פתרון תרגיל בית 6 בתורת החבורות
88-218 סמסטר א' תשע"ח

שאלות חימום

שאלות החימום הן שאלות קלות יותר בדרך כלל, אבל כדאי מאוד לוודא שיודעים איך לפתור אותן, אפילו בעל פה.

שאלה 1. מצאו את הסימן של התמורה

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & 2n-1 & 2n \\ 2 & 3 & 4 & \cdots & 2n & 1 \end{pmatrix} \in S_{2n}$$

פתרון. בכתיב של מכפלת מחזורים זרים, התמורה היא המחזור $(1,2,3,\ldots,2n)$, והוא מאורך זוגי. לכן הסימן הוא -1 והתמורה אי-זוגית.

שאלות רגילות

שאלה 2. תהי G חבורת-p סופית ותהי $N \lhd G$ לא טריוויאלית. הוכיחו כי $Z(G) \cap N \neq \{e\}$.

רמז: G פועלת על N על ידי הצמדה. העזרו בטיעון דומה לזה שראיתם בהרצאה בהוכחה ש-$Z(G)$ לא טריוויאלית.

פתרון. נעזר ברמז, לפיו G פועלת על N על ידי הצמדה. לפי משוואת המחלקות

$$|N| = |\mathrm{fp}| + \sum |\mathrm{orb}(x_i)|$$

כאשר fp הוא אוסף נקודות השבת (Fixed points), והסכימה היא על נציגים של המסלולים שאינם נקודות שבת.

מי הם המסלולים בפעולה? אלו הן מחלקות צמידות של G. לכן N היא איחוד זר של מחלקות צמידות של G. מי הן נקודות השבת של הפעולה? איברים שנשמרים תחת הצמדה מ-G, כלומר איברים ב-$Z(G)$.

ידוע לנו שהסדר של N הוא חזקת p, וגם שהגודל של כל מחלקות צמידות של איברים לא מרכזיים הוא חזקה חיובית של p. כלומר $|N|$ הוא סכום חזקות של p. בנוסף מחלקת הצמידות של היחידה $e \in N \cap Z(G)$ היא מגודל 1. לכן בהכרח N מכילה מחלקות צמידות נוספות מגודל 1, שכן אחרת במשוואה לעיל אגף שמאל מתחלק ב-p ואילו אגף ימין לא. מחלקות הצמידות מגודל 1 ב-N הן כאמור אלו המכילות איברים של $Z(G)$.

שאלה 3. יהי $f : G \to H$ הומומורפיזם. הוכיחו שאם G אבלית, אז $\operatorname{im} f$ אבלית. הסיקו שאם $G \cong H$ אז G אבלית אמ"מ H אבלית.

שאלה 4. עבור כל אחת מן ההעתקות הבאות קבעו והוכיחו האם היא הומומורפיזם, מונומורפיזם, אפימורפיזם או איזומורפיזם.

1. $f\colon \mathbb{Q}^* \to \mathbb{Q}^*$ המוגדרת לפי $f(x) = x^2$.
2. $f\colon \mathbb{R}^* \to \mathbb{R}_{>0}$ המוגדרת לפי $f(x) = x^4$ כאשר $\mathbb{R}_{>0}$ זו חבורת המספרים הממשיים החיוביים עם כפל רגיל.
3. $f\colon \mathbb{Z} \to \mathbb{Z}_3 \times \mathbb{Z}_6$ המוגדרת לפי $f(n) = (n \bmod 3,\, n \bmod 6)$.
4. $f\colon S_6 \to U_7 \times U_{11}$ המוגדרת לפי $f(\sigma) = (\sigma(1), \sigma(2))$.

פתרון. ההוכחות כאן לא מלאות!

