

אלגברה מופשטת – פתרון תרגיל 3

שאלה 1

- א. מצאו את שתי הספרות האחרונות של 5353^{202} .
ב. מצאו את $5773^{862} + 2013 \pmod{80}$.

פתרון

- א. יש לחשב את הביטוי $5353^{202} \pmod{100}$ ששווה לביטוי $53^{202} \pmod{100}$. אנחנו יודעים כי סדר כל איבר a מחלק את סדר החבורה, שנסמן n , ולכן מתקיים $a^n \equiv 1 \pmod{n}$ (אפשר גם להעזר במשפט אוילר 2 כדי להגיע לאותה מסקנה). מכאן $59^{100} \equiv 1 \pmod{100}$, לכן $53^{202} \equiv (53^{100})^2 \cdot 53^2 \equiv 1 \cdot 53^2 \pmod{100}$. בחישוב ישיר אפשר למצוא כי $53^2 \equiv 9 \pmod{100}$. לכן התשובה היא 09.
- ב. נשים לב כי $2000 \equiv 0 \pmod{80}$ וגם $13 \pmod{80}$. לכן $5773 = 72 \cdot 80 + 13 \equiv 13 \pmod{80}$. צריך לחשב את הביטוי $13^{862} + 13 \pmod{80}$. לפי משפט אוילר 2 נקבל כי מפני ש- $\varphi(80) = 32$, אז $13^{32} \equiv 1 \pmod{80}$. לכן $13^{862} = 13^{26 \cdot 32 + 30} = 13^{30} \pmod{80}$. מפני ש- $13^2 \equiv 9 \pmod{80}$, נרצה למצוא הפכי של 13. ישנו פתרון למשוואה $13x \equiv 1 \pmod{80}$ אם ורק אם קיים $k \in \mathbb{Z}$ כך ש- $80k + 59x = 1$. נשתמש באלגוריתם אוקלידס כדי למצוא את x , כלומר למצוא ביטוי של $\gcd(80, 13)$ כצירוף לינארי של 13 ושל 80:
$$(80, 13) = (13, 2) = (2, 1) = 1$$
$$\begin{array}{r} 80 = 6 \cdot 13 + 2 \\ 13 = 6 \cdot 2 + 1 \end{array}$$
כלומר $1 = 13 - 6 \cdot 2 = -6 \cdot 80 + 37 \cdot 13$. נחשב $13^{-2} \equiv 37^2 \equiv 9 \pmod{80}$. ולכן $5773^{862} + 2013 \equiv 9 + 13 \equiv 22 \pmod{80}$.

שאלה 2

- א. תהי D_5 החבורה הדיהדרלית מסדר 10. תארו את כל תתי-החבורות הלא טריוויאליות של D_5 . הוכיחו כי כולן חבורות אבליות.
- ב. מצאו תתי-חבורה נורמלית לא טריוויאלית של D_5 . האם יש יותר מאחת?

פתרון

- א. נציג את החבורה בצורה הרגילה, כחבורה הנוצרת על ידי האיברים $\langle \sigma, \tau \rangle$ כאשר מתקיימים היחסים $\sigma^5 = \tau^2 = e, \tau\sigma\tau^{-1} = \sigma^{-1}$. לפי משפט לגראנז' עבור $H \leq D_5$ מתקיים כי $|H| \mid |D_5| = 10$, כלומר $|H| \in \{1, 2, 5, 10\}$. תתי-החבורות

הטריוויאליות מתקבלות במקרים ש- $|H| \in \{1, 10\}$. אחרת, הסדר H הוא ראשוני, ולכן H ציקלית, ולכן היא חבורה אבלית. כעת אפשר לבנות תת-חבורות מחזקות של איבר אחד של D_5 . בדיקה "ידינית" תראה שהרשימה היא $\{e, \sigma, \sigma^2, \sigma^3, \sigma^4\}$, $\{e, \tau\}$, $\{e, \tau\}$, $\{e, \tau\}$, $\{e, \tau\}$, $\{e, \tau\}$. האם אתם יכולים להציג כל תת-חבורה כאשר D_5 מוצגת כחבורת תמורות?
 ב. תת-החבורה הנוצרת על ידי σ היא תת-החבורה הנורמלית הלא טריוויאלית היחידה של D_5 . אפשר לראות שאם H היא תת-חבורה לא טריוויאלית אחרת, אז $\sigma H \neq H\sigma$.

