

מבנים דיסקרטיים – תרגיל 5

כל סעיף שווה 10 נקודות.

שאלה 1

- א. תהי G חבורה. נגדיר $Z(G) = \{g \in G \mid \forall h \in G: gh = hg\}$. הוכיחו כי $Z(G) \trianglelefteq G$.
ב. הוכיחו ישירות לפי ההגדרה של תת חבורה נורמלית ש- $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$. אין קשר לסעיף א.

הוכחה

- סעיף א:** ראשית נוכיח כי $Z(G)$ תת חבורה. נבדוק זאת ע"י הקריטריון לתת-חבורה:
א. $Z(G) \neq \emptyset$: לכל $h \in G$ מתקיים $eh = h = he$ ולכן $e \in Z(G)$.
ב. סגירות לכפל: אם $x, y \in Z(G)$ אז לכל $h \in G$ מתקיים $(xy)h = x(yh) = x(hy) = (xh)y = (hx)y = h(xy)$ ובשוויון הכחול השתמשנו ב- $(y \in Z(G))$. לכן $xy \in Z(G)$.
ג. סגירות להופכי: יהי $x \in Z(G)$. אזי לכל $h \in G$ מתקיים $xh = hx$. נכפול את השוויון ב- x^{-1} מימין ונקבל $xhx^{-1} = h$. נכפול משמאל ב- x^{-1} ונקבל $hx^{-1} = x^{-1}h$. היות וזה נכון לכל $h \in H$ נובע $x^{-1} \in Z(G)$.
לסיכום, $Z(G)$ תת חבורה של G .

קעת נראה כי $Z(G)$ נורמלית. מהגדרת $Z(G)$ נובע שלכל $x \in Z(G)$ ו- $h \in G$ מתקיים $xh = hx$ (בפרט, $Z(G)$ אבלית). לכן, לכל $h \in G$ מתקיים $hZ(G) = \{hx \mid x \in G\} = \{xh \mid x \in G\} = Z(G)h$ כלומר $Z(G) \trianglelefteq G$. מש"ל.

- סעיף ב:** נשתמש בהגדרה הבאה לנורמליות: H נורמלית ב- G אם לכל $g \in G$ מתקיים $g^{-1}Hg = H$. בפועל מספיק לבדוק רק ש- $Hg \subseteq gH$ לכל $g \in G$. כי אם זה נכון אז $H = g^{-1}(gHg^{-1})g \subseteq g^{-1}Hg$.

נראה כי $x^{-1}SL_n(\mathbb{R})x \subseteq SL_n(\mathbb{R})$ לכל $x \in GL_n(\mathbb{R})$. יהי $y \in SL_n(\mathbb{R})$, אזי $\det(y) = 1$. לכן, $x^{-1}yx \in SL_n(\mathbb{R})$. מש"ל.
 $\det(x^{-1}yx) = \det(x^{-1}) \det(y) \det(x) = \det(x)^{-1} \cdot 1 \cdot \det(x) = 1$ וזה אומר ש-

שאלה 2

- א. תהי G חבורה סופית ויהי $g \in G$. הוכיחו כי $o(g)$ מחלק את $|G|$. [רמז: $o(g)$ קשור לגודל של תת חבורה מסויימת].
ב. הוכיחו שאם $|G| = p^n$ עבור p ראשוני אז קיים $g \in G$ כך ש- $o(g) = p$.

הוכחה

סעיף א: $o(g) = |\langle g \rangle|$ ולפי משפט לגרנז', $|\langle g \rangle|$ מחלק את $|G|$. לכן, $o(g) \mid |G|$. מש"ל.

¹ הערה: זה מקרה פרטי של משפט קושי (זה אותו קושי מאינפי): אם G חבורה סופית ו- p מחלק את $|G|$ אז קיים ב- G איבר מסדר p .

הערה: סעיף א של שאלה 2 הוא מסקנה ממשפט לגרנז'. אפשר להשתמש בו במבחן או בפתרון תרגילים.

