אלגברה מופשטת 1 – תרגול 3

<u>הגדרה</u>: $\mathrm{U_n} = \{$כל האיברים בין 1 לn כך שk זר ל$n\}$

דוגמה: $\mathrm{U}_{12} = \{1,5,7,11\}\,, |U_{12}| = 4$

שאלה: האם 5 נמצא בU_{10}?

פתרון: לא. 5 מחלק את 10.

הערה: ניתן בקלות להראות ש$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$

ולכן $\varphi\left(p_1^{k_1}p_2^{k_2}\dots p_m^{k_m}\right) = \varphi\left(p_1^{k_1}\right)\cdots\varphi\left(p_m^{k_m}\right) = p_1^{k_1}\dots p_m^{k_m}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_m}\right)$

שאלה: $\varphi(60) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 16$

<u>הגדרה</u>: סדר של חבורה הוא מספר האיברים בחבורה ומסומן ב$|G|$.

<u>הגדרה</u>: סדר של איבר בG הוא $O(a) = \min\{n \in \mathbb{N} | a^n = 1\}$ ואם לא קיים n כזה אז $O(a) = \infty$.

דוגמאות:

1. $U_6 = \{1,5\}, O(1) = 1\,, O(5) = 2$
2. $\mathrm{Gln}(\mathbb{R}), n = 2\,, b = \begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix}, b^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \to O(b) = 3$

הערה: אם G סופית אזי לכל a בG מתקיים: $O(a)|G$.

הערה: בהינתן חבורה סופית מסדר n, אם קיים איבר a בG כך ש$O(a)=n$ אזי G נקראת ציקלית.

דוגמה: $\mathrm{U}_6 = \{1,5\}, |U_6| = 2, O(5) = 2 \to$ U_6 ציקלית

תרגיל: תהי G חבורה $H \leq G$ תת קבוצה סגורה לכפל מגודל סופי ולא ריקה. הוכיחו כי H היא תת חבורה של G.

תזכורת: תת חבורה מקיימת את התנאים הבאים:

1. H מכילה את איבר היחידה
2. H סגורה לכפל
3. H מכילה את ההפכיים של עצמה.

פתרון: נתון שהיא סגורה לכפל, וגם שהיא לא ריקה. נביט באיבר b שבH. נביט בקבוצה $\{b^n : n \in \mathbb{N}\} \subset H$ זו קבוצה סופית, ולכן קיימים n,m: $\mathrm{b}^n = b^m$. אם נכפול את שתי האגפים b^{-m-1} נקבל כי האיבר ההופכי של b הוא $b^{-1} = b^{n-m-1}$.

מצד שני, n-m-1>0 כי אם זה שווה ל0 נקבל שb=1 ואז אין משמעות לחזקות, כולן חוזרות ל1, בסתירה להנחה שלנו.

קיבלנו שלכל איבר בH יש גם את ההופכי שלו.

ראינו גם כי איבר היחידה נמצא בH, כי H סגורה לכפל ולכל מספר יש הופכי, לכן יש גם יחידה. מ.ש.ל. ■

תרגיל: תהי G חבורה אבלית. הוכיח שאוסף האיברים מסר סופי הוא תת חבורה.

פתרון: איבר היחידה מסדר סופי, לכן הוא נמצא וענינו על הקריטריון הראשון.

נביט בשני איברים מסדר סופי a,b בG, ונראה שהמכפלה שלהם מסדר סופי. נניח כי $\mathrm{O(a)} = \mathrm{n}\,, \mathrm{O(b)} = \mathrm{m}$. $(\mathrm{ab})^{\mathrm{nm}} = (a^n)^m (b^m)^n = 1 \cdot 1$.

ניקח איבר מסדר סופי b כך שO(b)=k. מתקיים כי $b^k = 1 = b \cdot b^{k-1} = 1 \to b^{k-1} = b^{-1}$.

והוכחנו כי שלושת התנאים מתקיימים. מ.ש.ל. ■

<u>חיתוך ואיחוד של חבורות</u>

<u>משפט</u>: חיתוך של תת חבורות (לאו דווקא סופי) הוא תת חבורה.

