בס"ד

תרגול מס' 6 במבנים אלגבריים 1

סדר של איבר בחבורה (המשך).

טענה: נניח בחבורה G מתקיים עבור $g,h\in G$: 1. $gh=hg$ 2. $\left(o\left(g\right),o\left(h\right)\right)=1$

אזי: $o\left(gh\right)=o\left(g\right)\cdot o\left(h\right)$.

הוכחה:

נסמן: $o\left(g\right)=n,\ o\left(h\right)=k$ ו- $o\left(gh\right)=m$. צ"ל: $m=nk$.

1. <u>היתכנות</u>: $\left(gh\right)^{nk}\underset{gh=hg}{=}g^{nk}\cdot h^{nk}=\underbrace{\left(g^{n}\right)}_{e}^{k}\cdot\underbrace{\left(h^{k}\right)}_{e}^{n}=e\cdot e=e$

2. <u>מינימליות</u>: נתבונן ב- $g^{mk}=g^{mk}\cdot e=g^{mk}\cdot h^{mk}\underset{gh=hg}{=}\left(gh\right)^{mk}=\underbrace{\left(\left(gh\right)^{m}\right)}_{e}^{k}=e^{k}=e$

מכאן ש- $n\mid mk$ אבל: $\left(n,k\right)=1$ ולכן: $n\mid m$. באותו האופן מוכיחים גם כי: $k\mid m$.

מכאן שגם: $\left[n,k\right]\mid m$. אבל: $\left[n,k\right]=\frac{nk}{\left(n,k\right)}=nk$ כלומר: $nk\mid m\ \Leftarrow\ nk\leq m$. □

<u>תרגיל</u>: הוכח שכל חבורה G אבלית מסדר 6 היא ציקלית.

<u>פתרון</u>: שלבים בפתרון:

1. מתוך משפט לגרנז': $\forall a\in G:\ o(a)\in\{1,2,3,6\}$.
2. אם יש איבר מסדר 6 סיימנו.
3. כיוון ש-$\left|G\right|$ זוגי ישנו לפחות איבר אחד a מסדר 2 (ראה תרגיל).
4. אם ישנו עוד איבר b מסדר 2, אזי: $\left\langle a,b\right\rangle=\{1,a,b,ab\}$ ת"ח מסדר 4 אשר לא מחלק את 6 בסתירה למשפט לגרנז'.
5. יש בהכרח איבר b מסדר 3 ומכיון ש-$\left(2,3\right)=1$ ו-$ab=ba$ (אבליות) ישנו איבר מסדר 6 (ראה תרגיל). ולכן ציקלית.

<u>תרגיל</u>: תן דוגמה של חבורה בה לשני איברים יש סדרים סופיים זרים אך למכפלתם יש סדר אינסופי.

<u>פתרון</u>: עבור: $\mathbf{GL}_2(\mathbb{R}) \ni a=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, b=\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}$ מתקיים: $o(a)=4,\ o(b)=3$

אבל: $ab=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ הוא מסדר אינסופי שכן: $\forall n\in\mathbb{N}: (ab)^n=\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}\neq I_2$.

הגדרה: העתקה בין חבורות $\varphi:(G,\bullet)\to(H,*)$ היא ***הומומורפיזם*** אם היא <u>משמרת פעולה</u>, כלומר:

$$\forall a,b\in G:\quad \varphi(a\bullet b)=\varphi(a)*\varphi(b).$$

בנוסף,

- אם φ היא חח"ע אז היא נקראת ***מונומורפיזם***.
- אם φ היא על אז היא נקראת ***אפימורפיזם***.
- אם φ היא גם חח"ע וגם על אז היא נקראת ***איזומורפיזם***.

דוגמאות:

1. $\varphi:\mathbb{Z}\to\mathbb{Z},\ x\mapsto 2x$ היא מונומורפיזם.
2. $\varphi:U_{10}\to\langle 9\rangle,\ x\mapsto x^2$ היא אפימורפיזם.
3. $\varphi:(\mathbb{R},+)\to\left(\mathbb{R}^+=(0,\infty),\cdot\right),\ x\mapsto 2^x$ היא איזומורפיזם.

טענה: בהינתן הומומורפיזם של חבורות $f:G\to H$, אז:

א. $f:1_G\mapsto 1_H$

ב. $x^{-1}\in G\ \Rightarrow\ f\left(x^{-1}\right)=f(x)^{-1}$.

הוכחה:

א. מתוך שימור הפעולה: $f(1_G)=f(1_G\cdot 1_G)=f(1_G)\cdot f(1_G)$ ומכאן בהכרח: $f(1_G)=1_H$.

ב. עפ"י א': $1_H=f(1_G)=f\left(x\cdot x^{-1}\right)=f(x)\cdot f\left(x^{-1}\right)$ ומכאן שבהכרח: $f\left(x^{-1}\right)=f(x)^{-1}$.

מסקנה: בהינתן איזומורפיזם של מונואידים: $G \simeq H$ מתקיים: $Gr(G) \simeq Gr(H)$ (הצמצום של האיזומורפיזם לקבוצת ההפיכים מעביר כל איבר הפיך בצורה חח"ע לאיבר הפיך בתמונה).

