תרגיל 3 – אלגברה מופשטת

1. תהי G חבורה ויהי $a \in G$. הגדנו $< a > = \{a^k : k \in Z\} \le G$.

1.1 הוכיחו כי אם $o(a) = n$ אז $< a > = \{1, a, ..., a^{n-1}\}$ והאיברים $1, a, ..., a^{n-1}$ שונים זה מזה.

הוכחה:

נראה כי $< a > = \{1, a, ..., a^{n-1}\}$ באמצעות הכלה דו כיוונית.

ברור, מהגדרת $< a >$ כי $< a > \supseteq \{1, a, ..., a^{n-1}\}$.

עבור ההכלה בכיוון ההפוך, יהי $a^k \in < a >$ עבור $k \in Z$ כלשהו.

נחלק את k ב n עם שארית ונקבל ש $k = qn + r$ עבור $0 \le r < n$.

נשים לב, $a^k = a^{qn+r} = (a^n)^q a^r = ea^r = a^r$. מכיוון ש $0 \le r < n$,
$a^k = a^r \in < a >$.

כעת, נותר להראות כי האיברים $1, a, ..., a^{n-1}$ שונים זה מזה.

נניח בשלילה כי קיימים $0 \le i < j \le n-1$ כך ש $a^i = a^j$. אזי $a^{j-i} = e$
למרות ש $1 \le j - i < n$ בסתירה לכך ש $o(a) = n$.

1.2 הוכיחו כי (בכל מקרה) הסדר של a שווה לסדר של החבורה שהוא יוצר.

הוכחה: אם הסדר של a סופי, זה נובע מיידית מסעיף 1.1

נניח כי $o(a) = \infty$ ונוכיח כי $< a > = \{a^k : k \in Z\}$ היא אינסופית. מ"ל כי לכל $m, n \in Z$ שונים, $a^m \ne a^n$.

אבל, אם עבור $m < n$, $a^m = a^n$ אז $a^{n-m} = e$ בסתירה לכך ש $o(a) = \infty$.

לכן, כל אברי $< a > = \{a^k : k \in Z\}$ שונים זה מזה והחבורה אינסופית.

2. פתרו את המשוואה $(123)^2 x = (12)(132)^{-1}$.

פתרון:

$$(132)^{-1}=(312)$$
$$(12)(132)^{-1}=(12)(312)=(32)$$
$$(123)^{2}=(123)(123)=(132)$$
$$\Rightarrow (132)x=(32)$$
$$(132)^{-1}=(312)$$
$$x=(312)(32)=(21)$$

3. ענו על הסעיפים הבאים.

3.1 הוכיחו שבחבורת הסימטריה S_n כל שני מחזורים זרים מתחלפים זה עם זה.

פתרון: נניח שקיימים טבעיים r,l ו- $i_1,i_2\dots i_r,i_{r+1},i_{r+2},\dots i_{r+l}$ איברים שונים בין 1 ל-n. נתבונן בתמורות $\sigma=(i_{r+1}\,i_{r+2}\dots i_{r+l})(i_1\,i_2\dots i_r)$, $\tau=(i_1\,i_2\dots i_r)(i_{r+1}\,i_{r+2}\dots i_{r+l})$. קל לראות שאם $1\le k\le r-1$ או $r+1\le k\le r+l-1$ אז $\tau(i_k)=\sigma(i_k)=i_{k+1}$ וכן $\tau(i_{r+l})=\sigma(i_{r+l})=i_{r+1}$, $\tau(i_r)=\sigma(i_r)=i_1$. כמו כן כל ערך אחר בין 1 ל-n הוא נקודת שבת של τ וגם של σ. מכאן $\tau=\sigma$ והמחזורים הזרים מתחלפים.

3.2 הוכיחו שאם α,β הם מחזורים זרים, אזי $ord(\alpha\beta)=lcm(ord(\alpha),ord(\beta))$.

הוכחה: נסמן $ord(\alpha)=n, ord(\beta)=m$, $k=lcm(ord(\alpha),ord(\beta))$. תחילה נשים לב שמתקיים $(\alpha\beta)^k=\alpha^k\beta^k=id$ (מדוע?) ולכן $ord(\alpha\beta)\le k$. נוכיח את אי-השוויון ההפוך. נניח שמתקיים $(\alpha\beta)^t=id$, אזי $\alpha^t\beta^t=id$ ולכן $\alpha^t=\beta^t=id$ (מדוע?) ומכאן $n|t\wedge m|t$. לכן, לפי הגדרת lcm נקבל $k\le t$.

3.3 תהי G חבורה ויהו $a,b\in G$ איברים מתחלפים. נניח כי $o(a)=n,o(b)=m$ כאשר m,n מספרים זרים. הוכיחו כי $o(ab)=nm$.

הוכחה: נוכיח:

1. $(ab)^{nm}=e$
2. (מינימליות:) אם $d\in N$ מקיים כי $(ab)^d=e$ אז $nm\le d$.

הוכחה: 1. מכיוון ש a,b איברים מתחלפים,

$(ab)^{nm}=a^{nm}b^{nm}=(a^n)^m(b^m)^n=ee=e$.

2. יהי $d\in N$ המקיים $(ab)^d=e$. אזי $a^db^d=e \Leftarrow a^d=b^{-d}$.

טענה: $a^d=e$.

הוכחה: $o(a^d)=\frac{n}{(n,d)}$ ובפרט, $o(a^d)\,|\,n$.

$o(b^{-d})=\frac{m}{(m,-d)}$ ובפרט $o(b^{-d})\,|\,m$.

לכן, $o(a^d)$ מחלק את m,n. מכך נובע שהוא מחלק את $(n,m)=1$ (נתון כי m,n זרים). לכן, $o(a^d)=1$ ו $a^d=e$. ברור כי גם $b^d=e$.

