פתרון תרגיל בית 3

27 בנובמבר 2012

4.2.11 נסמן ב־A_4 את תת־החבורה של S_4 הכוללת, מלבד תמורת הזהות, את התמורות שיש להן נקודת שבת אחת, ואת אלו המחליפות שני זוגות של ערכים. הוכח שזו אכן תת־חבורה. מה האינדקס שלה?

פתרון דרך א': נרשום את כל איברי A_4.

$$A_4 = \left\{ \begin{array}{cccc} id & (123) & (132) & (124) \\ (142) & (134) & (143) & (234) \\ (243) & (12)(34) & (13)(24) & (14)(23) \end{array} \right\}$$

מצאנו כאן 12 איברים. ניתן לבדוק ידנית שהפעולה סגורה (בסך הכל 144 זוגות לבדוק) ושיש הופכי. ניתן להראות כי על ידי כפל ב־(12) ניתן להגיע לכל שאר החבורה, ולכן האינדקס הוא $[S_4 : A_4] = 2$.
דרך ב': נשים לב כי כל תמורה ב־A_4 ניתן לכתוב כמכפלה של מספר זוגי של חילופים (מחזורים מאורך 2). בדיקה תראה כי אין עוד תמורות שכאלה חוץ מאלו שכבר מצאנו, וברור כי הפעולה סגורה בקבוצה שכזו. לפיכך זו תת־חבורה. החלוקה לקוסטים היא בבירור חלוקה בין האיברים שאורכם בחילופים הוא זוגי, לבין אלו שהוא אי־זוגי. לפיכך $[S_4 : A_4] = 2$. □

4.3.2 אם $a \in H \leq G$ אז הסדר של a ב־H שווה לסדר שלו ב־G.

פתרון נביט ב־$\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$. זו תת־חבורה של H, ולכן גם תת־חבורה של G. אנו הגדרנו סדר של איבר כעוצמת החבורה $\langle a \rangle$, ולכן זה טריוויאלי.
בחוברת התרגילים, סדר של איבר מוגדר בצורה אחרת,[1] אך הטיעון הוא דומה. $\langle a \rangle \subseteq H \cap G$, ולכן לא יכול להיות שקיים n_G כך שב־G $a^{n_G} = 1$ אבל לא ב־H או להיפך. מכאן עולה כי כל הפתרונות של המשוואה $a^n = 1$ הם זהים, בין אם נעבוד ב־H או ב־G. בפרט הפתרון החיובי־ממש הנמוך ביותר הוא זהה. □

4.3.8 אם $x, y \in G$ מתחלפים ו־$(o(x), o(y)) = 1$, אז $o(xy) = o(x)\,o(y)$.

פתרון יהיו $x, y \in G$ מתחלפים. אזי ניתן להוכיח באינדוקציה כי $(xy)^n = x^n y^n$. מכאן ברור ש־$(xy)^{o(x)o(y)} = x^{o(x)o(y)} y^{o(x)o(y)} = 1 \cdot 1 = 1$. לנו נותר להראות כי $o(x)\,o(y)$ הוא מינימלי. ניזכר כעת כי $(o(x), o(y)) = 1$. נניח כי קיים n כך ש־$(xy)^n = x^n y^n = 1$. אזי $x^n = y^{-n}$. לכן הסדר של x^n שווה לסדר של y^{-n}, אך הסדר של y^{-n} שווה לסדר של y^n (כי $y^{nk} = 1$ א.ס.ם. $y^{-nk} = 1$). ביחד מצאנו כי הסדר של x^n שווה לסדר של y^n. ברור ש־$o(x^n) \mid o(x)$. כמו כן $o(y^n) \mid o(y)$.

[1] הגדרה 4.3.1.

בהתחשב בכך ש־$o(x^n) = o(y^n)$, אנו מצאנו כאן מחלק משותף של המספרים הזרים $o(x), o(y)$. המחלק המשותף האפשרי היחיד הוא אם כן $o(x^n) = 1$. לפיכך $x^n = 1$, ו־$n \mid o(x)$. באופן דומה מראים כי $n \mid o(y)$. לפי שני טיעונים אלו יחדיו, מתקיים $n \mid [o(x), o(y)]$. מכיוון שהם זרים, הכפולה המשותפת הקטנה ביותר שלהם היא מכפלתם, ומצאנו כי $n \mid o(x)\, o(y)$. מכאן ברור שאכן $o(x)\, o(y)$ הוא מינימלי, כמבוקש. □

4.3.10 תהי $G = \{a_1, \ldots, a_n\}$ חבורה אבלית. נסמן $b = a_1 a_2 \cdots a_n$.

