פתרון אלגברה מופשטת - תרגיל 1 (88-211)

שאלה 1

בדקו האם קבוצת המספרים הממשיים $\mathbb{R}$ מהווה חבורה למחצה לגבי הפעולות הבינאריות הבאות:

א) $a*b=a^2+ab$

לא – אין אסוציאטיביות.

ב) $a*b=\sqrt{a+b}$

לא- אין אסוציאטיביות

ג) $a*b=(a^2+b^2)/2$

לא- אין אסוציאטיביות

שאלה 2

בדקו עבור כל אחת מהקבוצות הבאות עם הפעולות הנתונות האם היא: חבורה למחצה/ מונואיד/ חבורה. כמו כן, בדקו האם הפעולה היא קומוטטיבית.

א. $(\mathbb{Z},\bullet)$ כאשר $a\bullet b=a+b+2$

זאת חבורה. איבר היחידה הוא $e=-2$, וההופכי של b הוא $-4-b$. הפעולה היא קומוטטיבית.

ב. $(\mathbb{Z}_4,\cdot)$

כן מונואיד, לא חבורה (מכיוון שאפס לא הפיך). הפעולה היא קומוטטיבית.

ג. $(\mathbb{Z},-)$

הפעולה אינה אסוציאטיבית ולכן זאת לא חבורה למחצה. הפעולה אינה קומוטטיבית.

ד. $(Map(\mathbb{N},\mathbb{N}),\circ)$ כאשר $Map(\mathbb{N},\mathbb{N})=\{f:\mathbb{N}\to\mathbb{N}\}$

ראינו שזה מונואיד, וזאת לא חבורה מכיוון שלא כל פונקציה היא הפיכה. הפעולה אינה קומוטטיבית.

ה. $(P(X),\Delta)$, באשר X קבוצה כלשהי ו- Δ ההפרש הסימטרי המוגדר ע"י

$A\Delta B=(A\bigcup B)\setminus(A\cap B)$ לכל $A,B\in P(X)$.

זאת חבורה. אסוציאטיביות ידועה מבדידה. האיבר הנייטרלי הוא הקבוצה הריקה.וקל לבדוק שכל איבר הוא ההופכי של עצמו. הפעולה היא קומוטטיבית.

שאלה 3

א. תהי $A=\{0,1,2,3,4,5,6\}$. על המכפלה הקרטזית $A\times A=\{(a,b)\,|\,a,b\in A\}$ נגדיר פעולה בינרית ע"י $(a,b)*(c,d)=(ac-bd,ad+bc)$, כאשר הפעולות באגף ימין הן חיבור וכפל מודולו 7.

(i) הוכיחו ש- $A\times A$ מונואיד קומוטטיבי.

(ii) האם כל איבר ב $A\times A$, פרט ל $(0,0)$, הוא הפיך ?

ב. אותה שאלה כמו בא', כאשר $A=\{0,1,2,3,4\}$ והפעולות הן מודולו 5.

(i) הוכח ש $A\times A$ מונואיד קומוטטיבי.

(ii) האם כל איבר ב $A\times A$, פרט ל $(0,0)$, הוא הפיך ?

<u>פתרון:</u>

א. ניתן לבדוק בצורה ישירה כי הפעולה היא אסוציאטיבית וקומוטטיבית, וכי (1,0) הוא איבר יחידה. כל איבר פרט ל $(0,0)$ הוא הפיך. אכן, ההפכי של (a,b) הוא $\left(a\left(a^2+b^2\right)^{-1},-b\left(a^2+b^2\right)^{-1}\right)$ (שימו לב כי

(A*,·) הוא חבורה כפלית (מודולו 7), ולכן לכל איבר פרט לאפס יש הופכי) בדקו כי $a^2+b^2\neq 0$ לכל $(a,b)\neq(0,0)$ (זה לא נכון בהכרח בכל שדה, כפי שקורה בסעיף ב'). רצוי לעשות את השאלה הזו בכל מקרה – היא מראה את האנלוגיה למספרים המרוכבים (מה ההופכי של a+bi ב-$\mathbb{C}$?)

