תרגול 7

מר טאהר עודה
נכתב ע"י בר וייסמן

24 באוגוסט 2023

מבוא לתורת החבורות

הגדרה. קבוצה לא ריקה G ביחד עם פעולה בינארית $* : G \times G \to G$ נקראת חבורה אם מתקיים לכל $a, b, c \in G$:

1. אסוציאטיביות: $a * (b * c) = (a * b) * c$.
2. קיים איבר $e \in G$ המקיים $\forall x \in G$, $x = e * x = x * e$. (ל-e קוראים אדיש).
3. לכל $x \in G$ קיים $b \in G$ כך ש-$x * b = e$. (את b מסמנים ע"י $b = x^{-1}$).

הגדרה. חבורה $(G, *)$ נקראת אבלית (Abel) אם לכל $a, b \in G$ מתקיים

$$a * b = b * a$$

דוגמה.

1. $(\mathbb{N}, +)$ אינה חבורה.
2. $(\mathbb{Z}, +)$ היא חבורה אבלית.
3. $(\mathbb{Z}, *)$ אינה חבורה (אין הופכי לכל $x \in \mathbb{Z}$ אשר שונה מ-± 1).
4. $(\mathbb{F}, +)$ היא חבורה אבלית, לכל שדה $\mathbb{F}$ ופעולת החיבור המוגדרת עליו.
5. $(\mathbb{F}, *)$ אינה חבורה (אין הופכי ל-0).
6. $(\mathbb{F} \setminus \{0_{\mathbb{F}}\}, *)$ היא חבורה אבלית.
7. $(\{\pm 1\}, *)$ היא חבורה אבלית.
8. $(n\mathbb{Z}, +)$ היא חבורה אבלית ($n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n, \dots\}$).
9. $(\mathbb{Z}_n, +_{\mod n})$ היא חבורה אבלית.
10. $(\mathbb{Z}_n, \cdot_{\mod n})$ אינה חבורה.

הגדרה. סדר של חבורה הוא מספר האיברים שיש בה, כלומר $|G|$.
אם יש בה מספר סופי של איברים, אז G נקראת חבורה סופית.
אחרת, היא נקראת חבורה אינסופית (לא נתייחס לעוצמת החבורה - $\aleph_0$/א/...).

<u>שתי חבורות חשובות:</u>

1. $GL_n(\mathbb{F}) = \{A \in M_n(\mathbb{F}) \mid |A| \neq 0\}$ ביחד עם פעולת כפל מטריצות מהווה חבורה. זו חבורה לא אבלית עבור $n > 1$.
2. $SL_n(\mathbb{F}) = \{A \in M_n(\mathbb{F}) \mid |A| = 1\}$ ביחד עם פעולת כפל מטריצות מהווה חבורה לא אבלית.

<u>תכונות:</u> (לכל $m, n \in \mathbb{Z}$)

1. האדיש בכל חבורה הוא יחיד.
2. $\left(a^{-1}\right)^{-1} = a$.
3. $\left(a^{-1}\right)^{n} = \left(a^{n}\right)^{-1}$.
4. $a^{m+n} = a^m * a^n$.
5. $(a*b)^{-1} = b^{-1} * a^{-1}$.
6. חוק הצמצום: $a * b = c * b \Longleftarrow a = c$.
7. $\left(a^m\right)^n = a^{m \cdot n}$.

תרגיל. הראו שאם בחבורה G כל איבר הופכי לעצמו ($b^{-1} = b$) אז G אבלית.

פתרון. יהיו $a, b \in G$, נוכיח כי $ab = ba$:

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

ולכן G אבלית.

תרגיל. תהי G חבורה. האם לכל $a, b \in G$ מתקיים $(ab)^{-2} = b^{-2}a^{-2}$?