מכיוון ש $o(a)=n, o(b)=m$, $m\,|\,d, n\,|\,d$. מכיוון ש m,n זרים, נובע כי

$mn\,|\,d$

(הוכיחו) ובפרט $mn\le d$.

4. ענו על הסעיפים הבאים.

4.1 בחבורה S_8 מצאו איברים מסדר $4,7,12,15,19,20$. אם אין איבר מסדר מסויים, הסבירו מדוע.

פתרון: $o\big((123)(45678)\big)=15$, $o\big((123)(4567)\big)=12$, $o(1234567)=7$, $o(1234)=4$. אין איבר מסדר 19, שכן 19 הינו מספר ראשוני. אם היה קיים איבר מסדר 19, בפירוק שלו למחזורים זרים היה חייב להופיע מחזור מאורך 19 וזה כמובן לא ייתכן.
אין איבר מסדר 20. הסבר: נניח שיש לנו איבר מסדר 20. ניתן לכתוב אותו כמכפלה של מחזורים זרים. על מנת שה- lcm של הסדרים יהיה 20, חייב להופיע בפירוק מחזור באורך 5 (כי צריך כפולה של 5, ו-10 הוא גדול מדי). בנוסף, צריך שיהיה מחזור מאורך 4. אבל שני מחזורים זרים, אחד מאורך 4 ואחד מאורך 5, דורשים שימוש ב-9 מספרים שונים, ואין 9 מספרים שונים ב- S_8.

4.2 הוכיחו שהמחזורים $(13524),(12345)\in S_6$ מתחלפים, על אף שאינם זרים.

פתרון: קל לראות שמתקיים $(12345)(13524)=(14253)=(13524)(12345)$.

5. ענו על הסעיפים הבאים.

5.1 כתבו את לוח הכפל של החבורה הדיהדרלית D_3.

פתרון:

$\bullet$	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
e	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	e	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	e	σ	$\sigma^2\tau$	τ	$\sigma\tau$
τ	τ	$\sigma^2\tau$	$\sigma\tau$	e	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	e	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	e

5.2 תהי $H=\langle(14),(13)\rangle$ תת חבורה של S_4. רשמו את לוח הכפל שלה והוכיחו שהיא איזומורפית ל D_3. כתבו את האיזומורפיזם בצורה מפורשת.

פתרון: $H=<e,(14),(13),(143),(134),(34)>$.

לוח הכפל של H הוא:

$\bullet$	e	(134)	(143)	(13)	(14)	(34)
e	e	(134)	(143)	(13)	(14)	(34)
(134)	(134)	(143)	e	(14)	(34)	(13)
(143)	(143)	e	(134)	(34)	(13)	(14)
(13)	(13)	(34)	(14)	e	(143)	(134)
(14)	(14)	(13)	(34)	(134)	e	(143)
(34)	(34)	(14)	(13)	(143)	(134)	e

לכן, ההתאמה: $\begin{matrix} \tau \leftrightarrow (13) \\ \sigma \leftrightarrow (134) \end{matrix}$

וההתאמות הנובעות מכך: $\begin{matrix} (e \leftrightarrow e) \\ \sigma^2 \leftrightarrow (143) \\ \sigma\tau \leftrightarrow (14) \\ \sigma^2\tau \leftrightarrow (34) \end{matrix}$

נותנות איזומורפיזם. אכן, אם נחליף כל איבר בטבלה של D_3 באיבר המתאים לו, נקבל את טבלת הכפל של החבורה H.

6. ענו על הסעיפים הבאים:

6.1 הוכיחו שחבורת קליין, כלומר תת חבורה של S_4 המוגדרת על-ידי $V = K_4 = \langle (12)(34),(13)(24) \rangle$, איזומורפית ל U_8.

פתרון: החבורה הנתונה מורכבת מארבעה איברים:
$V = \{id,(12)(34),(13)(24),(14)(23)\}$. דוגמה לאיזומורפיזם אפשרי $f: V \to U_8$:

$f(id)=1$, $f((12)(34))=3,\ f((13)(24))=5,\ f((14)(23))=7$ (ויש לבדוק שזהו אכן איזומורפיזם).
שימו לב, שהחבורות V,U_8 שתיהן איזומורפיות ל- $Z_2\times Z_2$.

6.2 רשמו את איברי תת החבורה של S_6 הנוצרת על ידי שני האיברים $(145)(263),(15)(36)$.

פתרון: האיברים הם: $\{id,(145)(263),(15)(36),(154)(236),(26)(45),(14)(23)\}$.

7. תהי G חבורה ו $H\subseteq G$ תת קבוצה לא ריקה הסגורה לכפל.

7.1 הוכיחו כי אם H סופית אז $H\le G$.

הוכחה: לפי הקריטריון המקוצר מ"ל כי H סגורה להופכי (נתון כי היא לא ריקה וסגורה לכפל).

יהי $b\in H$ ועלינו להראות שקיים לו הופכי ב- H. נתבונן ב- $A=\{b^n : n\in\mathbb{N}\}\subseteq H$. מכיוון ש- $|H|<\infty$ גם A קבוצה סופית ולכן קיימים m,n (נניח בה"כ כי $m>n$) כך ש- $b^m=b^n$. מתקיים $bb^{m-n-1}=b^{m-n}=e$.

לכן $b^{-1}=b^{m-n-1}\in H$ ויש סגירות לגבי הופכי ב- H.

7.2 האם סעיף 7.1 נכון בהינתן כי H אינסופית?

תשובה: לא. למשל, עבור $G=(Z,+)$ תת הקבוצה הלא ריקה $H=N$ סגורה לחיבור. מכיוון שהיא לא סגורה להופכי H אינה תת חבורה.

בהצלחה! ☺