סעיף ב: יהי $h \in G, h \neq e$. אזי לפי סעיף א, $o(h) \mid p^n$. היות ו- p ראשוני, זה אומר ש- $o(h) = p^m$ עבור $m \geq 0$ כלשהו. היות ו- $g \neq e, o(h) \neq 1$ ולכן $m > 0$. נגדיר $g = h^{p^{m-1}}$. אנו טוענים כי $o(g) = p$. באמת, $g^p = (h^{p^{m-1}})^p = h^{p^m} = h^{o(h)} = e$, ולכן $o(g) \mid p$. מצד שני, $g = h^{p^{m-1}} \neq e$ (כי $o(h) = p^m > p^{m-1}$) ולכן $o(g) \neq 1$. לכן, (היות ו- p ראשוני) נובע ש- $o(g) = p$. כדרוש. **מש"ל.**

שאלה 3

- הראו ש- $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*$ ו- $SL_n(\mathbb{R}) \cong GL_n(\mathbb{R})$.
- הראו ש- $\mathbb{C}^*/\mathbb{R}_+ \cong \mathbb{T}$ ומתקיים $\mathbb{R}_+ \leq \mathbb{C}^*$ כאשר $\mathbb{T} = \{z: |z| = 1\}$ ו- $\mathbb{R}_+ = \{r \in \mathbb{R}: r > 0\}$.
- הראו ש- $\mathbb{R}^*/\mathbb{R}_+ \cong \{\pm 1\}$ ו- $\mathbb{R}_+ \leq \mathbb{R}^*$. מה הקוסטים של \mathbb{R}_+ ב- \mathbb{R}^* ?
- רשות:** הראו כי $\mathbb{C}^*/\{\pm 1\} \cong \mathbb{C}^*$.

[בחבורות $\mathbb{C}^*, \mathbb{R}^*, \mathbb{R}_+, \mathbb{T}, \{\pm 1\}$ הפעולה היא כפל מספרים רגיל. אין צורך להוכיח כי אלו חבורות.]

[הדרכה: בכיתה אמרנו שכדי להוכיח $G/K \cong H$ מספיק למצוא הומומורפיזם $f: G \rightarrow H$ כך ש- $\ker f = K$ ואז להשתמש במשפט האיזומורפיזם הראשון. שימו לב שזה אומר ש- $K \leq G$ כי גרעין של הומומורפיזם הוא תמיד נורמלי].

פיתרון

סעיף א: נגדיר הומומורפיזם $f: GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ ע"י $f(A) = \det A$. הומומורפיזם כי $f(AB) = \det(AB) = \det A \cdot \det B = f(A)f(B)$ לכל $A, B \in GL_n(\mathbb{R})$.

על כי לכל $a \in \mathbb{R}^*$ המטריצה $A = \begin{bmatrix} a & 0 & \dots & 0 \\ 0 & 1 & \dots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{bmatrix} \in GL_n(\mathbb{R})$ מקיימת $f(A) = \det A = a$.

בנוסף, $\ker f = \{A \in GL_n(\mathbb{R}) \mid f(A) = 1\} = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\} = SL_n(\mathbb{R})$.

לכן, לפי משפט האיזומורפיזם $GL_n(\mathbb{R})/SL_n(\mathbb{R}) = GL_n(\mathbb{R})/\ker f \cong \mathbb{R}^*$.

סעיף ב: נגדיר הומומורפיזם $f: \mathbb{C}^* \rightarrow \mathbb{T}$ ע"י $f(z) = \frac{z}{|z|}$ (שימו לב ש- $|z| \neq 0$ כי $z \neq 0$). הומומורפיזם כי $f(zw) = \frac{zw}{|zw|} = \frac{zw}{|z||w|} = \frac{z}{|z|} \cdot \frac{w}{|w|} = f(z)f(w)$ לכל $z, w \in \mathbb{C}^*$.

על כי לכל $a \in \mathbb{T}$ מתקיים $a \in \mathbb{C}^*$ ו- $f(a) = \frac{a}{|a|} = \frac{a}{1} = a$.

אנו טוענים כי $\ker f = \mathbb{R}_+$. באמת, לכל $a \in \mathbb{R}_+$ מתקיים $f(a) = \frac{a}{|a|} = \frac{a}{a} = 1$ ולכן $a \in \ker f$. מצד שני, אם $x \in \ker f$, אז $\frac{x}{|x|} = 1$, כלומר $|x| = x$. היות ו- $x \in \mathbb{R}_+$ (כי $x \neq 0$), נובע ש- $x \in \mathbb{R}_+$.

