

תרגיל 4 – אלגברה מופשטת 1

1. ענו על הסעיפים הבאים:

1.1 כמה חבורות אבליות מסדר 1323 קיימות, עד כדי איזומורפיזם?
תשובה: $1323 = 3^3 \cdot 7^2$. לכן מספר החבורות האבליות מסדר 1323, עד כדי איזומורפיזם הוא: $\rho(3)\rho(2) = 3 \cdot 2 = 6$.

1.2 בכמה מהן יש איבר מסדר 49?
תשובה: יש איבר מסדר 49 אם ורק אם Z_{49} מופיע בפירוק. יש $\rho(3) = 3$ חבורות כאלה. (כש Z_{49} מופיע בפירוק, כל מה שנשאר לקבוע הוא החלק המתאים ל 3^3).

1.3 בכמה מהן יש איבר מסדר 147?
תשובה: ב-3 מהן.
הסבר: אם בחבורה G יש איבר a מסדר 147 אזי $\langle a \rangle$ חבורה ציקלית מסדר 147 והיא מכילה איבר מסדר $49 \mid 147$.
מצד שני, אם בחבורה כנ"ל יש איבר a מסדר 49, אזי מכיוון ש $3 \mid 1323$, (לפי משפט קושי או לפי הפירוק לחבורות ציקליות) קיים איבר b מסדר 3. מכיוון ש G אבלית ו $(3,49) = 1$, $o(ab) = 3 \cdot 49 = 147$ ולכן קיים בחבורה איבר מסדר 147.
בסה"כ החבורות הנ"ל המכילות איבר מסדר 147 הן בדיוק אלה המכילות איבר מסדר 49. לכן מספרן הוא 3.

1.4 מצאו את מספר החבורות האבליות מסדר 6860 (עד כדי איזומורפיזם). בכמה מהן יש חבורה 7-סילו ציקלית?
תשובה: $6860 = 2^2 \cdot 5 \cdot 7^3$. לכן יש $2 \cdot 1 \cdot 3 = 6$ חבורות אבליות מסדר 6860. ת"ח 7-סילו תהיה ציקלית אם ורק אם, הגורם Z_{343} מופיע בפירוק. יש $\rho(2)\rho(1) = 2 \cdot 1 = 2$ כאלה, עד כדי איזומורפיזם.

2. תהי $G = C_5 \times C_{25} \times C_{625}$. קבעו מהו מספר האיברים מכל סדר ב G .
פתרון:

לפני תחילת השאלה נשים לב לשתי העובדות הבאות:

* בחבורה ציקלית G מסדר n , מספר האיברים שסדרם מחלק את m עבור $m \mid n$ הוא m . הוכחה: $m \mid n$ לכן $|G| = n$. מכיוון ש G ציקלית, קיימת ב G תת חבורה יחידה מסדר m , נסמנה H . ממשפט לגרנז' ברור כי הסדר של כל איבר ב H מחלק את m . נראה שגם ההפך נכון. יהי $a \in G$ כך ש $o(a) \mid m$, אזי $\langle a \rangle$ ת"ח מסדר $o(a)$. אבל H חבורה ציקלית (כת"ח של חבורה ציקלית) מסדר m ו $o(a) \mid m$ לכן קיימת ל H ת"ח $M \leq H$ מסדר $o(a)$. אבל M ו $\langle a \rangle$ תתי חבורות של G מסדר m . לכן, לפי משפט המיזן של תתי חבורות של חבורות ציקליות, $\langle a \rangle = M \leq H$ ו $a \in H$. לכן האיברים שסדרם מחלק את m הם בדיוק אברי H וכאלה יש m .

* יהיו G, H, K חבורות. אזי, הסדר של $(a, b, c) \in G \times H \times K$ מחלק n טבעי כלשהו אמ"ם. $o(a), o(b), o(c) \mid n$.

הוכחה: נניח $o(a, b, c) \mid n$ אזי $(a, b, c)^n = (a^n, b^n, c^n) = (e, e, e)$ לכן $o(a), o(b), o(c) \mid n$.

בכיוון ההפוך, אם $o(a), o(b), o(c) | n$, אז $(a^n, b^n, c^n) = (e, e, e)$ ו $(a, b, c)^n = (e, e, e)$.

כעת, ניגש לפתרון השאלה.

נשים לב, לכל $(x_1, x_2, x_3) \in G$ מתקיים $(x_1, x_2, x_3)^{625} = (x_1^{625}, x_2^{625}, x_3^{625}) = (1, 1, 1)$ לכן, הסדר של כל איבר ב G מחלק את 625. לכן, הסדרים היחידים האפשריים לאיברים מ G הם: 1, 5, 25, 125, 625. נבדוק כמה איברים יש מכל סדר כזה.

*איבר היחידה הוא האיבר היחיד מסדר 1.

* כל איבר מסדר המחלק את 5 הוא מהצורה (x_1, x_2, x_3) כש $o(x_i) | 5$ לכל $1 \leq i \leq 3$. לפי עובדה א', בכל אחת מהחבורות C_5, C_{25}, C_{625} מספר האיברים שסדרם מחלק את 5 הוא 5. לכן, מספר האיברים $(x_1, x_2, x_3) \in G$ שסדרם מחלק את 5 הוא 5^3 . נוריד את האיבר היחיד מסדר 1, ונקבל: מספר האיברים מסדר 5 הוא $5^3 - 1 = 124$.

* כל איבר מסדר המחלק את 25 הוא מהצורה (x_1, x_2, x_3) כש $o(x_i) | 25$ לכל $1 \leq i \leq 3$. דרישה זו לא מגבילה את בחירת x_1, x_2 . לגבי x_3 , לפי עובדה א' יש 25 איברים ב C_{625} שסדרם מחלק את 25. לכן, מספר האיברים שסדרם מחלק את 25 הוא: $5 \times 25 \times 25 = 5^5$. נוריד את האיברים שסדרם מחלק את 5 ונקבל: מספר האיברים מסדר 25 הוא: $5^5 - 5^3 = 3000$.

