תרגיל 2 – אלגברה מופשטת 1

1. מצאו את קבוצה המנה G/H של החבורות G לגבי תת החבורות H.

1.1 $G=Z$, $H=5Z$.

פתרון:

$$G/H=\{gH \mid g\in G\}=\{0+5Z,1+5Z,2+5Z,3+5Z,4+5Z\}=\{[0],[1],[2],[3],[4],[5]\}=Z_5$$

1.2 $G=(R^2,+)$, $H=\{0\}\times R$.

פתרון:

$$G/H=\{gH \mid g\in G\}=\{(a,b)+\{0\}\times R \mid (a,b)\in R^2\}=\{\{(a,b)+(0,x)\mid x\in R\}\mid (a,b)\in R^2\}$$
$$=\{\{(a,x+b)\mid x\in R\}\mid (a,b)\in R^2\}=\{\{(a,y)\mid y\in R\}\mid (a,b)\in R^2\}=\{\{(a,y)\mid y\in R\}\mid a\in R\}$$

נשים לב: זוהי בדיוק קבוצת הישרים המקבילים לציר ה y.

1.3 $G=(R^2,+)$, $H=\{(t,4t)\mid t\in R\}$.

פתרון:

$$G/H=\{gH \mid g\in G\}=\{(a,b)+H \mid (a,b)\in R^2\}=\{\{(a,b)+(t,4t)\mid t\in R\}\mid (a,b)\in R^2\}$$
$$=\{\{(a+t,b+4t)\mid t\in R\}\mid (a,b)\in R^2\}\overset{x=a+t}{=}\{\{(x,b+4(x-a))\mid l\in R\}\mid (a,b)\in R^2\}$$
$$=\{\{(x,4x+b-4a)\mid l\in R\}\mid (a,b)\in R^2\}\overset{c=b-4a}{=}\{\{(x,4x+c)\mid x\in R\}\mid c\in R\}$$

נשים לב: זוהי בדיוק קבוצת הישרים המקבילים בעלי שיפוע 4.

1.4 $G=U_{30}$, $H=\{1,11\}$.

פתרון:

נשים לב: $U_{30}=\{1,7,11,13,17,19,23,27\}$ ו $H\leq G$ ($11^2=1 \bmod 30$)

לפי משפט לגרנז',

$$[G:H]=\frac{|G|}{|H|}=\frac{8}{2}=4$$

הקוסטים השמאליים:

$$1H=\{1,11\},7H=\{7,17\},13H=\{13,23\},19H=\{19,29\}$$

הם ארבעה קוסטים שונים זה מזה.

לכן,

$$G/H=\{\{1,11\},\{7,17\},\{13,23\},\{19,29\}\}$$

(שימו לב, איחוד כל הקוסטים השמאליים, אכן שווה ל G).

1.5 $G=S_n$, $H=A_n$.

פתרון: על פי משפט לגרנז',

$$[G:H]=\frac{|G|}{|H|}=\frac{n!}{n!/2}=2$$

וכן, אחד הקוסטים השמאליים הוא $eH=H$.

מכיוון ש G/H היא איחוד זר של שני קוסטים:

$G/H=\{H,H^c\}$.

1.6. $G=(C^*,\cdot)$, $H = \{z \in C \mid \|z\| = 1\}$.

פתרון:

$$C/H=\{xH \mid x\in C^*\}=\{x\{z\in C \mid \|z\|=1\}\mid x\in C^*\}=\{\{xz\in C \mid \|z\|=1\}\mid x\in C^*\}$$
$$=\{\{y\in C \mid \|y\|=\|x\|\}\mid x\in C^*\}=\{\{y\in C \mid \|y\|=\|x\|\}\mid x\in R_+\}$$

נשים לב: זוהי קבוצת כל המעגלים סביב ראשית הצירים.

2. הוכיחו:

2.1. תהי G חבורה, $H,K\le G$ תתי חבורות מסדר m,n בהתאמה. הוכיחו: אם $(m,n)=1$ אזי $H\cap K=\{e\}$.

