הגדרה קלה עם

מבנה אלגברי.

הגדרה: תהא G היא קבוצה ויהי עם פעולה בינארית

$$*: G\times G \longrightarrow G$$

המקיימת

1) **סגירות.** לכל $a,b\in G$ $\quad a*b\in G$ (לעתים מכנים
$*$, אם אין חשש לבלבול).

2) **אסוציאטיביות.** לכל $a,b,c\in G$

$$a*(b*c)=(a*b)*c$$

3) **קיום איבר יחידה.** קיים $e\in G$ כך שלכל $a\in G$
$a*e=e*a=a$ — איבר

4) **קיום הופכיים משמאל.** לכל $a\in G$ קיים $b\in G$ כך ש
$a*b=b*a=e$

טענה

1) האיבר היחיד b הנ"ל הוא יחיד ומסומן a^{-1}.
2) לכל $a\in G$ $\quad a=(a^{-1})^{-1}$
3) לכל $a,b\in G$ $\quad (ab)^{-1}=b^{-1}a^{-1}$
4) $e^{-1}=e$.

הוכחה

1) יהי $b\in G$ הופכי של a. נניח $ac=ca=e$, $ab=ba=e$
אז מאסוציאטיביות:

$$b=eb=(ca)b=c(ab)=ce=c$$

2) נוכיח מיידית מהגדרה. יהי

דוגמאות:

4) "כפל": $G=\{0,1\}$ והפעולה $*$ מתוארת ע"י הטבלה משמאל.

$*$	0	1
0	0	1
1	1	0

כלומר כי $0*0=0$; $1^{-1}=1$ כי $1*1=0\oplus 0=0$

א. הוכיחו כי הפעולה $*$ מוגדרת היטב.

ב. הוכיחו כי $(G,*)$ חבורה אבלית.

2) $G=\{0,1,\dots,n-1\}$ עבור $n\geq 2$ והפעולה $*$ היא חיבור מודולו n. תהיה זו הטענה כי $(G,*)=(\mathbb{Z}_n,+)$.

3) $G=\mathbb{Z}_2^n$ עליה הפעולה הקואורדינטית עם $*$ מאיבר ל"י. $(\mathbb{Z}_2^n,+)$ תקרא הקוביה ה-n מימדית.

לשם עזרה $n=2$ איבריה הם $\{00,01,10,11\}$

ושם $1^{-1}=0$

4) $G=(\mathbb{Z},+)$ – חבורה אינסופית.

5) מספרים אלגבריים $A\times A$ עם פעולת הכפל.

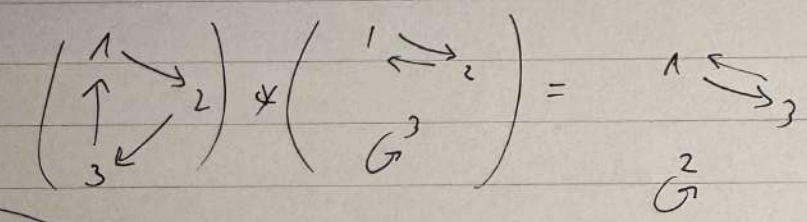
נזכיר כי קבוצת הטרנספורמציות הבאות: $\forall a,b\in\mathbb{R}$ $a\neq 0$ $x\to ax+b$. תהווה חבורה ביחס לפעולת הרצף (או חבורה חלוטית). שם קצר היא חבורה קומבינטורית. איברי החבורה מתוארים בשפה מתמטית ע"י חבורת תמורות סופית. אוסף כל התמורות מסדר n נסמנו S_n ונקרא לו חבורת התמורות על n איברים $\{1,2,\dots,n\}$

