מבנים אלגבריים 1

מרצה: ד"ר אהרון רזון

המחלקה למתמטיקה ולמדעי המחשב

אוניברסיטת בר־אילן

סמסטר א', תש"ס

תכן ענינים

1. **יסודות על חבורות:**

הגדרה של אגודה, מונואיד וחבורה. הגדרה של חבורה חלופית. תכונות פשוטות (צמצום, הפוך של מכפלה). חזקות. דֻגמאות לחבורות. חבורות חלקיות. החבורה החלקית הנוצרת ע"י קבוצה חלקית. קונגרואנציות. חבורות צקליות סופיות ואינסופיות. סדר של אבר.

תרגילים לסעיף 1.

פתרונות תרגילים לסעיף 1.

2. **מושגים בסיסיים מתורת המספרים:**

יחס החִלוק. אנדוקציה. מספרים ראשוניים. המשפט היסודי של האריתמטיקה. המחלק המשותף הגדול ביותר והכפולה המשותפת הקטנה ביותר. חִלוק עם שארית. האלגוריתם של אוקליד למציאת מ.מ.ג.ב. . המשפט הקטן של פרמה. המשפט של אוילר. החבורה $(\mathbb{Z}/n\mathbb{Z})^\times$.

תרגילים לסעיף 2.

פתרונות תרגילים לסעיף 2.

3. **חבורת תמורות:**

הצגת תמורה כמכפלה של מחזורים זרים. רִשום תמורה כמכפלה של חִלופים. תמורות זוגיות ואי־זוגיות.

תרגילים לסעיף 3.

פתרונות תרגילים לסעיף 3.

4. **הומומורפיזמים:**

הגדרות (הומומורפיזם, מונומורפיזם, אפימורפיזם, איזומורפיזם). דֻגמאות להומומורפיזמים בין חבורות. גרעין ותמונה של הומומורפיזם. הצגה של חבורה. משפט קיילי. אוטומורפיזמים, הרכבת הומומורפיזמים ואוטומורפיזמים פנימיים.

תרגילים לסעיף 4.

פתרונות תרגילים לסעיף 4.

5. **חבורת המנה:**

אינדקס. משפט לגרנג'. חבורה חלקית לחבורה ציקלית. חבורה חלקית נורמלית. חבורת המנה. חבורה חלקית לחבורת המנה. דֻּגמאות לחבורות חלקיות נורמליות. חבורת דיהדר. ההומומורפיזם הטבעי. משפטי האיזומורפיזמים.

תרגילים לסעיף 5.

פתרונות תרגילים לסעיף 5.

6. **חבורות אבליות:**

מכפלה ישרה של חבורות. מכפלה ישרה פנימית. משפט השאריות הסיני. מיון של חבורות אבליות סופיות.

תרגילים לסעיף 6.

פתרונות תרגילים לסעיף 6.

7. **פעולות של חבורות על קבוצות:**

הגדרת פעולה משמאל. משפט קיילי המוכלל. פעולת ההצמדה. מחלקות צמידות. מסלול ומיצב. מֶרְכָּז של חבורה. נֻסחת המחלקה. משפט על המֶרְכָּז של חבורה מסדר p^n. משפט קושי.

תרגילים לסעיף 7.

פתרונות תרגילים לסעיף 7.

8. **משפטי סילו:**

משפט 1 (קיום של תת־חבורה סילוב). משפט 2 (צמידות של תת־חבורות סילוב). משפט 3 (כמות של תת־חבורות סילוב).

תרגילים לסעיף 8.

פתרונות תרגילים לסעיף 8.

9. **חבורות מסדר קטן:**

חבורות מסדר קטן מ 60. פשטות A_5. חבורות מסדר 6. חבורת הקווטרניוניים. חבורות מסדר $8-12$.

תרגילים לסעיף 9.

פתרונות תרגילים לסעיף 9.

רשימת משפטים.

מבחן לדֻגמה.

להלן מספר דֻגמאות למערכות אלגבריות עם פעולה אחת או שתיים:

קבוצה	פעולה	סוג	
$\mathbb{N}$	חבור	אגודה	semi-group
$\mathbb{N}$	כפל	מונואיד	monoid
$\mathbb{Z}$	חבור	חבורה	group
$\mathbb{Z}$	כפל	מונואיד	
$\mathbb{Z}$	חבור + כפל	חוג	ring
$\mathbb{Q}$	חבור	חבורה	
$\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$	כפל	חבורה	
$\mathbb{Q}$	חבור + כפל	שדה	field

הגדרה: תהי S קבוצה לא ריקה. **פעולה בִּינארית** ב S היא העתקה $f\colon S \times S \to S$. הזוג (S, f) נקרא **מערכת אלגברית עם פעולה אחת**.

דֻגמה: (א) $S = \{a, b\}$ ו f מגדרת ע״י טבלת הכפל

f	a	b
a	b	a
b	a	a

(ב) $S' = \{a', b'\}$ ו f' מגדרת ע״י טבלת הכפל

f'	a'	b'
a'	b'	b'
b'	b'	a'

שימו לב שהמערכות (א) ו (ב) שקולות ע״י ההעתקה המגדרת ע״י $a \leftrightarrow b'$ ו $b \leftrightarrow a'$.

הגדרה: שתי מערכות אלגבריות עם פעולה אחת (S, f) ו (T, g) נקראות **שקולות** (**אזומורפיות**) אם קימת פונקציה חח״ע ועל ממערכת אחת לשניה $\varphi\colon S \to T$ כך ש $\varphi(f(a,b)) = g(\varphi(a), \varphi(b))$ לכל $a, b \in S$.

דֻגמה: $S = \mathbb{R}$ עם פעולת החבור ו $T = \mathbb{R}_+ := \{x \in \mathbb{R} \,|\, x > 0\}$ עם פעולת הכפל.
השקילות $\varphi\colon S \to T$ מגדרת ע״י $\varphi(x) = 2^x$ ואכן מתקים

$$\varphi(x+y) = 2^{x+y} = 2^x \cdot 2^y = \varphi(x) \cdot \varphi(y)$$

הגדרה: החֹק האסוציאטיבי. מערכת אלגברית S עם פעולה (שנסמן אותה פשוט ככפל) מקימת את החֹק האסוציאטיבי אם לכל $x, y, z \in S$ מתקים $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

הגדרה: קבוצה עם פעולה אסוציאטיבית נקראת **אגודה**.

הערה: באגודה אפשר להשתמש בחפשיות בכללי החזקות $x^r \cdot x^s = x^{r+s}$ ו $(x^r)^s = x^{rs}$ עבור $r, s \in \mathbb{N}$.

הגדרה: בקבוצה S עם פעולה f, אבר e קרוי **ניטרלי** אם $f(e,x) = x = f(x,e)$ $\quad (ex = x = xe)$ לכל x.

הערה: אם קים אבר ניטרלי, אז הוא יחיד.

אכן, אם e' הוא אבר ניטרלי נוסף, אז $e = ee' = e'$.

סִמון: ב"כפל" נסמן את האבר הניטרלי ב "1".

ב"חבור" נסמן את האבר הניטרלי ב "0".

הגדרה: אגודה עם אבר ניטרלי נקראת **מונואיד**.

הגדרה: אבר a במונואיד יקרא **הפיך** אם קים b כך ש $ab = 1 = ba$ $\quad (a+b = 0 = b+a)$.

הערה: אם a הפיך, אז יש לו הפוך יחיד.

אכן, נניח $ab = 1 = ba$ וגם $ac = 1 = ca$. אזי

$$c = 1 \cdot c = (ba)c = bac = b(ac) = b \cdot 1 = b\ .$$

סִמון להפוך של a: בכתיב כפלי a^{-1}.

בכתיב חבורי $-a$.

מסקנות מההגדרה: (א) $(a^{-1})^{-1} = a$, $-(-a) = a$.

(ב) אם a, b הפיכים, אז ab הפיך וכן $(ab)^{-1} = b^{-1}a^{-1}$ כי

$$(ab)(b^{-1}a^{-1}) = 1 = (b^{-1}a^{-1})(ab)\ .$$

הגדרה: חֹק החִלוף (החֹק הקומוטטיבי). מערכת S עם פעולה f מקימת את חֹק החִלוף (החֹק הקומוטטיבי) אם $f(a,b) = f(b,a)$ לכל $a, b \in S$.

כאשר משתמשים בכתיב חבורי מניחים כי חֹק החִלוף מתקים, כלומר $a+b = b+a$. לכן $-(a+b) = -a-b = -(b+a)$.

הגדרות: (1) מונואיד שכל אבריו הפיכים קרוי **חבורה**.

אם מתקים חֹק החִלוף, נאמר שהחבורה היא **חלופית** (**קומוטטיבית**, **אבלית**). אחרת, החבורה **אינה חלופית** (**אינה קומוטטיבית**, **אינה אבלית**).

(2) קבוצה R שבה מגדרות שתי פעולות שנקרא להן חבור וכפל נקראת **חוג** אם:

(א) R ביחס לחבור היא חבורה חלופית.

(ב) R ביחס לכפל היא אגודה.

(ג) מתקימים חֻקי הפִּלוג (החֻקים הדיסטריבוטיביים):

$(b+c)a = ba + ca$ ו $a(b+c) = ab + ac$ לכל $a, b, c \in R$.

(3) חוג F נקרא **שדה** אם $F \setminus \{0\}$ היא חבורה חלופית ביחס לכפל.

סִמון: עבור מונואיד S, נסמן ב $S^\times$ את קבוצת האברים ההפיכים ב S.

הערה: אם F הוא שדה, אז $F^\times$ הוא מונואיד חלקי של F.

הגדרה: תהי S מערכת עם פעולה, נניח פעולת כפל, ותהי $S' \subseteq S$ קבוצה חלקית. S' נקראת **מערכת חלקית** ביחס לפעולת הכפל המושרית מ S אם לכל $x, y \in S'$ גם $x \cdot y \in S'$.

טענה: *יהי S מונואיד ותהי $G = S^\times$. אזי G חבורה.*

הוכחה: * G סגורה תחת הכפל: $a, b \in G \Leftarrow a, b$ הפיכים ב $S \Leftarrow ab$ הפיך ב $S \Leftarrow ab \in G$.

* בודאי מתקים החֹק האסוציאטיבי.

* $1 \in G$ בהיותו הפיך והוא ניטרלי ב G.

* $a \in G \Rightarrow a^{-1} \in G$. ∎

דֻגמאות: (א) $S = \mathbb{Z} \supset \mathbb{Z}^\times = \{1, -1\} = G$ היא חבורה.

(ב) $S = M_n(\mathbb{R}) \supset M_n(\mathbb{R})^\times =: GL_n(\mathbb{R}) = G$ קבוצת כל המטריצות ההפיכות (ביחס לכפל מטריצות) היא חבורה.

(ג) תהי X קבוצה כלשהיא. אסף כל הפונקציות מ X ל X, $S = \{g \mid g\colon X \to X\}$, הוא מונואיד ביחס לכפל (הרכבת פונקציות). החבורה $G = S^\times$ היא אסף כל הפונקציות החח"ע ועל.

(ג1) מקרה פרטי: $X = \{1, \ldots, n\}$. אזי S היא חבורת התמורות על הקבוצה $\{1, \ldots, n\}$. סמנה S_n והיא נקראת **החבורה הסמטרית מדרגה** n.

דֻגמאות לשדות: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

הערה: במונואיד, כל אבר הפיך נתן לצמצום. כלומר אם a הפיך וכן $ax = ay$, אז $x = y$.
אכן, $x = a^{-1}ax = a^{-1}ay = y$.

מסקנה: תהי G חבורה ויהי "1" האבר הניטרלי. אם $e \in G$ מקים $e^2 = e$, אז $e = 1$.

חבורות חלקיות

הגדרה: תהי G חבורה. קבוצה חלקית $H \subseteq G$ תקרא **חבורה חלקית** (או **תת־חבורה**) אם H היא חבורה ביחס לפעולה המגדרת ב G. כלומר

(א) $1 \in H$;

(ב) $a, b \in H \Leftarrow ab \in H$; ו

(ג) $a \in H \Leftarrow a^{-1} \in H$.

הערה: נתן להחליף את (א) ב

(א') $H \neq \emptyset$.

אכן, אם $1 \in H$, אז $H \neq \emptyset$. להיפך, אם $H \neq \emptyset$, אז קים $h \in H$. לכן מ (ג), $h^{-1} \in H$, ומ (ב), $1 = h \cdot h^{-1} \in H$.

סִמון: תהי G חבורה. אם H היא תת־חבורה של G, אנו מסמנים $H \leq G$.

דֻגמאות: (א) $2\mathbb{Z} \leq (\mathbb{Z}, +)$ (הזוגיים) חבורה חלקית.

(ב) $3\mathbb{Z} \leq (\mathbb{Z}, +)$ חבורה חלקית.

(ג) $\mathbb{Q}_+ \leq (\mathbb{Q}^\times, \cdot)$ הרציונלים החיוביים –חבורה חלקית.

(ד) $\{z \in \mathbb{C} \,|\, z^n = 1\} \leq (\mathbb{C}^\times, \cdot)$ חבורה חלקית. אכן, 1 הוא שרש של המשואה $z^n = 1$ ואם z_1, z_2 שרשים נוספים, אז מהמשואות $z_1^n z_2^n = 1$ ו $(z_1 z_2)^n = 1 = (z^n)^{-1}$ נובע שגם $(z_1^{-1})^n = (z^n)^{-1} = 1$ ו $z_1 z_2$ ו z_1^{-1} הם שרשים.

החבורה החלקית הנוצרת ע"י קבוצה חלקית

תהי G חבורה ותהי $X \subseteq G$ קבוצה חלקית. מהי החבורה החלקית הקטנה ביותר המכילה את X?

טענה: *תהי G חבורה ותהי $X \subseteq G$ קבוצה חלקית. אזי $\bigcap\{H \,|\, X \subseteq H \leq G\}$ היא החבורה החלקית הקטנה ביותר המכילה את X.*

הוכחה: נסמן $\mathcal{H} = \{H \,|\, X \subseteq H \leq G\}$ ו $K = \bigcap_{H \in \mathcal{H}} H$. K היא תת־חבורה של G כי

(א) $(\forall H \in \mathcal{H})\ 1 \in H \Leftarrow 1 \in \bigcap_{H \in \mathcal{H}} H = K$.

$$a, b \in K \Leftarrow (\forall H \in \mathcal{H})\ a, b \in H \Leftarrow (\forall H \in \mathcal{H})\ ab \in H \Leftarrow ab \in \bigcap_{H \in \mathcal{H}} H = K \qquad \text{(ב)}$$

$$a \in K \Leftarrow (\forall H \in \mathcal{H})\ a \in H \Leftarrow (\forall H \in \mathcal{H})\ a^{-1} \in H \Leftarrow a^{-1} \in \bigcap_{H \in \mathcal{H}} H = K \qquad \text{(ג)}$$

אם H היא חבורה חלקית של G המכילה את X, אז מהגדרת K נובע ש $K \leq H$. מכאן K היא החבורה החלקית הקטנה ביותר המכילה את X. ∎

סִמון: תהי G חבורה ותהי $X \subseteq G$ קבוצה חלקית. אנו מסמנים ב $\langle X \rangle$ את החבורה החלקית המזערית של G המכילה את X וקוראים לה **תת־החבורה הנוצרת ע"י** X.

טענה: *תהי G חבורה ותהי $X \subseteq G$ קבוצה חלקית לא ריקה. נסמן $X^{-1} = \{x^{-1} \mid x \in X\}$ ו $Y = X \cup X^{-1}$.*
תהי Z קבוצת כל המכפלות הסופיות של אברי Y. אזי $Z = \langle X \rangle$.

הוכחה: נראה הכלה בשני הכוונים.

כוון ראשון: $\langle X \rangle \supseteq Z$. $\langle X \rangle$ היא חבורה והיא מכילה את X. לכן $Y \subseteq \langle X \rangle$ ולכן $Z \subseteq \langle X \rangle$.

כוון שני: $\langle X \rangle \subseteq Z$. מהגדרת $\langle X \rangle$ כתת־החבורה המזערית של G המכילה את X, מספיק להראות ש Z חבורה. אכן

(א') $Z \neq \emptyset$ כי $X \neq \emptyset$.

(ב) יהיו $z, z' \in Z$ ונניח ש $z = y_1 \cdots y_m$ ו $z' = y'_1 \cdots y'_n$ באשר $y_1, \ldots, y_m, y'_1, \ldots, y'_n \in Y$. אזי $zz' = y_1 \cdots y_m y'_1 \cdots y'_n \in Z$.

(ג) יהי $z \in Z$ ונניח ש $z = y_1 \cdots y_m$ באשר $y_1, \ldots, y_m \in Y$. אזי, כיון ש $y^{-1} \in Y$ (כי $y \in X$ או $y \in X^{-1} \Longrightarrow y^{-1} \in X^{-1}$ או $y^{-1} \in X$) לכל $y \in Y$, נובע ש $z^{-1} = (y_1 \cdots y_m)^{-1} = y_m^{-1} \cdots y_1^{-1} \in Z$.

משתי ההכלות נובע ש $Z = \langle X \rangle$. ∎

מסקנה: (א) $\langle X \rangle = \{y_1 \cdots y_m \mid y_i \in X \cup X^{-1}\}$.

(ב) אם $a \in G$, אז $\langle a \rangle$ היא החבורה הנוצרת ע"י האבר a. מכיון שכל מכפלה סופית של אברים מהקבוצה $\{a\} \cup \{a^{-1}\}$ היא מהצורה a^k עבור $k \in \mathbb{Z}$, נובע ש

$$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}.$$

הגדרה: חבורה שכל אבריה הם חזקות של אבר מסוים a נקראת חבורה **ציקלית** (**מעגלית**).

דֻגמאות: (א) אם G חבורה ו $a \in G$, אז $\langle a \rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, \ldots\}$.

(ב) $2 \in \mathbb{Q}^\times$, $\langle 2 \rangle = \{\ldots, \frac{1}{2^3}, \frac{1}{2^2}, \frac{1}{2}, 1, 2, 2^2, 2^3, \ldots\}$.

(ג) $1 \in \mathbb{Z}$, $\langle 1 \rangle = \{\ldots, -1-1-1, -1-1, -1, 0, 1, 1+1, 1+1+1, \ldots\} = \mathbb{Z}$ כחבורות חבוריות.

קונגרואנציות

יהי m מספר טבעי. עבור $a, b \in \mathbb{Z}$ נגדיר $a \equiv b \pmod{m}$ אם $m | a - b$. אנו קוראים זאת "a קונגרואנטי ל b מודולו m".

דֻגמה: $11 \equiv 29 \pmod{6}$, $11 \not\equiv 29 \pmod{5}$.

טענה: *יהיו* $a,b\in\mathbb{Z}$*. נסמן ב* r_1 *ו* r_2 *את השאריות המתקבלות מחִלוק* a *ו* b*, בהתאמה, ב* m*. כלומר* $a=mq_1+r_1$ *ו* $b=mq_2+r_2$ *באשר* $r_1,r_2,q_1,q_2\in\mathbb{Z}$ *ו* $0\le r_1,r_2<m$*. אזי* $a\equiv b \pmod m$ *אמ"ם* $r_1=r_2$*.*

הוכחה: אם $r_1=r_2$, אז $a-b=m(q_1-q_2)$ ולכן $a\equiv b \pmod m$.

כוון שני: נניח $a\equiv b \pmod m$. אזי $m|a-b$. לכן, כיון ש $a-b=m(q_1-q_2)+r_1-r_2$, נובע ש $m|r_1-r_2$. אולם $0\le r_1,r_2<m$ ולכן בהכרח $r_1-r_2=0$ (כי $-m<r_1-r_2<m$ יכול להתחלק ב m רק אם הוא שוה ל 0). כלומר $r_1=r_2$. ∎

מסקנה: יהי $a\in\mathbb{Z}$. אזי מתוך $a\equiv a \pmod m$ נובע ש a קונגרואנטי לאחד ורק לאחד מבין המספרים $0,1,\ldots,m-1$.

הערה: יחס ה $\equiv$ הוא יחס שקילות:

(א) רפלקסיביות: $a\equiv a$.

(ב) סמטריות: $a\equiv b \Leftarrow b\equiv a$.

(ג) טרנזיטיביות: $a\equiv b,\ b\equiv c \Leftarrow a\equiv c$.

מספר מחלקות השקילות הוא m. איחוד מחלקות השקילות הוא $\mathbb{Z}$ והוא איחוד זר:

$$\mathbb{Z}=\dot{\bigcup_{i=0}^{m-1}}[i],$$

באשר $[i]$ היא מחלקת השקילות המתאימה לשארית i.

סִמון: $\mathbb{Z}_m=\{[0],[1],\ldots,[m-1]\}$.

סִמון מקוצר: $\mathbb{Z}_m=\{0,1,\ldots,m-1\}$. לפעמים רושמים גם C_m במקום $\mathbb{Z}_m$.

טענה: *יהיו* $a_1,a_2,b_1,b_2\in\mathbb{Z}$ *כך ש* $a_1\equiv b_1 \pmod m$ *ו* $a_2\equiv b_2 \pmod m$*. אזי*

(א) $a_1+a_2\equiv b_1+b_2 \pmod m$.

(ב) $a_1\cdot a_2\equiv b_1\cdot b_2 \pmod m$.

הוכחה: נראה תחילה שלכל $a,b,c\in\mathbb{Z}$ מתקיים

(א') $a\equiv b \pmod m \Leftarrow a+c\equiv b+c \pmod m$.

(ב') $a\equiv b \pmod m \Leftarrow a\cdot c\equiv b\cdot c \pmod m$.

אכן, (א') נובע כי $m|a-b \Leftarrow m|(a+c)-(b+c) \Leftarrow a+c\equiv b+c$

ו (ב') נובע כי $m|a-b \Leftarrow m|(a-b)c \Leftarrow m|ac-bc \Leftarrow ac\equiv bc$.

עתה, (א) נובע מ (א') כי $a_1\equiv b_1, a_2\equiv b_2 \Leftarrow a_1+a_2\equiv b_1+a_2\equiv b_1+b_2$

ו (ב) נובע מ (ב') כי $a_1 \equiv b_1, a_2 \equiv b_2 \Leftarrow a_1a_2 \equiv b_1a_2 \equiv b_1b_2$. ∎

הגדרה: עבור $c \in \mathbb{Z}$, אנו מסמנים ב $[c]$ את מחלקת השקילות בה נמצא c. אנו מגדירים על $\mathbb{Z}_m$ פעולות חבור וכפל ע"י

סכום של שתי מחלקות שקילות: $[a_1] + [a_2] := [a_1 + a_2]$,

מכפלה של שתי מחלקות שקילות: $[a_1] \cdot [a_2] := [a_1 \cdot a_2]$.

בהשואה ל $\mathbb{Z}$, אין שמירה על מושג הסדר אולם הסוג נשמר:

קבוצה	**פעולה**	**סוג**
$\mathbb{Z}_m$	חבור	חבורה
$\mathbb{Z}_m$	כפל	מונואיד
$\mathbb{Z}_m$	חבור + כפל	חוג

חבורות ציקליות סופיות ואינסופיות

דֻגמאות: (א) $\mathbb{Z}_n = \{0, 1, \ldots, n-1\} = \langle 1 \rangle$ היא חבורה ציקלית סופית ביחס לחבור.

(ב) $\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \in \mathbb{C}$, $\langle \omega \rangle = \{z \in \mathbb{C} \mid z^n = 1\}$. בפרט, עבור $n = 4$, $\omega = i \in \mathbb{C}$ ו $\langle i \rangle = \{i^0, i^1, i^2, i^3\} = \{1, i, -1, -i\} = \{z \in \mathbb{C} \mid z^4 = 1\}$.

טענה: *תהי G חבורה ויהי $a \in G$.*

(א) *אם $\langle a \rangle$ אינסופית, אז $a^k \neq a^\ell$ לכל $k > \ell$ ב $\mathbb{Z}$.*

(ב) *אם $\langle a \rangle$ סופית, אז קים $n \geq 1$ מזערי כך ש $a^n = 1$ ו $\langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$ היא קבוצה בת n אברים.*

הוכחה: אם קימים $k > \ell$ וכן $a^k = a^\ell$, אז $a^{k-\ell} = 1$. לכן קים $n \geq 1$ מזערי כך ש $a^n = 1$. במקרה זה מתקבל $\langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$.

אכן, יהי $a^k \in \langle a \rangle$ ונכתב את k כ $k = nq + r$ עם $0 \leq r \leq n-1$. אזי

$$a^k = a^{nq+r} = (a^n)^q a^r = a^r.$$

הוכחת (א): מהדיון לעיל נובע שאם $\langle a \rangle$ היא אינסופית, אז בהכרח $a^k \neq a^\ell$ לכל $k > \ell$ (אחרת קים n כך ש $\langle a \rangle = \{1, a, \ldots, a^{n-1}\}$ חבורה סופית).

הוכחת (ב): אם $\langle a \rangle$ סופית, אז בודאי קימים $k > \ell$ כך ש $a^k = a^\ell$ (אחרת $\langle a \rangle$ אינסופית). לכן, מהדיון לעיל נובע ש $\langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$, באשר $n \geq 1$ הוא מזערי כך ש $a^n = 1$. נשאר להראות שכל האברים שונים ביניהם.

אכן, נניח בשלילה שקימים $0 \leq s < r \leq n-1$ כך ש $a^r = a^s$. אזי $a^{r-s} = 1$ ו $1 \leq r-s \leq n-1$, בסתירה למזעריות n. ∎

הגדרה: תהי G חבורה ויהי $a \in G$. מספר אברי החבורה $\langle a \rangle$ נקרא **הסדר** של a (אינסופי אם $\langle a \rangle$ אינסופית). מספר אברי חבורת G נקרא **הסדר** של G והוא מסומן ב $|G|$.

הערה: הסדר של אבר שוה לסדר של החבורה הציקלית הנוצרת ע"י אותו אבר.

משפט: *(א) כל חבורה ציקלית אינסופית איזומורפית ל $\mathbb{Z}$ ביחס לחבור.*

(ב) כל חבורה ציקלית סופית מסדר n איזומורפית ל $\mathbb{Z}_n$ ביחס לחבור.

הוכחה: תהי $\langle a \rangle$ החבורה הציקלית.

(א) נגדיר העתקה $\varphi\colon \mathbb{Z} \to \langle a \rangle$ ע"י $\varphi(k) = a^k$. φ היא חח"ע ועל מפני שכל חזקות a שונות ביניהן. כמו־כן φ היא איזומורפיזם כי

$$\varphi(k_1+k_2) = a^{k_1+k_2} = a^{k_1}a^{k_2} = \varphi(k_1)\varphi(k_2).$$

(ב) נגדיר $\varphi\colon \mathbb{Z}_n = \{0,1,2,\ldots,n-1\} \to \langle 1, a, a^2, \ldots, a^{n-1} \rangle = \langle a \rangle$ ע"י $\varphi(k) = a^k$ עבור $k \in \{0,1,2,\ldots,n-1\}$. זוהי העתקה חח"ע ועל. יהיו $k_1, k_2 \in \{0,1,2,\ldots,n-1\}$. אם $k_1+k_2 < n$, אז $\varphi(k_1+k_2) = \varphi(k_1)\varphi(k_2)$ כמו ב (א). אם $k_1+k_2 \geq n$, אז $0 \leq k_1+k_2-n \leq n-1$ ולכן

$$\varphi(k_1+k_2) = \varphi(k_1+k_2-n) = a^{k_1+k_2-n} = a^{k_1}a^{k_2}a^{-n} = a^{k_1}a^{k_2} = \varphi(k_1)\varphi(k_2).$$ ∎

תרגילים לסעיף 1

1. תהי G אגודה ובה אבר e המקים $ex = x$ לכל $x \in G$. כמו־כן לכל $a \in G$ קים $b \in G$ כך ש $ba = e$. הוכח/י כי G חבורה. (רמז: הוכח/י קודם שלכל a קים c כך ש $a = ce$ והסק/י ש e אבר ניטרלי.)

2. במונואיד סופי אבר a הנתן לצמצום מצד אחד הוא הפיך. (רמז: עין/י בחזקות של a.)

3. אגודה סופית G שבה כל אבר נתן לצמצום מימין ובנוסף קים אבר d הנתן לצמצום משמאל היא חבורה. (רמז: אם $d^s = d^r$ עבור $s > r$ מסוימים, הגדר/י $e = d^{s-r}$ והוכח/י שמתקימים תנאי תרגיל 1.)

4. G חבורה סופית. הוכח/י שקים N כך ש $x^N = 1$ לכל $x \in G$.

5. חוג R נקרא **תחום שלמות** אם $R \setminus \{0\}$ היא אגודה חלקית של R ביחס לכפל. הוכח/י שאם R תחום שלמות סופי וקומוטטיבי אזי R שדה.

6. R חוג עם אבר ניטרלי 1 ביחס לכפל. יהיו $a, b \in R$ כך ש $1 - ab$ הפיך. הוכח/י ש $1 - ba$ הפיך. (רמז: יהי $c = (1 - ab)^{-1}$. עין/י ב $1 + bca$.)

7. חוג R המקים $x^2 = x$ לכל $x \in R$ נקרא **חוג בוליאני**. הוכח/י שחוג כזה הוא קומוטטיבי. (רמז: הוכח/י קודם ש $x = -x$ לכל x ואחר־כך הצב/י $x = a + b$.)

8. (א) כל חבורה בת שני אברים איזומורפית ל $\mathbb{Z}_2$ ביחס לחבור.

   (ב) כל חבורה בת שלשה אברים איזומורפית ל $\mathbb{Z}_3$ ביחס לחבור.

9. (א) אם G חבורה קומוטטיבית ו $x_1, \ldots, x_k \in G$ אזי

$$\langle x_1, \ldots, x_k \rangle = \{\prod_{i=1}^{k} x_i^{r_i} \mid r_i \text{ שלמים כלשהם}\} .$$

   (ב) אם בנוסף x_i מסדר n_i אזי נתן להסתפק ב $0 \le r_i \le n_i - 1$ לכל i. הסק/י:

$$|\langle x_1, \ldots, x_k \rangle| \le n_1 n_2 \cdots n_k .$$

1. יהי $a \in G$. מהנתון קים $b \in G$ כך ש $ba = e$. כמו־כן קים $c \in G$ כך ש $cb = e$. אזי $a = ea = cba = ce$. לכן $ae = cee = ce = a$.

מכאן $ea = a = ae$ לכל $a \in G$. כלומר e הוא אבר ניטרלי ב G ולכן G הוא מונואיד.

יהי שוב $a \in G$ ויהיו $b, c \in G$ כך ש $ba = e$, $cb = e$ ו $a = ce$. אזי $ab = ceb = cb = e$.

מכאן שלכל a קים b כך ש $ab = e = ba$. כלומר כל $a \in G$ הוא הפיך ולכן G היא חבורה.

2. יהי e האבר הניטרלי במונואיד. נניח, בלי הגבלת הכלליות, כי a נתן לצמצום משמאל. כלומר לכל b, c במונואיד מתקים $ab = ac \Leftarrow b = c$.

כיון שהמונואיד סופי, הקבוצה $\{a^n \mid n \in \mathbb{N}\}$ היא סופית. לכן קימים $r < s$ כך ש $a^s = a^r$. נרשם זהות זאת כך: $\underbrace{a \cdots a}_{r \text{ פעמים}} \cdot e = \underbrace{a \cdots a}_{r \text{ פעמים}} \cdot a^m$, באשר $m = s - r$. עתה נתן לצמצם את a משמאל בזה אחר זה עד לקבלת הזהות $e = a^m$. נסמן $b = a^{m-1}$. אזי $ab = e = ba$, כלומר a הפיך.

3. כיון ש G סופית, קימים טבעיים $r < s$ כך ש $d^s = d^r$. נסמן $e = d^{s-r}$.

יהי $x \in G$. נכפל את שתי צדי המשואה $d^s = d^r$ ב x: $d^s x = d^r x$. אזי, כיון ש d נתן לצמצום משמאל, אנו מקבלים $ex = x$.

נניח $G = \{b_1, \ldots, b_n\}$ ויהי $a \in G$. כיון ש a נתן לצמצום מימין, הקבוצה $\{b_1 a, \ldots, b_n a\}$ מכילה n אברים שונים ולכן שוה ל G. בפרט קים $b \in G$ כך ש $ba = e$.

G מקימת אם־כן את תנאי תרגיל 1 ולכן היא חבורה.

4. אם G חבורה סופית, אז הסדר של כל אבר x ב G הוא סופי כי $\langle x \rangle \subseteq G$ ולכן $|x| = |\langle x \rangle| \leq |G|$. נסמן $N = \prod_{x \in G} |x|$. אזי $x^N = (x^{|x|})^{\frac{N}{|x|}} = 1$ לכל $x \in G$.

5. יהי R תחום שלמות סופי וקומוטטיבי. כדי להראות ש R הוא שדה יש להראות כי $R \setminus \{0\}$ היא חבורה חלופית ביחס לכפל. מהנתון $R \setminus \{0\}$ היא אגודה סופית. אנו נראה שכל אבר $a \in R \setminus \{0\}$ נתן לצמצום מימין ומשמאל ואז משאלה 3 ינבע ש $R \setminus \{0\}$ היא חבורה.

אכן, יהיו $a, b, c \in R \setminus \{0\}$ כך ש $ab = ac$. אזי, בעזרת חֹק הפלוג בחוג R, $a(b - c) = 0$. אולם $R \setminus \{0\}$ הוא מונואיד ביחס לכפל ולכן $b - c = 0$ (אחרת $b - c \in R \setminus \{0\} \Leftarrow a(b - c) \in R \setminus \{0\}$ מסגירות תחת הכפל במונואיד $R \setminus \{0\}$), כלומר $b = c$. לכן a נתן לצמצום משמאל. באפן דומה a נתן לצמצום מימין. מכאן $R \setminus \{0\}$ היא חבורה (חלופית כי R קומוטטיבי) ולכן R הוא שדה.

6. שימו־לב תחילה שבחוג מתקים $(-x) \cdot y = -(x \cdot y) = x \cdot (-y)$ לכל x, y. אכן, בכל חוג

מתקים $a \cdot 0 = 0 = 0 \cdot a$ לכל a (כי $0 = a \cdot 0 \Leftarrow a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$ ו $0 = 0 \cdot a \Leftarrow 0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$). לכן

$$(-x) \cdot y = -(x \cdot y) \Leftarrow x \cdot y + (-x) \cdot y = (x + (-x)) \cdot y = 0 \cdot y = 0 \Leftarrow x + (-x) = 0$$

ו $x \cdot (-y) = -(x \cdot y) \Leftarrow x \cdot y + x \cdot (-y) = x \cdot (y + (-y)) = x \cdot 0 = 0 \Leftarrow y + (-y) = 0$.

יהי עתה R חוג עם אבר ניטרלי 1 ביחס לכפל ויהיו $a, b \in R$ כך ש $1 - ab$ הפיך. נסמן $c = (1-ab)^{-1}$. אזי, בעזרת חֹק הפלוג, $1 = (1-ab)c = c - abc$ ולכן $abc = c - 1$. מכאן, בעזרת חֹק הפלוג,

$$(1-ba)(1+bca) = 1 + bca - ba - b(abc)a = 1 + bca - ba - b(c-1)a = 1.$$

באפן דומה, $1 = c(1-ab) = c - cab$ ולכן $cab = c - 1$. מכאן

$$(1+bca)(1-ba) = 1 - ba + bca - b(cab)a = 1 - ba + bca - b(c-1)a = 1.$$

כלומר $1 - ba$ הפיך ו $(1-ba)^{-1} = 1 + bca$.

7. בחוג מתקים $(-x) \cdot y = -(x \cdot y) = x \cdot (-y)$ ו $-(-z) = z$ לכל x, y, z ולכן

$$(-x)^2 = (-x) \cdot (-x) = -(x \cdot (-x)) = -(-(x \cdot x)) = x \cdot x = x^2$$

לכל x. מכאן, אם R הוא חוג בוליאני, אז $x = x^2 = (-x)^2 = -x$ לכל x. כמו־כן, לכל $a, b \in R$ מתקים

$$a + b = (a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$$

ולכן $ab + ba = 0$. מכאן $ab = -ba = ba$. כלומר R הוא חוג קומוטטיבי.

8. כיון שכל אבר בחבורה נתן לצמצום מימין ומשמאל, כל אבר בחבורה מופיע בדיוק פעם אחת בכל עמודה ובכל שורה בטבלת הכפל של החבורה.

(א) תהי $G = \{e, a\}$ חבורה בת שני אברים, באשר e אבר היחידה ב G. אזי יש רק דרך אחת למלא את טבלת הכפל של G ולכן טבלת הכפל ב G וטבלת החבור ב $(\mathbb{Z}_2, +)$ שקולות:

$(\mathbb{Z}_2, +)$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cong$

$(G, \cdot)$	e	a
e	e	a
a	a	e

לכן $(\mathbb{Z}_2, +) \cong G$ ע"י $e \mapsto [0]$ ו $a \mapsto [1]$.

(ב) תהי $G = \{e, a, b\}$ חבורה בת שלשה אברים, באשר e אבר היחידה ב G. אזי יש רק דרך אחת למלא את טבלת הכפל של G ולכן טבלת הכפל ב G וטבלת החבור ב $(\mathbb{Z}_3, +)$ שקולות:

$(\mathbb{Z}_3, +)$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$\cong$

$(G, \cdot)$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

(לא יתכן ש e מופיע במקום (a,a) בטבלה כי אז בהכרח b מופיע במקום (a,b) בטבלה, בסתירה לכך ש b מופיע כבר במקום (e,b) בטבלה.) לכן $G \cong (\mathbb{Z}_3,+)$ ע"י $e \mapsto [0]$, $a \mapsto [1]$ ו $b \mapsto [2]$.

9. (א) תהי G חבורה קומוטטיבית ויהיו $x_1,\dots,x_k \in G$. נסמן $X = \{x_1,\dots,x_k\}$. אזי ממשפט בסעיף 1 נובע כי

$$\langle x_1,\dots,x_k\rangle = \langle X\rangle = \{y_1\cdots y_n \mid y_i \in X \cup X^{-1}\},$$

באשר $X^{-1} = \{x_1^{-1},\dots,x_k^{-1}\}$. כיון ש G קומוטטיבית, כל מכפלה $y_1\cdots y_n$ עם $y_i \in X \cup X^{-1} = \{x_1,\dots,x_k,x_1^{-1},\dots,x_k^{-1}\}$ היא מהצורה $\prod_{i=1}^k x_i^{r_i}$ עם $r_i \in \mathbb{Z}$. כלומר

$$\langle x_1,\dots,x_k\rangle = \{\prod_{i=1}^k x_i^{r_i} \mid r_i,\dots,r_k \in \mathbb{Z}\}.$$

(ב) נניח בנוסף ש $|x_1| = n_1,\dots,|x_k| = n_k$. אזי, עבור $r_1,\dots,r_k \in \mathbb{Z}$, $\prod_{i=1}^k x_i^{r_i} = \prod_{i=1}^k x_i^{r_i'}$ באשר $0 \le r_i' \le n_i - 1$ מקיים $r_i \equiv r_i' \pmod{n_i}$, $i = 1,\dots,k$. לכן

$$\langle x_1,\dots,x_k\rangle = \{\prod_{i=1}^k x_i^{r_i} \mid 0 \le r_1 \le n_1 - 1,\dots,0 \le r_k \le n_k - 1\}.$$

מכאן $|\langle x_1,\dots,x_k\rangle| \le \#\{(r_1,\dots,r_k) \in \mathbb{Z}^k \mid 0 \le r_1 < n_1,\dots,0 \le r_k < n_k\} = n_1\cdots n_k$.

יחס החִלוק: יהיו $a, b \in \mathbb{Z}$. אנו אומרים ש a **מחלק** את b ומסמנים $a|b$ אם קים $c \in \mathbb{Z}$ כך ש $b = ac$. יחס החִלוק על $\mathbb{Z}$ מקים את התכונות הבאות:

(א) $a|b \Leftarrow a|bd$ לכל d.

(ב) $a|b \,\&\, b|a \Leftarrow a = \pm b$.

(ג) היחס טרנזיטיבי: $a|b \,\&\, b|c \Leftarrow a|c$.

(ד) $c|a_1 \,\&\, c|a_2 \Leftarrow c|a_1 + a_2$.

ובאנדוקציה: $c|a_1 \,\&\, \cdots \,\&\, c|a_n \Leftarrow c|\sum_{i=1}^{n} a_i d_i$ לכל $d_1, \ldots, d_n$.

אנדוקציה: תהי $T_1, T_2, \ldots, T_n, \ldots$ סדרת טענות המקימת

(א) T_1 נכון ו

(ב) $T_n \Leftarrow T_{n+1}$ לכל n.

אזי T_n נכון לכל n.

הערה 1: תכונת האנדוקציה נובעת מ

תכונת הסדר הטוב: בכל קבוצה לא ריקה של מספרים טבעיים קים מספר קטן ביותר.

אכן, תהי $T_1, T_2, \ldots, T_n, \ldots$ סדרת טענות המקימת את אקסיומות האנדוקציה (א) ו (ב). נסתכל בקבוצה $\{k \in \mathbb{N} \mid T_k$ לא נכון$\}$. אם הקבוצה ריקה, אז T_n נכון לכל n וסימנו. אחרת, יש בקבוצה אבר מזערי m. $m \neq 1$ כי T_1 נכון. לכן, עבור $n = m - 1$, T_n נכון. מכאן, כיון ש $T_n \Leftarrow T_{n+1}$, T_m נכון. סתירה.

הערה 2: נתן להחליף את אקסיומת (ב) של האנדוקציה באקסיומה

(ב') $T_1, T_2, \ldots, T_{n-1} \Leftarrow T_n$ לכל n.

מספרים ראשוניים: $p \in \mathbb{Z}$ הוא מספר **ראשוני** אם $p \neq 0, \pm 1$ ו p מתחלק רק ב $\pm 1, \pm p$.

המשפט היסודי של האריתמטיקה: *כל מספר טבעי $n > 1$ נתן לכתיבה בצורה אחת ויחידה כמכפלה $n = p_1 \cdot p_2 \cdots p_r$, באשר $p_1 \leq \ldots \leq p_r$ ראשוניים ו $r \geq 1$.*

הוכחה: יהי $n > 1$ מספר טבעי. נוכיח את הטענה באנדוקציה על n.

קיום הפרוק: עבור $n = 2$, $2 = 2$ הוא פרוק.

נניח כי קים פרוק לכל מספר טבעי k בין 2 ל $n - 1$ (ראו הערה 2). אם n הוא ראשוני, אז $n = n$ הוא פרוק. אחרת $n = k_1 k_2$, באשר $1 < k_1, k_2 < n$. אזי k_1, k_2 הם מכפלות של מספרים ראשוניים ולכן גם n.

יחידות הפרוק: עבור $n=2$ היחידות ברורה.

נניח כי הפרוק יחיד לכל מספר טבעי קטן מ n. אם n הוא ראשוני, אז הפרוק $n=n$ הוא יחיד. אחרת, נניח שני פרוקים $n=p_1\cdots p_r=q_1\cdots q_s$, באשר $p_1\leq\ldots\leq p_r$, $q_1\leq\ldots\leq q_s$ מספרים ראשוניים ו $r,s>1$.

אם $p_1=q_1$, נצמצם ונסים על סמך האנדוקציה. נניח בשלילה ש $p_1\neq q_1$. נניח $p_1<q_1$. אזי

$$p_1(p_2\cdots p_r-q_2\cdots q_s)=p_1p_2\cdots p_r-p_1q_2\cdots q_s$$
$$=q_1q_2\cdots q_s-p_1q_2\cdots q_s=(q_1-p_1)q_2\cdots q_s<n$$

הם שני אפנים לפרוק מספר טבעי קטן מ n. לכן p_1 חיב להיות אחד הגורמים בפרוק של אגף ימין. אולם $p_1\neq q_2,\ldots,q_s$ כי $p_1<q_1\leq q_2\leq\ldots\leq q_s$. לכן $p_1|q_1-p_1$. מכאן $p_1|q_1$. אבל $p_1<q_1$ ושניהם ראשוניים. סתירה. ∎

המחלק המשותף הגדול ביותר והכפולה המשותפת הקטנה ביותר

הגדרה: יהיו $a,b\in\mathbb{Z}$ לא שניהם אפס. נניח

$$a=\pm p_1^{\alpha_1}\cdots p_k^{\alpha_k} \text{ ו } b=\pm p_1^{\beta_1}\cdots p_k^{\beta_k}$$

עם $\alpha_i,\beta_i\geq 0$, $i=1,\ldots,k$, הם פרוקים של a ו b, בהתאמה, כמכפלה של מספרים ראשוניים. נסמן

$$\gamma_i=\min(\alpha_i,\beta_i) \text{ ו } \delta_i=\max(\alpha_i,\beta_i),$$

$i=1,\ldots,k$. אזי

$(a,b)=p_1^{\gamma_1}\cdots p_k^{\gamma_k}$ הוא **המחלק משותף הגדול ביותר** (**מ.מ.ג.ב.**) של a,b ו

$[a,b]=p_1^{\delta_1}\cdots p_k^{\delta_k}$ היא **הכפולה משותפת הקטנה ביותר** (**כ.מ.ק.ב.**) של a,b.

