תזכורת:

תהי G חבורה. תת קבוצה לא ריקה $H\subseteq G$ הינה תת-חבורה אם:

1) סגורה לכפל: לכל $h_1,h_2\in H$ גם $h_1h_2\in H$

2) סגורה להפכיים: לכל $h\in H$ גם $h^{-1}\in H$

דוגמאות:

-1) תהי G חבורה. אזי, G תת-חבורה של עצמה

0) תהי G חבורה כלשהי: $H=\{e\}$ תת-חבורה $(e^{-1}=e\ ,\ e\cdot e=e)$

תת חבורה טריוויאלית

1) תהי G חבורה כלשהי. יהי $g\in G$. נגדיר

$$g^0=e \quad g^1=g \qquad g^{n+1}=g^ng\ ,\ g^{-n-1}=g^{-n}g^{-1}$$

טענה:

תהי G חבורה, $g\in G$. לכל $n,m\in\mathbb{Z}$. מתקיים $g^n\cdot g^m=g^{n+m}$

הוכחה:

באינדוקציה

נגדיר את הקבוצה

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

זאת תת חבורה.

סגירות לכפל: $a,b\in\langle g\rangle$ אזי $a=g^n, b=g^m$. לפי הטענה,

$$ab=g^{n+m}\in\langle g\rangle$$

סגירות להפכיים: $(g^n)^{-1}=g^{-n}\in\langle g\rangle \Leftarrow g^n\cdot g^{-n}=e$

תת-החבורה $\langle g\rangle$ נקראת תת-החבורה הציקלית הנוצרת על ידי g.

ה'.ו תהי החבורה הקטנה ביותר שמכילה את g.
כלומר, יהי $H \leq G$ תת חבורה. כך e $g \in H$ אז $\langle g \rangle \leq H$
נראה דוגמאות של חבורות ציקליות
הוכחה:
יהי $g \in H$. לכל $n \geq 1$, $g^n \in H$ (אינדוקציה על n: יהי $g^n \in H$
$g^{n+1} = g^n \cdot g \in H$
סגירות
אזי $g^{-n} = (g^n)^{-1} \in H$ כי H סגורה להפכים. $g^0 = e \in H$

ב) $G = \mathbb{Z}$ (עם חיבור (+))
$a \in \mathbb{Z} \Leftarrow$ $a^2 = a+a, a^3 = a+a+a, \ldots$

$\langle a \rangle = a\mathbb{Z} = \{na : n \in \mathbb{Z}\} = \{b \in \mathbb{Z} : a | b\}$
זו תת חבורה (מקרה פרטי של תת חבורה ציקלית
$0\mathbb{Z} = \langle 0 \rangle = \{0\}$

טענה:
תהי $H \leq \mathbb{Z}$ תת חבורה. אזי ק"ם $a \geq 0$ כך e $H = a\mathbb{Z}$
הוכחה:
אם $H = \{e\} = \{0\}$ תת החבורה הטריוויאלית, $H = 0\mathbb{Z}$
נניח $H \neq \{0\}$
לכן יש ב- H איברים לא אפס"ם
H סגורה להפכים ולכן תמיד יש בה איברים חיוביים
אזי הקבוצה $S = \{b \in H : b > 0\}$ לא ריקה
ניקח $a = \min S$. אזי לפי ההגדרה של S $a \in S \subseteq H$
לכן $a \in H$ ולכן $\langle a \rangle = a\mathbb{Z} \leq H$

יהי $b\in H$. לפי חילוק עם שארית $b=qa+r$

כאשר $q\in\mathbb{Z}$ ו- $0\le r<a$

בפרט $r=b-qa=b+(-qa)\in H$

לכן $r\in H$. ובכל לא יתכן ש $1\le r\le a-1$. כי a הוא

האיבר החיובי המינימלי לכן $r=0$ ו- $b=qa\in a\mathbb{Z}$

לכן $H\subseteq a\mathbb{Z}$. ומה"נ $H=a\mathbb{Z}$

3) $G=GL_2(\mathbb{R})$ (מטריצות 2×2 הפיכות מעל $\mathbb{R}$) עם כפל מטריצות

ניקח $a=\begin{pmatrix}1&1\\0&1\end{pmatrix}$, $b=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$

נתבונן בתת-חבורות הציקליות $<a>,<b>$

$$a^2=\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}1&2\\0&1\end{pmatrix}$$

$$a^3=a^2a=\begin{pmatrix}1&3\\0&1\end{pmatrix}$$

מוכיחים באינדוקציה על n $\quad a^n=\begin{pmatrix}1&n\\0&1\end{pmatrix},\ a^{-n}=\begin{pmatrix}1&-n\\0&1\end{pmatrix}$

לכן: $<a>=\left\{\begin{pmatrix}1&n\\0&1\end{pmatrix}:n\in\mathbb{Z}\right\}$

$$b^2=\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}=\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$$

$$b^3=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\qquad b^4=\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