לכן, לפי משפט האיזומורפיזם $\mathbb{C}^*/\mathbb{R}_+ = \mathbb{C}^*/\ker f \cong \mathbb{T}$.

סעיף ג: נגדיר הומומורפיזם $f: \mathbb{R}^* \rightarrow \{\pm 1\}$ ע"י $f(x) = \frac{x}{|x|}$ (שימו לב ש- $|x| \neq 0$ כי $x \neq 0$). הומומורפיזם כי $f(zw) = \frac{zw}{|zw|} = \frac{zw}{|z||w|} = \frac{z}{|z|} \cdot \frac{w}{|w|} = f(z)f(w)$ לכל $z, w \in \mathbb{R}^*$.

על כי $f(1) = 1$ ו- $f(-1) = -1$ (בדקו!).

אנו טוענים כי $\ker f = \mathbb{R}_+$. באמת, לכל $a \in \mathbb{R}_+$ מתקיים $f(a) = \frac{a}{|a|} = \frac{a}{a} = 1$ ולכן $a \in \ker f$. מצד שני, אם $x \in \ker f$, אז $\frac{x}{|x|} = 1$, כלומר $x = |x|$. היות ו- $|x| \in \mathbb{R}_+$ (כי $x \neq 0$), נובע ש- $x \in \mathbb{R}_+$.

$$\frac{\mathbb{R}^*}{\mathbb{R}_+} = \frac{\mathbb{R}^*}{\ker f} \cong \{\pm 1\} \leq \mathbb{R}_+ \leq \mathbb{R}^* \quad \text{לכן, לפי משפט האיזומורפיזם}$$

הקוסטים של \mathbb{R}_+ ב- \mathbb{R}^* הם הקטעים $(0, \infty)$ ו- $(-\infty, 0)$.

סעיף ד: נגדיר $f: \mathbb{C}^* \rightarrow \mathbb{C}^*$ ע"י $f(z) = z^2$. f הומומורפיזם כי $f(zw) = (zw)^2 = z^2 w^2 = f(z)f(w)$ לכל $z, w \in \mathbb{C}^*$.

אנו טוענים כי f על. באמת, לכל $z \in \mathbb{C}^*$ קיים $r \in \mathbb{R}$ ו- $\theta \in [0, 2\pi)$ כך ש- $z = re^{i\theta}$. אזי

$$f\left(\sqrt{r} \cdot e^{i\frac{\theta}{2}}\right) = r \cdot e^{i\theta} = re^{i\theta} = z$$

אנו טוענים כי $\ker f = \{\pm 1\}$. באמת, $f(1) = f(-1) = 1$ ולכן $\{\pm 1\} \subseteq \ker f$. מצד שני, אם $z \in \ker f$ אז $z^2 = 1$, כלומר $z^2 - 1 = 0 = (z+1)(z-1)$. היות וב- \mathbb{C} אין מחלקי 0 (כי הוא שדה), בהכרח $z+1 = 0$ או $z-1 = 0$, לכן, $z = 1$ או $z = -1$.

$$\frac{\mathbb{C}^*}{\{\pm 1\}} = \frac{\mathbb{C}^*}{\ker f} \cong \{\pm 1\} \leq \mathbb{C}^* \quad \text{לכן, לפי משפט האיזומורפיזם}$$

שאלה 4

תהי G חבורה ו- $H_1, H_2 \leq G$. הוכיחו כי אם $\gcd(|H_1|, |H_2|) = 1$ אז $H_1 \cap H_2 = \{e\}$. [רמז: מסקנה ממשפט לגרנז'.]

הוכחה

נסמן $K = H_1 \cap H_2$. אזי K תת חבורה של H_1 ולכן לפי משפט לגרנז' (או מסקנה ממשפט לגרנז'), $|K|$ מחלק את $|H_1|$. באותו אופן, $|K|$ מחלק את $|H_2|$. לכן, $|K|$ מחלק את $\gcd(|H_1|, |H_2|) = 1$, כלומר $|K| = 1$ ולכן $H_1 \cap H_2 = K = \{e\}$. **מש"ל.**

שאלה 5

תהי G חבורה סופית.

