נושא 3. **מבנים אלגבריים**

1). יחסים. יחס השקילות. קבוצת המנה. חלוקה של קבוצה (חזרה)

הגדרה 1. <u>יחס בינרי</u> או <u>יחס דו-מקומי</u> או פשוט <u>יחס R</u> מהקבוצה A לקבוצה B הוא כלל המתאים לכל זוג סדור $<a,b>\in A\times B$ של איברים $a\in A, b\in B$ בדיוק אחת מן הטענות הבאות: "a מתייחס אל b" (מסומן $a\mathrm{R}b$) או "a לא מתייחס אל b" (מסומן $a\mathrm{R}b$). יחס מקבוצה A לקבוצה A ייקרא <u>יחס ב- A</u>.

כל יחס R מ- A אל B מגדיר באופן יחיד תת-קבוצה $\{<a,b>|\, a\mathrm{R}b\}\subseteq A\times B$ ולהפך כל תת-קבוצה $S\subseteq A\times B$ מגדירה יחס R מ- A אל B באופן הבא: "$a\mathrm{R}b$ אם ורק אם $<a,b>\in S$". לכן את יחס R מ- A ל- B מגדירים כתת-קבוצה של $A\times B$.

הגדרה 2. יחס R בקבוצה A נקרא <u>יחס השקילות</u> ב- A אם הוא:
1) רפלקסיבי (ז"א $((\forall a)(aRa)$),
2) סימטריות (ז"א $((\forall a)(\forall b)(a\mathrm{R}b\to b\mathrm{R}a)$),
3) טרנזיטיביות (ז"א $((\forall a)(\forall b)(\forall c)(a\mathrm{R}b\wedge b\mathrm{R}c\to a\mathrm{R}c)$),

הגדרה 3. יהא R יחס שקילות על A. יהא $a\in A$.
<u>מחלקת השקילות</u> של a ביחס R היינה $a/\mathrm{R}=\{b\in A\,|\,a\mathrm{R}b\}$

במקום הסימון a/R משתמשים גם ב- $\overline{a}$

הגדרה 4. קבוצה $A/\mathrm{R}=\{\overline{a}\,|\,a\in A\}$ כל המחלקות השקילות של R נקראת <u>קבוצת המנה</u> של A לפי R.

התכונה הבסיסית של יחסי השקילות מנוסחת במשפט הבא:

משפט: יהי R יחס השקילות ב- A. אזי קבוצת המנה A/R היא חלוקה של A, כלומר, כל $a\in A$ שייך לאיבר של A/R ואיברי A/R זרים זה לזה.

דוגמה. נגדיר יחס $\equiv^4$ ב- Z לפי הנוסחה
$$\equiv^4=\{<n,m>\in Z\times Z\,|\,n\text{-}m \text{ מתחלק ב-}4\}$$
במילים אחרות נכתוב $n\equiv^4 m$ כאשר $n\text{-}m$ מתחלק ב-4. (במקום $n\equiv^4 m$ כותבים גם $x\equiv y(\mathrm{mod}4)$ ואומרים "x שווה ל- y מודולו 4").
יחס R_4 היא יחס השקילות ב- Z.

למשל מחלקת השקילות של מספר 1- ביחס $\equiv^4$ היא
$$-\overline{1}=\{...,-9,-5,-1,3,7,11,...\}=\{4a-1\,|\,a\in Z\}$$
אם $n\text{-}m$ מתחלק ב-4 אז $\overline{n}=\overline{m}$. לכן יש בדיוק ארבע מחלקות השקילות זרות:
$$A_0=\overline{0}=\{...,-8,-4,0,4,8,...\},$$
$$A_1=\overline{1}=\{...,-7,-3,1,5,9,...\},$$
$$A_2=\overline{2}=\{...,-6,-2,2,6,10,...\},$$
$$A_3=\overline{3}=\{...,-5,-1,3,7,11,...\}.$$

יש לטעון שכל $n\in Z$ ניתן לכתיבה באופן יחיד כצורה $n=4a+r$ (כאשר $0\le r<4$) ו- $n\in A_r$. אזי קבוצת המנה $Z_4=Z/_{\equiv^4}$ היינה $Z_4=\{A_0,A_1,A_2,A_3\}$
ו- $Z=A_0\cup A_1\cup A_2\cup A_3$.

