תרגול 11 — מבנים אלגבריים תשע"ג

8 בינואר 2013

תקציר

מחלקות צמידות, קשר לחבורה נורמלית, מְרַכֵּז (Centralizer) של איבר, מספר האיברים במחלקת צמידות, נוסחת המחלקות, מחלקות צמידות ב־S_n.

בשיעור זה נגדיר את המושג מחלקת צמידות, ונשתמש בו ובתכונותיו כדי לספור איברים בחבורה. הרעיון הוא שניתן לספור את איברי החבורה בכמה שיטות שונות, וכך לגלות פרטים על החבורה.

1 יחס הצמידות ומחלקות צמידות

הגדרה 1.1 תהי G חבורה. יהיו $g,h\in G$. אנו נאמר כי g **צמוד ל־**h אם קיים $r\in G$ כך ש־$g=rhr^{-1}$.

משפט 1.2 היחס g צמוד ל־h הוא יחס שקילות.

הוכחה: רפלקסיביות: יהי $g\in G$. אזי $g=ege^{-1}$, ולכן g צמוד לעצמו.
סימטריות: יהיו $g,h\in G$ כך ש־g צמוד ל־h. אזי קיים $r\in G$ כך ש־$g=rhr^{-1}$. לפיכך גם $h=r^{-1}gr$ ולכן בעזרת r^{-1} ניתן לקבוע כי h צמוד ל־g.
טרנזיטיביות: יהיו $f,g,h\in G$ כך ש־f צמוד ל־g וש־g צמוד ל־h. לפיכך קיימים $r,s\in G$ כך ש־$f=rgr^{-1}, g=shs^{-1}$. אזי $f=rgr^{-1}=rshs^{-1}r^{-1}=(rs)h(rs)^{-1}$. לפיכך, בעזרת rs ניתן לקבוע כי f צמוד ל־h. ■

הגדרה 1.3 תהי G חבורה, ויהי $g\in G$. אנו נגדיר את **מחלקת הצמידות של** g כקבוצת האיברים בחבורה הצמודים אליו. הסימון הוא

$$\mathcal{C}_g=\left\{xgx^{-1}\mid x\in G\right\}$$

למחלקת הצמידות אין סימון סטנדרטי. סימונים אחרים הנמצאים בשימוש הם $\operatorname{conj}(g)$, $\mathcal{C}\ell(g)$ וגם $\mathcal{K}_g$. אין צורך לחשוש מריבוי הסימונים, העיקר הכוונה.

כאמור לעיל, היחס הוא יחס שקילות, ולכן הוא מחלק את G למחלקות שקילות. באופן ברור, מכיוון שהיחס שלנו הוא רפלקסיבי, לכל איבר מתקיים $g\in\mathcal{C}_g$.

למה 1.4 יהי $g\in G$. אזי $\mathcal{C}_g=\{g\}$ א.ס.ם. $g\in Z(G)$.

הוכחה: $(\Longleftarrow)$ נניח כי $\mathcal{C}_g=\{g\}$. אזי לכל $x\in G$ מתקיים $xgx^{-1}=g$. על ידי הכפלה ב־x מימין יתקבל $xg=gx$. היות והטענה מתקיימת לכל $x\in G$, הרי שמצאנו ש־$g\in Z\left(G\right)$.
הכיון השני נשאר כתרגיל. ∎

משפט 1.5 תהי $H\leq G$. אזי H נורמלית ב־G א.ס.ם. H היא איחוד של מחלקות צמידות של איברים ב־G. ננסח זאת גם בצורה פורמלית.

$$H\trianglelefteq G\Longleftrightarrow\exists S\subseteq G,H=\bigcup_{s\in S}\mathcal{C}_s$$

