הרצאה 5

26 באפריל 2019

1 חבורות ציקליות

1.1 תזכורת

בשיעור הקודם ראינו: בחבורה סופית לכל איבר יש סדר. לכל איבר g קיים k כך ש- $g^k = e$.
ה-k המינימלי נקרא הסדר של g ומסומן $o(g)$.
הגדרנו את תת-החבורה שנוצרת על ידי g בתור: $< g >= g^0 \cdot g^1 \cdots g^{k-1}$.

דוגמה. עבור $(\mathbb{Z}_{12}, +)$: $< 3 >= \{0, 3, 3+3 = 6, 9\}$ ומכיוון ש-$3+3+3+3 = 0$ מתקיים $o(3) = 4$.

משפט. הצגנו את משפט לגרנז': $H < G$ אזי $|H|||G|$. ולכן עבור הדוגמה שלנו מתקיים $o(3) = 4|12$.

מסקנה. סדר של איבר מחלק את סדר החבורה. כלומר עבור $g \in G$ אזי $o(g)||G|$.

טענה 1. מסקנה: אם הסדר של $n = |G|$ אז: $g^n = e$.

הוכחה. יהא $k = o(g)$. אז אמרנו כי: $k|n$, כלומר $n = a \cdot k$. ואז: $g^n = g^{k \cdot a} = (g^k)^a = e^a = e$. ■

1.2 חבורה ציקלית

הגדרה. אם חבורה $G =< g >$ אומרים שG היא ציקלית לg ו-g יוצר שלה. היא נראית כך: $G = \{e, g, g^1.g^2 \cdots g^{k-1}\}$.

דוגמה. Z_n היא ציקלית והיוצר שלה הוא 1. ולכן נסמן $Z_n =< 1 >$.

משפט. כל חבורה ציקלית מסדר n איזומורפית ל-$\mathbb{Z}_n$.

הוכחה. אם G ציקלית מסדר n אזי קיים $g \in G$ כך ש-$G =< g >$ והיא נראית כך: $G = \{e, g, g^2 \cdots g^{n-1}\}$ וזה איזומורפי ל-$\mathbb{Z}_n = \{0, 1, 2, 3, ..., n-1\}$. האיזומורפיזם הוא: $\Phi : G \to \mathbb{Z}_n$, $\Phi(g^i) = i$.

נבדוק את האיזומורפיזם:

שימור הפעולה - $\Phi(g^i \cdot g^j) = \Phi(g^{i+j}) = i + j = \Phi(g^i) + \Phi(g^j)$ מחיבור חזקות והגדרת האיזומורפיזם.

השאלה היא מה קורה כאשר $i + j = n + a$ ($a < n$) כלומר כאשר הם גדולים מ-n. נבדוק: $g^{i+j} = g^{n+a} = g^n \cdot g^a = g^a$. אותו דבר ניתן להראות על $\mathbb{Z}_n$.

לכן $\Phi(g^i g^j) = \Phi(g^a) = a = i + j = \Phi(g^i)\Phi(g^j)$ - וכאן באה תכונת הציקליות של החבורה לידי ביטוי. ■

דוגמה. יפה לראות כי למשל ל-Z_{12} יש כמה יוצרים. למשל: $Z_{12} =< 1 >$ אך גם $Z_{12} =< 5 >= \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\}$.

מסקנה. זה מוביל אותנו למסקנה מעניינת: היוצרים של Z_{12} הם האיברים ב-Z_{12} שזרים ל-12, כלומר $\{1, 5, 7, 11\}$.

משפט. $a \in \mathbb{Z}_n$ הוא יוצר $\iff$ מתקיים $(a, n) = 1$.