* כל איבר מסדר המחלק את 125 הוא מהצורה (x_1, x_2, x_3) כש $o(x_i) | 125$ לכל $1 \leq i \leq 3$. דרישה זו לא מגבילה את בחירת x_1, x_2 . לגבי x_3 , לפי עובדה א' יש 125 איברים ב C_{625} שסדרם מחלק את 125. לכן, מספר האיברים שסדרם מחלק את 125 הוא: $5 \times 25 \times 125 = 5^6$. נוריד את האיברים שסדרם מחלק את 25 ונקבל: מספר האיברים מסדר 125 הוא: $5^6 - 5^5 = 12500$.

* לפי האמור בהתחלה, כל האיברים שסדרם לא מחלק את 125, סדרם 625. לכן, מספר האיברים מסדר 625 הוא: $5 \times 25 \times 625 - 5^6 = 5^7 - 5^6 = 62500$.

3. הוכיחו או הפריכו:

3.1. קיימת חבורה פשוטה G מסדר 20.

הפרכה: $20 = 2^2 \cdot 5$ לכן הסדר של G הוא מהצורה p^2q עבור p, q ראשוניים. עפ"י משפט מהתרגול, G אינה פשוטה.

3.2. קיימת חבורה פשוטה G מסדר 30.

הפרכה: תהי G מסדר 30. נראה כי G אינה פשוטה. $30 = 2 \cdot 3 \cdot 5$

לפי משפט סילו 3, מספר ת"ח 5-סילו של G מקיים $n_5 = 1 + 5k | 6$. לכן, $n_5 = 1$ או $n_5 = 6$. אם $n_5 = 1$ אזי P_5 חבורת 5-סילו, נורמלית ב G ו אינה פשוטה. לכן, נניח $n_5 = 6$. הוא מספר ראשוני לכן החיתוך בין שתי חבורות שונות

מסדר 5 הוא טריוויאלי. לכן, חבורות ה-5 סילו תורמות, מעבר לאיבר היחידה, ארבעה איברים כל אחת. בסה"כ הן מכילות $25 = 1 + 6 \cdot 4$ איברים. לפי משפט סילו 3, מספר ת"ח 3-סילו של G מקיים $n_3 = 1 + 3k \mid 10$. לכן, $n_3 = 1$ או $n_3 = 10$. אם $n_3 = 1$ אזי $P_3 \triangleleft G$ כאשר P_3 חבורת 3-סילו ו- G אינה פשוטה. לכן, מ"ל $n_3 = 1$. נניח בשלילה $n_3 = 10$. אזי, מכיוון ש $(3,5) = 1$ אין איברים, למעט הזהות, המשותפים לחבורת 3-סילו וחבורת 5-סילו. בנוסף מכיוון ש 3 ראשוני החיתוך של כל שתי חבורות 3 סילו הוא טריוויאלי. לכן, מספר האיברים בחבורות 3-סילו לא כולל הזהות הוא $20 = 10 \cdot 2$. בסה"כ קיימים לפחות $20 + 25$ איברים שונים ב G בסתירה לכך ש G מסדר 30. לכן, $n_3 = 1$. מש"ל.

3.3. תהי G חבורה מסדר 55 כך שיש בה יותר מארבעה איברים מסדר 5, אזי G אינה אבלית.

הוכחה: $|G| = 55 = 5 \cdot 11$ לכן חבורת 5-סילו ב G היא מסדר 5. כעת, כל איבר מסדר 5 שייך לחבורה מסדר 5. אבל חבורה מסדר 5 מכילה רק ארבעה איברים מסדר 5 (ואת איבר הזהות). לכן, מהקיום של חמישה איברים מסדר 5, נובע הקיום של יותר מחבורה אחת מסדר 5, דהיינו יותר מחבורת 5-סילו אחת. לכן, כל חבורת 5-סילו ב G אינה נורמלית. אבל, בחבורה אבלית כל תת חבורה היא נורמלית, לכן G אינה אבלית.

4. ענו על הסעיפים הבאים:

4.1. מצאו את כל החבורות מסדר 637, עד כדי איזומורפיזם.

פתרון: $637 = 7^2 \cdot 13$. תהי G חבורה מסדר 637. לפי משפט סילו, מספר חבורות 7-סילו n_7 מקיים $n_7 = 1 + 7k \mid 13$. לכן, $n_7 = 1$ ו-תת החבורה 7-סילו P_7 נורמלית. באופן דומה, מספר חבורות 13-סילו n_{13} מקיים $n_{13} = 1 + 13k \mid 49$. לכן, $n_{13} = 1$ ו-תת החבורה 13-סילו P_{13} נורמלית. מכיוון ש $|P_7| = 7^2$ ו- $|P_{13}| = 13$ ראשוני, P_7 ו- P_{13} אבליות.

מכיוון ש P_7 ו- P_{13} תת חבורות נורמליות, $P_7 P_{13} \leq G$ ו- $P_7, P_{13} \triangleleft P_7 P_{13}$. מכיוון ש $|P_7|$ ו- $|P_{13}|$ זרים, $P_7 \cap P_{13} = \{e\}$ לכן (מכיוון ש $P_7 \cdot P_{13} = P_7 P_{13}$) לפי משפט פיצול חבורות $P_7 P_{13} \cong P_7 \times P_{13}$ חבורה אבלית כמכפלה של חבורות אבליות. אבל $P_7 P_{13} \leq G$ ו- $|P_7 P_{13}| = 7^2 \cdot 13 = |G|$ לכן, $P_7 P_{13} = G$ ו- G אבלית. לכן לפי משפט הפיצול של חבורות אבליות סופיות החבורות מסדר $637 = 7^2 \cdot 13$ עד כדי איזומורפיזם הן החבורות: $Z_{49} \times Z_{13} \cong Z_{637}$ ו- $Z_7 \times Z_7 \times Z_{13}$.