הערה: מההגדרה נובע

(א) עבור $a,b>0$ מתקים $(a,b)[a,b]=ab$.

(ב) ה מ.מ.ג.ב של a,b מקים $(a,b)|a,b$ ו $c|a,b \Leftarrow c|(a,b)$.

להיפך, אם $d\in\mathbb{N}$ מקים $d|a,b$ ו $c|a,b \Leftarrow c|d$, אז $d=(a,b)$.

עבור $x\in\mathbb{Q}$ אנו מסמנים ב $[x]$ את המספר השלם (היחיד) המקים $[x]\leq x<[x]+1$.

חִלוק עם שארית: *יהיו* $a,b\in\mathbb{Z}$ *עם* $b\neq 0$*. אזי קימים* $q,r\in\mathbb{Z}$ *כך ש*

$$a=bq+r \text{ ו } 0\leq r<|b|.$$

הוכחה: אם $b>0$, אז $q:=\left[\frac{a}{b}\right]$ ו $r:=a-bq$ מקימים $a=bq+r$ ו $q\leq\frac{a}{b}<q+1$. לכן $bq\leq a<bq+b$ (כי $b>0$) ומכאן $0\leq r=a-bq<b$.

אם $b<0$, אז קיימים לפי הפסקה הקודמת $q',r'\in\mathbb{Z}$ כך ש $a=(-b)q'+r'$ ו $0\le r'<-b$. לכן $q:=-q'$ ו $r:=r'$ מקיימים $a=bq+r$ ו $0\le r<|b|$. ∎

האלגוריתם של אוקליד למציאת מ.מ.ג.ב.: *יהיו* $a,b\in\mathbb{Z}$ *עם* $b\neq 0$. *ע"י חלוק עם שארית נמצא* $q_1,\ldots,q_{k+1}\in\mathbb{Z}$ ו $r_1,\ldots r_k\in\mathbb{Z}$ עם $|b|>r_1>r_2>\ldots>r_k>r_{k+1}=:0$ כך ש

$$\begin{aligned} a &= bq_1+r_1\\ b &= r_1q_2+r_2\\ r_1 &= r_2q_3+r_3\\ &\vdots\\ r_{k-2} &= r_{k-1}q_k+r_k\\ r_{k-1} &= r_kq_{k+1}. \end{aligned}$$

אזי $r_k=(a,b)$.

הוכחה: נראה כי $r_k|a,b$ וכי $c|a,b\Rightarrow c|r_k$ ומזה ינבע כי $r_k=(a,b)$.

חלק א: $r_k|a,b$. נוכיח תחילה באנדוקציה על ℓ כי $r_k|r_{k-\ell}$ עבור $\ell=1,\ldots,k-1$.

אכן, מהמשואה האחרונה $r_k|r_{k-1}$ ולכן טענת האנדוקציה נכונה עבור $\ell=1$. יהי $2\le\ell\le k-1$ ונניח כי $r_k|r_{k-1},\ldots,r_k|r_{k-(\ell-1)}$. אזי $r_k|r_{k-(\ell-1)}q_{k-(\ell-2)}+r_{k-(\ell-2)}=r_{k-\ell}$.

עתה, $r_k|r_1,r_k|r_2\Rightarrow r_k|r_1q_2+r_2=b$ ומכאן גם $r_k|bq_1+r_1=a$.

חלק ב: $c|a,b\Rightarrow c|r_k$. יהי $c\in\mathbb{Z}$ המקיים $c|a,b$. נוכיח באנדוקציה על ℓ כי $c|r_\ell$, $\ell=1,\ldots,k$.

אכן, $c|a-bq_1=r_1$ ומכאן גם $c|b-r_1q_2=r_2$. יהי $3\le\ell\le k$ ונניח כי $c|r_1,\ldots,c|r_{\ell-1}$. אזי $c|r_{\ell-2}-r_{\ell-1}q_\ell=r_\ell$.

בפרט, עבור $\ell=k$, $c|r_k$. ∎

משפט: *יהיו* $a,b\in\mathbb{Z}$ *לא שניהם אפס. אזי קיימים* $u,v\in\mathbb{Z}$ *כך ש* $(a,b)=au+bv$.

הוכחה: בסמונים של המשפט הקודם, נוכיח באנדוקציה על ℓ כי קיימים $u_\ell,v_\ell\in\mathbb{Z}$ כך ש $r_\ell=au_\ell+bv_\ell$ עבור $\ell=1,\ldots,k$.

אכן, הטענה נכונה עבור $\ell=1$: $r_1=a-bq_1=a\cdot 1+b\cdot(-q_1)$. לכן גם עבור $\ell=2$:

$$r_2=b-r_1q_2=b-(a-bq_1)q_2=a\cdot(-q_2)+b\cdot(1+q_1q_2).$$

יהי $3\le\ell\le k$ ונניח כי $r_i=au_i+bv_i$ לכל i בין 1 ל $\ell-1$. אזי

$$r_\ell=r_{\ell-2}-r_{\ell-1}q_\ell=(au_{\ell-2}+bv_{\ell-2})-(au_{\ell-1}+bv_{\ell-1})q_\ell=au_\ell+bv_\ell,$$

באשר $u_\ell=u_{\ell-2}-u_{\ell-1}q_\ell$ ו $v_\ell=v_{\ell-2}-v_{\ell-1}q_\ell$.

בפרט, עבור $\ell=k$, $(a,b)=r_k=au+bv$, באשר $u=u_k,v=v_k$. ∎

הגדרה: $a, b \in \mathbb{Z}$ יקראו **זרים** אם הם ללא גורם משותף, כלומר אם $(a,b) = 1$.

הערה: $a, b \in \mathbb{Z}$ זרים אם"ם קימים $u, v \in \mathbb{Z}$ כך ש $au + bv = 1$.

אכן, התנאי ההכרחי נובע מהמשפט. כמו־כן, התנאי שקימים $u, v \in \mathbb{Z}$ כך ש $au + bv = 1$ הוא מספיק כי $(a,b)|a, b \Leftarrow (a,b)|au + bv = 1$ ולכן $(a,b) = 1$.

מסקנה: *יהיו* $a, b, c \in \mathbb{Z}$ *כך ש* $c|ab$ *וכן* a, c *זרים. אזי* $c|b$.

הוכחה: כיון ש $(a,c) = 1$, נובע מהמשפט שקימים $u, v \in \mathbb{Z}$ כך ש $au + cv = 1$. כפל ב b נותן $b = \underbrace{abu}_{c|} + \underbrace{cbv}_{c|}$ ולכן $c|b$. ∎

הערה: נתן להוכיח את המסקנה גם ע"י שמוש בעובדה ש $\mathbb{Z}$ הוא חוג בעל פריקות יחידה (המשפט היסודי של האריתמטיקה).

טענה: *כל* $a, b \in \mathbb{Z} \setminus \{0\}$ *נתנים לפרוק (לאו דוקא יחיד) בצורה* $a = a_1a_2$, $b = b_1b_2$ עם a_1, a_2, b_1, b_2 ב $\mathbb{Z}$ כך ש $(a_1, a_2) = 1$, $(b_1, b_2) = 1$, $(a_1, b_1) = 1$, $(a_2, b_2) = 1$ וכן $(a,b) = a_1b_1$ ו $[a,b] = a_2b_2$.

הוכחה: נניח, לשם פשטות, $a, b \in \mathbb{N}$ ונפרק אותם בצורה $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ ו $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ עם $\alpha_i, \beta_i \geq 0$, $i = 1, \ldots, k$. יהיו $\gamma_i = \min(\alpha_i, \beta_i)$ ו $\delta_i = \max(\alpha_i, \beta_i)$, $i = 1, \ldots, k$. נסמן

$$a_1 = \prod_{\substack{i \\ \alpha_i = \gamma_i}} p_i^{\gamma_i}, \qquad b_1 = \frac{(a,b)}{a_1} = \prod_{\substack{j \\ \beta_j = \gamma_j < \delta_j = \alpha_j}} p_j^{\gamma_j},$$

$$a_2 = \frac{a}{a_1} = \prod_{\substack{i \\ \beta_i = \gamma_i < \delta_i = \alpha_i}} p_i^{\delta_i}, \qquad b_2 = \frac{[a,b]}{a_2} = \prod_{\substack{j \\ \alpha_j = \gamma_j \leq \delta_j = \beta_j}} p_j^{\delta_j}.$$

אזי $a_1, a_2, b_1, b_2 \in \mathbb{N}$, $a_1b_1 = (a,b)$, $a_2b_2 = [a,b]$, $a_1a_2 = a$ ו $b_1b_2 = \frac{(a,b)[a,b]}{a_1a_2} = \frac{ab}{a} = b$. כמו־כן, $(a_1, a_2) = 1$, $(b_1, b_2) = 1$, $(a_1, b_1) = 1$ ו $(a_2, b_2) = 1$. ∎

דוגמה: $a = 2 \cdot 3^2 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13^4$ ו $b = 2^3 \cdot 3^5 \cdot 5 \cdot 7^2 \cdot 11^3 \cdot 13^2$.

אזי $a_1 = 2 \cdot 3^2 \cdot 7^2 \cdot 11$, $a_2 = 5^3 \cdot 13^4$, $b_1 = 5 \cdot 13^2$ ו $b_2 = 2^3 \cdot 3^5 \cdot 7^2 \cdot 11^3$ זרים ביניהם ומקימים $a_1b_1 = (a,b)$ ו $a_2b_2 = [a,b]$.

ראינו ש $\mathbb{Z}_n$ הוא חוג. במקרה ש n הוא מספר ראשוני, $\mathbb{Z}_n$ הוא אפילו שדה. כלומר, בנוסף, $\mathbb{Z}_n \setminus \{0\}$ היא חבורה חלופית ביחס לכפל:

משפט: *יהי* $p \in \mathbb{N}$ *מספר ראשוני. אזי* $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$.

הוכחה: יש להראות שכל $[a] \in \mathbb{Z}_p \setminus \{[0]\}$ הוא הפיך.

אכן, יהי $a \in \{1, 2, \ldots, p-1\}$. אזי $(a, p) = 1$. לכן קיימים $u, v \in \mathbb{Z}$ כך ש $au + pv = 1$. מכאן $au \equiv 1 \pmod{p}$. לכן $[a][u] = [1]$, כלומר $[a]$ הפיך. ∎

הוכחה אחרת: יהי $a \in \mathbb{Z}$ כך ש $(a, p) = 1$. נכפל את a ב $1, 2, \ldots, p-1$:

$$1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a. \qquad (*)$$

p אינו מחלק אף אחד מהמספרים ב $(*)$ (מיחידות הפרוק). לכן $[a], [2a], \ldots, [(p-1)a]$ מחלקות שונות מאפס. כמו־כן, אף שני מספרים מ $(*)$ אינם קונגרואנטים. אכן, יהיו $p > r_1 \geq r_2 > 0$ כך ש $r_1 a \equiv r_2 a \pmod{p}$. אזי $p | (r_1 - r_2)a$. לכן, כיון ש $(a, p) = 1$, $p | r_1 - r_2$. מכאן, כיון ש $0 \leq r_1 - r_2 < p$, נובע $r_1 - r_2 = 0$. כלומר $r_1 = r_2$.

עתה, הקבוצות $\{[1], [2], \ldots, [p-1]\}$ ו $\{[a], [2a], \ldots, [(p-1)a]\}$ מכילות $p-1$ מחלקות שונות שכלן שונות מ $[0]$. לכן הן שוות. מכאן אחת ורק אחת מבין המחלקות של הקבוצה השניה תקים $[ax] = [1]$ ולכן $[x]$ הוא ההפכי של $[a]$.

כל a בקבוצה $\{1, \ldots, p-1\}$ הוא זר ל p. לכן מהטעון לעיל נובע שלכל $[a]$ בקבוצה $\mathbb{Z}_p \setminus \{[0]\} = \{[1], \ldots, [p-1]\}$ יש הפיך. ∎

המשפט הקטן של פרמה: *יהי* p *מספר ראשוני ויהי* $a \in \mathbb{Z}$ *כך ש* $p \nmid a$ *(*p *אינו מחלק את* a*). אזי* $a^{p-1} \equiv 1 \pmod{p}$.

הוכחה: כיון ש $(a, p) = 1$ נובע מהטעון לעיל ש

$$\{[a], [2a], \ldots, [(p-1)a]\} = \{[1], [2], \ldots, [p-1]\}.$$

לכן $$[a] \cdot [2a] \cdots [(p-1)a] = [1] \cdot [2] \cdots [p-1].$$

כלומר $$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}.$$

מכאן $$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

כיון ש $((p-1)!, p) = 1$ נתן, בעזרת טענת העזר הבאה, לצמצם את $(p-1)!$ ולקבל

$$a^{p-1} \equiv 1 \pmod{p}. \qquad ∎$$

טענת עזר: *יהיו* $a, b, c, m \in \mathbb{Z}$ *כך ש* $c \cdot a \equiv c \cdot b \pmod{m}$ *ו* $(c, m) = 1$*. אזי* $a \equiv b \pmod{m}$.

הוכחה: $c \cdot a \equiv c \cdot b \pmod{m}$ פירושו $m | c(a-b)$. לכן, כיון ש $(c, m) = 1$, $m | a - b$. כלומר $a \equiv b \pmod{m}$. ∎

נמצא כעת את $\mathbb{Z}_m^\times$ עבור מספר טבעי m.

טענה: *עבור* $a \in \mathbb{Z}$, $[a] \in \mathbb{Z}_m^\times$ אמ"ם $(a,m)=1$.

הוכחה: $[a] \in \mathbb{Z}_m^\times \Leftrightarrow$ קים $x \in \mathbb{Z}$ כך ש $ax \equiv 1 \pmod m \Leftrightarrow$ קים $x \in \mathbb{Z}$ וקים $k \in \mathbb{Z}$ כך ש $ax - 1 = mk \Leftrightarrow$ קימים $u, v \in \mathbb{Z}$ כך ש $au + mv = 1 \Leftrightarrow (a,m)=1$. ∎

סִמון: $U(m) = \{a \in \mathbb{Z} \mid 1 \le a \le m,\ (a,m)=1\}$.

מהטענה נובע ש $U(m) = \mathbb{Z}_m^\times$ היא חבורה ביחס לכפל מודולו m.

דֻגמה: $U(8) = \{1,3,5,7\}$.

סִמון: מספר האברים בחבורה $U(m)$ מסמן ב $\Phi_m = |U(m)|$ והפונקציה $\Phi\colon \mathbb{N} \to \mathbb{N}$ המגדרת ע"י $\Phi(m) = \Phi_m$ נקראת פונקצית Φ של אוילר.

המשפט הבא הוא הכללה של משפט פרמה עבור $m = p$.

המשפט של אוילר: *יהי* $m \in \mathbb{N}$ *ויהי* $a \in \mathbb{Z}$ *כך ש* $(a,m)=1$. *אזי* $a^{\Phi(m)} \equiv 1 \pmod m$.

הוכחה: ההוכחה דומה להוכחה של משפט פרמה. נניח $U(m) = \{a_1, a_2, \ldots, a_k\}$, באשר $k = \Phi_m$. אזי $aa_1, aa_2, \ldots, aa_k$ בלתי קונגרואנטים זה לזה: $aa_i \equiv aa_j \pmod m \Leftarrow m|a(a_i - a_j) \Leftarrow m|a_i - a_j$ (כי $(a,m)=1$) $\Leftarrow a_i = a_j$ (כי $0 \le |a_i - a_j| < m$). כמו־כן, כיון ש $(a,m)=1$ ו $(a_i,m)=1$, נובע מטענת העזר הבאה כי $(aa_i, m) = 1$ לכל i בין 1 ל k. לכן הקבוצה $\{[aa_1], \ldots, [aa_k]\}$ מכילה k מחלקות שקילות שונות ומוכלת בקבוצה $\{[c] \mid c \in \mathbb{Z},\ (c,m)=1\} = \{[a_1], \ldots, [a_k]\}$. מכאן הקבוצות זהות וכמו בהוכחת משפט פרמה אנו מקבלים

$$aa_1 \cdot aa_2 \cdots aa_k \equiv a_1 \cdot a_2 \cdots a_k \pmod m.$$

לכן

$$a^k a_1 \cdots a_k \equiv a_1 \cdots a_k \pmod m.$$

כיון ש a_i זר ל m לכל i בין 1 ל k, נתן לצמצם אותם ולקבל $a^k \equiv 1 \pmod m$. ∎

טענת עזר: *יהיו* $a, b, m \in \mathbb{Z}$ *כך ש* $(a,m)=1$ *ו* $(b,m)=1$. *אזי* $(ab,m)=1$.

הוכחה: כיון ש $(a,m)=1$ ו $(b,m)=1$, קימים $u_1, v_1, u_2, v_2 \in \mathbb{Z}$ כך ש $au_1 + mv_1 = 1$ ו $bu_2 + mv_2 = 1$. לכן

$$ab \cdot u_1u_2 + m \cdot (bv_1u_2 + mv_1v_2 + au_1v_2) = (au_1 + mv_1)(bu_2 + mv_2) = 1.$$

מכאן $(ab,m)=1$. ∎

דֻגמה: $m=9$, $a=4$. אזי $U(9)=\{1,2,4,5,7,8\}$ ו

$$4\cdot 1\equiv 4,\ 4\cdot 2\equiv 8,\ 4\cdot 4\equiv 7,\ 4\cdot 5\equiv 2,\ 4\cdot 7\equiv 1,\ 4\cdot 8\equiv 5\ (\mathrm{mod}\ 9).$$

מכאן $4\cdot 1\cdot 4\cdot 2\cdot 4\cdot 4\cdot 4\cdot 5\cdot 4\cdot 7\cdot 4\cdot 8\equiv 4\cdot 8\cdot 7\cdot 2\cdot 1\cdot 5\ (\mathrm{mod}\ 9)$.

לכן $4^6\cdot 1\cdot 2\cdot 4\cdot 5\cdot 7\cdot 8\equiv 4\cdot 8\cdot 7\cdot 2\cdot 1\cdot 5\ (\mathrm{mod}\ 9)$

ולכן $4^6\equiv 1\ (\mathrm{mod}\ 9)$.

נמצא כעת את $\Phi(m)$:

משפט: *יהי* $m>1$ *מספר שלם. נניח* $m=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_k^{\alpha_k}$*, באשר* $p_1,p_2,\ldots,p_k$ *מספרים ראשוניים שונים ו* $\alpha_i>0$*,* $i=1,\ldots,k$*. אזי*

$$\Phi(m)=m(1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})\cdots(1-\tfrac{1}{p_k})\ .$$

הוכחה: נפרק את ההוכחה לשלשה מקרים.

מקרה א: $m=p^r$*,* p *ראשוני.* כדי למצא את קבוצת האברים בין 1 ל p^r הזרים ל p^r, יש להוריד את כל המספרים המתחלקים ב p (כי $(a,p^r)=1\Leftrightarrow(a,p)=1$). יש p^{r-1} כאלו. לכן

$$\Phi(p^r)=p^r-p^{r-1}=p^{r-1}(p-1)=p^r(1-\tfrac{1}{p})\ .$$

מקרה ב: $m=p^rq^s$*,* p,q *ראשוניים שונים.* יש $\frac{m}{p}$ אברים המתחלקים ב p, $\frac{m}{q}$ אברים המתחלקים ב q ו $\frac{m}{pq}$ אברים המתחלקים גם ב p וגם ב q. לכן

$$\Phi(m)=m-\tfrac{m}{p}-\tfrac{m}{q}+\tfrac{m}{pq}=m(1-\tfrac{1}{p})(1-\tfrac{1}{q})\ .$$

מקרה ג: *המקרה הכללי:* $m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$*.* ע"י שקולים דומים מקבלים

$$\Phi(m)=m-\sum_i\frac{m}{p_i}+\sum_{i<j}\frac{m}{p_ip_j}-\sum_{i<j<k}\frac{m}{p_ip_jp_k}+\ldots+(-1)^k\frac{m}{p_1\cdots p_k}\ .$$
$$=m(1-\frac{1}{p})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})$$

כאן השתמשנו בפתוח הפולינום $(X-a_1)\cdots(X-a_k)$ בצורה

$$X^k-\sum_i a_iX^{k-1}+\sum_{i<j}a_ia_jX^{k-2}-\sum_{i<j<k}a_ia_ja_kX^{k-3}+\ldots+(-1)^ka_1\cdots a_k$$

עבור $X=1$ ו $a_i=\frac{1}{p_i}$, $i=1,\ldots,k$. ∎

דֻגמה: $\Phi(77)=77(1-\frac{1}{7})(1-\frac{1}{11})=60$.

הגדרה: יהי $m \in \mathbb{N}$ ויהי $a \in \mathbb{Z}$ כך ש $(a,m)=1$. **הסדר של** a **לפי** m הוא המספר הטבעי הקטן ביותר t כך ש $a^t \equiv 1 \pmod m$ והוא מסומן ב $\mathrm{ord}_m a$.

דוגמה: $\mathrm{ord}_9 1 = 1$, $\mathrm{ord}_9 2 = 6$, $\mathrm{ord}_9 4 = 3$.

שאלה: *עבור אלו* $m \in \mathbb{N}$ *החבורה* $\mathbb{Z}_m^\times$ *היא ציקלית?*

או בנוסח אחר: עבור אלו $m \in \mathbb{N}$ *קים* $a \in U(m)$ *כך ש* $\mathrm{ord}_m a = \Phi(m)$*?*

בתורת המספרים a *נקרא* **שורש פרימיטיבי מודולו** m.

דוגמה: עבור $m=8$, $U(8)=\{1,3,5,7\}$ ו $3^2 \equiv 1,\ 5^2 \equiv 1,\ 7^2 \equiv 1$ מודולו 8 ולכן הסדר של $3,5,7$ הוא 2 ואין אבר שהסדר שלו הוא $\Phi(8)=4$.

תשובה (ללא הוכחה): $\mathbb{Z}_m^\times$ ציקלית אך ורק עבור הערכים הבאים של m:

$$m = 2, 4, p^r, 2p^r ,$$

באשר $p \geq 3$ ראשוני ו $r \geq 1$ טבעי.

במקרה ש $m=p$ ראשוני, העובדה ש $\mathbb{Z}_p^\times$ ציקלית נובעת מכך ש $\mathbb{Z}_p$ שדה ומהטענות הבאות.

טענה 1: *תהי* G *חבורה ויהי* $a \in G$ *אבר מסדר* n *המקים גם* $a^m = 1$*. אזי* $n|m$*.*

הוכחה: נרשם $m = nq + r$ עם $r, q \in \mathbb{Z}$ ו $0 \leq r < n$. אזי $1 = a^m = a^{nq}a^r = a^r$ כי $a^n = 1$. לכן ממזעריות n כך ש $a^n = 1$ נובע כי $r = 0$. מכאן $m = nq$; כלומר $n|m$. ∎

טענה 2: *תהי* G *חבורה ויהיו* a, b *אברים ב* G *מסדרים* r, s*, בהתאמה, כך ש* $ab = ba$ *ו* $(r,s) = 1$*. אזי קים אבר ב* G *מסדר* rs*.*

הוכחה: נוכיח ש ab מסדר rs.

קודם כל $(ab)^{rs} = a^{rs}b^{rs} = (a^r)^s(b^s)^r = 1$.

נניח $t = |ab|$, כלומר $t \geq 1$ הוא מזערי כך ש $(ab)^t = 1$. בודאי $t \leq rs$. נוכיח $t \geq rs$ ואז נסיק $t = rs$.

אכן, כיון ש $a^r = 1$, $b^{rt} = a^{rt}b^{rt} = (ab)^{rt} = ((ab)^t)^r = 1^r = 1$ ולכן מטענה 1 נובע ש $s|rt$ (כי $s = |b|$). מכאן, כיון ש $(r,s) = 1$, נובע ש $s|t$. באותו אופן $r|t$. לכן $rs|t$ (כי $(r,s) = 1$). ∎

טענה 3: *תהי* G *חבורה ויהי* $a \in G$*. נניח* $r = |a|$ *ויהי* $t \in \mathbb{N}$ *כך ש* $t|r$*. אזי* $|a^{\frac{r}{t}}| = t$*.*

הוכחה: $(a^{\frac{r}{t}})^t = a^r = 1$ ועבור $t' < t$, $(a^{\frac{r}{t}})^{t'} = a^{\frac{r}{t}t'} \neq 1$ כיון ש $\frac{r}{t}t' < r$. ∎

טענה 4: *תהי G חבורה ויהיו $a,b\in G$ עם $|a|=r,\ |b|=s$ כך ש $ab=ba$. אזי קיים $c\in G$ כך ש $|c|=[r,s]$.*

הוכחה: נתן לרשם $[r,s]=r_1s_1$ עם $r_1,r_2\in\mathbb{N}$ כך ש $r_1|r,\ s_1|s$ ו $(r_1,s_1)=1$. אזי מטענה 3 נובע כי $|a^{\frac{r}{r_1}}|=r_1$ ו $|b^{\frac{s}{s_1}}|=s_1$. נסמן $a_1=a^{\frac{r}{r_1}}$ ו $b_1=b^{\frac{s}{s_1}}$. אזי $|a_1|=r_1,\ |b_1|=s_1$. לכן מטענה 2 נובע כי $c=a_1b_1$ הוא אבר מסדר $[r,s]=r_1s_1$. ∎

משפט: *יהי $p>1$ מספר ראשוני. אזי $\mathbb{Z}_p^\times$ היא חבורה ציקלית.*

סקיצה של ההוכחה: נבחר $a\in\mathbb{Z}_p^\times$ מסדר מרבי r. אזי $1,a,\ldots,a^{r-1}$ שונים ביניהם. לכן, כיון ש $(a^i)^r=a^{ri}=1$ (כי $a^r=1$), יש למשואה $X^r=1$ r פתרונות שונים בשדה $\mathbb{Z}_p$.

נוכיח שכל $b\in\mathbb{Z}_p^\times$ הוא חזקה של a. לשם כך מספיק להראות ש b פותר את המשואה $X^r=1$. (כאן אנו משתמשים בעובדה שאם F שדה ו $f(X)$ פולינום מעל F, אז $a\in F$ הוא שרש של f אם"ם $(X-a)|f(X)$ מעל F. כמו־כן אנו משתמשים בעובדה שחוג הפולינומים מעל F הוא חוג בעל פריקות יחידה.)

אכן, נניח $|b|=s$. על פי טענה 4 קיים $c\in\mathbb{Z}_p^\times$ כך ש $|c|=[r,s]$. מבחירת r נובע שבהכרח $r=[r,s]$ ולכן $s|r$. לכן $b^r=(b^s)^{\frac{r}{s}}=1$. ∎

10. (א) אם p ראשוני הוכח/י כי $p|\binom{p}{i}$ עבור $i = 1, 2, \ldots, p-1$, באשר $\binom{p}{i} = \frac{p!}{i!\,(p-i)!}$.

(ב) הוכח/י באינדוקציה כי $p|n^p - n$.

(ג) הסק/י את משפט פרמה: אם $p \nmid a$ אזי $a^{p-1} \equiv 1 \pmod{p}$.

11. a, b, c מספרים שלמים $\neq 0$. הוכח/י:

(א) $(a, [b, c]) = [(a, b), (a, c)]$.

(ב) $[a, (b, c)] = ([a, b], [a, c])$.

12. (א) יהיו $b, c \in \mathbb{N}$, $b < c$ וכן $c = bq + r$ באשר $0 \leq r < b$. הראה/י שאם $a^b \equiv 1 \pmod{m}$ וכן $a^c \equiv 1 \pmod{m}$ אזי $a^r \equiv 1 \pmod{m}$.

(ב) נניח $(a, m) = 1$ וכן $\mathrm{ord}_m a = b$. אם $a^c \equiv 1 \pmod{m}$ הוכח/י $b|c$ ובפרט $b|\Phi(m)$.

(ג) אם $a > 1$ טבעי ו n טבעי הראה/י כי $\mathrm{ord}_{a^n-1} a = n$ והסק/י ש $n|\Phi(a^n - 1)$.

13. מצא/י אבר a בשדה $\mathbb{Z}_{17}$ כך שכל אבר $\neq 0$ בשדה שוה לחזקה של a.

14. מצא/י אבר a ב $U(18)$ כך שכל אבר של $U(18)$ שוה לחזקה של a.

15. מהו מספר אברי $U(n)$ באשר $n = 30,\ 50,\ 900,\ 6930,\ 27573$?

16. הראה/י כי כל חבורה בת ארבעה אברים איזומורפית ל $U(5)$ או ל $U(8)$.

17. תהי G חבורה ציקלית מסדר n ויהי a יוצר שלה.

(א) אם $(k, n) = d$ אזי הסדר של a^k הוא $\frac{n}{d}$.

(ב) מספר היוצרים של G הוא $\Phi(n)$.

(ג) בהסתמך על כך ש $U(25)$ ציקלית (נסה/י למצא יוצר) מצא/י מהו מספר היוצרים. מצא/י את התשובה לשאלה דומה במקרה של $U(27)$.

10. (א) יהי p מספר ראשוני. אזי p מופיע (בדיוק פעם אחת) בפרוק של $p! = 1 \cdot 2 \cdots (p-1) \cdot p$ למכפלה של מספרים ראשוניים, אולם p לא מופיע בפרוק של $i! = 1 \cdot 2 \cdots i$ ושל $(p-i)! = 1 \cdot 2 \cdots (p-i)$ למכפלה של מספרים ראשוניים עבור $i = 1, 2, \ldots, p-1$. לכן $p | \frac{p!}{i!\,(p-i)!} = \binom{p}{i}$. (שימו־לב ש $\binom{p}{i} \in \mathbb{N}$.)

(ב) עבור $n = 1$, $p | 0 = 1^p - 1$. נניח באינדוקציה ש $p | n^p - n$ ונוכיח כי $p | (n+1)^p - (n+1)$.
אכן, בעזרת פתוח הבינום של ניוטון ($(a+b)^m = \sum_{i=0}^{m} \binom{m}{i} a^i b^{m-i}$),

$$
\begin{aligned}
(n+1)^p - (n+1) &= \Big(\sum_{i=0}^{p} \binom{p}{i} n^i 1^{p-i}\Big) - (n+1) \\
&= \binom{p}{p} n^p + \Big(\sum_{i=1}^{p-1} \binom{p}{i} n^i\Big) + \binom{p}{0} n^0 - n - 1 \\
&= (n^p - n) + \sum_{i=1}^{p-1} \binom{p}{i} n^i
\end{aligned}
$$

מסעיף (א) $p | \sum_{i=1}^{p-1} \binom{p}{i} n^i$ ומהנחת האינדוקציה $p | n^p - n$. לכן $p | (n+1)^p - (n+1)$.

(ג) מסעיף (ב) נובע ש $p | a^p - a = a(a^{p-1} - 1)$. לכן אם $a \nmid p$, אז $p | a^{p-1} - 1$. כלומר $a^{p-1} \equiv 1 \pmod p$.

11. נניח $a = \pm p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $b = \pm p_1^{\beta_1} \cdots p_k^{\beta_k}$ ו $c = \pm p_1^{\gamma_1} \cdots p_k^{\gamma_k}$, באשר $p_1, \ldots, p_k$ מספרים ראשוניים שונים ו $\alpha_i, \beta_i, \gamma_i \in \mathbb{N} \cup \{0\}$, $i = 1, \ldots, k$.

(א) לכל $\alpha, \beta, \gamma \in \mathbb{N} \cup \{0\}$ מתקיים

$$
\min(\alpha, \max(\beta,\gamma)) = \begin{cases} \alpha & \alpha \le \beta \le \gamma \\ \alpha & \alpha \le \gamma \le \beta \\ \alpha & \beta \le \alpha \le \gamma \\ \gamma & \beta \le \gamma \le \alpha \\ \alpha & \gamma \le \alpha \le \beta \\ \beta & \gamma \le \beta \le \alpha \end{cases} = \max(\min(\alpha,\beta), \min(\alpha,\gamma)) .
$$

מכאן

$$
(a, [b,c]) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \max(\beta_i,\gamma_i))} = \prod_{i=1}^{k} p_i^{\max(\min(\alpha_i,\beta_i), \min(\alpha_i,\gamma_i))} = [(a,b),(a,c)] .
$$

(ב) לכל $\alpha, \beta, \gamma \in \mathbb{N} \cup \{0\}$ מתקיים

$$\max(\alpha, \min(\beta, \gamma)) = \begin{cases} \beta & \alpha \le \beta \le \gamma \\ \gamma & \alpha \le \gamma \le \beta \\ \alpha & \beta \le \alpha \le \gamma \\ \alpha & \beta \le \gamma \le \alpha \\ \alpha & \gamma \le \alpha \le \beta \\ \alpha & \gamma \le \beta \le \alpha \end{cases} = \min(\max(\alpha, \beta), \max(\alpha, \gamma)) .$$

מכאן

$$[a, (b, c)] = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \min(\beta_i, \gamma_i))} = \prod_{i=1}^{k} p_i^{\min(\max(\alpha_i, \beta_i), \max(\alpha_i, \gamma_i))} = ([a, b], [a, c]) .$$

12. (א) נניח $c = bq + r$, $a^b \equiv 1 \pmod{m}$ ו $a^c \equiv 1 \pmod{m}$ (בפרט $(a, m) = 1$). נסמן ב [ ] את מחלקת השקילות מודולו m. אזי

$$[1] = [a^c] = [a^{bq+r}] = [(a^b)^q \cdot a^r] = [a^b]^q \cdot [a^r] = [a^r].$$

כלומר $a^r \equiv 1 \pmod{m}$.

(ב) נניח $(a, m) = 1$, $b = \operatorname{ord}_m a$ ו $a^c \equiv 1 \pmod{m}$. נרשם $c = bq + r$ עם $0 \le r < b$. כיון ש $a^b \equiv 1 \pmod{m}$, נובע מסעיף (א) ש $a^r \equiv 1 \pmod{m}$. אולם b הוא מזערי כך ש $a^b \equiv 1 \pmod{m}$. לכן $r = 0$. כלומר $b|c$. משפט אוילר אומר $a^{\Phi(m)} \equiv 1 \pmod{m}$. לכן בפרט אנו מקבלים $b|\Phi(m)$.

(ג) יהיו $a > 1$ ו n מספרים טבעיים. נסמן $m = a^n - 1$. אזי $a^n \equiv 1 \pmod{m}$. אם גם $a^\ell \equiv 1 \pmod{m}$ עבור $0 < \ell < n$, אז $m|a^\ell - 1$. אולם $0 < a^\ell - 1 < a^n - 1 = m$, סתירה. לכן $n = \operatorname{ord}_m a$. מסעיף (ב) נובע אם־כן ש $n|\Phi(m) = \Phi(a^n - 1)$.

13. כיון ש 17 מספר ראשוני, $\mathbb{Z}_{17}^\times = \{[1], [2], \ldots, [16]\}$ היא חבורה ציקלית מסדר 16. למשל $[3]$ הוא יוצר כי $[3]^1 = [3]$, $[3]^2 = [9]$, $[3]^3 = [10]$, $[3]^4 = [13]$, $[3]^5 = [5]$, $[3]^6 = [15]$, $[3]^7 = [11]$, $[3]^8 = [16]$, $[3]^9 = [14]$, $[3]^{10} = [8]$, $[3]^{11} = [7]$, $[3]^{12} = [4]$, $[3]^{13} = [12]$, $[3]^{14} = [2]$, $[3]^{15} = [6]$, $[3]^{16} = [1]$. (שימו־לב שבעזרת שאלה 17 (ב) מספר היוצרים של $\mathbb{Z}_{17}^\times$ הוא $\Phi(16) = 8 = 16 \cdot (1 - \frac{1}{2})$. לכן לא כל אבר $\neq [1]$ ב $\mathbb{Z}_{17}^\times$ הוא יוצר. למשל $[2]$ אינו יוצר כי $[2]^8 = [1]$.)

14. כיון ש $18 = 2 \cdot 3^2$, $U(18) = \{1, 5, 7, 11, 13, 17\}$ היא חבורה ציקלית מסדר $\Phi(18) = 6$. (על־פי שאלה 17 (ב) מספר היוצרים שלה הוא $\Phi(6) = 2$.) למשל 5 הוא יוצר כי $5^1 \equiv 5$, $5^2 \equiv 7$, $5^3 \equiv 17$, $5^4 \equiv 13$, $5^5 \equiv 11$, $5^6 \equiv 1$ מודולו 18.

15. $|U(30)| = \Phi(2\cdot 3\cdot 5) = 30\cdot(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5}) = 2\cdot 3\cdot 5\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5} = 2\cdot 4 = 8$.

$|U(50)| = \Phi(2\cdot 5^2) = 50\cdot(1-\frac{1}{2})(1-\frac{1}{5}) = 2\cdot 5^2\cdot\frac{1}{2}\cdot\frac{4}{5} = 5\cdot 4 = 20$.

$|U(900)| = \Phi(2^2\cdot 3^2\cdot 5^2) = 900\cdot(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5}) = 2^2\cdot 3^2\cdot 5^2\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5} = 240$.

$|U(6930)| = \Phi(2\cdot 3^2\cdot 5\cdot 7\cdot 11) = 6930\cdot(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})(1-\frac{1}{7})(1-\frac{1}{11}) = 1440$.

$|U(27573)| = \Phi(3\cdot 7\cdot 13\cdot 101) = 27573\cdot(1-\frac{1}{3})(1-\frac{1}{7})(1-\frac{1}{13})(1-\frac{1}{101}) = 14400$.

16. תהי $G=\{1,a,b,c\}$ חבורה בת ארבעה אברים. ישנן רק שתי דרכים אפשריות למלא את טבלת הכפל של G.

דרך א: *בהנחה* $a^2=c$. הנחה זו קובעת את טבלת הכפל באפן יחיד: 1 חיב להופיע במקומות (a,b) ו (b,a) ולכן b מופיע במקומות (a,c) ו (c,a). מכאן c חיב להופיע במקום (b,b) ולכן a מופיע במקומות (b,c) ו (c,b). לבסוף נשאר ש 1 מופיע במקום (c,c).

$(G,\cdot)$	1	a	b	c
1	1	a	b	c
a	a	c	1	b
b	b	1	c	a
c	c	b	a	1

$\cong$

$(U(5),\cdot)$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

במקרה זה $G\cong U(5)$ ע"י $1\mapsto 1$, $a\mapsto 2$, $b\mapsto 3$ ו $c\mapsto 4$. (שימו־לב ש $(U(5),\cdot)\cong(\mathbb{Z}_4,+)$ ע"י $[0]\mapsto 1$, $[1]\mapsto 2$, $[3]\mapsto 3$ ו $[2]\mapsto 4$.)

שימו־לב שההנחה $a^2=b$ גם נותנת טבלת כפל שאיזומורפית לטבלת הכפל של $U(5)$. גם ההנחות $b^2=a$, $b^2=c$, $c^2=a$ ו $c^2=b$ נותנות את אותה טבלת הכפל (עד כדי איזומורפיזם). לכן יש רק עוד דרך אחת ויחידה למלא את טבלת הכפל של G:

דרך ב: *בהנחה* $a^2=b^2=c^2=1$. גם פה, הנחה זו קובעת את טבלת הכפל באפן יחיד: c חיב להופיע במקומות (a,b) ו (b,a) ולכן b מופיע במקומות (a,c) ו (c,a). מכאן a מופיע במקומות (b,c) ו (c,b).

$(G,\cdot)$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

$\cong$

$(U(8),\cdot)$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

במקרה זה $G\cong U(8)$ ע"י $1\mapsto 1$, $a\mapsto 3$, $b\mapsto 5$ ו $c\mapsto 7$.

17. תהי G חבורה ציקלית מסדר n ויהי a יוצר שלה. כלומר $G = \langle a \rangle = \{1, a, a^2 \ldots, a^{n-1}\}$ ולכן $|a| = |\langle a \rangle| = |G| = n$.

(א) נניח $(k,n) = d$. אזי $k = k_1 d$ ו $n = n_1 d$ עם $(k_1, n_1) = 1$. לכן $(a^k)^{\frac{n}{d}} = (a^{k_1 d})^{\frac{n}{d}} = (a^n)^{k_1} = 1$. כמו־כן, אם $(a^k)^t = 1$, אז $n|kt$ (טענה ו בעמוד 2.8). לכן $n_1 d | k_1 dt$ ולכן $n_1 | k_1 t$. מכאן, כיון ש $(k_1, n_1) = 1$, $n_1 | t$. לכן $t \geq n_1 = \frac{n}{d}$. כלומר $|a^k| = \frac{n}{d}$.

(ב) ראינו בסעיף (א) ש $|a^k| = \frac{n}{d}$, באשר $d = (k,n)$. לכן

$$G = \langle a^k \rangle \Leftrightarrow \frac{n}{d} = n \Leftrightarrow (k,n) = d = 1 \Leftrightarrow k \in U(n).$$

מכאן מספר היוצרים של G הוא $|U(n)| = \Phi(n)$.

(ג) כיון ש $25 = 5^2$, $U(25)$ היא חבורה ציקלית מסדר $20 = (1 - \frac{1}{5}) \cdot 25 = \Phi(25) = n$. לכן מסעיף (ב) נובע כי מספר היוצרים שלה הוא $8 = (1-\frac{1}{5})(1-\frac{1}{2}) \cdot 20 = \Phi(20) = \Phi(\Phi(25)) = \Phi(n)$. למשל 2 מהוה יוצר של $U(25)$, כלומר אברי $U(25)$ הם $2^1, 2^2, \ldots, 2^{20}$ מודולו 25. אכן, אם הסדר של 2 הוא לא 20, אז הוא צריך לחלק את 20 (זה נובע למשל מסעיף (א)). יש לבדוק האם $2^k \equiv 1 \pmod{25}$ רק עבור $k|20$: $2^2 \equiv 4 \pmod{25}$, $2^4 \equiv 16 \pmod{25}$, $2^5 \equiv 7 \pmod{25}$ ו $2^{10} \equiv 24 \pmod{25}$. לכן הסדר של 2 הוא 20, כלומר 2 הוא יוצר של $U(25)$.

כיון ש $27 = 3^3$, $U(27)$ היא חבורה ציקלית מסדר $18 = (1-\frac{1}{3}) \cdot 27 = \Phi(27) = n$. לכן מספר היוצרים שלה הוא $6 = (1-\frac{1}{3})(1-\frac{1}{2}) \cdot 18 = \Phi(18) = \Phi(n)$. למשל 2 הוא יוצר של $U(27)$ (צריך לחשב רק 2^k עבור $k|18$ ולבדוק ש $2^k \equiv 1 \pmod{27}$ רק אם $k = 18$).

בסעיף זה נדון בחבורת התמורות על הקבוצה $\{1,\ldots,n\}$. סמנה S_n והיא נקראת **החבורה הסמטרית מדרגה** n. אבר $\sigma \in S_n$ הנו תמורה על $\{1,\ldots,n\}$, כלומר פונקציה חח"ע ועל

$$\sigma\colon \{1,\ldots,n\} \to \{1,\ldots,n\}.$$

אנו מסמנים זאת כך: $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$.

יש $n!$ תמורות על $\{1,\ldots,n\}$, לכן $|S_n| = n!$.

$1 \in S_n$ היא העתקת הזהות, כלומר $1 = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$.

אנו מגדירים מכפלת תמורות כהרכבת פונקציות: אם $\tau = \begin{pmatrix} 1 & 2 & \ldots & n \\ \tau(1) & \tau(2) & \ldots & \tau(n) \end{pmatrix}$, אז

$$\begin{aligned} \sigma\tau &= \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix} \begin{pmatrix} 1 & 2 & \ldots & n \\ \tau(1) & \tau(2) & \ldots & \tau(n) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \ldots & n \\ (\sigma\tau)(1) & (\sigma\tau)(2) & \ldots & (\sigma\tau)(n) \end{pmatrix} \end{aligned}$$

באשר $(\sigma\tau)(i) = \sigma(\tau(i))$, $i = 1,\ldots,n$. לדֻגמה,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}.$$

הצגת תמורה כמכפלה של מחזורים זרים

יהי $\sigma \in S_n$. נגדיר יחס שקילות על $\{1,2,\ldots,n\}$ ע"י: $i \sim j$ אם"ם קים $\tau \in \langle\sigma\rangle$ כך ש $\tau(i) = j$ אם"ם קים $\ell \geq 0$ כך ש $\sigma^\ell(i) = j$. אזי $\{1,2,\ldots,n\}$ מתפרקת למחלקות שקילות

$$\{1,2,\ldots,n\} = \{a_{1,1},\ldots,a_{1,r_1}\} \dot\bigcup \{a_{2,1},\ldots,a_{2,r_2}\} \dot\bigcup \ldots \dot\bigcup \{a_{k,1},\ldots,a_{k,r_k}\}$$

כך ש

$$\sigma(a_{i,1}) = a_{i,2},\ \sigma(a_{i,2}) = a_{i,3},\ldots,\sigma(a_{i,r_i-1}) = a_{i,r_i},\ \sigma(a_{i,r_i}) = a_{i,1},$$

$i = 1,\ldots,k$, ולכן σ נתנת להצגה כמכפלה של מחזורים זרים:

$$\sigma = (a_{1,1}\ldots a_{1,r_1})(a_{2,1}\ldots a_{2,r_2})\cdots(a_{k,1}\ldots a_{k,r_k}).$$

הגדרה: יהיו $a_1,\ldots,a_r \in \{1,\ldots,n\}$ שונים ביניהם. אנו מסמנים ב $(a_1\ldots a_r)$ את התמורה הבאה:

ואם $a_1 \mapsto a_2, \ldots, a_{r-1} \mapsto a_r, a_r \mapsto a_1$ ו־$b \in \{1, \ldots, n\}$, $b \neq a_1, \ldots, a_r$, אז $b \mapsto b$.