1. הפונקציה f היא הומומורפיזם. אבל היא לא מונומורפיזם כי למשל $f(1) = f(-1) = 1$. היא גם לא אפימורפיזם, כי למשל $-1 \notin \operatorname{im} f$, שהרי לכל $x \in \mathbb{Q}^*$ מתקיים $x^2 > 0$.
2. הפונקציה f היא הומומורפיזם, באופן דומה לסעיף הקודם. אבל היא לא מונומורפיזם, שוב, כי למשל $f(1) = f(-1) = 1$. הפעם היא כן אפימורפיזם, כי לכל $x \in \mathbb{R}_{>0}$ קיים שורש רביעי $\sqrt[4]{x} \in \mathbb{R}^*$ שהוא ממשי שאינו אפס, ואז $f(\sqrt[4]{x}) = x$.
3. הפונקציה היא הומומורפיזם, כשההוכחה מסתמכת על כך שחיבור מודולו n מוגדר היטב. היא לא מונומורפיזם, כי הסדר של המקור גדול ממש מסדר התמונה, או למשל כי $f(0) = f(6) = ([0], [0])$. היא לא אפימורפיזם, כי $\mathbb{Z}$ ציקלית ואילו $\mathbb{Z}_3 \times \mathbb{Z}_6$ לא ציקלית, וכל התמונות של חבורה ציקלית הן ציקליות. אפשר גם להוכיח ישירות כי למשל $(1,3) \notin \operatorname{im} f$: אם n נשלח ל-$(1,3)$, אז לפי הרכיב השני $n \equiv 3 \pmod 6$, ונסיק $n \equiv 0 \pmod 3$. לא יתכן שבאותו הזמן גם $n \equiv 1 \pmod 3$.
4. הפונקציה הזו היא לא הומומורפיזם. למשל כי היחידה לא נשלחת ליחידה, או ש-$f(\mathrm{id} \cdot \mathrm{id}) \neq f(\mathrm{id}) f(\mathrm{id})$. בפרט זה לא מונומורפיזם או אפימורפיזם.

שאלה 5. יהי p ראשוני, ותהי G חבורה מסדר p^3.

1. הוכיחו שניתן ליצור את G עם תת־קבוצה בת שלושה איברים $a, b, c \in G$ (כלומר $G = \langle a, b, c\rangle$). רמז: משפט לגראנז' כמה וכמה פעמים.
2. בחרו p. תנו דוגמה מפורשת לחבורה G אבלית מסדר p^3 שאפשר ליצור עם שני איברים $a, b \in G$, אבל לא עם איבר אחד.
3. אתגר: הראו שישנה חבורה לא אבלית מסדר p^3 שאפשר ליצור עם שני איברים לפי ההדרכה הבאה: התבוננו בקבוצה (שכבר פגשנו מעל $\mathbb{R}$)
$$H(\mathbb{Z}_p) = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \middle| \, x, y, z \in \mathbb{Z}_p \right\}$$
ועל האיברים $a = \left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right), b = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. הראו כי $\left|\left\langle a, aba^{-1}b^{-1} \right\rangle\right| = p^2$, והסיקו מזה ש-$H(\mathbb{Z}_p) = \langle a, b \rangle$

פתרון.

1. כמסקנה ממשפט לגראנז' אנחנו יודעים שהסדרים האפשריים של איברים ב-G הם $\{1,p,p^2,p^3\}$. אם קיים איבר $a\in G$ מסדר p^3, אז G ציקלית ומתקיים $G=\langle a\rangle$. לכן נוכל לבחור **כל** זוג איברים $b,c\in G$, ויתקיים

$$G=\langle a\rangle\leq\langle a,b,c\rangle\leq G$$

כלומר $G=\langle a,b,c\rangle$.
אם לא קיים איבר מסדר p^3, אבל קיים איבר $a\in G$ מסדר p^2, אבל תת־החבורה $\langle a\rangle$ מכילה p^2 איברים. לכן קיים איבר $e\neq b\in G\setminus\langle a\rangle$ והסדר שלו הוא לפחות p. לכן

$$|\langle a,b\rangle|\geq|\langle a\rangle\cup\{b\}|>|\langle a\rangle|=p^2$$

כי $b\notin\langle a\rangle$. אבל הסדר של $\langle a,b\rangle$ חייב לחלק את p^3, ולכן הוא בדיוק p^3. כך נוכל לבחור כל איבר נוסף $c\in G$ ונקבל

$$G=\langle a,b\rangle\leq\langle a,b,c\rangle\leq G$$

ושוב נקבל $G=\langle a,b,c\rangle$.
אם לא קיימים איברים מסדר p^3 או p^2, אז הסדר של כל האיברים הוא p, פרט לאיבר היחידה. יהי $a\in G$ איבר מסדר p. אז $p=|\langle a\rangle|$. נבחר $e\neq b\in G\setminus\langle a\rangle$ מסדר p (ודאו שברור לכם למה קיים b כזה). אז לפי לגראנז' הסדר של תת־החבורה $\langle a,b\rangle$ מחלק את $|G|=p^3$, ובנוסף הוא חייב להיות גדול מ-p, כי $|\langle a\rangle\cup\{b\}|=p+1$. לכן $|\langle a,b\rangle|\geq p^2$. אם $|\langle a,b\rangle|=p^3$, נסיים כמו מקודם. אחרת, $|\langle a,b\rangle|=p^2$ ונוכל לבחור $e\neq c\in G\setminus\langle a,b\rangle$ מסדר p ומטיעון דומה נסיק $G=\langle a,b,c\rangle$.