4.2. מצאו את כל החבורות מסדר 34, עד כדי איזומורפיזם.

פתרון: $34 = 2 \cdot 17$. לפי משפט מהתרגול החבורות היחידות מסדר $2p$ עבור p ראשוני הן Z_{2p} ו- D_p , לכן החבורות היחידות מסדר 34 הן Z_{34} ו- D_{17} .

4.3. מצאו את כל החבורות מסדר 121 עד כדי איזומורפיזם.

פתרון: כל חבורה מסדר $121 = 11^2$ היא אבלית (מכיוון שסדרה הוא ריבוע של מספר ראשוני). לכן, לפי פיצול חבורות אבליות החבורות היחידות, עד כדי איזומורפיזם, מסדר 121 הן Z_{121} ו- $Z_{11} \times Z_{11}$.

4.4. מצאו את כל החבורות מסדר 35, עד כדי איזומורפיזם. **פתרון:** $35 = 5 \cdot 7$ מכיוון ש $7 \not\equiv 1 \pmod{5}$ לפי משפט מהתרגול חבורה מסדר 35 היא בהכרח ציקלית. לכן החבורה היחידה מסדר 35, עד כדי איזומורפיזם היא Z_{35} .

5. (שאלה ממבחן מועד א', קיץ 2004)

לתכשיט בצורת מגן דוד יש שישה משולשים בקצוות. ניתן לצבוע כל משולש באחד משלושה צבעים נתונים. כמה תכשיטים שונים כאלה אפשר לייצר אם ניתן לסובב את התכשיט ולהפכו?

פתרון: צריך לספור את המסלולים השונים עד כדי פעולת החבורה D_6 . ניתן לבנות אותה כך:

נמספר את המשולשים בקצוות ב- 1,2,3,4,5,6 ואז: $D_6 = \langle a, b \rangle$ כאשר:

$$b = (1,2,3,4,5,6) \text{ ו- } a = (2,6)(3,5)(1,4) \text{ . נקבל:}$$

$$b^2 = (1,3,5)(2,4,6) \quad b^3 = (1,4)(2,5)(3,6) \quad b^4 = (1,5,3)(2,6,4) \quad b^5 = (1,6,5,4,3,2)$$

$$ab = (1,6)(2,5)(3,4) \quad ab^2 = (1,5)(2,4)(3,6) \quad ab^3 = (1,4)(2,3)(5,6)$$

$$ab^4 = (1,3)(4,6)(2,5) \quad ab^5 = (1,2)(3,6)(4,5)$$

נרשום את הטבלה הבאה:

type	$g \in type$	$\# g \in type$	$ X_g $	סה"כ
(1)(2)(3)(4)(5)(6)	id	1	3^6	$3^6 = 729$
(a,b,c,d,e,f)	b, b^5	2	3	$2 \cdot 3 = 6$
$(a,b,c)(d,e,f)$	b^2, b^4	2	3^2	$2 \cdot 3^2 = 18$
$(a,b)(c,d)(e,f)$	b^3, ab, ab^3, ab^5	4	3^3	$4 \cdot 3^3 = 108$
$(a,b)(c,d)(e)(f)$	a, ab^2, ab^4	3	3^4	$3 \cdot 3^4 = 243$

$$.k = \frac{1}{12}(729 + 6 + 18 + 108 + 243) = 92 \text{ :Burnside משפט}$$

6. (הוכחה אלטרנטיבית למשפט קושי)

תהי G חבורה סופית ויהי p ראשוני המחלק את סדר החבורה. נגדיר,

$$X = \{(g_1, g_2, \dots, g_p) \in G \times G \times \dots \times G : g_1 g_2 \dots g_p = e\}$$

ותהי C חבורה ציקלית מסדר p הנוצרת ע"י איבר c .

6.1. הוכיחו כי p מחלק את $|X|$.

הוכחה: איבר (g_1, g_2, \dots, g_p) שייך ל X אם ורק אם, $\cdot g_p = (g_1 g_2 \dots g_{p-1})^{-1}$

כלומר $X = \{(g_1, g_2, \dots, g_{p-1}, (g_1 g_2 \cdots g_{p-1})^{-1}) \in G \times G \times \dots \times G : g_1, g_2, \dots, g_p \in G\}$
 לכן $|X| = |G|^{p-1}$ (מספר האפשרויות לכל אחד מהאיברים g_i עבור $1 \leq i \leq p-1$, הוא $|G|$). מכיון ש p מחלק את $|G|$, הוא מחלק את $|X|$.

6.2. הוכיחו כי קיימת פעולה יחידה של C על X כך ש $c \cdot (g_1, \dots, g_p) = (g_2, \dots, g_p, g_1)$

הוכחה: יחידות: מכיון ש c הוא היוצר של C קביעת הפעולה של c על X קובעת

את הפעולה של כל C על X . אכן, כל $h \in C$ ניתן להבעה בצורה $h = c^n$ עבור $n \in \mathbb{N}$ כלשהו (שימו לב ש C סופית). לכן, לפי אסוציאטיביות הפעולה,

$$h \cdot (g_1, \dots, g_p) = c^n \cdot (g_1, \dots, g_p) = c \cdot (c \cdot (\dots \cdot c \cdot (g_1, \dots, g_p)))$$

X נקבעה באופן יחיד. לכן, אם קיימת פעולה כ"ל היא יחידה.

