

פתרון תרגיל בית 4 במבנים אלגבריים

89-214 סמסטר א' תשע"ז

הוראות בהגשת הפתרון יש לרשום בכל דף שם מלא, מספר ת"ז ומספר קבוצת תרגול. תאריך הגשת התרגיל הוא בתרגול בשבוע המתחיל בתאריך י"ח כסלו ה'תשע"ז, 18.12.2016.

שאלות חימום

שאלות החימום הן שאלות שאינן להגשה, והן בדרך כלל קלות יותר. אבל כדאי מאוד לוודא שידועים איך לפתור אותן, אפילו בעל פה.

שאלה 1. כמה תת-חבורות יש לחבורה \mathbb{Z}_{30} ? בכמה מהן יש איבר מסדר 2? פתרון. מדובר בחבורה ציקלית סופית, ולכן קיימת לה תת-חבורה יחידה מכל סדר שמחלק את 30. כלומר יש לה שמונה תת-חבורות, מן הסדרים $\{1, 2, 3, 5, 6, 10, 15, 30\}$. יש איבר מסדר 2 בתת-החבורה אם ורק אם תת-החבורה מסדר זוגי.

שאלה 2. מצאו איבר מסדר 6 בחבורה S_5 . רמז: מצאו איבר מסדר 2 ב- S_2 ואיבר מסדר 3 ב- S_3 .

פתרון. האיברים מסדר 6 בחבורה S_5 הם בדיוק התמורות שניתן לרשום כמכפלה של מחזורים זרים מאורך 2 ומאורך 3. למשל התמורה (12)(345).

שאלה 3. תהי G חבורה. יהיו $a, b \in G$ איברים שמתחלפים (כלומר $ab = ba$). הוכיחו כי $\langle a, b \rangle$ חבורה אבלית.

פתרון. ראינו שבתת-החבורה $\langle a, b \rangle$ כל איבר הוא מילה סופית באותיות $\{a, a^{-1}, b, b^{-1}\}$. מפני ש- $ab = ba$, אז כל מילה כזו אפשר להציג כ- $a^i b^j$ עבור $i, j \in \mathbb{Z}$. יהיו שני איברים $a^i b^j, a^k b^l \in \langle a, b \rangle$ ומתקיים

$$a^i b^j a^k b^l = a^{i+k} b^{j+l} = a^k b^l a^i b^j$$

כי a ו- b מתחלפים. כלומר כל זוג איברים ב- $\langle a, b \rangle$ מתחלף, ולכן זו חבורה אבלית.

שאלה 4. מצאו את הסימן של התמורה

$$\begin{pmatrix} 1 & 2 & 3 & \dots & 2n-1 & 2n \\ 2 & 3 & 4 & \dots & 2n & 1 \end{pmatrix}$$

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

שאלות להגשה

שאלה 5. חשבו את האינדקסים של תת-החבורות הבאות:

א. $[\mathbb{Z} \times \mathbb{Z} : \langle (1, 1) \rangle]$. רמז: מצאו קבוצה אינסופית של מחלקות שונות.

ב. $[2\mathbb{Z} \times S_3 : 6\mathbb{Z} \times \langle \text{id} \rangle]$.

פתרון.

א. נראה ש- $\{(0, n) + \mathbb{Z} \times \mathbb{Z}\}$ היא קבוצה אינסופית של מחלקות שונות. אם

$$(0, n) + \mathbb{Z} \times \mathbb{Z} = (0, m) + \mathbb{Z} \times \mathbb{Z}$$

זה אומר ש- $\langle (1, 1) \rangle - (0, n) - (0, m) \in \langle (1, 1) \rangle$. כלומר ש- $(k, k) = (0, n - m)$ לאיזשהו $k \in \mathbb{Z}$. לכן $k = 0 = n - m$ ולכן $n = m$. כלומר עבור $n \neq m$ מדובר במחלקות שונות. לכן $[\mathbb{Z} \times \mathbb{Z} : \langle (1, 1) \rangle] = \infty$ (ודאו שאתם יודעים למה לא יתכן שיש יותר מ- \aleph_0 מחלקות שונות).