2). הגדרה של מבנה אלגברי . חבורות .

הגדרה 1 . *פעולה בינרית* בקבוצה A היא פונקציה $\mathrm{P}: A\times A\to A$, ז"א לכל זוג סדור $<a,b>$ של איברים $a,b\in A$ מותאם איבר $c\in A$ (נסמן $c=a\mathrm{P}b$).

תהי A קבוצה לא ריקה בעלת אחת או כמה פעולות בינריות .

הגדרה 2 . קבוצה לא ריקה A ביחד עם פעולות בינריות המוגדרות בה נקראת *מבנה אלגברי*.

דוגמאות: Z לפי חיבור , Z לפי כפל , Z לפי חיסור , Z לפי חיבור וכפל - מבנים אלגבריים , N לפי חיסור , Z לפי חילוק , N לפי חילוק *אינן* מבנים אלגבריים

נעבור עכשיו למקרים פרטיים של מבנים אלגבריים כאשר הפעולות בעלות איזהו תכונות . נתחיל ממבנים אלגבריים עם פעולה בינרית אחת. הדוגמה החשובה של מבנה כזה היינה *חבורה*.

תהי G קבוצה לא ריקה בעלת פעולה בינרית P . נסמן איברים של הקבוצה G באותיות $a, b, c, a_0, a^*, \ldots$

הגדרה 3 . קבוצה G נקראת *חבורה* (לפי פעולה P) אם מתקיימות בה התכונות הבאות:

1) $(\forall a)(\forall b)(\forall c)((a\mathrm{P}b)\mathrm{P}c=a\mathrm{P}(b\mathrm{P}c))$ (אסוציאטיביות)
2) $(\exists a_0)(\forall a)(a\mathrm{P}a_0=a_0\mathrm{P}a=a)$ (קיימות איבר נייטרלי)
3) $(\forall a)(\exists a^*)(a\mathrm{P}a^*=a^*\mathrm{P}a=a_0)$ (קיימות איבר סימטרי לאיבר שרירותי)

במילים אחרות חבורה היא מבנה אלגברי עם פעולה בינרית אחת בעלת תכונות 1) – 3) .

הגדרה 4 . חבורה G נקראת קומוטטיבית אם מתקיימת בה התכונה

4) $(\forall a)(\forall b)(a\mathrm{P}b=b\mathrm{P}a)$ (קומוטטיביות)

כשנכתבת הפעולה P באופן דלעיל, נאמר כי G חבורה *כפלית*. במקרה הזה במקום P משתמשים בסימון $\cdot$ (או לא כותבים שום סימן) , לאיבר נייטרלי קוראים *יחידה* (נסמן אותו e או 1) , לאיבר a^* הסימטרי לאיבר a קוראים *ההפכי* של a (נסמן a^{-1}).
לעיתים, במיוחד אם G קומוטטיבית, מסומנת הפעלה P ב- $+$ ו- G קרויה אז חבורה חיבורית. במקרה האחרון מסומן איבר נייטרלי ב- 0 וקרוי איבר *האפס*, האיבר הסימטרי יסומן ב- $-a$ וייקרא *השלילי* של a .

הגדרה 5 . תת-קבוצה $H\subseteq G$ תיקרא תת-חבורה של G אם H עצמה חבורה תחת הפעולה המוגדרת ב- G .

דוגמאות.

1. הקבוצה Z של השלמים יוצרת חבורה קומוטטיבית תחת פעולת החיבור . השלמים הזוגיים יוצרים תת-חבורה של Z . השלמים אי-הזוגיים *לא יוצרים* תת-חבורה של Z .
2. הקבוצות $Q\setminus\{0\}$ ו- $R\setminus\{0\}$ יוצרות חבורות קומוטטיביות תחת פעולת הכפל ו- $Q\setminus\{0\}$ היא תת-חבורה של $R\setminus\{0\}$.
3. התמורה של n סמנים היא פונקציה חד-חד ערכית $p:\{1,2,\ldots,n\}\to\{1,2,\ldots,n\}$. נגדיר מכפלת תמורה $p:\{1,2,\ldots,n\}\to\{1,2,\ldots,n\}$ בתמורה $q:\{1,2,\ldots,n\}\to\{1,2,\ldots,n\}$ כהרכבה $q\circ p$ של פונקציות p ו- q . כך נקבל החבורה הסימטרית S_n ממעלה n .