קיום: נגדיר פעולה של C על X ע"י $c^n \cdot (g_1, \dots, g_p) = (g_{1+n}, \dots, g_{p+n})$ לכל $n \in \mathbb{N}$ כאשר האינדקסים נלקחים מודולו p . הפונקציה המתוארת מ $C \times X$ ל X מוגדרת

$$(g_1, g_2, \dots, g_p) \in X$$

$$\cdot (g_2, \dots, g_p, g_1) \in X \Leftrightarrow g_1 = (g_2 \cdots g_p)^{-1} \Leftrightarrow g_1 g_2 \cdots g_p = e$$

ובאינדוקציה על $n \in \mathbb{N}$ נקבל $(g_{1+n}, \dots, g_{p+n}) \in X$.

בנוסף, אם $c^n = c^k$ אז $c^{n-k} = e$ ו $n-k \mid o(c) = p$. לכן $n = k + dp$ ומתקיים

$$c^k \cdot (g_1, \dots, g_p) = (g_{1+k}, \dots, g_{p+k}) = (g_{1+k+dp}, \dots, g_{p+k+dp}) = (g_{1+n}, \dots, g_{p+n}) = c^n \cdot (g_1, \dots, g_p)$$

מכיון שהאינדקסים נלקחים מודולו p .

$$\text{ברור כי } e \cdot (g_1, \dots, g_p) = c^p \cdot (g_1, \dots, g_p) = (g_{1+p}, \dots, g_{p+p}) = (g_1, \dots, g_p) \text{ וכן,}$$

$$c^k \cdot (c^l \cdot (g_1, \dots, g_p)) = c^k \cdot (g_{1+l}, \dots, g_{p+l}) = (g_{1+l+k}, \dots, g_{p+l+k}) = (g_{1+k+l}, \dots, g_{p+k+l}) = c^{k+l} \cdot (g_1, \dots, g_p)$$

לכן, זוהי פעולה של C על X .

6.3. הוכיחו שבכל מסלול בפעולה הזו יש איבר יחיד או p איברים.

הוכחה: הסדר של כל מסלול מחלק את $|C| = p$.

6.4. מצאו מסלול בעל איבר יחיד עבור פעולה זו.

$$[(e, e, \dots, e)] = \{(e, \dots, e)\} \text{ תשובה:}$$

6.5. הראו כי קיים עוד מסלול בעל איבר יחיד עבור פעולה זו.

הוכחה: מספר המסלולים בעלי איבר יחיד הוא מספר נקודות השבת של הפעולה.

מכיון ש C חבורת p - מספר נקודות השבת של הפעולה $|F|$ מקיים

$$|X| \equiv |F| \pmod{p} \quad (|X| \text{ מתחלק ב } p) \text{ אבל ראינו } |F| \geq 1 \text{ לכן}$$

$|F| \geq p \geq 2$. לכן יש לפחות עוד מסלול אחד בעל איבר יחיד.

6.6. הסיקו שב G יש איבר מסדר p .

הוכחה: יהי $(g_1, g_2, \dots, g_p) \neq (e, e, \dots, e)$ השייך למסלול בעל איבר יחיד. אזי

$$c \cdot (g_1, \dots, g_p) = (g_2, \dots, g_p, g_1) = (g_1, \dots, g_p) \text{ מכיון ש}$$

$$g_1 = g_2 = \dots = g_p \text{ לכן, } c \cdot (g_1, \dots, g_p) = (g_2, \dots, g_p, g_1) = (g_1, \dots, g_p) \text{ ומכיון ש } g_1^p = g_1 g_2 \cdots g_p = e, (g_1, \dots, g_p) \in X$$

7. תהי G חבורה מסדר 12 ויהיו n_2 ו n_3 מספר חבורות ה-2-סילו וה-3-סילו בהתאמה.

7.1. מהם ערכי n_2 האפשריים? (הביאו דוגמאות לכך שכל הערכים המדוברים אכן אפשריים).

תשובה: נשים לב $|G| = 2^2 \cdot 3$. לפי משפט סילו 3, $3 \mid n_2 = 1 + 2k$ לכן $n_2 = 1$ או $n_2 = 3$.

נראה כי שני הערכים אפשריים.
 * עבור $G = Z_{12}$ $|G| = 12$ ול G יש רק חבורת 2-סילו אחת (אחרת חבורת 2-סילו לא תהיה נורמלית, בסתירה לכך שת"ח של חבורה אבלית בהכרח נורמלית).
 * עבור $G = D_6$ $|G| = 12$. ל G יש יותר מחבורת 2-סילו אחת שכן כל איבר מסדר 2 שייך לחבורת 2-סילו (הוא יוצר חבורת 2-זו בתורה מוכלת בחבורת 2-סילו). אבל כל חבורת 2-סילו ב G היא מסדר ארבע ויש יותר מארבעה איברים מסדר 2 ב G (כל ששת השיקופים הם מסדר 2). לכן, חייב להתקיים $n_2 = 3$.

7.2. מהם ערכי n_3 האפשריים? (שוב, הביאו דוגמאות).

תשובה: לפי משפט סילו 3, $3 \mid n_3 = 1 + 3k$ לכן $n_3 = 1$ או $n_3 = 4$. נראה כי שני הערכים אפשריים.

* עבור $G = Z_{12}$ $|G| = 12$ ול G יש רק חבורת 3-סילו אחת (אחרת חבורת 3-סילו לא תהיה נורמלית, בסתירה לכך שת"ח של חבורה אבלית בהכרח נורמלית).
 * עבור $G = A_4$ $|G| = 12$. ב G יש 8 איברים מסדר 3 (העגילים באורך 3). כל אחד מהם שייך לחבורת 3-סילו. לכן, קיימת יותר מחבורת 3-סילו אחת, (שאם לא כן ב G היו רק שני איברים מסדר 3). לכן, חייב להתקיים $n_3 = 4$.