ב. אינדקס של תת־חבורות הוא כפלי (הוכיחו!). כלומר אם $K \leq H \leq G$, אז

$$[G : K] = [G : H] [H : K]$$

בפרט נקבל

$$[2\mathbb{Z} \times S_3 : 6\mathbb{Z} \times \langle \text{id} \rangle] = [2\mathbb{Z} \times S_3 : 6\mathbb{Z} \times S_3] [6\mathbb{Z} \times S_3 : 6\mathbb{Z} \times \langle \text{id} \rangle]$$

ולכן נוכל לחשב בנפרד. המחלקות השמאליות של $6\mathbb{Z} \times S_3$ בחבורה $2\mathbb{Z} \times S_3$ הן

$$\{(0, \text{id}) (6\mathbb{Z} \times S_3), (2, \text{id}) (6\mathbb{Z} \times S_3), (4, \text{id}) (6\mathbb{Z} \times S_3)\}$$

וכמובן שיש העתקה חח"ע ועל למחלקות השמאליות של $6\mathbb{Z}$ -ב- $2\mathbb{Z}$. באופן דומה, את האינדקס של $6\mathbb{Z} \times \langle \text{id} \rangle$ -ב- $6\mathbb{Z} \times S_3$ אפשר לחשב לפי האינדקס של $\langle \text{id} \rangle$ -ב- S_3 , שהוא 6. לכן האינדקס המבוקש הוא $3 \cdot 6 = 18$.

שאלה 6. חשבו בעזרת משפט אוילר:

א. שתי הספרות האחרונות של 543^{3838} .

ב. $89^{214} \pmod{91}$.

הערה. ניתן להעזר בנוסחה הבאה לחישוב פונקציית אוילר של מספר שלם n :

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

כאשר p_1, \dots, p_k המספרים הראשוניים המחלקים את n .

פתרון.

א. יש לחשב את הביטוי מודולו 100. לאחר חישוב נקבל $\varphi(100) = 40$. לכן אם מספר שלם a זר ל-100, לפי משפט אוילר

$$a^{\varphi(100)} \equiv a^{40} \equiv 1 \pmod{100}$$

לכן מפני ש- $(43, 100) = 1$,

$$543 \equiv 43 \pmod{100}$$

$$543^{3838} \equiv 43^{40 \cdot 96 - 2} \equiv 1^{96} \cdot 43^{-2} \pmod{100}$$

ונותר לנו למצוא הופכי כפלי של 43 בחבורה U_{100} . כלומר רוצים למצוא מספר x שמקיים

$$43x \equiv 1 \pmod{100}$$

לפי אלגוריתם אוקלידס המורחב נקבל $x = 7$ (חשבו!), ולכן

$$543^{3838} \equiv 43^{-2} \equiv 7^2 \equiv 49 \pmod{100}$$

וקיבלנו ששתי הספרות האחרונות הן 49.

ב. באופן דומה לסעיף הקודם, נחשב

$$\varphi(91) = 91 \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{13}\right) = 72$$

ושוב נוכל להשתמש במשפט אוילר כי $(89, 91) = 1$,

$$89^{214} \equiv 89^{3 \cdot 72 - 2} \equiv 89^{-2} \pmod{91}$$

בעזרת אלגוריתם אוקלידס המורחב (חשבו!) נמצא את ההופכי הכפלי של 89 בחבורה U_{91} , שהוא 45. לכן

$$89^{-2} \equiv 45^2 \equiv 23 \pmod{91}$$

שאלה 7. תהי G חבורה. יהיו $a, b \in G$ איברים מסדר אי זוגי, כך ש- $\langle a \rangle \cap \langle b \rangle = \{e\}$ וגם $ab = ba$.

הוכיחו כי $o(a^2b^2) = [o(a), o(b)]$. כלומר שהסדר של a^2b^2 שווה לכפולה המשותפת המזערית של הסדרים $o(a)$ ו- $o(b)$.

פתרון. ראינו שאם a איבר מסדר סופי, אז את הסדר של חזקה של האיבר a^k ניתן לחישוב מהסדר של a לפי הנוסחה

$$o(a^k) = \frac{o(a)}{(o(a), k)}$$

בפרט, עבור $k = 2$, אם $o(a)$ אי זוגי, נקבל

$$o(a^2) = \frac{o(a)}{(o(a), 2)} = o(a)$$

כמובן שגם $o(b^2) = o(b)$. לכן מספיק להוכיח

$$o(a^2b^2) = [o(a^2), o(b^2)]$$

וודאו שאתם מבינים למה אפשר גם להסתפק בהוכחת $(o(ab) = [o(a), o(b)])$. נסמן $d = [o(a^2), o(b^2)]$ ו- $d' = o(a^2b^2)$. נוכיח כי $d' | d$ וגם $d | d'$ ונסיק $d' = d$. לפי הגדרה $o(a^2) | d$ ולכן $a^{2d} = e$. באותו אופן, מפני ש- $d | d'$ נקבל $b^{2d'} = e$. כעת נשתמש בנתון ש- $ab = ba$, כדי להראות

$$(a^2b^2)^d = a^{2d}b^{2d} = e \cdot e = e$$

לכן $o(a^2b^2) | d$, כלומר $d' | d$.