פתרון. נעלה את הביטוי בחזקת -1:

$$abab = (ab)^2 \underset{7}{==} \left((ab)^{-2}\right)^{-1} = \left(b^{-2}a^{-2}\right)^{-1} = \left(a^{-2}\right)^{-1}\left(b^{-2}\right)^{-1} = a^2b^2$$

$$abab = a^2b^2 \iff ba = ab$$

ולכן זה נכון רק בחבורות אבליות.

הערה. לכל שדה $\mathbb{F}$, נגדיר $\mathbb{F}^* := \mathbb{F} \setminus \{0\}$.

תרגיל. האם $(\mathbb{Q} \setminus \{0\}, *)$ מהווה חבורה, כאשר $a * b := \frac{a \cdot b}{2}$?

פתרון.

1. תחילה, ברור כי הקבוצה אינה ריקה. נבדוק סגירות - יהיו $a,b\in\mathbb{Q}\setminus\{0\}$. אזי

$$a*b=\frac{a\cdot b}{2}\underbrace{\in}_{\text{בשדה אין מחלקי 0}}\mathbb{Q}\setminus\{0\}$$

2. נבדוק אסוציאטיביות: יהיו $a,b,c\in\mathbb{Q}^*$, אזי

$$(a*b)*c=\frac{a\cdot b}{2}*c=\frac{\frac{a\cdot b}{2}\cdot c}{2}=\frac{abc}{4}$$

$$a*(b*c)=a*\frac{b\cdot c}{2}=\frac{a\cdot\frac{b\cdot c}{2}}{2}=\frac{abc}{4}=(a*b)*c$$

3. קיום אדיש: נחפש $x\in\mathbb{Q}\setminus\{0\}$ כך שלכל $y\in\mathbb{Q}\setminus\{0\}$ מתקיים $x*y=y$.

$$x*y=\frac{x\cdot y}{2}=y\Longrightarrow x=2$$

מכאן, 2 הוא האיבר האדיש.

4. קיום הופכי: יהי $x\in\mathbb{Q}\setminus\{0\}$, מחפשים $y\in\mathbb{Q}\setminus\{0\}$ כך ש-

$$x*y=2\Longrightarrow\frac{x\cdot y}{2}=2\Longrightarrow y=\frac{4}{x}\in\mathbb{Q}\setminus\{0\}$$

הגדרה. תהי $(G,*)$ חבורה. תת-קבוצה $\emptyset\neq H\subseteq G$ נקראת תת-חבורה אם $(H,*)$ מהווה חבורה. מסמנים $H<G$

משפט. $H<G\iff$ התנאים הבאים מתקיימים:

א. $e_G\in H$ (שקול ל-$H\neq\emptyset$).

ב. לכל $a,b\in H$ מתקיים $ab\in H$.

ג. לכל $a\in H$ מתקיים $a^{-1}\in H$.

הערה. לכל חבורה G יש שתי תת-חבורות טריוויאליות: $G,\{e_G\}$.

דוגמה.

1. $n\mathbb{Z}<\mathbb{Z}$.

2. $SL_n(\mathbb{F})<GL_n(\mathbb{F})$.

3. $D(GL_n(\mathbb{F}))<GL_n(\mathbb{F})$ (מטריצות הפיכות אלכסוניות).

4. אם G חבורה ו-$g\in G$ אזי $\langle g\rangle=\{g^k\mid k\in\mathbb{Z}\}$ היא תת-חבורה של g.
(נקראת תת-החבורה הציקלית של הנוצרת ע"י g)

הערה. $\langle g\rangle$ היא תמיד תת-חבורה אבלית:

$$g^{k_1}*g^{k_2}=g^{k_1+k_2}=g^{k_2+k_1}=g^{k_2}*g^{k_1}$$

הגדרה. תהי G חבורה ויהי $g\in G$. הסדר של g הוא המספר הטבעי הקטן ביותר $n\in\mathbb{N}$ כך ש-

$$\underbrace{g*g*\cdots*g}_{\text{פעמים } n}=g^n=e_G$$

מסמנים $o\left(g\right)=n$, ואם לא קיים n כזה מסמנים $o\left(g\right)=\infty$.