7.3. האם יתכן ש $n_2 = 3$ ו $n_3 = 4$?

תשובה: לא. הוכחה: נראה כי אם $n_3 = 4$ אז $n_2 = 1$. נניח כי $n_3 = 4$. הוא מספר ראשוני לכן החיתוך בין שתי חבורות שונות מסדר 3 הוא טריוויאלי. לכן, חבורות ה-3-סילו תורמות, מעבר לאיבר היחידה, שני איברים כל אחת. בסה"כ הן מכילות $9 = 1 + 4 \cdot 2$ איברים. הסדר של כל האיברים שספרנו, למעט הזהות, הוא 3. בסה"כ נשארו $3 = 12 - 9$ איברים. כעת, קיימת לפחות חבורת 2-סילו אחת. אבל חבורת 2-סילו היא מסדר 4 וכל האיברים בה אינם מסדר 3. לכן היא חייבת להכיל את הזהות ואת שלושת האיברים שלא ספרנו. אבל, זה נכון לכל חבורת 2-סילו, לכן כל חבורות ה-2-סילו זהות, דהיינו קיימת חבורת 2-סילו יחידה.

7.4. הראו כי $n_2 = n_3 = 1$ אם ורק אם G אבלית.

הוכחה: אם G אבלית אז כל תת חבורה שלה היא נורמלית, בפרט $n_2 = n_3 = 1$ (חבורת p -סילו נורמלית אמ"ם $(n_p = 1)$. בכיוון השני, אם $n_2 = n_3 = 1$ אז חבורת 2-סילו $P_2 \triangleleft G$ וחבורת 3-סילו $P_3 \triangleleft G$. מכיוון ש $P_2 \triangleleft G$ ו $P_3 \triangleleft G$ $P_2 P_3 \leq G$ (ואפילו ת"ח נורמלית). מתקיים $P_2, P_3 \triangleleft P_2 P_3$, $P_2 \cap P_3 = \{e\}$ (מכיוון ש $(|P_2|, |P_3|) = (4, 3) = 1$ ו $P_2 \cdot P_3 = P_2 P_3$). לכן לפי משפט פיצול חבורות, $P_2 P_3 \cong P_2 \times P_3$. אבל P_2 היא מסדר $4 = 2^2$ ולכן אבלית. בדומה P_3 אבלית (ואפילו ציקלית) מכיוון שסדרה ראשוני. לכן $P_2 P_3 \cong P_2 \times P_3$ אבלית כמכפלה קרטזית של חבורות אבליות. לסיים נשים לב כי $P_2 P_3 \leq G$ כך ש $|G| = |P_2 P_3| = |P_2 \times P_3| = 4 \cdot 3 = 12 = |G|$, לכן, $P_2 P_3 = G$ ו G אבלית.

8. נתבונן בחבורה S_7 .

8.1. הוכיחו כי $S_7 = \langle (12...7), (54) \rangle$.

הוכחה: ראינו בתרגול כי $S_7 = \langle (12...7), (12) \rangle$ לכן מ"ל $(12) \in \langle (12...7), (54) \rangle$.
 אבל, $(12...7)^{-1}(45)(12...7) = (7...21)(45)(7...21)^{-1} = (34) \in \langle (12...7), (54) \rangle$,
 כעת, $(12...7)^{-1}(34)(12...7) = (7...21)(34)(7...21)^{-1} = (21) \in \langle (12...7), (54) \rangle$ לכן
 $S_7 = \langle (12...7), (12) \rangle \subseteq \langle (12...7), (54) \rangle$ ו $(12) \in \langle (12...7), (54) \rangle$
 כלומר $S_7 = \langle (12...7), (54) \rangle$.

8.2. מצאו את מספר מחלקות הצמידות ב S_7 . מהו הגודל של כל אחת מהן?
פתרון: מספר מחלקות הצמידות ב S_7 הוא מספר הטיפוסים של תמורות על הקבוצה $\{1, \dots, 7\}$ שהוא $\rho(7) = 15$.

8.3. כמה איברים ב S_7 מתחלפים עם $a = (125)$?

פתרון: נתבונן ב S_7 הפועלת על עצמה ע"י הצמדה. $\sigma * \beta = \sigma\beta\sigma^{-1}$.
 גודל הדרוש הוא הסדר של המייצב של $a = (125)$ ביחס לפעולת ההצמדה:
 $|Stb(a)| = |\{\sigma \in S_7 : \sigma * a = a\}| = |\{\sigma \in S_7 : \sigma a \sigma^{-1} = a\}| = |\{\sigma \in S_7 : \sigma a = a \sigma\}|$
 אבל $|Stb(a)| = \frac{|S_7|}{|[a]|}$ כאשר $|[a]|$ הוא גודל המסלול של a , דהיינו גודל מחלקת הצמידות של a . אבל, מחלקת הצמידות של a מכילה בדיוק את כל התמורות הניתנות להצגה כעגיל מאורך 3. יש $2! = 70$ תמורות כאלה, לכן
 $|Stb(a)| = \frac{|S_7|}{|[a]|} = \frac{5040}{70} = 72$. כלומר, מספר האיברים המתחלפים עם $a = (125)$ הוא 72.

9. ענו על הסעיפים הבאים.

9.1. תהי G חבורה בת 35 איברים. הוכיחו כי G פתירה.
הוכחה: $|G| = 35 = 3 \cdot 5$ וראינו בתרגול כי כל חבורה מסדר pq עבור p, q ראשוניים פתירה.