2. עד כדי איזומורפיזם, אפשר לבחור רק את $\mathbb{Z}_{p^2}\times\mathbb{Z}_p$. למשל עבור $p=2$ נבחר את $G=\mathbb{Z}_4\times\mathbb{Z}_2$, ואת האיברים $a=(1,0)$, $b=(1,1)$. זה מתאים למקרה השני של הסעיף הקודם, שבו אין איבר מסדר p^3, אבל $o(a)=p^2$ ובחרנו את $b\neq(0,0)$ כך ש-$b\notin\langle a\rangle$.

3. ברור שחבורה לא אבלית לא ניתן ליצור עם איבר אחד. לפי ההדרכה נחשב כי $aba^{-1}b^{-1}=\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}$ (הוא גם איבר מסדר p). הכפל בחבורה מקיים

$$\begin{pmatrix}1&x&z\\0&1&y\\0&0&1\end{pmatrix}\begin{pmatrix}1&x'&z'\\0&1&y'\\0&0&1\end{pmatrix}=\begin{pmatrix}1&x+x'&xy'+z+z'\\0&1&y+y'\\0&0&1\end{pmatrix}$$

בתת־החבורה $\left\langle a,aba^{-1}b^{-1}\right\rangle$ ליוצרים יש במיקום $(2,3)$ רכיב 0, ולכן באינדוציה לכל איבר בתת־החבורה יש 0 במיקום $(2,3)$ (הראו שתת־החבורה איזומורפית ל-$\mathbb{Z}_p\times\mathbb{Z}_p$). אזי $b\notin\left\langle a,aba^{-1}b^{-1}\right\rangle$ ולפי הסעיף הראשון נסיק שהיא מסדר p^3. אבל $\left\langle a,aba^{-1}b^{-1}\right\rangle\subseteq\langle a,b\rangle$ ולכן a,b יוצרים את $H(\mathbb{Z}_p)$.

שאלה 6. בתרגיל הזה נראה שוב שאי אפשר לומר ששתי תמורות הן "צמודות סתם" מבלי לומר באיזו חבורה עובדים.

1. מצאו את מחלקת הצמידות של $A_4\ni(132)$.

2. תנו דוגמה לשתי תמורות שאינן צמודות ב-A_4, אבל כן צמודות ב-S_4. הוכיחו שהן גם צמודות ב-A_5. רמז: הביטו מעלה.

3. הוכיחו שאם יש זוג תמורות שאינן צמודות ב-A_n, אך כן צמודות ב-S_n, אז הן גם צמודות ב-A_{n+2}.

פתרון.

1. מנוסחת ההצמדה ב-S_n אנחנו יודעים שכל התמורות הצמודות של (132) הן מחזורים מאורך 3. אבל במקרה זה, לא כל המחזורים מאורך 3 צמודים ל-(132). בפרט, אם $\sigma \in A_4$, אז
$$\sigma\,(132)\,\sigma^{-1} = (\sigma(1), \sigma(3), \sigma(2))$$
חישוב ב-A_4 יראה כי מחלקת הצמידות היא $\{(234)\,,(143)\,,(124)\,,(132)\}$.

2. לפי החישוב בסעיף הקודם, התמורה (123) לא צמודה ל-(132) ב-A_4, אבל לפי מיון מחלקות הצמידות ב-S_n התמורות האלו צמודות ב-S_4. נחפש $\tau \in A_5$ כך ש-
$$\tau\,(132)\,\tau^{-1} = (\tau(1), \tau(3), \tau(2)) = (123)$$
אם נבחר את (23) נקבל שהתמורות צמודות, אך $(23) \notin A_5$. לכן נבחר $\tau = (45)\,(23)$ ונקבל שהן אכן צמודות, וגם ש-τ זוגית. דוגמה אחרת: מהצמדה בתמורה (14532) נקבל את (142).

3. אם $a, b \in A_n$ לא צמודות ב-A_n, אך כן צמודות ב-S_n, אז קיימת $\sigma \in S_n$ כך ש-$\sigma a \sigma^{-1} = b$. בודאי ש-$\sigma \notin A_n$ שכן הנחנו כי a, b לא צמודות ב-A_n. לכן התמורה $\sigma \cdot (n+1, n+2)$ היא זוגית (מכפלה של שתי תמורות אי זוגיות) ובהצמדה של a נקבל
$$\sigma\cdot(n+1,n+2)\,a\,(\sigma\cdot(n+1,n+2))^{-1} = (n+1,n+2)\,(n+1,n+2)\,\sigma a \sigma^{-1} = b$$
ונעזרנו בכך ש-$(n+1, n+2)$ מתחלפת עם σ ועם a, כי אין להם מספרים משותפים שהן מזיזות. לכן a, b צמודות ב-A_{n+2}.