שאלה 3

היו $H, K \leq G$ תת-חבורות. הגדרנו מכפלת תת-חבורות $HK = \{hk : h \in H, k \in K\}$.

- הוכיחו כי $HK = KH$ אם ורק אם $HK = KH$.
- הסיקו מהסעיף הקודם כי אם $N \triangleleft G$ תת-חבורה נורמלית, אז $HN \leq G$ תת-חבורה.
- הוכיחו כי אם $N_1, N_2 \triangleleft G$ תת-חבורות נורמליות, אז $N_1 \cap N_2 \triangleleft G$ וגם $N_1 N_2 \triangleleft G$ תת-חבורות נורמליות.

פתרון

- (\Rightarrow) נניח כי $HK = KH$. שימו לב כי הנתון $HK = KH$ **לא אומר** שלכל $h \in H, k \in K$ מתקיים $hk = kh$. מן הנתון נדע שאם $hk \in HK$, אז קיימים $h' \in H, k' \in K$ כך שמתקיים $hk = k'h'$. נראה כי HK היא תת-חבורה בעזרת הקריטריון המקוצר. יש להראות כי $\emptyset \neq HK \subseteq G$ ההכלה מתקיימת מסגירות הפעולה של G . כמו כן HK לא ריקה כי היא מכילה את איבר היחידה, שכן $e \in H$ וגם $e \in K$, ולכן $e \cdot e = e \in HK$. כעת נשאר להראות שלכל $a, b \in HK$ מתקיים $ab^{-1} \in HK$. נרצה להראות שאם $h_1 k_1, h_2 k_2 \in HK$ אז $h_1 k_1 (h_2 k_2)^{-1} \in HK$. מתקיים כי $h_1 k_1 (h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1}$, ונסמן $h_3 = h_2^{-1}$, $k_3 = k_1 k_2^{-1} \in K$. כעת לפי הנתון עבור $k_3 h_3$ קיימים $h'_3 \in H, k'_3 \in K$ כך שמתקיים $h'_3 k'_3 = k_3 h_3$. לכן $h_1 k_1 k_2^{-1} h_2^{-1} = h_1 k_3 h_3 = h_1 h'_3 k'_3$. מפני ש- $h_1 h'_3 \in H, k'_3 \in K$ קיבלנו כי $h_1 k_1 (h_2 k_2)^{-1} \in HK$, ולכן $HK \leq G$.
- (\Leftarrow) נשים לב שעבור חבורה X מתקיים $X = X^{-1} = \{a^{-1} : a \in X\}$. לכן אם

