תרגיל 4 מבוא לתורת החבורות

שאלה 4.1 קודם כל נזכיר: עבור $a,b \in \mathbb{Z}$ מספרים שלמים, הכופל המשותף המזערי שלהם - $m = \operatorname{lcm}(a,b)$ - הוא המספר הכי קטן שמקיים $a \mid m$ ו $b \mid m$. אפשר להוכיח שאם יש מספר אחר x כך ש $a \mid x$ ו $b \mid x$ אזי $m \mid x$. כמו כן, ידוע כי

$$\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$$

1. תהינה G,H חבורות שבהן לכל איבר יש סדר סופי. ניקח $g \in G$ ו $h \in H$. הוכיחו כי הסדר של (g,h) בחבורה $G \times H$ הוא

$$\operatorname{lcm}(\operatorname{o}(g), \operatorname{o}(h))$$

פתרון: נסמן $m = \operatorname{lcm}(\operatorname{o}(g), \operatorname{o}(h))$ בגלל ש $\operatorname{o}(g) \mid m$ וגם $\operatorname{o}(h) \mid m$ אז ברור ש

$$g^m = e = h^m$$

ולכן

$$(g,h)^m = (g^m, h^m) = (e,e)$$

מצד שני, אם k הוא מספר כך ש

$$(g,h)^k = (g^k, h^k) = (e,e)$$

אז בעצם

$$g^k = e, \quad h^k = e$$

ולכן

$$\operatorname{o}(g) \mid k, \quad \operatorname{o}(h) \mid k$$

ומכאן

$$m \mid k$$

כלומר m הוא באמת הסדר כנדרש.

2. הוכיחו כי $\mathbb{Z}_n \times \mathbb{Z}_m$ היא חבורה ציקלית אם ורק אם n ו m זרים.

פתרון: נניח ש $\gcd(m,n) = 1$. נסמן ב a יוצר של $\mathbb{Z}_n$ וב b יוצר של $\mathbb{Z}_m$. כלומר:

$$\operatorname{o}(a) = n \quad \operatorname{o}(b) = m$$

לפי הסעיף הקודם

$$\operatorname{o}(a,b) = \operatorname{lcm}(n,m) = \frac{nm}{\gcd(n,m)} = nm$$

מפני ש $\gcd(m,n)=1$. לכן*

$$\mathrm{o}(a,b)=nm=|\mathbb{Z}_n\times\mathbb{Z}_m|$$

ולכן זו חבורה ציקלית.

מצד שני, נניח ש $\mathbb{Z}_n\times\mathbb{Z}_m$ חבורה ציקלית ונניח ש (a,b) יוצר אז:

$$\mathrm{o}(a,b)=|\mathbb{Z}_n\times\mathbb{Z}_m|=nm$$

אבל מצד שני,

$$(a,b)^{\mathrm{lcm}(m,n)}=(e,e)$$

ולכן

$$\mathrm{lcm}(m,n)=mn$$

ולכן

$$\gcd(n,m)=1$$

כנדרש.

שאלה 4.2 תהי $G=\langle g\rangle$ חבורה ציקלית ו $H\leq G$ תת חבורה. הוכיחו כי גם H חבורה ציקלית.

הדרכה: קחו את ה k המינימלי עבורו $g^k\in H$. הוכיחו כי $H=\langle g^k\rangle$.

פתרון: נפעל לפי ההדרכה: ברור מההגדרה ש

$$\langle g^k\rangle\subseteq H$$

ניקח $h\in H$ צריך להוכיח

$$h\in\langle g^k\rangle$$

היות ש $h\in G$ אז קיים m כך ש $a^m=h$ כלומר $a^m\in H$. נבצע חילוק עם שארית

$$m=qk+r\quad(0\leq r<k)$$

ולכן

$$g^mg^{-qk}=g^r$$

אבל

$$g^m\in H$$

ו

$$g^{-qk}\in H$$

ולכן

$$g^r\in H$$

מה שמכריח $r=0$ (אחרת יש סתירה למינימליות של k) ולכן $k\mid m$ ולכן $g^m\in\langle g^k\rangle$ כנדרש.

שאלה 4.3 בכל אחד מהמקרים הבאים. תארו את הקוסטים של תת החבורה H בחבורה G (לא משנה אם קוסטים ימניים או שמאליים, אין הבדל בדוגמאות כאן):

1. $G = U_{30}$ ו $H = \langle 11 \rangle$.

פתרון: נשים לב שב U_{30} יש בסך הכל את 8 האיברים הבאים:

$$U_{30} = \{1, 7, 11, 13, 17, 19, 23, 29\}$$

כמו כן,

$$H = \{1, 11\}$$

נחשב את שאר הקוסטים

$$H7 = \{7, 17\}$$

$$H13 = \{13, 23\}$$

$$H19 = \{19, 29\}$$

2. $G = (\mathbb{C}\backslash\{0\}, \cdot)$ ו $H = \{z \in \mathbb{C} \mid |z| = 1\}$

פתרון: קל לראות ש

$$zw^{-1} \in H \iff |zw^{-1}| = 1 \iff |z| = |w|$$

ולכן אם ניקח $w \in \mathbb{C}$ מספר מרוכב שונה מ 0. זה אומר בעצם ש

$$Hw = \{z \in \mathbb{C} \mid |z| = |w|\}$$

הסבר: מצד אחד אם $|z| = |w|$ אז באמת $zw^{-1} \in H$ כי $|zw| = |z||w|^{-1}$

3. עבור A, B חבורות כלשהן. $G = A \times B$ ו $H = A \times \{e\}$.

