

תרגול 5: הומומורפיזם/איזומורפיזם, מחלקות

מונומורפיזם: פונקציה $\varphi: G \rightarrow H$ תקרא **מונומורפיזם** אם היא הומומורפיזם חד חד ערכי. מונומורפיזם נקרא גם שיכון.

אפימורפיזם: פונקציה $\varphi: G \rightarrow H$ תקרא **אפימורפיזם** אם היא הומומורפיזם על.

איזומורפיזם: פונקציה $\varphi: G \rightarrow H$ תקרא **איזומורפיזם** אם היא הומומורפיזם חד חד ערכי ועל.

סימון: $G \cong H$ משמעותו G איזומורפי ל H כלומר קיימת פונקציה איזומורפית $\varphi: G \rightarrow H$. המשמעות המעשית היא שהקבוצות G ו H הם למעשה זהות והפונקציה φ היא מילון שמתאים לכל איבר ב G איבר ב H .

תרגיל: הראו ש \mathbb{Z} אינה איזומורפית ל \mathbb{Q} .

פתרון: \mathbb{Z} היא חבורה ציקלית, ו \mathbb{Q} היא לא.

תרגיל: הראו ש \mathbb{Q}^* אינה איזומורפית ל \mathbb{Q} .

פתרון: ב \mathbb{Q} אין איברים מסדר סופי פרט ל 0 (אם $n \neq 0, q \in \mathbb{Q}$ אזי $nq = 0 \Rightarrow q = 0$), וב- \mathbb{Q}^* יש איבר (יחיד) מסדר 2 והוא -1 ($q^2 = 1 \Leftrightarrow q = \pm 1$).

תרגיל: הראו שלא קיים שיכון $f: GL_3(\mathbb{Q}) \rightarrow \mathbb{Q}^{20} = \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \dots \times \mathbb{Q}$.

פתרון: החבורה $GL_3(\mathbb{Q})$ אינה אבלית, אך אם קיים שיכון (מונומורפיזם), אזי $\text{Im}(f) \leq \mathbb{Q}^{20}$ אבל כל תת-חבורה של חבורה אבלית היא אבלית, ולכן $GL_3(\mathbb{Q}) \cong \text{Im}(f)$ היא אבלית, סתירה.

תרגיל: בדקו עבור כל שתיים מהחבורות הבאות האם הן איזומורפיות $\mathbb{R}, \mathbb{R}^*, \mathbb{R}^{>0}$

פתרון: $\mathbb{R} \neq \mathbb{R}^*$ לפי אותה הוכחה עבור $\mathbb{Q} \neq \mathbb{Q}^*$. $\mathbb{R} \cong \mathbb{R}^{>0}$ לפי הומומורפיזמים (איזומורפיזמים) $e^x: \mathbb{R} \rightarrow \mathbb{R}^{>0}, \log x: \mathbb{R}^{>0} \rightarrow \mathbb{R}$. $\mathbb{R}^{>0} \neq \mathbb{R}^*$ לפי טרנזיטיביות של איזומורפיזמים, כיוון שאם $\mathbb{R}^{>0} \cong \mathbb{R}^*$ אזי $\mathbb{R} \cong \mathbb{R}^*$, סתירה.

מחלקות בחבורה:

מחלקות ימניות ושמאליות:

הגדרה: תהי G חבורה $H \leq G$ ויהי $a \in G$

מחלקה שמאלית מוגדרת ע"י $aH := \{ah \mid h \in H\}$

מחלקה ימנית מוגדרת ע"י $Ha := \{ha \mid h \in H\}$

דוגמא: $G = \mathbb{Z}$, $H = 6\mathbb{Z}$, $a = 2$ ונקבל ש

$$2 + 6\mathbb{Z} = 6\mathbb{Z} + 2 = \{\dots, -10, -4, 2, 8, 14, \dots\}$$

משפט: אם $H \leq G$, אז מתקיים:

- א. $aH = bH$ או $aH \cap bH = \emptyset$ כלומר כל 2 מחלקות שמאליות (ימניות) זהות או זרות.
- ב. $aH = H$ אם ורק אם $a \in H$.

