חבורות ציקליות

תזכורת

תהא G חבורה, $A \subseteq G$ ת"ק. אם $\langle A\rangle = G$ אז A נקראת קבוצת יוצרים. אם יש בG איבר $g\in G$ כך ש$G=\langle g\rangle = \langle\{g\}\rangle$ אז G נקראת חב' ציקלית.

הראינו

כל חבורה ציקלית היא אבלית. לא כל חבורה ציקלית היא אבלית.

משפט

תהא G חב' ציקלית. אם הסדר של G אינו סופי אז $G\cong\mathbb{Z}$. אם הסדר של G הוא n (n מס' טבעי) אז $G\cong \mathbb{Z}_n$.

הוכחה

תהא G חב' ציקלית. אז קיים $y\in G$ כך ש$G=\langle g\rangle$.

מקרה א. לכל k סופי $g^k\neq e$.
במקרה זה לכל $j\neq i$ שלמים $g^j\neq g^i$, אחרת, כלומר אם $g^j=g^i$, אז $g^{-i}g^j = g^{-i}g^i \Leftarrow e=g^{j=i}$ בסתירה לתנאי המקרה.
נתבונן בהעתקה $\varphi:\mathbb{Z}\to G$ המוגדרת ע"י $\varphi(k) := g^k$. φ חח"ע לפי $g^j\neq g^i$. φעל כי $\{g^m : m\in\mathbb{Z}\}=\langle g\rangle=G$. לכן לכל איבר $x\in G$ קיים m שלם כך ש$\varphi(m)=g^m=x$.
φ הומומורפיזם כי לכל $m_1,m_2\in\mathbb{Z}$

$$\varphi(m_1+m_2)=g^{m_1+m_2}=g^{m_1}g^{m_2}=\varphi(m_1)\varphi(m_2)$$

<u>מסקנה</u>: φ איזומורפיזם, ולכן במקרה א $G\cong\mathbb{Z}$ (והסדר של G אינו סופי).

מקרה ב. קיים $k\neq 0$ שלך כך ש$g^k=e$.
ראשית, ניתן להניח בה"כ שk חיובי. אחרת, אז $-k$ חיובי ו$g^{-k}=\left(g^k\right)^{-1}=$ $e^{-1}=e$.
קיים n חיובי מינימלי עבורו $g^n=e$, כלומר $n:=\min\left\{k\in\mathbb{N}: g^k=e\right\}$.

<u>טענת עזר</u>: במקרה זה, G חבורה מסדר n שאיבריה $G=\left\{g^0,g^1,...g^{n-1}\right\}$.
<u>הוכחת ט.ע.</u>: ראשית, לפי ההנחה $G=\langle g\rangle=\{g^m:m\in\mathbb{Z}\}$. כעת, לפי משפט השארית של אוקלידס, לכל m שלם קיימים $q\in\mathbb{Z}$, $0\le r<n$ שלם כך ש$m=nq+r$, ולכן

$$g^m=g^{nq_m+r_m}=g^{nq_m}g^{r_m}=(g^n)^{q_m}g^{r_m}=e^{q_m}g^{r_m}=g^{r_m}\in\left\{g^i:0\le i\le n\right\}$$

מכאן $G=\langle g\rangle=\{g^m:m\in\mathbb{Z}\}\subseteq\left\{g^i:0\le i<n\right\}$. מאידך, ברור $G=\langle g\rangle\left\{g^i:i\in\mathbb{Z}\right\}\supseteq\left\{g^i:0\le i<n\right\}$ לכן $G=\left\{g^0,...g^{n-1}\right\}$.
כדי להשלים הוכחת ט.ע., נותר להראות שאין $0\le j_1<j_2<n$

כך ש-$g^{j_2} = g^{j_1}$. אחרת $e = g^{j_2 - j_1}$, $0 < j_2 - j_1 < n$, סתירה למינימליות n.
מש"ל ט.ע.