פתרון: אם (a_1, b_1) ו (a_2, b_2) שני איברים ב $A \times B$ אז

$$(a_1, b_1) \cdot (a_2, b_2)^{-1} \in H \iff (a_1, b_1) \cdot (a_2^{-1}, b_2^{-1}) \in H \iff (a_1 a_2^{-1}, b_1 b_2^{-1}) \in H$$
$$\iff b_1 b_2^{-1} = e \iff b_1 = b_2$$

ולכן אפשר לתאר קוסט כללי ככה:

$$H(a, b) = \{(x, y) \in A \times B \mid y = b\}$$

4. $G = \mathrm{GL}_n(\mathbb{R})$ ו $H = \mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid |A| = 1\}$

פתרון: זה די דומה לסעיף 2. שתי מטריצות A, B נמצאות באותו קוסט אם

$$AB^{-1} \in \mathrm{SL}_2(\mathbb{R}) \iff |AB^{-1}| = 1 \iff |A| = |B|$$

ולכן אפשר לתאר את הקוסטים ככה: עבור $A \in \mathrm{GL}_n(\mathbb{R})$

$$HA = \{X \in \mathrm{GL}_n(\mathbb{R}) \mid |A| = |X|\}$$

שאלה 4.4 תהי G חבורה סופית ויהיו H,K שתי תתי חבורות כך ש

$$\gcd(|H|,|K|)=1$$

הוכיחו כי $H\cap K=\{e\}$.

פתרון: הוכחנו כבר בעבר שחיתוך תתי חבורות הוא תת חבורה. ולכן $H\cap K$ תת חבורה של G. אבל $H\cap K$ תת חבורה גם של H וגם של K. לפי משפט לגרנז' נקבל ש

$$|H\cap K| \mid |H|, \quad |H\cap K| \mid |K|$$

ולכן

$$|H\cap K| \mid \gcd(|H|,|K|)=1$$

זה מכריח

$$|H\cap K|=1$$

ולכן

$$H\cap K=\{e\}$$

שאלה 4.5 יהיו p,q ראשוניים שונים. תהי G חבורה מסדר pq. הוכיחו כי כל תת חבורה ממש של G (כלומר, תת חבורה $H\leq G$ כך ש $H\neq G$) היא ציקלית.

פתרון: לפי משפט לגרנז'

$$|H| \mid |G|=pq$$

אבל בגלל ש $H\neq G$, לא ייתכן ש $|H|=pq$. לכן האפשרויות שנותרו הן $|H|=1$ שאז זו חבורה בגודל 1שוודאי ציקלית. או $|H|=p$ או $|H|=q$ שאז החבורה ציקלית כי הסדר שלה ראשוני.

שאלה 4.6 לכל חבורה G יש לפחות 2 תתי חבורות "טריויאליות": G ו $\{e\}$. מצאו את כל החבורות G (סופיות או אינסופיות) שאלה תתי החבורות היחידות שלהן. במילים אחרות מצאו את כל החבורות שאין להם תתי חבורות לא טריויאליות.

הערה: הכוונה שלי היא להגיע לתשובה בסגנון הזה: "אלה בדיוק החבורות האבליות מסדר 15 ו 7" (הכוונה היא לא לתאר במפורט את החבורה והכפל שלה)

פתרון: אפשרות אחת היא ש Gהיא חבורה עם איבר אחד בלבד. אם זה לא המצב אז ניקח $g\in G$ כלשהוא כך ש $g\neq e$. בוודאי מתקיים

$$\langle g\rangle \leq G$$

ולכן לפי ההנחה

$$\langle g\rangle = G$$

לכן **כל איבר (למעט הניטראלי) יוצר את** G. בפרט G ציקלית. ניקח איזשהוא $a\in G$ כך ש $a\neq e$. הרגע ראינו ש

$$\langle a\rangle = G$$

עכשיו נפריד ל 2 מקרים: אפשרות א': $\mathrm{o}(a)=\infty$, במצב הזה $a \neq a^k$ לכל $k>1$. אבל גם a^2 יוצר את G כלומר

$$\langle a^2 \rangle = G$$

ולכן

$$a \in \langle a^2 \rangle$$

כלומר

$$a = (a^2)^k$$

סתירה.

אז לא ייתכן שהסדר של a אינסופי.

אפשרות ב':

$$\mathrm{o}(a) = n$$

ואז בעצם

$$|G| = n$$

אבל ראינו שכל איבר לא טריויאלי יוצא את G ולכן לכל $g \in G$ כך ש $g \neq e$ מתקיים

$$\mathrm{o}(g) = n$$

עכשיו, ינסתכל על a^k(עבור $1 \leq k < n$) שהרגע אמרנו שהסדר שלו הוא n. לפי נוסחא

$$\mathrm{o}(a^k) = \frac{n}{\gcd(n,k)}$$

ולכן בהכרח

$$\gcd(n,k) = 1$$

זה אומר שכל מספר עד n זר ל n זאת בדיוק ההגדרה של n ראשוני.

מסקנה: G חייבת להיות חבורה עם $|G|$ ראשוני. מצד שני לחבורה עם סדר ראשוני אין תתי חבורות ממש לפי משפט לגרז' ולכן התשובה הסופית היא: כל החבורות עם סדר ראשוני (או 1).