הוכחה: (כיוון ראשון) נניח כי H נורמלית ב־G. אנו צריכים למצוא S שתקיים $H=\bigcup_{s\in S}\mathcal{C}_s$. אנו ניקח $S=H$. נראה שויון קבוצות בעזרת הכלה דו־כיוונית. ההכלה $H\subseteq\bigcup_{s\in H}\mathcal{C}_s$ נובעת מכך שכל מחלקת צמידות נובעת מהאיבר שיוצר אותה. נותר להראות את ההכלה ההפוכה. הצורה הכללית של איברים ב־$\bigcup_{s\in H}\mathcal{C}_s$ היא xsx^{-1} עבור $s\in H,x\in G$ מסוימים. מכיוון ש־H נורמלית ב־G, הרי שההצמדה של s על ידי איבר מ־G נשארת בתוך H. אם כן, ברור כי $xsx^{-1}\in H$. כך הראנו הכלה גם בכיוון השני. לסיכום, יש שויון בין הקבוצות, והראנו כי H היא איחוד של מחלקות צמידות.
(כיוון שני) נניח כי קיימת S כך ש־$H=\bigcup_{s\in S}\mathcal{C}_s$. צריך להוכיח כי $H\trianglelefteq G$. נביט באיבר כללי מ־H, ונראה כי הצמדתו גם היא ב־H. איבר כללי הוא מהצורה xsx^{-1} עבור $s\in S,x\in G$. יהי $y\in G$ נתון. אזי $y\left(xsx^{-1}\right)y^{-1}=\left(yx\right)s\left(yx\right)^{-1}\in\mathcal{C}_s\in H$. אם כן הראנו כי H סגורה להצמדות. נזכיר כאן כי נתון לנו ש־$H\leq G$, ולכן $H\trianglelefteq G$. ∎

2 נוסחת המחלקות

הגדרה 2.1 תהי G חבורה, ויהי $g\in G$. אזי נגדיר את **המְרַכֵּז** (Centralizer) של g ב־G כקבוצת כל האיברים ב־G המתחלפים עם g. הסימון הוא

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

הערה 2.2 שימו לב, יש להבדיל בעברית בעזרת הניקוד בין מֶרְכָּז של חבורה (Center) לבין מְרַכֵּז של איבר בחבורה (Centralizer). הראשון הוא קבוצת האיברים המתחלפים עם כל איברי החבורה, והשני הוא קבוצת כל האיברים המתחלפים עם איבר ספציפי; הראשון הוא במשקל מֶרְחָב, והשני הוא במשקל מְלַמֵּד.

למה 2.3 לכל $g\in G$ מתקיים $Z\left(G\right)\leq C_G\left(g\right)\leq G$.

הוכחה: ראשית נראה כי $C_G\left(g\right)\leq G$. יהיו $x,y\in C_G\left(g\right)$. אזי מתקיים

$$\left(xy\right)g=x\left(yg\right)=x\left(gy\right)=\left(xg\right)y=\left(gx\right)y=g\left(xy\right)$$

ולפיכך $C_G\left(g\right)$ סגורה לכפל. נראה סגירות להפיך. יהי $x\in C_G\left(g\right)$. אזי $xg=gx$. נכפיל ב־x^{-1} מימין ומשמאל ונקבל $gx^{-1}=x^{-1}g$, ולפיכך גם $x^{-1}\in C_G\left(g\right)$. לפי הקריטריון לתת־חבורות, $C_G\left(g\right)\leq G$.

כעת נותר עוד חלק בהוכחה: $Z(G) \le C_G(g)$. מכיוון שאלו הן שתי תתי־חבורות, כל שיש להראות הוא הכלה. ואכן יהי $x \in Z(G)$. אזי לכל $g \in G$ מתקיים $xg = gx$. בפרט עבור g שלנו זה מתקיים. לפיכך $Z(G) \le C_G(g)$. ■

משפט 2.4 תהי G חבורה סופית, ויהי $g \in G$. אזי $|\mathcal{C}_g| = [G : C_G(g)]$.

הוכחה: האינדקס של המְּרַכֵּז של g הוא מספר הקוסטים הימניים[1] של $C_G(g)$. אנו ננסה להראות התאמה חח"ע ועל בין הקוסטים האלו לאיברי $\mathcal{C}_g$ השונים. נקבע כלל התאמה $C_G(g)\,x \longleftrightarrow x^{-1}gx$. עלינו להראות כי ההתאמה הזו היא חח"ע ועל.

יהיו x, y באותו קוסט ימני. אזי קיים $c \in C_G(g)$ כך ש־$y = cx$. מכיוון ש־c נמצא במְּרַכֵּז של g, $cg = gc$. אם כן

$$y^{-1}gy = (cx)^{-1}\,g\,(cx) = x^{-1}c^{-1}gcx = x^{-1}c^{-1}cgx = x^{-1}gx$$

השתמשנו כאן בשני הנתונים שלנו על c. אם כן מצאנו כי עבור שני נציגים של קוסט ימני מתקבלת אותה ההצמדה של g. אם $C_G(g)\,x = C_G(g)\,y$ אז $y^{-1}gy = x^{-1}gx$.