אם $n=2$ אז ב- S_2 יש רק שני תמורות : $\varepsilon=\begin{pmatrix}1&2\\1&2\end{pmatrix}$, $\varphi=\begin{pmatrix}1&2\\2&1\end{pmatrix}$,

ומתקיימים השוויונות $\varepsilon\varepsilon=\varepsilon$, $\varepsilon\varphi=\varphi$, $\varphi\varepsilon=\varphi$, $\varphi\varphi=\varepsilon$

קל להראות שהתכונות 1) – 3) מתקיימות וקומוטטיביות גם מתקיימת .

נתבונן במקרה $n=3$.

ב- S_3 יש ששה תמורות :

$$\varepsilon=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad \sigma_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad \varphi_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},$$
$$\sigma_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad \sigma_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad \varphi_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

לוח הכפל ב- S_3 הוא :

	ε	σ_1	σ_2	σ_3	φ_1	φ_2
ε	ε	σ_1	σ_2	σ_3	φ_1	φ_2
σ_1	σ_1	ε	φ_1	φ_2	σ_2	σ_3
σ_2	σ_2	φ_2	ε	φ_1	σ_3	σ_1
σ_3	σ_3	φ_1	φ_2	ε	σ_1	σ_2
φ_1	φ_1	σ_3	σ_1	σ_2	φ_2	ε
φ_2	φ_2	σ_2	σ_3	σ_1	ε	φ_1

בעזרת הלוח ניתן לבדוק התקיימות של התכונות 1) – 3) .

בפרט ε היינו איבר נייטרלי (יחידה) , $(\sigma_1)^{-1}=\sigma_1$, $(\sigma_2)^{-1}=\sigma_2$, $(\sigma_3)^{-1}=\sigma_3$, $(\varphi_1)^{-1}=\varphi_2$, $(\varphi_2)^{-1}=\varphi_1$ ובודאי $(\varepsilon)^{-1}=\varepsilon$. קל לראות שקומוטטיביות *לא מתקיימת*.

3). חוגים , תחומים שלמים ושדות .

נעבור למבנים אלגבריים בעלות שני פעולות ביניריות .

הגדרה 1 תהי K קבוצה לא ריקה ונתונות בה שני פעולות , חיבור (אשר תסומן ב- +) וכפל .
הקבוצה K תיקרא *חוג* אם מתקיימות בה התכונות הבאות :

1) $(\forall a)(\forall b)(\forall c)((a+b)+c=a+(b+c))$ (אסוציאטיביות של חיבור)
2) $(\exists 0)(\forall a)(a+0=0+a=a)$ (קיימות אפס)
3) $(\forall a)(\exists(-a))(a+(-a)=(-a)+a=0)$ (קיימות איבר שלילי לאיבר שרירותי)
4) $(\forall a)(\forall b)(a+b=b+a)$ (קומוטטיביות של חיבור)
5) $(\forall a)(\forall b)(\forall c)((ab)c=a(bc))$ (אסוציאטיביות של כפל)
6) $(\forall a)(\forall b)(\forall c)(((a+b)c=ac+bc)\wedge(c(a+b)=ca+cb))$ (דיסטריבוטיביות)

הגדרה 2 . חוג K נקרא *קומוטטיבי* אם מתקיימת בה התכונה
7) $(\forall a)(\forall b)(ab=ba)$ (קומוטטיביות של כפל)

הגדרה 3 . חוג K נקרא *חוג עם יחידה* כאשר מתקיימת בה התכונה
8) $(\exists 1)(\forall a)(a\cdot 1=1\cdot a=a)$ (קיימות יחידה)

הגדרה. איברים $a,b\in K$ של חוג K נקראים *מחלקי אפס* אם $a\neq 0$, $b\neq 0$ אך $ab=0$.