עם $*$ = הרכבה. הקבוצה

$$S_3=\left\{ \begin{array}{c} 1\\ 3\quad 2 \end{array},\ \begin{array}{c} 1\\ 2\quad 3 \end{array},\ \begin{array}{c} 1\\ 3\quad 2 \end{array},\ \begin{array}{c} 1\rightleftarrows 2\\ 3 \end{array},\ \begin{array}{c} 1\rightleftarrows 3\\ 2 \end{array},\ \begin{array}{c} 1\quad 2\\ 3 \end{array} \right\}$$

לדוגמא:

$$\begin{pmatrix} 1\rightleftarrows 2\\ 3 \end{pmatrix} * \begin{pmatrix} 1\\ 3\quad 2 \end{pmatrix} = \begin{array}{c} 1\\ 3\quad 2 \end{array}$$



G_1 G_2 G_3

$$G = \left\{ \omega_n^k \mid n > k \geq 0 \right\} \quad \text{ערכי } k \text{ ו-} n \text{ טבעיים.}$$

$e^{\frac{2\pi i}{n}}$

תחת פעולת הכפל. כאשר $*$ הפעולה כפל. כאשר n שלם, ו-k טבעי.

$$\omega_n^k * \omega_n^j = \omega_n^{k+j}$$

$(\mathbb{Z}_n, +)$ הוא חבורה ביחס לחיבור. אותו דבר לחיבור.

הגדרה תהי $\varphi : G \to H$ פונקציה. G, H חבורות. φ נקראת **הומומורפיזם** אם

$$\forall g_1, g_2 \in G \quad \varphi(g_1 *_G g_2) = \varphi(g_1) *_H \varphi(g_2)$$

נקרא — **איזומורפיזם** (בין החבורות).
הומומורפיזם חח"ע נקרא **מונומורפיזם**.
אם קיים איזומורפיזם בין G, H נאמר שהן **איזומורפיות** — ונכתוב $G \cong H$.

דוגמה $\varphi : (\mathbb{Z}_n, +) \longrightarrow \left\{ \omega_n^k \mid n > k \geq 0 \right\}$

$$k \longmapsto \omega_n^k$$

הוא איזומורפיזם מכיוון שמדובר בפונקציה חח"ע ועל בין קבוצות סופיות באותו גודל.

$$\forall k,j \quad \varphi(k+j) = \omega_n^{k+j} = \omega_n^k \cdot \omega_n^j = \omega_n^k * \omega_n^j$$

ולכן ההעתקה φ הומומורפיזם.

דוגמה $(\mathbb{Z}_4, +) \not\cong (\mathbb{Z}_2^2, \oplus)$ אינן איזומורפיות למרות שהן חבורות מסדר 4. נראה זאת על ידי הבחנה בכך שלחבורה הראשונה יש איבר מסדר 4 ולשנייה לא.

הגדרה יהי $g \in G$ איבר בחבורה G, נסמן ב- $o(g)$ את הסדר (order) של g והוא המספר הטבעי הקטן ביותר k המקיים

$$e = \underbrace{g * g * \cdots * g}_{k}$$

אם לא קיים כזה, נגדיר $o(g) = \infty$.

נניח כי $\varphi: G \to H$ הוא איזומורפיזם בין G ל-H. לכל $g \in G$

$$o(g) = o(\varphi(g))$$

כלומר, האיזומורפיזם שומר על סדר האיברים. אכן,

$$\varphi(\underbrace{g * \cdots * g}_{k}) = \underbrace{\varphi(g) * \cdots * \varphi(g)}_{k}$$

מכאן קל לראות כי $(\mathbb{Z}_n^2, \oplus)$ אינה איזומורפית ל- $(\mathbb{Z}_{2n}, +)$: עבור $1 \in \mathbb{Z}_{2n}$ מתקיים $o(1) = 2n$ ולכן אין איזומורפיזם בין החבורות. כל איבר ב- $(\mathbb{Z}_n^2, \oplus)$ הוא מסדר 1 או 2. מכאן שלא ייתכן