תמורה כזאת נקראת **מחזור** (**ציקלוס**, **cycle**). היא מקיימת

$$(a_1 \ldots a_r) = (a_2 \ldots a_r a_1) = \ldots = (a_i a_{i+1} \ldots a_r a_1 \ldots a_{i-1}) = \ldots = (a_r a_1 \ldots a_{r-1}).$$

כמו־כן $(a_1 \ldots a_r)^{-1} = (a_r \ldots a_1)$.

שני מחזורים $(a_1 \ldots a_r)$ ו $(b_1 \ldots b_s)$ נקראים זרים אם $\{a_1, \ldots, a_r\} \cap \{b_1, \ldots, b_s\} = \emptyset$. במקרה זה המחזורים מתחלפים: $(a_1 \ldots a_r)(b_1 \ldots b_s) = (b_1 \ldots b_s)(a_1 \ldots a_r)$.

דֻגמה: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 5 & 8 & 1 & 2 & 7 & 4 \end{pmatrix}$. הפרוק למחלקות שקילות הוא

$$\{1,2,3,4,5,6,7,8\} = \{1,3,5\} \cup \{2,6\} \cup \{4,8\} \cup \{7\}.$$

אזי $\sigma = (135)(26)(48)(7) = (26)(135)(7)(48)$, באשר (135) היא התמורה $1 \mapsto 3, 3 \mapsto 5, 5 \mapsto 1$ ו $i \mapsto i$ לכל $i \neq 1,3,5$, $(2,6)$ היא התמורה $2 \mapsto 6, 6 \mapsto 2$ ו $i \mapsto i$ לכל $i \neq 2,6$, $(4,8)$ היא התמורה $4 \mapsto 8, 8 \mapsto 4$ ו $i \mapsto i$ לכל $i \neq 4,8$, ו (7) היא בעצם תמורת הזהות $i \mapsto i$ לכל i.

ההפכי של σ הוא

$$\sigma^{-1} = \begin{pmatrix} 3 & 6 & 5 & 8 & 1 & 2 & 7 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 1 & 8 & 3 & 2 & 7 & 4 \end{pmatrix}$$

והוא אכן שוה ל $(7)(48)(26)(153) = (7)(84)(62)(531)$.

טענה: *הסדר של מחזור שוה לאורכו.*

הוכחה: אם $\tau = (a_1 \ldots a_r)$ הוא מחזור מאורך r ב S_n, אז $\tau^r = 1$ כי

$$\tau^r(a_i) = \tau^{r-1}(a_{i+1}) = \ldots = \tau^i(a_r) = \tau^{i-1}(a_1) = \ldots = \tau(a_{i-1}) = a_i\ ,$$

$i = 1, \ldots, r$, ועבור $b \in \{1, \ldots, n\}$, $b \neq a_1, \ldots, a_r$, $\tau^r(b) = \tau^{r-1}(b) = \ldots = \tau(b) = b$.

כמו־כן, לכל $1 \leq i < r$, $\tau^i(a_1) = a_{i+1} \neq a_1$ ולכן $\tau^i \neq 1$. מכאן $|\tau| = r$. ∎

בדֻגמה הקודמת $\sigma = \tau_1\tau_2\tau_3\tau_4$ עם $\tau_1 = (135)$ מסדר 3, $\tau_2 = (2,6)$ מסדר 2, $\tau_3 = (4,8)$ מסדר 2 ו $\tau_4 = (7) = 1$ מסדר 1.

הגדרה: יהיו $c_1, \ldots, c_k$ אברים בחבורה G כך ש $c_ic_j = c_jc_i$ לכל i,j. אנו אומרים שאין **יחסים** בין האברים אם מתקים התנאי הבא: אם קימת זהות מהצורה $c_1^{\ell_1} \cdots c_k^{\ell_k} = 1$ עם $\ell_1, \ldots, \ell_k \in \mathbb{Z}$, אז בהכרח $c_1^{\ell_1} = 1, \ldots, c_k^{\ell_k} = 1$.

שימו־לב שאם $\tau_1, \ldots, \tau_k$ הם מחזורים זרים ב S_n, אז אין ביניהם יחסים.

סִמּון: הכפולה המשותפת הקטנה ביותר (כ.מ.ק.ב.) של $r_1, r_2, \ldots, r_k \in \mathbb{N}$ מסומנת ב $[r_1, r_2, \ldots, r_k]$.

בעזרת הטענה הבאה, הסדר של σ מהדֻגמה למעלה הוא $|\sigma| = [3,2,2,1] = 6$.

טענה: *תהי σ תמורה אשר בתור מכפלה של מחזורים זרים היא מהצורה*

$$\sigma = (a_{1,1} \ldots a_{1,r_1})(a_{2,1} \ldots a_{2,r_2}) \cdots (a_{k,1} \ldots a_{k,r_k}).$$

אזי $|\sigma| = [r_1, r_2, \ldots, r_k]$.

הוכחה: נסמן $m = [r_1, \ldots, r_k]$ ו $\tau_1 = (a_{1,1} \ldots a_{1,r_1}), \ldots, \tau_k = (a_{k,1} \ldots a_{k,r_k})$.

כיון ש $\tau_i^{r_i} = 1$ ו $r_i | m$, נובע כי $\tau_i^m = 1$, $i = 1, \ldots, k$. לכן

$$\sigma^m = (\tau_1 \cdots \tau_k)^m = \tau_1^m \cdots \tau_k^m = 1.$$

אם $\ell \in \mathbb{N}$ מקים $\sigma^\ell = 1$, אזי $\tau_1^\ell \cdots \tau_k^\ell = 1$. לכן, כיון שאין יחסים בין $\tau_1, \ldots, \tau_k$, נובע ש $\tau_1^\ell = 1, \ldots, \tau_k^\ell = 1$. כיון ש $|\tau_i| = r_i$, מתקיים $r_i | \ell$, $i = 1, \ldots, k$. לכן $m | \ell$. מכאן $|\sigma| = m$. ∎

דֻגמה: הסדר של התמורה $(1364)(258)(7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 6 & 1 & 8 & 4 & 7 & 2 \end{pmatrix}$ הוא $[4,3,1] = 12$.

רִשום תמורה כמכפלה של חִלופים

הגדרה: מחזור באורך 2 קרוי **חִלוף** (**טרנספוזיציה**, **transposition**).

כל מחזור באורך r הוא מכפלה של $r - 1$ חִלופים. אכן

$$(a_1 a_2 \ldots a_r) = (a_1 a_2)(a_2 a_3) \cdots (a_{r-1} a_r).$$

דֻגמה: $(34)(23)(12) = (1234)$. אכן $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 4$ ו $4 \mapsto 3 \mapsto 2 \mapsto 1$.

נניח $\sigma \in S_n$ היא מכפלה של k מחזורים זרים:

$$\sigma = (a_{1,1} \ldots a_{1,r_1})(a_{2,1} \ldots a_{2,r_2}) \cdots (a_{k,1} \ldots a_{k,r_k}).$$

אזי σ נתנת לרִשום כמכפלה של $(r_1 - 1) + (r_2 - 1) + \ldots + (r_k - 1) = r_1 + \ldots + r_k - k = n - k$ חִלופים.

הגדרה: σ נקראת **זוגית** אם $n - k$ זוגי.

σ נקראת **אי־זוגית** אם $n - k$ אי־זוגי.

כל תמורה זוגית נתנת לכתיבה כמכפלה של מספר זוגי של חִלופים.

כל תמורה אי־זוגית נתנת לכתיבה כמכפלה של מספר אי־זוגי של חִלופים.

דֻגמה: $(123)(4)\in S_4=(123)$ נתנת לכתיבה כמכפלה של 2 חִלופים: $(23)(12)=(123)$, וגם כמכפלה של 4 חִלופים: $(14)(23)(14)(12)=(123)$ (כי החִלופים $(2,3)$, $(1,4)$ זרים, לכן מתחלפים, ו $(14)(14)=1$).

טענה: *אם מכפילים תמורה בחִלוף משתנה הזוגיות.*

הוכחה: נניח σ היא תמורה ב S_n המתפרקת למכפלה של k מחזורים זרים. נכפיל את σ בחִלוף (a_1b_1), באשר $a_1,b_1\in\{1,\dots,n\}$. די להוכיח שמספר המחזורים משתנה ב 1 כי $n-k$ זוגי אם"ם $n-(k\pm 1)$ אי־זוגי. ההוכחה מתפרקת לשני מקרים.

מקרה א: a_1,b_1 *מופיעים באותו מחזור.* במקרה זה σ מכילה מחזור מהצורה $(a_1\dots a_rb_1\dots b_s)$. אזי

$$(a_1b_1)(a_1a_2\dots a_rb_1b_2\dots b_s)=(a_1a_2\dots a_r)(b_1b_2\dots b_s)$$

כי $a_1\mapsto a_2,\dots,a_{r-1}\mapsto a_r$, $a_r\mapsto b_1\mapsto a_1$, $b_1\mapsto b_2,\dots b_{s-1}\mapsto b_s$, ו $b_s\mapsto a_1\mapsto b_1$. כמו־כן

$$(a_1\dots a_rb_1\dots b_s)(a_1b_1)=(a_1b_2\dots b_s)(b_1a_2\dots a_r).$$

מקרה ב: a_1,b_1 *מופיעים במחזורים זרים.* במקרה זה σ מכילה מכפלה של שני מחזורים זרים מהצורה $(a_1\dots a_r)(b_1\dots b_s)$. אזי

$$(a_1b_1)(a_1\dots a_r)(b_1\dots b_s)=(a_1\dots a_rb_1\dots b_s)\quad\text{ו}$$

$$(a_1\dots a_r)(b_1\dots b_s)(a_1b_1)=(a_1b_2b_3\dots b_sb_1a_2a_3\dots a_r).\quad\blacksquare$$

טענה: *תמורה היא זוגית (בהתאמה, אי־זוגית) אם"ם היא מכפלה של מספר זוגי (בהתאמה, אי־זוגי) של חִלופים.*

הוכחה: כוון אחד נובע מתוך ההגדרה: תמורה זוגית (בהתאמה, אי־זוגית) בודאי שנתנת לכתיבה כמכפלה של מספר זוגי (בהתאמה, אי־זוגי) של חִלופים.

להפך, נניח $\sigma=\tau_1\tau_2\cdots\tau_m$ היא מכפלה של מספר זוגי (בהתאמה, אי־זוגי) m של חִלופים $\tau_1,\tau_2,\dots,\tau_m$. אזי, מהטענה הקודמת נובע ש τ_m אי־זוגית $\Leftarrow$ $\tau_{m-1}\tau_m$ זוגית $\Leftarrow$ $\tau_{m-2}\tau_{m-1}\tau_m$ אי־זוגית $\Leftarrow\dots\Leftarrow$ $\sigma=\tau_1\cdots\tau_m$ זוגית (בהתאמה, אי־זוגית) אם m זוגי (בהתאמה, אי־זוגי). $\blacksquare$

סִמון: קבוצת התמורות הזוגיות ב S_n מסומנת ב A_n.

A_n היא תת־חבורה של S_n כי $\mathrm{id}=1\in A_n$ (למשל $\mathrm{id}=(12)(12)$), A_n סגורה תחת הכפל (אם התמורות σ_1,σ_2 הן מכפלות של מספר זוגי של חִלופים, אז גם מכפלתן היא כזאת) ו A_n סגורה תחת לקיחת ההפכי (אם $\sigma=\tau_1\cdots\tau_m$ היא מכפלה של מספר זוגי m של חִלופים $\tau_1,\dots,\tau_m$, אז גם $\sigma^{-1}=\tau_m\cdots\tau_1$ היא כזאת).

אם נכפיל את אברי A_n בחִלוף (12) נקבל את כל התמורות האי־זוגיות ב S_n. לכן

$$|A_n|=\frac{|S_n|}{2}=\frac{n!}{2}.$$

דֻגמה: $S_2=\{\mathrm{id},(12)\}$ ו $A_2=\{\mathrm{id}\}$.

$S_3=\{\mathrm{id},(123),(132),(12),(13),(23)\}$ ו $A_3=\{\mathrm{id},(123),(132)\}$.

סדר 1 $A_4=\{\mathrm{id},$.

סדר 3 $(123),(132),(124),(142),(134),(143),(234),(243),$

סדר 2 $(12)(34),(13)(24),(14)(23)\}$

תרגילים לסעיף 3

18. תהי $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 5 & 4 & 1 & 10 & 9 & 2 & 8 & 6 \end{pmatrix}$.
רשמ/י את σ כמכפלה של מחזורים זרים וכן כמכפלה של חִלופים וקבע/י את הזוגיות של σ ואת הסדר של σ.

19. רשמ/י את $(345)(234)(123)(671)(567)(456)$ כמכפלה של מחזורים זרים.

20. הראה/י שאם $n \geq 3$, אזי A_n נוצרת ע"י מחזורים מסדר 3.

21. כמה אברים מסדר 2 יש בחבורה A_n, עבור $n \leq 8$?

22. כמה אברים מסדר 3 יש בחבורה S_n, עבור $n \leq 6$?

23. (א) הראה/י ש S_n נוצרת ע"י $n-1$ החִלופים $(12),(13),\ldots,(1n)$ וגם ע"י $n-1$ החִלופים $(12),(23),\ldots,(n-1\,n)$.

(ב) הראה/י שאם μ היא תמורה כלשהיא, אזי

$$\mu(i_1 i_2 \ldots i_r)\mu^{-1} = (\mu(i_1)\mu(i_2)\ldots\mu(i_r)).$$

(ג) הראה/י ש (12) ו $(12\ldots n)$ יוצרים את S_n.

(רמז: חשב/י $\mu(12)\mu^{-1}$ באשר μ חזקה של $(12\ldots n)$.)

24. אם $H < S_n$, אזי $H < A_n$ או מספר התמורות הזוגיות השיכות ל H שוה למספר התמורות האי־זוגיות השיכות ל H.

18. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 5 & 4 & 1 & 10 & 9 & 2 & 8 & 6 \end{pmatrix} = (135)(2798)(4)(6\,10)$.

מכאן $\sigma = (15)(13)(28)(29)(27)(6\,10)$

ולכן σ היא תמורה זוגית. הסדר של σ הוא $12 = [3,4,2]$.

19. $(127)(3)(4)(5)(6) = (456)(567)(671)(123)(234)(345)$.

20. יהי $n \geq 3$ מספר טבעי. A_n היא קבוצת התמורות ב S_n הנתנות לִרשום כמכפלה של מספר זוגי של חִלופים. לכן כדי להראות ש A_n נוצרת ע"י מחזורים מסדר 3, מספיק להראות שכל מכפלה של שני חִלופים שונים $(a\,b)$ ו $(c\,d)$, באשר $a, b, c, d \in \{1, \ldots, n\}$, היא מכפלה של מחזורים מסדר 3.

מקרה א: $(a\,b)$ ו $(c\,d)$ *חִלופים זרים.* במקרה זה $(a\,b)(c\,d) = (a\,d\,c)(a\,b\,c)$.

מקרה ב: $a = c$. במקרה זה $(a\,b)(a\,d) = (a\,d\,b)$.

21. ב A_2 וב A_3 אין אברים מסדר 2.

אבר מסדר 2 ב A_4, A_5, A_6 ו A_7 הוא מכפלה של שני חִלופים זרים $(a\,b)$ ו $(c\,d)$. מספר המכפלות מהצורה $(a\,b)(c\,d)$ ב A_n הוא

$$\frac{1}{2!}\binom{n}{2}\binom{n-2}{2} = \frac{1}{2}\cdot\frac{n(n-1)}{2}\cdot\frac{(n-2)(n-3)}{2} = \frac{n(n-1)(n-2)(n-3)}{8}.$$

לכן ב A_4 יש 3 אברים מסדר 2 ($(12)(34), (13)(24), (14)(23)$), ב A_5 יש 15 אברים מסדר 2, ב A_6 יש 45 אברים מסדר 2 וב A_7 יש 105 אברים מסדר 2.

אבר מסדר 2 ב A_8 הוא מכפלה של שני חִלופים זרים (יש $210 = \frac{8\cdot7\cdot6\cdot5}{8}$ חִלופים כאלו) או מכפלה של ארבעה חִלופים זרים $(a\,b)$, $(c\,d)$, $(e\,f)$ ו $(g\,h)$. מספר המכפלות מהצורה $(a\,b)(c\,d)(e\,f)(g\,h)$ ב A_8 הוא

$$\frac{1}{4!}\cdot\binom{8}{2}\binom{6}{2}\binom{4}{2}\binom{2}{2} = \frac{1}{24}\cdot\frac{8\cdot7}{2}\cdot\frac{6\cdot5}{2}\cdot\frac{4\cdot3}{2}\cdot\frac{2\cdot1}{2} = 105.$$

לכן מספר האברים מסדר 2 ב A_8 הוא $315 = 105 + 210$.

22. ב S_2 אין אבר מסדר 3.

אבר מסדר 3 ב A_3, A_4 ו A_5 הוא מחזור מסדר 3. כיון ש $(a\,b\,c) = (b\,c\,a) = (c\,a\,b)$ ו $(a\,c\,b) = (c\,b\,a) = (b\,a\,c)$, מספר המחזורים מסדר 3 ב S_n הוא

$$2\cdot\binom{n}{3} = 2\cdot\frac{n(n-1)(n-2)}{3!} = \frac{n(n-1)(n-2)}{3}.$$

לכן ב S_3 יש 2 אברים מסדר 3 ($(123),(132)$), ב S_4 יש 8 אברים מסדר 3 וב S_5 יש 20 אברים מסדר 3.

אבר מסדר 3 ב S_6 הוא מחזור מסדר 3 (יש $40 = \frac{6\cdot5\cdot4}{3}$ מחזורים כאלו) או מכפלה של שני מחזורים זרים מסדר 3, $(a\,b\,c)$ ו $(d\,e\,f)$. מספר המכפלות מהצורה $(a\,b\,c)(d\,e\,f)$ ב S_6 הוא

$$\frac{1}{2}\cdot\frac{6\cdot5\cdot4}{3}\cdot\frac{3\cdot2\cdot1}{3}=40\,.$$

לכן מספר האברים מסדר 3 ב S_6 הוא $80 = 40 + 40$.

23. (א) כל תמורה ב S_n נתנת לִרשום כמכפלה של חִלופים. לכן כדי להראות ש $(12),(13),\ldots,(1\,n)$ יוצרות את S_n, מספיק להראות שכל חִלוף $(i\,j)$ נתן לרִשום כמכפלה של חִלופים מהצורה $(1\,k)$. אכן, $(i\,j)=(1\,i)(1\,j)(1\,i)$.

נוכיח כעת באינדוקציה על k ($2\le k\le n$) שנתן לרשום את החִלוף $(1\,k)$ כמכפלה של חִלופים מהצורה $(i\;i+1)$. עבור $k=2$, $(1\,2)$ הוא כבר חִלוף מהצורה הזו. נניח כי הטענה נכונה עבור k, $2\le k<n$. אזי

$$(1\;k+1)=(1\,k)(k\;k+1)(1\,k)$$

היא גם מכפלה של חִלופים מהצורה $(i\;i+1)$.

לכן מהפסקה הראשונה נובע שגם החִלופים $(12),(23),\ldots,(n-1\;n)$ יוצרים את S_n.

(ב) תהי μ תמורה ויהי $(i_1i_2\ldots i_r)$ מחזור ב S_n. יהי $j\in\{1,\ldots,n\}$. אם j אינו שיך לקבוצה $\{\mu(i_1),\mu(i_2),\ldots,\mu(i_r)\}$, אז $\mu^{-1}(j)\notin\{i_1,i_2,\ldots,i_r\}$ ולכן

$$\mu(i_1i_2\ldots i_r)\mu^{-1}(j)=\mu\mu^{-1}(j)=j\,.$$

מצד שני, אם $j=\mu(i_k)$ עבור k בין 1 ל $r-1$, אז

$$\mu(i_1i_2\ldots i_r)\mu^{-1}(j)=\mu(i_1i_2\ldots i_r)(i_k)=\mu(i_{k+1})$$

ואם $j=\mu(i_r)$, אז

$$\mu(i_1i_2\ldots i_r)\mu^{-1}(j)=\mu(i_1i_2\ldots i_r)(i_r)=\mu(i_1)\,.$$

לכן $\mu(i_1i_2\ldots i_r)\mu^{-1}=(\mu(i_1)\mu(i_2)\ldots\mu(i_r))$.

(ג) יהי $\mu=(12\ldots n)^k$, באשר $1\le k\le n-2$. אזי קל לראות ש $\mu(1)=k+1$ ו $\mu(2)=k+2$. על־פי סעיף (ב) $\mu(12)\mu^{-1}=(\mu(1)\,\mu(2))=(k+1\;k+2)$. לכן

$$(12),(23),\ldots,(n-1\;n)\in\langle(12),(12\ldots n)\rangle\,.$$

מכאן, על־פי סעיף (א) $\langle(12),(12\ldots n)\rangle=S_n$.

24. תהי H חבורה חלקית של S_n. יש להראות שאם H אינה חבורה חלקית של A_n, אז מספר התמורות הזוגיות השיכות ל H שוה למספר התמורות האי־זוגיות השיכות ל H. אכן, במקרה זה H מכילה תמורה אי־זוגית τ. יהיו $\sigma_1,\sigma_2,\ldots,\sigma_r$ התמורות הזוגיות ב H ויהיו $\tau_1=\tau,\tau_2,\ldots,\tau_s$ התמורות האי־זוגיות ב H. אזי

$\tau\sigma_1, \tau\sigma_2, \ldots, \tau\sigma_r$ הן תמורות אי־זוגיות שונות. לכן $s \leq r$. כמו־כן $\tau\tau_1, \tau\tau_2, \ldots, \tau\tau_s$ הן תמורות זוגיות שונות. לכן $r \leq s$. מכאן $s = r$.

בסעיף 1 הגדרנו איזומורפיזם בין מערכות אלגבריות עם פעולה אחת S,T כהעתקה חח"ע ועל $\varphi\colon S\to T$ המקימת $\varphi(x\cdot y)=\varphi(x)\cdot\varphi(y)$ לכל $x,y\in S$.

בחוגים ובפרט בשדות, שהן מערכות אלגבריות עם שתי פעולות $+$ ו $\cdot$, איזומורפיזם היא העתקה חח"ע ועל φ בין המערכות המקימת $\varphi(x+y)=\varphi(x)+\varphi(y)$ ו $\varphi(x\cdot y)=\varphi(x)\cdot\varphi(y)$ לכל $x,y\in S$.

הערה: אם S היא מערכת אלגברית, T היא קבוצה ו $\varphi\colon S\to T$ היא העתקה חח"ע ועל, נתן להגדיר על T פעולה ההופכת אותה למערכת אלגברית שאיזומורפית ל S ע"י $a\cdot b=\varphi(\varphi^{-1}(a)\cdot\varphi^{-1}(b))$ לכל $a,b\in T$.

הגדרה: יהיו S,T מערכות אלגבריות עם פעולה אחת. העתקה $\varphi\colon S\to T$ נקראת **הומומורפיזם** אם

$$\varphi(x\cdot y)=\varphi(x)\cdot\varphi(y)\quad \text{לכל } x,y\in S.$$

במקרה של שתי פעולות, נדרש דרישה דומה גם על הפעולה השניה.

אם φ חח"ע, אזי φ נקרא **מונומורפיזם** ואנו מסמנים זאת כך $\varphi\colon S\hookrightarrow T$.

אם φ על, אזי φ נקרא **אפימורפיזם**. במקרה זה אנו אומרים ש T היא **תמונה הומומורפית** של S.

אם φ חח"ע ועל, אזי φ נקרא כאמור **איזומורפיזם** ואנו מסמנים זאת כך $\varphi\colon S\cong T$.

הערה: אם $\varphi\colon S\to T$ היא איזומורפיזם, אז גם $\varphi^{-1}\colon T\to S$ איזומורפיזם.

אכן, $a\cdot b=\varphi(\varphi^{-1}(a)\cdot\varphi^{-1}(b))$ עבור $a,b\in T$. לכן $\varphi^{-1}(a\cdot b)=\varphi^{-1}(a)\cdot\varphi^{-1}(b)$.

טענה: *אם $\varphi\colon S\to T$ אפימורפיזם ו S אסוציאטיבית, אזי גם T אסוציאטיבית.*

הוכחה: יהיו $a,b,c\in T$. כיון ש φ על קיימים להם מקורות $x,y,z\in S$, כלומר $a=\varphi(x)$, $b=\varphi(y)$ ו $c=\varphi(z)$. המערכת S אסוציאטיבית ולכן $(xy)z=x(yz)$. כיון ש φ הומומורפיזם

$$\varphi(xy)\varphi(z)=\varphi(x)\varphi(yz)$$

ולכן
$$(\varphi(x)\varphi(y))\varphi(z)=\varphi(x)(\varphi(y)\varphi(z)).$$

כלומר
$$(ab)c=a(bc).$$

מכאן T אסוציאטיבית. ∎

דוגמה: ההעתקה $\varphi\colon\mathbb{Z}\to\mathbb{Z}_m$ המוגדרת ע"י $\varphi(a)=[a]$ היא הומומורפיזם בין מערכות אלגבריות עם שתי פעולות כי

$$\varphi(a+b)=[a+b]=[a]+[b]=\varphi(a)+\varphi(b)$$

ו
$$\varphi(ab)=[ab]=[a][b]=\varphi(a)\varphi(b).$$

כמו־כן, φ היא על. לכן, בעזרת הטענה נובע שב $\mathbb{Z}_m$ מתקימים החֻקים האסוציאטיביים

$$([a]+[b])+[c]=[a]+([b]+[c])\quad \text{ו}\quad ([a][b])[c]=[a]([b][c]).$$

באפן דומה נתן להראות ש $\mathbb{Z}_m$ מקימת את שאר האקסיומות של חוג.

טענה: *יהי $\varphi\colon S\to T$ אפימורפיזם ויהי "1" אבר ניטרלי ב S. אזי $e=\varphi(1)$ אבר ניטרלי ב T.*

הוכחה: נקח $a\in T$ ונוכיח $ea=a=ae$.

כיון ש φ על, קים $x\in S$ כך ש $\varphi(x)=a$.

ב S מתקים $1\cdot x=x=x\cdot 1$

ולכן $\varphi(1\cdot x)=\varphi(x)=\varphi(x\cdot 1)$.

מכאן $\varphi(1)\cdot\varphi(x)=\varphi(x)=\varphi(x)\cdot\varphi(1)$.

כלומר $e\cdot a=a=a\cdot e$. ∎

דרשנו העתקה "על" אולם לעתים אין צרך בדרישה זו, למשל בחבורות.

טענה: *יהי $\varphi\colon G_1\to G_2$ הומומורפיזם בין חבורות ויהיו $1_{G_1},1_{G_2}$ האברים הניטרלים ב G_1,G_2, בהתאמה. אזי $1_{G_2}=\varphi(1_{G_1})$.*

הוכחה: נסמן $e=\varphi(1_{G_1})$. כיון ש $1_{G_1}=1_{G_1}\cdot 1_{G_1}$,

$$e=\varphi(1_{G_1})=\varphi(1_{G_1}\cdot 1_{G_1})=\varphi(1_{G_1})\cdot\varphi(1_{G_1})=e^2.$$

בחבורה, לכל אבר יש הפיך. נכפל את המשואה לעיל ב e^{-1} ונקבל

$$1_{G_2}=e^{-1}\cdot e=e^{-1}\cdot e^2=e=\varphi(1_{G_1}).$$ ∎

הגדרה: אם S,T מונואידים, אזי העתקה $\varphi\colon S\to T$ נקראת **הומומורפיזם של מונואידים** אם φ הוא הומומורפיזם ובנוסף $\varphi(1_S)=1_T$.

לכן אם φ הוא הומומורפיזם בין חוגים עם יחידה ופרט בין שדות, אנו מניחים $\varphi(0)=0$ ו $\varphi(1)=1$.

דֻגמאות: 1. יהיו M,M' מונואידים. ההעתקה השולחת כל $a\in M$ ליחידה $1'$ של M' היא הומומורפיזם של M לתוך M'.

2. יהי $M=(\mathbb{Z},\cdot)$ המונואיד הכפלי של השלמים. ההעתקה φ מ M לתוך M השולחת כל $a\in M$ ל 0 מקימת $\varphi(ab)=0=\varphi(a)\varphi(b)$ לכל $a,b\in M$, אבל היא אינה הומומורפיזם של מונואידים כי $\varphi(1)=0\neq 1$.

טענה: *יהי $\varphi\colon S\to T$ הומומורפיזם בין מונואידים. אזי כל אבר הפיך ב S עובר לאבר הפיך ב T.*

הוכחה: נקח $a\in S$ הפיך ויהי $b\in S$ ההפכי שלו. כלומר

$$ba=1_S=ab.$$

אזי $\varphi(ba)=\varphi(1_S)=\varphi(ab)$

ולכן $\varphi(b)\varphi(a) = 1_T = \varphi(a)\varphi(b)$.

מכאן $\varphi(a)$ הפיך ו $(\varphi(a))^{-1} = \varphi(b) = \varphi(a^{-1})$. (בכתיב חבורי $\varphi(-a) = -\varphi(a)$.) ∎

מסקנה: *אם $\varphi\colon H \to G$ הוא הומומורפיזם של חבורות, אזי התמונה של φ היא חבורה חלקית של G. אנו מסמנים חבורה זו ב $\mathrm{Im}(\varphi)$, כלומר* $\mathrm{Im}(\varphi) = \{\varphi(h) \mid h \in H\} = \varphi(H)$.

הערה: אם $\varphi\colon M \to M'$ הומומורפיזם בין מונואידים, אז באנדוקציה נובע שלכל $a \in M$ ו $k \in \mathbb{N}$ מתקיים $\varphi(a^k) = \varphi(a)^k$. אם a הוא הפיך, ראינו כי $\varphi(a^{-1}) = \varphi(a)^{-1}$. מכאן נובע ש $\varphi(a^k) = \varphi(a)^k$ לכל $k \in \mathbb{Z}$.

דֻגמאות להומומורפיזמים בין חבורות:

1. תהי G חבורה ויהי a אבר כלשהו ב G. ההעתקה $\varphi_a\colon (\mathbb{Z},+) \to G$ המגדרת ע"י $\varphi_a(n) = a^n$ היא הומומורפיזם כי $\varphi(m+n) = a^{m+n} = a^m a^n = \varphi(m)\varphi(n)$.
2. באופן דומה, ההעתקה $(\mathbb{R},+) \to (\mathbb{C}^\times,\cdot)$ המגדרת ע"י $\theta \mapsto e^{i\theta}$ היא הומומורפיזם.
3. תהי $\mathrm{sign}\colon S_n \to \{1,-1\} = (\mathbb{Z},\cdot)^\times$ ההעתקה המגדרת ע"י $\mathrm{sign}(\sigma) = 1$ אם σ תמורה זוגית ו $\mathrm{sign}(\sigma) = -1$ אם σ תמורה אי־זוגית. אזי sign היא הומומורפיזם כי תמורה היא זוגית אם"ם היא נתנת לכתיבה כמכפלה של מספר זוגי של חִלופים ולכן $\mathrm{sign}(\sigma\tau) = \mathrm{sign}(\sigma)\mathrm{sign}(\tau)$.
4. תהי G חבורת תמורות של קבוצה X (כלומר $G < S(X)$) ותהי Y קבוצה חלקית ש X **המיוצבת** ע"י G, כלומר $\alpha(Y) \subseteq Y$ לכל $\alpha \in G$. יהי $\alpha|_Y$ הצמצום של α ל Y. אזי ההעתקה $G \to S(Y)$ הנתנת ע"י $\alpha \mapsto \alpha|_Y$ היא הומומורפיזם הנקרא **הומומורפיזם הצמצום**.
5. יהי F שדה ויהי $\mathrm{M}_n(F)$ חוג המטריצות מסדר $n \times n$ מעל F. אנו מסמנים ב $\mathrm{GL}(n,F)$ את החבורה $\mathrm{M}_n(F)^\times$ של כל המטריצות ההפיכות (ביחס לכפל מטריצות) של $\mathrm{M}_n(F)$. היא נקראת **החבורה הלינארית הכללית מסדר** n.

נבנה הומומורפיזם
$$\varphi\colon \mathrm{GL}(n,F) \to F^\times$$
($F^\times$ השדה ללא האפס) ע"י
$$\varphi(A) = \det(A).$$
φ הומומורפיזם כי $\varphi(AB) = \det(AB) = \det(A)\det(B) = \varphi(A)\varphi(B)$.

דֻגמה להומומורפיזם בין חוגים: נסמן ב $F[X]$ את חוג הפולינומים מעל השדה F. תהי A מטריצה ב $\mathrm{M}_n(F)$. ההעתקה
$$\varphi\colon F[X] \to \mathrm{M}_n(F)$$
המגדרת ע"י
$$\varphi(g(X)) = g(A)$$
(הצבת המטריצה בפולינום)

הנה הומומורפיזם: $(g+f)(A) = g(A) + f(A)$.

טענה: *אם $\varphi\colon F_1 \to F_2$ הומומורפיזם בין שדות, אז φ היא חח"ע.*

הוכחה: יהיו $a, b \in F_1$ כך ש $\varphi(a) = \varphi(b)$. בעזרת הטענה הקודמת $\varphi(-b) = -\varphi(b)$. עבור אברים x, y בשדה אנו מסמנים $x - y = x + (-y)$. אזי

$$\varphi(a - b) = \varphi(a) + \varphi(-b) = \varphi(a) - \varphi(b).$$

נניח בשלילה כי $a \neq b$. אזי $0 \neq c = a - b$ מקיים $\varphi(c) = 0$. אולם, מההערה הקודמת נובע ש $\varphi(0) = 0$ ו $\varphi(1) = 1$. בשדה מתקיים $0 \cdot x = 0$ לכל x (בדקו!). לכן

$$1 = \varphi(1) = \varphi(c \cdot c^{-1}) = \varphi(c) \cdot \varphi(c^{-1}) = 0 \cdot \varphi(c^{-1}) = 0.$$

סתירה. ∎

משפט: *יהיו φ ו ψ הומומורפיזמים של חבורה G לתוך חבורה G' ותהי X קבוצת יוצרים עבור G, כלומר $G = \langle X \rangle$. נניח $\varphi(x) = \psi(x)$ לכל $x \in X$. אזי $\varphi = \psi$.*

הוכחה: נסמן $G_1 = \{a \in G \mid \varphi(a) = \psi(a)\}$. אזי $1 \in G_1$ כי $\varphi(1) = 1' = \psi(1)$. אם $a, b \in G_1$, אז $ab \in G_1$ כי $\varphi(ab) = \varphi(a)\varphi(b) = \psi(a)\psi(b) = \psi(ab)$. כמו־כן, אם $a \in G_1$, אז $\varphi(a^{-1}) = \varphi(a)^{-1} = \psi(a)^{-1} = \psi(a^{-1})$. לכן G_1 היא חבורה חלקית של G המכילה את X. מכאן $G = \langle X \rangle \subseteq G_1$ ולכן $G_1 = G$. לכן $\varphi(a) = \psi(a)$ לכל $a \in G$, כלומר $\varphi = \psi$. ∎

הגדרה: אם $\varphi\colon H \to G$ הוא הומומורפיזם בין חבורות, אזי $\mathrm{Ker}(\varphi) = \{h \in H \mid \varphi(h) = 1_G\}$ הוא **הגרעין** של φ.

אם $\varphi\colon R \to S$ הוא הומומורפיזם בין חוגים, אזי $\mathrm{Ker}(\varphi) = \{a \in R \mid \varphi(a) = 0_S\}$ הוא **הגרעין** של φ.

הערה: אם $\varphi\colon H \to G$ הוא הומומורפיזם בין חבורות, אזי $\mathrm{Ker}(\varphi)$ היא חבורה חלקית של H.

אכן, $1 \in \mathrm{Ker}(\varphi)$ כי $\varphi(1) = 1$; $\varphi(h_1) = 1, \varphi(h_2) = 1 \Leftarrow \varphi(h_1 h_2) = \varphi(h_1)\varphi(h_2) = 1$; ו $\varphi(h) = 1 \Leftarrow \varphi(h^{-1}) = (\varphi(h))^{-1} = 1$.

הערה: יהי $\varphi\colon H \to G$ הומומורפיזם בין חבורות. אזי φ חח"ע אם"ם $\mathrm{Ker}(\varphi) = \{1\}$.

אכן, $\varphi(h_1) = \varphi(h_2) \Leftarrow h_1 = h_2$ אם"ם $\varphi(h_1 h_2^{-1}) = 1 \Leftarrow h_1 h_2^{-1} = 1$.

הצגה של חבורה

הצגה של חבורה G **כחבורת מטריצות** היא הומומורפיזם $\varphi\colon G \to \mathrm{GL}(n, F)$

עבור n טבעי ושדה F כלשהם.

הצגה של חבורה G **כחבורת תמורות** היא הומומורפיזם $\varphi\colon G \to S(X)$

באשר $S(X)$ היא קבוצת הפונקציות החח"ע ועל מקבוצה X לתוך עצמה.

כאשר φ היא חח"ע נאמר שההצגה **נאמנה.**

הערה: לפעמים הצגה של חבורה כחבורת מטריצות שקולה להצגה של החבורה כחבורת תמורות. למשל, $S_3 = S(\{1,2,3\}) \cong \mathrm{GL}(2,\mathbb{Z}_2)$ (ראו סעיף 9).

ההעתקה $\varphi\colon G \to S(X)$ מתאימה לכל $g \in G$ איבר $\varphi(g) \in S(X)$; כלומר $\varphi(g)\colon X \to X$ היא העתקה חח"ע ועל.

משפט קיילי (Cayley): *לכל חבורה G קיימת הצגה נאמנה כחבורת פונקציות חח"ע ועל של הקבוצה G.*

כאשר G סופית מסדר n היא נתנת להצגה נאמנה בתוך החבורה S_n.

הוכחה: יש להראות $G \hookrightarrow S(G)$.

עבור $g \in G$ נגדיר פונקציה חח"ע ועל מ G ל G שנסמן אותה g_ℓ (ℓ עבור left): $g_\ell\colon G \to G$ מוגדרת ע"י כפל משמאל ב g, $g_\ell(x) = gx$ לכל $x \in G$.

g_ℓ חח"ע כי $gx = gy \Leftarrow x = y$.

g_ℓ על כי $gx = y \Leftarrow x = g^{-1}y$.

φ הומומורפיזם: יש להראות $(gh)_\ell = g_\ell h_\ell$. אכן, $(gh)_\ell(x) = (gh)x$ ו $(g_\ell h_\ell)(x) = g_\ell(h_\ell(x)) = g(hx)$ לכל $x \in G$. לכן התוצאה נובעת מהחֹק האסוציאטיבי $(gh)x = g(hx)$.

φ חח"ע: מספיק להראות $\mathrm{Ker}(\varphi) = \{1\}$. אכן, אם g_ℓ היא פונקצית הזהות, כלומר $g_\ell(x) = x$ לכל $x \in G$, אזי $gx = x$ לכל $x \in G$, זאת אומרת $g = 1$.

כאשר G סופית מסדר n, אזי $S(G) \cong S_n$ ולכן $G \hookrightarrow S_n$. ∎

תוצאה: *כל חבורה סופית מסדר n איזומורפית לחבורה חלקית של S_n.*

הסבר: אם $G = \{x_1, x_2, \ldots, x_n\}$, אז ההעתקה $G \hookrightarrow S_n$ מגדרת ע"י $g \mapsto \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$ באשר $i_1, i_2, \ldots, i_n$ נתנים ע"י כפל של g משמאל באברי G: $gx_1 = x_{i_1}, gx_2 = x_{i_2}, \ldots, gx_n = x_{i_n}$.

משפט: *אם F שדה, אזי החבורה $\mathrm{GL}(n,F)$ מכילה חבורה איזומורפית ל S_n ולכן לכל חבורה מסדר n יש הצגה נאמנה ב $\mathrm{GL}(n,F)$:* $\qquad G \hookrightarrow S_n \hookrightarrow \mathrm{GL}(n,F)$.

הוכחה: נסמן $e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$. אזי $I = \begin{pmatrix} | & | & & | \\ e_1 & e_2 & \ldots & e_n \\ | & | & & | \end{pmatrix}$ היא מטריצת היחידה ב $\mathrm{GL}(n,F)$.

נגדיר העתקה $\qquad S_n \to \mathrm{GL}(n,F)$

ע"י $$\sigma \mapsto M_\sigma = \begin{pmatrix} | & | & & | \\ e_{\sigma(1)} & e_{\sigma(2)} & \cdots & e_{\sigma(n)} \\ | & | & & | \end{pmatrix}.$$

לדֻגמה, $$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \mapsto M_\sigma = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

כדי להראות שההעתקה היא הומומורפיזם יש להראות $M_\sigma M_\tau = M_{\sigma\tau}$ עבור $\sigma, \tau \in S_n$. לשם כך נוכיח שויון בין העמודות ה i־יות: $(M_\sigma M_\tau)e_i = M_{\sigma\tau}e_i$, עבור $i = 1, \ldots, n$.

שימו־לב שעבור מטריצה M ב $M_n(F)$ מתקיים

$$M = MI = M \begin{pmatrix} | & | & & | \\ e_1 & e_2 & \cdots & e_n \\ | & | & & | \end{pmatrix} = \begin{pmatrix} | & | & & | \\ Me_1 & Me_2 & \cdots & Me_n \\ | & | & & | \end{pmatrix}.$$

בפרט

$$\begin{pmatrix} | & | & & | \\ e_{\sigma(1)} & e_{\sigma(2)} & \cdots & e_{\sigma(n)} \\ | & | & & | \end{pmatrix} = M_\sigma = \begin{pmatrix} | & | & & | \\ M_\sigma e_1 & M_\sigma e_2 & \cdots & M_\sigma e_n \\ | & | & & | \end{pmatrix}.$$

לכן $$M_\sigma e_i = e_{\sigma(i)}.$$

מכאן $$(M_\sigma M_\tau)e_i = M_\sigma(M_\tau e_i) = M_\sigma(e_{\tau(i)}) = e_{\sigma(\tau(i))} = e_{(\sigma\tau)(i)} = M_{\sigma\tau}e_i.$$

ההעתקה היא חח"ע כי אם σ בגרעין, כלומר $M_\sigma = I$, אז $e_{\sigma(i)} = M_\sigma e_i = Ie_i = e_i$ ולכן $\sigma(i) = i$, $i = 1, \ldots, n$; מכאן $\sigma = \mathrm{id}$.

קבלנו אם־כן ש $S_n \hookrightarrow \mathrm{GL}(n, F)$ ולכן $\mathrm{GL}(n, F)$ מכילה חבורה חלקית שאיזומורפית ל S_n: $S_n \cong \{M_\sigma \mid \sigma \in S_n\} < \mathrm{GL}(n, F)$. ∎

אוטומורפיזמים

הגדרה: הומומורפיזם של מונואיד M לתוך עצמו נקרא **אנדומורפיזם** ואיזומורפיזם של M על M נקרא **אוטומורפיזם**.

הערה: העתקת הזהות היא אוטומורפיזם. אם φ הוא אנדומורפיזם של חבורה G כך ש φ היא העתקת הזהות על קבוצה של יוצרים של G, אז ממשפט קודם נובע כי $\varphi = \mathrm{id}$.

הערה: אם φ הוא אנדומורפיזם של חבורה G, אזי הקבוצה $\mathrm{Fix}(\varphi) = \{a \in G \mid \varphi(a) = a\}$ היא חבורה חלקית של G.

הרכבת הומומורפיזמים: יהיו $\varphi\colon M \to M'$ ו $\psi\colon M' \to M''$ הומומורפיזמים של מונואידים. אזי עבור $a, b \in M$, $\psi\varphi(ab) = \psi(\varphi(ab)) = \psi(\varphi(a)\varphi(b)) = (\psi\varphi(a))(\psi\varphi(b))$. כמו־כן $\psi\varphi(1) = \psi(1') = 1''$ היחידה של M''. לכן $\psi\varphi\colon M \to M''$ הוא הומומורפיזם. אם φ ו ψ הם איזומורפיזמים, אז גם $\psi\varphi$ הוא איזומורפיזם.

הגדרה: עבור מונואיד M אנו מסמנים ב $\mathrm{End}(M)$ את קבוצת האנדומורפיזמים של M וב $\mathrm{Aut}(M)$ את קבוצת האוטומורפיזמים של M שהיא קבוצה חלקית של $\mathrm{End}(M)$.

העתקת הזהות היא אוטומורפיזם, הרכבת אוטומורפיזם היא אוטומורפיזם ואם $\varphi\colon M \to M$ אוטומורפיזם, אז גם $\varphi^{-1}\colon M \to M$ אוטומורפיזם. לכן $\mathrm{Aut}(M)$ היא חבורה הנקראת **חבורת האוטומורפיזמים** של M. באופן דומה $\mathrm{End}(M)$ הוא מונואיד הנקרא **מונואיד האנדומורפיזמים** של M.