נתבונן בהעתקה $\varphi : \mathbb{Z}_n \to G$ המוגדרת ע"י $\forall k \in \mathbb{Z}_n \; \varphi(k) := g^k$.
φ על כי לכל $x \in G$, לפי ט.ע. קיים $0 \le m < n$ כך ש-$x = g^m$, ולכן, לכל x קיים מקור, כי $x = g^m = \varphi(m)$.
מכיוון ש-$|G| = |\mathbb{Z}_n|$ ו-φ על, לכן φ גם חח"ע.
לבסוף, φ הומ'. אכן לכל $m_1, m_2 \in \mathbb{Z}_n$

$$\varphi(m_1 + m_2) = g^{(m_1+m_2) \bmod n} = g^{m_1+m_2} = g^{m_1} g^{m_2} = \varphi(m_1)\varphi(m_2)$$

<u>מסקנה</u>: במקרה ב' G סופית מסדר n ואיז' ל-$\mathbb{Z}_n$.

דוגמה

א)

$$G = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k : k \in \mathbb{Z} \right\} \subseteq SL_2(\mathbb{F})$$

חבורה ציקלית לפי הגדרתה.
<u>הערה</u>: $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ (הוכח!)

$$\begin{pmatrix} 1 & k_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & k_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{k_1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{k_2} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{k_1+k_2} = \begin{pmatrix} 1 & k_1+k_2 \\ 0 & 1 \end{pmatrix} \xrightarrow{e} k_1+k_2$$

אם $\mathbb{F} = \mathbb{R}$ (או כל שדה אחר מסדר אינסופי) $G \cong \mathbb{Z}$. אם $\mathbb{F}$ שדה עם <u>מאפיין</u> p אז $G \cong \mathbb{Z}_p$.

תזכורת

הסדר של אבר $g \in G$: $o(g) := |\langle g \rangle|$

תרגיל

הוכיחו: אם $o(g) = n < \infty$ אז $o(g) = \min\left\{k \in \mathbb{N} : g^k = e\right\}$. אם $o(g)$ הוא אינסופי, אז לא קיים k טבעי כך ש-$g^k = e$.
<u>רמז</u>: הוכחת המשפט לעיל.

נושא חדש: מחלקות ימניות ושמאליות

הגדרה

תהא G חבורה. $H \leq G$ ת"ח של G.
מחלקה ימנית בG היא קבוצה $Hg = \{hg : h \in H\}$ כל$g \in H$ איבר כלשהו.
מחלקה שמאלית בG היא קבוצה $gH := \{gh : h \in H\}$ כש$g \in G$ איבר כלשהו.

דוגמאות

1)

$$G = \mathbb{Z}$$

$$H = 4\mathbb{Z}$$

כיוון ש$\mathbb{Z}$ אבלית מחלקות ימניות=מחלקות שמאליות.

$$0 + 4\mathbb{Z} = 4\mathbb{Z}$$

$$1 + 4\mathbb{Z} = \{..., -3, 1, 5, 9, ...\} = \{n \in \mathbb{Z} : n \mathrm{mod} 4 \equiv 1\}$$

$$2 + 4\mathbb{Z} = \{..., -2, 2, 6, 10, ...\} = \{n \in \mathbb{Z} : n \mathrm{mod} 4 \equiv 2\}$$

$$3 + 4\mathbb{Z} = \{..., -1, 3, 7, 11, ...\} = \{n \in \mathbb{Z} : n \mathrm{mod} 4 \equiv 3\}$$

האיחוד של ארבעת המחלקות האלה הוא $\mathbb{Z}$.

2)

$$G = \mathbb{R}^2$$

$$(x_0, y_0) \neq (0,0), H = \{r(x_0, y_0) : r \in \mathbb{R}\}$$

H הוא ישר העובר דרך הראשית.
$H + \vec{v}$ - ישר המקבלית לH.
אם $\vec{v} \in H$ אז $\vec{v} + H = H$.

בשתי הדוגמאות

מחלקות ימניות מתלכדות או זרות, ואיחודן כל התבורה.

3) תרגילון

$$G = S_3$$

$$H = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\rangle$$

חשב את המחלקות הימניות והשמאליות של H ב-G.