נעבור לכיוון השני. יהיו x, y המקיימים $y^{-1}gy = x^{-1}gx$. אזי $xy^{-1}gyx^{-1} = g$ או $\left(yx^{-1}\right)^{-1} g \left(yx^{-1}\right) = g$ או $g\left(yx^{-1}\right) = \left(yx^{-1}\right) g$. לפיכך $yx^{-1} \in C_G(g)$, ואז יתקיים $C_G(g)\,yx^{-1} = C_G(g)$ או $C_G(g)\,x = C_G(g)\,y$. אם כן, הראנו כי לכל איבר במחלקת הצמידות מותאם איבר אחד ויחיד מהקוסטים הימניים, וכן להפך. התאמה כזו היא הפיכה, ובפרט שומרת עוצמה, ומתקיים $|\mathcal{C}_g| = [G : C_G(g)]$.

לסיום ההוכחה נעיר מפני מה דרשנו ש־G סופית. ובכן, הסיבה היא שכך אנו בטוחים שהביטויים לעיל מוגדרים היטב. ■

מסקנה 2.5 (נוסחת המחלקות) תהי G חבורה סופית. נסמן על ידי S תת־קבוצה של G כך שלכל איבר ב־$\mathcal{C}_g$ יד נציג אחד ויחיד ב־S. אזי

$$o(G) = \sum_{g \in S} |\mathcal{C}_g| = \sum_{g \in S} [G : C_G(g)] = \sum_{g \in S} \frac{o(G)}{|C_G(g)|}$$

ניתן לפצל את S לאיברים שבמחלקת הצמידות שלהם יש יותר מאיבר אחד ולכאלה שאין להם אלא איבר אחד במחלקת הצמידות, הם עצמם. לפי למה 1.4, איבר שאין במחלקת הצמידות שלו איברים מלבדו הוא איבר במְּרַכֵּז. נסמן $S' = \{g \in S \mid \mathcal{C}_g \ne \{g\}\}$, כך ש־$S \setminus S' = Z(G)$. נזכיר כאן שבאופן טריוויאלי $C_G(g) = G$ עבור $g \in Z(G)$. אזי ניתן לרשום את הנוסחא

$$\begin{aligned} o(G) &= \sum_{g \in S} \frac{o(G)}{|C_G(g)|} = \sum_{g \in Z(G)} \frac{o(G)}{|C_G(g)|} + \sum_{g \in S'} \frac{o(G)}{|C_G(g)|} \\ &= \sum_{g \in Z(G)} \frac{o(G)}{o(G)} + \sum_{g \in S'} \frac{o(G)}{|C_G(g)|} = |Z(G)| + \sum_{g \in S'} \frac{o(G)}{|C_G(g)|} \end{aligned}$$

אם כן, נוסחת המחלקות היא

$$o(G) = \sum_{g \in S} \frac{o(G)}{|C_G(g)|} = |Z(G)| + \sum_{g \in S'} \frac{o(G)}{|C_G(g)|}$$

[1] ניתן לעבוד גם עם קוסטים שמאליים.

לשני הנוסחים קוראים **נוסחת המחלקות**. לנוסחא זו יש שימושים רבים; נראה אחד מהם.

תרגיל: תהי G חבורה מסדר p^n, p ראשוני. אזי $Z(G) \neq \{e\}$. במילים נאמר כי מֶרְכַּז החבורה איננו טריוויאלי.

פתרון: נציב בנוסחת המחלקות את הנתונים. ובכן, $o(G) = p^n$. לכל g נציג יחיד של מחלקת צמידות קיים n_g כך ש־$|C_G(g)| = p^{n_g}$. אם $g \notin Z(G)$ אז $n_g \neq n$. אם כן, נציב את כל אלו בנוסחא ונקבל

$$p^n = |Z(G)| + \sum_{g \in S'} \frac{p^n}{p^{n_g}} = |Z(G)| + \sum_{g \in S'} p^{n-n_g}$$

נעביר אגף ונקבל $|Z(G)| = p^n - \sum_{g \in S'} p^{n-n_g}$. נראה כעת כי הביטוי באגף שמאל מתחלק ב־p. ברור ש־p^n מתחלק בו, אבל גם p^{n-n_g} מתחלק ב־p אם $n \neq n_g$, וזה בדיוק המקרה $g \in S'$. אם כן, אגף שמאל הוא חיסור של איברים המתחלקים באותו p, ולכן גם הוא מתחלק ב־p. מכך נובעת תכונה דומה גם באגף ימין: $p \mid |Z(G)|$. בפרט $|Z(G)| \neq 1$ ולכן המֶרְכַּז איננו תת־החבורה הטריוויאלית. ■

3 מחלקות צמידות ב־S_n

דוגמא: נביט ב־S_4, ונחפש את מחלקת הצמידות של $\sigma = (1\,2)(3\,4)$. נתחיל ונחשב מה ההצמדות של σ על ידי ששת החילופים ב־S_4.