- נניח כי $G \trianglelefteq H$. הוכיחו כי לכל $g \in G$ מתקיים $g^{|G/H|} \in H$. [הדרכה: מספיק להראות $g^{|G/H|}H = H$ (מדוע?). הפעילו את סעיף א של שאלה 2 על החבורה G/H .]
- נניח כי $G \trianglelefteq H_1, H_2$ חבורות שונות המקיימות $|H_1| = |H_2| < 1$. הוכיחו כי קיים $n < |G|$ כך שלכל $g \in G$ מתקיים $g^n = e$. [רמז: השתמשו בסעיף א עם $H = H_1$ ו- $H = H_2$.]
- רשות:** הראו כי אם G צקלית ו- k מחלק את $|G|$ אז ל- G יש בדיוק תת חבורה אחת מגודל k .

הוכחה

סעיף א: היות ו- $H \trianglelefteq G$, היא חבורה. לכן, לפי מסקנה ממשפט לגרנז' (על החבורה G/H), לכל $X \in G/H$ מתקיים $X^{|G/H|} = H$ (זכרו ש- H היא היחידה של G/H). יהי $g \in G$. נבחר $X = gH$. אזי לפי מה שהראינו $H = (gH)^{|G/H|} = H$. זה אומר ש- $eH = (gH)^{|G/H|} = H = eH$, לכן, מסעיף במשפט לגרנז' ($aH = bH$ אם ורק אם $a = b$), נובע ש- $e = g^{|G/H|}$, לכן, קיבלנו שלכל $g \in G$ מתקיים $g^{|G/H|} \in H$. **מש"ל.**

סעיף ב: תהיינה H_1, H_2 כנ"ל ונסמן $m = |H_1| = |H_2|$. אזי לפי משפט לגרנדז' $\frac{|G|}{|H_1|} = \frac{|G|}{|H_1|} = \frac{|G|}{m}$.
 באותו אופן, $\frac{|G|}{|H_2|} = \frac{|G|}{m}$. יהי $g \in G$, אזי לפי סעיף א (עם $H = H_1$) מתקיים $g^{\frac{|G|}{m}} \in H_1$.
 באותו אופן, $g^{\frac{|G|}{m}} \in H_2$. לכן, לכל $g \in G$ מתקיים $g^{\frac{|G|}{m}} \in H_1 \cap H_2$. נסמן $k = |H_1 \cap H_2|$. היות ו-
 H_1, H_2 הן שתי קבוצות שונות בעלות גודל זהה, בהכרח $k < m$ (בדקו!). לפי מסקנה ממשפט לגרנדז'
 (על החבורה $(H_1 \cap H_2)$), לכל $x \in H_1 \cap H_2$ מתקיים $x^k = e$. הראנו שלכל $g \in G$ מתקיים $g^{\frac{|G|}{m}} \in H_1 \cap H_2$
 ולכן, $g^{\frac{|G|}{m} \cdot k} = \left(g^{\frac{|G|}{m}}\right)^k = e$.

לסיכום, הראינו כי לכל $g \in G$ מתקיים $g^{\frac{|G|}{m} \cdot k} = e$. היות ו- $k < m$ אז $k < |G|$. לכן נבחר
 $n = \frac{|G|}{m} \cdot k$ וגמרנו. **מש"ל.**

סעיף ג: תהי G חבורה ציקלית, יהי $x \in G$ כך ש- $\langle x \rangle = G$ ויהי $|G| = k$. אזי G אבלית ולכן כל תת
 חבורה של G היא נורמלית. בניח בשלילה של- G יש שתי תתי חבורות שונות בגודל k , אזי הן
 נורמליות ולכן לפי סעיף ב, קיים $n < |G|$ כך שלכל $g \in G$ מתקיים $g^n = e$. אבל זה אומר ש-
 $x^n = e$, כלומר $n = o(x) \leq |G|$ וזו סתירה. לכן, ל- G יש לכל היותר תת חבורה אחת מגודל k .

נותר להראות שאכן יש תת חבורה כזו. היות ו- $|G| = k$, אז $\frac{|G|}{k} = 1$ מספר שלם. נגדיר $y = x^{\frac{|G|}{k}}$. אזי
 $o(y) = k$ (בדקו!) ולכן $o(y) = k$, כלומר $\langle y \rangle$ תת חבורה בגודל k של G . **מש"ל.**