מבנים אלגבריים

תרגיל בית 7
פתרונות

תזכורת המרכז של איבר $x \in G$ הוא הת"ח $C_G(x) = \{g \in G \mid gx = xg\}$.

1. מהו $C_G(x)$ אם ידוע שהחבורה G אבלית? מהו אם ידוע ש $x \in Z(G)$?

פתרון נניח G אבלית ויהי $x \in G$. לכן, לכל $g \in G$, מתקיים $gx = xg$. לסיכום

$$C_G(x) = \{g \in G \mid gx = xg\} = \{g \in G\} = G$$

באופן דומה, גם כאשר $x \in Z(G)$, לכל $g \in G$, מתקיים $gx = xg$. מצאנו כי בשני המקרים האלו, $C_G(x) = G$. ■

2. הוכח או הפרך: לכל איבר $x \in G$, $C_G(x)$ הוא תח"נ.

פתרון נפריך על ידי דוגמא נגדית: נביט בחבורה D_3[1] [2], וניקח את האיבר τ. נחשב את המרכז שלו. בחבורה D_3 יש שני טיפוסים של איברים: הסיבובים σ^i והשיקופים $\sigma^i\tau$, כאשר i בין 0 ל־2. נתחיל לחפש סיבובים במרכז:

$$\sigma^i\tau = \tau\sigma^{3-i} \stackrel{?}{=} \tau\sigma^i$$

הפתרון הוא כאשר $3 - i \equiv i \pmod 3$, דהיינו $i = 0$. לכן רק id שייך למרכז של τ מכל הסיבובים, ושאר הסיבובים מעבירים את τ לשיקופים האחרים. נחשב כעת, באופן דומה, אילו שיקופים נמצאים במרכז:

$$\begin{aligned} \sigma^i\tau\tau &= \sigma^i \\ \tau\sigma^i\tau &= \sigma^{3-1} \end{aligned}$$

שוב, הפתרון הוא $3 - i \equiv i \pmod 3$, או $i = 0$. לכן השיקוף היחיד כאן הוא τ. לסיכום, $C_{D_3}(\tau) = \{id, \tau\}$. זו איננה תח"נ של D_3; לדוגמא, $\sigma\tau\sigma^{-1} = \tau\sigma \notin C_{D_3}(\tau)$. ■

3. הוכח או הפרך: $Z(G) \subseteq C_G(x)$ לכל $x \in G$.

[1] כרגיל, נסמן σ סיבוב ו־τ שיקוף.

[2] כבר אמרנו שהחבורה הדיהדרלית והחבורה הסימטרית הן החבורות ה'מעצבנות' המשמשות כר פורה להצמחת דוגמאות נגדיות?

פתרון נוכיח: יהי $x \in G$ ויהי $g \in Z(G)$. נבדוק האם $g \in C_G(x)$, דהיינו האם $gx = xg$. מכיוון ש־$g \in Z(G)$, לכל $h \in G$ מתקיים $gh = hg$. בפרט עבור x שלנו מתקיים $gx = xg$, ולכן $g \in C_G(x)$. לסיכום, $Z(G) \subseteq C_G(x)$ לכל $x \in G$. (שימו לב, זו אפילו תת־חבורה. הוכיחו!) ■

4. הוכח $C_G(a) \cap C_G(b) \subseteq C_G(ab)$. תן דוגמא בה ההכלה הזו היא שיוויון, ותן דוגמה שבה אין שיוויון.

פתרון ראשית, נוכיח את ההכלה. יהיו $a, b \in G$ ויהי $g \in C_G(a) \cap C_G(b)$. אנו רוצים להראות שמתקיים $g \in C_G(ab)$, דהיינו $gab = abg$. ואכן

$$gab \overset{g \in C_G(a)}{=} agb \overset{g \in C_G(b)}{=} abg$$

ולכן $g \in C_G(ab)$. בכך הוכחנו $C_G(a) \cap C_G(b) \subseteq C_G(ab)$.

דוגמא בה <u>מתקיים שויון</u> היא כל חבורה אבלית: שם בכל מקרה $C_G(a) = C_G(b) = C_G(ab) = G$, וההכלה טריוויאלית.

דוגמא בה <u>אין שויון</u>: נשתמש בהפרכה שהצגנו בסעיף 2. נביט ב־D_3. כבר חישבנו שם ש־$C_{D_3}(\tau) = \{id, \tau\} = \langle\tau\rangle$. ניקח $a = b = \tau$, ונקבל $C_G(a) = \langle\tau\rangle$, אבל $C_G(b) = D_3$, לפי שאלה 1 (כי $id \in Z(G)$). אבל $\langle\tau\rangle \neq D_3$. ■

תזכורת תהי $G = \langle a \rangle$ חבורה ציקלית סופית מסדר n, ויהי $m \mid n$. אזי יש ב־G איבר מסדר m: $a^{\frac{n}{m}}$.

תזכורת שדות סופיים קיימים רק מסדרים p^r כאשר p ראשוני. במקרים אלו, המאפיין של השדה הוא p, והחבורה הכפלית של השדה $F^\times$ היא ציקלית מסדר $p^r - 1$.