1. הוכיחו: $b^2 = 1$.
2. אם יש איבר יחיד מסדר 2, הוא שווה ל־b.
3. בכל חבורה אבלית מסדר זוגי יש איבר מסדר 2.
4. אם יש יותר מאיבר אחד מסדר 2, אז $b = 1$.
5. אם G מסדר אי־זוגי אז $b = 1$.

פתרון

1. לכל אחד מהאיברים ב־G יש הפיך, כי היא חבורה. נסמן על ידי σ את התמורה המעבירה כל איבר להופכי לו. נשתמש בכך שהחבורה אבלית, ונרשום מחדש את b כדלהלן:

$$b = a_{\sigma(n)} a_{\sigma(n-1)} \cdots a_{\sigma(1)}$$

ואז יתקיים

$$\begin{aligned} b^2 &= (a_1 a_2 \cdots a_n) \cdot \left(a_{\sigma(n)} a_{\sigma(n-1)} \cdots a_{\sigma(1)}\right) \\ &= a_1 a_2 \cdots a_{n-1} \left(a_n a_{\sigma(n)}\right) a_{\sigma(n-1)} \cdots a_{\sigma(1)} \\ &= a_1 a_2 \cdots a_{n-1} \cdot 1 \cdot a_{\sigma(n-1)} \cdots a_{\sigma(1)} = \cdots = 1 \end{aligned}$$

כמבוקש.

2. אנו נזכור כי החבורה אבלית, ולכן בלי הגבלת הכלליות אנו יכולים לסדר מחדש את האינדקסים של איברי G. אנו נמספר את 1 על ידי a_1, ואת האיבר היחיד מסדר 2 על ידי a_2. אזי a_1, a_2 הם הפתרונות היחידים של המשוואה $x^2 = 1$. אם כן, ל־a_3 יש איזה איבר הופכי השונה ממנו, שאיננו קודם לו. נמספר איבר זה a_4. נמשיך באופן רקורסיבי, באותה הדרך: נניח שמספרנו את כל האיברים עד האיבר ה־$2k-1$. אזי האיבר ההופכי ל־a_{2k-1} איננו מופיע לפניו (לפי הבניה). כך ניתן למספרו a_{2k}. בסיכומו של התהליך אנו נקבל את המשוואה

$$\begin{aligned} b &= a_1 a_2 a_3 a_4 \cdots a_{2n-1} a_{2n} = 1 \cdot a_2 \cdot a_3 \cdot a_3^{-1} \cdots a_{2n-1} \cdot a_{2n-1}^{-1} \\ &= 1 \cdot a_2 \left(a_3 a_3^{-1}\right) \cdots \left(a_{2n-1} a_{2n-1}^{-1}\right) = 1 \cdot a_2 \cdot 1 \cdots 1 = a_2 \end{aligned}$$

בסיכומו של דבר מצאנו $b = a_2$, כמבוקש.

3. תהי G אבלית. ברור כי $B = \{g \in G \mid g \neq g^{-1}\}$ היא מעוצמה זוגית, כי $g \in B$ א.ס.ם. $g^{-1} \in B$, ורק כאשר הם שני איברים שונים. לכן חבורה היא מסדר זוגי א.ס.ם. הקבוצה $H = G \setminus B$ היא מסדר זוגי. התנאי בהגדרת B הוא שקול לתנאי $g^2 \neq 1$ או לתנאי g מסדר שאיננו מחלק את 2. לכן $H = \{g \in G \mid o(g) \in \{1,2\}\}$. קל לראות כי H חבורה. כידוע, בחבורה יש איבר יחיד מסדר 1, הוא איבר היחידה. ביחד אנו מקבלים כי הסדר של G הוא הסכום $|B| + |\{g \in G \mid o(g) = 2\}| + 1$. עד כה הראנו כי המחובר הראשון הוא אי־זוגי, והמחובר האחרון הוא זוגי. מכאן נובע שהמחובר האמצעי הוא אי־זוגי, ובפרט איננו 0. לכן יש לפחות איבר אחד g בחבורה מסדר זוגי שהסדר של g הוא 2.