הגדרה. חוג קומוטטיבי K אם איבר יחידה נקרא *תחום שלם* אם אין ל- K מחלקי אפס .

הגדרה. חוג קומוטטיבי K אם איבר יחידה נקרא *שדה* אם מתקיימת בה התכונה
9) $(\forall a)((a\neq 0)\rightarrow \exists(a^{-1})(aa^{-1}=a^{-1}a=1))$ (קיימות איבר הפכי לאיבר שרירותי)

קל לראות ששדה בהכרח תחום שלם, כי אם $ab=0$ ו- $a\neq 0$ אזי
$$b=1\cdot b=a^{-1}ab=a^{-1}\cdot 0=0$$

נעיר, כי שדה מהווה חבורה קומוטטיבית תחת פעולת החיבור ושדה ללא איבר אפסי מהווה חבורה קומוטטיבית תחת פעולת הכפל.

דוגמאות.

1. המספרים הרציונליים Q והמספרים הממשיים R יוצרים כל אחד שדה ביחס לפעולות הכפל והחיבור הרגילות.
2. המספרים השלמים Z יוצרים תחום שלם ביחס לפעולות הכפל והחיבור הרגילות אך לא שדה.
3. פונקציות $f:[0,1]\rightarrow[0,1]$ יוצרות חוג קומוטטיבי עם יחידה ביחס לפעולות הכפל והחיבור של פונקציות אך הן לא מהוות תחום שלם. דוגמאות של מחלקי אפס היינן
$$f(x)g(x)\equiv 0 \quad \text{כי} \quad f(x)=\begin{cases}0, & x\in[0,1)\\ 1, & x=1\end{cases},\ g(x)=\begin{cases}1, & x\in[0,1)\\ 0, & x=1\end{cases}$$
4. מטריצות ריבועיות מהסדר 2 יוצרות חוג לא קומוטטיבי עם יחידה ביחס לפעולות הכפל והחיבור של מטריצות עם מחלקי אפס. דוגמאות של מחלקי אפס היינן
$$AB=\begin{pmatrix}1&2\\3&6\end{pmatrix}\begin{pmatrix}2&-10\\-1&5\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix} \quad \text{כי} \quad B=\begin{pmatrix}2&-10\\-1&5\end{pmatrix},\ A=\begin{pmatrix}1&2\\3&6\end{pmatrix}$$

4). חוג השלמים מודולו n.

נתבונן במקרה מעניין של חוגים סופיים כשבקבוצה הנתונה יש בדיוק n איברים.

יהיו $n\in N$, $x,y\in Z$

הגדרה. אומרים ש- *x שווה ל- y מודולו n* אם $x-y$ מתחלק ב- n. (סימון $x\equiv y(\mathrm{mod}\,n)$)

נגדיר יחס $\equiv^n$ ב- Z לפי הנוסחה
$$\equiv^n=\{<x,y>\in Z\times Z \mid x\equiv y(\mathrm{mod}\,n)\}$$

נתבונן בקבוצת המנה $Z_n=Z/_{\equiv^n}$. נסמן $\bar{x}=x/_{\equiv^n}$. אזי $Z_n=\{\bar{0},\bar{1},...,\overline{n-1}\}$

נגדיר ב- Z_n פעולות החיבור והכפל:
$$\bar{x}+\bar{y}=\bar{z}\Leftrightarrow((\forall x)(\forall y)(x\in\bar{x}\wedge y\in\bar{y}\rightarrow(x+y)\in\bar{z}))$$
$$\bar{x}\bar{y}=\bar{z}\Leftrightarrow((\forall x)(\forall y)(x\in\bar{x}\wedge y\in\bar{y}\rightarrow xy\in\bar{z})).$$

ניתן להוכיח כי ביחס הפעולות האלה קבוצה Z_n מהווה חוג עם יחידה. האיבר האפס הוא $\bar{0}$ והאיבר היחידה היינו $\bar{1}$.