הוכחה:

$$H\cap K\le H,K$$

לכן, לפי משפט לגרנז',

$$|H\cap K|\,\big|\,|H|=m \quad , \quad |H\cap K|\,\big|\,|K|=n$$
$$\Rightarrow |H\cap K|\,\big|\,(m,n)=1$$
$$\Rightarrow |H\cap K|=1$$
$$\Rightarrow H\cap K=\{e\}$$

2.2. תהי G חבורה כך ש $|G|<60$, קיים $a\in G$ מסדר 5 ו $S_3\le G$. מצאו את הסדר של G.

פתרון: קיים $a\in G$ מסדר 5. לכן, לפי מסקנה ממשפט לגרנז', $5\,\big|\,|G|$.

בנוסף, מכיוון ש $S_3\le G$ ת"ח מסדר 6, $6\,\big|\,|G|$.

מכיוון ש $(5,6)=1$, $5\cdot 6=30\,\big|\,|G|$. אבל, $|G|<60$, לכן $|G|=30$.

3. הוכיחו:

3.1. אם G חבורה אבלית ו $a,b\in G$ איברים מסדר m,n בהתאמה כך ש $(m,n)=1$, אזי $o(ab)=mn$.

הוכחה:

$$(ab)^{mn}=a^{mn}b^{mn}=(a^m)^n(b^n)^m=e^ne^m=e$$

לכן: מ"ל מינמליות. יהא $t\in N$ כך ש $(ab)^t=e$. אזי,

$$(ab)^t=e\Rightarrow a^tb^t=e\Rightarrow a^t=b^{-t}\Rightarrow a^t\in\langle a\rangle\cap\langle b\rangle$$

אבל, $\langle a\rangle$ חבורה מסדר m ו $\langle b\rangle$ חבורה מסדר n ו $(m,n)=1$. לכן, לפי השאלה הקודמת, $\langle a\rangle\cap\langle b\rangle=\{e\}$.

לכן, $a^t=e$ ו $o(a)=m\mid t$.

בדומה, $b^t=a^{-t}=e$, לכן $o(b)=n\mid t$.

בסה"כ $[m,n]=mn\mid t$. לכן, $mn\le t$. מש"ל.

3.2. אם G חבורה אבלית מסדר 6 אז G חבורה ציקלית.

רמז: אם G חבורה מסדר זוגי אז קיים $a\in G$ מסדר 2.

הוכחה: מ"ל: קיים איבר מסדר 6 ב G. נניח בשלילה, כי לא קיים איבר כנ"ל.

לפי משפט לגרנז', לכל $a\in G$, $o(a)\,\|\,|G|$, כלומר $o(a)\in\{1,2,3,6\}$.

לפי התזכורת ברמז, קיים איבר $a \in G$, $o(a)=2$.
אם קיים איבר $b \in G$ כך ש $o(b)=3$, אזי לפי סעיף א', $o(ab)=6$ בסתירה להנחה.
לכן, לא קיימים איברים מסדר 3 ב G .
בסה"כ, לכל $c \in G$ שאינו הזהות, $o(c)=2$.
בפרט, יהי $c \neq a$ מסדר 2 . אזי,

$$< a,c >= \{e,a,c,ac\} \text{ (בדקו)}$$

תת חבורה של G מסדר 4 , בסתירה למשפט לגרנז' (שכן 4 לא מחלק את $|G|=6$).
מש"ל.

4. ענו על הסעיפים הבאים:

4.1 חשבו $197^{81} \bmod 34$.
פתרון:
$197 \equiv 27 \bmod 34$ לכן $197^{81} \equiv 27^{81} \bmod 34$.
$(27,34)=1$, לכן, $27 \in U_{34}$ ולפי משפט אוילר: $27^{\varphi(34)} \equiv 1 \bmod 34$.
נחשב, $\varphi(34)=\varphi(2)\varphi(17)=1\cdot 16=16$. לכן, $27^{16} \equiv 1 \bmod 34$ ו

$$197^{81} \equiv 27^{81} \bmod 34 \equiv 27^{16\cdot 5+1} \bmod 34 = (27^{16})^5 27 \bmod 34 \equiv 1\cdot 27 \bmod 34 \equiv 27 \bmod 34$$