בכיוון השני, מפני ש- $d' = o(a^2b^2)$,

$$a^{2d'}b^{2d'} = (a^2b^2)^{d'} = e$$

ולכן $a^{2d'} = b^{-2d'} \in \langle b \rangle$. כלומר $a^{2d'} \in \langle b \rangle$ אבל נתון $\langle a \rangle \cap \langle b \rangle = \{e\}$ ומפני שברור ש- $a^{2d'} \in \langle a \rangle$, נסיק $a^{2d'} = e$. באופן דומה מראים $b^{2d'} = e$. לכן $o(a^2) | d'$ וגם $o(b^2) | d'$ ולכן $d = [o(a^2), o(b^2)] | d'$. כלומר $d = d'$, כדרוש.

שאלה 8. תהי G חבורה, ויהיו $H, K \leq G$ תת-חבורות.

- א. הוכיחו שאם H ו- K סופיות כך ש- $(|H|, |K|) = 1$, אז $H \cap K = \{e\}$.
- ב. נקרא לתת-חבורה של G נאותה אם היא מוכלת ממש ב- G . הוכיחו ש- G אינה איחוד של שתי תת-חבורות נאותות. כלומר שאם $G = H \cup K$, אז $G = H$ או $G = K$.
- ג. תנו דוגמה לחבורה שהיא איחוד של שלוש תת-חבורות נאותות שלה. רמז: אפשר לבחור חבורה מסדר 4.

פתרון. א. יהי איבר $x \in H \cap K$. בפרט $x \in H$ וגם $x \in K$. לפי מסקנה ממשפט לגראנז' מתקיים $x^{|H|} = e$ וגם $x^{|K|} = e$, ולכן $o(x)$ מחלק גם את $|H|$ וגם את $|K|$. מן הנתון, המחלק המשותף המירבי של $|H|$ ו- $|K|$ הוא 1, ואילו סדר של איבר הוא לפחות 1, ולכן $o(x) = 1$. לכן $x = e$, כי זה האיבר היחיד מסדר 1.

אפשר להוכיח גם בעזרת איפיון הממ"מ כצירוף לינארי, לפיו קיימים $s, t \in \mathbb{Z}$ כך ש- $s|H| + t|K| = 1$. לכן

$$x = x^{s|H|+t|K|} = \left(x^{|H|}\right)^s \left(x^{|K|}\right)^t = e^s \cdot e^t = e$$

כלומר $x = e$. לסיכום קיבלנו כי $H \cap K = \{e\}$.

- ב. אם $H \subseteq K$, כאשר H ו- K תת-חבורות נאותות, אז בודאי $H \cup K = K \neq G$. לכן ניתן להניח ש- H לא מוכלת ב- K , ובאופן דומה נניח ש- K לא מוכלת ב- H . יהיו $h \in H \setminus K$ ו- $k \in K \setminus H$. אם נניח בשלילה ש- $G = H \cup K$, אז $H \cup K$ חבורה, ולכן סגורה לפעולה. בפרט, $hk \in H \cup K$ כי h ו- k שייכים לאיחוד. נשים לב ש- H חבורה, ולכן $h^{-1} \in H$. אם $hk \in H$, אז גם

$$h^{-1}hk = k \in H$$

וזה לא יתכן לפי בחירת k . אבל אם $hk \in K$, אז מפני ש- $k^{-1} \in K$ נקבל

$$hkk^{-1} = h \in K$$

וגם זה לא יתכן. לכן $hk \notin H \cup K$, וזו סתירה לכך ש- $G = H \cup K$.

- ג. אפשר לבחור את $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. נבחר את שלוש תת-החבורות $\langle (1, 0) \rangle$, $\langle (0, 1) \rangle$ ו- $\langle (1, 1) \rangle$, שכל אחת מהן היא מסדר 2, ולכן הן נאותות. קל לראות שהאיחוד שלהן הוא G , כי ב- G יש שלושה איברים לא טריוויאלים וכל אחד מהם נמצא בדיוק באחת מתת-החבורות האלו.