שאלה 7. תהי G חבורה שבה לכל $x, y \in G$ מתקיים $(xy)^{2018} = x^{2018}y^{2018}$. נסמן שלוש תת־קבוצות
$$A = \left\{g^{2018} \,\middle|\, g \in G\right\}$$
$$B = \left\{g^{2017} \,\middle|\, g \in G\right\}$$
$$C = \left\{g \,\middle|\, g \in G, g^{2018} = e\right\}$$

1. הוכיחו $A, B, C \lhd G$. צריך להוכיח שהן תת־חבורות, וגם שהן נורמליות. רמז: כדאי לא לעבוד קשה ולהעזר בהומומורפיזמים.
2. הוכיחו שכל איברי A מתחלפים עם כל איברי B. באופן שקול, הוכיחו שלכל $x, y \in G$ מתקיים $x^{2018}y^{2017} = y^{2017}x^{2018}$.
3. הוכיחו שלכל $g, h \in G$ מתקיים $[g, h]^{2018\cdot 2017} = e$ כאשר $[g, h] = ghg^{-1}h^{-1}$.

פתרון.

1. רוב התשובות לסעיף זה הוכיחו "לפי הגדרה" שתת־הקבוצות בשאלה הן תת־חבורות. כלומר שהן לא ריקות, סגורות לפעולה וסגורות לפעולה. את הנורמליות הוכיחו לפי זה שהן נשמרות תחת הצמדה באיברי G.

ישנה דרך נוספת, שהיא יותר קצרה: נשים לב שההעתקה $f\colon G \to G$ המוגדרת לפי $f(g) = g^{2018}$ היא הומומורפיזם לפי הנתון בשאלה. נחשב שהגרעין של f הוא בדיוק $\ker f = C$, ולכן C היא תת־חבורה נורמלית. זהו, לא צריך יותר כלום עבור C.

נחשב גם שהתמונה של f היא $\operatorname{im} f = A$, ולכן $A \leq G$. את הנורמליות של A נוכיח לפי הצמדה. יהי $x \in G$ ויהי $a \in A$, כך ש-$a = g^{2018}$. נרצה להראות $xax^{-1} \in A$. נראה שמדובר באיבר של G בחזקת 2018 לפי

$$xax^{-1} = xg^{2018}x^{-1} = xgx^{-1}xgx^{-1} \dots xgx^{-1} = \left(xgx^{-1}\right)^{2018}$$

כלומר $xax^{-1} \in A$, ולכן $A \lhd G$.

עבור B נצטרך להתאמץ קצת יותר. נגדיר העתקה $\phi : G \to G$ לפי $\phi(g) = g^{-2017}$. נבדוק שזהו הומומורפיזם:

$$\begin{aligned}\phi(xy) = (xy)^{-2017} = \left(y^{-1}x^{-1}\right)^{2017} &= xx^{-1}\left(y^{-1}x^{-1}\right)^{2017}y^{-1}y\\ &= x\left(x^{-1}y^{-1}\right)^{2018}y = xx^{-2018}y^{-2018}y = x^{-2017}y^{-2017} = \phi(x)\phi(y)\end{aligned}$$

והתמונה שלו היא $\operatorname{im}\phi = B^{-1} = B$, כי אם $b \in B$, אז קיים g כך ש-$b = g^{2017}$, ולכן $b^{-1} = \left(g^{-1}\right)^{2017}$ (כלומר גם $b^{-1} \in B$). לכן $B \leq G$. את הנורמליות של B מוכיחים בצורה דומה להוכחת הנורמליות של A.

2. נעזר בנתון בשאלה שלכל $x, y \in G$ מתקיים $(xy)^{2018} = x^{2018}y^{2018}$ וגם לפי הסעיף הקודם $(xy)^{2017} = y^{2017}x^{2017}$ כי

$$(xy)^{2017} = \phi((xy)^{-1}) = \phi(y^{-1}x^{-1}) = \phi(y^{-1})\phi(x^{-1}) = y^{2017}x^{2017}$$

לכן

$$x^{2018}y^{2017} = xx^{2017}y^{2017} = x\,(yx)^{2017} = y^{-1}yx\,(yx)^{2017} = y^{-1}\,(yx)^{2018} = y^{2017}x^{2018}$$

כלומר $f(x)\phi(y^{-1}) = \phi(y^{-1})f(x)$, ולכן גם $f(x)\phi(y) = \phi(y)f(x)$.