4.2 מצאו את שתי הספרות האחרונות של $20087853^{199}+876$.
פתרון: נחשב, $20087853^{199} \bmod 100 = 53^{199} \bmod 100$.
$(53,100)=1$, לכן, $53 \in U_{100}$ ולפי משפט אוילר: $53^{\varphi(100)} \equiv 1 \bmod 100$.
נחשב, $\varphi(100)=100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=40$. לכן, $53^{40} \equiv 1 \bmod 100$ ו

$$53^{199} \equiv 53^{40\cdot 5-1} \bmod 100 \equiv (53^{40})^5 53^{-1} \bmod 100 \equiv 1\cdot 53^{-1} \bmod 100 \equiv 53^{-1} \bmod 100$$

נשים לב, מכיוון ש $53 \in U_{100}$, $53^{-1} \bmod 1$ מוגדר היטב.
נמצא את $53^{-1} \bmod 100$ באמצעות אלגוריתם אוקלידס המוכלל.

$$(100,53) \underset{\substack{100=1\cdot 53+47\\ 47=100-1\cdot 53}}{=} (53,47) \underset{\substack{53=1\cdot 47+6\\ 6=53-1\cdot 47\\ 6=53-1\cdot(100-1\cdot 53)\\ 6=-1\cdot 100+2\cdot 53}}{=} (47,6) \underset{\substack{47=7\cdot 6+5\\ 5=47-7\cdot 6\\ 5=(100-1\cdot 53)-7\cdot(-1\cdot 100+2\cdot 53)\\ 5=8\cdot 100-15\cdot 53}}{=} (6,5) \underset{\substack{6=1\cdot 5+1\\ 1=6-1\cdot 5\\ 1=(-1\cdot 100+2\cdot 53)-1\cdot(8\cdot 100-15\cdot 53)\\ 1=-9\cdot 100+17\cdot 53}}{=} 1$$

לכן,

$$17\cdot 53-9\cdot 100=1 \Rightarrow 17\cdot 53 \equiv 1 \bmod 100 \Rightarrow 53^{-1} \equiv 17 \bmod 100$$

בסה"כ, $20087853^{199} \bmod 100 \equiv 17 \bmod 100$ ו

$$(20087853^{199}+876) \bmod 100 = 17+76 \bmod 100 = 93 \bmod 100$$

לכן, שתי הספרות האחרונות של המספר הנתון הן, 93 .

5. יהיו X,Y חבורות ו $f: X \to Y$ הומומורפיזם. תהי $H \lhd X$ ת"ח נורמלית. הוכיחו כי $f(H)$ ת"ח נורמלית של $f(X)$. האם בהכרח $f(H) \lhd Y$?

הוכחה: לכל $G \le X$, $f(G) \le f(Y)$. לכן, מ"ל נורמליות של $f(H)$ ב $f(X)$.
יהיו $g \in f(X), y \in f(H)$ מ"ל $gyg^{-1} \in f(H)$.
אבל, $g \in f(X), y \in f(H) \Leftarrow$ קיימים $x \in X, h \in H$ כך ש $g=f(x), y=f(h)$.
מהנורמליות של H ב X , $xhx^{-1} \in H$. לכן, $f(xhx^{-1}) \in f(H)$.

לכן, $f(xhx^{-1}) = f(x)f(h)f(x)^{-1} \in H$. מש"ל.
נראה כי לא בהכרח $f(H) \lhd Y$.
דוגמה נגדית: יהיו $Y = D_3$ ו $H = X =< \tau >= \{e,\tau\}$. נגדיר $f: X \to Y$ את ההעתקת ההכלה, $f(x) = x$. נשים לב, $H \lhd X$ מכיוון שחבורה תמיד נורמלית בעצמה ואילו, $f(H) = H$ אינה תת חבורה נורמלית של $Y = D_3$.
(אכן, עבור $\sigma \in Y$, $\tau \in f(H) = H$ $f(H) \not\ni \sigma\tau\sigma^{-1} = \tau\sigma^2\sigma^{-1} = \tau\sigma$).

