בס"ד

תרגול מס' 1 במבנים אלגבריים 1

מערכות אלגבריות

<u>הגדרה</u>: מערכת אלגברית היא הזוג: $(S,\bullet)$ כאשר S היא קבוצת איברים לא ריקה, ו- $\bullet$ היא פעולה בינארית המוגדרת על איברי S. (כלומר: $\forall a,b\in S: a\bullet b=c\in S$ - פעולה בינארית עם סגירות).

<u>הגדרה</u>: מערכת אלגברית $(S,\bullet)$ מקיימת את **החוק האסוציאטיבי** אם:

$$\forall a,b,c\in S:\ (a\bullet b)\bullet c=a\bullet(b\bullet c).$$

מערכת אלגברית המקיימת את החוק האסוציאטיבי נקראת **אגודה**.

<u>תרגיל</u>: מצא פעולה מעל קבוצה בת שני איברים שאינה אסוציאטיבית.

<u>פתרון</u>:

נניח: $S=\{a,b\}$. נגדיר את הפעולה באמצעות "לוח הכפל" שלה:

	a	b
a	b	b
b	b	a

אכן: $(b\bullet a)\bullet a=b$ לעומת: $b\bullet(a\bullet a)=a$.

<u>תרגיל</u>: מצא את מספר הפעולות הבינאריות מעל קבוצה X סופית בעלת $|X|=n$ איברים.

<u>פתרון</u>:

כל פעולה בינארית מאופיינת ע"י לוח כפל. לוח הכפל הוא בן n^2 מקומות, כאשר לכל מקום ישנן n אפשרויות. לכן מס' האפשרויות הוא בסה"כ: n^{n^2} (לאו דווקא אגודות).

<u>הגדרה</u>: במערכת $(S,\bullet)$ אבר e נקרא **האיבר הניטרלי** אם $\forall a\in S:\ a\bullet e=e\bullet a=a$.

<u>הערה</u>: אם קיים איבר ניטרלי, אז הוא בהכרח יחיד.

<u>הגדרה</u>: אגודה עם איבר ניטרלי נקראת **מונואיד**.

<u>דוגמה</u>: תהי X קבוצה כלשהי. אוסף כל הפונקציות מ- X ל- X, $S=\{f:X\to X\}$ היא מונואיד ביחס להרכבת פונקציות. האיבר הניטרלי כאן הוא פונקצית הזהות.

<u>הגדרה</u>: מערכת $(S,\bullet)$ מקיימת את **חוק החילוף** אם: $\forall a,b\in S:\ a\bullet b=b\bullet a$.

מערכת כזו נקראת **קומוטטיבית** או **אבלית** (על שם המתמטיקאי נילס אבל).

<u>תרגיל:</u> תהא X קבוצת איברים. הוכח כי המערכת: $S=\left(P\left(X\right),\cap\right)$ היא מונואיד אבלי.

($P\left(X\right)$ היא קבוצת החזקה של X).

<u>פתרון:</u>

הסגירות לגבי פעולת החיתוך ברורה. נבדוק אסוציאטיביות:

$$\forall A,B,C\in P\left(X\right):\ \left(A\cap B\right)\cap C=A\cap\left(B\cap C\right)=A\cap B\cap C$$

ולכן אגודה. האיבר הניטרלי הוא X: $\forall A\in P\left(X\right):\ A\cap X=A$ ולכן זהו מונואיד.

לגבי האבליות: $\forall A,B\in P\left(X\right):\ A\cap B=B\cap A$. ולכן זהו מונואיד אבלי.

(<u>הערה</u>: אותה ההוכחה נכונה עבור פעולת האיחוד אלא שאז האיבר הניטרלי הוא הקבוצה הריקה).

<u>הגדרה:</u> בהינתן מונואיד $\left(S,\bullet\right)$ איבר $a\in S$ יקרא **הפיך** אם קיים איבר **הופכי** $b\in S$ כך ש:

$a\bullet b=b\bullet a=e$. נסמן אותו ב- a^{-1}.

<u>הערה:</u> לאיבר הפיך יש איבר הופכי יחיד.