כך נוצר $(\mathbb{Z}_n, +)$ היא חבורה מחזורית שכן $\mathbb{Z}_n = \{1^k\}$

כך ש:

$$G = \{g^k \mid k \geq 0\}$$

הגדרה: חבורה G תיקרא מחזורית אם קיים $g \in G$

הזוכה לשם מחולל החבורה ונכתוב:

$$\Rightarrow i-j \geq \langle g \rangle 0.$$

מכיוון שלפי הנחתנו $i \geq j \geq 0$ קיבלנו $n \geq i-j \geq 0$

ומכאן שכל האיברים $g^0, g^1, g^2, g^3, \ldots, g^n$

הם בהכרח שונים זה מזה, כלומר $n+1$ איברים נפרדים ב G בסתירה לכך שהסדר של G הוא n.

לכן הסיומת היא $g^{-k} = (g^{-1})^k$.

$g^0 = e$ לכן

אזי $g^k = e$ אזי $k = 0$

לכן את הסיומת הזו ניתן

$$g^k = \underbrace{g * \cdots * g}_{k}$$

אזי $k = 0$

G נקראת חבורה $g \in G$ נאמר

אין דרך בחבורה **סופית**. במקרה כזה נקרא אותה אז סדר

בהמשך נראה שלכל איבר בחבורה אלו, נקרא לסדר

הסימון g^k משמש הרבה מאוד על הסדר הכללי.
g יוצר של G אז $G=\{g^k\}$

"יוצר"

המחלקה $\mathbb{Z}_n$ קרוי גם כך כי כפי שנראה זהו
משפט 1 או 2. לחוגה $\mathbb{Z}_n$ יש יותר מחוגה אחת "יוצר"
אחת. כך למשל עבור $n=4$ נקבל

$$\mathbb{Z}_4 = \{1\cdot k \mid k\} = \{3\cdot k \mid k\}$$

$1, 1+1, 1+1+1, 1+1+1+1$

$3, \underbrace{3+3}_{=2}, \underbrace{3+3+3}_{=1}, \underbrace{1+3}_{=0}$

אבל לא G אז $\mathbb{Z}_4$ יוצר אחד. כך למשל

$$2+2=4=0 \quad \dots, 2=2+2+2 \Longrightarrow \{2\cdot k\} = \{0,2\}$$

חסרים 1,3

בהינתן חבורה אלגברית G ואיבר $g\in G$ נגדיר את תת החבורה
$\langle g\rangle$ שנוצרת על ידי g

$$\langle g\rangle = \{g^k \mid k\in\mathbb{Z}\} \left(= \{g^k \mid k\in\mathbb{N}\}\right)$$

נרצה כי הקשר בין תת החבורה $\langle g\rangle$ לבין החבורה $\mathbb{Z}_{o(g)}$:
הוא $o(g)$ הוא הקשר האלגברי הטבעי ביותר! שזוג החבורות

$$\varphi : \mathbb{Z}_{o(g)} \longrightarrow \langle g\rangle$$
$$k \longmapsto g^k$$

אזי $\varphi(h)\varphi(m) = g^h g^m = g^{h+m} = \varphi(h+m)$

שאלה: $\mathbb{Z}_4$ חוגים לקי. מהו בחוג הזה "בקוד"
איך מצא "כל תבורה" בקוד.

דוגמאות

1) $\mathbb{Z}_4$:
$\langle 0 \rangle = \{0\}$
$\langle 1 \rangle = \mathbb{Z}_4$
$\langle 2 \rangle = \{0,2\} \cong \mathbb{Z}_2$
$\langle 3 \rangle = \mathbb{Z}_4$

2) $\mathbb{Z}_2^2$:
$\langle 00 \rangle = \{00\}$
$\langle 01 \rangle = \{10, 00\} \cong \mathbb{Z}_2$
$\langle 10 \rangle = \{00, 10\} \cong \mathbb{Z}_2$
$\langle 11 \rangle = \{00, 11\} \cong \mathbb{Z}_2$