דוגמה. $\mathbb{Z}_6=\{0,1,2,3,4,5\}$. האדיש הוא 0, ולכן $o\left(0\right)=1$.

$$\begin{aligned}o\left(1\right)&=6\\o\left(2\right)&=3\\o\left(3\right)&=2\\o\left(4\right)&=3\\o\left(5\right)&=6\end{aligned}$$

משפט. אם $e\neq x\in\mathbb{Z}_n$ כך ש-$\gcd\left(x,n\right)=1$ (כלומר, x ו-n זרים) אזי $o\left(x\right)=n$.

הערה.

1. אם $|G|<\infty$ אזי לכל $g\in G$ מתקיים $o\left(g\right)<\infty$.
2. אם $|G|=\infty$ אזי לכל $g\in G$, $o\left(g\right)\leq\infty$.
3. אם $g^n=e$ אז $o\left(g\right)\mid n$.

תרגיל. מצאו את הסדרים של האיברים הבאים בחבורות המתאימות:

1. $i\in\mathbb{C}^*$.
2. $\begin{bmatrix}0&1\\-1&0\end{bmatrix}\in SL_n\left(\mathbb{R}\right)$.

פתרון.

1. הפעולה היא כפל, $i^1,i^2,i^3\neq1$ אבל $i^4=1$, ולכן $o\left(i\right)=4$.
2. הפעולה היא כפל מטריצות, ולכן

$$A^2=\begin{bmatrix}0&1\\-1&0\end{bmatrix}^2=\begin{bmatrix}-1&0\\0&-1\end{bmatrix}\neq I$$

$$\Longrightarrow A^4=\begin{bmatrix}-1&0\\0&-1\end{bmatrix}^2=I$$

מכאן $o\left(A\right)\mid 4$, ולכן לא ייתכן שהסדר הוא 3, ומתקיים $o\left(A\right)=4$.

תרגיל. יהיו $a,b\in G$ כך ש-$o\left(a\right)=o\left(b\right)=5$ וגם $a^{3}=b^{3}$. הוכיחו כי $a=b$.

פתרון.

$$a^{3}=b^{3}\Longrightarrow a^{6}=b^{6}\Longrightarrow a\cdot\underbrace{a^{5}}_{e}=b\cdot\underbrace{b^{5}}_{e}$$

$$\Longrightarrow a=b$$

טענה. לכל $x,y\in G$ מתקיים $o\left(x\right)=o\left(yxy^{-1}\right)$.

הוכחה. נוכיח עבור סדרים סופיים.

נסמן $o\left(x\right)=n$ ו-$o\left(yxy^{-1}\right)=m$. נראה כי $m\mid n\wedge n\mid m$, ומכך בגלל ש-$n,m\in\mathbb{N}$ נקבל $n=m$.

$$\begin{aligned}\left(yxy^{-1}\right)^{n} & =\left(yxy^{-1}\right)\left(yxy^{-1}\right)\cdots\left(yxy^{-1}\right)\\ & =yx^{n}y^{-1}=yey^{-1}=e\Longrightarrow m\mid n\end{aligned}$$

$$e=\left(yxy^{-1}\right)^{m}=yx^{m}y^{-1}$$

$$\Longrightarrow y^{-1}ey=x^{m}\Longrightarrow x^{m}=e\Longrightarrow n\mid m$$

בסך הכל, קיבלנו כי $n=m$. $\square$

הערה. באותו האופן בדיוק ניתן להוכיח כי $o\left(x\right)=o\left(x^{-1}\right)$ לכל $x\in G$.