הוכחה: G חבורה $\{\mathrm{H_i}\}_{i \in I}$ אוסף של תתי חבורות. האם $\mathrm{H} = \bigcap_{\mathrm{i \in I}} H_i$. לכל i בו $\mathrm{H_i}$ היא תת חבורה, ולכן איבר היחידה שייך לחיתוך. $a, b \in \bigcap_{i \in I} H_i \to \forall i \in I : a, b \in H_i \to a \cdot b \in H_i \to a \cdot b \in \bigcap_{i \in I} H_i$ והוכחנו סגירות לכפל. כעת נוכיח באופן דומה כי לכל איבר קיים הפיך. נניח *b* שייך לאיחוד $\bigcap_{\mathrm{i \in I}} H_i$ לכן לכל *i* שנבחר $b \in H_i$ אבל $\mathrm{H_i}$ תת חבורה, ולכן $\forall i \in I : b^{-1} \in H_i \to \forall b \in \bigcap_{i \in I} H_i : b^{-1} \in \bigcap_{i \in I} H_i$. והוכחנו כי לכל איבר קיים הופכי. מ.ש.ל. ■.

תרגיל: תנו דוגמה לכך שאיחוד של שתי תתי חבורות הוא לאו דווקא תת חבורה.

פתרון: נביט בחבורה $(\mathbb{Z}_6, +)$. ובתתי החבורות $2\mathbb{Z}_6 = \{0,2,4\}, 3\mathbb{Z}_6 = \{0,3\} \to 2\mathbb{Z}_6 \cup 3\mathbb{Z}_6 = \{0,2,3,4\}$ אבל אין כאן סגירות, כי *3+4* לא בתת חבורה.

תזכורת: בהינתן שתי חבורות *B,A* מגדירים $A \times B = \{(a, b): a \in A, b \in B\}$

$(a, b) \cdot (c, d) = (a \cdot_A c, b \cdot_B d)$.

תרגיל: עבור *n>1* האם $\mathbb{Z}_n \times \mathbb{Z}_n$ ציקלית?

פתרון: הסדר של החבורה הוא n^2, האם קיים איבר מסדר כזה? נבדוק.

צריך להתקיים ש$\mathrm{n(a,b)} = (na, nb) = (0,0) \to O\big((a, b)\big) \le n < n^2$ ולכן היא אינה ציקלית ■.

תרגיל: תהי *G* חבורה, ו*a,b* איברים בה. אם *a,b* מסדר סופי, האם גם המכפלה שלהם $(\mathrm{a \cdot b})$ היא מסדר סופי?

פתרון: באופן כללי התשובה היא לא. חשוב לדעת שבמקרה שמדובר בחבורה אבלית, התשובה היא דווקא כן. מקרה שבו המכפלה של שתי איברים מסדר סופי היא לא מסדר סופי ניתן למצוא בחבורה $G = GL_2(\mathbb{R})$.
נביט במטריצות $\mathrm{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}. O(a) = 4, O(b) = 3. a \cdot b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ואנחנו יודעים שלכל *n* טבעי מתקיים כי $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ ולכן הסדר של המכפלה הוא ∞. מ.ש.ל. ■.

<u>כמה הערות על סדרים</u>:

א. אם *G* חבורה, $g \in G$ עבור *n* טבעי $\mathrm{g^n} = 1$ אז *O(g)|n*.
ב. אם *G=<a>* ציקלית מסדר *n*. אזי לכל *g* ב*G* מתקיים $g^n = 1$.

ג. בחבורה סופית הסדר של איבר הוא סופי.
ד. $O\left(a^i\right) \leq O(a)$
ה. $O(a) = O(a^{-1})$

נוכיח את תכונה (ה׳):

1. נניח כי *O(a)=n* (לא אינסוף). אזי $(a^{-1})^n = (a^n)^{-1} = 1^{-1} = 1$ ונותר להוכיח ש*n* הוא מינימלי. נניח בשלילה ש*n* לא מינימאלי. אזי קיים *n>m* כך ש$1 = (a^{-1})^m = (a^m)^{-1}$. כעת נכפול ב$a^m$ את שני האגפים, ונקבל $\mathrm{a}^{\mathrm{m}} = 1$ בסתירה לכך ש*O(a)=n*.
2. כעת נניח כי $O(a) = \infty$. נניח בשלילה ש$O(a^{-1}) = n < \infty$. ז״א, ע״פ הגדרה ש$(a^{-1})^n = 1$ ואם נכפול בשתי האגפים ב a^{n} נקבל כי $\mathrm{a}^{\mathrm{n}} = 1$ בסתירה להנחה.

מ.ש.ל. ■