6. הוכיחו את הטענות הבאות:

6.1 אם $H \leq G$ אז לכל $g \in G$, $gHg^{-1} \leq G$ ת"ח מסדר $|H|$.
הוכחה: יהי $g \in G$, אזי:

$$*\ e \in H \Rightarrow geg^{-1} = e \in gHg^{-1} \Rightarrow H \neq \phi$$

$$*\ x_1, x_2 \in gHg^{-1} \Rightarrow \exists h_1, h_2 \in H: \quad x_1 = gh_1g^{-1}, x_2 = gh_2g^{-1}$$
$$\Rightarrow x_1x_2^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1}) = g(h_1h_2^{-1})g^{-1} \in gHg^{-1}$$

לכן $gHg^{-1} \leq G$.
נתבונן בהעתקה: $x \mapsto gxg^{-1}$ מ H ל gHg^{-1} .
מ"ל כי ההעתקה הנ"ל חח"ע ועל.
מהגדרתה ברור כי היא על. בנוסף, אם $gxg^{-1} = gyg^{-1}$ עבור $x, y \in H$, מצמצום נקבל, $x = y$. לכן, ההעתקה הנ"ל היא גם חח"ע והסדר של gHg^{-1} שווה לסדר של H .

6.2 אם $K \leq H \lhd G$ ו H חבורה ציקלית סופית אז $K \lhd G$.
הוכחה: מ"ל כי לכל $g \in G$, $gKg^{-1} = K$.
מכיוון ש H נורמלית ב G , לכל $g \in G$, $gKg^{-1} \leq gHg^{-1} = H$.
לכן, $gKg^{-1} \leq H$ מאותו הסדר של $K \leq H$.
מכיוון ש H חבורה ציקלית סופית, לא קיימות ב H תתי חבורות שונות מאותו הגודל.
לכן, $gKg^{-1} = K$. מש"ל.

7. תהי $D_4 =< \sigma, \tau >$ החבורה הדיהדרלית מסדר 4 , כש $o(\sigma) = 4, o(\tau) = 2$.
נגדיר: $H = \{e, \tau\sigma, \sigma^2, \tau\sigma^3\}$, $K = \{e, \tau\sigma\}$. הוכיחו כי $H \lhd D_4$ ו $K \lhd H$ אבל K אינה ת"ח נורמלית של D_4 .
הוכחה: $|D_4| = 8$, $|H| = 4$ ו $|K| = 2$. לכן, $[D_4 : H] = 2, [H : K] = 2$ ת"ח מאינדקס 2.
לכן, $H \lhd D_4$ ו $K \lhd H$.
נראה כי K אינה ת"ח נורמלית של D_4 .
מ"ל: קיימים $k \in K$ ו $d \in D_4$ כך ש $dkd^{-1} \notin K$.
ניקח $d = \sigma, k = \tau\sigma$ ונקבל: $dkd^{-1} = \sigma\tau\sigma\sigma^{-1} = \sigma\tau = \tau\sigma^3 \notin K$.

8. יהיו H, K תתי חבורות של G . הוכיחו:

8.1 $KH = HK$ כקבוצות, אם ורק אם $HK \leq G$.
הוכחה: $(\Leftarrow)$ $e \in H, K \Leftarrow e = ee \in HK$. יהיו $x, y \in HK$, מ"ל $xy^{-1} \in HK$.
$x, y \in HK$, לכן קיימים $h_1, h_2 \in H, k_1, k_2 \in K$ כך ש $x = h_1k_1, y = h_1k_1$.

לכן, $xy^{-1} = h_1k_1k_2^{-1}h_2^{-1} \in HKKH = HKH = HHK = HK$.
(שימו לב כי עבור חבורה G, $GG = G$).
$(\Rightarrow)$ עבור $X \subseteq G$ נסמן $X^{-1} = \{a^{-1} \mid a \in X\}$. נשים לב, אם $X \le G$ אזי $X^{-1} = X$.
בפרט, $H, K, HK \le G$ לכן: $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$.