ב. ההוכחה שזהו מונואיד חילופי היא כמו בא', אך לא לכל איבר שונה מ 0 יש הפכי. למשל, ל-(1,2) אין הפכי.

<u>שאלה 4</u>

האם $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a,b\in R, a^2+b^2>0\right\}$ היא חבורה למחצה, מונואיד או חבורה (ביחס לפעולת

כפל מטריצות)?

<u>פתרון:</u> ניתן לבדוק על פי בדיקה ישירה שזו חבורה.

<u>שאלה 5</u>

א) תהי $G=\left\{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid A,B,C\in\mathbb{R}\right\}$. הוכיחו ש- G היא חבורה ביחס לכפל מטריצות (חבורה זו נקראת **Heisenberg group**). האם היא אבלית?

ב) תהיינה $(H,*),(G,\cdot)$ חבורות. נגדיר פעולה + על המכפלה הקרטזית G × H כדלהלן:

$$(g_1,h_1) + (g_2,h_2) = (g_1\cdot g_2,h_1*h_2)$$

הוכיחו כי G × H היא חבורה תחת פעולה זו.

<u>פתרון:</u>

א) בדיוקת האקסיומות (בקשר לקיום הופכי: למרות שידוע שיש הופכי ב- $GL_3(R)$,

(הדטרמיננטה $\neq 0$) צריך עדיין להראות שהוא איבר ב- G). החבורה אינה אבלית. שימו לב: כדי להראות סגירות ו/או קומוטטיביות – יש צורך לבדוק תכונות אלה על איברים מהחבורה עצמה – ולא להראות, למשל, שכפל של איבר מ- G באיבר אחר מ- $GL_3(R)$ אינו קומוטטיבי.

ב) בדיקת האקסיומות.

<u>שאלה 6</u>

א) תהי G חבורה סופית, $a,b \in G$. הוכיחו: $|ab| = |ba|$

(רמז: אם $|ab|=n,\ |ba|=m$, הסתכלו על $(ba)^{n+1}$ ועל $(ab)^{m+1}$).

ב) תהי G חבורה, $g \in G$, $|g|=n$. הוכיחו ש- $g^a = g^b$ אמ"מ $a \equiv b \pmod n$.

<u>פתרון:</u>

א) נסתכל על $(ba)^{n+1}$:

$$(ba)^{n+1} = ba*\ldots*ba = b*(ab)^n*a = ba \Rightarrow (ba)^n = 1 \Rightarrow m \mid n$$

ואם נסתכל על $(ab)^{m+1}$ נקבל ש- $n \mid m$. לכן $n=m$.

ב) ישום ישיר של המשפט הבא: אם $g^m = 1$ אז $|g|$ מחלק את m.

<u>שאלה 7</u>

א. נגדיר $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a,b,c \in \mathbb{Z}_3 \right\}$. הוכיחו כי G חבורה ביחס לפעולת כפל מטריצות, מצאו את הסדר של G ואת הסדר של כל איבר ב G.

ב. תהי G חבורה. אם לכל $a,b \in G$ מתקיים $(ab)^3 = a^3b^3$ האם G אבלית?

<u>פתרון:</u>

א) G מוכלת ב $GL_3(\mathbb{Z}_3)$ (חבורת המטריצות ההפיכות מסדר 3*3 מעל $\mathbb{Z}_3$). ברור שזוהי קבוצה לא ריקה, לכן נותר לבדוק סגירות לכפל ולהופכי – בדקו זאת ישירות. הסדר של G הוא 3*3*3 = 27 (כי יש שלוש אפשרויות לבחור את a, שלוש אפשרויות לבחור את b ושלוש – את c). בודקים ישירות כי כל איבר ב G פרט לאיבר היחידה הוא מסדר 3 (ז"א – עבור כל **מטריצה** – כשמכפילים אותה בעצמה 3 פעמים – נקבל את איבר היחידה – מטריצת הזהות. אין הכוונה לבדוק את הסדר של האיברים ב- $\mathbb{Z}_3$).

ב) לא. החבורה מסעיף א) מהווה דוגמא נגדית.