דוגמאות.

1. אם *n=2* אז $Z_2=\{\bar{0},\bar{1}\}$ כאשר $\bar{0}=\{...,-4,-2,0,2,4,...\}$, $\bar{1}=\{...-3,-1,1,3,5,...\}$. לחיבור ולכפל מקבלים טבלאות:

+	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

*	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

ניתן לבדוק ש-Z_2 מהווה שדה ולמצוא : $-\overline{0}=\overline{0}$, $-\overline{1}=\overline{1}$, $\overline{1}^{-1}=\overline{1}$.

2. אם $n=3$ אז $Z_3=\{\overline{0},\overline{1},\overline{2}\}$ כאשר

$\overline{0}=\{...,-6,-3,0,3,6,...\}$, $\overline{1}=\{...-5,-2,1,4,7,...\}$, $\overline{2}=\{...,-4,-1,2,5,8,...\}$.

לחיבור ולכפל מקבלים טבלאות :

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

*	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

בעזרת הטבלאות בודקים שגם Z_3 מהווה שדה ומוצאים : $-\overline{0}=\overline{0}$, $-\overline{1}=\overline{2}$, $-\overline{2}=\overline{1}$, $\overline{1}^{-1}=\overline{1}$, $\overline{2}^{-1}=\overline{2}$.

3. אם $n=4$ אז $Z_4=\{\overline{0},\overline{1},\overline{2},\overline{3}\}$ כאשר

$\overline{0}=\{...,-8,-4,0,4,8,...\}$, $\overline{1}=\{...-7,-3,1,5,9,...\}$,

$\overline{2}=\{...,-6,-2,2,6,10,...\}$, $\overline{3}=\{...,-5,-1,3,7,11,...\}$.

לחיבור ולכפל מקבלים טבלאות :

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

*	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

בעזרת הטבלאות בודקים ש-Z_4 *לא מהווה* שדה. לאיבר $\overline{2}$ לא קיים איבר $\overline{2}^{-1}$.
גם אנו רואים ש- $\overline{2}\cdot\overline{2}=\overline{0}$. אז Z_4 אינו תחום שלם. אבל ניתן לבדוק ש-Z_4 מהווה חוג קומוטטיבי עם יחידה. האיברים השליליים הם : $-\overline{0}=\overline{0}$, $-\overline{1}=\overline{3}$, $-\overline{2}=\overline{2}$, $-\overline{3}=\overline{1}$.

<u>*משפט*</u>: חוג Z_n השלמים מודולו n הוא שדה אם ורק אם מספר n ראשוני .

<u>*על הוכחה*</u> . אם מספר n אינו ראשוני אז קיימת הצגה $n=n_1n_2$ כאשר $n_1>1$, $n_2>1$, $n_1,n_2,n\in N$ וניתן להראות כי $\overline{n}_1\overline{n}_2=\overline{0}$. אם מספר n הוא ראשוני אז קיימות של $\overline{m}^{-1}$ לכל m טבעי הקטן מ-n נובע מהקיימות של הצגה $nu+mv=1$ (כאשר $u,v\in Z$) למספרים זרים n ו-m .

<u>*טענה חשובה*</u>. (ללא הוכחה). אם מספר n הוא ראשוני אז את האיבר ההפכי $\overline{m}^{-1}$ ל- $\overline{m}$ בשדה Z_n הוא $\overline{v}$ כאשר v מוגדר מהנוסחה $nu+mv=1$.

כדי למצוא הצגה $nu+mv=1$ ניתן להשתמש באלגוריתם אויקלידס .

נראה את השיטה בדוגמה .

<u>דוגמה</u> . מצא $\overline{7}^{-1}$ בשדה Z_{19} .

<u>פתרון</u>.

שלב 1:

1. מחלקים $n=19$ ב- $m=7$ עם שארית . קיבלנו

$\underline{19} = \underline{7}\cdot 2 + \underline{5}$ (1) , (שארית 5)

2. מחלקים מחלק הקודם 7 בשארית 5 . קיבלנו

$\underline{7} = \underline{5}\cdot 1 + \underline{2}$ (2) , (שארית 2)

3. מחלקים מחלק הקודם 5 בשארית 2 . קיבלנו

$\underline{5} = \underline{2}\cdot 2 + \underline{1}$ (3) (שארית 1)

(חוזרים עד קבלת שארית 1).