תרגיל: הראו שמחלקה gH היא חבורה אם ורק אם $g \in H$.

פתרון: אם $g \in H$ אזי $gH = H$ כי הכפלה באיבר משמאל היא חח"ע ועל (כפי שראינו בתרגול הראשון). אם gH היא חבורה, אז $e \in gH$ ולכן קיים $h \in H$ כך ש $gh = e$, ולכן $g = h^{-1} \in H$. כלומר $g \in gH \cap H$ ולכן לפי המשפט הנ"ל, נקבל $gH = H$.

משפט: $H \leq G$, אז $a, b \in G$ $aH = bH \Leftrightarrow b^{-1}a \in H$. עבור מחלקות ימניות:

$Ha = Hb \Leftrightarrow ab^{-1} \in H$. היחס $a \sim b \Leftrightarrow b^{-1}a \in H$ הוא יחס שקילות. מחלקות השקילות הן בדיוק המחלקות השמאליות.

מסקנה: $G = \coprod xH$ $H \leq G$ (כאשר \coprod הוא איחוד זר שעובר על נציגי כל המחלקות השמאליות).

תרגיל בית: תהי $H \leq G$ הוכיחו: $g_2 \in Hg_1 \Leftrightarrow Hg_2 = Hg_1$

הגדרה: תהי G חבורה, ותהי X תת-קבוצה של G , אזי $X^{-1} := \{x^{-1} \mid x \in X\}$.

תרגיל בית: הוכיחו או הפריכו: במונואיד הכפלי של תת-קבוצות של G , X^{-1} הוא ההפכי של X . רמז: מהו H^{-1} עבור $H \leq G$.

תרגיל: $(Hg)^{-1} = ?$

פתרון:

$$(Hg)^{-1} = \{(hg)^{-1} \mid h \in H\} = \{g^{-1}h^{-1} \mid h \in H\} = \{g^{-1}h \mid h \in H\} = g^{-1}H$$

משפט: קיימת התאמה חח"ע (פונקציה חח"ע ועל):

$$\{\text{מחלקות שמאליות}\} \leftrightarrow \{\text{מחלקות ימניות}\}$$

$$gH \mapsto Hg^{-1} \text{ המוגדרת ע"י}$$

תרגיל בית: האם $gH \mapsto Hg$ היא התאמה חח"ע כנ"ל?

משפט: אם $H \leq G$ ת"ח סופית אז לכל מחלקה xH מתקיים $|xH| = |H|$.

הגדרה: $[G : H]$ הוא מס' המח' הימניות (השמאליות) של H ב G נקרא האינדקס של H ב G .

משפט לגראנז' (נוסח א'): תהי G סופית ו- $H \leq G$ אז $|G| = [G : H]|H|$

משפט לגראנז' (נוסח ב'): תהי G סופית ו- $H \leq G$ אז $|H| \mid |G|$ כלומר סדר התת-חבורה מחלק את סדר החבורה.

מסקנה חשובה ממשפט לגראנז':

$$\text{יהיו } K \leq H \leq G \text{ ת"ח. אזי } [G : K] = [G : H][H : K]$$

תרגיל: $|G| = 20$. לפי משפט לגראנז' איזה סדר אפשרי לתתי החבורות של G ?

פתרון: סדר התת-חבורה מחלק את סדר החבורה לכן סדר התתי חבורות של G חייב לחלק את 20 ולכן הסדרים האפשריים הם: 1, 2, 4, 5, 10, 20. אלה גם הסדרים היחידים האפשריים עבור איברים ב G , כפי שנראה במשפט הבא.

תרגיל בית: אותה שאלה עם שינוי קטן. תהי $H \leq G$ כאשר ידוע שב- H יש איבר מסדר 2, מהם הסדרים האפשריים של H ? (פתרו שאלה זו אחרי התרגילים בעמוד הבא).

משפט: תהי G סופית ו- $g \in G$ אז $o(g) \mid |G|$ כלומר סדר איבר בחבורה סופית מחלק את סדר החבורה. (ההוכחה מיידית לפי משפט לגרנג' והגדרת סדר של איבר).