4. נמשיך את הסימונים מהסעיף הקודם. לכל איבר ב־B קיים איבר הפיך, השונה ממנו (כי אחרת $x^2 = 1$ ו־$x \in H$). כמובן האיבר הזה יחיד. אנו נסדר את האיברים האלה זוגות זוגות של הפיכים, כפי שעשינו בסעיף 2, ונקבל שמכפלתם היא מכפלת 1־ים, ולכן היא 1 בעצמה.
כעת נעבור לחלק השני, H. ניתן להראות בקלות כי $H \leq G$.
תהי $A \subseteq H$ קבוצה יוצרת מינימלית של H, קרי: קבוצה שכל איברי H הם מכפלות סופיות של איבריה, אבל לא ניתן להשמיט ממנה אף איבר מאיבריה בלא לאבד איברים ב־H.[2] נסמן את איברי A כך: $A = \{a_1, \ldots, a_n\}$. לפי התכונה של A, כל איבר ב־H הוא מהצורה $a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n}$ עבור $i_j = 0, 1$ לכל $1 \leq j \leq n$.
נראה כי ההצגה על ידי הסדרה $i_1, \ldots, i_n$ היא יחידה. נניח בשלילה כי קיימות שתי הצגות שונות כאלה, $\hat{i_1}, \ldots, \hat{i_n}$ ו־$\tilde{i_1}, \ldots, \tilde{i_n}$. אם כך, מתקיים שויון לא טריויאלי בין איברי A. ניתן לחלץ משויון זה כי אחד האיברים ב־A הוא מכפלה של איברים אחרים ב־A, ובסתירה למינימליות A. אם כן, הראנו כי ההצגה הנ"ל היא יחידה.
מצאנו כי $H = \left\{a_1^{i_1} a_2^{i_2} \cdots a_n^{i_k} \mid i_j = 0, 1\right\}$, וכי לכל סדרת i_j יתקבל איבר אחר. לכן הסדר של H הוא מספר הסדרות האפשריות i_j, 2^n.[3]
נחשב כעת את מכפלת כל איברי H. נביט ב־a_j מסוים. מחצית האיברים ב־H מחושבים בעזרת $i_j = 1$, דהיינו האיבר a_j מופיע בחישובם. במחצית האחרת $i_j = 0$ ובמקרים אלו a_j אינו מופיע בחישוב. סך הכל a_j מופיע בחישוב 2^{n-1} פעמים. באופן דומה כל שאר האיברים מופיעים 2^{n-1} פעמים. ביחד, מכפלתם ההיא $a_1^{2^{n-1}} a_2^{2^{n-1}} \cdots a_n^{2^{n-1}}$. לפי הנתון, $n > 1$, ולכן $2^{n-1} \mid 2$, ולכל איבר מסדר 2 מתקיים $x^{2^{n-1}} = 1$. בפרט, המכפלה הנ"ל היא למעשה מכפלת 1־ים.
לסיכום, הפרדנו את G לשתי קבוצות, H ו־B. הראנו בנפרד כי מכפלת כל איברי הקבוצה בכל אחת מהן היא 1, ולכן מכפלת כל איברי G היא 1, כמבוקש.

5. לפי משפט לגרנז', הסדר של b מחלק את $|G|$. מכיוון ש־$|G|$ הוא אי־זוגי, אז גם $o(b)$ הוא אי־זוגי. כבר ראינו בסעיף 1 שהסדר הזה מחלק את 2, ולכן $o(b) = 1$. □

4.3.12 הוכיחו: עבור p ראשוני, בחבורה מסדר $2p$ יש איבר מסדר p.

פתרון נסמן את החבורה שלנו G. לפי משפט לגרנז', כל איברי G הם מסדרים $1, 2, p, 2p$. אך יש רק איבר אחד מסדר 1, בכל חבורה שהיא. אם קיים איבר בחבורה G מסדר p אז סיימנו. אם קיים איבר g מסדר $2p$, אז הסדר של g^2 הוא p, כמבוקש. אם כן, אנו נניח בשלילה כי אין בחבורה איברים מסדרים $p, 2p$. יש רק איבר יחיד מסדר 1 ולכן כל שאר $2p - 1$ האיברים הם מסדר 2. אם $p = 2$ אז סיימנו. אחרת, לפי תרגיל 3.4.6, אותו פתרנו בעבר, אנו יודעים ש־G אבלית. יהיו $a \neq b$ שני איברים מסדר 2.

[2] מפני ש־H סופית, ברור ש־A מוגדרת היטב; היא תוצאה של אלגוריתם סופי.
[3] ניתן להתייחס ל־A כאל בסיס למרחב הוקטורי H, שהוא איזומורפי ל־$\mathbb{Z}_2^n$.

אזי נביט בקבוצה $H = \{1, a, b, ab\}$. ניתן להראות כי H חבורה, ולכן $H \leq G$. לפי משפט לגרנז', מכאן נובע $|H| \mid |G|$, זאת אומרת $4 \mid 2p$. אנו הנחנו לעיל כי $p \neq 2$, ולכן זו סתירה. אם כן, יש איברים בחבורה מסדר p או מסדר $2p$, ולפי הטיעון לעיל, קיים איבר בחבורה מסדר p. □

4.4.6 חשבו $6^{48} \mod 11$.