אוטומורפיזם פנימי: תהי G חבורה. עבור $a \in G$ אנו מגדירים את **האוטומורפיזם הפנימי** (או **ההצמדה**) I_a להיות ההעתקה $x \mapsto axa^{-1}$ ב G. I_a היא אכן אוטומורפיזם כי

$$I_a(xy) = axya^{-1} = (axa^{-1})(aya^{-1}) = I_a(x)I_a(y)$$

וההפכי של I_a נתון ע"י $I_{a^{-1}}$.

ההעתקה $G \to \mathrm{Aut}(G)$ הנתנת ע"י $a \mapsto I_a$ היא הומומורפיזם כי

$$I_{ab}(x) = abx(ab)^{-1} = a(bxb^{-1})a^{-1} = aI_b(x)a^{-1} = I_a(I_b(x))$$

לכל $x \in G$ ולכן $I_{ab} = I_aI_b$. מכאן $\{I_a \mid a \in G\}$ היא חבורה חלקית של $\mathrm{Aut}(G)$. חבורה זאת מסומנת ב $\mathrm{Inn}(G)$ ונקראת **חבורת האוטומורפיזמים הפנימיים** של G.

תרגילים לסעיף 4

25. תהי G חבורה סופית וקומוטטיבית מסדר n ויהי k זר ל n. נגדיר העתקה $\varphi\colon G \to G$ ע"י $\varphi(x) = x^k$.
הוכח/י כי φ איזומורפיזם והסק/י שלכל $a \in G$ קים פתרון יחיד למשואה $x^k = a$.

26. הראה/י שההעתקה $\varphi\colon (\mathbb{C}^\times, \cdot) \to (\mathbb{R}, +)$ המוגדרת ע"י $\varphi(z) = \log|z|$ היא הומומורפיזם ומצא/י את הגרעין.

27. האם $(\mathbb{Z}, +) \cong (\mathbb{Q}, +)$?

28. הראה/י ש $a \mapsto a^{-1}$ הוא אוטומורפיזם של חבורה G אם"ם G היא אבלית ואם G היא אבלית, אז $a \mapsto a^k$ הוא אנדומורפיזם לכל $k \in \mathbb{Z}$.

29. (א) קבע/י את $\mathrm{Aut}(\mathbb{Z})$.
(ב) קבע/י את $\mathrm{Aut}(\mathbb{Z}_n)$.

30. קבע/י את $\mathrm{Aut}(S_3)$.

25. נתון G קומוטטיבית, $|G| = n$, $(k,n) = 1$ ו $\varphi\colon G \to G$ המוגדרת ע"י $\varphi(x) = x^k$.

φ הומומורפיזם: כיון ש G קומוטטיבית, $\varphi(xy) = (xy)^k = x^k y^k = \varphi(x)\varphi(y)$.

φ חח"ע: $\varphi(x) = \varphi(y) \Leftarrow x^k = y^k \Leftarrow (xy^{-1})^k = x^k y^{-k} = 1$. נסמן $z = xy^{-1}$. אזי $z \in G$ ו $z^k = 1$. לכן הסדר של z מחלק את n וגם מחלק את k. כיון ש $(k,n) = 1$, z מסדר 1. כלומר $z = 1$ ולכן $x = y$.

כיון ש $|G|$ סופי, φ היא על אם"ם φ היא חח"ע. מכאן φ היא איזומורפיזם.

יהי $a \in G$. כיון ש φ על, קים פתרון למשואה $x^k = a$ וכיון ש φ חח"ע, הפתרון הוא יחיד.

26. נתונה ההעתקה $\varphi\colon (\mathbb{C}^\times, \cdot) \to (\mathbb{R}, +)$ המוגדרת ע"י $\varphi(z) = \log|z|$.

φ הומומורפיזם: $\varphi(zw) = \log|zw| = \log(|z||w|) = \log|z| + \log|w| = \varphi(z) + \varphi(w)$.

הגרעין הוא מעגל היחידה: $\ker\varphi = \{z \mid \log|z| = 0\} = \{z \mid |z| = 1\}$.

27. $(\mathbb{Z},+) \not\cong (\mathbb{Q},+)$. אכן, נניח קים איזומורפיזם $\varphi\colon \mathbb{Z} \to \mathbb{Q}$ ויהי $\varphi(1) = \frac{m}{n}$, באשר $m \in \mathbb{Z}$ ו $n \in \mathbb{N}$. אזי, כיון ש $\mathbb{Z} = \langle 1 \rangle$, $\varphi(\mathbb{Z}) = \{\frac{mk}{n} \mid k \in \mathbb{Z}\} \neq \mathbb{Q}$ (למשל, אם p מספר ראשוני זר ל n, אז $\frac{1}{p} \in \mathbb{Q} \smallsetminus \varphi(\mathbb{Z})$). כלומר φ אינה על, סתירה.

28. ההעתקה $\varphi_{-1}\colon G \to G$ המוגדרת ע"י $a \mapsto a^{-1}$ היא בברור חח"ע ועל. לכן φ_{-1} היא אוטומורפיזם אם"ם φ_{-1} היא הומומורפיזם אם"ם $b^{-1}a^{-1} = (ab)^{-1} = \varphi_{-1}(ab) = \varphi_{-1}(a)\varphi_{-1}(b) = a^{-1}b^{-1}$ לכל $a, b \in G$ אם"ם $ab = ba$ לכל $a, b \in G$ אם"ם G אבלית.

אם G אבלית, אז ההעתקה $\varphi_k\colon G \to G$ המוגדרת ע"י $a \mapsto a^k$ היא אנדומורפיזם כי

$$\varphi_k(ab) = (ab)^k = a^k b^k = \varphi_k(a)\varphi_k(b)\,.$$

29. (א) כיון ש $(\mathbb{Z},+) = \langle 1 \rangle$, כל אנדומורפיזם $\alpha\colon \mathbb{Z} \to \mathbb{Z}$ נקבע ע"י ערכו ב 1. אם α הוא אוטומורפיזם, אז $\alpha(1)$ חיב להיות יוצר של $(\mathbb{Z},+)$ ולכן $\alpha(1) = 1$ (במקרה זה $\alpha = \mathrm{id}$) או $\alpha(1) = -1$. מכאן $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{id}, \iota\}$, באשר $\iota\colon \mathbb{Z} \to \mathbb{Z}$ הוא האוטומורפיזם המוגדר ע"י $\iota(n) = -n$ לכל $n \in \mathbb{Z}$. שימו־לב כי $\iota^2 = \mathrm{id}$ ולכן $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

(ב) כיון ש $\mathbb{Z}_n = \langle [1] \rangle$, כל אנדומורפיזם נקבע ע"י ערכו ב $[1]$. אכן,

$$\alpha([k]) = \alpha(\underbrace{[1] + \ldots + [1]}_{\text{פעמים } k}) = \underbrace{\alpha([1]) + \ldots + \alpha([1])}_{\text{פעמים } k}$$

ולכן $\alpha([k]) = [k] \cdot \alpha([1])$, באשר המכפלה היא בחוג $\mathbb{Z}_n$. אם α הוא אוטומורפיזם, אז $\alpha([1])$ חיב להיות יוצר של $\mathbb{Z}_n$ ולכן $\alpha([1]) \in \mathbb{Z}_n^\times$ (ראו פתרון שאלה 17 (ב)). עבור כל $[m] \in \mathbb{Z}_n^\times$ נסמן ב $\alpha_{[m]}\colon \mathbb{Z}_n \to \mathbb{Z}_n$ את האוטומורפיזם המוגדר ע"י $\alpha_{[m]}([k]) = [km] = [k][m]$ לכל $[k] \in \mathbb{Z}_n$. אזי

$$\mathrm{Aut}(\mathbb{Z}_n) = \{\alpha_{[m]} \mid [m] \in \mathbb{Z}_n^\times\}.$$

שימו־לב כי $\alpha_{[m_1]} = \alpha_{[m_2]}$ אם"ם $[m_1] = [m_2]$ ו $\alpha_{[m_1]}\alpha_{[m_2]} = \alpha_{[m_1 m_2]}$ עבור $[m_1], [m_2] \in \mathbb{Z}_n^\times$. לכן $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$.

30. $S_3 = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ עם $1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ ו $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ המקיימים $\sigma^3 = 1$, $\tau^2 = 1$ ו $\tau\sigma^2 = \sigma\tau$. לכן $S_3 = \langle \sigma, \tau \rangle$. שימו־לב ש σ, σ^2 הם אברים מסדר 3 ו $\tau, \tau\sigma, \tau\sigma^2$ הם אברים מסדר 2. אם $\alpha\colon S_3 \to S_3$ אוטומורפיזם, אז הוא נקבע ע"י ערכיו ב σ וב τ. כיון ש $|\sigma| = 3$, $|\alpha(\sigma)| = 3$ ולכן $\alpha(\sigma) \in \{\sigma, \sigma^2\}$. כמו־כן, כיון ש $|\tau| = 2$, $|\alpha(\tau)| = 2$ ולכן $\alpha(\tau) \in \{\tau, \tau\sigma, \tau\sigma^2\}$.

עבור $s \in \{\sigma, \sigma^2\}$ ו $t \in \{\tau, \tau\sigma, \tau\sigma^2\}$, תהי $\alpha_{s,t}\colon S_3 \to S_3$ ההעתקה המוגדרת על ידי $\alpha_{s,t}(\tau^i\sigma^j) = t^i s^j$. כדי להראות ש $\alpha_{s,t}$ הומומורפיזם, מספיק לבדוק כי $\alpha_{s,t}(\tau\sigma^2) = \alpha_{s,t}(\tau) \cdot \alpha_{s,t}(\sigma)$. שימו־לב כי $\alpha_{\sigma,\tau} = \mathrm{id}$. נסמן $\beta = \alpha_{\sigma,\tau\sigma}$ ו $\gamma = \alpha_{\sigma^2,\tau}$.

אזי β הומומורפיזם כי

$$\beta(\sigma)\beta(\tau) = \sigma(\tau\sigma) = (\sigma\tau)\sigma = (\tau\sigma^2)\sigma = (\tau\sigma)\sigma^2 = \beta(\tau\sigma^2),$$

$\beta^2 = \alpha_{\sigma,\tau\sigma^2}$ כי $\beta^2(\sigma) = \beta(\sigma) = \sigma$ ו $\beta^2(\tau) = \beta(\tau\sigma) = (\tau\sigma)\sigma = \tau\sigma^2$ ו $\beta^3 = \mathrm{id}$ כי $\beta^3(\sigma) = \beta(\sigma) = \sigma$ ו $\tau = \tau\sigma^2)\sigma^2$... $\beta^3(\sigma) = \beta(\sigma) = \sigma$ ו $\beta^3(\tau) = \beta(\tau\sigma^2) = (\tau\sigma)\sigma^2 = \tau$. בפרט β חח"ע ועל (כי $\beta \circ \beta^2 = \beta^2 \circ \beta = \mathrm{id}$) ולכן β אוטומורפיזם.

כמו־כן, γ הומומורפיזם כי

$$\gamma(\sigma)\gamma(\tau) = \sigma^2\tau = \sigma(\sigma\tau) = \sigma\tau\sigma^2 = \tau\sigma^2\sigma^2 = \tau\sigma^4 = \gamma(\tau\sigma^2)$$

ו $\gamma^2 = \mathrm{id}$ כי $\gamma^2(\sigma) = \gamma(\sigma^2) = \sigma^4 = \sigma$ ו $\gamma^2(\tau) = \gamma(\tau) = \tau$. בפרט γ חח"ע ועל (כי $\gamma \circ \gamma = \mathrm{id}$) ולכן γ אוטומורפיזם.

שימו־לב כי $\gamma\beta = \alpha_{\sigma^2,\tau\sigma^2}$ כי $\gamma\beta(\sigma) = \gamma(\sigma) = \sigma^2$ ו $\gamma\beta(\tau) = \gamma(\tau\sigma) = \tau\sigma^2$. כמו־כן $\beta\gamma = \alpha_{\sigma^2,\tau\sigma} = \gamma\beta^2$ כי $\beta\gamma(\sigma) = \beta(\sigma^2) = \sigma^2 = \gamma(\sigma) = \gamma\beta(\sigma) = \gamma\beta^2(\sigma)$ ו

$$\beta\gamma(\tau) = \beta(\tau) = \tau\sigma = \tau\sigma^4 = \gamma(\tau\sigma^2) = \gamma((\tau\sigma)\sigma) = \gamma\beta(\tau\sigma) = \gamma\beta^2(\tau).$$

לכן

$$\mathrm{Aut}(S_3) = \{\alpha_{\sigma,\tau}, \alpha_{\sigma,\tau\sigma}, \alpha_{\sigma,\tau\sigma^2}, \alpha_{\sigma^2,\tau}, \alpha_{\sigma^2,\tau\sigma^2}, \alpha_{\sigma^2,\tau\sigma}\} = \{\mathrm{id}, \beta, \beta^2, \gamma, \gamma\beta, \gamma\beta^2\} \cong S_3.$$

סעיף 5: חבורת המנה

משפט לגרנג'

נוכיח כאן את משפט לגרנג' האומר שאם H היא חבורה חלקית של חבורה סופית G, אז $|H|\,||G|$.

הגדרה: תהי G חבורה ותהי $H \subseteq G$ חבורה חלקית. $a, b \in G$ יקראו **קונגרואנטים מימין מודולו** H אם $ab^{-1} \in H$. נסמן $a \equiv b \pmod H$.

הערה: $\equiv$ הוא יחס שקילות. אכן,

רפלקסיביות: $a \equiv a$ כי $aa^{-1} = 1 \in H$;

סימטריות: $a \equiv b \Leftarrow ab^{-1} \in H \Leftarrow ba^{-1} = (ab^{-1})^{-1} \in H \Leftarrow b \equiv a$;

טרנזיטיביות: $a \equiv b, b \equiv c \Leftarrow ab^{-1} \in H, bc^{-1} \in H \Leftarrow ac^{-1} = ab^{-1}bc^{-1} \in H \Leftarrow a \equiv c$.

סִמון: עבור $a \in G$ אנו מסמנים ב $[a]$ את מחלקת השקילות $\{b \in G \mid b \equiv a\}$.

טענה: $[a] = \{ha \mid h \in H\}$.

הוכחה: נראה הכלה בשני הכוונים.

כוון א: $\supseteq$. $b = ha \Leftarrow ab^{-1} = a(ha)^{-1} = aa^{-1}h^{-1} = h^{-1} \in H \Leftarrow a \equiv b \Leftarrow b \in [a]$.

כוון ב: $\subseteq$. $b \in [a] \Leftarrow h^{-1} := ab^{-1} \in H \Leftarrow hab^{-1} = 1 \Leftarrow b = ha$. ∎

סִמון: $Ha = \{ha \mid h \in H\}$.

באפן כללי, אם $\emptyset \neq A, B \subseteq G$, אז $AB = \{ab \mid a \in A,\, b \in B\}$.

כיון ש G אסוציאטיבית מתקים $(AB)C = A(BC)$.

שימו־לב כי $Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow [a] = [b]$.

הגדרה: תהי G חבורה ותהי $H \subseteq G$ חבורה חלקית. קבוצה מהצורה Ha, באשר $a \in G$, נקראת **מחלקה ימנית**.

אזי $G = \dot\bigcup_i Ha_i$ הוא אחוד זר של מחלקות ימניות.

הגדרה: מספר המחלקות (הימניות) של H בתוך G נקרא **האינדקס** של H בתוך G ומסומן ב $[G : H]$.

דֻגמה: אם $G = (\mathbb{Z}, +)$ ו $H = (m\mathbb{Z}, +)$, אז $a, b \in G$ קונגרואנטים מודולו H אם"ם הם קונגרואנטים מודולו m. האינדקס של H ב G הוא $[\mathbb{Z} : m\mathbb{Z}] = m$ כי

$$\mathbb{Z} = m\mathbb{Z} \dot\bigcup (m\mathbb{Z} + 1) \dot\bigcup \ldots \dot\bigcup (m\mathbb{Z} + m - 1),$$

באשר $m\mathbb{Z} + \ell = \{mn + \ell \mid n \in \mathbb{Z}\}$.

משפט לגרנג': *תהי* G *חבורה סופית ותהי* $H \subseteq G$ *חבורה חלקית. אזי*

(א) $|H| \big| |G|$.

(ב) $[G:H] \big| |G|$.

(ג) $|G| = [G:H] \cdot |H|$.

הוכחה: (א) ו (ב) נובעים מ (ג).

הוכחת (ג): אם $a \in G$, אז $|Ha| = |H|$. אכן, ההעתקה $Ha \to H$ המגדרת ע"י $h \mapsto ha$ היא חח"ע ועל (כי $h_1 a = h_2 a \Leftrightarrow h_1 = h_2$). נניח $[G:H] = r$, כלומר

$$G = Ha_1 \dot{\bigcup} Ha_2 \dot{\bigcup} \ldots \dot{\bigcup} Ha_r$$

עם $a_1, a_2, \ldots, a_r \in G$. האחוד הוא זר. לכן

$$|G| = |Ha_1| + |Ha_2| + \ldots + |Ha_r| = r \cdot |H| = [G:H] \cdot |H|. \quad \blacksquare$$

תוצאה 1: *אם* G *חבורה סופית ו* $a \in G$*, אז* $|a| \big| |G|$ *וכן* $a^{|G|} = 1$.

הוכחה: כיון ש $\langle a \rangle$ היא חבורה חלקית של G, $|\langle a \rangle| \big| |G|$ $= |a|$. נסמן $|a| = k$ ו $|G| = kt$; אזי $a^{|G|} = (a^k)^t = 1$. $\blacksquare$

תוצאה 2: *אם* G *חבורה מסדר* p*, באשר* p *מספר ראשוני, אז* G *ציקלית.*

הוכחה: יהי $1 \neq a \in G$. אזי $|a| \big| p$ ו $|a| > 1$ ולכן $|a| = p$. מכאן הקבוצה $\{1, a, \ldots, a^{p-1}\}$ מכילה p אברים שונים ולכן זו כל החבורה G. $\blacksquare$

תוצאה 3: *אם* $a \in U(m)$*, אז* $a^{\Phi(m)} = 1$.

הוכחה: תוצאה זו נובעת מתוצאה 1 כיון ש $|U(m)| = \Phi(m)$. $\blacksquare$

הטענה הבאה היא היבט נוסף למשפט לגרנג'.

טענה: *תהי* G *חבורה סופית ונניח* $K < H < G$*. אזי* $[G:K] = [G:H][H:K]$.

הוכחה: ממשפט לגרנג' $[G:K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G:H][H:K]$. $\blacksquare$

הערה: הטענה לעיל נכונה גם עבור חבורות אינסופיות בתנאי שהאינדקסים סופיים. לדֻגמה, אם $m|n$, אז $n\mathbb{Z} \subseteq m\mathbb{Z} \subseteq \mathbb{Z}$ ו $[\mathbb{Z}:n\mathbb{Z}] = n = m \cdot \frac{n}{m} = [\mathbb{Z}:m\mathbb{Z}][m\mathbb{Z}:n\mathbb{Z}]$.

הערה: יתכן מצב ש $k \big| |G|$ אבל אין חבורה חלקית מסדר k. לדֻגמה, A_4 היא חבורה מסדר 12 ואין לה חבורה חלקית מסדר 6 (בדקו!).

טענה: *תהי G חבורה מסדר זוגי. אזי יש ב G אבר מסדר 2.*

הוכחה: אבר מסדר 2 הוא אבר $\neq 1$ והפוך לעצמו.

אם אין ב G אבר מסדר 2 נראה שיש ב G מספר אי־זוגי של אברים ונקבל סתירה. אכן, במקרה זה, $G = \{1, a_1, a_1^{-1}, a_2, a_2^{-1}, \ldots, a_k, a_k^{-1}\}$. (שימו־לב ש $a_j \neq a_i, a_i^{-1} \Leftarrow a_j^{-1} \neq a_i, a_i^{-1}$.)

לכן קים $a \in G$ $1 \neq$ כך ש $a^{-1} = a$ ולכן G מכילה את החבורה החלקית $\{1, a\}$ מסדר 2. ∎

הטענה הבאה היא דֻגמה לשמוש במשפט לגרנג'.

טענה: *תהי G חבורה קומוטטיבית מסדר 6. אזי G היא ציקלית.*

הוכחה: בעזרת תוצאה 1, הסדר של אבר $\neq 1$ ב G הוא 2, 3 או 6. אם קים אבר מסדר 6 ב G, אז סימנו.

בעזרת הטענה הקודמת קים אבר $b \in G$ מסדר 2. נניח בשלילה שקים עוד אבר $c \in G$ מסדר 2. אזי גם $bc \neq 1$ מסדר 2. מכאן $\{1, b, c, bc\}$ היא חבורה חלקית כי לכל אבר יש הפוך וכן $cb = bc$, $(bc)b = b(bc) = c$, $(cb)c = c(cb) = b$ בגלל הקומוטטיביות. אולם $4 \nmid 6$ ולפי משפט לגרנג' לא תתכן חבורה חלקית מסדר 4.

לכן נניח שקים ב G אבר a מסדר 3. כיון ש $ab = ba$ ו $(2,3) = 1$, ab הוא אבר מסדר 6 (טענה 2 מסעיף 2, עמוד 2.8). מכאן $G = \langle ab \rangle$ היא ציקלית. ∎

מהן החבורות החלקיות של החבורות הציקליות ?

משפט: *(א) אם $G = \langle a \rangle$ ציקלית אינסופית, אזי עבור כל $m \geq 1$ טבעי קימת חבורה חלקית $\langle a^m \rangle$ ואלו כל החבורות החלקיות של G, פרט ל $\{1\} = \langle 1 \rangle$.*

(ב) אם $G = \langle a \rangle$ היא ציקלית מסדר m, אזי עבור כל מספר טבעי q כך ש $q|m$ קימת חבורה חלקית אחת ורק אחת מסדר q והיא $\langle a^{\frac{m}{q}} \rangle$.

הוכחה: (א) נניח $G > H \neq \langle 1 \rangle$ ויהי $m \geq 1$ טבעי מזערי כך ש $a^m \in H$ ולכן $\langle a^m \rangle \subseteq H$.

נניח $a^k \in H$ ונרשם $k = ms + t$ עם $0 \leq t < m$. אזי $a^t = a^k a^{-ms} \in H$ ולכן $t = 0$ (ממזעריות m כך ש $a^m \in H$). לכן $k = ms$ ו $a^k = (a^m)^s \in \langle a^m \rangle$. מכאן $H = \langle a^m \rangle$.

בכתיב החבורי, כל החבורות החלקיות של $\mathbb{Z}$ הן $m\mathbb{Z}$ עבור $m \geq 1$ ו $\{0\}$.

(ב) כיון ש $|a| = m$, מתקים $|a^{\frac{m}{q}}| = q$ (טענה 3 מסעיף 2, עמוד 2.8). לכן $\langle a^{\frac{m}{q}} \rangle$ היא חבורה חלקית של G מסדר q. זה מראה קיום.

תהי H חבורה חלקית של G מסדר q. ממשפט לגרנג' נובע ש $q|m$. צריך להוכיח כי $H = \langle a^{\frac{m}{q}} \rangle$. זה ברור כאשר $q = 1$.

אם $q > 1$, נבחר $r \geq 1$ טבעי מזערי כך ש $a^r \in H$. אזי, כמו ב (א) מוכיחים שאם $a^k \in H$, אז $r|k$ ו $H = \langle a^r \rangle$. בפרט, $a^m = 1 \in H$ ולכן $r|m$. כיון ש $|a| = m$, $a^k \neq 1$ עבור $0 < k < m$ ולכן

$$.H=\langle a^r\rangle=\{1,a^r,a^{2r},\ldots,a^{(\frac{m}{r}-1)r}\}$$

לכן $\frac{m}{r}=|H|=q$ ולכן $r=\frac{m}{q}$. מכאן

$$.H=\{1,a^{\frac{m}{q}},a^{\frac{2m}{q}},\ldots,a^{(q-1)\frac{m}{q}}\}=\langle a^{\frac{m}{q}}\rangle$$

בכתיב החבורי, החבורה החלקית של $\mathbb{Z}_m$ מסדר q היא $\{0,\frac{m}{q},\frac{2m}{q},\ldots,(q-1)\frac{m}{q}\}$. (החבור הוא מודולו m לכל $q|m$.) ∎

חבורה חלקית נורמלית

תהי G חבורה ותהי $H\subseteq G$ חבורה חלקית. זכרו ש $a,b\in G$ קונגרואנטים מימין מודולו H אם $ab^{-1}\in H$.

הערה: אם $a\equiv b$, אז $ac\equiv bc$ לכל $c\in G$.

אכן, $a\equiv b \Leftarrow ab^{-1}\in H$ ... כלומר: $a\equiv b \Rightarrow ac(bc)^{-1}=acc^{-1}b^{-1}=ab^{-1}\in H \Rightarrow ac\equiv bc$.

אולם יתכן $a\equiv b$ ו $ca\not\equiv cb$.

דֻגמה: אברי S_3 הם

$$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}.$$

נסמן $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=1$, $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\sigma$ ו $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\tau$. אזי $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\sigma^2$, $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\tau\sigma$ ו $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\tau\sigma^2$. אזי

$$.S_3=\{1,\sigma,\sigma^2,\tau,\tau\sigma,\tau\sigma^2\}$$

שימו־לב ש $\tau^2=1$, $\sigma^3=1$ ו $\sigma\tau=\tau\sigma^2$.

תהי $G=S_3$ ותהי $H=\{1,\tau\}$. אזי $\tau\equiv 1$ כי $\tau\cdot 1^{-1}=\tau\in H$ אולם $\sigma\cdot\tau\not\equiv\sigma\cdot 1$ כי

$$.(\sigma\cdot\tau)(\sigma\cdot 1)^{-1}=\sigma\tau\sigma^{-1}=\tau\sigma^2\sigma^{-1}=\tau\sigma\notin H$$

הגדרה: אברים $a,b\in G$ נקראים **קונגרואנטים משמאל מודולו** H אם $b^{-1}a\in H$.

דֻגמה: בסמונים של הדֻגמה הקודמת, $a=\tau\sigma$ ו $b=\sigma$ קונגרואנטים מימין כי $ab^{-1}=\tau\sigma\sigma^{-1}=\tau$ ב H אולם הם אינם קונגרואנטים משמאל כי $b^{-1}a=\sigma^{-1}\tau\sigma=\sigma^2\tau\sigma=\tau\sigma\sigma=\tau\sigma^2\notin H$ (שימו־לב ש $\sigma\sigma\tau=\sigma(\tau\sigma^2)=(\sigma\tau)\sigma^2=\tau\sigma^2\sigma^2=\tau\sigma\sigma^3=\tau\sigma$).

הגדרה: קבוצה מהצורה aH נקראת **מחלקה שמאלית**.

הערה: $a,b\in G$ קונגרואנטים משמאל אם"ם $aH=bH$ ולכן ca,cb קונגרואנטים משמאל לכל $c\in G$.

כמקודם G היא אחוד זר של המחלקות השמאליות. אם G סופית, אז מספר המחלקות השמאליות הוא באפן דומה $[G:H]=\frac{|G|}{|H|}$.

טענה: *ההעתקה $\{Hx \mid x\in G\}\to\{xH \mid x\in G\}$ הנתנת ע"י $Hx\mapsto x^{-1}H$ היא התאמה חח"ע ועל בין קבוצת המחלקות הימניות לבין קבוצת המחלקות השמאליות של G.*

הוכחה: ההעתקה מוגדרת היטב (כלומר אינה תלויה בנציג של מחלקת השקילות הימנית) כי $Ha=Hb \Leftarrow$ $ab^{-1}\in H \Leftarrow (ab^{-1})^{-1}=ba^{-1}=(b^{-1})^{-1}a^{-1}\in H \Leftarrow a^{-1}H=b^{-1}H$.

כיון ש $(Hx)^{-1}=x^{-1}H^{-1}=x^{-1}H$, ההעתקה היא חח"ע ועל. ∎

הגדרה: אם $ab^{-1}\in H \Leftarrow b^{-1}a\in H$ לכל $a,b\in G$ (קונגרואנציה מימין היא גם קונגרואנציה משמאל), אנו אומרים שהקונגרואנציה היא **קונגרואנציה דו־צדדית** (מימין ומשמאל).

דֻגמה 1: $G=\mathbb{Z}$ ו $H=m\mathbb{Z}$. בגלל הקומוטטיביות מקבלים שקונגרואנציה מימין היא גם קונגרואנציה משמאל בשלמים.

בעזרת קונגרואנציה זו הגדרנו בסעיף 2 את החבורה $(\mathbb{Z}_m,+)$. החבור בה מוגדר היטב, כלומר אם $a_1\equiv b_1 \pmod m$ ו $a_2\equiv b_2 \pmod m$, אז $a_1+a_2\equiv b_1+b_2 \pmod m$.

דֻגמה 2: $G=S_3=\{1,\sigma,\sigma^2,\tau,\tau\sigma,\tau\sigma^2\}$ כמו בדֻגמה קודמת ו $H=\{1,\sigma,\sigma^2\}$.

המחלקות הימניות ב G הן $H=\{1,\sigma,\sigma^2\}$ ו $H\tau=\{\tau,\tau\sigma^2,\tau\sigma\}$ והמחלקות השמאליות ב G הן $H=\{1,\sigma,\sigma^2\}$ ו $\tau H=\{\tau,\tau\sigma,\tau\sigma^2\}$. מתקים $H\tau=\tau H$

S_3 אינה קומוטטיבית, אך היא מקימת $Ha=aH$ לכל $a\in G$.

הערה: אם H היא חבורה חלקית של G שהקונגרואנציה שלה היא דו־צדדית, אז הכפל מודולו H מוגדר היטב.

אכן, נניח $a_1\equiv b_1$ ו $a_2\equiv b_2$. אזי $a_1a_2\equiv b_1a_2$ (בעזרת קונגרואנציה מימין) ו $b_1a_2\equiv b_1b_2$ (בעזרת קונגרואנציה משמאל). לכן $a_1a_2\equiv b_1b_2$.

טענה: *תהי H חבורה חלקית של G. אזי הטענות הבאות הן שקולות:*

(א) הקונגרואנציה היא דו־צדדית, כלומר $ab^{-1}\in H \Leftarrow b^{-1}a\in H$ לכל $a,b\in G$;

(ב) $aH=Ha$ לכל $a\in G$.

הוכחה: נוכיח גרירה בשני הכוונים.

(ב) $\Leftarrow$ (א): נניח $aH=Ha$ לכל $a\in G$. אזי לכל $a,b\in G$ מתקים

$$ab^{-1}\in H \Rightarrow Ha=Hb \Rightarrow aH=bH \Rightarrow b^{-1}a\in H\,.$$

(א) $\Leftarrow$ (ב): נניח $ab^{-1} \in H \Leftarrow b^{-1}a \in H$ לכל $a,b \in G$. נקח $a \in G$ ו $h \in H$ כלשהם ויהי $b = ha$. אזי $ab^{-1} = aa^{-1}h^{-1} = h^{-1} \in H$ ועל סמך ההנחה $a^{-1}h^{-1}a = b^{-1}a \in H$. זה מתקים לכל $h \in H$ ו $a \in G$. לכן $a^{-1}Ha \subseteq H$ ומכאן $Ha \subseteq aH$ לכל $a \in G$. לכן גם $Ha^{-1} \subseteq a^{-1}H$ ומכאן $aH = a(Ha^{-1})a \subseteq a(a^{-1}H)a = Ha$ לכל $a \in G$. לכן $aH = Ha$ לכל $a \in G$. ∎

הגדרה: תהי G חבורה. חבורה חלקית H של G נקראת **חבורה חלקית נורמלית** אם לכל $a \in G$ מתקים $Ha = aH$. אנו מסמנים זאת ע"י $H \triangleleft G$.

דֻגמה: ראינו בדֻגמאות קודמות שעבור $S_3 = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ מתקים כי $\{1, \sigma, \sigma^2\} \triangleleft S_3$ אבל $\{1, \tau\} \ntriangleleft S_3$.

הערה: יחס הנורמליות אינו יחס טרנסיטיבי, כלומר יתכן $K \triangleleft H \triangleleft G$ אך $K \ntriangleleft G$.

זכרו שאם $\emptyset \neq X, Y \subseteq G$, אז מכפלתן מוגדרת ע"י $XY = \{xy \mid x \in X,\, y \in Y\}$.

טענה: *אם $H \triangleleft G$, אז $\{Hx \mid x \in G\}$ היא חבורה ביחס לכפל של קבוצות חלקיות לא ריקות ב G.*

הוכחה: הכפל ב $\{Hx \mid x \in G\}$ הוא אסוציאטיבי כי הכפל של קבוצות אסוציאטיבי: $X(YZ) = (XY)Z$ (כיון ש $(xy)z = x(yz)$ לכל $x \in X$, $y \in Y$, $z \in Z$).

אם H היא חבורה חלקית, אז $HH = H$ כי $HH = \{xy \mid x \in H,\, y \in H\}$ ולכן $HH \subseteq H$ ומצד שני $h = 1 \cdot h$ לכל $h \in H$ ולכן $H \subseteq HH$.

מכאן, אם H היא חבורה חלקית נורמלית של G, אז לכל $x, y \in G$ מתקים מאסוציאטיביות ב G ש $(Hx)(Hy) = H(xH)y = HHxy = H(xy)$ ולכן יש סגירות תחת הכפל.

H הוא אבר ניטרלי כי $H(Hx) = HHx = Hx$ ו $(Hx)H = HxH = HHx = Hx$ (מנורמליות) לכל $x \in G$.

ההפכי של Hx, עבור $x \in G$, הוא Hx^{-1} כי $(Hx)(Hx^{-1}) = Hxx^{-1} = H \cdot 1 = H$ וגם $(Hx^{-1})(Hx) = H$. ∎

הגדרה: אם $H \triangleleft G$, החבורה $\{Hx \mid x \in G\}$ נקראת **חבורת המנה** של G ביחס ל H ומסומנת ב G/H.

ראינו שהכפל ב $G/H = \{Hx \mid x \in G\}$ נתון ע"י $(Hx)(Hy) = Hxy$ לכל $x, y \in G$, H אבר ניטרלי ו $(Hx)^{-1} = Hx^{-1}$ עבור $x \in G$.

אם G קומוטטיבית, כל חבורה חלקית H היא נורמלית. במקרה זה נסמן את הפעולה ב $+$ ואת המחלקה של $x \in G$ ב $H + x = \{h + x \mid h \in H\}$. אזי $G/H = \{H + x \mid x \in G\}$.

דֻגמה: אם $G = \mathbb{Z}$ ו $H = m\mathbb{Z}$, אז $G/H = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$.

הגדרה: תהי $H \lhd G$. **קבוצת מייצגים** עבור G/H היא קבוצה חלקית X של G כך שלכל מחלקה Ha קים $a' \in X$ אחד ורק אחד כך ש $a' \in Ha$. שימו־לב ש X אינה חבורה אך נתן להגדיר עליה **כפל מודולו** H ע"י $a'b' = (ab)'$ כי $(Ha)(Hb) = Hab$.

דֻגמה: קבוצת מיצגים עבור $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ היא $\{0, 1, 2, \ldots, m-1\}$. מוגדר עליה חבור מודולו m.

הערה: אם G סופית ו $H \lhd G$, אז $|G/H| = [G:H] = \frac{|G|}{|H|}$.

טענה: *$H \lhd G$ אם"ם $aha^{-1} \in H$ לכל $h \in H$ ולכל $a \in G$.*

הוכחה: אם $H \lhd G$, אז $aH = Ha$ לכל $a \in G$ ולכן $aHa^{-1} = H$ לכל $a \in G$. מכאן $aha^{-1} \in H$ לכל $h \in H$ ו $a \in G$.

להיפך, נניח $aha^{-1} \in H$ לכל $h \in H$ ו $a \in G$. אזי $aHa^{-1} \subseteq H$ לכל $a \in G$. מכאן $H = a^{-1}(aHa^{-1})a \subseteq a^{-1}Ha$ ולכן $aH \subseteq Ha$ לכל $a \in G$. מכאן גם $H \subseteq aHa^{-1}$ ולכן $Ha \subseteq aH$ לכל $a \in G$. צרוף שתי ההכלות נותן $aH = Ha$ לכל $a \in G$, כלומר $H \lhd G$. ∎

דֻגמה: תהי $G = \mathrm{GL}(n, F)$ חבורת כל המטריצות $n \times n$ ההפיכות מעל שדה F ונסמן ב H את תת־החבורה $\mathrm{SGL}(n, F)$ המכילה את כל המטריצות בעלות דטרמיננטה 1, כלומר $H = \{A \in G \mid |A| = 1\}$. אזי $H \lhd G$.

אכן, יהיו $A \in H, B \in G$. כיון ש $|A| = 1$, $|BAB^{-1}| = |B||A||B|^{-1} = |B||B|^{-1} = 1$ ולכן $BAB^{-1} \in H$.

משפט: *אם G חבורה קומוטטיבית סופית ו p מספר ראשוני המקים $p||G|$, אזי קים אבר ב G מסדר p.*

הוכחה: נוכיח את המשפט באינדוקציה על $|G|$, כלומר הנחת האינדוקציה היא: *טענת המשפט נכונה עבור כל חבורה מסדר $< n$*. קיום אבר מסדר p מחיב $p||G|$. לכן אם $p \nmid n$, הטענה נכונה באפן ריק. נניח אם־כן $p|n$.

אם $n = 1$, הטענה נכונה באפן ריק. נניח אזי $n > 1$. נקח $1 \neq a \in G$ ונתבונן בחבורה $H = \langle a \rangle$. אם $p||H|$, ודאי H מכילה אבר מסדר p (כי H ציקלית) ואותו אבר הוא ב G ומסדר p. אם $p \nmid |H|$, נתבונן בחבורה G/H (G קומוטטיבית ולכן $H \lhd G$). כיון ש $|H| > 1$, $|G/H| = \frac{|G|}{|H|} < n$. בנוסף, כיון ש $p||G|$ ו $p \nmid |H|$, נובע ש $p||G/H|$.

מהנחת האינדוקציה נובע שקים אבר Hb מסדר p בחבורת המנה G/H, כלומר $Hb \neq H$ ו $Hb^p = (Hb)^p = H$. מכאן $b \notin H$ ו $b^p \in H$. נסמן $r = |H|$. אזי $p \nmid r$. כיון ש $b^p \in H$, $(b^p)^r = (b^p)^{|H|} = 1$. לכן $(b^r)^p = (b^p)^r = 1$. מכאן, אם $b^r \neq 1$, אז b^r הוא אבר מסדר p (כי p מספר ראשוני) וסימנו.

נראה שאכן $b^r \neq 1$. נניח בשלילה ש $b^r = 1$. אזי $(Hb)^r = Hb^r = H$. אולם מצד שני Hb הוא אבר מסדר p ב G/H ולכן $p|r$, סתירה. ∎

טענה: *תהי G חבורה ותהי H חבורה חלקית נורמלית.*

(א) אם $H < K < G$, אזי $K \triangleleft H$ וכן $K/H < G/H$.

(ב) אם $L < G/H$, אזי קימת חבורה חלקית K, $H < K < G$, כך ש $L = K/H$.

הוכחה: (א) $G \triangleleft H$, כלומר $aH = Ha$ לכל $a \in G$. בפרט $aH = Ha$ לכל $a \in K$ ולכן $K \triangleleft H$.

בודאי $K/H \subseteq G/H$. נראה ש $K/H = \{Ha \mid a \in K\}$ היא חבורה חלקית:

אבר היחידה H של G/H הוא ב K/H כי $1 \in K$ ולכן $H = H \cdot 1 \in K/H$.

סגירות תחת כפל: יהיו $Ha, Hb \in K/H$. אזי $a, b \in K$. כיון ש K חבורה, $ab \in K$ ולכן $(Ha)(Hb) = Hab \in K/H$.

סגירות תחת הפכי: יהי $Ha \in K/H$. אזי $a \in K$. כיון ש K חבורה, $a^{-1} \in K$ ולכן $(Ha)^{-1} = Ha^{-1} \in K/H$.

(ב) נגדיר $K = \{a \in G \mid Ha \in L\}$.

כיון ש $L < G/H$, $H \in L$ (H הוא אבר היחידה ב G/H). לכן, אם $a \in H$, אז $Ha = H \in L$ ואם־כן $a \in K$. מכאן $H \subseteq K$.

נוכיח $K < G$: $1 \in K$ כי אפילו $H \subseteq K$.

סגירות תחת כפל: יהיו $a, b \in K$. אזי $Ha, Hb \in L$. כיון ש L היא חבורה חלקית של G/H, $Hab = (Ha)(Hb) \in L$ ולכן $ab \in K$.

סגירות תחת הפכי: יהי $a \in K$. אזי $Ha \in L$. כיון ש L היא חבורה חלקית של G/H, $Ha^{-1} = (Ha)^{-1} \in L$ ולכן $a^{-1} \in K$.

לבסוף, $L = K/H$ כי $Ha \in L \Leftrightarrow a \in K$. ∎

משפט: *תהי G חבורה קומוטטיבית סופית. אם $m \mid |G|$, אזי קימת ל G חבורה חלקית מסדר m.*

הוכחה: נוכיח את הטענה באינדוקציה על $|G|$.

אם $m = 1$, אז $\{1\}$ היא חבורה חלקית של G מסדר 1. נניח $m > 1$ ויהי p מספר ראשוני כך ש $p \mid m$ ולכן $p \mid |G|$. ממשפט קודם נובע שקימת ל G חבורה חלקית H מסדר p. נתבונן בחבורת המנה G/H (G קומוטטיבית ולכן $G \triangleleft H$). G/H היא חבורה קומוטטיבית מסדר

$$|G/H| = \frac{|G|}{|H|} = \frac{|G|}{p} < |G|$$

ולכן, על סמך האינדוקציה, קימת חבורה חלקית ב G/H מכל סדר המחלק את $|G/H|$. כיון ש $m \mid |G|$, $\frac{m}{p} \mid \frac{|G|}{p} = \frac{|G|}{|H|}$ ולכן קימת חבורה חלקית $L < G/H$ עם $|L| = \frac{m}{p}$.

על סמך הטענה הקודמת, $L = K/H$, באשר $G > K$. לכן, כיון ש $\frac{m}{p} = |L| = \frac{|K|}{|H|} = \frac{|K|}{p}$, נובע כי $|K| = m$. ∎

הגדרה: חבורה G שאין לה חבורות חלקיות נורמליות פרט ל G ול $\{1\}$ נקראת **חבורה פשוטה**.

הערה: אם G היא חבורה מסדר ראשוני, אז $G \lhd G$, $\{1\} \lhd G$ הן כל החבורות החלקיות הנורמליות ולכן G חבורה פשוטה.

חבורה פשוטה לא מסדר ראשוני צריכה להיות, על פי המשפט הקודם, לא קומוטטיבית.

דֻגמאות לחבורות חלקיות נורמליות

טענה: *תהי G חבורה ותהי H חבורה חלקית כך ש $[G:H] = 2$. אזי $H \lhd G$.*

הוכחה: יהי $x \in G$. אם $x \in H$, אז $xH = H = Hx$. אם $x \notin H$, אז $Hx \neq H$ ו $xH \neq H$. כיון ש $[G:H] = 2$, מספר המחלקות הימניות = מספר המחלקות השמאליות = 2. לכן

$$H \dot{\bigcup} Hx = G = H \dot{\bigcup} xH.$$

מכאן $Hx = G \setminus H = xH$.

קבלנו ש $Hx = xH$ לכל $x \in G$, כלומר $H \lhd G$. ∎

דֻגמה: חבורת דיהדר. עבור מספר טבעי n, הקבוצה D_n של סבובים ושיקופים המעתיקות מצולע משוכלל בן n צלעות על עצמו היא חבורה הנקראת **חבורת דיהדר** (**dihedral group**). אברי החבורה נקראים **סימטריות** של המצולע. אם a הוא סבוב ב $\frac{360^\circ}{n}$ ו b הוא שקוף סביב ציר סימטריה כלשהוא של המצולע, אז

$$D_n = \{1, a, a^2, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1}\},$$

באשר $a^n = 1$, $b^2 = 1$ ו $ab = ba^{n-1}$. לכן D_n מכילה $2n$ אברים: $1, a, a^2, \ldots, a^{n-1}$ הם סבובים (a^i הוא סבוב ב $\frac{360^\circ i}{n}$) ו $b, ba, ba^2, \ldots, ba^{n-1}$ הם שקופים.

שימו־לב כי $H = \{1, a, \ldots, a^{n-1}\} \lhd D_n$ כי $[D_n : H] = 2$.

$n = 3$: $D_3 = \{1, a, a^2, b, ba, ba^2\}$ עם $a^3 = 1$, $b^2 = 1$ ו $ab = ba^2$. לכן, בסמונים של הדֻגמאות הקודמות, $D_3 \cong S_3$ ע"י $a \leftrightarrow \sigma$ ו $b \leftrightarrow \tau$.