5. לאילו שדות סופיים יש איבר x המקיים $x^4 = -1$?[3]

פתרון נשים לב שאפס אינו מקיים את המשוואה, ולכן אנו מחפשים את הפתרון בחבורה הכפלית $F^\times$. אם $x^4 = -1$ אז $x^8 = (-1)^2 = 1$, ולכן מתקיים $o(x) \mid 8$. מנגד, אם המאפיין של השדה איננו 2[4], אז $x^4 \neq 1$, כי $-1 \neq 1$, ולכן $o(x) \nmid 4$. הפתרון הוא $o(x) = 8$. אם כן נדרוש שב־$F^\times$ יהיה איבר x מסדר 8, ואז הוא יקיים את המשוואה. לפי התזכורת + משפט לגרנז', הדרישה היא שהסדר של $F^\times$ יתחלק ב־8. בהתחשב בכך שסדרי השדות הסופיים האפשריים הם מהצורה p^r, עבור p ראשוני, אנו מחפשים מקרים בהם $8 \mid |F^\times| = |F| - 1 = p^r - 1$, או $p^r - 1 \equiv 0 \pmod 8$, או $p^r \equiv 1 \pmod 8$. במקרה זה, פתרונות אפשריים הם השדות מסדרים $9, 17, 25, 41$. שימו לב! אין שדה סופי מסדר 33, כי הוא איננו חזקת ראשוני.

כעת נחזור ונטפל במקרה בו השדה הוא ממאפיין 2. במקרה זה $-1 = 1$, ולכן $x^4 = 1$, ואנו מפשים מתי יש איבר שסדרו יחלק את 4. אבל בכל שדה כזה, 1 הוא איבר מסדר המחלק את 4,[5] ולכן 1 הוא פתרון מתאים.

לסיכום, השדות האפשריים הם השדות ממאפיין 2 או מסדר המקיים $p^r \equiv 1 \pmod 8$. ■

[3] ענינו על שאלה זו בכיתה, אבל כאן הפתרון מוצג אחרת, מומלץ לעקוב אחריו.

[4] נטפל במאפיין 2 בנפרד, בסוף הפתרון.

[5] $o(1) = 1$.

6. לאילו שדות סופיים יש איבר x המקיים $x^4+x^3+x^2+x=-1$?

פתרון נשים לב שהפתרון נמצא בחבורה הכפלית של השדה, ב־$F^\times$, כי אפס אינו פותר את המשוואה. הזהות המבוקשת היא $x^4+x^3+x^2+x+1=0$. נשים לב שאם נכפיל משוואה זו בפולינום $x-1$, נקבל שאנו מחפשים פתרונות של המשוואה $x^5-1=0$, או $x^5=1$.לכן אנו מחפשים ב־$F^\times$ איבר מסדר מחלק 5: $5 \mid o(x)$. בפנינו שתי אפשרויות:

- $o(x)=5$. ואז, לפי התזכורת + לגרנז', הדרישה היא שהחבורה $F^\times$ תהיה מסדר המתחלק ב־5. כמו קודם, אנו מחפשים מקרה עבורו $5 \mid |F^\times| = p^r-1$, או $p^r \equiv 1 \pmod 5$. פתרונות אפשריים הם השדות מסדרים $11, 16, 31, 41$.[6] מצאנו כי במקרים אלו יש בחבורה הכפלית של השדה איבר מסדר 5, הפותר את המשוואה $x^5-1=(x-1)\left(x^4+x^3+x^2+x+1\right)=0$. נותר להראות כי במקרה זה, האיבר x שמצאנו איננו שורש של הגורם $x-1$, ואז הוא יהיה שורש של הגורם האחר, $x^4+x^3+x^2+x+1$. הוכיחו בעצמכם מדוע העובדה $o(x)=5$ מוכיחה זאת!
- $o(x)=1$. ואז, כמו בכל חבורה, האפשרות היחידה היא $x=1$, איבר היחידה של החבורה שלנו $F^\times$. נציב 1 במשוואה, ונראה מתי הוא פותר את המשוואה.

$$\begin{aligned} 1^4+1^3+1^2+1+1 &= 0 \\ 5 &= 0 \end{aligned}$$

אם כן, 1 הוא פתרון למשוואה הנ"ל כאשר $5=0$, דהיינו כאשר המאפיין של השדה הוא 5.

לסיכום, השדות הסופיים המתאימים הם שדות ממאפיין 5 או שדות שסדרם מקיים $p^r \equiv 1 \pmod 5$. ■

הערה כללית שאלות מסוג זה על שדות סופיים פותרים כך:

- ראשית בודקים אם אפס הוא פתרון.
- אח"כ ננסה למצוא מה הסדרים האפשריים ל־x לפי הנתון בפולינום. בדרך כלל הכי נוח להביא את הפולינום לצורה $x^n-1=0$, ואז הסדר מחלק את n. בשאלה 5 היה לנו עוד נתון (הסדר לא מחלק את 4).
- בשלב הבא מחפשים מה ניתן ללמוד מהתנאים שמצאנו על הסדרים. הרבה פעמים יהיה איזה תנאי חריג על המאפיין, שבהיעדרו הפתרון יהיה $p^r \equiv 1 \pmod n$.
- אוספים את כל הנתונים, ומסכמים.

בהצלחה!

[6] שימו לב! גם כאן אין שדה מסדר 6, 21 או 51!