שיעור 2
שדות

קבוצות מספרים וסימוליהן

המספרים הטבעיים	$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$
המספרים השלמים	$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$
המספרים הרציונלים	$\mathbb{Q} = \left\{\frac{m}{n} \middle| m, n \in \mathbb{Z}, n \neq 0\right\}$
המספרים הממשיים	$\mathbb{R}$

מספרים מרוכבים

2.1 הגדרה: (מספר מרוכב)
מספר מרוכב הינו זוג (a, b) של מספרים ממשיים. נסמן ב- $\mathbb{C}$ את קבוצת המספרים המרוכבים:

$$\mathbb{C} = \mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{ \text{זוגות סדורים של מספרים ממשיים} \}$$

נגדיר פעולות חיבור וכפל על הקבוצה $\mathbb{C}$.

<u>חיבור</u>:

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

<u>כפל</u>:

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1)$$

שימו לב, כי שני מספרים מרוכבים $z_1 = (a_1, b_1)$ ו- $z_2 = (a_2, b_2)$ הם שווים אם"ם $a_1 = a_2$ ו- $b_1 = b_2$. יהיו a_1 ו- a_2 מספרים ממשיים. אז

$$(a_1, 0) + (a_2, 0) = (a_1 + a_2, 0) \ , \qquad (a_1, 0) \cdot (a_2, 0) = (a_1 a_2, 0) \ .$$

ז"א שההתאמה $(a, 0) \mapsto a$ שומרת על פעולות החיבור והכפל. כמו כן לכל מספר מרוכב z מתקיים

$$z = z + (0, 0)$$

ו-

2.2 הגדרה: (i) המספר המרוכב $(0, 1)$ יסומן באות i.

התכונהה מיוחדת של המספר i היא

$$i^2 = i \cdot i = (0, 1) \cdot (0, 1) = (0.0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0) = -1 \ .$$

כפי שנהוג עבור מספרים ממשיים גם כאן המוסכמה היא שפעולת הכפל קודמת לחיבור, ולכן ניתן להשמיט סוגריים לפעמים. למשל

$$z_1 + z_2 \cdot z_3 := z_1 + (z_2 \cdot z_3) \ .$$

חישוב קצר עבור $a, b \in \mathbb{R}$ מראה ש-

$$a + b \cdot i = (a,0) + (b,0) \cdot (0,1) = (a,0) + (b \cdot 0 - 0 \cdot 1, b \cdot 1 + 0 \cdot 0) = (a,0) + (0,b) = (a,b) \ .$$

לכן נהוג לכתוב מספר מרוכב $z = (a,b) \in \mathbb{C}$ בצורה $z = a + bi$. בסימון זה פעולות החשבון הן

$$\begin{aligned}(a_1 + b_1 i) + (a_2 + b_2 i) &= (a_1 + a_2) + (b_1 + b_2) i \ , \\ (a_1 + b_1 i) \cdot (a_2 + b_2 i) &= (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i \ .\end{aligned}$$

עבור $a_1, b_1, a_2, b_2 \in \mathbb{R}$.

2.3 הגדרה: (ההופכי החיבורי המספר הנגדי)
יהי $z = a + ib$ מספר מרוכב. **המספר הנגדי** של z הוא המספר המרוכב היחיד w כך ש־

$$z + w = 0 \ .$$

המספר הנגדי יסומן ב $-z$ וניתן ע"י

$$-z = -a + (-b) i \ .$$

2.4 הגדרה: (המספר ההופכי הכפלי)
יהי $z = a + ib$ מספר מרוכב. **המספר ההופכי** של z הוא המספר המרוכב היחיד w כך ש־

$$z \cdot w = 1 \ ,$$

והוא יסומן ב- z^{-1} וניתן ע"י

$$z^{-1} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} \ .$$

דוגמא.
ההפכי הכפלי של $2 + i$ הוא $\frac{2}{5} + \frac{-1}{5} \cdot i$

דוגמא.
ההפכי הכפלי של i הוא $-i$.