שאלה 8

הוכיחו ש:

א) b מחלק את a אמ"מ $a\mathbb{Z}$ היא ת"ח של $b\mathbb{Z}$.

ב) $a\mathbb{Z}+b\mathbb{Z}=(a,b)\mathbb{Z}$

ג) $a\mathbb{Z}\cap b\mathbb{Z}=[a,b]\mathbb{Z}$.

פתרון:

א) $a\mathbb{Z}\leq b\mathbb{Z}$ ולכן קיים $n\in\mathbb{N}$ כך ש- $a=bn$ כלומר $b\,|\,a$. מצד שני, אם $b\,|\,a$ אז קיים $n\in\mathbb{N}$ כך ש- $a=bn$. אם $x\in a\mathbb{Z}$ אז $x=am\rightarrow x=bnm\rightarrow x\in b\mathbb{Z}$.

ב) נוכיח בהכלה דו כיוונית.

$\subseteq$: ידוע כי ניתן להציג את $\gcd(a,b)$ כצ"ל של a,b, כלומר $\gcd(a,b)=au+bv,\quad u,v\in\mathbb{Z}$. יהי $x\in a\mathbb{Z}+b\mathbb{Z}$ אזי קיימים $n_1,n_2\in\mathbb{N}$ כך ש- $x=an_1+bn_2$. אנחנו צריכים למצוא $m\in\mathbb{Z}$ כך ש- $(a,b)m=an_1+bn_2$. נקח $m=\frac{a}{(a,b)}\cdot n_1+\frac{b}{(a,b)}\cdot n_2$ וסיימנו.

$\supseteq$: נכון כי ה- gcd(a,b) הוא צירוף לינארי של a,b.

ג) $x\in[a,b]\mathbb{Z}\Leftrightarrow\exists m\in\mathbb{Z}:x=[a,b]m\Leftrightarrow[a,b]\,|\,x\Leftrightarrow a\,|\,x\wedge b\,|\,x\Leftrightarrow x\in a\mathbb{Z}\cap b\mathbb{Z}$.

שאלה 9

א) מצאו את הספרה האחרונה של המספר 63^{63}.

ב) מצאו את הסדר של $35\in(\mathbb{Z}_{75},+)$.

פתרון:

א.
$$63^{63}=(6*10+3)^{63}=3^{63}\bmod 10$$
$$63=15*4+3\quad,\quad 3^4=81=1\bmod 10\Rightarrow 3^{63}=\underbrace{(3^4)}_{=1\bmod 10}{}^{15}*3^3=7\bmod 10$$

לכן סיפרת היחידות:7

ב.האיבר הנייטרלי הוא 0,והפעולה היא חיבור,לכן צריך למצוא את הסדר k של a=35 :

אזי, על פי הנוסחה: "1^{35}" = 35·1 = 35 (כש-1 יוצר את Z_{75}).

לכן 15 = 75/5 = 75/(75,35) = $|1^{35}|$.

<u>שאלה 10</u>

אילו מתת-החבורות הציקליות הבאות הן סופיות (במקרה זה מצאו את מספר האיברים) ואילו מהן אינסופיות:

א) $\left\langle a = cis18^\circ \right\rangle$ ב- $\left(\mathbb{C}^*,\cdot\right)$ (רמז: האם קיים n כך ש- $a^n = 1$?)

ב) $\left\langle a = 1+i \right\rangle$ ב- $\left(\mathbb{C}^*,\cdot\right)$

ג) $\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$ ב- $\left(GL_2\left(\mathbb{R}\right),\cdot\right)$

<u>פתרון:</u>

א) נשים לב ש- $a^{20}=1$ (כי $(cis18)^{20}=cis(18*20)=cis(360)=1$) ולכן מספר האיברים בחבורה ציקלית סופית זו הוא 20.

ב) אם נרשום את a כ- $a = r*cis\alpha$ אז נראה ש- $r \neq 1$ ולכן לא קיים n כך ש- $a^n=1$. ז"א שתת חבורה זו היא אינסופית.

ג) $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \Rightarrow a^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \Rightarrow .....$

ולכן לעולם לא נגיע ל- I_2, ולכן החבורה ציקלית אינסופית.