D_3 היא חבורת הסימטריות על משולש שוה צלעות: a הוא סבוב ב 120°, a^2 הוא סבוב ב 240° ו b, ba, ba^2 הם שקופים סביב שלשת צירי הסימטריה של המשולש.

$n = 4$: D_4 היא חבורת הסימטריות של סיבובים ושיקופים על רבוע. אם a הוא סבוב ב 90°, אז a^2 הוא סבוב ב 180°, a^3 הוא סבוב ב 270° ו $a^4 = 1$ הוא סבוב ב 360°, כלומר העתקת הזהות. אם b הוא שקוף סביב

אחד האלכסונים של הרבוע, אז ba^2 הוא שקוף סביב האלכסון השני ו ba ו $ab = ba^3$ הם שקופים סביב שני צירי הסימטריה הנוספים של הרבוע. לכן

$$D_4 = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\},$$

באשר a, b מקימים $a^4 = 1$, $b^2 = 1$ ו $ab = ba^3$.

$D_4 \triangleright \{1, a, a^2, a^3\}$ כי $[D_4 : \{1, a, a^2, a^3\}] = 2$.

משפטי האיזומורפיזמים

טענה: *אם* $\varphi\colon G_1 \to G_2$ *הומומורפיזם של חבורות, אזי* $\ker\varphi \triangleleft G_1$.

הוכחה: ראינו כבר כי $\ker\varphi < G_1$. נראה נורמליות: יהיו $a \in \ker\varphi$ ו $b \in G_1$. אזי, כיון ש $\varphi(a) = 1$,

$$\varphi(bab^{-1}) = \varphi(b)\varphi(a)\varphi(b^{-1}) = \varphi(b)\varphi(b)^{-1} = 1.$$

לכן $bab^{-1} \in \ker\varphi$. מכאן $\ker\varphi \triangleleft G_1$. ∎

טענה: *תהי* H *חבורה חלקית נורמלית של חבורה* G.

נגדיר העתקה $\nu\colon G \to G/H$

ע"י $\nu(a) = Ha$.

אזי ν *הומומורפיזם ו* $\ker\nu = H$. ν *נקרא* **ההומומורפיזם הטבעי** *(או* **ההומומורפיזם הקנוני***)*.

הוכחה: ν הומומורפיזם: $\nu(ab) = Hab = (Ha)(Hb) = \nu(a)\nu(b)$.

כמו־כן $\ker\nu = \{a \in G \mid \nu(a) = H\} = \{a \in G \mid Ha = H\} = H$. ∎

משפט האיזומורפיזם ה I: *אם* $\varphi\colon G_1 \to G_2$ *אפימורפיזם, אז קים איזומורפיזם* $\psi\colon G_1/\ker\varphi \overset{\cong}{\to} G_2$ *כך ש* $\varphi = \psi \circ \nu$*, באשר* $\nu\colon G_1 \to G_1/ker\varphi$ *הוא ההומומורפיזם הטבעי.*

הוכחה: נסמן $H = \ker\varphi$.

נגדיר העתקה $\psi\colon G_1/H \to G_2$

ע"י $\psi(Ha) = \varphi(a)$.

ψ חד־ערכית וחד־חד ערכית:

$$\psi(Ha) = \psi(Hb) \Leftrightarrow \varphi(a) = \varphi(b) \Leftrightarrow \varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) = 1.$$

$$\Leftrightarrow ab^{-1} \in H = \ker\varphi \Leftrightarrow Ha = Hb$$

ψ על: יהי $c \in G_2$. כיון ש φ היא על, קים $a \in G_1$ כך ש $c = \varphi(a)$. אבל $\psi(Ha) = \varphi(a)$ ואם־כן $\psi(Ha) = c$.

ψ הומומורפיזם: $\psi((Ha)(Hb))=\psi(Hab)=\varphi(ab)=\varphi(a)\varphi(b)=\psi(Ha)\psi(Hb)$.

מכאן $\psi\colon G_1/H\to G_2$ הוא איזומורפיזם המקים $\varphi=\psi\circ\nu$. ∎

הערה: אם לא דורשים במשפט ההומומורפיזם ש φ על, מקבלים $G_1/\ker\varphi\cong\varphi(G_1)$.

משפט האיזומורפיזם ה II: *תהי G חבורה ויהיו $H\lhd G$ ו $K<G$. אזי* $KH<G$ ו

$$KH/H\cong K/K\cap H.$$

הוכחה: נתבונן בהומומורפיזם הטבעי $\nu\colon G\to G/H$. אזי $\nu(K)<G/H$ ולכן

$$K'=\{c\in G\mid cH\in\nu(K)\}<G$$

(כפי שהוכחנו את הטענה על חבורה חלקית לחבורת מנה). כיון ש $\nu(K)=\{aH\mid a\in K\}$, נובע ש $c\in K'$ $\Leftrightarrow cH\subseteq KH\Leftrightarrow c\in KH$. מכאן $KH=K'<G$ (ראו גם שאלה 31 (ד)) ועל פי הטענה על חבורה חלקית לחבורת מנה,

$$\nu(K)=K'/H=KH/H.$$

יהי $\nu_K\colon K\to KH/H$ הצמצום של ν ל K. אזי ν_K הוא אפימורפיזם ולכן ממשפט האיזומורפיזם ה I נובע ש $K/\ker(\nu_K)\cong KH/H$. עתה

$$\ker(\nu_K)=\{a\in K\mid aH=H\}=\{a\in K\mid a\in H\}=K\cap H\,.$$

לכן $K/K\cap H\cong KH/H$. ∎

אם $f\colon A\to B$ העתקה בין קבוצות ו $C\subseteq B$, אז מגדירים $f^{-1}(C)=\{a\in A\mid f(a)\in C\}$.

טענה: *יהי $\varphi\colon G_1\to G_2$ הומומורפיזם בין חבורות.*

(א) $H_1<G_1\Leftarrow\varphi(H_1)<G_2$.

(ב) $H_2<G_2\Leftarrow\ker\varphi<\varphi^{-1}(H_2)<G_1$.

הוכחה: (א) $\varphi(H_1)$ היא חבורה חלקית של G_2:

$1\in H_1\Leftarrow 1=\varphi(1)\in\varphi(H_1)$.

$\bar a=\varphi(a)\in\varphi(H_1)$, $a\in H_1\Leftarrow a^{-1}\in H_1\Leftarrow\bar a^{-1}=\varphi(a)^{-1}=\varphi(a^{-1})\in\varphi(H_1)$.

$\bar b=\varphi(b)$, $\bar a=\varphi(a)$, $a,b\in H_1\Leftarrow ab\in H_1\Leftarrow\bar a\bar b=\varphi(a)\varphi(b)=\varphi(ab)\in\varphi(H_1)$.

(ב) $\ker\varphi=\{a\in G_1\mid\varphi(a)=1\}=\varphi^{-1}(\{1\})$.

$1\in H_2$, לכן $\ker\varphi<\varphi^{-1}(H_2)=\{a\in G_1\mid\varphi(a)\in H_2\}$.

$\varphi^{-1}(H_2)$ היא חבורה חלקית של G_1:

$1 \in \varphi^{-1}(H_2)$ כי $\varphi(1) = 1 \in H_2$.

$a \in \varphi^{-1}(H_2) \Leftarrow \varphi(a) \in H_2 \Leftarrow \varphi(a^{-1}) = \varphi(a)^{-1} \in H_2 \Leftarrow a^{-1} \in \varphi^{-1}(H_2)$.

$a, b \in \varphi^{-1}(H_2) \Leftarrow \varphi(a), \varphi(b) \in H_2 \Leftarrow \varphi(ab) = \varphi(a)\varphi(b) \in H_2 \Leftarrow ab \in \varphi^{-1}(H_2)$. ∎

משפט: *יהי* $\varphi\colon G_1 \to G_2$ *אפימורפיזם בין חבורות.*

(א) *ההתאמה בין הקבוצות* $\{H_1 \mid \ker\varphi < H_1 < G_1\} \to \{H_2 \mid H_2 < G_2\}$

הנתנת ע"י $H_1 \mapsto \varphi(H_1)$

היא חח"ע ועל. ההתאמה ההפוכה נתנת ע"י $H_2 \to \varphi^{-1}(H_2)$.

(ב) *בהתאמה הקודמת, חבורות חלקיות נורמליות עוברות לחבורות חלקיות נורמליות ולהיפך:*

$$H_1 \lhd G_1 \Leftrightarrow \varphi(H_1) \lhd G_2.$$

(ג) *אם קורה (ב), אז* $G_1/H_1 \cong G_2/\varphi(H_1)$ *(או, לחלופין,* $G_1/\varphi^{-1}(H_2) \cong G_2/H_2$*).*

הוכחה: **(א) ההתאמה היא חח"ע: יהיו** $\ker\varphi < H_1, K_1 < G_1$ **כך ש** $H_1 \neq K_1$. **יש להראות כי** $\varphi(H_1) \neq \varphi(K_1)$.

אכן, $H_1 \neq K_1$. **נניח למשל שקים** $a \in H_1 \setminus K_1$. **נניח בשלילה ש** $\varphi(a) \in \varphi(K_1)$. **אזי** $\varphi(a) = \varphi(b)$ **עבור** $b \in K_1$. **לכן** $\varphi(ab^{-1}) = 1$ **ומכאן** $ab^{-1} \in \ker\varphi < K_1$. **לכן** $a \in K_1 b = K_1$, **בסתירה לכך ש** $a \notin K_1$.

ההתאמה היא על: נקח $H_2 < G_2$. **בעזרת הטענה הקודמת** $\ker\varphi < \varphi^{-1}(H_2) < G_1$. **כמו־כן מתקים** $\varphi(\varphi^{-1}(H_2)) = H_2$. **(באפן כללי, אם** $f\colon A \to B$ **היא העתקה על בין קבוצות ו** $C \subseteq B$ **היא קבוצה חלקית, אז** $f(f^{-1}(C)) = C$**).**

(ב) נראה גרירה בשני הכוונים.

$\varphi(H_1) \lhd G_2 \Leftarrow H_1 \lhd G_1$: **נניח** $H_1 \lhd G_1$. **אזי** $aH_1 = H_1 a$ **לכל** $a \in G_1$. **לכן** $\varphi(aH_1) = \varphi(H_1 a)$ **ולכן** $\varphi(a)\varphi(H_1) = \varphi(H_1)\varphi(a)$ **לכל** $a \in G_1$. **כאשר** a **עובר על אברי** G_1, $\varphi(a)$ **עובר על אברי** G_2 **כי** φ **על. מכאן** $\varphi(H_1) \lhd G_2$.

$\varphi^{-1}(H_2) \lhd G_1 \Leftarrow H_2 \lhd G_2$: **נניח** $H_2 \lhd G_2$. **יהיו** $a \in G_1$ **ו** $b \in \varphi^{-1}(H_2)$. **אזי** $\varphi(b) \in H_2$. **לכן, כיון ש** $H_2 \lhd G_2$, $\varphi(a)\varphi(b)\varphi(a)^{-1} \in H_2$. **מכאן** $\varphi(aba^{-1}) \in H_2$ **ולכן** $aba^{-1} \in \varphi^{-1}(H_2)$ **לכל** $a \in G_1$ **ו** $b \in \varphi^{-1}(H_2)$. **לכן** $\varphi^{-1}(H_2) \lhd G_1$.

(ג) נתבונן בהרכבה $G_1 \xrightarrow{\varphi} G_2 \xrightarrow{\nu} G_2/\varphi(H_1)$, **באשר** $\nu\colon G_2 \to G_2/\varphi(H_1)$ **הוא ההומומורפיזם הטבעי. כיון ש** ν, φ **הם על, ההרכבה** $\nu\varphi\colon G_1 \to G_2/\varphi(H_1)$ **היא אפימורפיזם. לכן, בעזרת משפט האיזומורפיזם**

ה I, $G_1/\ker(\nu\varphi) \cong G_2/\varphi(H_1)$. נראה כי $\ker(\nu\varphi) = H_1$:

$$\ker(\nu\varphi) = \{a \in G_1 \mid \nu\varphi(a) = 1_{G_2/\varphi(H_1)} = \varphi(H_1)\}.$$

לכן

$$a \in \ker(\nu\varphi) \Leftrightarrow \varphi(H_1)\varphi(a) = \nu(\varphi(a)) = \varphi(H_1) \Leftrightarrow \varphi(a) \in \varphi(H_1).$$
$$\Leftrightarrow a \in \varphi^{-1}(\varphi(H_1)) = H_1$$

מכאן $\ker(\nu\varphi) = H_1$ ולכן $G_1/H_1 \cong G_2/\varphi(H_1)$. ∎

משפט האיזומורפיזם ה III: אם $G \triangleleft G$ ו $H \triangleleft G$, $H < K \triangleleft G$, אז $G/K \cong (G/H)/(K/H)$.

הוכחה: נפעיל את חלק (ג) של המשפט עבור ההומומורפיזם הטבעי $\nu\colon G \to G/H$ (שימו־לב ש $\ker \nu = H < K$). עתה $\nu(K) = \{Ha \mid a \in K\} = K/H$ כיון ש $H < K$. לכן

$$G/K \cong (G/H)/\nu(K) = (G/H)/(K/H).$$ ∎

תרגילים לסעיף 5

31. (א) תהי G חבורה. אם $X, Y \subseteq G$ לא ריקות, אזי $(XY)^{-1} = Y^{-1}X^{-1}$.

(ב) אם $H < G$, אז $H = H^{-1} = HH = HH^{-1}$.

(ג) אם $H \subseteq G$ קבוצה חלקית לא ריקה וכן $HH^{-1} \subseteq H$, אזי $H < G$.

(ד) אם $H, K < G$, אזי $HK < G$ אם"ם $HK = KH$. בפרט, אם $H \triangleleft G$, אז $HK < G$.

(ה) מצא/י ב S_3 חבורות חלקיות H, K כך ש HK אינה חבורה חלקית.

32. יהיו $K < H < G$ חבורות. הוכח/י ש $[G : K]$ סופי אם"ם $[G : H]$ ו $[H : K]$ סופיים ובמקרה כזה

$[G : K] = [G : H][H : K]$.

33. יהיו H, K שתי חבורות חלקיות של חבורה G.

(א) הראה/י כי $(H \cap K)x = Hx \cap Kx$ ונצל/י זאת על מנת להוכיח כי

$[G : H \cap K] \leq [G : H][G : K]$.

(ב) אם $[G : K], [G : H]$ סופיים וזרים, אז $[G : H \cap K] = [G : H][G : K]$.

34. אם S אגודה כפלית, נגדיר את **המֶרְכָּז** של S על ידי

$Z(S) = \{a \in S \mid$ לכל $x \in S$ $ax = xa\}$.

(א) אם $Z(S) \neq \emptyset$, אז $Z(S)$ אגודה חלקית. אם S מונואיד, אז $Z(S)$ מונואיד חלקי.

(ב) אם S חבורה, אז $Z(S)$ חבורה חלקית נורמלית ב S.

35. (א) אם $H < G$, אזי לכל $a \in G$ מתקיים $aHa^{-1} < G$.

(ב) אם $H < G$ ו $|H| = k$ סופי ואין ל G חבורה חלקית נוספת מסדר k, אזי $H \triangleleft G$.

(ג) אם $K < H \triangleleft G$ וכן H ציקלית סופית, אז $K \triangleleft G$.

36. בחבורה $D_4 = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$, באשר $a^4 = 1$, $b^2 = 1$, $ab = ba^3$, מצא/י חבורה חלקית H ובה חבורה חלקית K כך ש $K \triangleleft H \triangleleft D_4$ ואילו $K \ntriangleleft D_4$.

37. G חבורה, $H < G$ ונגדיר $N(H) = \{a \in G \mid aH = Ha\}$. הוכח/י

(א) $N(H) < G$ וכן $N(H) = G$ אם ורק אם $H \triangleleft G$.

(ב) $H \triangleleft N(H)$ וכן אם $H \triangleleft K < G$, אזי $K < N(H)$.

38. (א) אם $K \triangleleft G$ ו $a \in G$ מסדר סופי, אזי הסדר של Ka ב G/K מחלק את הסדר של a ב G.

(ב) יהיו G חבורה סופית, $K \triangleleft G$ ו $[G : K] = s$. אם $(r, s) = 1$ ו $a^r \in K$, אז $a \in K$.

39. יהיו $K \triangleleft G$. אם ל G/K יש חבורת מנה שהיא ציקלית אינסופית, אזי לכל n טבעי, G מכילה חבורה חלקית נורמלית מאינדקס n. (רמז: הוכח/י שיש ל G תמונה הומומורפית מסדר n.)

31. (א) $(XY)^{-1}=\{(xy)^{-1}\mid x\in X,\,y\in Y\}=\{y^{-1}x^{-1}\mid x\in X,\,y\in Y\}=Y^{-1}X^{-1}$.

(ב) נניח $H<G$.

$H=H^{-1}$: אם $h^{-1}\in H^{-1}$, באשר $h\in H$, אז $h^{-1}\in H$ ולכן $H^{-1}\subseteq H$. מצד שני, אם $h\in H$, אז $h=(h^{-1})^{-1}\in H^{-1}$ ולכן $H\subseteq H^{-1}$.

$H=HH$: אם $h_1h_2\in HH$, באשר $h_1,h_2\in H$, אז $h_1h_2\in H$. להיפך, אם $h\in H$, אז $h=h\cdot 1\in HH$.

לבסוף, $HH^{-1}=HH=H$ כי $H^{-1}=H$.

(ג) נניח $\emptyset\neq H\subseteq G$ ו $HH^{-1}\subseteq H$. אזי קיים $h\in H$ ולכן $1_G=h\cdot h^{-1}\in HH^{-1}\subseteq H$. כדי להוכיח $H<G$ יש להראות סגירות תחת הפכי וסגירות תחת כפל.

סגירות תחת הפכי: יהי $h\in H$. אזי $h^{-1}=1\cdot h^{-1}\in HH^{-1}\subseteq H$.

סגירות תחת מכפלה: יהיו $h_1,h_2\in H$. כיון ש $h_2^{-1}\in H$, $h_1h_2=h_1\cdot(h_2^{-1})^{-1}\in HH^{-1}\subseteq H$.

(ד) יהיו $H,K<G$. צריך להוכיח $HK<G\Leftrightarrow HK=KH$.

נניח $HK<G$. אזי $HK\overset{(ב)}{=}(HK)^{-1}\overset{(א)}{=}K^{-1}H^{-1}\overset{(ב)}{=}KH$.

להיפך, נניח $HK=KH$. לפי חלק (ג) מספיק להוכיח $(HK)(HK)^{-1}=HK$. אכן
$HK(HK)^{-1}\overset{(א)}{=}HKK^{-1}H^{-1}\overset{(ב)}{=}HKH^{-1}\overset{(ב)}{=}HKH\overset{\text{נתון}}{=}HHK\overset{(ב)}{=}HK$.

אם $H\lhd G$, אז $Ha=aH$ לכל $a\in G$ ובפרט $HK=KH$. לכן $HK<G$.

(ה) תהי $S_3=\{1,\sigma,\sigma^2,\tau,\tau\sigma,\tau\sigma^2\}$ עם $\sigma^3=\tau^2=1$ ו $\sigma\tau=\tau\sigma^2$. כיון ש τ ו $\tau\sigma$ הם אברים מסדר 2, $H=\{1,\tau\}$ ו $K=\{1,\tau\sigma\}$ הן חבורות חלקיות של S_3. אולם $HK=\{1,\tau,\tau\sigma,\sigma\}$ ולכן $|S_3|=6\nmid 4=|HK|$. מכאן, על־פי משפט לגרנג', $HK\not< S_3$.

32. יהיו $K<H<G$ חבורות. אם $[G:K]<\infty$, בודאי $[H:K]<\infty$ כי
$\{aK\mid a\in H\}\subseteq\{aK\mid a\in G\}$.

כמו־כן, $[G:H]\le[G:K]$ כי אם $G=Ka_1\cup\ldots\cup Ka_r$, אז $G=HG=Ha_1\cup\ldots\cup Ha_r$. (אולם יכול להיות $a_ia_j^{-1}\notin K$ אך $a_ia_j^{-1}\in H$.)

נניח עתה ש $[G:H]=r$ ו $[H:K]=s$. צריך להוכיח $[G:K]=rs$. אכן, נרשם $G=\dot\bigcup_{j=1}^{r}Hy_j$ ו $H=\dot\bigcup_{i=1}^{s}Kx_i$ עבור $x_i\in H, y_j\in G$. אזי לכל j ולכל $i_1\neq i_2$, $Kx_{i_1}y_j\cap Kx_{i_2}y_j=\emptyset$. (באפן כללי: אם $S\cap T=\emptyset$, אז $Sy\cap Ty=\emptyset$. אכן, אם $sy=ty$, אז $s=t$.) לכן

$$G=\dot\bigcup_{j=1}^{r}Hy_j=\dot\bigcup_{j=1}^{r}\Big(\dot\bigcup_{i=1}^{s}Kx_iy_j\Big)=\dot\bigcup_{j,i}Kx_iy_j$$

ומכאן $[G:K]=rs$.

33. (א) $(H\cap K)x\subseteq Hx\cap Kx$ כי אם $gx\in(H\cap K)x$, אז $g\in H\cap K$ ולכן $gx\in Hx\cap Kx$.
$(H\cap K)x\supseteq Hx\cap Kx$ כי אם $hx=kx\in Hx\cap Kx$, אז $h=k\in H\cap K$ ולכן $hx=kx\in(H\cap K)x$.
מכאן $(H\cap K)x=Hx\cap Kx$.

עתה, מספר המחלקות Hx הוא $[G:H]$ ומספר המחלקות Kx הוא $[G:K]$. לכן מספר החתוכים $Hx\cap Kx$ הוא לכל היותר $[G:H][G:K]$. אולם, בעזרת החלק הראשון, מספר החתוכים $Hx\cap Kx=(H\cap K)x$ הוא $[G:H\cap K]$ ולכן $[G:H\cap K]\leq[G:H][G:K]$.

דרך נוספת: כדי להראות $[G:H\cap K]\leq[G:H][G:K]$ נוכיח כי ההעתקה

$$\{(H\cap K)x\mid x\in G\}\to\{Hy\mid y\in G\}\times\{Kz\mid z\in G\}$$

המוגדרת ע"י

$$(H\cap K)x\mapsto(Hx,Kx)$$

היא חד־ערכית (מוגדרת היטב) וחח"ע.

אכן, $(Hx,Kx)=(Hy,Ky)$ אם"ם $xy^{-1}\in H\cap K$ אם"ם $(H\cap K)x=(H\cap K)y$.

(ב) נסמן $r=[G:H]$ ו $s=[G:K]$. נתון $(r,s)=1$. יש להוכיח $[G:H\cap K]=rs$. בחלק (א) הוכחנו $[G:H\cap K]\leq rs$. נראה אי־שויון הפוך.

על סמך התרגיל הקודם, המופעל על $H\cap K<H<G$, $[G:H\cap K]=[G:H][H:H\cap K]$. לכן $r|[G:H\cap K]$. באפן דומה, הפעלת התרגיל הקודם על $H\cap K<K<G$ נותנת $s|[G:H\cap K]$. לכן, כיון ש $(r,s)=1$, $rs|[G:H\cap K]$ ומכאן $rs\leq[G:H\cap K]$.

34. (א) תהי S אגודה כפלית ונניח $Z(S)=\{a\in S\mid ax=xa \text{ לכל } x\in S\}\neq\emptyset$. כדי להראות ש $Z(S)$ היא אגודה חלקית של S, יש להראות סגירות תחת הכפל: אם $a,b\in Z(S)$, אז $ax=xa$ ו $bx=xb$ לכל $x\in S$. לכן

$$(ab)x=a(bx)=a(xb)=(ax)b=(xa)b=x(ab)$$

לכל $x\in S$. כלומר $ab\in Z(S)$.

אם S הוא מונואיד עם אבר ניטרלי 1, אז $1\in Z(S)$ כי $1\cdot x=x=x\cdot 1$ לכל $x\in S$. לכן $Z(S)$ הוא מונואיד חלקי של S.

(ב) אם S חבורה, אז $Z(S)$ היא חבורה חלקית. אכן, נשאר רק להראות סגירות תחת הפכי: אם $a\in Z(S)$, אז $ax=xa$ לכל $x\in S$ ולכן $xa^{-1}=a^{-1}x$ לכל $x\in S$. כלומר $a^{-1}\in Z(S)$.

נראה כי $H=Z(S)$ נורמלית ב S: $xa=ax$ לכל $a\in H$, $x\in S$ $\Leftarrow$ $xH=Hx$ לכל $x\in S$ $\Leftarrow$ $H\lhd S$.

35. (א) נתון $H < G$ ו $a \in G$. נוכיח $aHa^{-1} < G$:

קיום אבר יחידה: $1 = a \cdot 1 \cdot a^{-1} \in aHa^{-1}$.

סגירות תחת הפכי: $aha^{-1} \in aHa^{-1} \Leftarrow (aha^{-1})^{-1} = ah^{-1}a^{-1} \in aHa^{-1}$.

סגירות תחת כפל: $ah_1a^{-1}, ah_2a^{-1} \in aHa^{-1} \Leftarrow (ah_1a^{-1})(ah_2a^{-1}) = a(h_1h_2)a^{-1} \in aHa^{-1}$.

(ב) אם $|H| = k$, אז $|aHa^{-1}| = |H| = k$ לכל $a \in G$ כי $h_1 = h_2 \Leftrightarrow ah_1a^{-1} = ah_2a^{-1}$. לכן, אם איו ל G חבורה חלקית נוספת מסדר k, אז $aHa^{-1} = H$ לכל $a \in G$. כלומר $H \lhd G$.

(ג) נניח $K < H \lhd G$ ו H ציקלית סופית. צריך להוכיח ש $K \lhd G$. אנו נראה כי $aKa^{-1} = K$ לכל $a \in G$.

אכן $aKa^{-1} < aHa^{-1} = H$, כיון ש $H \lhd G$. כמו־כן $|aKa^{-1}| = |K|$. מכאן K ו aKa^{-1} הן חבורות חלקיות של החבורה הציקלית הסופית H ושתיהן מאותו סדר. אולם לחבורה ציקלית סופית יש חבורה חלקית יחידה מכל סדר המחלק את סדר החבורה. מכאן $aKa^{-1} = K$.

36. תהי $D_4 = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$, באשר $a^4 = 1$, $b^2 = 1$, $ab = ba^3$.

אזי $H = \{1, ba, a^2, ba^3\}$ ו $K = \{1, ba\}$ הן חבורות חלקיות של D_4 המקימות $K \lhd H \lhd D_4$ כי $[D_4 : H] = 2 = [H : K]$, אולם $K \ntriangleleft D_4$ כי $b(ba)b^{-1} = b^2ab = ab \notin K$.

37. יהיו $H < G$ ונגדיר $N(H) = \{a \in G \mid aH = Ha\}$.

(א) $N(H)$ היא חבורה חלקית של G:

קיום אבר יחידה: $1 \cdot H = H \cdot 1 \Leftarrow 1 \in N(H)$.

סגירות להפכי: $a \in N(H) \Leftarrow aH = Ha \Leftarrow a^{-1}(aH)a^{-1} = a^{-1}(Ha)a^{-1} \Leftarrow Ha^{-1} = a^{-1}H \Leftarrow a^{-1} \in N(H)$.

סגירות תחת כפל: $a, b \in N(H) \Leftarrow aH = Ha$, $bH = Hb \Leftarrow (ab)H = aHb = H(ab) \Leftarrow ab \in N(H)$.

מההגדרה נובע ש $N(H) = G \Leftrightarrow aH = Ha$ לכל $a \in G \Leftrightarrow H \lhd G$.

(ב) $H \subseteq N(H)$ כי אם $a \in H$, אז $aH = H = Ha$ ולכן $a \in N(H)$. כמו־כן $H \lhd N(H)$ כי $aH = Ha$ לכל $a \in N(H)$.

נניח $H \lhd K < G$. אזי $a \in K \Leftarrow aH = Ha \Leftarrow a \in N(H)$. מכאן $K < N(H)$.

38. (א) יהיו $K \lhd G$ ו $a \in G$ מסדר m. יהי r הסדר של Ka ב G/K. אזי, כיון ש $(Ka)^m = Ka^m = K$, נובע מטענה 1 בסעיף 2 ש $r|m$.

(ב) יהיו G חבורה סופית, $K \lhd G$ ו $s = [G : K]$. נניח $(r, s) = 1$ וקים $a \in G$ כך ש $a^r \in K$. אזי $(Ka)^r = Ka^r = K$ ולכן הסדר של Ka מחלק את r. כמו־כן, על פי משפט לגרנג', הסדר של Ka מחלק את

סדר החבורה G/K שהוא $s = [G:K] = |G/K|$. לכן הסדר של Ka מחלק את $1 = (r,s)$ ולכן Ka הוא מסדר 1, כלומר $Ka = K$. מכאן $a \in K$.

39. יהיו $K \lhd G$ ונניח שיש ל G/K חבורת מנה שהיא ציקלית אינסופית. כלומר קימת $L \lhd G/K$ כך ש $(G/K)/L \cong \mathbb{Z}$.

(הערה: על פי טענה על חבורה חלקית לחבורת מנה, $H = \{a \in G \mid Ka \in L\}$ מקימת $K < H < G$ ו $L = H/K$. אזי $H/K \lhd G/K$. בהכרח $H \lhd G$ כי

$$Kghg^{-1} = (Kg)(Kh)(Kg)^{-1} \in H/K$$

ולכן $ghg^{-1} \in H$ לכל $h \in H, g \in G$. בעזרת משפט האיזומורפיזם ה III,

$$(G/K)/L = (G/K)/(H/K) \cong G/H.)$$

יהיו $\nu \colon G \to G/K$, $\mu \colon G/K \to (G/K)/L$ ו $\varphi \colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ההומומורפיזמים הטבעיים. אזי ההרכבה $\psi \colon G \to \mathbb{Z}/n\mathbb{Z}$ הנתנת ע"י

$$G \xrightarrow{\nu} G/K \xrightarrow{\mu} (G/K)/L \cong \mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/n\mathbb{Z}$$

היא הומומורפיזם על. יהי $M = \ker(\psi)$. אזי, בעזרת משפט האיזומורפיזם ה I, $G/M \cong \mathbb{Z}/n\mathbb{Z}$ ולכן $[G:M] = |G/M| = |\mathbb{Z}/n\mathbb{Z}| = n$. מכאן $M \lhd G$ (בתור גרעין של הומומורפיזם) והיא מאינדקס n.

מכפלה ישרה

הגדרה: יהיו $G_1,\dots,G_k$ חבורות. נגדיר חבורה הנקראת **המכפלה הישרה** של $G_1,\dots,G_k$:

$$G_1\times\cdots\times G_k=\{(a_1,\dots,a_k)\mid a_i\in G_i,\ i=1,\dots,k\}.$$

המכפלה מוגדרת ע"י $(a_1,\dots,a_k)(b_1,\dots,b_k)=(a_1b_1,\dots,a_kb_k)$,

אבר היחידה הוא $(1,\dots,1)$ וההפכי של אבר מוגדר ע"י $(a_1,\dots,a_k)^{-1}=(a_1^{-1},\dots,a_k^{-1})$.

שימו־לב שאם $G_1,\dots,G_k$ חבורות סופיות, אז $|G_1\times\cdots G_k|=|G_1|\cdots|G_k|$.

דוגמה: החבורה מסדר 4 $U(8)\cong\{1,a,b,c\}$ המקימת $a^2=b^2=c^2=1$, $ab=c=ba$, $ac=b=ca$, $bc=a=cb$ איזומורפית למכפלה הישרה של $H_1=\{1,a\}$ ו $H_2=\{1,b\}$:

$$\{1,a,b,c\}\cong H_1\times H_2$$

ע"י $(1,1)\leftrightarrow 1$, $(a,1)\leftrightarrow a$, $(1,b)\leftrightarrow b$ ו $(a,b)\leftrightarrow c$.

דוגמה: לחבורה הציקלית מסדר 4 $U(5)\cong\{1,a,a^2,a^3\}$ המקימת $a^4=1$ אין פרוק למכפלה ישרה של שתי חבורות מסדר 2 כי יש לה רק חבורה חלקית אחת מסדר 2 והיא $\{1,a^2\}$.

הערה: חבורה ציקלית מסדר ראשוני אי אפשר לפרק.

הגדרה: G נקראת **מכפלה ישרה פנימית** של $H_1,\dots,H_k<G$ אם

(א) כל אבר של G נתן לכתיבה בצורה אחת ויחידה בתור: $h_1h_2\cdots h_k$ באשר $h_i\in H_i$.

(ב) אם $i\neq j$, $h_i\in H_i, h_j\in H_j$, אז $h_ih_j=h_jh_i$.

משפט: (1) אם $G=G_1\times\cdots\times G_k$, אזי *$G$ היא מכפלה ישרה פנימית של* $H_1,\dots,H_k<G$ ו $H_i\cong G_i$, $i=1,\dots,k$.

(2) אם *G היא מכפלה ישרה פנימית של* $H_1,\dots,H_k<G$, אז $G\cong H_1\times\cdots\times H_k$.

הוכחה: (1) נקח $H_i=\{(1,\dots,1,\overset{i}{a_i},1,\dots,1)\mid a_i\in G_i\}$. בודאי $H_i\cong G_i$. יש להראות שמתקים (א) ו (ב).

(א) יהי $(a_1,\dots,a_k)\in G$. אזי $(a_1,\dots,a_k)=h_1\cdots h_k$, באשר $h_i=(1,\dots,1,a_i,1,\dots,1)$.

יחידות: אם גם $(a_1,\dots,a_k)=h'_1\cdots h'_k$, באשר $h'_i=(1,\dots,1,a'_i,1,\dots,1)\in H_i$, אז $(a_1,\dots,a_k)=h'_1\cdots h'_k=(a'_1,\dots,a'_k)$. לכן $a'_i=a_i$ ולכן $h'_i=h_i$ לכל i.

(ב) $h_ih_j=(1,\dots,1,\overset{i}{a_i},1,\dots,1,\overset{j}{a_j},1,\dots,1)=h_jh_i$.

(2) נניח $H_1,\dots,H_k<G$ ומתקים (א) ו (ב).

נגדיר העתקה $H_1 \times \cdots \times H_k \to G$

ע"י $(h_1, \dots, h_k) \mapsto h_1 \cdots h_k$.

העתקה זו חח"ע ועל על סמך (א). ההעתקה היא הומומורפיזם כי

$$(h_1, \dots, h_k)(h'_1, \dots, h'_k) = (h_1h'_1, \dots, h_kh'_k) \mapsto h_1h'_1h_2h'_2 \cdots h_kh'_k$$

ובגלל ההתחלפות (ב) עבור $i \neq j$, $h_1h'_1 \cdots h_kh'_k = (h_1 \cdots h_k)(h'_1 \cdots h'_k)$. ∎

הערה: בחבורות קומוטטיביות תנאי (ב) מיותר.

הערה: תנאי (ב) מבטיח ש $H_i \lhd G$ כי $H_ih_j = h_jH_i$ עבור $i \neq j$ ו $H_ih_i = H_i = h_iH_i$ ולכן $H_ih_1 \cdots h_k = h_1 \cdots h_kH_i$.

הגדרה שקולה למכפלה ישרה פנימית: *חבורה G היא מכפלה ישרה פנימית של* $H_1, \dots, H_k < G$ אם

(א') $G = H_1 \cdots H_k$ ו $H_i \cap (\prod_{j \neq i} H_j) = \{1\}$; ו

(ב') $H_i \lhd G$, $i = 1, \dots, k$.

הוכחה: לשם פשטות, נוכיח את הטענה במקרה $k = 2$. יש להראות כי

(א') $G = H_1H_2$, $H_1 \cap H_2 = \{1\}$ ו (ב') $H_i \lhd G$, $i = 1, 2$ שקולים ל

(א) הצגה אחת ויחידה ו (ב) התחלפות.

(א),(ב) $\Leftarrow$ (א'),(ב'): מתוך (א) נובע $G = H_1H_2$ כי $G \subseteq H_1H_2 \subseteq G$.

$H_1 \cap H_2 = \{1\}$: יהי $h \in H_1 \cap H_2$. נתן לרשום את h בשני אפנים: $h = \underset{}{\overset{\in H_1}{h}} \cdot \overset{\in H_2}{1} = \overset{\in H_1}{1} \cdot \overset{\in H_2}{h}$.

לכן, מתוך היחידות שב (א) נובע $h = 1$.

(א),(ב) $\Rightarrow$ (א'),(ב'):

נוכיח (א): $G = H_1H_2$ ולכן קימת הצגה עבור כל אבר.

יחידות: אם $h_1h_2 = h'_1h'_2$, אז $H_1 \ni h'^{-1}_1h_1 = h'_2h_2^{-1} \in H_2$. כיון ש $H_1 \cap H_2 = \{1\}$, $h'^{-1}_1h_1 = h'_2h_2^{-1} = 1$ ולכן $h'_1 = h_1$, $h'_2 = h_2$.

נוכיח (ב): יהיו $h_1 \in H_1$, $h_2 \in H_2$. צריך להוכיח $h_1h_2 = h_2h_1$ או, לחלופין, $h_1h_2h_1^{-1}h_2^{-1} = 1$.

כיון ש $H_1 \lhd G$, $h_2h_1^{-1}h_2^{-1} \in H_1$ ולכן $h_1h_2h_1^{-1}h_2^{-1} = h_1(h_2h_1^{-1}h_2^{-1}) \in H_1$.

כיון ש $H_2 \lhd G$, $h_1h_2h_1^{-1} \in H_2$ ולכן $h_1h_2h_1^{-1}h_2^{-1} = (h_1h_2h_1^{-1})h_2^{-1} \in H_2$.

מכאן $h_1h_2h_1^{-1}h_2^{-1} \in H_1 \cap H_2 = \{1\}$. ∎

הגדרה: עבור חוגים $R_1, \dots, R_k$, אנו מגדירים את מכפלתם הישרה $R_1 \times \cdots \times R_k$ באפן דומה.

הגדרת החבור: $(a_1, \dots, a_k) + (b_1, \dots, b_k) = (a_1 + b_1, \dots, a_k + b_k)$.

הגדרת הכפל: $(a_1,\dots,a_k)(b_1,\dots,b_k)=(a_1b_1,\dots,a_kb_k)$.

טענה: *המכפלה הישרה של חבורות ציקליות מסדרים זרים היא חבורה ציקלית.*

הוכחה: זכרו שאם a,b הם אברים בחבורה המקימים $ab=ba$, $|a|=r$, $|b|=s$ ו $(r,s)=1$, אז ab הוא אבר מסדר rs.

תהי $G=G_1\times\cdots\times G_k$ מכפלה ישרה של חבורות ציקליות. אזי $G=H_1\cdots H_k$ היא מכפלה פנימית ישרה של $H_1,\dots,H_k<G$ עם $H_i\cong G_i$, באשר H_i היא ציקלית מסדר m_i ו $(m_i,m_j)=1$ עבור $i\neq j$. נניח ש a_i יוצר של H_i. אזי a_i מסדר m_i.

כיון ש $a_1a_2=a_2a_1$ ו $(m_1,m_2)=1$, האבר a_1a_2 הוא מסדר m_1m_2.

כיון ש $(a_1a_2)a_3=a_1a_3a_2=a_3(a_1a_2)$ ו $(m_1m_2,m_3)=1$ (כי $(m_1,m_3)=1$ ו $(m_2,m_3)=1$), האבר $a_1a_2a_3$ הוא מסדר $m_1m_2m_3$.

לבסוף מתקבל ש $a=a_1a_2\cdots a_k$ הוא אבר מסדר $m_1m_2\cdots m_k$. לכן $\langle a\rangle$ היא חבורה חלקית של G מסדר $m_1\cdots m_k$. אולם מצד שני $|G|=|G_1|\cdots|G_k|=m_1\cdots m_k$ ולכן $G=\langle a\rangle$ היא חבורה ציקלית.

∎

טענה הפוכה: *תהי G חבורה ציקלית מסדר $n=m_1m_2\cdots m_k$, באשר $(m_i,m_j)=1$ לכל $i\neq j$. אזי G היא מכפלה ישרה של חבורות ציקליות $H_1,\dots,H_k<G$ מסדרים $m_1,\dots,m_k$, בהתאמה.*

הוכחה: כיון ש G ציקלית, קימת לה חבורה חלקית (ציקלית) מכל סדר שמחלק את $n=|G|$. תהי $H_i<G$ חבורה חלקית מסדר m_i. אזי $H_i\cong\mathbb{Z}_{m_i}$. כיון ש $G\cong\mathbb{Z}_n$, מספיק אם־כן להוכיח כי $\mathbb{Z}_n\cong\mathbb{Z}_{m_1}\times\mathbb{Z}_{m_2}\times\cdots\times\mathbb{Z}_{m_k}$.

נגדיר העתקה
$$\varphi\colon \mathbb{Z}\to\mathbb{Z}_{m_1}\times\mathbb{Z}_{m_2}\times\cdots\times\mathbb{Z}m_k$$
ע"י
$$a\mapsto (a \pmod{m_1}, a \pmod{m_2},\dots,a \pmod{m_k}).$$

φ הומומורפיזם כי החבור מודולו m_i אינו תלוי בנציג. לכן ממשפט האיזומורפיזם הראשון נובע ש $\mathbb{Z}/\ker\varphi$ איזומורפית לחבורה חלקית של $\mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_k}$.

עתה, $\ker\varphi=n\mathbb{Z}$. אכן, $nc\in n\mathbb{Z}\Leftarrow nc\,(\bmod\, m_i)=0$ (כי $m_i|n$), $i=1,\dots,k\Leftarrow$ $(0,\dots,0)=(nc\,(\bmod\, m_1),\dots,nc\,(\bmod\, m_k))=\varphi(nc)\Leftarrow nc\in\ker\varphi$. להיפך, $m\in\ker\varphi\Rightarrow\varphi(m)=(m\,(\bmod\, m_1),\dots,m\,(\bmod\, m_k))=(0,\dots,0)\Rightarrow m\,(\bmod\, m_i)=0$, $i=1,\dots,k\Rightarrow n=m_1\cdots m_k|m$ (כי $(m_i,m_j)=1$ עבור $i\neq j$) $\Rightarrow m\in n\mathbb{Z}$.

לכן $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}=\mathbb{Z}/\ker\varphi$ איזומורפית לחבורה חלקית של $\mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_k}$. אולם $\mathbb{Z}_n$ מסדר n וגם $\mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_k}$ מסדר $n=m_1\cdots m_k$. לכן
$$\mathbb{Z}_n\cong\mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_k}.$$
∎

הערה: ההעתקה $\varphi\colon \mathbb{Z}\to\mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_k}$ היא למעשה הומומורפיזם של חוגים ומתקבל שהחוג $\mathbb{Z}_n$ איזומורפי למכפלה הישרה $\mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_k}$.

משפט השאריות הסיני: *יהיו $m_1,\ldots,m_k$ מספרים טבעיים זרים בזוגות ויהיו $b_1,\ldots,b_k\in\mathbb{Z}$. אזי למערכת המשוואות*

$$X\equiv b_1\,(\mathrm{mod}\ m_1)$$

$$X\equiv b_2\,(\mathrm{mod}\ m_2)$$

$$\vdots$$

$$X\equiv b_k\,(\mathrm{mod}\ m_k)$$

קים פתרון ב $\mathbb{Z}$ והוא יחיד מודולו $n=m_1\cdots m_k$.

הוכחה: מהטענה הקודמת נובע כי ההעתקה $\varphi\colon\mathbb{Z}\to\mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_k}$ היא על. אם נסתכל על b_i כאבר ב $\mathbb{Z}_{m_i}$, אז $(b_1,\ldots,b_k)\in\mathbb{Z}_{m_1}\times\cdots\times\mathbb{Z}_{m_k}$ ולכן קים $a\in\mathbb{Z}$, יחיד מודולו n, כך ש $\varphi(a)=(b_1,\ldots,b_k)$, כלומר $a\equiv b_1\,(\mathrm{mod}\ m_1),\ldots,a\equiv b_k\,(\mathrm{mod}\ m_k)$. ∎

תהי G חבורה קומוטטיבית מסדר $n=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$, באשר $p_1,\cdots,p_k$ מספרים ראשוניים שונים ו $r_1,\ldots,r_k$ שלמים חיוביים. אנו נראה בסעיף 8 שקימת ל G חבורה חלקית P_i *יחידה* מסדר $p_i^{r_i}$ (כיון ש G קומוטטיבית, $P_i\lhd G$) הנקראת **חבורת ה p_i סילוב** של G, $i=1,\ldots,k$.

משפט: *אם G קומוטטיבית סופית, אזי G היא המכפלה הישרה של חבורות הסילוב שלה.*

הוכחה: נניח $|G|=p_1^{r_1}\cdots p_k^{r_k}$ ותהי P_i חבורת ה p_i־סילוב של G, $i=1,\ldots,k$. יש להראות כי $G=P_1P_2\cdots P_k$ ו $P_i\cap(\prod_{j\neq i}P_j)=\{1\}$.