כנהוג ,לעתים נשמיט את סימן הכפל, ונרשום $z_1 z_2$ במקום $z_1 \cdot z_2$. בשל תכונות האסוציאטיביות מותר במקרים מסוימים להשמיט סוגריים, למשל

$$z_1 z_2 z_2 := (z_1 \cdot z_2) \cdot z_3 = z_1 \cdot (z_2 \cdot z_3)$$

עוד סימונים נוחים הם

$$\frac{z_1}{z_2} := z_1 \cdot z_2^{-1}$$

ו-

$$z_1 - z_2 := z_1 + (-z_2) \ .$$

בהנתן מספר ממשי אי־שלילי a נסמן ב־ $\sqrt{a} = a^{1/2}$ את השורש הריבועי האי־שלילי של a.

2.5 הגדרה: (הצמוד)
הצמוד ל המספר המרוכב $z=a+bi$ הוא המספר המרוכב

$$\bar{z}:=a-bi\ .$$

2.6 הגדרה: (הערך המוחלט)
הערך המוחלט של $z=a+bi$ הוא המספר הממשי

$$|z|:=\sqrt{a^2+b^2}\ .$$

שימו לב $a^2+b^2\geq 0$ ולכן $|z|$ מוגדר ו- $|z|\geq 0$.

2.7 משפט. (הצמוד)
יהי z מספר מרוכב.

1) $z=0 \quad \Leftrightarrow \quad |z|=0$.

2) $|z|=\sqrt{\bar{z}z}$.

3) אם $z\neq 0$ הרי $\dfrac{1}{z}=\dfrac{\bar{z}}{|z|^2}$

2.8 משפט. (הצמוד)
יהיו z, z_1, z_2 מספרים מרוכבים.

1) $\overline{z_1+z_2}=\bar{z}_1+\bar{z}_2$.

2) $\overline{z_1z_2}=\bar{z}_1\cdot\bar{z}_2$.

3) $\bar{\bar{z}}=z$.

4) $z=\bar{z}$ אם ורק אם $z\in\mathbb{R}$.

5) אם $z=bi$ כאשר $b\in\mathbb{R}$, אז $\bar{z}=-z$.

לשם מה יש לנו צורך במספרים מרוכבים? נתבונן במשוואה

$$x^2+2=0\ .$$

אין לה פתרון ב- $\mathbb{R}$. אולם אם נעבור למשוואה השקולה $x^2=-2$ רואים שיש פתרונות מרוכבים $x:=\sqrt{2}\cdot i$ ו- $x:=-\sqrt{2}\cdot i$. בדומה קל לראות שלכל משוואה ריבועית

$$Ax^2+Bx+C=0$$

עם מקדמים ממשיים יש פתרונות מרוכבים

$$x=\frac{-B\pm\sqrt{B^2-4AC}}{2A}\ .$$

מערכות ליניאריות מעל $\mathbb{C}$

דוגמא.

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

פיתרון.

$$\left(\begin{array}{cc|c} 1+i & 1-i & 3i \\ 3 & 2-i & 4 \end{array}\right) \xrightarrow{R_2\to 3R_1-(1+i)R_2} \left(\begin{array}{cc|c} 1+i & 1-i & 3i \\ 0 & -4i & -4+5i \end{array}\right)$$

$$-4iz_2=-4+5i \quad\Rightarrow\quad z_2=\frac{-4+5i}{-4i}=\frac{(-4+5i)4i}{(-4i)(4i)}=\frac{-16i-20}{16}=-\frac{5}{4}-i \ .$$

$$(1+i)z_1+(1-i)z_2=3i \ \Rightarrow\ (1+i)z_1+(1-i)\cdot\left(-\tfrac{5}{4}-i\right)=3i \ \Rightarrow\ (1+i)z_1+\left(-\tfrac{9}{4}+\tfrac{1}{4}\cdot i\right)=3i$$

$$\Rightarrow \qquad (1+i)z_1+=\tfrac{9}{4}+\tfrac{11}{4}\cdot i \qquad \Rightarrow \quad z_1=\frac{\frac{1}{4}+\frac{11}{4}\cdot i}{1+i}=\frac{5}{2}+\frac{1}{4}i \ .$$