8.2 אם $H \lhd G$ אזי $HK \le G$. אם גם $K \lhd G$, אזי $HK \lhd G$.
הוכחה: אם $H \lhd G$ אזי לכל $g \in G$ $gH = Hg$. בפרט, לכל $k \in K$ $kH = Hk$. ו
$KH = \bigcup_{k \in K} kH = \bigcup_{k \in K} Hk = HK$. לכן, לפי הסעיף הקודם, $KH \le G$.
אם בנוסף $K \lhd G$, צ"ל $HK \lhd G$. יהיו $hk \in HK$, $g \in G$. מ"ל $ghkg^{-1} \in HK$.
אבל, מהנורמליות של H, K ב G: $ghkg^{-1} = (ghg^{-1})(gkg^{-1}) \in HK$.

8.3 קיימת חבורה G ותתי חבורות $H, K \le G$ שאינן נורמליות כך ש $HK \le G$.
הוכחה: נתבונן ב $G = D_3$, $H = K = \langle \tau \rangle = \{id, \tau\}$. ראינו כי H ו K ת"ח לא נורמליות של G . אבל, $HK = HH = H \le G$.

9. הוכיחו או הפריכו את הטענות הבאות:

9.1 קיים מונומורפיזם $f : GL_2(R) \to (R^{16}, +)$.
הפרכה: נניח בשלילה כי קיים מונומורפיזם $f : GL_2(R) \to (R^{16}, +)$.
נתבונן בצמצום של f, $f : GL_2(R) \to \mathrm{Im}(f)$. אזי,

$$GL_2(R) \cong \mathrm{Im}(f) \le (R^{16}, +)$$

אבל $\mathrm{Im}(f) \le (R^{16}, +)$ אבלית ואילו $GL_2(R)$ אינה אבלית. סתירה להיותן איזומורפיות.

9.2 קיים מונומורפיזם $f : D_7 \to S_5$.
הפרכה: נשים לב: $|S_5| = 5! = 120$ ו $|D_7| = 2 \cdot 7 = 14$.
נניח בשלילה כי קיים מונומורפיזם $f : D_7 \to S_5$ אזי מכיוון ש f חח"ע,
$14 = |\mathrm{Im}(f)| = |D_7|$. אבל $\mathrm{Im}(f) \le S_5$. לכן עפ"י משפט לגרנז', $14 | 120$. סתירה.

9.3 קיים אפימורפיזם $f : C^* \to (R_+, \cdot)$.
הוכחה: נגדיר $f : C^* \to (R_+, \cdot)$ באופן הבא:

$$\forall z \in C^*, \qquad f(z) = \|z\|$$

אזי:
* f שומרת פעולות: $f(z_1z_2) = \|z_1z_2\| = \|z_1\|\|z_1\| = f(z_1)f(z_2)$
* f על: יהא $y \in R_+$ אזי עבור $y \in C^*$ מתקיים, $f(y) = \|y\| \underset{y \in R_+}{=} y$.

9.4 קיים איזומורפיזם $f : (R, +) \to (R_+, \cdot)$.
הוכחה: נגדיר $f : (R, +) \to (R_+, \cdot)$ באופן הבא:

$$\forall x \in R, \qquad f(x) = 2^x$$

אזי:
* f שומרת פעולות: $f(x+y) = 2^{x+y} = 2^x 2^y = f(x)f(y)$

* f על: יהא $y \in R_+$ אזי עבור $x = \log_2 y \in R$ מתקיים, $f(x) = 2^{\log_2 y} = y$.
* f חח"ע: אם עבור $x, y \in R$ $2^x = 2^y$ אזי $x = y$.

9.5 קיים אפימורפיזם $f: Z_{60} \to D_4$.

הפרכה: נניח בשלילה כי קיים אפימורפיזם $f: Z_{60} \to D_4$, אזי, מכיוון שאבליות נשמרת תחת אפימורפיזם ו Z_{60} אבלית נקבל ש D_4 אבלית. סתירה.

10. יהיו $m < n$ טבעיים. הוכיחו כי $m \mid n$ אם ורק אם קיים מונומורפיזם $f: Z_m \to Z_n$.