9.2. תהי G חבורה בת 125 איברים. האם בהכרח G פתירה?
תשובה: כן. $|G| = 5^3$ לכן G חבורת p עבור $p = 5$. לפי משפט, כל חבורת p פתירה.

9.3. תהי G חבורה מסדר 77. זהו את כל תתי החבורות שלה, עד כדי איזומורפיזם.
פתרון: $|G| = 7 \cdot 11$, לכן לפי משפט לגרנד' אם $H \leq G$ אזי $|H| \in \{1, 7, 11, 77\}$. ברור כי ל G יש תת חבורה יחידה מסדר 1 - $\{e\}$ ותת חבורה יחידה מסדר 77 - G .
 לפי משפט סילו קיימת ל G תת חבורה P_7 מסדר 7. בנוסף $11 \mid 77$ לכן $n_7 = 1$ כלומר, קיימת ת"ח יחידה מסדר 7. מכיוון ש 7 ראשוני לכן $P_7 \cong Z_7$. בדומה, קיימת ת"ח יחידה מסדר 11 $(n_{11} = 1 + 11k \mid 77)$, ומכיוון ש 11 ראשוני $P_{11} \cong Z_{11}$.

בסה"כ עד כדי איזומורפיזם תתי החבורות של G הן $\{e\}, Z_7, Z_{11}, G$.
 לחילופין, שימו לב כי $11 \not\equiv 1 \pmod{7}$, לכן לפי משפט מהתרגול G היא ציקלית. לכן
 כל תתי החבורות שלה הן ציקליות וקיימת לה תת חבורה יחידה מכל סדר המחלק
 את 77. בסה"כ, עד כדי איזומורפיזם תתי החבורות שלה הן Z_1, Z_7, Z_{11}, Z_{77} .

9.4. תתי G חבורה מסדר 4081. הוכיחו כי G ציקלית.
הוכחה: $|G| = 7 \cdot 11 \cdot 53$. נסמן ב n_p את מספר חבורות ה p סילו שלה.
 לפי משפט סילו 3, $n_{53} = 1 + 53k \mid 77$, לכן, $n_{53} = 1$. בדומה, $n_{11} = 1 + 11k \mid 371$, לכן
 $n_{11} = 1$. $n_7 = 1 + 7k \mid 583$. מכיוון ש $n_7 = n_{11} = n_{53} = 1$ תתי החבורות
 המתאימות נורמליות. מכיוון שמדובר בסדרים ראשוניים הן גם ציקליות. נסמן:
 $P_7 = \langle a \rangle, P_{11} = \langle b \rangle, P_{53} = \langle c \rangle$.
 טענה: היוצרים של שלוש תתי החבורות הנ"ל מתחלפים ביניהם.
 הוכחה: נראה את זה עבור היוצרים a, b . לגבי השאר, ניתן להוכיח באופן דומה.
 מתקיים $aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in P_{11}$ כי P_{11} נורמלית. בדומה,
 $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in P_7$ כי P_7 נורמלית. לכן $o(aba^{-1}b^{-1}) \mid 11$ וכן
 $o(aba^{-1}b^{-1}) \mid 7$ $\Leftrightarrow o(aba^{-1}b^{-1}) = 1$. לכן $aba^{-1}b^{-1} = e$ ו $ab = ba$. מש"ל.
 כעת, a, b, c הם שלושה איברים בחבורה שמתחלפים ביניהם וכן הסדרים שלהם
 זרים בזוגות לכן, $o(abc) = o(a)o(b)o(c) = 4081$, ולכן $G = \langle abc \rangle$ והחבורה היא
 ציקלית.

10. (שאלה ממבחן מועד ב', קיץ 2009)

נתייחס לחבורה הסימטרית S_p כאשר p הוא מספר ראשוני.
10.1. כמה איברים מסדר p יש בחבורה?
תשובה: כיוון ש- p הוא ראשוני, איבר מסדר p בתוך S_p יכול להיות רק עגיל באורך
 p . כאלו יש $(p-1)!$.

10.2. חשבו באמצעות סעיף א' את מספר תתי החבורות מסדר p בתוך S_p .
תשובה: כיוון שכל החבורות מסדר ראשוני הן זרות עד כדי איבר היחידה, סך האיברים
 שהן תורמות הוא: $1 + n_p(p-1)$ כאשר n_p הוא מספר תתי-החבורות מסדר p . כל
 איבר בת"ח שכזו, למעט הזהות, הוא מסדר p (שוב כיוון ש- p ראשוני) וכל איבר
 מסדר p שייך לתת חבורה כזו (התת חבורה שהוא יוצר היא מסדר p) לכן, אם נוסיף
 גם את איבר היחידה נקבל: $1 + n_p(p-1) = 1 + (p-1)!$. לכן, $n_p = (p-2)!$.

10.3. בעזרת סעיף ב' ומשפט סילו השלישי הוכיחו כי $(p-1)! \equiv (p-1) \pmod{p}$.
 (האם זה מוכר לכם כאחד המשפטים?)
הוכחה: לפי משפט סילו 3, $n_p \equiv 1 \pmod{p}$ לכן $(p-2)! \equiv 1 \pmod{p}$. נכפול את שני
 האגפים ב $(p-1) \pmod{p}$ ונקבל $(p-1)! \equiv (p-1) \pmod{p}$.
 שימו לב: זה אחד הכיוונים במשפט ווילסון.

11. (שאלה ממבחן מועד א', קיץ 2006)

מעל קבוצה $R \times R^*$ נגדיר פעולה $(a_1, b_1) \bullet (a_2, b_2) = (a_1 + b_1 a_2, b_1 b_2)$. הוכיחו:

11.1. $G = (R \times R^*, \bullet)$ חבורה.