שלב 2:

1. מהשוויון האחרון (3) מבטאים 1 . קיבלנו

$\underline{1} = \underline{5} - \underline{2}\cdot 2$ (4) ,

2. מבטאים מ-(2) את השארית 2 ומציבים אותו ל-(4) . מקבלים :

$$\underline{1} = \underline{5} - \underline{2}\cdot 2 = \underline{5} - (\underline{7} - \underline{5}\cdot 1)\cdot 2 = \underline{7}\cdot(-2) + \underline{5}\cdot 3$$

אז $\underline{1} = \underline{7}\cdot(-2) + \underline{5}\cdot 3$ (5)

3. מבטאים מ-(1) את השארית 5 ומציבים אותו ל-(5) . מקבלים :

$$\underline{1} = = \underline{7}\cdot(-2) + \underline{5}\cdot 3 = \underline{7}\cdot(-2) + (\underline{19} - \underline{7}\cdot 2)\cdot 3 = 19\cdot 3 + 7\cdot(-8)$$.

אז $19\cdot 3 + 7\cdot(-8) = 1$ (6)

(חוזרים עד שימוש כל השוויונות (1)-(3)).

שלב 3:

מהנוסחה (6) מוצאים את התשובה:

$$\overline{7}^{-1} = \overline{(-8)} = \overline{11}$$

נעיר כמציאת איבר ההפכי בעזרת הרכבת טבלת הכפל בשדה Z_{19} היינה דרך יותר-יותר ארוכה .

בשדה Z_n (כאשר n ראשוני) ניתן לפתור משוואות כקו בשדות מספריים.

<u>דוגמאות</u> .

1). פתרו את המשוואה $\overline{7}x + \overline{8} = \overline{13}$ בשדה Z_{19} (כלומר $7x + 8 \equiv 13 \pmod{19}$)

<u>פתרון</u>. קל לראות ש- $-\overline{8} = \overline{11}$ (כי $\overline{8} + \overline{11} = \overline{0}$). אז

$$\overline{7}x + \overline{8} = \overline{13} \Leftrightarrow \overline{7}x = \overline{13} + \overline{11} \Leftrightarrow \overline{7}x = \overline{5}$$,

$\overline{7}^{-1} = \overline{11}$ (מהדוגמה הקודמת) . לכן

$$\overline{7}x = \overline{5} \Leftrightarrow \overline{7}^{-1}\cdot\overline{7}\cdot x = \overline{7}^{-1}\cdot\overline{5} \Leftrightarrow x = \overline{7}^{-1}\cdot\overline{5} \Leftrightarrow x = \overline{11}\cdot\overline{5} \Leftrightarrow x = \overline{17}$$.

2) פתרו את המערכת: $\begin{cases}\overline{2}x+\overline{3}y=\overline{1}\\ \overline{4}x+\overline{2}y=\overline{0}\end{cases}$ בשדה Z_5 .

פתרון.

$$\begin{cases}\overline{2}x+\overline{3}y=\overline{1}\\ \overline{4}x+\overline{2}y=\overline{0}\end{cases}\Leftrightarrow\begin{cases}\overline{4}x+\overline{1}y=\overline{2}\\ \overline{4}x+\overline{2}y=\overline{0}\end{cases}\Leftrightarrow\begin{cases}\overline{4}x+y=\overline{2}\\ y=\overline{3}\end{cases}\Leftrightarrow\begin{cases}y=\overline{2}+\overline{1}x\\ y=\overline{3}\end{cases}\Leftrightarrow\begin{cases}x=y+\overline{3}\\ y=\overline{3}\end{cases}\Leftrightarrow\begin{cases}x=\overline{1}\\ y=\overline{3}\end{cases}$$

5). אלגברות בוליאניות.

נגדיר עכשיו דוגמה חשובה של מבנה אלגברי הקשור בצפיפות עם לוגיקה מתמטית .