הוכחה. יהי a יוצר של Z_{12}. אזי $o(a) = 12$ כלומר, ה-k המינמלי כך ש- $k \cdot a = 0$. זה למעשה שקול להגיד $ka = e \cdot 12$ ולכן ka הוא כפול של a וגם כפולה של 12. ומכיוון ש-$k = o(a)$ (המינימלי) אזי $ka = lcm(a, n) = [a, n]$. ולכן $[a, 12] = 12a$. ניזכר כי המכפלה המשותפת הכי קטנה מקיימת: $[a, n] = \frac{a \cdot n}{gcd(a,n)}$. אם נציב, נקבל מהמשוואה כי $gcd(a, n) = 1$. ■

דוגמה. ב-Z_{10}. מתקיים: $o(1) = 10, o(2) = 5, o(3) = 10, o(4) = 5, o(5) = 2, o(6) = 5, o(7) = 10, o(8) = 5, o(9) = 10$. ננסה לחלץ מכך נוסחה לסדר, ונראה כי כולם מתחלקים ב-10. לכן נוסחה שניתן לקבל היא $o(i) = \frac{n}{(n,i)}$.

קוסטים או מחלקות

הגדרה. תהא $G > H$ וכן יהא $x \in G$. מסמנים: $H \cdot x = \{h \cdot x | h \in H\}$ וזה נקרא קוסט ימני.

משפט. מתקיים:

א. הגודל של קוסט: $|Hx| = |H|$.

ב. כל שני קוסטים הם או שווים או זרים (כלומר החיתוך הוא הקבוצה הריקה).

ג. איחוד כל הקוסטים הוא G.

הוכחה. הסיבה לקיום ג. היא שלכל $x \in G$ מתקיים $x \in H \cdot x$ משום ש- $x = ex \in Hx$ שכן H תת חבורה וקיים בה האדיש e. ■

1.3 הוכחת משפט לגראנז'

הוכחה. מהמשפט הקודם מתקיים כי הקוסטים הם למעשה חלוקה של G, כלומר אם יש לנו k קוסטים שונים, אז יתקיים $|G| = k \cdot |H|$. ■

נרצה להוכיח את סעיף ב' של המשפט עליו ההוכחה מתבססת.

הוכחה. צריך להוכיח שאם שני קוסטים Hx, Hy אינם זרים, הם זהים. אי זרות פירושה כי קיים $z \in Hx \cap Hy$. ולכן: $\exists h_1 \in H : z = h_1 x$ וכן $\exists h_2 \in H : z = h_2 y$. כך ש- $h_1 x = h_2 y$ $\Leftarrow$ $h_2^{-1} h_1 = y x^{-1}$. נסמן: $h = h_2^{-1} h_1 \in H$ (השייכות מתקיימת מכך ש-H חבורה בפני עצמה ולכן יש סגירות לפעולה).

נרצה להראות כי $Hx = Hy$. שוויון קבוצות מראים בהכלה דו-כיוונית.

כיוון ראשון: $Hy \subseteq Hx$. יהא $u \in Hy$ כלומר $u = h_3 y$ עבור $h_3 \in H$. וממה שהראנו קודם, מתקיים $u = h_3 hx$ ולכן עבור $h' = h_3 h$ מתקיים כי $u \in Hx$.

כיוון שני: הכיוון הזה הוא סימטרי לכיוון הקודם כי ההבדל בין y ל-x סמנטי לחלוטין. ■

הקדמה - הגדרת חבורת הקוסטים: $Hx \cdot Hy = H(x \cdot y)$

משפט. תנאים שקולים לכך שקוסטים שווים:

א. $Hx = Hy$

ב. $y \cdot x^{-1} \in H$

ג. $x \cdot y^{-1} \in H$

ד. $x \in Hy$

ה. $y \in Hx$

הוכחה. תנאים שקולים זה אם ורק אם בין כל אחד מהם. למשל הוכחת ד' גורר א': $x \in Hy$, וכן ידוע כי $x \in Hx$ ואז $Hx \cap Hy = \emptyset$ ולכן לפי המשפט הקודם $Hx = Hy$. ■