הגדרה: יהא $(R,\bullet)$ מונואיד בו מוגדרת גם פעולת חיבור $+$. אזי המבנה $(R,\bullet,+)$ נקרא ***חוג*** אם:

- מתקיים חוק הפילוג: $a\bullet(b+c)=a\bullet b+a\bullet c,(b+c)\bullet a=b\bullet a+c\bullet a$,
- $(R,+)$ היא חבורה אבלית.

דוגמאות:

1. שדה הוא מקרה פרטי של חוג.
2. $(\mathbb{Z},\bullet,+)$: מונואיד לגבי הכפל וחבורה אבלית לגבי חיבור.
3. $(M_n(\mathbb{R}),\bullet,+)$: חבורה אבלית לגבי חיבור ומונואיד לגבי כפל מטריצות.
4. $(\mathbb{Z}_n,\bullet(\bmod n),+(\bmod n))$.

תרגיל: הראה כי תמונה הומומורפית של חבורה ציקלית היא חבורה ציקלית.

פתרון: אם: $f:G=\langle g\rangle\to H$ אזי: $\forall y\in \mathrm{Im}(f): y=f(g^k)=f(g)^k \Rightarrow \mathrm{Im}(f)=\langle f(g)\rangle$.

משפט: $\forall n,m\in\mathbb{N}: \mathbb{Z}_n\times\mathbb{Z}_m\simeq\mathbb{Z}_{nm} \Leftrightarrow (n,m)=1$ <u>איזומורפיזם של חוגים</u> (שתי הפעולות).

הוכחה:

<u>בכיוון</u> $\Leftarrow$: נגדיר העתקה: $\varphi:\mathbb{Z}_{nm}\to\mathbb{Z}_n\times\mathbb{Z}_m$ ע"י: $\varphi(x)=(x(\bmod m),x(\bmod n))$. נשים לב כי:

$$\varphi(x+y)=((x+y)(\bmod m),(x+y)(\bmod n))=(x(\bmod m),x(\bmod n))+(y(\bmod m),y(\bmod n))$$

כלומר יש שימור פעולה ביחס לחיבור ובאותו האופן מראים גם כי משתמרת פעולת הכפל.

כיוון ש: $(n,m)=1$, עפ"י משפט השאריות הסיני φ חח"ע ועל.

בכיוון $\Rightarrow$: מתוך: $\mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$ נסיק כי גם $\mathbb{Z}_n \times \mathbb{Z}_m$ ציקלית,

כלומר: $\exists (a,b) \in \mathbb{Z}_n \times \mathbb{Z}_m \ : \ o\big((a,b)\big) = nm$.

נשים לב כי: $(a,b)^{[n,m]} = \big([n,m]a, [n,m]b\big) = (nu, mv) = (0,0)$.

אם כן: $nm \le [n,m]$ אבל זה יתכן רק כאשר: $nm = [n,m]$ כלומר: $(n,m) = 1$. □

הגדרה: לכל מספר טבעי n נגדיר את פונקצית אוילר: $\varphi(n) = |U_n|$.

דוגמה: אם p מספר ראשוני, אז: $\varphi(p) = p-1$.

באופן יותר כללי, נחשב לכל חזקה טבעית k את $\varphi\left(p^k\right)$:

האיברים **שאינם** זרים ל- p^k הם: $\left\{p, 2p, 3p, ..., p^k = p^{k-1} \cdot p\right\}$ כלומר ישנם p^{k-1} כאלו.

לכן: $\varphi\left(p^k\right) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$.

טענה: אם $(n,m) = 1$ אז: $\varphi(nm) = \varphi(n) \cdot \varphi(m)$.

הוכחה: $(n,m) = 1 \ \Leftarrow \ \mathbb{Z}_{nm} \simeq \mathbb{Z}_n \times \mathbb{Z}_m \ \Leftarrow \ Gr\left(\mathbb{Z}_{nm}\right) \simeq Gr\left(\mathbb{Z}_n \times \mathbb{Z}_m\right)$ (לגבי כפל) לכן:

$$\varphi(nm) = |U_{nm}| = \left|Gr\left(\mathbb{Z}_{nm}\right)\right| = \left|Gr\left(\mathbb{Z}_n \times \mathbb{Z}_m\right)\right| = \left|Gr\left(\mathbb{Z}_n\right)\right| \cdot \left|Gr\left(\mathbb{Z}_m\right)\right| = |U_n| \cdot |U_m| = \varphi(n) \cdot \varphi(m).$$

מסקנה: נוסחה לחישוב הפונקציה של אוילר: בהינתן פירוק לגורמים ראשוניים: $n = \prod_i p_i^{k_i}$

נקבל: $\varphi(n) = \varphi\left(\prod_i p_i^{k_i}\right) = \prod_i \varphi\left(p_i^{k_i}\right) = \prod_i p_i^{k_i}\left(1 - \frac{1}{p_i}\right) = n \cdot \prod_i \left(1 - \frac{1}{p_i}\right)$.

דוגמה: $160 = 2^5 \cdot 5 \ \Rightarrow \ \varphi(160) = \left(2^5 - 2^4\right) \cdot 4 = 64$.