

פתרון מועד א' קיץ תשס"ו

שאלה 1:

א. נגדיר: $H = \left\{ \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ ונראה ש- $H \leq GL_2(\mathbb{R})$:

האיבר האדיש הוא: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$ כלומר: $b=1, a=0$.

קיימת סגירות: $\begin{pmatrix} b_1 & a_1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} b_2 & a_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} b_1 b_2 & a_1 + b_1 a_2 \\ 0 & 1 \end{pmatrix} \in H$

האיבר ההופכי של: $\begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix}$ הוא: $\begin{pmatrix} \frac{1}{b} & -\frac{a}{b} \\ 0 & 1 \end{pmatrix} \in H$.

כעת נשים לב ש- H היא תיאור מדויק של G . כלומר $G = H$ היא חבורה.

ב. לדוגמה: $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$

ג. ב-א' ראינו שאפשר לתאר את G כתת-חבורה ב- $GL_2(\mathbb{R})$.

נקרא לתיאור הזה: $\psi: G \rightarrow H \leq GL_2(\mathbb{R})$. הוא שומר פעולה ולכן הומומורפיזם.

התיאור הזה הוא חח"ע: $\ker(\psi) = \left\{ (a, b) \mid \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} = \{(1, 0)\} = e_G$

ד. נגזור: כל קומוטטור $[A, B] = ABA^{-1}B^{-1}$ עבור: $A = \begin{pmatrix} b_1 & a_1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} b_2 & a_2 \\ 0 & 1 \end{pmatrix}$

הוא מהצורה: $\begin{pmatrix} b_1 b_2 & a_1 + b_1 a_2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{b_1 b_2} & -\frac{a_1}{b_1} - \frac{a_2}{b_1 b_2} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ כאשר $x \in \mathbb{R}$.

מתקיים: $\forall x, y \in \mathbb{R} : \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$

מכאן ש: $G' = \langle \{ [A, B] \mid A, B \in G \} \rangle$ היא אבלית ולכן: $G'' = \{e\}$ ו- G פתירה.

שאלה 2:

א. ו-ב. ראה בהרצאה/ תרגול.

ג. נתון Y אבלית. כמו כן f הומומורפיזם. לכן:

$$\forall g_1, g_2 \in G: f(g_1) \cdot f(g_2) = f(g_2) \cdot f(g_1)$$

$$\Downarrow$$

$$f(g_1 g_2) = f(g_2 g_1)$$

$$\Downarrow$$

$$f(g_1 g_2 g_1^{-1} g_2^{-1}) = e_Y$$

כלומר: $\forall g_1, g_2 \in G: [g_1, g_2] \in \ker(f)$ ומתוך הסגירות של $\ker(f)$ מתקבל

שהנגזרת: $G' = \langle \{ [g_1, g_2] \mid g_1, g_2 \in G \} \rangle$ מוכלת ב- $\ker(f)$.

שאלה 3:

א. ראה בהרצאה.

ב. קל לראות כי: $Z_{50} \cong G$. ממשפט קיילי נובע כי קיים שיכון של G ב- S_{50} שמשוכן ע"י

הכלה ב- S_{97} .

ג. נסמן: $\sigma = (4\ 5)$, $\tau = (1, 2, \dots, 7)$ ונוכיח באמצעות מספר שלבים:

א. נשים לב כי ההצמדה נותנת: $\tau \sigma \tau^{-1} = (5\ 6)$

וכן הלאה באינדוקציה: $\tau(5\ 6)\tau^{-1} = (6\ 7)$

כך שניתן לקבל את כל החילופים מהצורה: $(i, i+1)$ מודולו 7.

ב. באמצעות החילופים: $(4\ 5)$ ו- $\{(i, i+1)\}$ ניתן לייצר:

$$(4\ 5)(5\ 6)(4\ 5) = (4\ 6)$$

$$(4\ 6)(6\ 7)(4\ 6) = (4\ 7)$$

וכן הלאה באינדוקציה עד שמייצרים את כל: $\{(4\ i)\}$.

ג. ניתן לייצר כל חילוף ב- S_7 ע"י $\{(4\ i)\}$: $(i\ j) = (4\ i)(4\ j)(4\ i)$.

ד. ניתן לייצר כל עגיל (ולכן גם כל תמורה שהיא מכפלת עגילים) ע"י חילופים.

ד. כיוון ש- $\sqrt{3}$ אינו מספר רציונאלי, $\mathbf{Z} \langle cis(\sqrt{3}\pi) \rangle$, לכן תמונות אפימורפיות הן:

$\mathbf{Z}, \mathbf{Z}_n \forall n \geq 1$ (כאשר הגרעינים הם: $\{0\}$ ו- $n\mathbf{Z}$ בהתאמה).

לחבורה: $D_3 = \langle a, b \mid a^2 = 1, b^3 = 1, ba = ab^2 \rangle$ יש שתי תתי-חבורת נורמאליות

(שיכולות לשמש כגרעין של אפימורפיזם כ"א): $\langle b \rangle, \langle e \rangle$.

לכן התמונות האפימורפיות הן: $\mathbf{Z}_2 \cong D_3 / \langle b \rangle, D_3 \cong D_3 / \langle e \rangle$.

שאלה 4:

א. שתי החבורות במכפלה הן ציקליות מסדרים זרים. לכן החבורה איזומורפית לחבורה

הציקלית \mathbf{Z}_{4900} שמספר האיברים שיכולים ליצור אותה הם: $\varphi(4900)$.