שאלה 9. יהי p ראשוני, ותהי G חבורה מסדר p^2 .

- א. הוכיחו שניתן ליצור את G עם תת-קבוצה בת שני איברים. רמז: משפט לגראנז' כמה פעמים.
- ב. בחרו p . תנו דוגמה מפורשת ל- G לא ציקלית מסדר p^2 , ולשני איברים $a, b \in G$ ש- $G = \langle a, b \rangle$.

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

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

כלומר $G = \langle a, b \rangle$. אם לא קיים איבר מסדר p^2 , אז הסדר של כל האיברים הוא p , פרט לאיבר היחידה. יהי $c \in G$ איבר מסדר p . אז $|\langle c \rangle| = p$, כי הסדר של תת-החבורה הציקלית שאיבר יוצר הוא הסדר של האיבר. נבחר $d \in G \setminus \langle c \rangle$ מסדר p (ודאו שברור לכם למה קיים d כזה). אז לפי לגראנז' הסדר של תת-החבורה $\langle c, d \rangle$ מחלק את $|G| = p^2$, ובנוסף הוא חייב להיות גדול מ- p , כי $|\langle c \rangle \cup \{d\}| = p+1$. לכן $|\langle c, d \rangle| = p^2$. כלומר $G = \langle c, d \rangle$, כדרוש.

ב. עד כדי איזומורפיזם, אפשר לבחור רק את $\mathbb{Z}_p \times \mathbb{Z}_p$. למשל אפשר לבחור את $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, ואת האיברים $a = (1, 0)$, $b = (1, 1)$, ששניהם מסדר 2.

שאלות רשות

את שאלות הרשות אין חובה לפתור, אבל אם פתרתם אותן, בבקשה צרפו את הפתרון שלהן.
שאלה 10. נקרא למטריצה M מטריצת תמורה אם היא מטריצה שכל האיברים בה הם אפסים ואחדות, ושכל שורה ובכל עמודה יש בדיוק פעם אחת 1. למשל

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

היא מטריצת תמורה בגודל 4×4 . הוכיחו שאוסף מטריצות התמורה בגודל $n \times n$ הוא חבורה עם הפעולה של כפל מטריצות. התאימו לכל איבר $\sigma \in S_n$ מטריצת תמורה M_σ באופן טוב (כלומר התאמה חח"ע ועל ששומרת על הפעולה), והוכיחו שהסימן של σ הוא הדטרמיננטה של M_σ .

שאלה 11. תהינה $\sigma, \tau \in S_n$ תמורות כך שמתקיים $\sigma = \tau^2$. במקרה זה נאמר כי τ היא שורש של σ . מצאו תנאי מספיק והכרחי שקובע האם לתמורה נתונה $\sigma \in S_n$ יש שורש. אם קיים שורש, איך אפשר לחשב אותו מפורשות?

פתרון. מבוסס על התשובה בקישור <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

$$\tau^2 = c_1 c_2 \dots c_k c_1 c_2 \dots c_k = c_1^2 c_2^2 \dots c_k^2$$

כלומר לתמורה יהיה שורש אם היא מכפלה של ריבועי מחזורים זרים, כמו c_i^2 . כעת צריך לבדוק מתי מחזור הוא ריבועי. נניח כי המחזור $c = (i_1 i_2 \dots i_m)$ הוא מחזור מאורך m . בדקו שאם m הוא אי זוגי, אז גם c^2 הוא מחזור מאורך m . אפשר להעזר בכך ש- $(m, 2) = 1$. אם m זוגי נקבל כי

$$c^2 = (i_1 i_3 \dots i_{m-1}) (i_2 i_4 \dots i_m)$$

שהיא מכפלה של שני מחזורים זרים מאורך $\frac{m}{2}$.

בסך הכל קיבלנו 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 התיאור הזה למצוא את השורש: 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 בתור

$$\sqrt{d_i} = (i_1 i_{(m+3)/2} i_2 i_{(m+5)/2} \dots i_{(m-1)/2} i_m i_{(m+1)/2})$$

כאשר האינדקסים נקבעים מודולו m , ולכל מחזור מאורך m זוגי, יהיה מחזור $d'_i = (j_1 j_2 \dots j_m)$ מאורך m בהצגה של σ ונוכל לבנות את השורש

$$\sqrt{d'_i} = (i_1 j_1 i_2 j_2 \dots i_m j_m)$$

בהצלחה!