נוכיח $G=P_1\cdots P_k$: ממשפט האיזומורפיזם השני $P_1P_2/P_1\cong P_2/P_1\cap P_2$ ו $P_1\cap P_2=\{1\}$ כי P_1,P_2 הן חבורות חלקיות מסדרים זרים. לכן $|P_2|=|P_2/P_1\cap P_2|=|P_1P_2/P_1|=\frac{|P_1P_2|}{|P_1|}$. מכאן $|P_1P_2|=|P_1||P_2|$. באפן דומה, כיון ש $P_1P_2\cap P_3=\{1\}$, $|P_1P_2P_3|=|P_1||P_2||P_3|$. לבסוף $|P_1\cdots P_k|=|P_1|\cdots|P_k|=p_1^{r_1}\cdots p_k^{r_k}=|G|$. קבלנו $P_1\cdots P_k<G$ בעלות אותו מספר אברים ולכן $P_1\cdots P_k=G$.

נוכיח $P_i\cap(\prod_{j\neq i}P_j)=\{1\}$: שימו־לב תחילה כי $|\prod_{j\neq i}P_j|=\prod_{j\neq i}|P_j|=\prod_{j\neq i}p_j^{r_j}$. יהי $a\in P_i\cap(\prod_{j\neq i}P_j)$. אזי הסדר של a מחלק את הסדר של P_i ואת הסדר של $\prod_{j\neq i}P_j$ ולכן את $(p_i^{r_i},\prod_{j\neq i}p_j^{r_j})=1$. מכאן $a=1$. ∎

מסקנה: *תהי G חבורה קומוטטיבית ויהי $G = P_1 \cdots P_k$ הפרוק שלה למכפלה ישרה של חבורות הסילוב שלה. אם כל P_i ציקלית, אז G ציקלית.*

הערה: תהי G חבורה קומוטטיבית. אזי G היא מכפלה ישרה של $H_1, \ldots, H_k < G$ אם"ם

(א") $G = H_1 \cdots H_k$ ומתוך $h_1 \cdots h_k = 1$ ($h_i \in H_i$) נובע $h_i = 1$ לכל i.

אכן, אם G היא מכפלה ישרה של $H_1, \ldots, H_k$ ו $h_1 \cdots h_k = 1 = \overset{\in H_1}{1} \cdots \overset{\in H_k}{1}$, אז מיחידות הפרוק נובע ש $h_i = 1$ לכל i. להיפך, נניח מתקיים (א") ו $h_1 \cdots h_k = h_1' \cdots h_k'$ עבור $h_i, h_i' \in H_i$. אזי $1 = (h_1 \cdots h_k)^{-1} h_1' \cdots h_k'$ ומקומוטטיביות G נובע כי $1 = \overset{\in H_1}{(h_1^{-1}h_1')}\ \overset{\in H_2}{(h_2^{-1}h_2')} \cdots \overset{\in H_k}{(h_k^{-1}h_k')}$. לכן $h_i^{-1}h_i' = 1$ ומכאן $h_i = h_i'$ לכל i.

הערה: כאשר הפעולה בחבורה G היא $+$, אז G היא **סכום ישר** של $H_1, \ldots, H_k < G$ אם מתקים $G = H_1 + \ldots + H_k$ ומתוך $h_1 + \ldots + h_k = 0$ ($h_i \in H_i$) נובע $h_i = 0$ לכל i. אנו מסמנים זאת ע"י $G = H_1 \oplus \ldots \oplus H_k$.

טענה: *תהי P חבורה ציקלית מסדר p^r, p ראשוני. אזי P אינה מכפלה ישרה של שתי חבורות $\neq 1$.*

הוכחה: נניח בשלילה ש $P = H_1 H_2$ היא מכפלה ישרה של H_1, H_2 עם $H_1 \neq 1, H_2 \neq 1$. אזי $|H_1| = p^{s_1}$ ו $|H_2| = p^{s_2}$, באשר $r = s_1 + s_2$ (כי $p^r = p^{s_1} p^{s_2}$). נניח למשל $s_2 \leq s_1$. אזי $0 < s_2 \leq s_1 < r$.

יהי $a \in P$ אבר מסדר p^r ונרשום $a = h_1 h_2$, באשר $h_i \in H_i$. אזי, כיון ש $p^{s_2} | p^{s_1}$ (כי $s_2 \leq s_1$), $a^{p^{s_1}} = h_1^{p^{s_1}} (h_2^{p^{s_2}})^{\frac{p^{s_1}}{p^{s_2}}} = 1 \cdot 1 = 1$, סתירה (כי $p^{s_1} < p^r$). ∎

משפט: *תהי P חבורה קומוטטיבית מסדר p^r, p ראשוני. אזי P היא מכפלה ישרה של חבורות ציקליות מסדרים $p^{s_1}, \ldots, p^{s_k}$ והמספרים $k, s_1, \ldots, s_k$ נקבעים באפן יחיד.*

כלומר, אם $P = H_1 \cdots H_k$ היא מכפלה ישרה של $H_1, \ldots, H_k$, באשר H_i ציקלית מסדר p^{s_i}, $i = 1, \ldots, k$, ו $s_1 \geq \ldots \geq s_k$ וגם $P = K_1 \cdots K_l$ היא מכפלה ישרה של $K_1, \ldots, K_l$, באשר K_j ציקלית מסדר p^{t_j}, $j = 1, \ldots, l$, ו $t_1 \geq \ldots \geq t_l$, אז $k = l$ ו $s_i = t_i$, $i = 1, \ldots, k$.

דֻגמה: אם P חבורה קומוטטיבית לא ציקלית מסדר $2^2 = 4$, אז $P = \{1, a, b, c\}$, באשר $ab = c$ ו $a^2 = b^2 = c^2 = 1$. יהיו $H = \{1, a\}$, $K = \{1, b\}$ ו $L = \{1, c\}$. אזי $P = HK = HL = KL$ הם פרוקים של P למכפלה ישרה של שתי חבורות ציקליות מסדרים $2, 2$.

דֻגמה: אם P חבורה קומוטטיבית מסדר $2^3 = 8$, אז יתכנו שלשה מקרים:

(א) P היא ציקלית. במקרה זה $P \cong \mathbb{Z}_8$.

(ב) $P = HK$ היא מכפלה ישרה של שתי חבורות ציקליות H, K מסדרים $4, 2$, בהתאמה. במקרה זה $P \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

(ג) $P = HKL$ היא מכפלה ישרה של שלש חבורות ציקליות H, K, L מסדרים $2, 2, 2$. במקרה זה $P \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

סימון: עבור מספר טבעי r, אנו מסמנים את מספר הסדרות $s_1, \ldots, s_k$ של מספרים טבעיים כך ש $s_1 + \ldots + s_k = r$ ו $s_1 \geq \ldots \geq s_k$ ב $\wp(r)$.

מסקנה: *מספר החבורות הקומוטטיביות הבלתי איזומורפיות מסדר p^r הוא $\wp(r)$.*

הוכחה: תהי P חבורה קומוטטיבית מסדר p^r ויהי $P = H_1 \cdots H_k$ פרוק למכפלה ישרה של חבורות ציקליות $H_1, \ldots, H_k$ מסדרים $p^{s_1}, \ldots, p^{s_k}$, בהתאמה. כיון ש $p^r = p^{s_1} \cdots p^{s_k}$, $r = s_1 + \ldots + s_k$. נניח $s_1 \geq \ldots \geq s_k$.

תהי P' חבורה קומוטטיבית נוספת מסדר p^r ויהי $P' = K_1' \cdots K_l'$ פרוק למכפלה ישרה של חבורות ציקליות $K_1', \ldots, K_l'$ מסדרים $p^{t_1}, \ldots, p^{t_l}$, בהתאמה. אזי $r = t_1 + \ldots + t_l$. גם עתה נניח $t_1 \geq \ldots \geq t_l$. אם $P \cong P'$, אז קימות $K_1, \ldots, K_l < G$ ציקליות מסדרים $p^{t_1}, \ldots, p^{t_l}$, בהתאמה, כך ש $P = K_1 \cdots K_l$ היא מכפלה ישרה שלהם. לכן $k = l$ ו $s_i = t_i$, $i = 1, \ldots, k$.

מכאן מספר החבורות הקומוטטיביות הבלתי איזומורפיות מסדר p^r הוא מספר הסדרות $s_1, \ldots, s_k$ כך ש $s_1 + \ldots + s_k = r$ ו $s_1 \geq \ldots \geq s_k$. ∎

משפט: *כל חבורה קומוטטיבית סופית איזומורפית לחבורה אחת ורק אחת מהצורה*

$$\bigoplus_{i,j} \mathbb{Z}_{p_i^{s_{i,j}}} = \bigoplus_i \Big(\bigoplus_j \mathbb{Z}_{p_i^{s_{i,j}}} \Big) .$$

הקבוצה $\{p_i^{s_{i,j}}\}$ נקבעת באפן יחיד. אבריה נקראים ***המחלקים היסודיים*** *(**elementary divisors**) של החבורה.*

אם $n = p_1^{r_1} p_2^{r_2} \cdots p_l^{r_l}$, באשר $p_1, \ldots, p_l$ מספרים ראשוניים שונים, אז מספר החבורות הקומוטטיביות הבלתי איזומורפיות מסדר n הוא $\wp(r_1)\, \wp(r_2) \cdots \wp(r_l)$.

הוכחה: תהי G חבורה קומוטטיבית מסדר $n = p_1^{r_1} \cdots p_l^{r_l}$. אזי $G = P_1 P_2 \cdots P_l$ היא מכפלה ישרה של חבורות הסילוב שלה, באשר P_i היא חבורת ה p_i-סילוב של G שהיא מסדר $p_i^{r_i}$, $i = 1, \ldots, l$.

$P_1 = H_{1,1} H_{1,2} \cdots H_{1,k_1}$ היא מכפלה ישרה של חבורות ציקליות $H_{1,1}, H_{1,2}, \ldots, H_{1,k_1}$ מסדרים $p_1^{s_{1,1}}, p_1^{s_{1,2}}, \ldots, p_1^{s_{1,k_1}}$, בהתאמה. אזי $r_1 = s_{1,1} + \ldots + s_{1,k_1}$. נניח $s_{1,1} \geq \ldots \geq s_{1,k_1} \geq 1$.

$P_2 = H_{2,1} H_{2,2} \cdots H_{2,k_2}$ היא מכפלה ישרה של חבורות ציקליות $H_{2,1}, H_{2,2}, \ldots, H_{2,k_2}$ מסדרים $p_2^{s_{2,1}}, p_2^{s_{2,2}}, \ldots, p_2^{s_{2,k_2}}$, בהתאמה. אזי $r_2 = s_{2,1} + \ldots + s_{2,k_2}$. נניח $s_{2,1} \geq \ldots \geq s_{2,k_2} \geq 1$.

לבסוף, $P_l = H_{l,1} H_{l,2} \cdots H_{l,k_l}$ היא מכפלה ישרה של חבורות ציקליות $H_{l,1}, H_{l,2}, \ldots, H_{l,k_l}$ מסדרים $p_l^{s_{l,1}}, p_l^{s_{l,2}}, \ldots, p_l^{s_{l,k_l}}$, בהתאמה. אזי $r_l = s_{l,1} + \ldots + s_{l,k_l}$. נניח $s_{l,1} \geq \ldots \geq s_{l,k_l} \geq 1$.

אזי $G=\prod_{\substack{1\le i\le l\\ 1\le j\le k_i}} H_{i,j}$, באשר $H_{i,j}$ היא ציקלית מסדר $p_i^{s_{i,j}}$ ולכן $H_{i,j}\cong \mathbb{Z}_{p_i^{s_{i,j}}}$. מכאן

$$G\cong \bigoplus_{\substack{1\le i\le l\\ 1\le j\le k_i}} \mathbb{Z}_{p_i^{s_{i,j}}}. \quad \blacksquare$$

דוגמה: תהי G חבורה קומוטטיבית מסדר $18000=2^4\cdot 3^2\cdot 5^3$. אזי $G=P_1P_2P_3$ היא מכפלה ישרה של חבורות הסילוב שלה P_1,P_2,P_3, באשר $|P_1|=2^4, |P_2|=3^2, |P_3|=5^3$. עתה $\wp(4)=5$, $\wp(2)=2$ ו $\wp(3)=3$. לכן מספר החבורות הקומוטטיביות הבלתי איזומורפיות מסדר 18000 הוא $5\cdot 2\cdot 3=30$.

חמשת החבורות הקומוטטיביות הבלתי איזומורפיות מסדר $2^4=16$ הן $\mathbb{Z}_{16}$, $\mathbb{Z}_8\oplus\mathbb{Z}_2$, $\mathbb{Z}_4\oplus\mathbb{Z}_4$, $\mathbb{Z}_4\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$ ו $\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$.

שתי החבורות הקומוטטיביות הבלתי איזומורפיות מסדר $3^2=9$ הן $\mathbb{Z}_9$ ו $\mathbb{Z}_3\oplus\mathbb{Z}_3$.

שלשת החבורות הקומוטטיביות הבלתי איזומורפיות מסדר $5^3=125$ הן $\mathbb{Z}_{125}$, $\mathbb{Z}_{25}\oplus\mathbb{Z}_5$ ו $\mathbb{Z}_5\oplus\mathbb{Z}_5\oplus\mathbb{Z}_5$.

שלושים החבורות הקומוטטיביות הבלתי איזומורפיות מסדר 18000 הן אם־כן:

(מחלקים יסודיים: $2^4,3^2,5^3$) $\quad \mathbb{Z}_{16}\oplus\mathbb{Z}_9\oplus\mathbb{Z}_{125}\cong\mathbb{Z}_{18000}$

(מחלקים יסודיים: $2^3,2,3^2,5^3$) $\quad \mathbb{Z}_8\oplus\mathbb{Z}_2\oplus\mathbb{Z}_9\oplus\mathbb{Z}_{125}\cong\mathbb{Z}_{9000}\oplus\mathbb{Z}_2$

(מחלקים יסודיים: $2^3,2^2,3^2,5^3$) $\quad \mathbb{Z}_4\oplus\mathbb{Z}_4\oplus\mathbb{Z}_9\oplus\mathbb{Z}_{125}\cong\mathbb{Z}_{4500}\oplus\mathbb{Z}_4$

(מחלקים יסודיים: $2^2,2,2,3^2,5^3$) $\quad \mathbb{Z}_4\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_9\oplus\mathbb{Z}_{125}\cong\mathbb{Z}_{4500}\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$

(מחלקים יסודיים: $2,2,2,2,3^2,5^3$) $\quad \mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_9\oplus\mathbb{Z}_{125}\cong\mathbb{Z}_{2250}\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$

(מחלקים יסודיים: $2^4,3,3,5^3$) $\quad \mathbb{Z}_{16}\oplus\mathbb{Z}_3\oplus\mathbb{Z}_3\oplus\mathbb{Z}_{125}\cong\mathbb{Z}_{6000}\oplus\mathbb{Z}_3$

וכך הלאה.

הגדרה: תהי G חבורה קומוטטיבית מסדר $n=p_1^{r_1}\cdots p_l^{r_l}$, באשר $p_1,\ldots,p_l$ ראשוניים שונים ונניח ש $\{p_i^{s_{i,j}} \mid i=1,\ldots,l,\ j=1,\ldots,k_i\}$ היא קבוצת המחלקים היסודיים של G. כלומר

$$G\cong \bigoplus_{1\le i\le l}\Big(\bigoplus_{1\le j\le k_i}\mathbb{Z}_{p_i^{s_{i,j}}}\Big).$$

נניח $s_{i,1}\ge s_{i,2}\ge\ldots\ge s_{i,k_i}\ge 1$, $i=1,\ldots,l$. אזי

$$G\cong\mathbb{Z}_{d_1}\oplus\mathbb{Z}_{d_2}\oplus\ldots\oplus\mathbb{Z}_{d_k},$$

באשר $k=\max_i k_i$ ו $d_1=\prod_i p_i^{s_{i,1}}, d_2=\prod_i p_i^{s_{i,2}},\ldots,d_k=\prod_i p_i^{s_{i,k}}$. שימו־לב שמתקים $n=d_1d_2\cdots d_k$ ו $d_k|d_{k-1}|\cdots|d_1$.

המספרים $d_1,\ldots,d_k$ נקבעים *באפן יחיד* ע"י הדרישות $G\cong\mathbb{Z}_{d_1}\oplus\ldots\oplus\mathbb{Z}_{d_k}$ ו $d_k|\cdots|d_1$. הם נקראים **הגורמים השמורים** (**invariant factors**) של G.

דֻגמה: הגורמים השמורים של החבורה

$$\mathbb{Z}_{2^3} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{5^3} \oplus \mathbb{Z}_{5^2}$$

הם $2^3 \cdot 3^2 \cdot 5^3$, $2^2 \cdot 3 \cdot 5^2$ ו 2 כי $2|2^2 \cdot 3 \cdot 5^2|2^3 \cdot 3^2 \cdot 5^3$.

תרגילים לסעיף 6

40. G חבורה סופית ו $H, K \lhd G$ ומתקים $G = HK$ וכן $|G| = |H||K|$. הוכח/י כי $G \cong H \times K$.

41. אם G מכפלה ישרה פנימית של H ו K הוכח/י כי $G/H \cong K$. הכלל/י תוצאה זו ליותר גורמים.

42. G קומוטטיבית ו G/H ציקלית אינסופית. הוכח/י שקימת $K < G$ כך ש G היא המכפלה הישרה של H ו K.

43. $G = H \times K$ באשר H ציקלית מסדר p^2 ו K ציקלית מסדר p^3. כמה אברים ב G הם מסדר p^2 וכמה חבורות חלקיות ל G הן מסדר p^2 ?

44. כמה חבורות קומוטטיביות בלתי איזומורפיות קימות מסדר 4320 ?

מצא/י עבור כל חבורה כזאת את המחלקים היסודיים ואת הגורמים השמורים.

40. יהיו $H,K\lhd G$ כך ש $G=HK$ ו $|G|=|H||K|$. אזי, על פי תרגיל 50 (א),
$$|H\cap K|=\frac{|H||K|}{|HK|}=\frac{|G|}{|G|}=1\,.$$
לכן $H\cap K=\{1\}$. מכאן G היא מכפלה ישרה פנימית של H,K ולכן $G\cong H\times K$.

41. תהי G מכפלה ישרה פנימית של $H,K<G$. אזי $G=HK$, $H\cap K=\{1\}$ ו $H,K\lhd G$. נגדיר העתקה $\varphi\colon G/H\to K$ ע"י $\varphi(Hhk)=k$, באשר $h\in H, k\in K$. ההעתקה היא חד־ערכית (מוגדרת היטב) וחח"ע כי
$$Hh_1k_1=Hh_2k_2\Leftrightarrow Hk_1=Hk_2\Leftrightarrow k_1k_2^{-1}\in H\cap K=\{1\}\Leftrightarrow k_1=k_2\,.$$
ההעתקה היא ודאי על כי לכל $k\in K$ מתקיים $Hk\mapsto k$. כמו־כן, φ היא הומומורפיזם כי
$$\varphi((Hh_1k_1)(Hh_2k_2))=\varphi((Hk_1)(Hk_2))=\varphi(Hk_1k_2)=k_1k_2=\varphi(Hh_1k_1)\varphi(Hh_2k_2)\,.$$
מכאן $G/H\cong K$.

נתן להכליל תוצאה זו באפן הבא: אם G היא מכפלה ישרה פנימית של $H_1,\dots,H_k<G$, אז
$$G/H_i\cong\prod_{j\neq i}H_j.$$
באפן כללי יותר, אם $I\subset\{1,\dots,k\}$ ו $J=\{1,\dots,k\}\setminus I$, אז $(\prod_{i\in I}H_i)\lhd G$ ו
$$G/(\prod_{i\in I}H_i)\cong\prod_{j\in J}H_j.$$

42. יהיו G קומוטטיבית ו G/H ציקלית אינסופית. יהי Ha יוצר של G/H ותהי $K=\langle a\rangle$. אם $g\in G$, אז $Hg\in\langle Ha\rangle$ ולכן קים $n\in\mathbb{Z}$ כך ש $Hg=Ha^n$. מכאן קים $h\in H$ כך ש $g=ha^n$. לכן $G=HK$. אם $a^m\in H\cap K$ עבור $m\neq 0$, אז $(Ha)^m=Ha^m=H$, בסתירה לכך ש $G/H=\langle Ha\rangle$ היא ציקלית אינסופית. לכן $H\cap K=\{1\}$. מכאן, כיון ש G קומוטטיבית, G היא מכפלה ישרה פנימית של H,K.

43. תהי $G=H\times K$, באשר H ציקלית מסדר p^2 ו K ציקלית מסדר p^3. אבר $(h,k)\in H\times K$ הוא מסדר p^2 אם"ם $(h,k)\neq(1,1)$, $(h^p,k^p)\neq(1,1)$ ו $(h^{p^2},k^{p^2})=(1,1)$. לכן (h,k) הוא מסדר p^2 אם"ם $|h|=p^2$ ו $|k|\le p^2$ או $|k|=p^2$ ו $|h|<p^2$. כיון ש H היא ציקלית מסדר p^2, יש לה רק חבורה חלקית אחת מסדר p ולכן יש בה p אברים מסדר $\le p$ ו p^2-p אברים מסדר p^2. באפן דומה, כיון ש K היא ציקלית מסדר p^3, יש לה רק חבורה חלקית אחת מסדר p ורק חבורה חלקית אחת מסדר p^2 ולכן יש בה p^2 אברים מסדר $\le p^2$ ו p^2-p אברים מסדר p^2. מכאן מספר האברים ב G מסדר p^2 הוא
$$(p^2-p)\cdot p^2+(p^2-p)\cdot p=(p^2-p)(p^2+p)=p^4-p^2\,.$$
זהו גם מספר האברים מסדר p^2 בכל החבורות החלקיות של G שהן ציקליות מסדר p^2. בכל חבורה ציקלית מסדר p^2 יש p^2-p אברים מסדר p^2 וחתוך של שתיים כאלו הוא חבורה חלקית מסדר $\le p$. לכן ל G יש $\frac{(p^2-p)(p^2+p)}{p^2-p}=p^2+p$ חבורות חלקיות ציקליות מסדר p^2.

יהיו P, Q החבורות החלקיות היחידות של H, K, בהתאמה, מסדר p. אזי $P \times Q$ היא החבורה החלקית היחידה של G שאיזומורפית ל $\mathbb{Z}_p \oplus \mathbb{Z}_p$. אכן, אם $L < G$ איזומורפית ל $\mathbb{Z}_p \oplus \mathbb{Z}_p$, אז L היא מכפלה ישרה פנימית של $\langle(h_1, k_1)\rangle$ ו $\langle(h_2, k_2)\rangle$, באשר $(h_1, k_1), (h_2, k_2) \in H \times K$ אברים מסדר p. לכן $h_1, h_2 \in P$ ו $k_1, k_2 \in Q$. אם $h_1 \neq 1$, אז קים i כך ש $h_2 = h_1^i$ ולכן $(1, k_1^{-i}k_2) = (h_1, k_1)^{-i}(h_2, k_2) \in L$. $k_1^{-i}k_2 \neq 1$, אחרת $\langle(h_2, k_2)\rangle = \langle(h_1, k_1)\rangle$. אם $h_1 = 1$, אז $h_2 \neq 1$ (אחרת $\langle(h_2, k_2)\rangle = \langle(h_1, k_1)\rangle$) ובאותו אפן קים $1 \neq k \in Q$ כך ש $(1, k) \in L$. באפן דומה קים $1 \neq h \in P$ כך ש $(h, 1) \in L$. מכאן $P \times Q < L$ ולכן $P \times Q = L$.

חבורה חלקית של G מסדר p^2 איזומורפית ל $\mathbb{Z}_{p^2}$ או ל $\mathbb{Z}_p \oplus \mathbb{Z}_p$. לכן מספר החבורות החלקיות של G מסדר p^2 הוא $p^2 + p + 1$.

44. $4320 = 2^5 \cdot 3^3 \cdot 5$ ולכן יש $\wp(5)\,\wp(3)\,\wp(1) = 7 \cdot 3 \cdot 1 = 21$ חבורות קומוטטיביות בלתי איזומורפיות מסדר 4320:

$\mathbb{Z}_{2^5} \oplus \mathbb{Z}_{3^3} \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{4320}$

מחלקים יסודיים: $2^5, 3^3, 5$, גורמים שמורים: 4320.

$\mathbb{Z}_{2^4} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^3} \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{2160} \oplus \mathbb{Z}_2$

מחלקים יסודיים: $2^4, 2, 3^3, 5$, גורמים שמורים: $2, 2160$.

$\mathbb{Z}_{2^3} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^3} \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{1080} \oplus \mathbb{Z}_4$

מחלקים יסודיים: $2^3, 2^2, 3^3, 5$, גורמים שמורים: $4, 1080$.

$\mathbb{Z}_{2^3} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^3} \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{1080} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

מחלקים יסודיים: $2^3, 2, 2, 3^3, 5$, גורמים שמורים: $2, 2, 1080$.

$\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^3} \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{540} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2$

מחלקים יסודיים: $2^2, 2^2, 2, 3^3, 5$, גורמים שמורים: $2, 4, 540$.

$\mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^3} \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{540} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

מחלקים יסודיים: $2^2, 2, 2, 2, 3^3, 5$, גורמים שמורים: $2, 2, 2, 540$.

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^3} \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{270} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

מחלקים יסודיים: $2, 2, 2, 2, 2, 3^3, 5$, גורמים שמורים: $2, 2, 2, 2, 270$.

$\mathbb{Z}_{2^5} \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{1440} \oplus \mathbb{Z}_3$

מחלקים יסודיים: $2^5, 3^2, 3, 5$, גורמים שמורים: $3, 1440$.

$\mathbb{Z}_{2^4} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{720} \oplus \mathbb{Z}_6$

מחלקים יסודיים: $2^4, 2, 3^2, 3, 5$, גורמים שמורים: $6, 720$.

$\mathbb{Z}_{2^3} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{360} \oplus \mathbb{Z}_{12}$

מחלקים יסודיים: $2^3, 2^2, 3^2, 3, 5$, גורמים שמורים: $12, 360$.

$\mathbb{Z}_{2^3} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{360} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$

מחלקים יסודיים: $2^3, 2, 2, 3^2, 3, 5$, גורמים שמורים: $2, 6, 360$.

$\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{180} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_2$

מחלקים יסודיים: $2^2, 2^2, 2, 3^2, 3, 5$, גורמים שמורים: $2, 12, 180$.

$\mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{180} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

מחלקים יסודיים: $2^2, 2, 2, 2, 3^2, 3, 5$, גורמים שמורים: $2, 2, 6, 180$.

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{90} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

מחלקים יסודיים: $2, 2, 2, 2, 2, 3^2, 3, 5$, גורמים שמורים: $2, 2, 2, 6, 90$.

$\mathbb{Z}_{2^5} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{480} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$

מחלקים יסודיים: $2^5, 3, 3, 3, 5$, גורמים שמורים: $3, 3, 480$.

$\mathbb{Z}_{2^4} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{240} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_3$

מחלקים יסודיים: $2^4, 2, 3, 3, 3, 5$, גורמים שמורים: $3, 6, 240$.

$\mathbb{Z}_{2^3} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{120} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_3$

מחלקים יסודיים: $2^3, 2^2, 3, 3, 3, 5$, גורמים שמורים: $3, 12, 120$.

$\mathbb{Z}_{2^3} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{120} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6$

מחלקים יסודיים: $2^3, 2, 2, 3, 3, 3, 5$, גורמים שמורים: $6, 6, 120$.

$\mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{60} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6$

מחלקים יסודיים: $2^2, 2^2, 2, 3, 3, 3, 5$, גורמים שמורים: $6, 12, 60$.

$\mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{60} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$

מחלקים יסודיים: $2^2, 2, 2, 2, 3, 3, 3, 5$, גורמים שמורים: $2, 6, 6, 60$.

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{30} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

מחלקים יסודיים: $2, 2, 2, 2, 2, 3, 3, 3, 5$, גורמים שמורים: $2, 2, 6, 6, 30$.

סעיף 7: פעולות של חבורות על קבוצות

הגדרה: **פעולה** (**שמאלית**) של חבורה G על קבוצה X היא העתקה $G \times X \to X$ השולחת (g,x) ל $g * x$ והמקימת את שתי התכונות הבאות:

(א) $1 * x = x$ לכל $x \in X$.

(ב) $(g_1g_2) * x = g_1 * (g_2 * x)$ לכל $g_1, g_2 \in G$ ולכל $x \in X$.

הערה: אם חבורה G פועלת (משמאל) על קבוצה X, אז כל $g \in G$ מגדיר העתקה $\ell_g\colon X \to X$ ע"י מכפלה משמאל: $\ell_g(x) = g * x$ לכל $x \in X$. שימו־לב כי $\ell_g \in S(X)$, באשר $S(X)$ היא חבורת כל הפונקציות החח"ע ועל מ X לתוך X. אכן, ℓ_g חח"ע כי $\ell_g(x) = \ell_g(y) \Leftarrow g * x = g * y \Leftarrow g^{-1} * (g * x) = g^{-1} * (g * y) \Leftarrow (g^{-1}g) * x = (g^{-1}g) * y \Leftarrow x = 1 * x = 1 * y = y$ ו ℓ_g על כי לכל $x \in X$, $\ell_g(g^{-1} * x) = g * (g^{-1} * x) = (gg^{-1}) * x = 1 * x = x$.

יתר על כן, ההעתקה $G \to S(X)$ המוגדרת ע"י $g \mapsto \ell_g$ היא הומומורפיזם של חבורות. אכן, לכל $x \in X$ $\ell_{g_1g_2}(x) = (g_1g_2) * x = g_1 * (g_2 * x) = \ell_{g_1}(\ell_{g_2}(x)) = (\ell_{g_1} \circ \ell_{g_2})(x)$ ולכן $\ell_{g_1g_2} = \ell_{g_1} \circ \ell_{g_2}$.

להיפך, אם $\varphi\colon G \to S(X)$ הוא הומומורפיזם, אז ההעתקה $G \times X \to X$ המוגדרת על ידי $(g,x) \mapsto \varphi(g)(x)$ היא פעולה שמאלית של G על X. אכן, אם נרשם $g \cdot x = \varphi(g)(x)$, אז $1 \cdot x = \varphi(1)(x) = \mathrm{id}_X(x) = x$ לכל $x \in X$ ו

$$(g_1g_2) \cdot x = \varphi(g_1g_2)(x) = \varphi(g_1) \circ \varphi(g_2)(x) = \varphi(g_1)(\varphi(g_2)(x)) = g_1 \cdot (g_2 \cdot x)$$

לכל $g_1, g_2 \in G$ ו $x \in X$.

משפט קיילי המוכלל: *תהי G חבורה ותהי $H < G$ חבורה חלקית. נסמן $X = \{cH \mid c \in G\}$. אזי קים הומומורפיזם $\varphi\colon G \to S(X)$ כך ש $\ker(\varphi)$ היא החבורה החלקית הנורמלית הגדולה ביותר של G המוכלת ב H.*

אם $[G:H] = m$, אז קים הומומורפיזם $G \to S_m$.

הוכחה: נגדיר פעולה של G על X באפן הבא: עבור $g \in G$ ו $cH \in X$, $g * cH = gcH$. זוהי אכן פעולה כי $1 * cH = cH$ ו $(gh) * cH = ghcH = g(h(cH)) = g * (h * cH)$ לכל $g, h \in G$ ו $cH \in X$. מכאן ההעתקה $G \to S(X)$ המוגדרת ע"י $g \mapsto \ell_g$ היא הומומורפיזם, באשר $\ell_g\colon X \to X$ היא ההעתקה המוגדרת ע"י $\ell_g(cH) = gcH$ לכל $cH \in X$.

במקרה ש $[G:H] = m$ סופי, $S(X) \cong S_m$ ולכן קים הומומורפיזם $\varphi\colon G \to S_m$.

יהי $K = \ker(\varphi)$. אזי $g \in K$ אם"ם $\ell_g = \mathrm{id}_X$ אם"ם $gcH = cH$ לכל $c \in G$ ולכן

$$K = \{g \in G \mid c^{-1}gc \in H \text{ לכל } c \in G\}\ .$$

$K < H$ כי $g \in K \Leftarrow g = 1^{-1} \cdot g \cdot 1 \in H$. כמו־כן, $K \lhd G$ בתור גרעין של הומומורפיזם.

אם גם $L < H$ ו $L \lhd G$, אז $L < K$. אכן, יהי $g \in L$. אזי, כיון ש $L \lhd G$, $c^{-1}gc \in L$ לכל $c \in G$ ולכן, כיון ש $L < H$, $c^{-1}gc \in H$ לכל $c \in G$. מכאן $g \in K$. ∎

הערה: במקרה ש $H = \{1\}$ מתקבלת ההצגה של קיילי $G \hookrightarrow S(G)$ המוגדרת ע"י $g \mapsto \ell_g$. שימו־לב שההצגה נאמנה, כלומר ההעתקה היא חח"ע, כיון שהגרעין K מוכל ב $H = \{1\}$ ולכן $K = \{1\}$. אם $|G| = n$, אז $G \hookrightarrow S_n$.

מסקנה 1: *אם $G < H$ ו $K \ntriangleleft G$ לכל $H < K \neq \{1\}$, אז $G \hookrightarrow S(X)$, באשר $X = \{cH \mid c \in G\}$. אם $[G : H] = m$, אז $G \hookrightarrow S_m$.*

הוכחה: לפי המשפט קים הומומורפיזם $\varphi\colon G \to S(X)$ כך ש $\ker(\varphi) \subseteq H$. לכן, כיון ש $\ker(\varphi) \lhd G$, $\ker(\varphi) = \{1\}$. כלומר φ חח"ע. ∎

דֻגמה: תהי $G = D_4 = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$, באשר $a^4 = b^2 = 1$ ו $ab = ba^3$ ותהי $H = \{1, b\}$. אזי $H \ntriangleleft G$ כי $aba^{-1} = ba^3a^{-1} = ba^2 \notin H$. לכן $K = \{1\}$ היא החבורה החלקית הנורמלית היחידה של G המוכלת ב H. מכאן, כיון ש $[D_4 : H] = 4$, $D_4 \hookrightarrow S_4$.

מסקנה 2: *יהיו $G < H$ עם $|G| = n$ ו $[G : H] = m$. אזי H מכילה חבורה חלקית נורמלית K של G כך ש $[G : K] | (m!, n)$.*

בפרט, אם $n \nmid m!$, אז $K \neq \{1\}$. אם בנוסף $|H| = \frac{n}{m}$ הוא מספר ראשוני, אז $H \lhd G$.

הוכחה: לפי המשפט קים הומומורפיזם $\varphi\colon G \to S_m$ כך ש $K = \ker(\varphi) \subseteq H$. אזי, בעזרת משפט האיזומורפיזם ה I, $G/K \hookrightarrow S_m$ ולכן $[G : K] | m!$. מצד שני, בעזרת משפט לגרנג', $[G : K] | |G| = n$. לכן $[G : K] | (m!, n)$.

בפרט, אם $n \nmid m!$, אז $[G : K] \neq n$ ולכן $K \neq \{1\}$. אם בנוסף H היא חבורה מסדר ראשוני, אז, בעזרת משפט לגרנג', כל חבורה חלקית לא טריביאלית של H היא H עצמה. לכן $K = H$ ומכאן $H \lhd G$. ∎

דֻגמה: יהיו $G < H$ עם $|G| = 20$ ו $|H| = 5$. אזי $[G : H] = 4$ ו $20 \nmid 24 = 4!$. לכן, כיון ש H היא מסדר ראשוני, $H \lhd G$.

דֻגמה נוספת: יהיו $G < H$ עם $|G| = 99$ ו $|H| = 11$. אזי $[G : H] = 9$ ו $99 \nmid 9!$. לכן, כיון ש H היא מסדר ראשוני, $H \lhd G$.

מסקנה 3: *תהי G חבורה סופית ויהי p המספר הראשוני הקטן ביותר כך ש $p | |G|$. נניח G מכילה חבורה חלקית H כך ש $[G : H] = p$. אזי $H \lhd G$.*

הוכחה: על פי מסקנה 2, H מכילה חבורה חלקית נורמלית K של G כך ש $[G:K]|(p!,|G|)$. אולם $p=(p!,|G|)$ כי ל $|G|$ אין גורם ראשוני המחלק את $(p-1)!$. לכן $H \subseteq K$ ושניהם מאינדקס p ב G. מכאן $H = K$ ולכן $H \lhd G$. ∎

הערה: ל G לא חיבת להיות חבורה חלקית מאינדקס p. לדֻגמה, ל A_4 אין חבורה חלקית מאינדקס 2 (ראו סעיף 9).

מסקנה 4: *תהי G חבורה (אינסופית) ו $G < H$ מאינדקס סופי. אזי H מכילה חבורה חלקית נורמלית של G מאינדקס סופי.*

הוכחה: יהי $m=[G:H]$. על פי המשפט קים הומומורפיזם $\varphi\colon G \to S_m$ כך ש $K=\ker(\varphi) \subseteq H$. בעזרת משפט האיזומורפיזם הראשון, $G/K \hookrightarrow S_m$. לכן G/K סופית ואם־כן $[G:K]=|G/K|$ סופי. כלומר, $K \lhd G$ מאינדקס סופי. ∎

פעולת ההצמדה

הגדרה: תהי G חבורה. שני אברים $x,y \in G$ נקראים **צמודים** אם קים $g \in G$ כך ש $y=gxg^{-1}$.

טענה: *תהי G חבורה. ההעתקה $G \times G \to G$ הנתנת ע"י $(g,x) \mapsto gxg^{-1}$ היא פעולה של G על עצמה.*

הוכחה: נסמן $g * x = gxg^{-1}$ עבור $g,x \in G$. אזי $1 * x = 1 \cdot x \cdot 1^{-1} = x$ לכל $x \in G$ ו

$$(g_1g_2) * x = g_1g_2x(g_1g_2)^{-1} = g_1g_2xg_2^{-1}g_1^{-1} = g_1 * (g_2xg_2^{-1}) = g_1 * (g_2 * x)$$

לכל $g_1,g_2,x \in G$. ∎

הערה: יחס ההצמדה הוא יחס שקילות:

רפלקסיביות: $x = 1 \cdot x \cdot 1^{-1}$.

סימטריות: $y = gxg^{-1} \Leftarrow x = g^{-1}y(g^{-1})^{-1}$.

טרנזיטיביות: $y=g_2xg_2^{-1}$, $z=g_1yg_1^{-1} \Leftarrow z=(g_1g_2)x(g_1g_2)^{-1}$.

מחלקות השקילות נקראות **מחלקות צמידות**.

הגדרה: תהי σ תמורה ב S_n ונפרק אותה למכפלה של מחזורים זרים

$$\sigma = (a_{1,1} \dots a_{1,r_1}) \cdots (a_{k,1} \dots a_{k,r_k}) \; ,$$

באשר $n = r_1 + r_2 + \dots + r_k$ ו $r_1 \ge r_2 \ge \dots \ge r_k$. הסדרה $(r_1,\dots,r_k)$ נקראת **הטפוס** (**type**) של σ.

מספר הטפוסים האפשריים ב S_n הוא אם כן $\wp(n)$ (ראו סוף סעיף 6).

משפט: *$\sigma, \tau \in S_n$ הן צמודות אם"ם הן מאותו טפוס.*

מכאן, מספר מחלקות הצמידות ב S_n הוא $\wp(n)$.

הוכחה: נניח $\sigma = (a_{1,1} \dots a_{1,r_1}) \cdots (a_{k,1} \dots a_{k,r_k})$

ו $\tau = (b_{1,1} \dots b_{1,r_1}) \cdots (b_{k,1} \dots b_{k,r_k})$.

תהי

$$\gamma = \begin{pmatrix} a_{1,1} & \dots & a_{1,r_1} & \dots & a_{k,1} & \dots & a_{k,r_k} \\ b_{1,1} & \dots & b_{1,r_1} & \dots & b_{k,1} & \dots & b_{k,r_k} \end{pmatrix}.$$

אזי חשוב נותן $\gamma\sigma\gamma^{-1} = \tau$. למשל

$$\gamma\sigma\gamma^{-1}(b_{1,1}) = \gamma\sigma(a_{1,1}) = \gamma(a_{1,2}) = b_{1,2} = \tau(b_{1,1}).$$

כלומר, אם σ, τ הן מאותו טפוס, אז הן צמודות.

להיפך, אם $\sigma, \gamma \in S_n$, אז σ ו $\gamma\sigma\gamma^{-1}$ הן מאותו טפוס. ∎

דֻגמה: המחזורים $\sigma = (1\,2\,3\,4\,5)$ ו $\tau = (5\,3\,1\,2\,4)$ הם מאותו טפוס ב S_5 ומתקיים

$$\begin{pmatrix} 5 & 3 & 1 & 2 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} (1\,2\,3\,4\,5) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix} = (5\,3\,1\,2\,4).$$

דֻגמה: יהיו $\sigma = (1\,3\,4)(2\,5)(6\,7)$ ו

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 5 & 3 & 1 & 7 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 4 & 2 & 5 & 6 & 7 \\ 4 & 5 & 3 & 6 & 1 & 7 & 2 \end{pmatrix}$$

תמורות ב S_7. אזי $\gamma\sigma\gamma^{-1} = (4\,5\,3)(6\,1)(7\,2)$ היא תמורה מאותו טפוס כמו σ.

דֻגמה: מספר מחלקות הצמידות ב S_5 הוא $\wp(5) = 7$, כמספר הטפוסים האפשריים של תמורות ב S_5 שהם מהצורה $(1\,2\,3\,4\,5)$, $(1\,2\,3\,4)(5)$, $(1\,2\,3)(4\,5)$, $(1\,2\,3)(4)(5)$, $(1\,2)(3\,4)(5)$, $(1\,2)(3)(4)(5)$ או $(1)(2)(3)(4)(5)$.

מסלול ומיצב

הגדרה: תהי G חבורה הפועלת על קבוצה X. נגדיר יחס על X ע"י $x \sim y$ אם קים $g \in G$ כך ש $g * x = y$. קל לראות שזהו יחס שקילות. מחלקת השקילות של $x \in X$ נקראת **המסלול** של x והיא שוה ל $G * x = \{g * x \mid g \in G\}$.

דֻגמה: יהיו $H < G$ ונגדיר פעולה של H על G ע"י $h * x = hx$ לכל $h \in H, x \in G$. המסלול של $x \in G$ הוא $H * x = \{hx \mid h \in H\} = Hx$. כלומר, המסלולים הם המחלקות הימניות.

דֻגמה: נגדיר פעולה של החבורה $G=\left\{\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix} \;\middle|\; 0\le\theta<2\pi\right\}$ על הקבוצה $X=\mathbb{R}^2$

ע"י $\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}*\begin{pmatrix}x\\ y\end{pmatrix}=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}$ (סבוב בזוית θ).

המסלולים הם מעגלים שמרכזם בראשית הצירים.

הגדרה: תהי G חבורה הפועלת על קבוצה X. **המְיַצֵב** (**stabilizer**) של $x\in X$ היא הקבוצה

$$\mathrm{Stb}(x)=\{g\in G\mid g*x=x\}.$$

טענה: *תהי G חבורה הפועלת על קבוצה X ויהי $x\in X$. אזי $\mathrm{Stb}(x)<G$.*

הוכחה: $1\in\mathrm{Stb}(x)$ כי $1*x=x$.

אם $g\in\mathrm{Stb}(x)$, אז $x=g*x$. לכן $x=1*x=(g^{-1}g)*x=g^{-1}*(g*x)=g^{-1}*x$ ומכאן $g^{-1}\in\mathrm{Stb}(x)$.

אם $g_1,g_2\in\mathrm{Stb}(x)$, אז $g_1*x=x$ ו $g_2*x=x$. לכן $x=g_1*x=g_1*(g_2*x)=(g_1g_2)*x$ ומכאן $g_1g_2\in\mathrm{Stb}(x)$. ∎

משפט: *תהי G חבורה הפועלת על קבוצה X ויהי $x\in X$. אזי מספר האברים במסלול של x הוא $|G*x|=[G:\mathrm{Stb}(x)]$. מכאן $|G*x|\,\big|\,|G|$.*

הוכחה: נסמן $H=\mathrm{Stb}(x)$. אזי $[G:\mathrm{Stb}(x)]$ הוא מספר אברי הקבוצה $\{gH\mid g\in G\}$.

נגדיר העתקה $G*x\to\{gH\mid g\in G\}$

ע"י $g*x\mapsto gH$.

יש להראות כי ההעתקה מוגדרת היטב והיא חח"ע ועל.

אכן, העתקה זו היא חד־ערכית (כלומר מוגדרת היטב) וחד־חד־ערכית כי

$$g_1*x=g_2*x\Leftrightarrow(g_2^{-1}g_1)*x=x\Leftrightarrow g_2^{-1}g_1\in\mathrm{Stb}(x)=H\Leftrightarrow g_1H=g_2H$$

ובודאי העתקה זו היא על כי כל אבר gH מתקבל מ $g*x$. ∎

דֻגמה: תהי $\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8\\3&6&5&8&1&2&7&4\end{pmatrix}$ תמורה ב S_8 ותהי $X=\{1,2,3,4,5,6,7,8\}$.

אזי $G=\langle\sigma\rangle=\{\mathrm{id},\sigma,\sigma^2,\sigma^3,\sigma^4,\sigma^5\}$ פועלת על X ע"י $\sigma^i*x=\sigma^i(x)$.