הגדרה. יהי $2\leq n\in\mathbb{N}$ פונקציית אוילר היא פונקצייה $\varphi:\mathbb{N}\to\mathbb{N}$ המוגדרת ע"י

$$\varphi\left(n\right)=\left|\left\{ x\in\mathbb{Z}_{n}\mid\gcd\left(x,n\right)=1\right\} \right|$$

דוגמה.

$$\varphi\left(8\right)=\left|\left\{ x\in\mathbb{Z}_{8}\mid\gcd\left(x,8\right)=1\right\} \right|=\left|\left\{ 1,3,5,7\right\} \right|=4$$

$$\varphi\left(10\right)=\left|\left\{ 1,3,7,9\right\} \right|=4$$

הערה.

$$\varphi\left(p\right)=p-1$$

$$\varphi\left(p^{n}\right)=p^{n}-p^{n-1}$$

אם $\gcd(m,n)=1$ אז $\varphi(m\cdot n)=\varphi(m)\cdot\varphi(n)$. למשל:

$$\begin{aligned}\varphi(65)&=\varphi(13\cdot 5)\\&=\varphi(13)\cdot\varphi(5)\\&=12\cdot 4=48\end{aligned}$$

הגדרה. יהי $n\in\mathbb{N}$. נגדיר את חבורת אוילר להיות

$$\mathbb{Z}_n^*=U_n=\{x\in\mathbb{Z}_n\mid \gcd(x,n)=1\}$$

עם פעולת כפל מודולו n. למשל, $\mathbb{Z}_8^*=\{1,3,5,7\}$. שימו לב:

$$|U_n|=\varphi(n)$$

דוגמה. נסתכל על $U_{10}=\{1,3,7,9\}$.

- האדיש הוא 1.
- ההופכי של 3 הוא 7.
- ההופכי של 7 הוא 3.
- ההופכי של 9 הוא 9.

חבורות ציקליות

הגדרה. תהי G חבורה. G נקראת חבורה ציקלית אם קיים $g\in G$ כך ש-

$$G=\langle g\rangle=\{g^k\mid k\in\mathbb{Z}\}$$

לאיבר g קוראים יוצר של G.

דוגמה.

1. $(\mathbb{Z},+)$ היא ציקלית: $\langle 1\rangle=\langle -1\rangle=\mathbb{Z}$.
2. לכל $n\in\mathbb{Z}$, $\mathbb{Z}_n$ ציקלית.

הערה. כל תת-חבורה של חבורה ציקלית היא ציקלית.

תרגיל. הוכיחו או הפריכו:

1. אם G ציקלית אז G אבלית.
2. $(\mathbb{Q},+)$ ציקלית.

פתרון.

1. הוכחנו לפני כן.
2. לא נכון. נניח בשלילה שקיים $\frac{p}{q} \in \mathbb{Q}$ כך ש-$\left\langle \frac{p}{q} \right\rangle = \mathbb{Q}$. נתבונן באיבר $\frac{1}{2q} \in \mathbb{Q}$.
   - כיוון ש-$\left\langle \frac{p}{q} \right\rangle = \mathbb{Q}$, מתקיים

$$\left(\frac{p}{q}\right)^k = \frac{1}{2q} \Longrightarrow \frac{kp}{q} = \frac{1}{2q} \Longrightarrow kp = \frac{1}{2}$$

   - סתירה! (סגירות כפל ב-$\mathbb{Z}$).

<u>כללים:</u>

1. אם $|G| = n$ ו-G ציקלית אזי מספר היוצרים של G הוא $\varphi(n)$. ולכל $d \mid n$ קיימים ב-G $\varphi(d)$ איברים בעלי סדר d.
2. משפט לגרנז' (ניסוח חלקי): אם G חבורה סופית ו-$H < G$ אזי $|H| \mid |G|$.

<u>תזכורת:</u> $o(g) = |\langle g \rangle|$.

מסקנה. אם G סופית אז לכל $g \in G$ מתקיים $o(g) \mid |G|$.