- אז $HK \leq G$, $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$ שכן גם $H^{-1} \leq G, K^{-1} \leq G$ הן תתי-חבורות.
- ב. אם $N \triangleleft G$ תתי-חבורה נורמלית, אזי מתקיים $HN = NH$. זהו בדיוק התנאי מהסעיף הקודם שדרוש כדי להוכיח כי HN תתי-חבורה.
- ג. נתון כי $N_1, N_2 \triangleleft G$, ולכן $N_1 \cap N_2 \leq G$ כי חיתוך תתי-חבורות הוא תתי-חבורה. נשאר להראות כי $N_1 \cap N_2 \triangleleft G$. יהיו $g \in G, h \in N_1 \cap N_2$. צריך להראות כי $ghg^{-1} \in N_1 \cap N_2$. מפני ש- $h \in N_1 \triangleleft G$, אז $ghg^{-1} \in N_1$ כי N_1 תתי-חבורה נורמלית. באופן דומה $ghg^{-1} \in N_2$, ולכן $ghg^{-1} \in N_1 \cap N_2$.
- נראה כי $N_1 N_2 \triangleleft G$. לפי הסעיף הקודם ידוע לנו כי $N_1 N_2$ תתי-חבורה, ונשאר להראות שהיא נורמלית. יהיו $g \in G, h \in N_1 N_2$. צריך להראות כי $ghg^{-1} \in N_1 N_2$. כיוון ש- $h \in N_1 N_2$ קיימים $h_1 \in N_1, h_2 \in N_2$ כך ש- $h = h_1 h_2$. כיוון ש- N_1 נורמלית נקבל $gh_1 g^{-1} \in N_1$ וכיוון ש- N_2 נורמלית נקבל $gh_2 g^{-1} \in N_2$. לכן $(gh_1 g^{-1})(gh_2 g^{-1}) = gh_1 h_2 g^{-1} = h \in N_1 N_2$ כפי שרצינו להראות.

שאלה 4

תארו את המחלקות השמאליות של תתי-החבורה H בחבורה G :

- א. $H = 12\mathbb{Z}, G = 3\mathbb{Z}$.
- ב. תהינה G_1, G_2 חבורות. $H = G_1 \times \{e_2\}, G = G_1 \times G_2$ כאשר e_2 הוא איבר היחידה של G_2 .
- ג. $G = U_{30}, H = \langle 13 \rangle$.

פתרון

- א. המחלקות הן $\{12\mathbb{Z}, 3+12\mathbb{Z}, 6+12\mathbb{Z}, 9+12\mathbb{Z}\}$. שימו לב כי G אבלית, ולכן H תתי-חבורה נורמלית. מכאן שכל מחלקה שמאלית $a+H$ שווה למחלקה ימנית $H+a$.
- ב. המחלקות הן מהצורה $(g_1, g_2) \cdot (G_1 \times \{e_2\})$. נראה כי קבוצת המחלקות איזומורפית ל- G_2 : $\{(g_1, g_2) \cdot (G_1 \times \{e_2\}) : g_1 \in G_1, g_2 \in G_2\}$ היא בעצם $\{(g_1 G_1 \times \{g_2\}) : g_1 \in G_1, g_2 \in G_2\} = \{(G_1 \times \{g_2\}) : g_2 \in G_2\} \cong G_2$.
- ג. ידוע לנו כי $|U_{30}| = \varphi(30) = 8$, ואפשר לחשב כי $U_{30} = \{1, 7, 11, 13, 17, 19, 23, 29\}$. תתי-החבורה H היא $\langle 13 \rangle = \{1, 13, 19, 7\}$. לפי משפט לגראנז' נקבל כי יש רק שתי מחלקות: $\langle 13 \rangle = \{1, 13, 19, 7\}, 11\langle 13 \rangle = \{11, 17, 23, 29\}$.

שאלה 5

תהי G חבורה. ראינו כי ישנה התאמה חח"ע ועל בין מחלקות שמאליות ולבין מחלקות ימניות לפי ההעתקה $\varphi: gH \mapsto Hg^{-1}$ כאשר $g \in G$ ו- $H \leq G$ תת-חבורה.

הוכיחו או הפריכו: ההעתקה $\psi: gH \mapsto Hg$ היא חח"ע ועל.