$$\begin{aligned}
(1\,2)(1\,2)(3\,4)(1\,2)^{-1} &= (1\,2)(3\,4)\\
(1\,3)(1\,2)(3\,4)(1\,3)^{-1} &= (1\,4)(2\,3)\\
(1\,4)(1\,2)(3\,4)(1\,4)^{-1} &= (1\,3)(2\,4)\\
(2\,3)(1\,2)(3\,4)(2\,3)^{-1} &= (1\,3)(2\,4)\\
(2\,4)(1\,2)(3\,4)(2\,4)^{-1} &= (1\,4)(2\,3)\\
(3\,4)(1\,2)(3\,4)(3\,4)^{-1} &= (1\,2)(3\,4)
\end{aligned}$$

ניתן לראות כי קיבלנו את כל האיברים ממבנה מחזורים $(--)(--)$. אם נמשיך להצמיד על ידי חילופים, אנו נשאר בתוך התמורות האלו. מכיוון שכל התמורות ב־S_4 הן הרכבת חילופים, הרי שלכל תמורה אני אשאר בתוך הקבוצה הזו. לסיכום,

$$\mathcal{C}_\sigma = \{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} = (--)(--)$$

משפט 3.1 תהיינה $\sigma, \tau \in S_n$ תמורות. אזי לתמורה $\rho = \tau\sigma\tau^{-1}$ יש מבנה מחזורים זהה לזה של σ.

הוכחה: נניח ש־$i \xrightarrow{\sigma} j$. נחפש את התמונות של i ושל j לפי τ. נסמנם r ו־s בהתאמה, $i \xrightarrow{\tau} r, j \xrightarrow{\tau} s$. אזי $\tau\sigma\tau^{-1}(r) = \tau\sigma(i) = \tau(j) = s$. נרשום מחדש משוואה זו, ונקבל $\rho(\tau(i)) = \tau(j)$. נכליל זאת, אם σ מורכבת ממכפלת המחזורים $\sigma = (a_1 a_2 \cdots a_{k_1})(b_1 b_2 \cdots b_{k_2}) \cdots (g_1 g_2 \cdots g_{k_l})$, מכפלה של l מחזורים, אז יתקיים

$$\rho = (\tau(a_1)\tau(a_2)\cdots\tau(a_{k_1}))(\tau(b_1)\tau(b_2)\cdots\tau(b_{k_2}))\cdots(\tau(g_1)\tau(g_2)\cdots\tau(g_{k_l}))$$

ניתן לראות כי ל־ρ יש מבנה מחזורים זהה לזה של σ. ניתן להראות כי אם ההצגה של σ היא של מחזורים זרים אז גם ההצגה של ρ היא של מחזורים זרים. ■

משפט 3.2 תהיינה $\sigma, \rho \in S_n$ תמורות בעלות אותו מבנה מחזורים זרים. אזי קיימת $\tau \in S_n$ כך ש־$\rho = \tau\sigma\tau^{-1}$.

הוכחה: נניח שהפירוק למחזורים זרים המתאים הוא

$$\begin{aligned} \sigma &= (a_1 a_2 \cdots a_{k_1}) \cdots (g_1 g_2 \cdots g_{k_l}) \\ \rho &= (a'_1 a'_2 \cdots a'_{k_1}) \cdots (g'_1 g'_2 \cdots g'_{k_l}) \end{aligned}$$

לצורך הוכחה זו אנו רושמים גם מחזורים מאורך 1. אזי נגדיר את τ באמצעות טבלה

$$\tau = \begin{pmatrix} a_1 & a_2 & \cdots & a_{k_1} & \cdots & g_1 & g_2 & \cdots & g_{k_l} \\ a'_1 & a'_2 & \cdots & a'_{k_1} & \cdots & g'_1 & g'_2 & \cdots & g'_{k_l} \end{pmatrix}$$

לפי החישוב שעשינו במשפט הקודם, τ מקיימת המבוקש. ■

מסקנה 3.3 ראינו בשני המשפטים האחרונים שכל מחלקת צמידות מכילה רק איברים ממבנה מחזורים אחיד, וכן שהיא מכילה את כל המחזורים ממבנה זה. לכן מחלקת צמידות ב־S_n היא כל האיברים מאותו מבנה מחזורים זרים, כפי שניתן לראות בדוגמא.

הערה 3.4 ב־A_n או בכל תת־חבורה אחרת של חבורת הסימטריה המשפט הזה איננו מתקיים בהכרח. דוגמאות בתרגיל הבית (מספר 8).