3) $\mathbb{Z}_5$:
$\langle 0 \rangle = \{0\}$
$\mathbb{Z}_5 \cong \langle 4 \rangle \cong \langle 1 \rangle \cong \langle 2 \rangle \cong \langle 3 \rangle$

4) $\mathbb{Z}_6$:
$\langle 0 \rangle = \{0\}$
$\langle 1 \rangle = \mathbb{Z}_6 \cong \langle 5 \rangle$
$\langle 2 \rangle = \{0,2,4\} \cong \mathbb{Z}_3 = \langle 4 \rangle$
$\langle 3 \rangle = \{0,3\} \cong \mathbb{Z}_2$

הגדרה: תהי G חבורה וקבוצה $H \subseteq G$, $H \neq \emptyset$ נקרא תת חבורה של G אם היא סגורה לפעולה $*$ הנורשת מ- G. כלומר:
1) $\forall h \in H$ $h^{-1} \in H$
2) $\forall h_1, h_2 \in H$ מתקיים $h_1 * h_2 \in H$

נזכיר כי ראינו קודם אסוציאטיביות שמן התכונה כי "ירושה" מ- G.
ישנו "מבחן" פשוט יותר בכדי לבדוק אם H תת חבורה.

טענה $H \neq \emptyset$ היא תת חבורה של G $G \supseteq H$ $\iff$

$$\forall h_1, h_2 \in H \quad h_1 h_2^{-1} \in H$$

דוגמה G את חבורה $\mathbb{Z}_n$ חבורה בקלות G היא בדיקה.
נניח לכן כי $G = \mathbb{Z}_n$ עבור טבעי n. אזי,
מקבלי את כל החבורות G חבורה נשאר את כל האפשרויות.
כלומר, אם $G_1 \cong G_2$ ע"י איזומורפיזם φ אזי יש
התאמה חח"ע ועל בין כל תת חבורות G_1 ו G_2 המוגדרת
ע"י: אם H_1 תת חבורה G_1 אז $\varphi(H_1)$ תת
חבורה G_2, ולהיפך.

תהא H תת חבורה $\mathbb{Z}_n$. אם $H \neq \{0\}$ נוכל
לבחור a (משום שיש כאלו) כך שהוא
הקטן ביותר. ונראה $H = \langle a \rangle$, שכן אם $b \in H$ אזי

$$b = qa + r \qquad 0 \leq r < a$$

אם $r = b - qa \in H$ בסתירה לכך ש a הוא המספר
הטבעי הקטן ביותר. לכן $r = 0$ ו $b = qa$
ומכאן ש- H היא אכן כל $\langle a \rangle$.

שאלה: עבור כל חבורה $\mathbb{Z}_n$ מצאו ע"י $\langle k \rangle$
עבור $h \in \mathbb{Z}_n$. מה גודל $\langle k \rangle$?

שלכן G מחזורית מסדר n. כלומר $G \cong \mathbb{Z}_n$. בפרט מספר היוצרים של G הוא $\varphi(n)$. מצד שני, $G \cong \underbrace{G \times \cdots \times G}_{k \text{ פעמים}}$ ולכן לפי הטענה הקודמת מספר היוצרים הוא לפחות n^k. לכן $\varphi(n) \geq n^k$, אבל זה לא אפשרי, שכן $\varphi(n) < n$ לכל $n > 1$. קיבלנו סתירה, ולכן G לא יכולה להיות מחזורית.

משפט לגרנז'. תהי G חבורה סופית ו- H תת חבורה שלה. אז $|H| \mid |G|$.