הוכחה: $(\Rightarrow)$ קיים מונומורפיזם $f: Z_m \to Z_n$ לכן $\operatorname{Im} f = f(Z_m) \le Z_n$. אבל, f חח"ע לכן $|\operatorname{Im} f| = |Z_m| = m$ וממשפט לגרנז' נובע כי $m \mid n = |Z_n|$.
$(\Leftarrow)$ Z_n חבורה ציקלית מסדר n . $m \mid n$ לכן קיימת ת"ח $H \le Z_n$ מסדר m . H ציקלית בתור ת"ח של חבורה ציקלית. לפי משפט המיון של חבורות ציקליות, $Z_m \cong H \le G$. לכן קיים איזומורפיזם, $f: Z_m \to H$. נסמן ב i את העתקת ההכלה $i: H \to Z_n$. אזי i מונומורפיזם. בסה"כ $i \circ f: Z_m \to Z_n$ מונומורפיזם כהרכבה של מונומורפיזמים.

11. מצאו את כל האוטומורפיזמים על $Z_2 \times Z_2$.

פתרון: החבורה $Z_2 \times Z_2$ היא החבורה $\{e, x, y, xy\}$ עבור $x = (1,0)$, $y = (0,1)$.
כל אוטומורפיזם φ חייב לשלוח את e ל e . מכיוון ש φ חייב להיות חח"ע $\varphi(x) = x'$ ו $\varphi(y) = y'$ הם בהכרח שני איברים שונים מ $\{x, y, xy\}$ ואז, $\varphi(xy) = \varphi(x)\varphi(y) = x'y'$ הוא האיבר השלישי של $\{x, y, xy\}$. ניתן לבדוק בקלות ש כל בחירה של x', y' כנ"ל מגדירה אוטומורפיזם. לכן, יש שישה אוטומורפיזמים – המתאימים לבחירת x', y' . 3 אפשרויות לבחירת x' ואז, שתי אפשרויות לבחירת y' .

12. ענו על הסעיפים הבאים:

12.1. יהיו G חבורה ו $H \lhd G$ ת"ח נורמלית כך ש $H \le Z(G)$. הוכיחו: אם G/H ציקלית, אז G אבלית.

הוכחה: נניח G/H ציקלית. אזי קיים $a \in G/H$ כך ש $G/H = \langle a \rangle$. קיים $g \in G$ כך ש $a = gH$. לכן, לכל $z \in G$ מתקיים $zH \in \langle gH \rangle$. לכן, קיים i_z שלם כך

$$zH = (gH)^{i_z} = g^{i_z}H \Rightarrow ze \in g^{i_z}H \Rightarrow \exists h_z \in H : z = g^{i_z}h_z$$

כעת, יהיו $x, y \in G$. מ"ל $xy = yx$.
עבור x קיימים i_x שלם ו $h_x \in H$ כך ש $x = g^{i_x}h_x$.
עבור y קיימים i_y שלם ו $h_y \in H$ כך ש $y = g^{i_y}h_y$.
לכן, מכיוון ש $H \le Z(G)$,

$$xy = g^{i_x}h_x g^{i_y}h_y = g^{i_x}g^{i_y}h_x h_y = g^{i_x+i_y}h_x h_y = g^{i_y+i_x}h_y h_x = h_y g^{i_y+i_x}h_x = h_y g^{i_y}h_x g^{i_x} = yx$$

12.2. תנו דוגמה לחבורה G כך ש $G/Z(G)$ אבלית אך אינה ציקלית.

דוגמה: נתבונן ב $G = D_4$. $Z(G) = \{e, \sigma^2\}$ (בידקו).

אזי, $4 = \frac{8}{2} = \frac{|G|}{|Z(G)|} = |G/Z(G)| = [G:Z(G)]$ אבלית מכיוון שכל חבורה מסדר 4 היא אבלית. נשים לב: $G/Z(G)$ אינה ציקלית. אחרת, לפי הסעיף הקודם נקבל ש $G = D_4$ אבלית.

בהצלחה! ☺