תרגיל. מצאו את כל תתי-החבורות של $\mathbb{Z}_8$.

פתרון. מאחר ו-$\mathbb{Z}_8$ ציקלית, כל תת-חבורה שלה היא גם ציקלית. מכאן, נוכל לבדוק את כל החבורות הנוצרות ע"י האיברים:

$$\langle 0 \rangle = \{0\}, \langle 1 \rangle = \mathbb{Z}_8 = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle, \langle 2 \rangle = \langle 6 \rangle = \{0,2,4,6\}, \langle 4 \rangle = \{0,4\}$$

משפט. U_n ציקלית $\iff$ $n = 1,2,4,p^k,2p^k$ כאשר p ראשוני אי-זוגי ו-$k \geq 1$.

חבורת התמורות

הגדרה. תהי Ω קבוצה סופית, ונניח כי $\Omega = \{1,...,n\}$. תמורה על Ω היא פונקציה חח"ע ועל $\sigma : \Omega \to \Omega$.

את אוסף כל התמורות על קבוצה בת n איברים מסמנים ב-S_n.
שימו לב, $|S_n| = n!$.
הקבוצה S_n יחד עם פעולת הרכבת פונקציות מהווה חבורה.

<u>תזכורת:</u> צורה מטריציונית של תמורה היא, למשל עבור $\Omega = \{1,2,3\}$ ו-σ מעבירה $1 \to 3, 2 \to 2, 3 \to 1$, היא

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

הצורה המעגלית של תמורה זו מתוארת כך: $\begin{pmatrix} 1 & 3 \end{pmatrix}$. 2 הוא נקודת שבת ולכן לא מצוין.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 3 & 2 & 4 & 9 & 10 & 8 & 6 & 1 & 7 \end{pmatrix} \Longrightarrow (\ 1\ \ 5\ \ 9\ )(\ 2\ \ 3\ )(\ 6\ \ 10\ \ 7\ \ 8\ )$$

התמורה ההופכית של σ היא $\begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix}$ (הופכים את השורות), בצורה מעגלית $(\ 3\ \ 1\ )$.

הערה. $(\ x\ \ y\ ) = (\ y\ \ x\ )$.

דוגמה. תמורה הופכית.

$$(\ 1\ \ 2\ \ 3\ \ 4\ )^{-1} = (\ 1\ \ 4\ \ 3\ \ 2\ ) = (\ 4\ \ 3\ \ 2\ \ 1\ )$$

$$(\ 1\ \ 2\ \ 3\ \ 4\ )(\ 1\ \ 4\ \ 3\ \ 2\ ) = (\ 1\ )(\ 4\ )(\ 3\ )(\ 2\ ) = id$$

נמצא את התמורה ההופכית של $(\ 1\ \ 5\ \ 9\ )(\ 2\ \ 3\ )(\ 6\ \ 10\ \ 7\ \ 8\ )$:

$$((\ 1\ \ 5\ \ 9\ )(\ 2\ \ 3\ )(\ 6\ \ 10\ \ 7\ \ 8\ ))^{-1} = (\ 1\ \ 9\ \ 5\ )(\ 2\ \ 3\ )(\ 6\ \ 8\ \ 7\ \ 10\ )$$

דוגמה. הרכבת תמורות בצורה מעגלית.

$$(\ 1\ \ 2\ \ 4\ \ 7\ )(\ 6\ \ 8\ )\circ(\ 6\ \ 9\ \ 1\ \ 3\ \ 2\ \ 7\ )\circ(\ 8\ \ 10\ ) = (\ 8\ \ 10\ \ 6\ \ 9\ \ 2\ \ 1\ \ 3\ \ 4\ \ 7\ )$$

$$(\ 1\ \ 4\ )(\ 2\ \ 3\ )\circ(\ 1\ \ 2\ )(\ 3\ \ 4\ ) = (\ 1\ \ 3\ )(\ 2\ \ 4\ )$$