אם $n=4q+r$ $(0\le r\le 3)$

אז $b^n=b^{4q}b^r=b^r$

$$<b>=\{b,b^2,b^3,e\}=\left\{\begin{pmatrix}0&1\\-1&0\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\begin{pmatrix}0&-1\\1&0\end{pmatrix},\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\},\ |<b>|=4$$

(4 $G = GL_2(\mathbb{R})$

$H = SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{matrix} a,b,c,d \in \mathbb{Z} \\ ad-bc=1 \end{matrix} \right\}$

נוכיח כי $H \le G$ תת חבורה

סגירות לכפל:

$A,B \in SL_2(\mathbb{Z}) \Rightarrow \det(AB) = \det A \cdot \det B = 1 \Rightarrow AB \in SL_2(\mathbb{Z})$

סגירות להפכים:

$A^{-1} = \frac{1}{\det A}(\operatorname{adj} A)$

כל האיברים של $\operatorname{adj} A$ הם דטרמיננטות של מינורים של A

ולכן שלמים

$A \in SL_2(\mathbb{Z}) \Rightarrow A^{-1} = \operatorname{adj}(A)$

לכן A^{-1} מטריצה שלמה $A^{-1} \in SL_2(\mathbb{Z})$

לכן $SL_2(\mathbb{Z}) \le GL_2(\mathbb{R})$ הינו תת חבורה

(5 תהי A קבוצה. $S_A = \{f : A \to A,$ f חח"ע ועל$\}$ (עם הרכבת פו')

יהי $a \in A$. המייצב של a הינו $Stab(a) = \{f \in S_A \mid f(a) = a\}$

אצ' $Stab(a) \le S_A$ הינו תת חבורה.

סגירות לכפל: $f,g \in Stab(a)$ אצ'

$f \circ g(a) = f(g(a)) = f(a) = a$

לכן $f \circ g \in Stab(a)$

איבר הופכי: $f \in Stab(a)$ אצ' $f(a) = a$ לכן $f^{-1}(a) = a$

ולכן $f^{-1} \in Stab(a)$

לכן $Stab(a)$ תת חבורה

הגדרה: תהי G חבורה, $g\in G$.
תהי $S=\{n\in\mathbb{N} \mid g^n=e\}$. הסדר של g הינו

$$O(g)=\begin{cases} \min S & : S\neq\emptyset \\ \infty & : S=\emptyset \end{cases}$$

במילים אחרות $O(g)$ הינו החזקה הקטנה ביותר כך e
$g^n=e$. $O(g)=\infty$ אם חזקה חיובית כזאת לא קיימת

הגדרה: תהי G חבורה. הסדר של G הינו העוצמה של הקבוצה
G, ורושמים $|G|$

טענה:
תהי G חבורה, $g\in G$. אזי $|\langle g\rangle|=O(g)$

הוכחה:
אם $O(g)=\infty$: צריך להוכיח שהחבורה הציקלית הינה אינסופית
$$\langle g\rangle=\{\dots,g^{-2},g^{-1},e,g^1,g^2,\dots\}$$
נוכיח שאם $n\neq m$ $g^n\neq g^m$
נב"ש $g^n=g^m$ אך $n\neq m$
בלי הגבלת הכלליות, $m<n$. אזי:
$$g^n=g^m \Rightarrow g^{n-m}=e$$
אבל $n-m\in\mathbb{N}$ ולכן $O(g)<\infty$ בסתירה.
לכן, כל החזקות של g שונות, $|\langle g\rangle|=\infty$

אם $O(g)<\infty$: אז תהי $T=\{n\in\mathbb{Z}: g^n=e\}$. נשים לב כי $T\leq\mathbb{Z}$
הינה תת חבורה של $\mathbb{Z}$
אכן $O(g)\in T$, לכן $T\neq\emptyset$

סגירות לכפל: $g^{n+m}=g^ng^m=e \Leftarrow n,m\in T$

לכן $n+m\in T$ (T סגורה לחיבור)

סגירות להופכי: $g^{-n}=(g^n)^{-1}=e^{-1}=e \Leftarrow g^n=e \Leftarrow n\in T$

$\Downarrow$

$-n\in T$

לכן T סגורה להופכיים

הוכחנו ש- $T\subseteq\mathbb{Z}$ תת-חבורה

הנחנו כי $o(g)$ סופי. לכן קיים איבר חיובי של T

בפרט T אינה תת החבורה הטריוויאלית.

הוכחנו שכל תת-חבורה לא טריוויאלית $T\subseteq\mathbb{Z}$

הינה $T=a\mathbb{Z}$ כאשר a הינו האיבר החיובי

המינימלי של T.

לפי ההגדרה של הסדר של איבר, האיבר החיובי

המינימלי של T הינו $o(g)$.