■

קבוצת השאריות בחלוקה ב- p

2.1 הגדרה: (קבוצת השארית בחלוקה ב-p)

לכל מספר ראשוני p הקבוצה $\mathbb{Z}_p$ היא קבוצת הסימנים

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

פעולות החשבון מוגדרות כך: יהיו i ו־ j שני מספרים מבין $0,1,\ldots,p-1$. החיבור מוגדר ע"י

$$\bar{i}+\bar{j}:=\bar{k}$$

כאשר $\bar{k}$ היא השארית של $i+j$ אחרי חלוקה ב- p. הכפל מוגדר ע"י

$$\bar{i}\cdot\bar{j}:=\bar{l}$$

כאשר $\bar{l}$ היא השארית של $i\cdot j$ אחרי חלוקה ב- p. התכונות הבאות מגדירות את הקבוצה:

(א) כל איבר הוא מספר שלם וחיובי.

(ב) לכל איבר בהקבוצה יש שארית שונה עם חלוקה ב-p.

(ג) מספרים עם אותה השאריות שווים זה לזה.

(ד) לכל מספר שלם k נתאים איבר ב- $\mathbb{Z}_p$ שיסומן $\bar{k}$ ויוגדר

$$\bar{k}=\mod(k,p) \ .$$

דוגמא. $\mathbb{Z}_3$ (קבוצה השאריות בחלוקה ב-3)

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

יש לקבוצה $\mathbb{Z}_3$ התכונות הבאות:

(א) כל איבר הוא מספר שלם וחיובי.

(ב) לכל איבר בהקבוצה יש שארית שונה עם חלוקה ב-3.

(ג) מספרים עם אותה השאריות שווים זה לזה.

(ד) לכל מספר שלם k נתאים איבר ב- $\mathbb{Z}_3$ שיסומן $\bar{k}$ ויוגדר

$$\bar{k} = \mod(k,3) \ .$$

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

איברים בקבוצה $\mathbb{Z}_3$ המתאימים למספרים שלמים שליליים:

שימו לב,

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

בגלל ש

$$-1 = 3\cdot(-1) + 2 \ ,$$

ו

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

בגלל ש

$$-2 = 3\cdot(-1) + 1 \ ,$$

ו

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

בגלל ש

$$-3 = 3\cdot(-1) + 0 \ .$$

עוד דוגמאות:

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

עבור $\mathbb{Z}_3$ טבלאות החיבור והכפל נראות כך:

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

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

שימו לב, $\bar{1} = \bar{2} \cdot \bar{2}$, ולכן $\bar{2}^{-1} = \bar{2}$. כלומר $\bar{2}$ הוא המספר ההופכי של $\bar{2}$ ב- $\mathbb{Z}_3$.

בדומה $\bar{0} = \bar{1} + \bar{2}$ ולכן $\bar{1} = \overline{-2}$. כלומר $\bar{1}$ הוא המספר הנגדי של $\bar{2}$ ב- $\mathbb{Z}_3$.

2.2 הגדרה: חיבור וכפל של איברים של $\mathbb{Z}_p$:
יהי $p \in \mathbb{N}$ מספר ראשוני ותהי

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\} \ ,$$

קבוצת השאריות בחלוקה ב- n. לכל $\bar{a}, \bar{b} \in \mathbb{Z}_p$ נגדיר

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

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

דוגמא.
חשבו ב- $\mathbb{Z}_{11}$:

(א) $\bar{3} \cdot \bar{7}$

(ב) $\bar{2} \cdot \bar{8}$

(ג) $-\bar{3}$

(ד) $(\bar{3})^{-1}$

פיתרון.