פתרון

נפריך על ידי דוגמה נגדית. נבחר $G = D_3$ החבורה הדיהדרלית מסדר 6 הנוצרת על ידי σ, τ באופן הסטנדרטי ותת-החבורה $H = \langle \tau \rangle = \{e, \tau\}$. נרצה למצוא $g_1, g_2 \in G$ כך שמתקיים $g_1H = g_2H$, אבל $Hg_1 \neq Hg_2$. כלומר למצוא $g_2^{-1}g_1 \in H$ כך ש- $g_1g_2^{-1} \notin H$. נבחר $g_1 = \sigma^{-1}\tau, g_2 = \sigma^{-1}$ ואכן $g_1 = \sigma^{-1}\tau, g_2 = \sigma^{-1}$ אבל $g_2^{-1}g_1 = \sigma \cdot \sigma^{-1}\tau = \tau \in H$ בעצם הראנו כי ψ אינה מוגדרת היטב במקרה זה.

שאלה 6

א. כתבו בכתוב מחזורים את כל האיברים מסדר 4 בחבורה S_4 .
ב. הוכיחו כי החבורות S_4 ו- D_{12} הן לא איזומורפיות, למרות ששתיהן חבורות לא אבליות מסדר 24.

פתרון

א. האיברים היחידים מסדר 4 בחבורה S_4 הם רק המחזורים מאורך 4. אפשר לבדוק ששאר האיברים בכתוב מחזורים זרים הם רק: איבר היחידה (סדר 1), תמורה המורכבת ממחזור אחד מאורך שתיים (סדר 2), תמורה המורכבת משני מחזורים מאורך שתיים (סדר 2) או תמורה המורכבת ממחזור אחד מאורך שלוש (סדר 3).
כלומר רשימת האיברים היא $(1, 2, 3, 4), (1, 2, 4, 3), (1, 3, 2, 4), (1, 3, 4, 2), (1, 4, 2, 3), (1, 4, 3, 2)$.
ב. בחבורה D_{12} יש איבר מסדר 12, אבל אין איבר מסדר זה בחבורה S_4 .

שאלה 7

עבור כל אחת מן הפונקציות הבאות הוכיחו כי היא הומומורפיזם. בדקו עבור כל פונקציה האם היא מונומורפיזם, האם היא אפימורפיזם והאם היא איזומורפיזם.

א. $f: (\mathbb{C}^*, \cdot) \rightarrow (\mathbb{C}^*, \cdot)$ המוגדרת על ידי $f(x) = x^5$.

ב. $f: (\mathbb{Q}^*, \cdot) \rightarrow (\mathbb{Q}^*, \cdot)$ המוגדרת על ידי $f(x) = x^5$.

- ג. $f: G_1 \times G_2 \rightarrow G_2 \times G_1$ כאשר $g_1 \in G_1, g_2 \in G_2$ איברי חבורות אבליות G_1, G_2 בהתאמה והפונקציה מוגדרת על ידי $f(g_1, g_2) = (g_2^{-1}, g_1)$.
- ד. $f: (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, \cdot)$ המוגדרת על ידי $f(x) = e^x$. הפונקציה הזו נקראת exp.

פתרון

- א. הפונקציה היא אפימורפיזם, אבל לא מונומורפיזם. למשל $f(1) = f(e^{\frac{2\pi i}{5}}) = 1$.
- ב. הפונקציה היא מונומורפיזם, אבל לא אפימורפיזם. למשל $\frac{1}{3}$ לא בתמונה.
- ג. הפונקציה היא איזומורפיזם. אפשר לראות כי $f^4 = id$. שימו לב כי התנאי שהחבורה G_2 היא אבלית הוא הכרחי. אחרת לא בטוח כי f מוגדרת היטב.
- ד. הפונקציה היא איזומורפיזם. האיזומורפיזם ההופכי הוא log.

שאלה 8

- א. מצאו אפימורפיזם $\varphi: (M_5(\mathbb{Q}), +) \rightarrow (\mathbb{Q}^5, +)$ כאשר \mathbb{Q}^5 היא מכפלה קרטזית של חמישה עותקים של \mathbb{Q} .

- ב. מצאו איזומורפיזם $\varphi: G \rightarrow \mathbb{C}^*$ כאשר $G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R}, a^2 + b^2 > 0 \right\}$ שהוכחתם בתרגיל 1 שהיא חבורה.

