

ת"ח הנוצרת ע"י ת"ק

הגדרה

תהא G חבורה. $\emptyset \neq A \subseteq G$ ת"ק לא ריקה של G .

$$\langle A \rangle := \bigcap_{\substack{H \leq G \\ A \subseteq H}} H$$

כלומר, $\langle A \rangle$ החיתוך של כל ת"ח של G המכילות את A .

טענה

$\langle A \rangle$ ת"ח של G

הוכחה

ראינו בסוף השיעור הקודם שחיתוך של ת"ח הוא ת"ח.

עובדה

$\langle A \rangle$ היא הת"ח המינימלית ביחס להכלה המכילה את A . ז.א. אם $B \leq G$, ו $A \subseteq B$ אז $\langle A \rangle \leq B$
הוכחה: השלם (תרגיל)

הערה

$\langle A \rangle$ נקראת ת"ח הנוצרת ע"י A .

סימון

A ת"ק לא ריקה של G . נסמן $A^{-1} := \{a^{-1} : a \in A\}$

משפט

תהא G חבורה. $\emptyset \neq A \subseteq G$. היא קבוצת כל המכפלות מאורך סופי של אברים מתוך $A \cup A^{-1}$.

הוכחה

נסמן $B := \{x_1 \cdot \dots \cdot x_k : k \in \mathbb{N}, \forall i x_i \in A \cup A^{-1}\}$ קבוצת כל המכפלות מאורך סופי של אברים מתוך $A \cup A^{-1}$.

1.ע.ט B ת"ח של G .

הוכחת ט.ע.1 B לא ריקה כי $\emptyset \neq A \subseteq B$.
 B סגורה לכפל, כי לכל שני איברים ב B $x_1 \dots x_k z_1 \dots z_m$ מכפלתם $x_1 \dots x_k z_1 \dots z_m$ היא מכפלה מאורך $k+m$ (סופי) של איברים מתוך $A \cup A^{-1}$ ולכן איבר ב B .
 B סגורה להופכי כי לכל איבר $x_1 \dots x_k \in B$, $(x_1 \dots x_k)^{-1} = x_k^{-1} x_{k-1}^{-1} \dots x_1^{-1} \in B$.
 B מש"ל ט.ע.

מסקנה: B ת"ח המכילה את A , לכן $\langle A \rangle \subseteq B$.

נותר להראות $B \subseteq \langle A \rangle$. זה נכון כי $\langle A \rangle$ היא ת"ח המכילה את A . בגלל שהיא תת חבורה היא סגורה תחת הופכי. לכן $A^{-1} \subseteq \langle A \rangle$. מכאן ש $\langle A \rangle \subseteq A \cup A^{-1}$. $\langle A \rangle$ ת"ח ולכן סגורה תחת כפל, לכן גם מכפלות מאורך סופי של איברים מתוך $A \cup A^{-1}$ נמצאים ב $\langle A \rangle$. מכאן $B \subseteq \langle A \rangle$. ■

משפט

תהא G חבורה. $\emptyset \neq A \subseteq G$. היא קבוצת כל המכפלות מאורך סופי של איברים מתוך $A \cup A^{-1}$.

דוגמאות

(1) $G = \mathbb{Z}$, $A = \{6, 10\}$, $\langle A \rangle = \{6k + 10m : k, m \in \mathbb{Z}\} = 2\mathbb{Z}$.
 באופן כללי, $G = \mathbb{Z}$, $A = \{m, n\}$, אזי $\langle A \rangle = (m, n)\mathbb{Z}$ - מחלק משותף מקסימלי של m ו n .
 אם ניקח מספרים ראשוניים $G = \mathbb{Z}$, $A = \{p_1, p_2\}$, כאשר p_1, p_2 ראשוניים, נקבל $\langle \{p_1, p_2\} \rangle = (p_1, p_2)\mathbb{Z} = \mathbb{Z}$.

הגדרה

תהא G חבורה. $\emptyset \neq A \subseteq G$. אם $\langle A \rangle = G$ אז A נקראת קבוצה יוצרת או קבוצת יוצרים של G .

הגדרה וסימון

תהא G חבורה. אם $A = \{g\}$ כאשר $g \in G$ (כלומר A קבוצה עם אבר אחד) אז מסמנים $\langle \{g\} \rangle := \langle g \rangle$ (כלומר משמיטים סוגריים מסולסלים).
 ת"ח כזו, כלומר שנוצרת ע"י קבוצה בת איבר אחד, נקראת ת"ח ציקלית.

עובדה

תהא G חבורה, $g \in G$.

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

הוכחה

על פי המשפט לאיל $\langle g \rangle$ שווה לקבוצת המכפלות מאורך סופי של $\{g, g^{-1}\}$.

דוגמה

$$\begin{aligned}G &= \mathbb{Z} \\ \langle 2 \rangle &= 2\mathbb{Z} \\ \langle m \rangle &= m\mathbb{Z} \\ \langle 1 \rangle &= \mathbb{Z} \text{ - יוצא ש } \mathbb{Z} \text{ נוצרת ע"י איבר אחד!}\end{aligned}$$

הגדרה

G חבורה ציקלית אם קיים $g \in G$ כך ש $G = \langle g \rangle$.

דוגמה: \mathbb{Z} ציקלית כי נוצרת ע"י 1. $\langle 1 \rangle = \mathbb{Z}$.

הגדרה

סדר של אבר $g \in G$ היא סדר ת"ח הנוצרת על ידו. סימון: $o(g) := |\langle g \rangle|$.

דוגמה: \mathbb{Z} , לכל $m \in \mathbb{Z}, m \neq 0$, $o(m) = |m\mathbb{Z}| = \infty$. עבור $m = 0$, $o(0) = |0 \cdot \mathbb{Z}| = 1$.

עוד דוגמה: לכל חב' G , $o(e) = |\langle e \rangle| = 1$.

טענה

תהא G חבורה, $g \in G$. $g = e$ אם $o(g) = 1$.
הוכחה: תרגיל

עובדה

כל חבורה ציקלית היא אבלית.

הוכחה

תהא G חבורה, $g \in G$ כך ש $G = \langle g \rangle$. אז $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ ולכן לכל $x, y \in G$ קיימים $m, n \in \mathbb{Z}$ כך ש $x = g^m, y = g^n$ ואז

$$xy = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = xy$$

שאלה - האם ההיפך נכון?

האם יש חב' אבלית שאינה ציקלית?

טענה לא כל חבורה אבלית היא ציקלית.

הוכחה \mathbb{Q} אינה ציקלית. אחרת קיים $q = \frac{a}{b} \in \mathbb{Q}$, שלמים a, b , כך ש $\langle q \rangle = \mathbb{Q}$. כלומר

$$\blacksquare \frac{1}{b+1} \notin \left\{ \frac{na}{b} : n \in \mathbb{Z} \right\} \text{ ברור. } \mathbb{Q} = \left\langle \frac{a}{b} \right\rangle = \left\{ \frac{a}{b}n : n \in \mathbb{Z} \right\}$$