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

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

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

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

■

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

מערכות ליניאריות מעל Z_p

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

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

פיתרון. המטריצה המורחבת היא

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

נבצע שיטת גאוס:

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

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

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

כדי להפוך האיבר המוביל בשורה השלישית ל $\bar{1}$ בהתאם עם שיטת גאוס אנחנו צריכים ההופכי של $\bar{2}$. מכיוון

$$\bar{2}\cdot\bar{2}=\bar{4}=\bar{1} \qquad\Rightarrow\qquad (\bar{2})^{-1}=\bar{2}\ .$$

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 ע"י הפעולות הבאות:

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

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

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

ולמערכת יש פתרון יחיד:

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

■

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

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

פיתרון. המטריצה המורחבת היא

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

שיטת גאוס:

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

כדי להפוך את ה $\bar{3}$ (האיבר המוביל) בשורה השנייה ל- $\bar{1}$, אנחנו צריכים לדעת מהי 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 סופי הוא

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

כלומר,

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

ושים לב שלמערכת יש חמישה פתרונות:

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

■

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

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

פיתרון.

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

לכן

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

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. ■

דוגמא. תנו דוגמה למערכת לינארית בעלת 27 פתרונות.

פיתרון.

מערכת 1 : המערכת

$$0x=0$$

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

■

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

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

פיתרון.

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

$$\left.\begin{aligned} x+\bar{3}y+\bar{2}z &=\bar{1}\\ \bar{3}y+\bar{2}z &=\bar{1}\\ z&=\bar{4} \end{aligned}\right\} \Rightarrow \left.\begin{aligned} x+\bar{3}y+\bar{2}\cdot\bar{4} &=\bar{1}\\ \bar{3}y+\bar{2}\cdot\bar{4} &=\bar{1}\\ z&=\bar{4} \end{aligned}\right\} \Rightarrow \left.\begin{aligned} x+\bar{3}y+\bar{3} &=\bar{1}\\ \bar{3}y+\bar{3} &=\bar{1}\\ z&=\bar{4} \end{aligned}\right\}$$

$$\Rightarrow \left.\begin{aligned} x+\bar{3}y &=\bar{1}-\bar{3}=-\bar{2}=\bar{3}\\ \bar{3}y &=\bar{1}-\bar{3}=-\bar{2}=\bar{3}\\ z&=\bar{4} \end{aligned}\right\} \Rightarrow \left.\begin{aligned} x+\bar{3}\cdot\bar{1} &=\bar{3}\\ y &=\bar{1}\\ z&=\bar{4} \end{aligned}\right\} \Rightarrow \left.\begin{aligned} x &=\bar{0}\\ y &=\bar{1}\\ z&=\bar{4} \end{aligned}\right\}$$

■

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

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

פיתרון.

$$\left(\begin{array}{ccc|c} \bar{1} & \bar{4} & \bar{1} & \bar{1}\\ \bar{3} & \bar{2} & \bar{3} & \bar{2}\\ \bar{4} & \bar{1} & \bar{4} & \bar{3} \end{array}\right) \xrightarrow[R_3\to\bar{R}_1+R_3]{R_2\to\bar{2}R_1+R_2} \left(\begin{array}{ccc|c} \bar{1} & \bar{4} & \bar{1} & \bar{1}\\ \bar{0} & \bar{0} & \bar{0} & \bar{4}\\ \bar{0} & \bar{0} & \bar{0} & \bar{4} \end{array}\right)$$

שורה סתירה: אין פתרון. ■

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

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

פיתרון.