הגדרה

תהא G חבורה, $H \leq G$ ת"ח. נגדיר יחס $\sim_{LH}$ על G: $y \sim_{LH} x$ אם $xH = yH$.
(בדומה: נגדיר $y \sim_{RH} x$ אם $Hx = Hy$)

טענה 1

$\sim_{LH}$ יחס שקילות.

הוכחה

1. רפלקסיבי: לכל $x \in G$, $xH = xH$.
2. סימטרי: לכל $x, y \in G$, $xH = yH \Leftrightarrow yH = xH$
3. טרנזיטיבי: לכל $x, y, z \in G$, $xH = yH \wedge yH = zH \Leftarrow xH = zH$

מסקנה 2

G איחוד זר של מחלקות שקילות תחת $\sim_{LH}$

טענה 3

לכל $h \in H$ $hH = H$

הוכחה

בגלל סגירות הכפל ב-H, ברור $hH = \{hx : x \in H\} \subseteq H$. מאידך לכל $x \in H$, $h^{-1}x \in H$ ולכן $x = h\left(h^{-1}x\right) \in hH$. מכאן $H \subseteq hH$.

טענה 4

לכל $x, y \in G$, $y \sim_{LH} x$ אמ"ם $y \in xH$.

הוכחה

$y \sim_{LH} x$ אמ"ם $xH = yH$. $\Leftarrow$ $y = ye \in xH$.
כיוון שני: נניח $y \in xH$ אז קיים $h \in H$ כך ש-$y = xh$, ואז $yH = (xh)H = x(hH) = xH$. לפי ההגדרה זה אומר $y \sim_{LH} x$.

במילים אחרות

טענה 4 אומרת שמחלקות השקילות תחת $\sim_{LH}$ הן <u>בדיוק</u> המחלקות השמאליות של H בG.

מסקנה 5

G היא איחוד זר של מחלקות שמאליות של H בG.

הוכחה

מסקנה 2 + טענה 4.

טענה 6

לכל $x, y \in G$, $|xH| = |yH|$.

הוכחה

נגדיר העתקה $\varphi : xH \to yH$ ע"י $\forall h \in H, \varphi(xh) = yh$

טענה: זו העתקה מוגדרת היטב, חח"ע ועל.

מוגדרת היטב, כי לכל $z \in xH$ קיים $h \in H$ כך ש$z = xh$, ואם $z = xh_2$, ואם $z = xh_1 \wedge z = xh_2$ אז $h_1 = h_2 \Leftarrow xh_1 = xh_2$. כלומר, לכל אבר $z \in xH$ קיים $h \in H$ יחיד כך ש$z = xh$ ואז $\varphi(z) = yh$.

חח"ע: $z_1 \neq z_2$ אברים שונים בxH אז קיימים $h_1, h_2 \in H$ כך ש$xh_1 = z_1$, $xh_2 = z_2$ו$h_1 \neq h_2$(מדוע?) ואז $\varphi(z_1) = yh_1 \neq yh_2 = \varphi(z_2)$.

על: כי לכל אבר $w \in yH$ קיים $h \in H$ כך ש$w = yh$ ואז $w = \varphi(xh)$, כלומר $xh \in xH$ מקור.

מסקנה 7

לכל $x \in G$ $|xH| = |H|$

הוכחה

נבחר $y = e$ בטענה 6 ואז $eH = H$

מסקנה 8 (אחד הניסוחים של משפט לגרנז')

אם G חבורה סופית, $H \leq G$ ת"ח, אז $|H|$מחלק את $|G|$.

הוכחה

לפי מסקנה 5, G איחוד זר של מחלקות שמאליות. כלומר $G = \coprod x_iH$ [1] לכן $|G| = \sum_i |x_iH|$. לפי מסקנה 7, כל המחוברים מאודו סדר $|H|$ ולכן $|G| = k|H|$ כאשר k מס' המחלקות השמאליות של $|H|$בG.

[1] $\coprod$ זה סימון לאיחוד זר