הגדרה 1 תהי B קבוצה לא ריקה ונתונות בה שני פעולות דו-מקומיות (אשר תסומן + ו- $\cdot$) וכעולה חד-מקומית אחת (אשר תסומן $\overline{\ }$) .
הקבוצה B תיקרא *אלגברה בוליאנית* אם מתקיימות בה התכונות הבאות :

1) $(\forall a)(\overline{\overline{a}}=a)$ (פעולה $\overline{\ }$ פעמיים) ,
2) $(\forall a)(\forall b)(a\cdot b=b\cdot a)$ (קומוטטיביות של $\cdot$) ,
3) $(\forall a)(\forall b)(\forall c)((a\cdot b)\cdot c=a\cdot(b\cdot c))$ (אסוציאטיביות של $\cdot$) ,
4) $(\forall a)(\forall b)(a+b=b+a)$ (קומוטטיביות של +) ,
5) $(\forall a)(\forall b)(\forall c)((a+b)+c=a+(b+c))$ (אסוציאטיביות של +) ,
6) $(\forall a)(\forall b)(\forall c)((a+b)\cdot c=(a\cdot c)+(b\cdot c))$ (דיסטריבוטיביות של $\cdot$ לפי +) ,
7) $(\forall a)(\forall b)(\forall c)((a\cdot b)+c=(a+c)\cdot(b+c))$ (דיסטריבוטיביות של + לפי $\cdot$) ,
8) $(\forall a)(\forall b)(\overline{a\cdot b}=\overline{b}+\overline{a})$ (פעולה $\overline{\ }$ של $\cdot$) ,
9) $(\forall a)(\forall b)(\overline{a+b}=\overline{b}\cdot\overline{a})$ (פעולה $\overline{\ }$ של +) ,
10) $(\forall a)(a+a=a)$ (אידמפוטנטיות של +) ,
11) $(\forall a)(a\cdot a=a)$ (אידמפוטנטיות של $\cdot$) ,
12) $(\forall a)(\forall b)((a+\overline{a})\cdot b=b)$,
13) $(\forall a)(\forall b)((a\cdot\overline{a})+b=b)$.

ניתן להוכיח כי $(\forall a)(\forall b)(a+\overline{a}=b+\overline{b})$, $(\forall a)(\forall b)(a\cdot\overline{a}=b\cdot\overline{b})$ - בתירגול .

נסמן $a+\overline{a}=1$, $a\cdot\overline{a}=0$ - כך מגדירים באלגברה בוליאנית את 0 ו- 1 .

קל לראות שמהתכונות 12) – 13) נובע כי

14) $(\exists 1)(\forall a)(1\cdot a=a)$ (קיימות יחידה) ,
15) $(\exists 0)(\forall a)(a+0=a)$ (קיימות אפס) .

נדגים דוגמאות של אלגברות בוליוניות.

1. נבין $\overline{\ }$ כשלילה $\neg$, + כדיסיונקציה $\vee$, $\cdot$ כקוניונקציה $\wedge$, ו- = כשקילות לוגית בקבוצה B כל הפסוקים . אז נקבל לכל $a,b,c\in B$:

1) $(\forall a)(\neg(\neg a)=a)$,
2) $(\forall a)(\forall b)(a\wedge b=b\wedge a)$, 3) $(\forall a)(\forall b)(\forall c)((a\wedge b)\wedge c=a\wedge(b\wedge c))$,
4) $(\forall a)(\forall b)(a\vee b=b\vee a)$, 5) $(\forall a)(\forall b)(\forall c)((a\vee b)\vee c=a\vee(b\vee c))$,
6) $(\forall a)(\forall b)(\forall c)((a\vee b)\wedge c=(a\wedge c)\vee(b\wedge c))$,
7) $(\forall a)(\forall b)(\forall c)((a\wedge b)\vee c=(a\vee c)\wedge(b\vee c))$,

8) $(\forall a)(\forall b)(\neg(a\wedge b)=\neg b\vee\neg a)$, 9) $(\forall a)(\forall b)(\neg(a\vee b)=\neg b\wedge\neg a)$,
10) $(\forall a)(a\vee a=a)$, 11) $(\forall a)(a\wedge a=a)$,
12) $(\forall a)(\forall b)((a\vee\neg a)\wedge b=b)$, 13) $(\forall a)(\forall b)((a\wedge\neg a)\vee b=b)$.