לכן, $T=o(g)\mathbb{Z}$

רוצים להוכיח כי $|\langle g\rangle|=o(g)$

יהי $x\in\langle g\rangle$. אזי $g^m=x$. לפי חילוק עם שארית:

$m=q\,o(g)+r$ ו- $0\le r<o(g)$

אזי $x=g^m=g^{q\,o(g)}g^r$. אבל $q\cdot o(g)\in o(g)\mathbb{Z}=T$

כלומר, $g^{q\cdot o(g)}=e$. לכן:

$$g^m=g^{q\cdot o(g)}g^r=g^r\in\{g^0,\dots,g^{o(g)-1}\}$$

וסה"כ $|\langle g\rangle|\le o(g)$

נותר להראות e, $g^0,\dots,g^{o(g)-1}$ שונים

נב"ש קיימים $0\le m<n\le o(g)-1$ כך ש $g^m=g^n$

אזי $g^{n-m}=e \Leftarrow n-m\in T$

וגם $0<n-m\le o(g)-1$

בסתירה למינימליות של $o(g)$. לכן $|\langle g\rangle|=o(g)$

מסקנה:

יהי $g\in G$ ויהי מספר סופי יהי $n\in\mathbb{Z}$. אזי $g^n=e \Longleftrightarrow o(g)|n$

הוכחה:

$$T=o(g)\mathbb{Z} \Leftarrow g^n=e \Longleftrightarrow n\in T \Longleftrightarrow n\in o(g)\mathbb{Z} \Longleftrightarrow o(g)|n$$

דוגמאות:

1) $G=GL_2(\mathbb{R})$. $a=\begin{pmatrix}1&1\\0&1\end{pmatrix}$, לכל $n\in\mathbb{N}$ $a^n=\begin{pmatrix}1&n\\0&1\end{pmatrix}\neq I$. לכן $o(a)=\infty$. וגם ראינו $\langle a\rangle=\left\{\begin{pmatrix}1&n\\0&1\end{pmatrix}:n\in\mathbb{Z}\right\}$ לכן $|\langle a\rangle|=\infty$

$b=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ ראינו כי $o(b)=4$ וגם $|\langle b\rangle|=4$

2) $G=\mathbb{Z}$ (עם חיבור) $o(g)=\begin{cases}1 & g=0\\ \infty & g\neq 0\end{cases}$

3) $G=\mathbb{Z}_n$ (מחלקות שקילות מודולו n) (פעולה): $[a]+[b]=[a+b]$

צריך להוכיח שהפעולה מוגדרת היטב. כלומר, לא תלויה בבחירה של הנציגים a,b של המחלקות שרוצים לחבר

למשל: $\mathbb{Z}_6$ $[4]+[5]=[9]=[3]$

$[4]=[-2]$ $[5]=[611]$ $[-2]+[611]=[609]=[3]$

נניח לכן שאם $[a_1]=[a_2]$, $[b_1]=[b_2]$

כלומר,

$a_1 \equiv a_2 \pmod n \Rightarrow n|(a_2-a_1)$

$b_1 \equiv b_2 \pmod n \Rightarrow n|(b_2-b_1)$

אז קיימים $c_1,c_2\in\mathbb{Z}$ כך ש

$$\begin{array}{l} a_2-a_1=c_1n \\ b_2-b_1=c_2n \end{array} \Rightarrow \begin{array}{l} a_2=a_1+c_1n \\ b_2=b_1+c_2n \end{array} \Rightarrow a_2+b_2=a_1+b_1+(c_1+c_2)n$$

$$\Downarrow$$

$$a_2+b_2\equiv a_1+b_1 \pmod n$$

לכן $[a_1+b_1]=[a_2+b_2]$ והחיבור של מחלקות מוגדר היטב

נחשב את הסדרים של כל האיברים של $\mathbb{Z}_6$

$[0]=e \Rightarrow O([0])=1$

$g=[1] \Rightarrow g^6=[6]=[0]=e \Rightarrow O([1])=6$

$g=[2] \Rightarrow O([2])=3 \quad (g^3=g^2g \quad [4]+[2]=[6]=[0]=e)$

$g=[3] \Rightarrow O([3])=2$

$g=[4] \Rightarrow O([4])=3$

$g=[5] \Rightarrow O([5])=O([1]^{-1})=O([1])=6$

טענה:

$G=\mathbb{Z}_n$ יהי $[a]\in\mathbb{Z}_n$. אזי $O([a])=\dfrac{n}{gcd(a,n)}$

הוכחה:

תהי k החזקה החיובית הכי קטנה כך ש $[a]^k=[ka]=e$.

צריך להוכיח $k=\dfrac{n}{gcd(a,n)}$

נשים לב כי $[a]^k=e \Leftrightarrow [ka]=[0] \Leftrightarrow ka\equiv 0 \pmod n \Leftrightarrow$

$\iff n|ka \iff n|ka$ וגם $n|kn \iff n|\gcd(ka,kn) \iff$

$\iff n|k\cdot\gcd(a,n) \iff \frac{n}{\gcd(a,n)}|k$

ולפי המסקנה הקודמת: $\iff k=\frac{n}{\gcd(a,n)}$ $(o(g)|n \iff g^n=e)$

(השתמשנו בכך שאם $n|x$ וגם $n|y$ אזי $n|\gcd(x,y)$)