נחשב: $49 = 2^2 \cdot 5^2 \cdot 7^2$. ניעזר בנוסחא: $\varphi(p^k) = p^k - p^{k-1}$

ומכאן: $\varphi(4900) = 2 \cdot 20 \cdot 42 = 1680$.

ב. מתוך $(67, 100) = 1$ מקבלים עפ"י משפט אוילר: $67^{\varphi(100)} = 67^{40} \equiv 1 \pmod{100}$.

מכאן: $67^{1998} = 67^{2000} \cdot 67^{-2} = \underbrace{(67^{40})^{50}}_{\equiv 1 \pmod{100}} \cdot (67^2)^{-1} \equiv 89^{-1} \pmod{100}$

נותר לחשב את ההופכי של 89 מודולו 100.

ניעזר באלגוריתם אוקלידס ונקבל: $1 = 9 \cdot 89 - 8 \cdot 100$ כלומר: $89^{-1} \equiv 9 \pmod{100}$.

ובסה"כ השארית היא: $9 + 6 = 15 \pmod{100}$.

ג. הכיוון הראשון ברור: $1^2 = 1, (p-1)^2 = p^2 - 2p + 1 \equiv 1 \pmod{p}$

הכיוון השני: אם מתקיים: $x^2 = 1 \pmod{p}$ אזי: $(x-1) \cdot (x+1) \equiv 0 \pmod{p}$.

עבור p ראשוני \mathbf{Z}_p^* היא חבורה (לגבי כפל) ואין בה מחלקי אפס לכן בהכרח אחד

מהגורמים מתאפס. מכאן: $x \equiv 1 \pmod{p}$ או: $x \equiv (-1) \pmod{p}$.

ד. נשים לב כי: $(p-1)! = \prod_{g \in \mathbf{Z}_p^*} g$ לכן (ראה תרגיל בית מס' 3) $[(p-1)!]^2 = 1$.

אם כן עפ"י הסעיף הקודם: $(p-1)! \in [p-1]$ ו- $1 \neq (p-1)! \in [p]$ ומתקיים: $(p-1)! + 1 \in [p]$.

שאלה 5:

- א. ראה בהרצאה.
- ב. ראה בתרגול באופן כללי שעבור $|G| = pq$, פתירה.
- ג. כיוון ש: $99 = 3^2 \cdot 11$ עפ"י סילו שלוש: $n_{11} = 1 + 11k_{11} \mid 9 = 1$ כלומר ישנה רק חבורת 11-סילו אחת ולכן היא נורמאלית כך ש- G בהכרח אינה פשוטה.

שאלה 6:

- א. ראה בהרצאה.
- ב. האיברים שמתחלפים עם α כלומר: $\beta\alpha = \alpha\beta \Leftrightarrow \beta\alpha\beta^{-1} = \alpha$, שייכים למייצב של α ב- S_9 תחת פעולת ההצמדה של S_9 על עצמה.
- מתקיים: $|(S_9)_\alpha| = \frac{|S_9|}{|[\alpha]|} = \frac{9!}{|[\alpha]|}$ ומכאן: $|[\alpha]| = [S_9 : (S_9)_\alpha] = \frac{|S_9|}{|(S_9)_\alpha|}$
- המסלול של α הוא מחלקת הצמידות שלה, אשר במקרה של S_9 מכיל את האיברים

$$|[\alpha]| = \binom{9}{4} \cdot 3! = \frac{9! \cdot 3!}{4! \cdot 5!}$$

$$\cdot |(S_9)_\alpha| = \frac{9! \cdot 4! \cdot 5!}{9! \cdot 3!} = 480 \text{ ובסה"כ:}$$

- ג. כיוון ש- X הוא איחוד זר של המסלולים שנוצרים ע"י הפעולה, מתקיים: $|X| = \sum_x |[x]|$

(כאשר נלקחים נציגי המסלולים בלבד).

כמו כן: $\forall x \in X : |[x]| \mid |G| = 14$ כלומר אורך מסלול משתייך לקבוצה: $\{1, 2, 7, 14\}$.

$$\text{ולכן: } 19 = n_1 \cdot 1 + n_2 \cdot 2 + n_3 \cdot 7 + n_4 \cdot 14$$

אם כן תיתכן פעולה בה לא תהיה נקודת שבת. למשל: $19 = 7 + 6 \cdot 2$, כלומר פעולה שתחלק את איברי הקבוצה למסלול אחד בן 7 איברים ושישה אחרים בני שניים כ"א, ובכל מקרה לא יהיה מסלול בן איבר אחד בלבד. כלומר הטענה אינה נכונה.

- ד. נשים לב כי כשמסובבים לוח 5×5 ב- 90° מקבלת תמורה a בה יש שישה עגילים בני ארבע איברים כ"א ועוד האיבר במרכז כנקודת שבת.

$$\text{מתקיים: } C_4 = \langle a \rangle = \{1, a, a^2, a^3\}$$

$g \in C_4$	$ X_g $
1	5^{25}
a	5^7
a^2	5^{13}
a^3	5^7

הטיפוס של a^3 זהה לזה של a .

הטיפוס של a^2 הוא 12 חילופים והמרכז כנקודת שבת.

בסה"כ מתקבלת הטבלה הבאה:

עפ"י משפט Burnside מספר המסלולים הוא:

$$k = \frac{1}{4} (5^{25} + 2 \cdot 5^7 + 5^{13})$$