<u>הערה:</u> יתכן הופכי רק מצד אחד. לדוגמה במונואיד: $M=\left\{f:\left[0,1\right]\to\left[0,1\right]\right\}$ הפונקציה:

$f\left(x\right)=\begin{cases}2x & 0\le x\le\frac{1}{2}\\ 0 & \frac{1}{2}<x\le 1\end{cases}$ היא הפיכה מימין. יחד עם $g\left(x\right)=\frac{x}{2}$ נקבל:

$\forall x\in\left[0,1\right]:\ \left(f\circ g\right)\left(x\right)=x$ כלומר: $f\circ g=id$ אבל אין ל- f הופכי שמאלי שכן אם f ראשונה

היא מאבדת את המידע של קלטים $\frac{1}{2}<x\le 1$ ולא ניתן לשחזרם.

באופן יותר כללי אפשר לומר שהפונקציות החח"ע הן הפיכות משמאל והעל הן הפיכות מימין.

<u>הגדרה:</u> מונואיד שכל איבריו הפיכים נקרא **חבורה**.

דוגמאות:

1. $\mathbb{Z}$ לגבי חיבור הוא חבורה אבלית. לגבי כפל רק מונואיד.
2. $\mathbb{R}^{\times}=\mathbb{R}\setminus\left\{0\right\}$ וכן $\mathbb{Q}^{\times}$ הן חבורות אבליות לגבי כפל.
3. $\mathbf{GL}_n\left(\mathbb{R}\right)=\left\{A\in M_n\left(\mathbb{R}\right)\mid\det\left(A\right)\neq 0\right\}$ היא חבורה כפלית לא אבלית.
4. $\mathbf{SL}_n\left(\mathbb{R}\right)=\left\{A\in M_n\left(\mathbb{R}\right)\mid\det\left(A\right)=1\right\}$ תת-חבורה של הקודמת.

<u>תרגיל:</u> תהא המערכת: $G=\left(\mathbb{R}\setminus\{-1\},\bullet\right)$ כאשר: $a\bullet b=a+b+ab$. הוכח G חבורה אבלית.

<u>פתרון:</u>

תחילה נוכיח סגירות. נניח בשלילה כי $\exists a,b\in G\,|\quad a\bullet b=a+b+ab=-1$.

כלומר: $a=-\frac{1+b}{1+b}=-1 \quad\Leftarrow\quad a(1+b)=-1-b$ בסתירה לכך ש: $a\in G$.

כעת נבדוק אסוציאטיביות:

$$(a\bullet b)\bullet c=(a+b+ab)\bullet c=a+b+ab+c+(a+b+ab)c$$
$$=a+b+c+ab+ac+bc+abc=a\bullet(b\bullet c)$$

ולכן אגודה. לגבי איבר ניטרלי נחפש איבר e כך ש:

$$a\bullet e=a\ \Rightarrow\ a+e+ae=a\ \ \Rightarrow\ \ e(1+a)=0$$

ידוע ש: $a\neq -1$ ולכן בהכרח: $e=0$. קיבלנו מונואיד. לגבי חבורה נמצא לכל איבר הופכי:

$$a\bullet b=e=0\ \Leftrightarrow\ a+b+ab=0\ \Leftrightarrow\ a(1+b)=-b\ \Leftrightarrow\ a=-\frac{b}{1+b}$$

ולכן: $\forall b\in G:\ b^{-1}=-\frac{b}{1+b}$ (ההופכי מוגדר היטב שכן $b\neq -1$). קיבלנו חבורה.

כמו כן ברור ש: $\forall a,b: a\bullet b=a+b+ab=b+a+ba=b\bullet a$ כלומר זו חבורה אבלית.

<u>תרגיל:</u> הוכח כי לכל החבורות בנות שני איברים או שלושה יש את אותו "לוח הכפל".

<u>פתרון:</u>

<u>לגבי חבורות עם שני איברים</u>: נניח $S=\{e,a\}$ (איבר אחד חייב להיות הניטרלי).

אזי ההופכי היחיד שיכול להיות ל- a הוא a בעצמו.

<u>לגבי חבורות עם שלושה איברים</u>: נניח: $S=\{e,a,b\}$.