הוכחה: *סגירות: יהיו $(a,b), (c,d) \in R \times R^*$ אזי $(a,b) \bullet (c,d) = (a+bc, bd) \in R \times R^*$ (סגור לכלל וחיבור ו R^* סגור לכפל).

אסוציאטיביות: יהיו $(a,b), (c,d), (f,g) \in R \times R^$ אזי:

$$((a,b) \bullet (c,d)) \bullet (f,g) = (a+bc, bd) \bullet (f,g) = (a+bc+ bdf, bdg)$$

$$(a,b) \bullet ((c,d) \bullet (f,g)) = (a,b) \bullet (c+df, dg) = (a+b(c+df), bdg) = (a+bc+ bdf, bdg)$$

$$\Rightarrow ((a,b) \bullet (c,d)) \bullet (f,g) = (a,b) \bullet ((c,d) \bullet (f,g))$$

איבר נייטרלי: נראה ש $e = (0,1)$ איבר נייטרלי של G . יהי $(a,b) \in R \times R^$ אזי

$$(a,b) \bullet (0,1) = (a+b \cdot 0, b \cdot 1) = (a,b) \quad , \quad (0,1) \bullet (a,b) = (0+1 \cdot a, 1 \cdot b) = (a,b)$$

הופכי: נראה כי לכל איבר $(a,b) \in R \times R^$, $(-a/b, 1/b)$ הופכי משמאל.

(ואז, מכיוון שכל איבר הפיך משמאל, כל איבר הפיך).

$$(-a/b, 1/b) \bullet (a,b) = (-a/b + (1/b) \cdot a, (1/b) \cdot b) = (0,1) = e$$

11.2. G אינה אבלית.

$$(1,2) \bullet (3,5) = (7,10) \neq (8,10) = (3,5) \bullet (1,2) \quad \text{הוכחה:}$$

11.3. קיים מונומורפיזם $G \rightarrow GL_2(R)$.

$$\text{הוכחה: נגדיר } f : G \rightarrow GL_2(R) \text{ ע"י } f(a,b) = \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix}$$

שימו לב כי מכיוון ש $b \in R^*$, $\begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} \in GL_2(R)$ ו f מוגדרת היטב.

נראה כי f הוא מונומורפיזם.

שמירת פעולה: לכל $(a,b), (c,d) \in G$ מתקיים:

$$f((a,b) \bullet (c,d)) = f((a+bc, bd)) = \begin{pmatrix} bd & a+bc \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & c \\ 0 & 1 \end{pmatrix} = f((a,b)) f((c,d))$$

לכן f הומו.

חח"ע: ברורה מההגדרה והגדרת השוויון בין מטריצות.

לכן f הוא מונומורפיזם.

11.4. G חבורה פתירה.

הוכחה: נשים לב f מהסעיף הקודם הוא מונומורפיזם. לכן, ע"י צמצום הטווח נקבל איזו':

$$f : G \rightarrow \text{Im}(f) = \left\{ \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} \mid a, b \in R \right\} \leq GL_2(R)$$

נסמן $H = \text{Im}(f)$, אזי $G \cong H$, לכן, G פתירה אם ורק אם H פתירה.

נראה כי H פתירה באמצעות חישוב קומוטטורים.

$$\text{לכל } A = \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} d & c \\ 0 & 1 \end{pmatrix}, A, B \in H \text{ נחשב את הקומוטטור:}$$

$$[A, B] = ABA^{-1}B^{-1} = \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{b} & -\frac{a}{b} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{d} & -\frac{c}{d} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} bd & a+bc \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{bd} & -\frac{a}{b} - \frac{c}{bd} \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -ad - c + a + bc \\ 0 & 1 \end{pmatrix}$$

כלומר כל קומוטטור הוא מהצורה $[A, B] = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ עבור $x \in R$ כלשהו.

אבל לכל $x, y \in R$, $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, לכן כל שני קומוטטורים מתחלפים.

לכן, H' הנוצרת ע"י הקומוטטורים, אבליה (אם היוצרים של ת"ח מתחלפים – החבורה אבליה).

לכן $H'' = \{e\}$, פתירה וכך גם G .

12. (שאלה ממבחן מועד א', קיץ 2006)

נסמן $[a, b] := aba^{-1}b^{-1}$ ("הקומוטטור") של $a, b \in G$ בחבורה G .
נגדיר ת"ח $G' := \langle \{[a, b] : a, b \in G\} \rangle \leq G$ הנוצרת ע"י קבוצת הקומוטטורים.

הוכיחו:

12.1. $G' \triangleleft G$.

הוכחה: מהגדרתה, $G' \leq G$. נוכיח נורמליות. יהיו $g \in G$, $h \in G'$, מ"ל $ghg^{-1} \in G'$.
כך $h \in G' = \langle \{[a, b] : a, b \in G\} \rangle$

$$h = A_1^{k_1} A_2^{k_2} \cdots A_n^{k_n} \text{ ש}$$

נראה תחילה שלכל קומוטטור A , $gAg^{-1} \in G'$. אכן, יהי $A = [a, b]$ קומוטטור אזי,

$$gAg^{-1} = g[a, b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) =$$

$$(gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} = [gag^{-1}, gbg^{-1}] \in G'$$

בנוסף, לכל חזקה $n \in \mathbb{Z}$ של A ,

$$(gAg^{-1})^n = (gAg^{-1})(gAg^{-1}) \cdots (gAg^{-1}) = gA^n g^{-1} \in G'$$

$$\text{לכן, } ghg^{-1} = gA_1^{k_1} A_2^{k_2} \cdots A_n^{k_n} g^{-1} = (gA_1^{k_1} g^{-1})(gA_2^{k_2} g^{-1}) \cdots (gA_n^{k_n} g^{-1}) \in G'$$

בגלל הסגירות של G' .