פתרון

- א. נשים לב כי $(M_5(\mathbb{Q}), +) \cong (\mathbb{Q}^{25}, +)$ לפי איזומורפיזם שמסדר כל אחד מאיברי מטריצה ששייכת ל- $M_5(\mathbb{Q})$ בשורה מאורך 25, כלומר וקטור ב- \mathbb{Q}^{25} . הוכיחו כי העתקה של מכפלה קרטזית $G_1 \times \dots \times G_n$ למכפלה קרטזית $G_1 \times \dots \times G_k$ עבור $k \leq n$ כשברכיב i היא העתקת הזהות של G_i היא הומומורפיזם על. כלומר יש להגדיר את ההעתקה $f(a_1, a_2, \dots, a_{25}) = (a_1, a_2, a_3, a_4, a_5)$ ולבדוק שהיא אכן אפימורפיזם.

- ב. נגדיר את האיזומורפיזם $\varphi: G \rightarrow \mathbb{C}^*$ לפי $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + bi$. ברור כי זו

פונקציה חח"ע ועל. נשאר להראות כי זהו הומומורפיזם: יהיו $M_1, M_2 \in G$ ונרצה להראות כי $\varphi(M_1 M_2) = \varphi(M_1) \varphi(M_2)$. נניח כי

$$\begin{aligned}
 & \text{אז נקבל כי } M_1 = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, M_2 = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \\
 \varphi(M_1 M_2) &= \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix}\right) = \\
 & ac-bd + (ad+bc)i = (a+bi)(c+di) = \varphi(M_1)\varphi(M_2)
 \end{aligned}$$

שאלת אתגר

יהיו תמורות $\sigma, \tau \in S_n$ כך שמתקיים $\sigma = \tau^2$, אז נקרא ל- τ **שורש** של σ . מצאו תנאי מספיק והכרחי שקובע האם לתמורה נתונה $\sigma \in S_n$ קיים שורש. אם קיים שורש לתמורה, איך אפשר למצוא אותו?

פתרון

(מבוסס על התשובה <http://math.stackexchange.com/a/266605>)

כל תמורה היא מכפלה של מחזורים זרים $\tau = c_1 c_2 \dots c_k$. מפני שמחזורים זרים מתחלפים נקבל כי $\tau^2 = c_1 c_2 \dots c_k c_1 c_2 \dots c_k = c_1^2 c_2^2 \dots c_k^2$. מכאן, שלתמורה יהיה שורש אם היא מכפלה של מחזורים ריבועיים זרים (כמו c_i^2).

כעת צריך לבדוק מתי מחזור יהיה ריבועי. נניח כי אורך המחזור $c = (i_1 i_2 \dots i_m)$ הוא m . בדקו שאם m הוא אי זוגי, אז גם c^2 הוא מאורך m . העזרו בכך ש- $(m, 2) = 1$. אם m זוגי, אז נקבל כי $c^2 = (i_1 i_3 \dots i_{m-1})(i_2 i_4 \dots i_m)$, מכפלה של שני מחזורים זרים מאורך $\frac{m}{2}$.

סך הכל התנאי הוא שלתמורה יש שורש אם ורק אם בהצגה של התמורה למחזורים זרים, לכל m זוגי מספר המחזורים מאורך m הוא זוגי. במקרה ולתמורה σ יש שורש, נוכל לפי הקריטריון הנ"ל למצוא שורש: נציג את σ כמכפלת מחזורים זרים $d_1 d_2 \dots d_k$. לכל מחזור d_i מאורך m אי זוגי נוכל למצוא את השורש שלו $\sqrt{d_i} = (i_1 i_{(m+1)/2} i_2 i_{(m+3)/2} \dots i_m i_{(m-1)/2})$ מאורך m זוגי, יהיה עוד מחזור $d'_i = (j_1 j_2 \dots j_m)$ מאורך m בהצגה של σ ונוכל לבנות את השורש $\sqrt{d_i d'_i} = (i_1 j_1 i_2 j_2 \dots i_m j_m)$.