אזי ההופכי היחיד שיכול להיות ל- a הוא b, שכן אם $a\bullet b=a$

אז $b=e$ ומאותה הסיבה גם לא יתכן ש: $a\bullet b=b$.

הוא הדין לגבי האיבר ההופכי של b שהוא a.

לכן לוח הכפל המתקבל הוא:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

<u>תרגיל:</u> יהא S מונואיד סופי עם צמצום מימין (או משמאל). הוכח כי S חבורה.

<u>פתרון:</u>

כדי להראות ש- S חבורה צ"ל שכל איבר הוא הפיך.

<u>נראה זאת בשתי דרכים</u>:

1. יהי $a\in S$. כיוון ש- S סופי, אזי אם נכפיל את a בעצמו הרבה פעמים, באיזשהו שלב בהכרח נחזור על איבר שכבר היינו בו. כלומר: $\exists i,k:1\le i<k:\ a^i=a^k$.

כיוון שנתון שמותר לצמצם, אזי אפשר לצמצם (מכיוון מסוים) ב- a^i ולקבל: $a^{k-i}=e$.

כלומר: $a\cdot a^{k-i-1}=e$ ולכן ההפכי מימין של a הוא a^{k-i-1}. כמו כן: $a^{k-i-1}\cdot a=e$ כלומר הוא גם הפכי משמאל. והוא שייך ל- S לכן a הפיך.

באותו האופן אפשר להראות שכל האיברים הפיכים ולכן זו חבורה.

2. לכל $a\in S$ נגדיר את הפונקציה: $f_a:S\to S$ ע"י: $f_a(x)=xa$.

טענה: f_a חח"ע. הוכחה: $\forall m,n\in S:\ \ f_a(m)=f_a(n)\ \Rightarrow\ ma=na\ \Rightarrow\ m=n$.

(השוויון האחרון מסתמך על תכונת הצמצום מימין).

כמו כן S סופי ולכן אם f_a חח"ע אז היא גם על. מכאן: $\exists b\in S:\ f_a(b)=e\ \Rightarrow\ ab=e$.

כמו כן אם נגדיר את $f_b(x)=bx$ נקבל שהיא על ולכן $\exists c\in S:\ f_b(c)=e\ \Rightarrow\ bc=e$

כלומר b הפיך וכיוון שיש רק הופכי אחד אזי: $a=c$ ומכאן ש- a הפיך גם משמאל ולכן הפיך.

באותו האופן אפשר להראות שכל האיברים הפיכים ולכן זו חבורה.

חבורות קונגרואנציה (שאריות)

יחס השקילות על קבוצה (רפלקסיביות, סימטריות, טרנזיטיביות) X מחלק את איברי X לתת-קבוצות זרות הנקראות **מחלקות שקילות**.

הגדרה: עבור $n\in\mathbb{N}$ נגדיר את היחס הבא על $\mathbb{Z}$:

$$\forall x,y\in\mathbb{Z}:\quad x\equiv y\pmod n\ \Leftrightarrow\ \exists k\in\mathbb{Z}:\ x-y=k\cdot n.$$

קל לראות שהיחס שהגדרנו הוא יחס שקילות, ועל כן הוא מחלק את $\mathbb{Z}$ למחלקות שקילות שהן השאריות השונות מודולו n. נסמן את המחלקה של מספרים עם שארית השווה ל- k ע"י: $\overline{k}$.

למשל: $5\equiv 2\pmod 3$, $8\equiv 2\pmod 3$ ועל כן: $2,5,8\in\overline{2}$.

הגדרה: המבנה $\mathbb{Z}_n=\left(\left\{\overline{0},\overline{1},\overline{2},\dots,\overline{n-1}\right\},\ +\pmod n\right)$ הוא חבורת **קונגרואנציה מודולו** n או **חבורת השאריות מודולו** n (החיבור הוא ע"י נציגי מחלקות, לעיתים נסתפק בסימון ללא הקו העליון).

למשל ב- $\mathbb{Z}_6$: $2^{-1}=4$.

הערה: לגבי כפל מודולו n (גם כאן הכפל נעשה ע"י נציגי מחלקות), $\mathbb{Z}_n$ אינה חבורה באופן כללי אלא רק מונואיד.