הגדרה

חבורה G נקראת **חבורה אבלית** אם $\forall x,y: xy = yx$

דוגמה

$\mathbb{Z}_n$ חבורה אבלית, כי $[a]+[b]=[a+b]=[b+a]=[b]+[a]$

U_n גם חבורה אבלית מאותה סיבה.

תזכורת

$H \subseteq G$ נקראת תת חבורה אם H חבורה ביחס לכפל המושרה מ G – ($\Leftrightarrow H \neq \phi$ סגורה לכפל ולהופכי).

הערה

חיתוך משפחה של תת חבורה הוא תת חבורה.

נניח שלכל $\lambda \in \Lambda$, $H_\lambda \leq G$ תת חבורה.

אז $\bigcap_{\lambda\in\Lambda} H_\lambda$ תת חבורה

לדוגמה, אם S תת קבוצה של חבורה G,

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

זו תת החבורה המינימלית שמכילה את S.

נתבונן במקרה שבו $S=\{a\}$.

מיד יוצא ש - $\forall n \in \mathbb{Z}: a^n \in \langle a\rangle$.

הגדרה

חבורה G נקראת **חבורה ציקלית** אם קיים $a \in G$ כך שמתקיים:

$$G = \{a^k | k \in \mathbb{Z}\}$$

דוגמאות

$$\mathbb{Z}_4 = \{0,1,2,3\} = \langle 1\rangle$$
$$\{1,4\} = \langle 4\rangle \leq U_5 = \{1,2,3,4\} = \langle 2\rangle$$

U_{12} לא ציקלית.

דוגמא כללית

$\mathbb{Z}$ ציקלית. $\mathbb{Z}$ נוצרת על ידי 1 (וגם על ידי -1) בלבד.

$\mathbb{Z}_n$ ציקלית לכל n, נוצרת על ידי 1 (למשל).

משפט

כל חבורה ציקלית איזומורפית היא $\mathbb{Z}$ או $\mathbb{Z}_n$ (לאיזשהו $n \geq 1$).

הגדרה

חזקות של a:

$$\begin{aligned} a^1 &= a \\ a^0 &= 1 \\ a^{n+1} &= a \cdot a^n \\ a^{-n} &= (a^n)^{-1} \end{aligned}$$

הוכחה

תהי G חבורה ציקלית, $G = \langle a \rangle$.

נחלק למקרים:

- $\underline{|G| = \infty}$

נגדיר פונקציה $f: \mathbb{Z} \to G$ לפי $f(n) = a^n$.

כמובן,

$$f(n+m) = a^{n+m} = a^n \cdot a^m = f(n) \cdot f(m)$$

לפי ההנחה, f על. f חד חד ערכית כי G אינסופית.

- $\underline{|G| = n}$

נוכיח ש - $G \cong \mathbb{Z}_n$. נבנה פונקציה $f: \mathbb{Z}_n \to G$ לפי $f([k]) = a^k$. צריך לבדוק שזה לא תלוי בנציגים. נוכיח ש - $a^n = 1$. נתבונן באיברים $\{1, a, a^2, \cdots\}$.

נסמן: $m = \min\{i, a^i = 1\}$. מכיוון ש – G סופית יש חזרות ברשימה, כלומר יש $k < k'$ כך ש - $a^k = a^{k'} \Leftarrow a^{k'-k} = 1$, ולכן $m < \infty$. לפי ההנחה, $1, a, a^2, \cdots$ שונים זה מזה. לכן, $n = |G| = |\{1, \cdots, a^{n-1}\}| = m$. כעת, אם $k' \equiv k (mod\ n)$ אז:

$$a^{k'-k} = a^{n \cdot \frac{k'-k}{n}} = (a^n)^{\frac{k'-k}{n}} = 1$$

f על כי G ציקלית, חד חד ערכית כי הוכחנו.

□