שאלת אתגר

הוכחתם בהרצאה את המסקנה הבאה ממשפט לגראנז': תהי G חבורה סופית, ויהיו $K \leq H \leq G$ תתי-חבורות, אזי $[G:K] = [G:H][H:K]$.

כעת הוכיחו את אותה תוצאה כאשר מניחים רק ש- K תת חבורה מאינדקס סופי ב- G . כלומר, מבלי להניח ש- G סופית, ומבלי להניח סופיות של H .

פתרון

ראשית יש להראות כי אם $[G:K]$ סופי, אז גם $[G:H]$ ו- $[H:K]$ סופיים. אחרי שמוכיחים זאת, אפשר להניח כי $G = \bigcup_{i=1}^n g_i H$ איחוד זר של מחלקות וגם $H = \bigcup_{j=1}^m h_j K$ איחוד זר של מחלקות כי מניחים $[G:H] = n, [H:K] = m$. כדי להוכיח את הדרוש מספיק להראות ש- $G = \bigcup_{i=1}^n \bigcup_{j=1}^m g_i h_j K$ ושזהו איחוד זר, שכן אז נקבל כי $[G:K] = mn$. נוכיח תחילה את השוויון. ברור שאגף ימין מוכל באגף שמאל G , ולכן נראה רק את ההכלה בכיוון ההפוך.

יהי $g \in G$, אזי מהשוויון $G = \bigcup_{i=1}^n g_i H$ נקבל שקיים $1 \leq i \leq n$ וקיים $h \in H$ כך ש- $g = g_i h$. כעת מפני ש- $h \in H$ ומהשוויון $H = \bigcup_{j=1}^m h_j K$, קיים $1 \leq j \leq m$ כך ש- $h = h_j k$. כך נקבל כי $g = g_i h \in g_i h_j K$ וסיימנו להוכיח את ההכלה הדו־צדדית.

כעת יש להוכיח כי האיחוד זר (זה החלק היותר קשה). כזכור, כל שתי מחלקות או שמתלכדות או שהן זרות. נניח $g_i h_j K = g_{i_2} h_{j_2} K$ ונראה בהכרח $g_{i_1} = g_{i_2}, h_{j_1} = h_{j_2}$. מהשוויון $g_i h_j K = g_{i_2} h_{j_2} K$ נקבל כי $g_i h_j \in (g_{i_2} h_{j_2})^{-1} g_i h_j K \leq H$. כיוון ש- $g_i^{-1} g_{i_2} \in H$ ו- $h_j^{-1} h_{j_2} \in H$ (הראו איך) כי $g_i^{-1} g_{i_2} \in H$ ומכאן נסיק (הראו איך) כי $g_i = g_{i_2}$. ולכן בהכרח $g_i = g_{i_2}$ שכן עבור $i_1 \neq i_2$ מתקיים כי $g_{i_1} \cdot g_{i_2}^{-1} \in H$ שייכים למחלקות שונות, שהן זרות. כעת מפני ש- $g_i h_j \in (g_{i_2} h_{j_2})^{-1} g_i h_j K \leq H$, ומן השלב האחרון קיבלנו כי $g_i^{-1} g_{i_2} = e$ (עבור e איבר היחידה), נקבל כי $h_j^{-1} g_{i_2}^{-1} g_i h_{j_2} = h_j^{-1} h_{j_2} \in K$ וטיעון דומה עבור H נקבל כי $h_{j_2} \in h_{j_1} K$. מפני ש- $H = \bigcup_{j=1}^m h_j K$ הוא איחוד זר, נקבל כי $h_{j_1} = h_{j_2}$ כדרוש.

בהצלחה!