מסקנה: לכל איבר $g \in G$ מתקיים $g^{|G|} = e$.

הוכחה: לפי המשפט $o(g) \mid |G|$ ולכן $\frac{|G|}{o(g)}$ הוא מספר שלם. אם כך מתקיים $e = e^{\frac{|G|}{o(g)}} = (g^{o(g)})^{\frac{|G|}{o(g)}} = e$.

המשפט הקטן של פרמה:

יהי $p > 0$ מס' ראשוני לכל מס' שלם a מתקיים $a^p \equiv a \pmod{p}$

הוכחה: הסדר של חבורת אוילר הוא $\varphi(p) = |Euler(p)| = p-1$ (מדוע?).

לכן לפי המסקנה לעיל, נקבל שעבור $a \neq 0$ מתקיים $a^{\varphi(p)} = a^{p-1} = e$. נכפיל את שני האגפים ב- a , ונקבל $a^p = a$. כעת נשאר להוכיח עבור המקרה של $a = 0$, אבל זה ברור.

דוגמא: $3^7 \equiv 3 \pmod{7}$.

תרגיל בית: כל חבורה מסדר p ראשוני היא ציקלית (ובפרט אבלית).

תרגיל: הראו שחבורה היא מסדר זוגי אם ורק אם קיים בה איבר מסדר 2.

הוכחה: \Leftarrow אם אין איברים מסדר 2, אז ניתן להצמיד כל איבר להפכי שלו (שהוא איבר שונה ממנו). ביחד עם איבר היחידה, נקבל מספר אי-זוגי.

\Rightarrow אם קיים איבר מסדר 2 אז לפי לגרנג' (או המשפט בתחילת העמוד) הסדר שלו (2) מחלק את סדר החבורה, ולכן סדר החבורה הוא זוגי.

תרגיל: תהי G חבורה מסדר $2p$ (p ראשוני) אז יש ל- G איבר מסדר p (בפרט תת חבורה מסדר p).

הוכחה:

נפטר קודם מהמקרה $p=2$. אם $p=2$ אזי G חבורה מסדר 4, ולכן היא בהכרח איזומורפית ל- $\mathbb{Z}_2 \times \mathbb{Z}_2$ או ל- \mathbb{Z}_4 (ראינו שאלה טבלאות הכפל היחידות האפשריות לחבורה מסדר 4). בשני המקרים קיימים איברים מסדר 2 (אפשר גם להשתמש בתרגיל הקודם).

כעת נניח ש p ראשוני אי-זוגי.

לפי משפט לגראנז' הסדרים האפשריים של איברים הם: $1, 2, p, 2p$.

אם יש איבר מסדר p אז סיימנו ואם יש איבר a מסדר $2p$ אז גם כן סיימנו כי

$(a^2)^p = a^{2p} = e \Rightarrow o(a^2) \leq p$. נשתמש כעת בתרגיל מתרגול קודם, האומר שאם $a^n = e$ אזי $n \mid o(a)$: לכן לפי הנ"ל נקבל ש $p \mid o(a^2)$, אבל לא ייתכן ש $o(a^2) = 1$ כי אז $o(a) \leq 2$ ונקבל סתירה להנחה ש $o(a) = 2p > 2$. לכן בהכרח $o(a) = p$.

כעת נניח בשלילה שכל האיברים בחבורה הם מסדר 2 (פרט לאיבר היחידה מסדר 1).

כבר ראינו בתרגול הראשון שחבורה כזאת בהכרח אבלית.

לכן החבורה G אבלית וכיוון שיש לפחות שני איברים שונים מסדר < 1 , קיימת ל G תת חבורה $\{1, a, b, ab\}$ האיזומורפית לחבורת קליין $(\mathbb{Z}_2 \times \mathbb{Z}_2)$ [הוכיחו את זה] ולכן נקבל לפי לגראנז' ש $4 \mid 2p$ סתירה לכן קיים איבר מסדר p או $2p$ \square