פתרון תרגיל 3

1 . א) צריך למצוא – עבור כל מספר a מקבוצת המספרים {0,...,11} את ה-k המינימלי כך שאם נחבר את a לעצמו k פעמים, נקבל 0 ב- Z_{12} (זו בדיוק הגדרת הסדר ; כאן הפעולה היא חיבור).
נסמן k זה ב- |a| . לכן –
$|0| = 1, |1|=12, |2| = 6, |3| = 4, |5| = 12, |6| = 2, |7| = 12, |8| = 3, |9| = 4, |10| = 6,$
$|11| = 12$.

ב) נשים לב ש- $u_{12} = \{1,5,7,11\}$ והפעולה פה היא כפל, ז"א – צריך למצוא את החזקה המינימלית k של $a \in u_{12}$ כך ש- $a^k \equiv 1 (\text{mod } 12)$. שוב, נסמן חזקה זו ב- |a|. אזי-
$|1| = 1, |5| = 2, |7| = 2, |11| = 2$.

2. א) סגירות מתקיימת מכיוון שפעולת החיבור סגורה ב-N ולכן $(f+g)(n) = f(n) + g(n) \in N$
אסוציאיטיביות גם כן מתקיימת בגלל האסוציאטיביות של פעולת החיבור ב-N
$$(f+(g+h))(n) = f(n) + (g+h)(n) = f(n) + (g(n) + h(n))$$
ובגלל האסוציטיביות ב- N נקבל:
$$f(n) + (g(n) + h(n)) = (f(n) + g(n)) + h(n) = (f+g)n + h(n) = ((f+g)+h)(n)$$
ומכאן אסוציאטיביות עבור פעולת החיבור מתקיימת ב-A.
נבדוק אם קיים איבר היחידה :
אנחנו מחפשים איבר $e \in A$ כך ש-
$$e + f = f + e = f$$
$$f + e = f \Leftrightarrow (f+e)(n) = f(n) + e(n) \forall n \in N$$
$$f(n) + e(n) = f(n) \Leftrightarrow e(n) = 0$$
(באופן מדויק יותר $f(n) + e(n) = f(n) \Leftrightarrow e(n) = e_N$ - e_N איבר היחידה של N)
וקיבלנו סתירה לכך ש- $e \in A$ מכיוון שאין יחידה חיבורית ב- N.

לכן $(A,+)$ היא **חבורה למחצה**.

ב)
סגירות מתקיימת מכיוון שפעולת החיבור סגורה ב- Z. (הסבר דומה לסעיף א')
אסוציאיטיביות מתקיימת בכלל האסוציאטיביות של פעולת החיבור ב- Z. (הסבר דומה לסעיף א')
איבר היחידה: התנאי שקיבלנו לקיום איבר יחידה עבור פעולת החיבור הוא שאיבר היחידה יהיה קיים בקבוצה אליה אנחנו מעתיקים.
מכיוון שכך קיום איבר יחידה ב- Z, $0 \in Z$ (0 הוא איבר יחידה ב-Z) אומר שקיים איבר יחידה ב-B והוא פונקצית ה"אפס" $e(z) = 0 \forall z \in Z$ ואכן:
$$(f+e)(z) = f(z) + e(z) = f(z) + 0 = f(z) \ \forall z \in Z$$
(התכונה ש- e היא יחידה משמאל נובעת מהקומוטטיביות של Z)
איבר הופכי:
לכל $f \in B$ נגדיר את הפונקציה $(-f): Z \to Z$ ע"י $(-f)(z) = -f(z) \ \forall z \in Z$
לפי הגדרת הפונקציה: $(-f) \in B$
ומתקיים:
$$(f + (-f))(z) = f(z) + ((-f)(z)) = f(z) + (-f(z)) = f(z) - f(z) = 0$$
ומצאנו איבר הופכי לכל $f \in B$

לכן $(B,+)$ היא **חבורה**.

3. א). <u>הטענה:</u> אם x,y איברים בחבורה (G,*) ו- <x> ≠<y> אז |x*y| = |x|·|y|.
<u>דוגמא נגדית:</u> נסתכל על החבורה $(\mathbb{Z}_{18},+\text{mod}18)$. נבחר x=2 ו- y=3. אזי:

$$<2>=\{0,2,4,6,8,10,12,14,16\}$$

$$<3>=\{0,3,6,9,12,15\}$$

ניתן לראות ש: $<2>\neq<3>$, וכן: $|2|=9,|3|=6$, $|2+3|=|5|=18$. ולכן $|2+3|\neq|2|\cdot|3|$
כיוון ש: $18\neq 54$.

ב). <u>הטענה:</u> תהי G חבורה מסדר זוגי. אם $x^3=y^3$ אז x=y.
<u>דוגמא נגדית:</u> נסתכל על החבורה הכיפלית $U_7=\{1,2,3,4,5,6\}$. זוהי חבורה מסדר זוגי.
נבחר: x=1 , y=2. אזי: $1^3=2^3=1(\text{mod}\,7)$, אך $1\neq 2$.

ג). <u>הטענה</u>: תהי G חבורה אבלית מסדר n. אז קיים איבר מסדר n ב-G.
<u>דוגמא נגדית:</u> נסתכל על החבורה הכיפלית $U_{12}=\{1,5,7,11\}$. זוהי חבורה מסדר 4. ומתקיים:
|1| = 1, |5| = 2, |7| = 2, |11| = 2 , ולא קיים איבר מסדר 4.

ד) <u>הטענה</u>: לא קיימת חבורה אינסופית G כך שלכל a∈G מתקיים $a^2=e$. <u>דוגמא נגדית:</u>
ניקח את החבורה $G=\bigtimes_{i=1}^{\infty}(\mathbb{Z}_2,+(\text{mod}\ \ 2))$, ז"א – זו המכפלה הקרטזית של Z_2 עם עצמו אינסוף פעמים. איבריה הם וקטורים אינסופיים $(a_1,a_2,\ldots)$ ולכן G היא חבורה אינסופית. אבל לכל איבר מתקיים

$$(a_1,a_2,\ldots)^2 = (2a_1,2a_2,\ldots)(\text{mod } 2) = (0,0,\ldots) = e_G$$

4. ההוכחה קלה – צ"ל רק סגירות לכפל ולהופכי – לפי חוקי מטריצות, מטריצת הכפל של שתי מטריצות שיש להן דטרמיננטה=1 – גם לה יש דטרמיננטה = 1; כנ"ל להופכי.

5. א) G מוכלת ב $GL_3(Z_3)$ (חבורת המטריצות ההפיכות מסדר 3*3 מעל Z_3). ברור שזוהי קבוצה סופית, לכן נותר לבדוק סגירות לכפל ולהופכי – בדקו זאת ישירות (למעשה מספיק לבדוק רק סגירות לכפל. למה?). 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- Z_3).
ב) לא. החבורה מסעיף א) מהווה דוגמא נגדית.

6. א)+ב) הת"ח הן $\{(0,0)\}$ ו-
$A=\{(0,0),(0,1)\},\quad B=\{(0,0),(1,0)\},\quad C=\{(0,0),(1,1)\}$.

ג) נניח ש $H,K<G$ כך ש $H\cup K=G$. בהכרח לא ייתכן ש $H\subseteq K$ או להיפך (מדוע?) לכן ניקח $a\in H\setminus K$ ו- $b\in K\setminus H$. אם $ab\in H$ אזי $b\in H$ (מדוע?) סתירה, ואם $ab\in K$ אזי $a\in K$, סתירה. לכן $ab\notin H\cup K$ ו- $H\cup K\neq G$.