12.2. G/G' אבליה.

הוכחה: יהיו $aG', bG' \in G/G'$. צ"ל $aG'bG' = bG'aG'$ אבל $aG'bG' = abG'$ ו $bG'aG' = baG'$, לפי משפט לגרנד', מתקיים שוויון אם ורק אם $abG' = baG'$, אבל $(ba)^{-1}(ab) \in G'$, אבל $[a^{-1}, b^{-1}] \in G'$, לכן $aG'bG' = bG'aG'$ ו G' אבליה.

12.3. אם $f : G \rightarrow Y$ הומומורפיזם ו Y חבורה אבליה אז $f \subseteq \ker f$.

הוכחה: נתון Y אבליה. כמו כן f הומומורפיזם. לכן:

$$\forall g_1, g_2 \in G: f(g_1) \cdot f(g_2) = f(g_2) \cdot f(g_1)$$

⇔

$$f(g_1 g_2) = f(g_2 g_1)$$

⇔

$$f(g_1 g_2 g_1^{-1} g_2^{-1}) = e_Y$$

כלומר: $\forall g_1, g_2 \in G: [g_1, g_2] \in \ker(f)$ ומתוך הסגירות של $\ker(f)$ מתקבל שהנגזרת: $G' = \langle \{ [g_1, g_2] \mid g_1, g_2 \in G \} \rangle$ מוכלת ב- $\ker(f)$.

13. (בונוס – 10 נק')

תהי G חבורה סופית, p מספר ראשוני ו $P \leq G$ תת חבורת - p . נתון כי $P = N(P)$. הוכיחו כי P חבורת - p סילו.

הדרכה: התבוננו ב P הפועלת על קבוצת תתי החבורות הצמודות ל P ב G , באמצעות הצמדה.

הוכחה: נניח בשלילה כי $P \neq N(P)$ ו P אינה חבורת - p סילו של G .

תהי $\text{conj}_G(P) := \{gPg^{-1} : g \in G\}$ קבוצת כל תתי החבורות הצמודות ל P ב G . פעולת ההצמדה $G \times \text{conj}_G(P) \rightarrow \text{conj}_G(P)$ המוגדרת ע"י $g * H = gHg^{-1}$ היא טרנזיטיבית

(שכן המסלול של P הוא $\text{conj}_G(P)$). לכן, $|\text{conj}_G(P)| = [P] = \frac{|G|}{|Stb(P)|}$ אבל

$$|\text{conj}_G(P)| = \frac{|G|}{|P|} \text{ לכן } P = N(P) = Stb(P) \text{ מתחלק ב } p \text{ שכן } P \text{ אינה חבורת } -p$$

סילו של G .

נתבונן בצמצום של הפעולה לחבורה P . כלומר P פועלת על $\text{conj}_G(P)$ באמצעות הצמודות. לפי משפט מההרצאה, מכיוון ש P חבורת- p מספר נקודות השבת $|F|$ של פעולה זו מקיים $|F| \equiv |\text{conj}_G(P)| \pmod{p} \equiv 0 \pmod{p}$.

ברור כי P נקודת שבת של פעולה זו. לכן $|F| > 1$. מכיוון ש $|F| \equiv 0 \pmod{p}$ יש לפחות $p \geq 2$ נקודות שבת. תהי $Q \in \text{conj}_G(P)$ נקודת שבת כך ש $Q \neq P$.

Q נקודת שבת לכן לכל $h \in P$, $hQh^{-1} = Q$. כלומר $P \leq N(Q)$. אבל $Q \in \text{conj}_G(P)$

משמעו Q צמוד ל P ב G . כלומר, קיים $g \in G$ כך ש $Q = gPg^{-1} = g * P$

לפי משפט מההרצאה: $Stb_G(Q) = gStb_G(P)g^{-1}$ כאשר $Stb_G(H)$ הוא המייצב של H

ב G ביחס לפעולה הנ"ל. אבל $Stb_G(H) = N(H)$ לכן:

$$N(Q) = Stb_G(Q) = gStb_G(P)g^{-1} = gN(P)g^{-1} = gPg^{-1} = Q$$

בסה"כ $P \leq N(Q) = Q$ תת חבורה מאותו סדר סופי של Q (מכיוון ש P, Q צמודות) לכן $P = Q$. בסתירה להנחה.

לכן P חבורת - p סילו של G .

14. (בונוס – 5 נק')

מצאו את ה- $n > 1$ הקטן ביותר שאינו ראשוני עבורו כל החבורות מסדר n איזומורפיות. **פתרון:** לכל מספר טבעי n קיימת חבורה ציקלית מסדר n . לכן עלינו למצוא $n > 1$ טבעי

לא ראשוני כך שכל חבורה מסדר n היא ציקלית.

אם n זוגי לא ראשוני ($n \neq 2$) אזי קיימת חבורה לא ציקלית מסדר $n - D_{n/2}$.
 אם ב n יש גורם ראשוני בחזקה הגדולה מאחת – כלומר $n = p^2 r$ עבור p
 ראשוני (כש p, r לא בהכרח זרים) אזי, החבורה $Z_p \times Z_p \times Z_r$ היא חבורה לא ציקלית
 מסדר $n = p^2 r$ (כל איבר בחבורה זו הוא מסדר pr לכל היותר).
 לכן, n הוא אי זוגי לא ראשוני שבפירוק שלו לראשוניים אין אף ראשוני החזקה גדולה
 מאחת.
 המספר הקטן ביותר מסוג זה הוא $n = 15$.
 בנוסף, אם $|G| = 15 = 3 \cdot 5$, אזי לפי משפט מהתירגול, מכיוון ש $5 \not\equiv 1 \pmod{3}$, G
 ציקלית. לכן $n = 15$ הוא המספר המבוקש.

בהצלחה! 😊