המסלולים הם בעצם המחזורים בפרוק של σ למחזורים זרים: $G*1=G*3=G*5=\{1,3,5\}$, $G*2=G*6=\{2,6\}$, $G*4=G*8=\{4,8\}$ ו $G*7=\{7\}$.

$\mathrm{Stb}(1)=\{\mathrm{id},\sigma^3\}$ כי $\mathrm{id}(1)=1$ $\sigma(1)\neq1$, $\sigma^2(1)\neq1$, $\sigma^3(1)=1$, $\sigma^4(1)\neq1$ ו $\sigma^5(1)\neq1$.

לכן $3=\frac{6}{2}=[G:\mathrm{Stb}(1)]=|G*1|$.

$\mathrm{Stb}(2)=\{\mathrm{id},\sigma^2,\sigma^4\}$ ואכן $2=\frac{6}{3}=[G:\mathrm{Stb}(2)]=|G*2|$.

$\mathrm{Stb}(4)=\{\mathrm{id},\sigma^2,\sigma^4\}$ ואכן $|G*4|=[G:\mathrm{Stb}(2)]=\frac{6}{3}=2$.

$\mathrm{Stb}(7)=G$ ואכן $|G*7|=[G:\mathrm{Stb}(7)]=1$.

הקבוצה X היא אחוד זר של המסלולים; כלומר $X=G*1\dot{\bigcup}G*2\dot{\bigcup}G*4\dot{\bigcup}G*7$. לכן $|X|=|G*1|+|G*2|+|G*4|+|G*7|$. ואכן $8=3+2+2+1$.

הערה: תהי G חבורה הפועלת על קבוצה X. אזי X מתפרק לאחוד זר של מסלולים ומספר האברים במסלול של $x\in X$ הוא $|G*x|=[G:\mathrm{Stb}(x)]$.

כאשר X סופית, מספר המסלולים סופי. נניח $X=G*x_1\dot{\bigcup}\dots\dot{\bigcup}G*x_k$. אזי

$$|X|=\sum_{i=1}^{k}|G*x_i|=\sum_{i=1}^{k}[G:\mathrm{Stb}(x_i)]\,.$$

כאשר G סופית וגם X סופית, אז $|X|=\sum_{i=1}^{k}\frac{|G|}{|\mathrm{Stb}(x_i)|}$.

נֻסחת המחלקה

הגדרה: תהי G חבורה. **המֶרְכָּז** (**center**) של G היא החבורה החלקית הנורמלית (ראו שאלה 34 (ב))

$$Z(G)=\{x\in G\mid\ gx=xg \text{ לכל } g\in G\}\,.$$

עבור $x\in G$ אנו מסמנים את קבוצת כל אברי החבורה המתחלפים עם x ב $C(x)$. כלומר $C(x)=\{g\in G\mid\ gx=xg\}$. $C(x)$ נקרא **המְרַכֵּז** (**centralizer**) של x.

הערה: תהי G חבורה סופית. נפעיל את G על עצמה ע"י פעולת ההצמדה, כלומר $g*x=gxg^{-1}$ לכל $g,x\in G$. אזי המסלול של $x\in X$ הוא $G*x=\{gxg^{-1}\mid\ g\in G\}$ והמיצב שלו הוא

$$\mathrm{Stb}(x)=\{g\in G\mid\ gxg^{-1}=x\}=\{g\in G\mid\ gx=xg\}=C(x)\,.$$

לכן מספר האברים במסלול של x הוא $|G*x|=[G:\mathrm{Stb}(x)]=[G:C(x)]=\frac{|G|}{|C(x)|}$.

שימו־לב כי $x\in Z(G)\Leftrightarrow gx=xg$ לכל $g\in G\Leftrightarrow g*x=gxg^{-1}=x$ לכל $g\in G\Leftrightarrow$ $G*x=\{x\}$. כלומר המסלולים בני אבר אחד הם אלו בדיוק המתקבלים ע"י אברי $Z(G)$. לכן, אם $x\in Z(G)$, אז $C(x)=G$ (כי $1=|G*x|=[G:C(x)]$). מכאן $Z(G)=\{x\in G\mid\ C(x)=G\}$.

יהיו $G*x_1,\dots,G*x_k$ המסלולים אשר מספר אבריהם גדול מ 1. אזי, כיון שמספר המסלולים בני אבר אחד הוא $|Z(G)|$,

$$|G|=|Z(G)|+\sum_{i=1}^{r}|G*x_i|\,.$$

מכאן אנו מקבלים את

נֻסחת המחלקה (**class formula**): $$|G|=|Z(G)|+\sum_{i=1}^{r}\frac{|G|}{|C(x_i)|}\,.$$

משפט: *תהי G חבורה מסדר p^n, באשר p מספר ראשוני. אזי $Z(G) \neq \{1\}$.*

הוכחה: בסמונים הקודמים, $p^n = |Z(G)| + \sum_{i=1}^{r} \frac{p^n}{|C(x_i)|}$.

$C(x_i) < G$ ולכן $|C(x_i)|\big|p^n$. מכאן $|C(x_i)| = p^{n_i}$ עבור $n_i \leq n$. לא יתכן $n_i = n$ כי אז $|C(x_i)| = p^n$, כלומר $C(x_i) = G$, אולם $x_i \notin Z(G)$. אם־כך $n_i < n$. לכן $p|p^{n-n_i}$ ולכן $p|\sum_{i=1}^{r} p^{n-n_i}$. מכאן $p\big||Z(G)|$ ובפרט $Z(G) \neq \{1\}$. ■

מסקנה: *אם p מספר ראשוני, אז כל חבורה בעלת p^2 אברים היא קומוטטיבית.*

הוכחה: תהי G חבורה מסדר p^2. על פי המשפט הקודם, $Z(G) \neq \{1\}$. לכן $|Z(G)| = p$ או $|Z(G)| = p^2$. אם $|Z(G)| = p^2$, אז $Z(G) = G$, כלומר G קומוטטיבית.

נניח בשלילה ש $|Z(G)| = p$. יהי $1 \neq a \in Z(G)$. אזי a הוא מסדר p. כמו־כן יהי $b \notin Z(G)$. אזי גם b הוא מסדר p (אם b היה מסדר p^2, אז G היתה ציקלית ובפרט קומוטטיבית).

כיון ש $a \in Z(G)$, $ab = ba$ ולכן $a^i b^j = b^j a^i$ לכל $i, j \in \mathbb{Z}$. מכאן $\langle a, b\rangle$ היא חבורה חלקית קומוטטיבית. היא מכילה את $Z(G)$ ואת b ולכן $|G| = |\langle a, b\rangle| > p$ (כי יש יותר מ p אברים בתוך החבורה). לכן $G = \langle a, b\rangle$ ומכאן $b \in Z(G)$, סתירה. ■

משפט קושי: *תהי G חבורה סופית ויהי p מספר ראשוני. אם $p\big||G|$, אז קים ב G אבר מסדר p.*

הוכחה: נוכיח את הטענה באינדוקציה. הנחת האינדוקציה: הטענה נכונה עבור כל חבורה מסדר קטן מ $|G|$.

אם $p \nmid |G|$, אז הטענה נכונה באפן ריק.

נניח $p\big||G|$. אם $p\big||Z(G)|$, אזי קים אבר מסדר p בתוך $Z(G)$ (ולכן בתוך G) על סמך המשפט המתאים שהוכח עבור חבורה קומוטטיבית.

אם $p \nmid |Z(G)|$, אז מִנֻסחת המכפלה $|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|C(x_i)|}$ נובע שקים מחובר ב $\sum$ שאינו מתחלק ב p. כלומר קים i כך ש $p \nmid \frac{|G|}{|C(x_i)|}$. לכן, כיון ש $p\big||G|$, $p\big||C(x_i)|$. עתה $C(x_i) < G$ ו $C(x_i) \neq G$ כי $x_i \notin Z(G)$. מכאן $|C(x_i)| < |G|$. נתן אם־כן להפעיל את הנחת האינדוקציה על $C(x_i)$ ולקבל שקים אבר מסדר p בתוך $C(x_i)$ ולכן בתוך G. ■

45. יהיו p, q ראשוניים וכן $q > p$. תהי G חבורה מסדר pq ונניח ש a אבר מסדר p ו b אבר מסדר q. נסמן $P = \langle a \rangle$ ו $Q = \langle b \rangle$. הוכח/י ש $P \lhd G$ והסק/י ש $bab^{-1} = a^r$, באשר $1 \leq r \leq p-1$. אם $r = 1$, הוכח/י כי G קומוטטיבית ואפילו ציקלית.

46. (א) בהמשך לתרגיל הקודם, הראה/י כי אפילו אם $r \neq 1$ מתקים

$$G = \{a^i b^j \mid i = 0, 1, \ldots, p-1;\ j = 0, 1, \ldots, q-1\}\ .$$

(ב) אם $r > 1$, אזי

$$b^j a b^{-j} = a^{r^j}$$

ואם־כן $a = a^{r^q}$ ולכן $r^q \equiv 1 \pmod{p}$. הסק/י ש r אבר מסדר q בחבורה $U(p)$ ולכן $q | p-1$.

47. מצא/י את 20 המספרים הקטנים ביותר n מהצורה pq, באשר p, q ראשוניים, כך שכל חבורה מסדר $n = pq$ היא ציקלית. (המספר הקטן ביותר הוא 15, $3 \nmid 5-1$.)

48. תהי G חבורה מסדר p^n, באשר p מספר ראשוני. הוכח/י שקימות חבורות חלקיות $G_1, \ldots, G_{n-1}$ המקימות: $|G_i| = p^i$, $G_i < G_{i+1}$ ו $G_i \lhd G$.

(רמז: קח/י $a \in Z(G)$ מסדר p. הגדר/י $G_1 = \langle a \rangle$ ועבר/י ל G/G_1.)

45. נתון: $p>q$, $|G|=pq$, $P=\langle a\rangle$ מסדר p ו $Q=\langle b\rangle$ מסדר q. אזי $P\lhd G$ על פי מסקנה 2 של משפט קיילי המוכלל (עבור $H=P$) כי $[G:P]=q$, $|G|=pq\nmid q!$ (כיון ש $p>q$) ו $|P|=p$ הוא מסדר ראשוני. (הערה: בעזרת משפטי סילוב שבסעיף הבא, מספר חבורות p־סילוב הוא מהצורה $kp+1$, באשר $kp+1|q$ ולכן, כיון ש $p>q$, $k=0$. מכאן P היא חבורת p־סילוב יחידה ב G ולכן נורמלית.)

כיון ש $P\lhd G$ ו $a\in P$, $b\in G$, נובע $bab^{-1}\in P=\langle a\rangle$. לכן קים r בין 1 ל $p-1$ כך ש $bab^{-1}=a^r$.

אם $r=1$, אז $bab^{-1}=a$ ולכן $ba=ab$. לכן, כיון ש $G=\langle a,b\rangle$, G קומוטטיבית. בנוסף, כיון ש $ab=ba$, $|a|=p$, $|b|=q$ ו $(p,q)=1$, נובע כי ab הוא אבר מסדר pq ב G. מכאן, כיון ש $|G|=pq$, G היא ציקלית.

46. (א) כמובן $\{a^ib^j \mid 0\le i\le p-1, 0\le j\le q-1\}\subseteq G$. כדי להוכיח שויון, מספיק להראות שהקבוצה באגף ימין מכילה pq אברים.

אכן, $P\cap Q$ היא חבורה חלקית של P ושל Q ולכן הסדר שלה מחלק את $(p,q)=1$ ומכאן $P\cap Q=\{1\}$. לכן אם קים שויון $a^ib^j=a^{i'}b^{j'}$, באשר $0\le i,i'\le p-1$ ו $0\le j,j'\le q-1$, אז $a^{i-i'}=b^{j'-j}\in P\cap Q=\{1\}$. מכאן $a^i=a^{i'}$, $b^j=b^{j'}$ ולכן $i=i'$, $j=j'$.

(ב) אם $2\le r\le p-1$, באשר $bab^{-1}=a^r$, אז G אינה קומוטטיבית. מתקים

$$b^2ab^{-2}=b(bab^{-1})b^{-1}=ba^rb^{-1}=(bab^{-1})^r=(a^r)^r=a^{r^2}\ ,$$
$$b^3ab^{-3}=b(b^2ab^{-2})b^{-1}=ba^{r^2}b^{-1}=(bab^{-1})^{r^2}=(a^r)^{r^2}=a^{r^3}$$

ולבסוף, $b^qab^{-q}=a^{r^q}$. אולם $|b|=q$ ולכן $b^q=1$. מכאן $a=a^{r^q}$. לכן $a^{r^q-1}=1$. אולם $|a|=p$ ולכן $p|r^q-1$. כלומר $r^q\equiv 1 \pmod p$.

כיון ש $2\le r\le p-1$, $(r,p)=1$ ולכן $r\in U(p)$. כמו־כן, מהפסקה הקודמת נובע שהסדר של r ב $U(p)$ מחלק את q. לכן, כיון ש q ראשוני, הסדר של r הוא 1 או q. אולם $2\le r\le p-1$ ולכן $r^1=r\not\equiv 1 \ (\bmod\ p)$. מכאן הסדר של r ב $U(p)$ הוא q. כיון ש $|U(p)|=p-1$, נובע $q|p-1$.

47. ראינו בתרגיל 46 (ב) שאם חבורה G מסדר pq אינה קומוטטיבית, באשר $p>q$ מספרים ראשוניים, אז בהכרח $q|p-1$. לכן אם $q\nmid p-1$, אז כל חבורה מסדר pq היא קומוטטיבית ואפילו ציקלית על פי תרגיל 45.

להיפך, אם $q|p-1$, אז פרט לחבורה הציקלית מסדר pq יש גם חבורה אחת מסדר pq שאינה קומוטטיבית. אכן, כיון ש $U(p)$ ציקלית מסדר $p-1$ ו $q|p-1$, נובע שקים אבר מסדר q בתוך $U(p)=\{1,2,\ldots,p-1\}$, נקרא לו r. אזי $2\le r\le p-1$. לכן החבורה

$$\langle a,b \mid\ a^p=1, b^q=1, bab^{-1}=a^r\rangle=\{a^ib^j \mid\ 0\le i\le p-1, 0\le j\le q-1\}$$

אינה קומוטטיבית ועל פי תרגיל 46 (א) היא מסדר pq.

דוגמה: אם $p=3$, $q=2$, אז $U(p)=\{1,2\}$ ו $2\in U(p)$ הוא אבר מסדר 2. החבורה הלא קומוטטיבית מסדר $6=3\cdot 2$ המתקבלת בדרך זה היא $\langle a,b \mid a^3=1, b^2=1, bab^{-1}=a^2\rangle$. כך יוצרים את S_3. באפן כללי: אם $p>2$ מספרים ראשוניים, אז $p-1$ הוא אבר מסדר 2 ב $U(p)$ כי $(p-1)^2\equiv 1 \pmod p$ ולכן $\langle a,b \mid a^p=1, b^2=1, bab^{-1}=a^{p-1}\rangle$ היא חבורה לא קומוטטיבית מסדר $2p$.

מסקנה: *יהיו $q<p$ מספרים ראשוניים. אזי $q \nmid p-1$ אם"ם כל חבורה מסדר pq היא ציקלית.*

מכאן 20 המספרים הקטנים ביותר n מהצורה pq, באשר p,q ראשוניים שונים, כך שכל חבורה מסדר $n=pq$ היא ציקלית הם: $15=3\cdot 5$, $33=3\cdot 11$, $35=5\cdot 7$, $51=3\cdot 17$, $65=5\cdot 13$, $69=3\cdot 23$, $77=7\cdot 11$, $85=5\cdot 17$, $87=3\cdot 29$, $91=7\cdot 13$, $95=5\cdot 19$, $115=5\cdot 23$, $119=7\cdot 17$, $123=3\cdot 41$, $133=7\cdot 19$, $141=3\cdot 47$, $143=11\cdot 13$, $145=5\cdot 29$, $159=3\cdot 53$, $161=7\cdot 23$.

48. יהי p מספר ראשוני. אנו נוכיח באינדוקציה על n שאם G היא חבורה מסדר p^n, אז קימות לה חבורות חלקיות $G_1,\ldots,G_{n-1}$ כך ש $G_1<G_2<\ldots<G_{n-1}<G$, $G_i\triangleleft G$ ו $|G_i|=p^i$, $i=1,\ldots,n-1$.

אכן, על פי משפט מסעיף 7, $Z(G)\neq\{1\}$ ולכן יש לה אבר a מסדר p. נסמן $G_1=\langle a\rangle$. אזי $|G_1|=p$. כמו־כן, כיון ש $G_1<Z(G)$, $xG_1=G_1x$ לכל $x\in G$ ולכן $G_1\triangleleft G$. נעבור לחבורת המנה G/G_1 שהיא מסדר $\frac{p^n}{p}=p^{n-1}$. אזי מהנחת האינדוקציה נובע שקימות ל G/G_1 חבורות חלקיות $G_2/G_1,\ldots,G_{n-1}/G_1$ המקימות $G_i/G_1<G_{i+1}/G_1$, $G_i/G_1\triangleleft G/G_1$ ו $|G_i/G_1|=p^{i-1}$. מכאן $G_1,G_2,\ldots,G_{n-1}$ הן חבורות חלקיות של G המקימות $G_i<G_{i+1}$, $G_i\triangleleft G$ ו $|G_i|=p^i$. (שימו־לב שאם $L<G/K$, אז $G>\{a\in G \mid Ka\in L\}=H$ מקימת $L=H/K$. אם בנוסף $L\triangleleft G/K$, אז $H\triangleleft G$ – ראו הערה בפתרון תרגיל 39.)

משפט 1 (קיום של תת־חבורה סילוב): *תהי G חבורה מסדר n ויהי p מספר ראשוני כך ש $p^k|n$. אזי קימת ל G חבורה חלקית H מסדר p^k.*

הוכחה: נוכיח את הטענה באינדוקציה על n. ההוכחה מתחלקת לשני מקרים.

מקרה (א): $p||Z(G)|$. נבחר $a \in Z(G)$ מסדר p. ($Z(G)$ קומוטטיבית ולכן על סמך המשפט המתאים שהוכח עבור חבורה קומוטטיבית, קים ל $Z(G)$ אבר מסדר p.) נתבונן ב $K = \langle a \rangle$. $K \lhd G$ כי $K \subseteq Z(G)$ ולכן $xK = Kx$ לכל $x \in G$. נעבור לחבורת המנה G/K. $\frac{n}{p} = |G/K| < n$ ו $p^k|n \Leftarrow p^{k-1}|\frac{n}{p}$. לכן, על סמך הנחת האינדוקציה, קימת ל G/K חבורה חלקית מסדר p^{k-1}. חבורה חלקית זו צורתה H/K באשר $H < G$. לכן $p^{k-1} = |H/K| = \frac{|H|}{|K|} = \frac{|H|}{p}$ ומכאן $|H| = p^k$.

מקרה (ב): $p \nmid |Z(G)|$. על פי נֻסחת המחלקה
$$|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|C(x_i)|},$$
באשר $x_1, \ldots, x_r$ מהוים מיצגים של מחלקות הצמידות השונות אשר מספר אבריהן > 1.

עתה $|Z(G)| \nmid p$ ולכן קים i כך ש $p \nmid \frac{|G|}{|C(x_i)|}$. $p^k||G|$ ולכן $p^k||C(x_i)|$, אחרת $p|\frac{|G|}{|C(x_i)|}$. מכאן $G > C(x_i)$ ו $C(x_i) \neq G$ (אחרת $gx_i = x_ig$ לכל $g \in G$, אולם $x_i \in C(x_i) \setminus Z(G)$). $|C(x_i)| < |G|$. נתן אם־כן להפעיל את הנחת האינדוקציה על $C(x_i)$ ולקבל שקימת חבורה חלקית של $C(x_i)$ (ולכן גם של G) מסדר p^k. ∎

הגדרה: תהי G חבורה מסדר n ויהי p מספר ראשוני המחלק את n. נניח $n = p^r m$ ו $p \nmid m$, כלומר r מרבי כך ש $p^r|n$. חבורה חלקית ל G מסדר p^r נקראת **חבורת p־סילוב** של G.

הגדרה: אם p הוא מספר ראשוני, חבורה שהסדר שלה הוא חזקה של p נקראת **חבורת־**p.

משפט 2 (צמידות של תת־חבורות סילוב): *תהי G חבורה סופית מסדר המתחלק במספר ראשוני p. תהי $H < G$ חבורת־p. אזי קימת חבורת p־סילוב ב G המכילה את H.*

יתר־על־כן, אם P היא חבורת p־סילוב של G, אז קים $x \in G$ כך ש $H < xPx^{-1}$.

הוכחה: נניח $|G| = p^r m$, באשר $p \nmid m$. תהי P חבורת p־סילוב של G. אזי $|P| = p^r$. נתבונן בקבוצה $T = \{xP \mid x \in G\}$ של המחלקות השמאליות של P בתוך G. שימו־לב ש $|T| = [G : P] = m$. נפעיל את H על T ע"י $h * xP = hxP \in T$ עבור $h \in H, xP \in T$. (קל לראות שזו אכן פעולה של H על T.) יהיו $H * x_1P, \ldots, H * x_kP$ המסלולים השונים. אזי $T = H * x_1P \dot\bigcup \ldots \dot\bigcup H * x_kP$ ולכן
$$m = |T| = \sum_{i=1}^{k} |H * x_iP| = \sum_{i=1}^{k} [H : \mathrm{Stb}(x_iP)].$$

כיון ש H היא חבורת־p, $[H : \mathrm{Stb}(x_iP)]$ היא חזקה של p לכל i. לא יתכן שבכל מסלול מספר האברים יהיה חזקה חיובית של p, כי אחרת ינבע $p|m$. לכן יש מסלול המכיל אבר אחד בלבד. כלומר קיים i כך ש $H * x_iP = \{x_iP\}$.
נסמן $x = x_i$. אזי $hxP = xP$ לכל $h \in H$. לכן $hx = hx \cdot 1 \in hxP = xP$ ולכן $h \in xPx^{-1}$ לכל $h \in H$. מכאן $H < xPx^{-1}$ (שימו־לב ש xPx^{-1} היא אכן חבורה). אולם $|xPx^{-1}| = |P| = p^r$ ולכן גם xPx^{-1} היא חבורת p־סילוב של G. ∎

הגדרה: תהי G חבורה. $A, B < G$ נקראות **צמודות** אם קים $x \in G$ כך ש $B = xAx^{-1}$.

מסקנה: *כל שתי חבורות p־סילוב צמודות.*

הוכחה: יהיו P_1, P_2 שתי חבורות p־סילוב של חבורה G. אזי, על פי משפט 2 עם P_1 במקום P ו P_2 במקום H, קים $x \in G$ כך ש $P_2 < xP_1x^{-1}$. אולם $|P_2| = p^r = |P_1| = |xP_1x^{-1}|$, באשר r הוא המספר הטבעי המרבי כך ש $p^r \big| |G|$. לכן $P_2 = xP_1x^{-1}$. כלומר P_1, P_2 צמודות. ∎

מסקנה: *תהי G חבורה סופית מסדר המתחלק במספר ראשוני p ותהי P חבורת p־סילוב ב G. אזי P היא חבורת p־סילוב יחידה ב G אם"ם $P \lhd G$.*

בפרט, אם G קומוטטיבית, אז יש ב G רק חבורת p־סילוב אחת.

הוכחה: אם P היא חבורת p־סילוב יחידה ב G, אז $P = aPa^{-1}$ לכל $a \in G$ (כי גם aPa^{-1} היא חבורת p־סילוב); כלומר $P \lhd G$.

להיפך, נניח $P \lhd G$ ותהי P' חבורת p־סילוב ב G. על סמך משפט 2 קים $a \in G$ כך ש $P' = aPa^{-1}$. אבל $P \lhd G$ ולכן $P' = aPa^{-1} = P$. כלומר P היא חבורת p־סילוב יחידה ב G.

אם G קומוטטיבית, אז $P \lhd G$ ומהפסקה השניה נובע ש P היא חבורת p־סילוב יחידה ב G. ∎

מהו מספר חבורות p־סילוב ? מתוך המסקנה של משפט 2, כל שתי חבורות p־סילוב צמודות ולכן אם P חבורת p־סילוב, אז מספר חבורות p־סילוב שוה למספר החבורות החלקיות הצמודות ל P. באפן כללי יותר: אם $K < G$, מהו מספר החבורות החלקיות של G הצמודות ל K ? זכרו ש $N(K) = \{x \in G \mid xK = Kx\}$ היא חבורה חלקית של G (שאלה 37 (א)).

טענה: *יהיו $K < G$. אזי מספר החבורות החלקיות של G הצמודות ל K הוא $[G : N(K)]$.*

הוכחה: נתבונן בקבוצת כל החבורות החלקיות של G ונפעיל על קבוצה זו את G באמצעות הצמדה: $x * A = xAx^{-1} < G$ עבור $x \in G, A < G$. מספר החבורות החלקיות של G הצמודות ל K הוא מספר האברים במסלול של K, כלומר $|\{xKx^{-1} \mid x \in G\}| = |G * K| = [G : \mathrm{Stb}(K)]$, באשר

$$\mathrm{Stb}(K) = \{x \in G \mid xKx^{-1} = K\} = \{x \in G \mid xK = Kx\} = N(K)\,.$$

לכן מספר החבורות החלקיות הצמודות ל K הוא $[G:N(K)]$. ∎

מסקנה: *תהי G חבורה סופית מסדר המתחלק במספר ראשוני p ותהי P חבורת p־סילוב של G. אזי מספר חבורות ה p־סילוב של G הוא $[G:N(P)]$.*

משפט 3 (כמות של תת־חבורות סילוב): *תהי G חבורה סופית מסדר המתחלק במספר ראשוני p. אזי מספר חבורות p־סילוב ב G הוא מהצורה $1+kp$.*

הוכחה: יהי r המספר הטבעי המרבי כך ש $p^r||G|$ ותהי P חבורת p־סילוב של G. אזי $|P|=p^r$. תהי $(P=)P_1,P_2,\dots,P_t$ רשימת כל חבורות p־סילוב ב G. נפעיל את P על $\{P_1,\dots,P_t\}$ ע"י הצמדה: $a*P_i=aP_ia^{-1}\in\{P_1,\dots,P_t\}$ עבור $a\in P$. מספר האברים במסלול $P*P_i=\{aP_ia^{-1}\mid a\in P\}$ הוא $[P:\mathrm{Stb}(P_i)]$ ולכן הוא מחלק את $|P|=p^r$. מכאן, מסלול שמספר אבריו $\neq 1$, מספר אבריו הוא חזקה חיובית של p. אנו נוכיח שרק מסלול אחד, מספר אבריו $=1$. זה יוכיח את טענת המשפט.

אכן, המסלול של P_1 מכיל את P_1 בלבד:

$$P*P_1=\{aP_1a^{-1}\mid a\in P\}=\{aPa^{-1}\mid a\in P\}=\{P\}=\{P_1\}.$$

להיפך, נניח שהמסלול של P_i מכיל את P_i בלבד ונוכיח ש $P_i=P$. אכן, נניח $aP_ia^{-1}=P_i$ לכל $a\in P$. אזי $aP_i=P_ia$ לכל $a\in P$ ולכן $PP_i=P_iP$. מכאן $P_iP<G$ (שאלה 31 (ד)). בנוסף, מההנחה ש $aP_ia^{-1}=P_i$ לכל $a\in P$ נובע $P_i\lhd P_iP$ כי

$$baP_i(ba)^{-1}=b(aP_ia^{-1})b^{-1}=bP_ib^{-1}=P_i$$

עבור $b\in P_i, a\in P$. לכן, בעזרת משפט האיזומורפיזם ה II, $P_iP/P_i\cong P/(P\cap P_i)$. לכן מתקיים ש $[P:P\cap P_i]=|P/(P\cap P_i)|=|P_iP/P_i|$ הוא חזקה של p. כמו־כן, כיון ש P_i היא חבורת p־סילוב, $|P_i|=p^r$. מכאן $|P_iP|=|P_iP/P_i|\cdot|P_i|=(p\text{ חזקה של})\cdot p^r$. בהכרח $|P_iP|=p^r$ (על סמך מרביות r כך ש $p^r||G|$). אולם $P_i,P<P_iP$ וכולם מסדר p^r. לכן $P_i=P_iP=P$. ∎

מסקנה: *תהי G חבורה מסדר n ויהי p מספר ראשוני המחלק את n. נניח $n=p^rm$ ו $p\nmid m$. אם מספר חבורות p־סילוב ב G הוא $1+kp$, אז $1+kp|m$.*

הוכחה: כמסקנה ממשפט 1, קימת $P<G$ כך ש $|P|=p^r$. כמסקנה ממשפט 2, מספר חבורות p־סילוב הוא $[G:N(P)]$, באשר $N(P)=\{a\in G\mid aP=Pa\}$. לבסוף, על סמך משפט 3, $[G:N(P)]=1+kp$ עבור מספר שלם אי־שלילי k מסוים.

שימו־לב כי $[G:P]=\frac{|G|}{|P|}=\frac{n}{p^r}=m$. לכן, כיון ש $P<N(P)<G$,

$$m=[G:P]=[G:N(P)][N(P):P]$$

ומכאן $1+kp=[G:N(P)]|m$. ∎

דֻגמה 1: תהי G חבורה מסדר $20 = 5 \cdot 4$. מספר חבורות 5־סילוב הוא מהצורה $1 + 5k$, באשר $1 + 5k|4$. מכאן $k = 0$ ולכן יש רק חבורת 5־סילוב אחת ב G והיא נורמלית ב G (על סמך אחת מהמסקנות של משפט 2).

דֻגמה 2: תהי G חבורה מסדר $99 = 3^2 \cdot 11$ ותהי H חבורה חלקית מסדר 11. מספר חבורות 11־סילוב הוא מהצורה $1 + 11k$, באשר $1 + 11k|9$. לכן $k = 0$ ולכן H היא חבורת 11־סילוב יחידה ב G. מכאן $H \lhd G$.

תהי K חבורת 3־סילוב ב G, כלומר $|K| = 3^2$. אם $1 + 3k|11$, אז $k = 0$. לכן $K \lhd G$.

דֻגמה 3: תהי G חבורה מסדר $175 = 5^2 \cdot 7$ ותהי H חבורה חלקית מסדר 5^2. כיון ש $1 + 5k|7 \Leftarrow k = 0$, $H \lhd G$.

דֻגמה 4: תהי G חבורה מסדר $30 = 2 \cdot 3 \cdot 5$, תהי H חבורה חלקית מסדר 5 ותהי K חבורה חלקית מסדר 3. נניח יש ב G $1 + 5k$ חבורות 5־סילוב ו $1 + 3k'$ חבורות 3־סילוב. אזי $1 + 5k|6$ ולכן $k = 0$ או $k = 1$ ו $1 + 3k'|10$ ולכן $k' = 0$ או $k' = 3$.

נניח בשלילה ש $H \not\lhd G$ וגם $K \not\lhd G$. אזי יש ב G 6 חבורות חלקיות $H = H_1, H_2, \ldots, H_6$ מסדר 5 ו 10 חבורות חלקיות $K = K_1, K_2, \ldots, K_{10}$ מסדר 3.

חבורות חלקיות שונות מסדר ראשוני נחתכות באבר היחידה בלבד (חתוך של שתי חבורות חלקיות הוא חבורה חלקית ועל פי משפט לגרנג', הסדר של חבורת החתוך חיב לחלק את הסדר של כל אחת מהחבורות החלקיות האלו). לדֻגמה, $|H_2| = 5 = |H_1|$. אם $|H_1 \cap H_2| = 5$, אז $H_1 = H_1 \cap H_2 = H_2$, בסתירה לכך ש $H_1 \neq H_2$.

לכן יש ב G, פרט לאבר היחידה, $(5-1) \cdot 6 = 24$ אברים מסדר 5 ו $(3-1) \cdot 10 = 20$ אברים מסדר 3. מכאן יוצא שב G יש לפחות $1 + 24 + 20 = 45$ אברים, בסתירה לכך ש G מכילה 30 אברים. מכאן נובע ש $H \lhd G$ או $K \lhd G$.

49. אם G חבורה סופית ו $K < G$ וכן H חבורת p־סילוב של K, אזי קימת חבורת p־סילוב P של G כך ש $H = P \cap K$.

50. (א) אם $H, K < G$ סופיות, אזי מספר אברי הקבוצה HK הוא $\frac{|H||K|}{|H \cap K|}$.
(רמז: עבור $h \in H$, $k \in K$ ו $a \in H \cap K$, רשמ/י $hk = (ha)(a^{-1}k)$.)
(ב) אם H, K חבורות־p וכן $HK = KH$, אזי HK חבורת־p ואם גם K חבורת p־סילוב, אזי $H < K$.
(ג) תהי P חבורת p־סילוב ב G. מתוך כך ש $P \lhd N(P)$, הוכח/י שאם H חבורת־p וכן $H < N(P)$, אזי $H < P$.

49. יהיו $H < K < G$, באשר G חבורה סופית ו H חבורת p־סילוב של K. נניח $|K| = p^t m$, באשר $p \nmid m$. אזי $|H| = p^t$. על פי משפט 2 של סילוב, קימת ב G חבורת p־סילוב P המכילה את H. לכן $H < P \cap K < K$. אזי $P \cap K$ היא חבורת־p, נניח $|P \cap K| = p^s$. כיון ש $H < P \cap K$, $p^t = |H| \leq |P \cap K| = p^s$ ולכן $t \leq s$. כמו־כן, כיון ש $P \cap K < K$, $p^s = |P \cap K| \big| |K| = p^t m$ ולכן $s \leq t$. מכאן $s = t$ ולכן $|P \cap K| = p^s = p^t = |H|$. לכן, כיון ש $H \subseteq P \cap K$, נובע $H = P \cap K$.

50. (א) יהיו $H, K < G$ חבורות סופיות. נגדיר העתקה

$$H \times K \to HK$$

ע"י

$$(h, k) \mapsto hk\,.$$

אזי לכל $g \in HK$ קימים בדיוק $|H \cap K|$ זוגות $(h, k) \in H \times K$ כך ש $hk = g$.

אכן, יהי $(h, k) \in H \times K$ כך ש $hk = g$. אזי, לכל $a \in H \cap K$, $(ha, a^{-1}k) \in H \times K$ מקיים $(ha)(a^{-1}k) = hk = g$. להיפך, אם $(h_1, k_1) \in H \times K$ מקיים $h_1 k_1 = g = hk$, אז $a := h^{-1}h_1 = kk_1^{-1} \in H \cap K$ ו $h_1 = ha$, $k_1 = a^{-1}k$.

מכאן $|HK| = \frac{|H \times K|}{|H \cap K|} = \frac{|H||K|}{|H \cap K|}$.

(ב) אם H, K חבורות־p ו $HK = KH$, אז HK חבורת־p. אכן, HK היא חבורה על פי תרגיל 31 (ד). נניח $|H| = p^r$, $|K| = p^s$ ו $|H \cap K| = p^t$ ($H \cap K < H, K$ ולכן גם היא חבורת־p). אזי, על פי חלק (א), $|HK| = \frac{|H||K|}{|H \cap K|} = \frac{p^r p^s}{p^t} = p^{r+s-t}$. כלומר HK היא חבורת־p.

אם K היא חבורת p־סילוב של G, אז $|G| = p^s m$, באשר $p \nmid m$. לכן, כיון ש $HK < G$ היא חבורת־p, $|HK| \leq p^s$. מצד שני, כיון ש $K < HK$, $|HK| \geq |K| = p^s$. מכאן $|HK| = p^s$ ולכן $K = HK$. מכאן $H < HK = K$.

(ג) תהי $P < G$ חבורת p־סילוב ותהי $H < N(P) = \{a \in G \mid aP = Pa\}$ חבורת־p. אזי $aP = Pa$ לכל $a \in H \subseteq N(P)$ ולכן $HP = PH$. מכאן, על פי סעיף (ב) עבור $K = P$, $H < P$.

דרך נוספת: $P \lhd N(P)$ (ראו תרגיל 37 (ב)), לכן P היא חבורת p־סילוב ב $N(P)$ נורמלית ולכן יחידה. עתה, $H < N(P)$ היא חבורת־p ועל פי משפט 2 של סילוב, H מוכלת בחבורת p־סילוב של $N(P)$. מכאן $H < P$.

חבורות מסדר קטן מ 60

משפט: *תהי G חבורה כך ש $1 < |G| < 60$ וכן G לא מסדר ראשוני. אזי G אינה פשוטה, כלומר קימת ל G חבורה חלקית ממש נורמלית לא טריביאלית.*

הוכחה: אם $|G| = p^k$, באשר p ראשוני ו $k > 1$, אז $Z(G) \neq \{1\}$ על פי משפט מסעיף 7. כמו־כן $Z(G) \triangleleft G$. לכן אם $Z(G) \neq G$, אז G אינה פשוטה. אם $Z(G) = G$, אז G קומוטטיבית וכל חבורה חלקית שלה היא נורמלית. כיון ש $k > 1$, קימת חבורה חלקית ממש לא טריביאלית ב G. לכן G אינה פשוטה גם במקרה זה. מכאן כל חבורה מסדר $4, 8, 16, 32, 9, 27, 25, 49$ אינה פשוטה.

ראינו בסעיף קודם שאם $n = |G| = p^r m$, באשר p הוא מספר ראשוני כך ש $p \nmid m$, $r \geq 1$, ו $m > 1$ ו $1 + kp|m \Leftarrow k = 0$, אז קימת חבורת p־סילוב יחידה ב G והיא נורמלית. לכן גם במקרה זה G אינה פשוטה. נציין זאת ע״י הסִמון $n(p)$. לדֻגמה, $6(3)$ מציין שאם G היא חבורה מסדר $6 = 3 \cdot 2$, אז G אינה פשוטה כי $1 + 3k|2$ $\Leftarrow k = 0$. נעבור עתה על כל המספרים n הגדולים מ 1 והקטנים מ 60 שהם לא מהצורה p^k, עבור p ראשוני, ונבדוק האם קים p ראשוני המחלק את n כך שמתקיים $n(p)$:

$6(3)$, $10(5)$, $12(?)$, $14(7)$, $15(5)$, $18(3)$, $20(5)$, $21(7)$, $22(11)$, $24(?)$, $26(13)$, $28(7)$, חבורה מסדר 30 אינה פשוטה על פי דֻגמה 4 מסעיף 8, $33(11)$, $34(17)$, $35(7)$, $36(?)$, $38(19)$, $39(13)$, $40(5)$, $42(7)$, $44(11)$, $45(5)$, $46(23)$, $48(?)$, $50(5)$, $51(17)$, $52(13)$, $54(3)$, $55(11)$, $56(?)$, $57(19)$, $58(29)$.

נשאר להראות שאם G חבורה מסדר $n \in \{12, 24, 36, 48, 56\}$, אז G אינה פשוטה.

$n = 12$: תהי H חבורת 2־סילוב של G, כלומר $|H| = 4$ ולכן $[G : H] = 3$. על פי משפט קיילי המוכלל (סעיף 7) קים הומומורפיזם $\varphi\colon G \to S_3$ כך ש $K = \ker(\varphi) \subseteq H$. אילו φ היתה חח״ע, אז $|G|\,|\,3!$. אולם $3! \nmid 12$ ולכן K היא חבורה חלקית נורמלית לא טריביאלית. כלומר G אינה פשוטה.

$n = 24$: תהי H חבורת 2־סילוב של G, כלומר $|H| = 8$ ולכן $[G : H] = 3$. כיון ש $3! \nmid 24$, G אינה פשוטה.

$n = 36$: תהי H חבורת 3־סילוב של G, כלומר $|H| = 9$ ולכן $[G : H] = 4$. כיון ש $4! \nmid 36$, G אינה פשוטה.

$n = 48$: תהי H חבורת 2־סילוב של G, כלומר $|H| = 16$ ולכן $[G : H] = 3$. כיון ש $3! \nmid 48$, G אינה פשוטה.

$n = 56$: $56 = 2^3 \cdot 7$. $1 + 7k|8 \Leftarrow k = 0$ או $k = 1$. אם $k = 0$, אז יש ב G חבורת 7־סילוב יחידה והיא נורמלית. אם $k = 1$, אז יש ב G 8 חבורות חלקיות שונות מסדר 7. כל אחת מכילה 6 אברים מסדר 7. סה״כ יש ב G $48 = 8 \cdot 6$ אברים מסדר 7. נשארו אם־כן ב G עוד $8 = 48 - 56$ אברים. תהי H חבורת 2־סילוב של G,

כלומר $|H| = 8$. הסדר של אבר ב H הוא חזקה של 2 ולכן H חיבת להיות מורכבת משמונת האברים שנותרו. מכאן H היא חבורת 2־סילוב יחידה ולכן נורמלית. כלומר G אינה פשוטה. ∎

פשטות A_5

אנו נראה שקימת חבורה פשוטה מסדר 60. החבורה A_5 היא מסדר $60 = \frac{120}{2} = \frac{5!}{2} = \frac{|S_5|}{2} = |A_5|$. אנו נראה כי A_5 היא חבורה פשוטה. ביתר כלליות: A_n היא פשוטה לכל $n \geq 5$.

משפט: *אם $n \geq 5$, אז החבורה A_n פשוטה.*

הוכחה: תהי $\{1\} \neq H \triangleleft A_n$ ונוכיח $H = A_n$.

ההוכחה מתחלקת לשני חלקים. בחלק (א) נראה שאם H מכילה מחזור מאורך 3, אז H מכילה כל מחזור מאורך 3 ובחלק (ב) נראה ש H מכילה מחזור מאורך 3. לכן, על פי חלק (א), H מכילה כל מחזור מאורך 3. על סמך תרגיל 20 מסעיף 3, A_n נוצרת ע"י כל המחזורים מאורך 3. מכאן ינבע $H = A_n$.

חלק (א): *אם H מכילה מחזור מאורך 3, אז H מכילה כל מחזור מאורך 3.* נניח $(a\,b\,c) \in H$. נקח $(a'\,b'\,c')$ כלשהוא ונוכיח $(a'\,b'\,c') \in H$. אנו נמצא $\gamma \in A_n$ כך ש $\gamma(a\,b\,c)\gamma^{-1} = (a'\,b'\,c')$ ואז התוצאה תנבע מכך ש $H \triangleleft A_n$.

כיון ש $n \geq 5$, קימים $d, e \neq a, b, c$. תהי

$$\gamma = \begin{pmatrix} a & b & c & d & e & \dots \\ a' & b' & c' & d' & e' & \dots \end{pmatrix}.$$

אזי $\gamma(a\,b\,c)\gamma^{-1} = (a'\,b'\,c')$. אם $\gamma \in A_n$, אז סימנו. אחרת γ תמורה אי־זוגית. במקרה זה נקח

$$\gamma' = (d'\,e')\gamma = \begin{pmatrix} a & b & c & d & e & \dots \\ a' & b' & c' & e' & d' & \dots \end{pmatrix}.$$

אזי γ' היא תמורה זוגית והיא מקימת $\gamma'(a\,b\,c)\gamma'^{-1} = (a'\,b'\,c')$.

חלק (ב): *H מכילה מחזור מאורך 3.* נוכיח זאת תחילה במקרה $n = 5$. תהי $\mathrm{id} \neq \sigma \in H$. אזי σ היא תמורה זוגית ולכן היא מהצורה $(a\,b\,c)$, $(a\,b)(c\,d)$ או $(a\,b\,c\,d\,e)$. לכן, אם σ אינה מחזור מאורך 3 קימים שני מקרים.

מקרה (1): *σ היא מהצורה $(a\,b)(c\,d)$.* נניח בלי הגבלת הכלליות ש $\sigma = (1\,2)(3\,4) \in H$. תהי

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix} = (3\,4\,5) \in A_5.$$

אזי, כיון ש $H \triangleleft A_n$, $H \ni \gamma\sigma\gamma^{-1} = (1\,2)(4\,5)$. לכן, כיון ש $\sigma^{-1} \in H$,

$$H \ni \gamma\sigma\gamma^{-1}\sigma^{-1} = (1\,2)(4\,5)(1\,2)(3\,4) = (4\,5)(3\,4) = (3\,5\,4).$$

כלומר, במקרה זה, ל H יש מחזור מאורך 3.

מקרה (2): *σ היא מהצורה $(a\,b\,c\,d\,e)$.* נניח בלי הגבלת הכלליות ש $H \ni (1\,2\,3\,4\,5) = \sigma$. תהי שוב $A_5 \ni (3\,4\,5) = \gamma$ כמו מקודם. אזי $H \ni \gamma\sigma\gamma^{-1} = (1\,2\,4\,5\,3)$ ומכאן

$$H \ni \gamma\sigma\gamma^{-1}\sigma^{-1} = (1\,2\,4\,5\,3)(5\,4\,3\,2\,1) = (1\,3\,4)\,.$$

כלומר גם במקרה זה ל H יש מחזור מאורך 3.

כמסקנה מחלקים (א) ו (ב) אנו מקבלים אם־כן ש A_5 פשוטה.