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

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

$$\Rightarrow \qquad \left.\begin{aligned} \bar{2}x &= \bar{1}-\bar{4}z-\bar{3}y &&= \bar{1}+\bar{1}z+\bar{2}y \\ \bar{4}y &= \bar{1}-\bar{3}z &&= 1+\bar{2}z \end{aligned}\right\}$$

$$\Rightarrow \qquad \left.\begin{aligned} \bar{x} &= \bar{2}^{-1}\cdot\bar{1}+\bar{2}^{-1}\cdot\bar{1}z+\bar{2}^{-1}\cdot\bar{2}y &&= \bar{3}+\bar{3}z+y \\ y &= \bar{4}^{-1}+\bar{4}^{-1}\cdot\bar{2}z &&= \bar{4}+\bar{4}\cdot\bar{2}z &&= \bar{4}+\bar{3}z \end{aligned}\right\}$$

$$\Rightarrow \qquad \left. x = \bar{3}+\bar{3}z+\bar{4}+\bar{3}z = \bar{7}+\bar{6}z = \bar{2}+zy = \bar{4}+\bar{3}z \right\}$$

תשובה סופית:

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

ישנן 5 פתרונות. ■

שדות

2.4 הגדרה: (שדה)
קבוצה לא ריקה $\mathbb{F}$, שבה פעולת חיבור '$+$' ופעולת כפל '$\cdot$' (הפעולות הדו-מקומיות) מוגדרות על הקבוצה, ויש בקבוצה איבר האפס (0) ואיבר יחידה 1, נקראת שדה אם מתקיים התנאים הבאים:

1) לכל $a,b\in\mathbb{F}$ מוגדר

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

ז"א הקבוצה $\mathbb{F}$ סגורה לגבי החיבור.

2) לכל $a,b\in\mathbb{F}$ מתקיים

$$a+b=b+a$$

(חוק החילוף).

3) לכל $a,b\in\mathbb{F}$ מתקיים

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

(חוק הקיבוץ).

4) קיים איבר $0\in\mathbb{F}$ כך שלכל $a\in\mathbb{F}$

$$a+0=a\ ,$$

(קיום איבר ניוטרלי בחיבור).

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

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

(קיום איבר נגדי).

6) לכל $a,b\in\mathbb{F}$ מוגדר פעולת הכפל כך ש

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

(ז"א קבוצה $\mathbb{F}$ סגורה לגבי הכפל)

7) לכל $a,b\in\mathbb{F}$ מתקיים
$$a\cdot b=b\cdot a$$
(חוק החילוף).

8) לכל $a,b,c\in\mathbb{F}$ מתקיים
$$a\cdot(b\cdot c)=(a\cdot b)\cdot c$$
(חוק הקיבוץ)

9) קיים איבר $1\in\mathbb{F}$ כך שלכל $a\in\mathbb{F}$,
$$a\cdot 1=a\ , \qquad \text{ו} \qquad 1\cdot a=a$$
(קיום איבר ניוטרליי לגבי הכפל)

10) לכל $a\in\mathbb{F}$ כך ש $a\neq 0$ קיים איבר $a^{-1}\in\mathbb{F}$ המקיים
$$a\cdot a^{-1}=1\ , \qquad \text{ו} \qquad a^{-1}\cdot a=1\ .$$
(קיום איבר הופכי)

11) לכל $a,b,c\in\mathbb{F}$
$$a\cdot(b+c)=a\cdot b+a\cdot c$$
(חוק הפילוג).

2.5 משפט. ()
יהי $\mathbb{F}$ שדה.

1) האיבר הנדגי החיבורי בתכונה 5 הוא יחיד.
2) האיבר ההפכי הכפלי בתכונה 10 הוא יחיד.

דוגמא.
הקבוצות $\mathbb{Q}$, $\mathbb{R}$ ו- $\mathbb{C}$ עם פעולות החשבון הרגילות הן שדות.

דוגמא.
$\mathbb{N}$ איננה שדה. כדי להראות זאת די למצוא דוגמה נגדית לאחת התכונות. ניקחאת המספר הטבעי 3. לא קיים ל־ 3 הפכי חיבורי.

דוגמא.
$\mathbb{Z}$ איננה שדה. דוגמה נגדית לתכונה 10: לא קיים איבר הופכי למספר השלם . 3.

משפט. ()
יהי $\mathbb{F}$ שדה ו־ a, b איברים.

1) $a\cdot 0=0$
2) $a\cdot(-1)=-a$