ניתן לבדוק שכל הנוסחאות האחרונות מתקיימות. אז קיבלנו את הדוגמה החשובה ביותר של אלגברה בוליאנית הנקראת <u>*אלגברה בוליאנית של הפסוקים*</u> .

2. יהי $B=P(A)$ – קבוצת כל תת-הקבוצות של הקבוצה A (ז"א קבוצת החזרה של A). לאיברים $a,b,...\in B$ של B (תת-קבוצות $a,b,...\subseteq A$) נבין $\cdot$ כחיתוך $\cap$, $+$ כיחוד $\cup$, ו- $\bar{a}$ כ- $A\setminus a$.

בודקים את התכונות 1)-13) :

1) $(\forall a)(A\setminus(A\setminus a)=a)$,
2) $(\forall a)(\forall b)(a\cap b=b\cap a)$, 3) $(\forall a)(\forall b)(\forall c)((a\cap b)\cap c=a\cap(b\cap c))$,
4) $(\forall a)(\forall b)(a\cup b=b\cup a)$, 5) $(\forall a)(\forall b)(\forall c)((a\cup b)\cup c=a\cup(b\cup c))$,
6) $(\forall a)(\forall b)(\forall c)((a\cup b)\cap c=(a\cap c)\cup(b\cap c))$,
7) $(\forall a)(\forall b)(\forall c)((a\cap b)\cup c=(a\cup c)\cap(b\cup c))$,
8) $(\forall a)(\forall b)(A\setminus(a\cap b)=(A\setminus a)\cup(A\setminus b))$,
9) $(\forall a)(\forall b)(A\setminus(a\cup b)=(A\setminus a)\cap(A\setminus b))$,
10) $(\forall a)(a\cup a=a)$, 11) $(\forall a)(a\cap a=a)$,
12) $(\forall a)(\forall b)((a\cup(A\setminus a))\cap b=b)$, 13) $(\forall a)(\forall b)((a\cap(A\setminus a))\cup b=b)$.

מתורת הקבוצות אנו יודעים שהנוסחאות האלה נכונות. כך רואים ש- $B=P(A)$ מהווה אלגברה בוליאנית .

3. יהי $B=\{0,1\}$. נגדיר : $\bar{0}=1$, $\bar{1}=0$. נגדיר $+$ ו- $\cdot$ לפי הטבלאות:

$+$	0	1
0	0	1
1	1	1

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

ניתן לבדוק שגם במקרה הזה נקבל אלגברה בוליאנית. גם יש לטעון שהדוגמה הזה היא מקרה פרטי של הדוגמה הקודמת כאשר $A=\{1\}$ ולכן $P(A)=\{\emptyset,\{1\}\}$.

4. יהי $B=[0,1]$. נגדיר לכל $x,y\in[0,1]$: $\bar{x}=1-x$, $x+y=\max\{x,y\}$, $x\cdot y=\min\{x,y\}$. את 0 ואת 1 נבין במשמעות רגילה. ניתן לבדוק שתכונות 1)- 11) מתקיימות. נבדוק כתכונות 12) – 13) לא מתקיימות אבל תכונות 14) – 15) מתקיימות. ל- $x,y\in[0,1]$ מקבלים:

$$x\cdot 1=\min\{x,1\}=x\ ,\ x+0=\max\{x,0\}=x$$

(התקיימות של 14) – 15)). אבל אם לדוגמה $x=0.5,\ y=0.7$ אז

$$(x+\bar{x})\cdot y=\min\{\max\{x,1-x\},y\}=\min\{\max\{0.5,0.5\},0.7\}=0.5\neq y$$

(תכונה 12) לא מתקיימת .
מכאן רואים

מהדוגמה האחרונה ברור שמהתכונות 14) – 15) לא נובע תכונות 12) – 13)