נוכיח כעת את חלק (ב) במקרה הכללי. נבחר $H \ni \sigma \neq \mathrm{id}$ כך שמספר ה j־ים אשר $\sigma(j) \neq j$ מזערי. נסמן מספר מזערי זה ב r. לא יתכן $r = 1$ (אם אבר אחד מוזז, אז בהכרח עוד אבר אחד מוזז) וגם לא יתכן $r = 2$ כי אז σ היא חִלוף ולכן אינה תמורה זוגית. מכאן $r \geq 3$. אם $r = 3$, אז σ היא מחזור מאורך 3 וסימנו. נניח $r \geq 4$ ונגיע לסתירה. בלי הגבלת הכלליות נוכל להניח ש $\sigma(j) \neq j$ עבור $j = 1, \ldots, r$.

אם $r = 4$, אז נתן להניח $\sigma = (1\,2)(3\,4)$. נקח, כמו במקרה $n = 5$, $\gamma = (3\,4\,5) \in A_n$. אזי $H \ni \gamma\sigma\gamma^{-1}\sigma^{-1} = (3\,5\,4)$, בסתירה לכך ש $r = 4$.

נניח עתה $r \geq 5$. קימים שני מקרים.

מקרה (1): *σ היא מכפלה של חִלופים זרים.* נניח בלי הגבלת הכלליות ש $\sigma = (1\,2)(3\,4)(5\,6)\cdots$. נקח שוב $\gamma = (3\,4\,5) \in A_n$. אזי $\gamma\sigma\gamma^{-1} = (1\,2)(4\,5)(3\,6)\cdots$ ומכאן

$$\gamma\sigma\gamma^{-1}\sigma^{-1} = (4\,5)(3\,6)\cdots(3\,4)(5\,6)\cdots.$$

אם $j > 5$, אז $\gamma(j) = j$ ולכן $\sigma(j) = j \Leftarrow \gamma\sigma\gamma^{-1}\sigma^{-1}(j) = j$. אזי $H \ni \gamma\sigma\gamma^{-1}\sigma^{-1}$ מזיזה פחות מ r אברים (כי 1 ו 2 לא מוזזים). כמו־כן $\sigma \neq \gamma\sigma\gamma^{-1}$ (למשל $\gamma\sigma\gamma^{-1}(4) = 5 \neq 3 = \sigma(4)$) ולכן $\gamma\sigma\gamma^{-1}\sigma^{-1} \neq \mathrm{id}$. קבלנו אם־כן סתירה למזעריות r.

מקרה (2): *קים בפרוק של σ למחזורים זרים לפחות מחזור אחד מאורך ≥ 3.* נניח בלי הגבלת הכלליות ש $\sigma = (1\,2\,3\,\ldots)\cdots$. בנוסף, מההנחה $r \geq 5$ נובע ש σ מזיזה לפחות עוד שני אברים, נניח 4 ו 5. אזי, עבור $\gamma = (3\,4\,5)$ אנו מקבלים $\gamma\sigma\gamma^{-1} = (1\,2\,4\,\ldots)\cdots$. מכאן $H \ni \gamma\sigma\gamma^{-1}\sigma^{-1}$ מזיזה פחות מ r אברים כי למשל 2 אינו מוזז: $\gamma\sigma\gamma^{-1}\sigma^{-1}(2) = \gamma\sigma\gamma^{-1}(1) = 2$. (שימו־לב, כמו במקרה הקודם, שאם $j > 5$, אז $\sigma(j) = j \Leftarrow \gamma\sigma\gamma^{-1}\sigma^{-1}(j) = j$.) כמו־כן $\sigma \neq \gamma\sigma\gamma^{-1}$ ולכן $\gamma\sigma\gamma^{-1}\sigma^{-1} \neq \mathrm{id}$. קבלנו סתירה למזעריות r. ∎

החבורה A_5

$|A_5| = 60 = 5 \cdot 3 \cdot 2^2$.

האברים מסדר 5 ב A_5 הם מהצורה $(a\,b\,c\,d\,e)$ ולכן מספרם הוא $24 = \frac{5\cdot4\cdot3\cdot2\cdot1}{5}$. מספר חבורות 5־סילוב הוא $1+5k$, באשר $1+5k|12$. לכן $k=1$ ויש ב A_5 6 חבורות 5־סילוב. (לא יתכן שיש ב A_5 חבורת 5־סילוב יחידה ולכן $k \neq 0$.) מכאן מספר האברים מסדר 5 הוא אכן $24 = (5-1)\cdot 6$.

האברים מסדר 3 צורתם $(a\,b\,c)$ ולכן מספרם $20 = \frac{5\cdot4\cdot3}{3}$. מספר חבורות 3־סילוב הוא $1+3k_1$, באשר $1+3k_1|20$. לכן $k_1=1$ או $k_1=3$ ($k_1 \neq 0$, אחרת יש ב A_5 רק חבורת 3־סילוב אחת). בהכרח $k_1=3$ ויש 10 חבורות 3־סילוב ב A_5, כי רק אז מספר האברים מסדר 3 הוא $20 = (3-1)\cdot 10$.

צורת האברים מסדר 2 היא $(a\,b)(c\,d)$ ומספרם $15 = \frac{3\cdot2}{2}\cdot\frac{5\cdot4}{2}\cdot\frac{1}{2}$. אין ב A_5 אברים מסדר 4, למרות ש $4|60$, כי תמורה מהצורה $(a\,b\,c\,d)$ היא אי־זוגית.

סך הכל יש ב A_5: 1 אבר יחידה + 24 אברים מסדר 5 + 20 אברים מסדר 3 + 15 אברים מסדר 2 = 60 אברים.

חבורת 2־סילוב ב A_5 מכילה 4 אברים, 3 מהם מסדר 2. מספר חבורות 2־סילוב הוא מהצורה $1+2k_2$, באשר $1+2k_2|15$. אזי $k_2=1$ או $k_2=2$. (כיון שיש ב A_5 בדיוק 15 אברים מסדר 2, לא יתכן שיש ל A_5 חבורת 2־סילוב אחת או 15 חבורות 2־סילוב ולכן לא יתכן $k_2=0$ ו $k_2=7$.) אם $k_2=1$, אז יש ב A_5 3 חבורות חלקיות מסדר 4 ולכל לכל היותר $9 = (4-1)\cdot 3$ אברים מסדר 2, אולם יש ל A_5 15 אברים מסדר 2. לכן $k_2=2$ ויש ב A_5 5 חבורות 2־סילוב. דֻגמה לחבורת 2־סילוב אחת כזו היא:

$$\{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}\,.$$

חבורות מסדר 6

חבורה מסדר ראשוני p היא ציקלית ואיזומורפית ל $\mathbb{Z}_p$. בתרגיל 16 ראינו כי כל חבורה בת 4 אברים איזומורפית ל $\mathbb{Z}_4 \cong U(5)$ או ל $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong U(8)$. חבורה קומוטטיבית מסדר 6 איזומורפית ל $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$. החבורה $S_3 \cong D_3$ (ראו סעיף 5) היא מסדר 6 ואינה קומוטטיבית.

טענה: *יש רק חבורה אחת (עד כדי איזומורפיזם) מסדר 6 שהיא אינה קומוטטיבית.*

הוכחה: תהי G חבורה לא קומוטטיבית מסדר $6 = 3\cdot 2$. אזי, על פי משפט קושי, קימים ב G אבר a מסדר 3 ואבר b מסדר 2. אזי $ab \neq ba$, אחרת ab הוא אבר מסדר 6 (כי $|a|=3$, $|b|=2$ ו $(2,3)=1$) ואז G היא ציקלית ובפרט קומוטטיבית.

אזי $1, a, a^2, b, ba, ba^2$ הם אברים שונים ב G. לדֻגמה, $ba \neq 1 \Leftarrow ba^2 \neq a$. כמו־כן, ab שונה מ $1, a, a^2, b, ba$ (למשל $ab \neq 1$ כי $b\cdot b = 1$) ולכן $ab = ba^2$. מכאן $G = \{1, a, a^2, b, ba, ba^2\}$, באשר $a^3=1$, $b^2=1$ ו $ab = ba^2$ ויש רק דרך אחת למלא את לוח הכפל ב G:

$(G,\cdot)$	1	a	a^2	b	ba	ba^2
1	1	a	a^2	b	ba	ba^2
a	a	a^2	1	ba^2	b	ba
a^2	a^2	1	a	ba	ba^2	b
b	b	ba	ba^2	1	a	a^2
ba	ba	ba^2	b	a^2	1	a
ba^2	ba^2	b	ba	a	a^2	1

לדֻגמה, $ba = ba^4 = ba^2 \cdot a^2 = aba^2 = a(ab) = a^2 \cdot b$ ו $ba^2 \cdot b = abb = a$. ∎

דֻגמה: החבורה $\mathrm{GL}(2,\mathbb{Z}_2)$ של כל המטריצות 2×2 ההפיכות מעל השדה $\mathbb{Z}_2$ היא מסדר 6 כי

$$\mathrm{GL}(2,\mathbb{Z}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}$$

והיא אינה קומוטטיבית כי $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ ו $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ מקימות $AB = BA^2 \neq BA$. לכן, על פי הטענה, $S_3 \cong GL(2,\mathbb{Z}_2)$. שימו־לב כי $\mathrm{GL}(2,\mathbb{Z}_2) = \langle A, B \mid A^3 = I, B^2 = I, AB = BA^2 \rangle$. כמו־כן $S_3 = \langle \sigma, \tau \mid \sigma^3 = \mathrm{id}, \tau^2 = \mathrm{id}, \sigma\tau = \tau\sigma^2 \rangle$, באשר $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ ו $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. מכאן $S_3 \cong \mathrm{GL}(2,\mathbb{Z}_2)$ ע״י $A \leftrightarrow \sigma$ ו $B \leftrightarrow \tau$.

חבורות מסדר 8

החבורות הקומוטטיביות הבלתי איזומורפיות מסדר 8 הן, על פי משפט המיון של חבורות קומוטטיביות (סעיף 6), $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ ו $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. כמו־כן החבורה הדיהדרית $D_4 = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$ המוגדרת ע״י $a^4 = b^2 = 1$ ו $ab = ba^3$ (ראו סעיף 5) היא חבורה לא קומוטטיבית מסדר 8. ישנה עוד חבורה אחת לא קומוטטיבית מסדר 8.

הגדרה: **חבורת הקווטרניוניים** Q היא החבורה הנוצרת ע״י שני אברים a ו b המקימים את היחסים $a^4 = b^4 = 1$, $a^2 = b^2$ ו $bab^{-1} = a^3$. אזי $Q = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$ היא חבורה לא קומוטטיבית מסדר 8. (קל לבנות את טבלת הכפל של Q בעזרת יחסים אלו ועל ידי כך להראות ש Q היא אכן חבורה.)

טענה: *אם בחבורה G כל אבר פרט ליחידה הוא מסדר 2, אז G קומוטטיבית.*

הוכחה: מהנתון, $c = c^{-1}$ לכל $c \in G$. לכן, לכל $a, b \in G$ מתקיים $ab = a^{-1}b^{-1} = (ba)^{-1} = ba$. כלומר G קומוטטיבית. ∎

טענה: *כל חבורה מסדר 8 איזומורפית לאחת החבורות (הבלתי־איזומורפיות) הבאות:* $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, D_4 או Q.

הוכחה: תהי G חבורה לא קומוטטיבית מסדר 8. אם קיים ב G אבר מסדר 8, אז G ציקלית ולכן קומוטטיבית. אם כל אבר ב G פרט ליחידה הוא מסדר 2, אז G קומוטטיבית על פי הטענה הקודמת. לכן יש ב G אבר a מסדר 4. תהי $H = \langle a \rangle$. אזי $[G:H] = 2$ ולכן $H \lhd G$ (ראו סעיף 5). יהי b אבר כלשהוא ב $G \setminus H$. אזי $bab^{-1} \in H$. אבל $|bab^{-1}| = |a|$ ולכן $bab^{-1} \in \{a, a^3\}$. תהי $K = \langle b \rangle$. אזי, כיון ש $H \lhd G$, $HK < G$. אולם $H \cup K \subseteq HK$ ולכן $|HK| > 4$. כמו־כן, על פי משפט לגרנג', $|HK| \, \big| \, |G| = 8$. לכן $|HK| = 8$ ומכאן $HK = G$. כיון ש G אינה קומוטטיבית, $bab^{-1} \neq a$ ולכן $bab^{-1} = a^3$. בנוסף, הסדר של b הוא 2 או 4. אם $|b| = 2$, אז $b^2 = 1$ ולכן $G = \langle a, b \mid a^4 = 1, b^2 = 1, ab = ba^3 \rangle \cong D_4$. אם $|b| = 4$, אז $|H| = |K| = 4$. לכן, על פי תרגיל 50 (א), $|H \cap K| = \frac{|H||K|}{|HK|} = \frac{4 \cdot 4}{8} = 2$. מכאן $\{1, a^2\} = H \cap K = \{1, b^2\}$ ולכן $a^2 = b^2$. במקרה זה, אם־כן, $G = \langle a, b \mid a^4 = b^4 = 1, a^2 = b^2, bab^{-1} = a^3 \rangle \cong Q$. ∎

חבורות מסדר 9

על פי מסקנה מסעיף 7, אם p הוא מספר ראשוני, אז כל חבורה מסדר p^2 היא קומוטטיבית. מכאן, כל חבורה מסדר $3^2 = 9$ היא קומוטטיבית ועל פי משפט המיון של חבורות קומוטטיביות היא איזומורפית ל $\mathbb{Z}_9$ או ל $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.

חבורות מסדר 10

טענה: *תהי G חבורה מסדר $2p$, באשר p מספר ראשוני אי־זוגי. אזי* $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_p \cong \mathbb{Z}_{2p}$ *או* $G \cong D_p$.

הוכחה: בעזרת משפט קושי (סעיף 7) קימים ב G אבר a מסדר p ואבר b מסדר 2. יהיו $H = \langle a \rangle$ ו $K = \langle b \rangle$. אזי $H \lhd G$ כיון ש $[G:H] = 2$. כמו־כן, $H \cap K = \{1\}$ כיון ש $(2,p) = 1$. לכן $G = \{1, a, \ldots, a^{p-1}, b, ba, \ldots, ba^{p-1}\}$. מצד שני, a, b מקימים את היחסים $a^p = 1$, $b^2 = 1$ ו $bab^{-1} = a^r$ עבור r מתאים בין 1 ל $p-1$ (כי $H \lhd G$), כלומר $ab = ba^r$. יחסים אלו קובעים את טבלת הכפל של G ולכן מגדירים את החבורה G עד כדי איזומורפיזם. כיון ש $b^2 = 1$,

$$a = b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$$

ומכאן $a^{r^2-1} = 1$. לכן $p = |a| \, \big| \, r^2 - 1 = (r-1)(r+1)$ (ראו גם תרגילים 45 ו 46). כיון ש p ראשוני, $p | r+1$ או $p | r-1$ ולכן $r \equiv \pm 1 \pmod p$. אולם $1 \leq r \leq p-1$ ולכן $r = 1$ או $r = p-1$. אם $r = 1$, אז $ab = ba$ ולכן G קומוטטיבית. במקרה זה $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_p \cong \mathbb{Z}_{2p}$. אם $r = p-1$, אז $G = \langle a, b \mid a^p = 1, b^2 = 1, ab = ba^{p-1} \rangle \cong D_p$. ∎

בפרט, חבורה מסדר $10 = 2 \cdot 5$ איזומורפית ל $\mathbb{Z}_{10} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_5$ או ל D_5.

טענה: *כל חבורה מסדר 12 איזומורפית לאחת מחמש החבורות הבאות:*

$\mathbb{Z}_{12} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3$, $\mathbb{Z}_2 \oplus \mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$, D_6, A_4 או

$$\langle b, c \mid b^4 = c^6 = 1, b^2 = c^3, bc = c^5 b\rangle = \{1, c, c^2, c^3, c^4, c^5, b, cb, c^2b, c^3b, c^4b, c^5b\}.$$

הוכחה: תהי G חבורה מסדר $12 = 2^2 \cdot 3$. מספר חבורות 2־סילוב ב G הוא $m_2 = 1 + 2k$, באשר $m_2|3$. לכן $m_2 = 1$ או $m_2 = 3$. מספר חבורות 3־סילוב ב G הוא $m_3 = 1 + 3k'$, באשר $m_3|4$. לכן $m_3 = 1$ או $m_3 = 4$. קיימים שלשה מקרים.

מקרה (א): $m_2 = 1$ ו $m_3 = 1$. במקרה זה קימות ל G חבורה חלקית H נורמלית מסדר 4 וחבורה חלקית נורמלית K מסדר 3. אזי $HK < G$ וכיון ש $|HK|\,|H| = 4$ וגם $|HK|\,|K| = 3$, $|HK| = 12$ ומכאן $G = HK$. על פי תרגיל 40, $G \cong H \times K$. מכאן, כיון ש H, K הן חבורות קומוטטיביות, גם G היא קומוטטיבית. לכן, על פי משפט המיון של חבורות קומוטטיביות, $G \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$ או $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$.

מקרה (ב): $m_2 = 1$ ו $m_3 \neq 1$. במקרה זה G אינה קומוטטיבית כי חבורת 3־סילוב של G אינה נורמלית. כמו־כן קימת ל G חבורת 2־סילוב יחידה H והיא נורמלית ב G. יהי a אבר מסדר 3 ב G ותהי $K = \langle a \rangle$. כיון ש $H \lhd G$, $HK < G$ וכמו במקרה (א) נובע $G = HK$.

נניח בשלילה ש H ציקלית. אזי קים ב H אבר b מסדר 4. כיון ש $H \lhd G$, $aba^{-1} \in H$. לכן, כיון ש $|aba^{-1}| = |b|$, $aba^{-1} \in \{b, b^3\}$. אולם G אינה קומוטטיבית ולכן $aba^{-1} \neq b$. מכאן $aba^{-1} = b^3 = b^{-1}$. אבל אז, כיון ש $a^3 = 1$,

$$b = a^3ba^{-3} = a^2b^{-1}a^{-2} = (a^2ba^{-2})^{-1} = (ab^{-1}a^{-1})^{-1} = aba^{-1} = b^{-1},$$

בסתירה לכך ש b הוא אבר מסדר 4.

לכן $H = \{1, b_1, b_2, b_3\}$, באשר b_1, b_2, b_3 הם אברים מסדר 2. כיון ש $H \lhd G$, $ab_ia^{-1} \in \{b_1, b_2, b_3\}$ עבור $i = 1, 2, 3$. לא יתכן $ab_ia^{-1} = b_i$, $i = 1, 2, 3$, אחרת $G = HK$ קומוטטיבית. נניח, בלי הגבלת הכלליות, $ab_1a^{-1} = b_2$. אזי $ab_2a^{-1} \neq ab_1a^{-1} = b_2$. כמו־כן, כיון ש $a^3 = 1$,

$$b_1 = a^3b_1a^{-3} = a^2(ab_1a^{-1})a^{-2} = a^2b_2a^{-2} = a(ab_2a^{-1})a^{-1}$$

ולכן $ab_2a^{-1} \neq b_1$ (כי $b_1 \neq b_2 = ab_1a^{-1}$). מכאן $ab_2a^{-1} = b_3$ ו $ab_3a^{-1} = a(ab_2a^{-1})a^{-1} = b_1$. היחסים $a^3 = 1$, $b_1^2 = b_2^2 = b_3^2 = 1$, $b_1b_2 = b_3 = b_2b_1$, $ab_1 = b_2a$, $ab_2 = b_3a$ ו $ab_3 = b_1a$ קובעים באפן יחיד את G עד כדי איזומורפיזם.

בחבורה A_4 יש 3 אברים מסדר 2 ו 8 אברים מסדר 3 (ראו סוף סעיף 3). לכן בהכרח יש לה חבורת 2־סילוב אחת ו 4 חבורות 3־סילוב כמו במקרה (ב). לכן במקרה זה $G \cong A_4$.

מקרה (ג): $m_2 \neq 1$. הערה: במקרה זה $m_3 = 1$. אכן, אם $m_3 = 4$, אז יש ב G $8 = (3-1) \cdot 4$ אברים מסדר 3 ובהכרח ארבעת האברים שנותרו מהוים חבורת 2־סילוב יחידה, בסתירה לכך ש $m_2 \neq 1$.

תהי H חבורת 2־סילוב של G. אזי $[G:H] = 3$ ולכן, על פי משפט קיילי המוכלל, קים הומומורפיזם $\varphi\colon G \to S_3$ כך ש $\ker(\varphi) \subseteq H$. אבל $|G| = 12 \nmid 3!$ ולכן $\ker(\varphi) \neq \{1\}$. כמו־כן $H \ntriangleleft G$ (כי $m_2 \neq 1$) ולכן $\ker(\varphi) = \{1, z\}$ היא חבורה חלקית נורמלית של G מסדר 2. לכן $gzg^{-1} = z$ לכל $g \in G$ ומכאן $z \in Z(G)$.

יהי a אבר מסדר 3 ב G ויהי $c = az$. אזי, כיון ש $az = za$, $|a| = 3$, $|z| = 2$ ו $(2,3) = 1$, c הוא אבר מסדר 6. תהי $K = \langle c \rangle$. אזי, כיון ש $[G:K] = 2$, $K \triangleleft G$.

כיון ש $|K| = 6 \nmid 4 = |H|$, $H \not\subseteq K$. יהי $b \in H \setminus K$. אזי

$$G = \{1, c, c^2, c^3, c^4, c^5, b, cb, c^2b, c^3b, c^4b, c^5b\} = HK.$$

כיון ש $K \triangleleft G$, $bcb^{-1} \in K$. לכן, כיון ש $|bcb^{-1}| = |c|$, $bcb^{-1} \in \{c, c^5\}$. אולם G אינה קומוטטיבית ולכן $bcb^{-1} \neq c$. מכאן $bcb^{-1} = c^5$.

עתה, הסדר של b הוא 2 או 4.

אם $|b| = 2$, אז $G = \langle b, c \mid b^2 = c^6 = 1, bc = c^5b \rangle \cong D_6$.

אם $|b| = 4$, אז $H = \langle b \rangle$. על פי תרגיל 50 (א), $|H \cap K| = \frac{|H||K|}{|HK|} = \frac{4 \cdot 6}{12} = 2$. לכן $\{1, c^3\} = H \cap K = \{1, b^2\}$ ומכאן $b^2 = c^3$. טבלת הכפל של G נקבעת אם־כן באפן יחיד ע״י היחסים: $b^4 = 1$, $c^6 = 1$, $b^2 = c^3$ ו $bc = c^5b$. ∎

הערה: החבורה $\mathbb{Z}_2 \times S_3$ היא מסדר $12 = 2 \cdot 3!$ והיא איזומורפית ל D_6.

טענה: *אין ל A_4 חבורה חלקית מסדר 6.*

הוכחה: ראינו בסעיף זה שחבורה מסדר 6 איזומורפית לחבורה הציקלית $\mathbb{Z}_6$ או לחבורה

$$D_3 \cong \langle a, b \mid a^3 = b^2 = 1, ab = ba^2 \rangle = \{1, a, a^2, b, ba, ba^2\}.$$

אולם ב A_4 אין אבר מסדר 6 ולכן $A_4 \not\hookleftarrow \mathbb{Z}_6$. כמו־כן, ב D_3 שלשת השקופים (האברים מסדר 2), b, ba, ba^2, לא מתחלפים. למשל $b(ba) = b^2a = a \neq a^2 = bba^2 = b(ab) = (ba)b$. לעומת זאת, ב A_4 יש רק שלשה אברים מסדר 2, $(1\,2)(3\,4)$, $(1\,3)(2\,4)$, $(1\,4)(2\,3)$, אבל הם מתחלפים ביניהם. לדֻגמה, $\big((1\,2)(3\,4)\big)\big((1\,3)(2\,4)\big) = (1\,4)(2\,3) = \big((1\,3)(2\,4)\big)\big((1\,2)(3\,4)\big)$. מכאן גם $A_4 \not\hookleftarrow D_3$. לכן אין ב A_4 חבורה חלקית מסדר 6. ∎

תרגילים לסעיף 9

51. אם p,q ראשוניים שונים ו G חבורה מסדר p^2q, הוכח/י כי: או שקימת חבורת p־סילוב נורמלית או שקימת חבורת q־סילוב נורמלית. (רמז: הבחן/י בין $p > q$ לבין $p < q$.)

52. אם $|G| = n$ ו n אינו ראשוני ומקים $60 < n \leq 70$, אז G אינה פשוטה.

53. העזר/י בתרגיל 24 והוכח/י שאם $H \triangleleft S_n$, $n \geq 5$, וכן $\{1\} \neq H \neq S_n$, אז $H = A_n$.

51. יהיו p, q ראשוניים שונים ותהי G חבורה מסדר p^2q. נבחין בין שני מקרים.

מקרה (א): $p > q$. $1 + kp | q \Leftarrow k = 0$. לכן ל G יש חבורת p־סילוב יחידה והיא נורמלית.

מקרה (ב): $p < q$. מספר חבורות q־סילוב הוא $1 + kq$, באשר $1 + kq | p^2$. המחלקים של p^2 הם $1, p, p^2$.

אם $1 + kq = 1$, אז קימת חבורת q־סילוב יחידה ולכן נורמלית.

לא יתכן $1 + kq = p$ כי $p < q$.

נניח $1 + kq = p^2$. תהי P חבורת p־סילוב ב G. אזי $|P| = p^2$. מצד שני, בחבורת q־סילוב של G יש q אברים. לכן מספר האברים בתוך כל חבורות ה q־סילוב של G פרט לאבר היחידה הוא $p^2 \cdot (q-1) = p^2q - p^2$. נותרו ב G אם־כן p^2 אברים והם בהכרח אברי P. טעון זה נכון עבור כל חבורת p־סילוב של G. מכאן P היא חבורת p־סילוב יחידה ולכן נורמלית.

52. תהי G חבורה מסדר n. ראינו שאם $n = p^k$, באשר p מספר ראשוני ו $k > 1$, אז G אינה פשוטה. לכן חבורה מסדר $2^6 = 64$ אינה פשוטה.

כמו־כן ראינו שאם $n = p^r m$, באשר p מספר ראשוני המחלק את n, $m > 1$ ו $p \nmid m$, אז מתוך $1 + kp | m$ $\Leftarrow$ $k = 0$ נובע ש G אינה פשוטה. נציין זאת ע"י $n(p)$. אם $60 < n \leq 70$, $n \neq 64$ ו n אינו ראשוני, אז קים ראשוני p המחלק את n כך שמתקיים $n(p)$ ולכן כל חבורה מסדר n אינה פשוטה. אכן,

$62(31)$, $63(7)$, $65(13)$, $66(11)$, $68(17)$, $69(23)$, $70(7)$.

53. תהי $H \triangleleft S_n$, $n \geq 5$, כך ש $\{1\} \neq H \neq S_n$. אם $H < A_n$, אז $H \triangleleft A_n$. לכן, כיון ש A_n פשוטה עבור $n \geq 5$, $H = A_n$.

נניח בשלילה ש $H \not< A_n$. אזי, על פי תרגיל 24, מספר התמורות הזוגיות ב H שוה למספר התמורות האי־זוגיות ב H. נתבונן בחבורה החלקית $H \cap A_n$ של כל התמורות הזוגיות ב H. מתקים $H \cap A_n \triangleleft A_n$. (באפן כללי: אם $H \triangleleft G$ ו $K < G$, אז $H \cap K \triangleleft K$. אכן, לכל $a \in K$ מתקים $aHa^{-1} \subseteq H$ ו $aKa^{-1} \subseteq K$ ומכאן $a(H \cap K)a^{-1} \subseteq H \cap K$.)

אזי, כיון ש A_n פשוטה עבור $n \geq 5$, $H \cap A_n = A_n$ או $H \cap A_n = \{1\}$.

אם $H \cap A_n = A_n$, אז $|H \cap A_n| = |A_n| = \frac{n!}{2}$ ולכן יש גם $\frac{n!}{2}$ תמורות אי־זוגיות ב H. סך הכל יש ב H אם־כן $n!$ אברים ולכן $H = S_n$, בסתירה לכך ש $H \neq S_n$.

אם $H \cap A_n = \{1\}$, אז $H = \{1, \sigma\}$, באשר σ היא תמורה אי־זוגית המקימת $\sigma^2 = 1$. כיון ש $H \triangleleft S_n$, $\tau\sigma\tau^{-1}$ הוא אבר מסדר 2 ב H לכל $\tau \in S_n$. לכן $\tau\sigma\tau^{-1} = \sigma$ ומכאן $\tau\sigma = \sigma\tau$ לכל $\tau \in S_n$. כלומר $\sigma \in Z(S_n)$.

טענה: $Z(S_n) = \{1\}$ עבור $n \geq 3$.

הוכחה: נניח בשלילה שקימת $\sigma \in Z(S_n)$ $\sigma \neq 1$. אזי, כיון ש $n \geq 3$, קימת תמורה $\sigma' \in S_n$, $\sigma \neq \sigma'$, מאותו טפוס של σ (ראו סעיף 7). למשל, אם $\sigma = (1\,2\,\ldots)(\ldots)\cdots(\ldots)$, נתן לקחת $\sigma' = (1\,3\,\ldots)(\ldots)\cdots(\ldots)$. כיון ששתי תמורות מאותו טפוס הן צמודות, קימת $\tau \in S_n$ כך ש $\sigma \neq \sigma' = \tau\sigma\tau^{-1}$. מכאן $\tau\sigma \neq \sigma\tau$, בסתירה לכך ש $\sigma \in Z(S_n)$. ∎

עתה $\sigma \in Z(S_n) = \{1\}$ ולכן $\sigma = 1$, בסתירה לכך ש σ הוא אבר מסדר 2.

(הערה: במקרה שלנו σ הוא אבר מסדר 2 ב S_n ולכן σ היא מכפלה של חִלופים זרים, נניח $\sigma = (a_1\,b_1)(a_2\,b_2)\cdots(a_k\,b_k)$. אזי קים $\tau \in S_n$ כך ש $\tau\sigma\tau^{-1} = (a_2\,b_1)(a_1\,b_2)\cdots(a_k\,b_k) \neq \sigma$.)

רשימת משפטים

סעיף 1: יסודות על חבורות.

1. *(א) כל חבורה ציקלית אינסופית איזומורפית ל $\mathbb{Z}$ ביחס לחבור.*

(ב) כל חבורה ציקלית סופית מסדר n איזומורפית ל $\mathbb{Z}_n$ ביחס לחבור.

סעיף 2: מושגים בסיסיים מתורת המספרים.

2. המשפט היסודי של האריתמטיקה: כל מספר טבעי $n > 1$ נתן לכתיבה בצורה אחת ויחידה כמכפלה $n = p_1 \cdot p_2 \cdots p_r$, באשר $p_1 \leq \ldots \leq p_r$ ראשוניים ו $r \geq 1$.

3. יהיו $a, b \in \mathbb{Z}$ לא שניהם אפס. אזי קיימים $u, v \in \mathbb{Z}$ כך ש $(a, b) = au + bv$.

4. תהי G חבורה ויהי $a \in G$ אבר מסדר n המקים גם $a^m = 1$. אזי $n|m$.

5. תהי G חבורה ויהיו a, b אברים ב G מסדרים r, s, בהתאמה, כך ש $ab = ba$ ו $(r, s) = 1$. אזי ab הוא אבר מסדר rs.

סעיף 3: חבורת תמורות.

6. תהי σ תמורה אשר בתור מכפלה של מחזורים זרים היא מהצורה

$$\sigma = (a_{1,1} \ldots a_{1,r_1})(a_{2,1} \ldots a_{2,r_2}) \cdots (a_{k,1} \ldots a_{k,r_k}).$$

אזי $|\sigma| = [r_1, r_2, \ldots, r_k]$.

7. נניח $\sigma \in S_n$ היא מכפלה של k מחזורים זרים. אזי σ היא זוגית, כלומר $n - k$ זוגי, אם"ם היא מכפלה של מספר זוגי של חִלופים.

סעיף 4: הומומורפיזמים.

8. אם $\varphi\colon H \to G$ הוא הומומורפיזם של חבורות, אז $\mathrm{Im}(\varphi) < G$ ו $\ker(\varphi) < H$.

סעיף 5: חבורת המנה.

9. משפט לגרנג': תהי G חבורה סופית ותהי $H < G$. אזי $|G| = [G : H] \cdot |H|$.

10. אם G חבורה סופית, אז $a^{|G|} = 1$ לכל $a \in G$.

11. (א) אם $G = \langle a \rangle$ ציקלית אינסופית, אזי עבור כל $m \geq 1$ טבעי קימת חבורה חלקית $\langle a^m \rangle$ ואלו כל החבורות החלקיות של G, פרט ל $\langle 1 \rangle = \{1\}$.

(ב) אם $G = \langle a \rangle$ היא ציקלית מסדר m, אזי עבור כל מספר טבעי q כך ש $q|m$ קימת חבורה חלקית אחת ורק אחת מסדר q והיא $\langle a^{\frac{m}{q}} \rangle$.

12. $G \triangleleft H$, כלומר $aH = Ha$ לכל $a \in G$, אם"ם $aha^{-1} \in H$ לכל $a \in G$.

13. יהיו $H \triangleleft G$.

(א) אם $H < K < G$, אזי $H \triangleleft K$ וכן $K/H < G/H$.

(ב) אם $L < G/H$, אזי קימת חבורה חלקית K, $H < K < G$, כך ש $L = K/H$.

14. יהיו $H < G$ כך ש $[G:H] = 2$. אזי $H \triangleleft G$.

15. **משפט האיזומורפיזם ה** I : אם $\varphi\colon G_1 \to G_2$ הומומורפיזם של חבורות, אז $\ker(\varphi) \triangleleft G_1$ ו $G_1/\ker(\varphi) \cong \operatorname{Im}(\varphi) < G_2$.

16. **משפט האיזומורפיזם ה** II: יהיו $H \triangleleft G$ ו $K < G$. אזי $KH < G$ ו $KH/H \cong K/K \cap H$.

17. יהי $\varphi\colon G_1 \to G_2$ הומומורפיזם בין חבורות.

(א) $\varphi(H_1) < G_2 \Leftarrow H_1 < G_1$.

(ב) $\ker\varphi < \varphi^{-1}(H_2) < G_1 \Leftarrow H_2 < G_2$.

18. יהי $\varphi\colon G_1 \to G_2$ הומומורפיזם על בין חבורות.

(א) ההתאמה בין הקבוצות $\{H_1 \mid \ker\varphi < H_1 < G_1\} \to \{H_2 \mid H_2 < G_2\}$

הנתנת ע"י $H_1 \mapsto \varphi(H_1)$

היא חח"ע ועל. ההתאמה ההפוכה נתנת ע"י $\varphi^{-1}(H_2) \leftarrow H_2$.

(ב) בהתאמה הקודמת, $H_1 \triangleleft G_1 \Leftrightarrow \varphi(H_1) \triangleleft G_2$.

(ג) אם קורה (ב), אז $G_1/H_1 \cong G_2/\varphi(H_1)$ (או, לחלופין, $G_1/\varphi^{-1}(H_2) \cong G_2/H_2$).

19. **משפט האיזומורפיזם ה** III: אם $H \triangleleft G$ ו $K \triangleleft G$, $H < K$, אז $G/K \cong (G/H)/(K/H)$.

סעיף 6: חבורות אבליות.

20. המכפלה הישרה של חבורות ציקליות מסדרים זרים היא חבורה ציקלית.

21. אם G קומוטטיבית סופית, אז G היא המכפלה הישרה של חבורות הסילוב שלה.

22. תהי P חבורה קומוטטיבית מסדר p^r, p ראשוני. אזי P היא מכפלה ישרה של חבורות ציקליות מסדרים $p^{s_1}, \ldots, p^{s_k}$ והמספרים $k, s_1, \ldots, s_k$ נקבעים באפן יחיד.

מספר החבורות הקומוטטיביות הבלתי איזומורפיות מסדר p^r הוא $\wp(r)$, באשר $\wp(r)$ הוא מספר הסדרות $s_1, \ldots, s_k$ כך ש $s_1 + \ldots + s_k = r$ ו $s_1 \geq \ldots \geq s_k$.

23. **משפט המיון של חבורות קומוטטיביות סופיות:** כל חבורה קומוטטיבית סופית איזומורפית לחבורה אחת ורק אחת מהצורה

$$\bigoplus_{i,j} \mathbb{Z}_{p_i^{s_{i,j}}} = \bigoplus_i \Big(\bigoplus_j \mathbb{Z}_{p_i^{s_{i,j}}}\Big) .$$

הקבוצה $\{p_i^{s_{i,j}}\}$ נקבעת באפן יחיד.

אם $n = p_1^{r_1} p_2^{r_2} \cdots p_l^{r_l}$, באשר $p_1, \ldots, p_l$ מספרים ראשוניים שונים, אז מספר החבורות הקומוטטיביות הבלתי איזומורפיות מסדר n הוא $\wp(r_1)\,\wp(r_2)\cdots\wp(r_l)$.

סעיף 7: פעולות של חבורות על קבוצות.

24. משפט קיילי המוכלל: יהיו $H < G$ כך ש $[G:H] = m$. אזי קים הומומורפיזם $\varphi\colon G \to S_m$ כך ש $\ker(\varphi) \subseteq H$. בפרט, אם $|G| \nmid m!$, אז H מכילה חבורה חלקית נורמלית לא טריביאלית של G.

25. $\sigma, \tau \in S_n$ הן צמודות אם"ם הן מאותו טפוס. מכאן, מספר מחלקות הצמידות ב S_n הוא $\wp(n)$.

26. נֻסחת המחלקה: $|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|C(x_i)|}$, באשר $C(x_i)$ עובר על מסלולי הצמידות הלא טריביאליים.

27. תהי G חבורה מסדר p^n, באשר p מספר ראשוני. אזי $Z(G) \neq \{1\}$.

28. אם p מספר ראשוני, אז כל חבורה בעלת p^2 אברים היא קומוטטיבית.

29. משפט קושי: תהי G חבורה סופית ויהי p מספר ראשוני. אם $p\big||G|$, אז קים ב G אבר מסדר p.

סעיף 8: משפטי סילוב.

30. אם $p^k\big||G|$, באשר p מספר ראשוני, אז קימת ל G חבורה חלקית מסדר p^k.

31. אם $H < G$ חבורת־p, אז קימת ל G חבורת p־סילוב המכילה את H.

יתר־על־כן, אם P היא חבורת p־סילוב של G, אז קים $x \in G$ כך ש $H < xPx^{-1}$.

32. כל שתי חבורות p־סילוב צמודות.

33. חבורת p־סילוב היא יחידה אם"ם היא נורמלית.

34. תהי P חבורת p־סילוב של G. אזי מספר חבורות ה p־סילוב של G הוא $[G : N(P)]$, באשר $N(P) = \{x \in G \mid xP = Px\}$.

35. אם $|G| = p^r m$ ו $p \nmid m$, אז מספר חבורות p־סילוב ב G הוא $1 + kp$, באשר $1 + kp|m$.

סעיף 9: חבורות מסדר קטן.

36. תהי G חבורה כך ש $1 < |G| < 60$ וכן G לא מסדר ראשוני. אזי G אינה פשוטה.

37. אם $n \geq 5$, אז החבורה A_n פשוטה.

38. יש רק חבורה אחת (עד כדי איזומורפיזם) מסדר 6 שהיא אינה קומוטטיבית.

39. כל חבורה מסדר 8 איזומורפית לאחת החבורות $\mathbb{Z}_8$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, D_4 או Q.

40. תהי G חבורה מסדר $2p$, באשר p מספר ראשוני אי־זוגי. אזי $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_p \cong \mathbb{Z}_{2p}$ או $G \cong D_p$.

41. כל חבורה מסדר 12 איזומורפית לאחת מחמש החבורות הבאות:

$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, D_6, A_4 או $\langle b, c \mid b^4 = c^6 = 1, b^2 = c^3, bc = c^5 b \rangle$.

42. אין ל A_4 חבורה חלקית מסדר 6.

מבחן לדֻגמה במבנים אלגבריים 1

מרצים: פרופ' מלכה שפס, פרופ' שלום פייגלשטוק וד"ר אהרון רזון

משך הבחינה: שעתיים וחצי

ללא חומר עזר

חלק I - ענה/י על 8 שאלות מתוך 9

(5 נק') 1. נניח ש $a|n$ ו $b|n$.

א) $n|[a,b]$.

ב) $(\frac{n}{a},\frac{n}{b}) = \frac{n}{[a,b]}$.

ג) $[a,b] = \frac{n}{(a,b)}$.

ד) כל התשובות האחרות אינן נכונות.

(5 נק') 2. תהי M חבורה למחצה (אגודה) סופית.

א) אם לכל $a \in M$ קימים r, s כך ש $a^r = a^s$, $r \neq s$, אז M חבורה.

ב) לא חיבים להיות אברים b, c ב M כך ש $bc = bc^2$.

ג) M חיב להיות מונואיד.

ד) כל התשובות האחרות אינן נכונות.

(5 נק') 3. תהי G חבורה ציקלית ו H תת־חבורה.

א) אם G/H צקלית, אז H טריביאלי (כלומר $H = \{1\}$).

ב) קימת תת־חבורה $K \triangleleft G$ כך ש $G = H \times K$.

ג) אם קימת תת־חבורה K לא טריביאלית כך ש $H \cap K = \{1\}$, אזי $(|H|,|K|) = 1$.

ד) כל התשובות האחרות אינן נכונות.

(5 נק') 4. תהי $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 4 & 6 & 2 & 1 & 7 & 3 & 5 \end{pmatrix}$.

א) הסדר של τ הוא 18.

ב) אם $\sigma = (3\,8)$, אז $\tau\sigma\tau^{-1} = (5\,6)$.

ג) $\tau \in A_8$.

ד) כל התשובות האחרות אינן נכונות.

(5 נק') 5. תהי $T = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{R},\ a, d \neq 0 \right\}$.

א) T תת־חבורה נורמלית של $GL(2, \mathbb{R})$.

ב) T חבורה אבלית.

ג) הגרעין של $\det\colon T \to \mathbb{R}^\times$ הוא $\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}$.

ד) כל התשובות האחרות אינן נכונות.

(5 נק') 6. יהיו G חבורה אבלית, $\varphi\colon G \times B \to B$ פעולה שמאלית ו $f\colon H \to G$ הומומורפיזם של חבורות. נכתב $\varphi(g, b) = g * b \in B$.

א) ההעתקה $\varphi_1\colon H \times B \to B$ המוגדרת ע"י $\varphi_1(h, b) = f(h) * b$ היא פעולה שמאלית.

ב) ההעתקה $\varphi_2\colon G \times B \to B$ המוגדרת ע"י $\varphi_2(g, b) = g^{-1} * b$ היא פעולה שמאלית.

ג) ההעתקה $\varphi_3\colon G \times B \to B$ המוגדרת ע"י $\varphi_3(g, b) = g^2 * b$ היא פעולה שמאלית.

ד) כל התשובות **נכונות**.

(5 נק') 7. תהי G חבורה מסדר 8. אלו מהתכונות הבאות חיבות להיות נכונות ? (i) G קומוטטבית; (ii) $Z(G)$ אינו טריביאלי; (iii) ל G יש תת־חבורה נורמלית מסדר 4; (iv) ל G יש אבר מסדר 4.

א) (i), (ii), (iii).

ב) (iii), (iv).

ג) (ii), (iii).

ד) כל התשובות האחרות אינן נכונות.

(5 נק') 8. ב A_4

א) יש 3 מחלקות צמידות.

ב) יש תתי־חבורות מסדרים $1, 2, 3, 6, 12$.

ג) יש 4 צמודים ל $(1\,2\,3)$.

ד) כל התשובות האחרות אינן נכונות.

(5 נק') 9. תהי G חבורה מסדר 56.

א) אם G לא אבלית ויש לה תת־חבורה נורמלית מסדר 8, אז יש לה 8 תתי־חבורות מסדר 7.

ב) אם יש ל G תת־חבורה נורמלית מסדר 7, אז יש ב G 7 תתי־חבורות מסדר 2.

ג) ל G לא יכולים להיות תתי־חבורות נורמליות מסדרים 7 ו 8.

ד) כל התשובות האחרות אינן נכונות.

חלק II - ענה/י על 3 שאלות מתוך 4

(20 נק') 10. א) הוכח/י שההעתקה $\beta\colon G \to \operatorname{Aut}(G)$

המוגדרת ע"י $g \mapsto \big(f_g\colon G \to G \mid \ f_g(h) = ghg^{-1}\big)$

היא הומומורפיזם של חבורות.

ב) תהי $\operatorname{Inn}(G) = \beta(G)$. הוכח/י ש $\operatorname{Inn}(G) \lhd \operatorname{Aut}(G)$.

(הערה: בדרך כלל, תמונה הומומורפית אינה חיבת להיות נורמלית.)

(20 נק') 11. אם $G = H \times K$ ו $N \lhd H$, הוכח/י ש

$G/(N \times K) \cong H/N$.

(20 נק') 12. תהי G חבורה מסדר 195. הוכח/י ש G מכילה תת־חבורה נורמלית H כך ש G/H ציקלית.

(20 נק') 13. א) הוכח/י שאם לחבורה G יש תת־חבורה נורמלית H, $H < Z(G)$, כך ש G/H ציקלית, אז G אבלית.

ב) תן/י דֻגמה לחבורה G כך ש $G/Z(G)$ אבלית אבל לא ציקלית.

ב ה צ ל ח ה ! ! !