פתרון ראשית נזכיר כי $6^{-1} \equiv 2 \pmod{11}$. לפי משפט פרמה הקטן, לכל $a \in \mathbb{Z} \setminus \{0\}$, מתקיים $a^{11-1} = a^{10} \equiv 1 \pmod{11}$. לכן

$$6^{48} = 6^{-2} \cdot 6^{50} = 2^2 \cdot \left(6^{10}\right)^5 \equiv 4 \cdot (1)^5 = 4 \pmod{11}$$

לסיכום, $6^{48} \equiv 4 \pmod{11}$. □

4.4.7 הוכיחו: לכל n שלם, $n^5 \equiv n \pmod{30}$.

פתרון מכיוון ש־30 הוא מספר פריק, די להראות את קיום הטענה עבור גורמיו, מרוכזים לפי ראשוני. זאת אומרת שדי להוכיח $n^5 \equiv n \pmod{p}$ כאשר $p = 2, 3, 5$. אנו נעבוד עם המשפט הקטן של פרמה. המשפט קובע כי עבור p ראשוני, $n^p \equiv n \pmod{p}$. לפיכך

$$\begin{aligned} n^5 &\equiv n^3 \equiv n^2 \equiv n \pmod{2} \\ n^5 &\equiv n^3 \equiv n \pmod{3} \\ n^5 &\equiv n \pmod{5} \end{aligned}$$

מכאן נובע כי עבור $p = 2, 3, 5$ מתקיים $p \mid n^5 - n$, ולכן גם עבור $lcm(2, 3, 5) = 30$ מתקיים $30 \mid n^5 - n$, או $n^5 \equiv n \pmod{30}$. □

4.6.2 כל חבורה מסדר ראשוני היא ציקלית.

פתרון תהי G חבורה מסדר p. בפרט קיים ב־G איבר g מסדר שונה מ־1, דהיינו איבר שאינו איבר יחידה. נביט בחבורה הנוצרת על ידיו, $\langle g \rangle$. בבירור, הסדר של החבורה גדול מ־1, אך לפי משפט לגרנז' הסדר מחלק את הראשוני p. מצאנו אם כן $p \mid o(p) > 1$, ומראשוניות יוצא $o(p) = p$. אם כן, $\langle p \rangle = G$, ו־G ציקלית. □

4.6.3 הוכיחו שחבורה ציקלית היא אבלית.

פתרון נסמן יוצר של החבורה $g \in G$. יהיו שני איברים בחבורה, g^n, g^m. אזי

$$g^n \cdot g^m = g^{n+m} = g^{m+n} = g^m \cdot g^n$$

אם כן, היא אבלית. □

4.6.8 תהי $G = \langle a \rangle$ חבורה ציקלית מסדר 10. מצא את האינדקסים ואת הקוסטים הימניים של $H_1 = \langle a^2 \rangle$ ושל $H_2 = \langle a^5 \rangle$.

פתרון ראשית נרשום את איברי התת־חבורות: $H_1 = \left\{a^2, a^4, a^6, a^8, a^{10} = 1\right\}, H_2 = \left\{a^5, a^{10} = 1\right\}$. לפיכך עוצמתם היא $|H_1| = 5, |H_2| = 2$. מכאן, האינדקסים הם $[G : H_1] = \frac{10}{5} = 2, [G : H_2] = \frac{10}{2} = 5$. הקוסטים הם לפיכך כדלהלן:

$$\begin{aligned} 1 \cdot H_1 &= H_1 = \left\{1, a^2, a^4, a^6, a^8\right\} \\ aH_1 &= \left\{a, a^3, a^5, a^7, a^9\right\} \end{aligned}$$

$$\begin{aligned} 1 \cdot H_2 &= H_2 = \left\{1, a^5\right\} \\ aH_2 &= \left\{a, a^6\right\} \\ a^2H_2 &= \left\{a^2, a^7\right\} \\ a^3H_2 &= \left\{a^3, a^8\right\} \\ a^4H_2 &= \left\{a^4, a^9\right\} \end{aligned}$$

מצאנו כאן כי אכן האינדקס תואם את מספר הקוסטים. לסיום נזכיר כי על ידי העתקה $a^n \mapsto n + 10\mathbb{Z}$ ניתן למצוא התאמה מלאה בין G לבין $\mathbb{Z}_{10}$. $\square$