3. נעזר בזהויות מהסעיף הקודם ונחשב

$$\begin{aligned}\left(ghg^{-1}h^{-1}\right)^{2018\cdot 2017} &= \left(\left(ghg^{-1}h^{-1}\right)^{2018}\right)^{2017} = \left((gh)^{2018}\left(g^{-1}h^{-1}\right)^{2018}\right)^{2017}\\ &= \left(g^{-1}h^{-1}\right)^{2018\cdot 2017}(gh)^{2018\cdot 2017}\\ &= \left(g^{-2018}h^{-2018}\right)^{2017}\left(g^{2018}h^{2018}\right)^{2017}\\ &= h^{-2018\cdot 2017}g^{-2018\cdot 2017}h^{2018\cdot 2017}g^{2018\cdot 2017}\\ &= \left(h^{-2017}\right)^{2018}\left(g^{-2018}\right)^{2017}h^{2018\cdot 2017}g^{2018\cdot 2017}\\ &= g^{-2018\cdot 2017}h^{-2018\cdot 2017}h^{2018\cdot 2017}g^{2018\cdot 2017} = e\end{aligned}$$

או שנוכיח בעזרת ההומורפיזמים f ו-ϕ. קל לראות שהם מתחלפים, כי לכל $x \in G$ מתקיים

$$f(\phi(x)) = \left(x^{-2017}\right)^{2018} = \left(x^{2018}\right)^{-2017} = \phi(f(x))$$

ולכן

$$\begin{aligned}\left(ghg^{-1}h^{-1}\right)^{2018\cdot 2017} &= \left(\left(hgh^{-1}g^{-1}\right)^{2018}\right)^{-2017} = \phi\left(f\left(hgh^{-1}g^{-1}\right)\right)\\ &= \phi\left(f\left(h\right)f\left(g\right)f\left(h^{-1}\right)f\left(g^{-1}\right)\right)\\ &= \phi\left(f\left(h\right)\right)\phi\left(f\left(g\right)\right)\phi\left(f\left(h^{-1}\right)\right)\phi\left(f\left(g^{-1}\right)\right)\\ &= \phi\left(f\left(h\right)\right)f\left(\phi\left(g\right)\right)\phi\left(f\left(h^{-1}\right)\right)\phi\left(f\left(g^{-1}\right)\right)\\ &= \phi\left(f\left(h\right)\right)\phi\left(f\left(h^{-1}\right)\right)f\left(\phi\left(g\right)\right)f\left(\phi\left(g^{-1}\right)\right)\\ &= \phi\left(f\left(h\right)f\left(h^{-1}\right)\right)f\left(\phi\left(g\right)\phi\left(g^{-1}\right)\right) = \phi\left(e\right)f\left(e\right) = e\end{aligned}$$

שאלות אתגר

אם פתרתם את שאלות האתגר, ואין לשאלה פתרון, בבקשה שלחו לי את הפתרון שלהן.

שאלה 8. יהי p ראשוני. נזכיר כי חבורה נקראת חבורת-p אם הסדר של כל איבר הוא חזקה של p. כמו כן ראינו שלחבורת-p סופית יש מרכז לא טריוויאלי. מצאו חבורת-p עם מרכז טריוויאלי.

הדרכה אפשרית (אם אתם מוצאים חבורות אחרות נשמח לשמוע): התבוננו על קבוצת המטריצות האינסופיות מעל $\mathbb{Z}_p$ מהצורה

$$\begin{pmatrix} A & 0 \\ 0 & I_\infty \end{pmatrix}$$

כאשר I_∞ היא מטריצת יחידה אינסופית, 0 היא מטריצת אפס בגודל מתאים והמטריצה $A\in GL_n(\mathbb{Z}_p)$ היא משולשית עליונה (סופית, עבור n טבעי כלשהו) עם אחדות על האלכסון. הסבירו למה כפל מטריצות עדין מוגדר כאן (זה חשוב שבכל שורה ובכל עמודה יש מספר סופי של איברים לא אפסיים), והסיקו שמתקבלת חבורה. הוכיחו שהסדר של כל איבר הוא חזקה של p וכדי להראות שהמרכז טריוויאלי העזרו בזהויות הבאות על מטריצות בלוקים סופיות:

$$\begin{pmatrix} M & 0 \\ 0 & I_n \end{pmatrix}\begin{pmatrix} I_n & I_n \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} M & M \\ 0 & I_n \end{pmatrix}, \qquad \begin{pmatrix} I_n & I_n \\ 0 & I_n \end{pmatrix}\begin{pmatrix} M & 0 \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} M & I_n \\ 0 & I_n \end{pmatrix}$$