} & \bar{0} & \bar{4} & \bar{2} \\ \bar{0} & \bar{1} & \bar{2} & \bar{4} \\ \bar{0} & \bar{0} & \bar{0} & \bar{0} \end{array}\right)$$

$$\Rightarrow \left.\begin{array}{ccc} x &= -\bar{4}z+\bar{2} &= z+\bar{2} \\ y &= -\bar{2}z+\bar{4} &= \bar{3}z+\bar{4} \end{array}\right\}$$

תשובה סופית:

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

ישנם 5 פתרונות.

2.5 שדות

הגדרה 2.8 שדה

קבוצה לא ריקה $\mathbb{F}$, שבה פעולת חיבור "$+$" ופעולת כפל "$\cdot$" (הפעולות הדו-מקומיות) מוגדרות על הקבוצה, נקראת שדה אם התנאים הבאים מתקיימים. לכל איבר $a\in\mathbb{F}$ ולכל איבר $b\in\mathbb{F}$ ולכל איבר $c\in\mathbb{F}$:

(1 $\mathbb{F}$ סגורה תחת חיבור:

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

(2 $\mathbb{F}$ סגורה תחת כפל:

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

(3 חוק החילוף I:

$$a+b=b+a$$

4) חוק החילוף II:

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

5) חוק הקיבוץ I:

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

6) חוק הקיבוץ II:

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

7) חוק הפילוג:

$$a\cdot(b+c) = a\cdot b + a\cdot c \ .$$

8) קיום איבר ניוטרלי:

קיים איבר $0 \in \mathbb{F}$ כך ש-

$$a+0 = a \ .$$

9) קיום איבר יחיד (האיבר ניוטרל לגבי כפל):

קיים איבר $1 \in \mathbb{F}$ כך ש-

$$a\cdot 1 = a \ , \qquad \text{ו} \qquad 1\cdot a = a \ .$$

10) קיום איבר נגדי:

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

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

11) קיום איבר הופכי:

לכל $a \in \mathbb{F}$ כך ש $a \neq 0$ קיים איבר $a^{-1} \in \mathbb{F}$ המקיים

$$a\cdot a^{-1} = 1 \ , \qquad \text{ו} \qquad a^{-1}\cdot a = 1 \ .$$

משפט 2.5

יהי $\mathbb{F}$ שדה.

1) עבור $a \in \mathbb{F}$, האיבר הנגדי החיבורי $-a$ הוא יחיד.

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

דוגמה 2.28

א) הקבוצה $\mathbb{R}$ של מספרים ממשיים שדה.

ב) הקבוצה $\mathbb{C}$ של מספרים מרובכים שדה.

דוגמה 2.29

קבעו אם הקבוצה $\mathbb{N}$ שדה.

פתרון:

$\mathbb{N}$ לא שדה. כדי להראות זאת די למצוא דוגמה נגדית לאחת התכונות.:
נבחור $a = 3 \in \mathbb{N}$. לא קיים איבר נגדי שב- $\mathbb{N}$. הרי

$$-3 + 3 = 0$$

אבל $-3 \notin \mathbb{N}$.

משפט 2.6

יהי $\mathbb{F}$ שדה יהיו $a, b \in \mathbb{F}$, יהי 0 האיבר הניוטרלי הכפלי ו- -1 האיבר הנגדי לאיבר הניוטרלי החיבורי.

1) $a \cdot 0 = 0$

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

3) אם $a \cdot b = 0$ ו- $a \neq 0$ אז $b = 0$.

הוכחה: תרגיל בית! ■