המשפט הקטנטן של חבורות

הרעיון שלו: חבורות H, G ניתן לבנות חבורה חדשה שמכילה את $G \times H$ כאוסף הזוגות: הקל: המכפלה היא בעלת אסוציאטיביות ($H \times G$ כמקרה):

$$\forall \substack{g_1, g_2 \in G \\ h_1, h_2 \in H} \quad (g_1, h_1) * (g_2, h_2) = (g_1 * g_2, h_1 * h_2)$$

לא קשה להוכיח כי אכן חבורה, וכן ניתן לבנות את המכפלה בכמה דרכים שונות. קל לראות, שמתקיים השוויון הבא:

$$(G \times H) \times K \cong G \times (H \times K)$$
$$((g,h),k) \longmapsto (g,(h,k))$$

לכן נוכל לכתוב $G \times H \times K$. ובאופן כללי מכפלה של n חבורות $G \times \cdots \times G$ נסמנה G^n. כל קבוצה של n איברים $(g_1, \ldots, g_n)$ כאשר $g_i \in G$ לכל i מהווה איבר במכפלה.

מסתבר כי תבורה אבלית נוצרת כמכפלה ישירה של חבורות ציקליות:

משפט המיון לחבורות אבליות סופיות

תהא G חבורה אבלית סופית. אז קיימים $n_k \geq \dots \geq n_2 \geq n_1$ כך ש־

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$$

דוגמאות

1) $\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$

2) אבל $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$ אף על פי ששניהם הן חבורות מסדר 4 וכן אבליות. $\mathbb{Z}_2 \times \mathbb{Z}_2$.

הגדרה חשובה

לכל חבורה אבלית "חשובה": עבור $n \geq 1$ נגדיר ע"י הכלל

$$\{ k \mid 1 \leq k < n, \ \gcd(k,n) = 1 \}$$

חבורה כזו שכל איבריה זרים ל־n בכפל מודולו n שסימנו ב־ $\mathbb{Z}_n^*$, ונקראת לפעמים חבורת אוילר. אזי כבר מיד אוקלידס היה יודע ש־

$$\gcd(k,n)=1 \text{ ו־ } \gcd(m,n)=1 \implies \gcd(km,n)=1$$

מאלגוריתם אוקלידס מובטח כי קיימים שלמים x,y כך ש־ $nx+ky=1$.

נשתמש בהעובדה (בקורס – נשים הוכחה אסוף) כי עבור n, m זרים מתקיים

$$\mathbb{Z}_{nm}^* = \mathbb{Z}_n^* \times \mathbb{Z}_m^*$$

שם בפרט לראות את אחד מהמשפטים שנראה בהמשך (ובעצם כמעט את כולם ...).

בפרט קבוצת הפונקציות $\mathbb{Z}_p^*$ היא אבלית (ולכן ציקלית) בגודל $p-1$, ולכן בין $2=p$ בגודל $1-p$, ולכן בין $2=p$.

כלומר

$$\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\} \cong \mathbb{Z}_3^* \times \mathbb{Z}_5^*$$

$$\cong \mathbb{Z}_2 \times \mathbb{Z}_4$$

את כך: $\mathbb{Z}_4 \cong \mathbb{Z}_5^*$ אחד השלושה הבאים

$$\mathbb{Z}_4 \xrightarrow{\varphi} \mathbb{Z}_5^*$$

$$k \longmapsto 2^k$$

$0 \mapsto 1$
$1 \mapsto 2$
$2 \mapsto 4$
$3 \mapsto 3$

$\varphi(j+k) = 2^{j+k} = 2^j \cdot 2^k = \varphi(j)\varphi(k)$

מכאן שלכל $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$,

$$|\mathbb{Z}_n^*| = |\mathbb{Z}_{p_1^{k_1}}^*| \cdot \ldots \cdot |\mathbb{Z}_{p_m^{k_m}}^*|$$

$$= (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_m^{k_m} - p_m^{k_m-1}) = p_1^{k_1}\left(1 - \frac{1}{p_1}\right) \cdots p_m^{k_m}\left(1 - \frac{1}{p_m}\right)$$

$$= n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_m}\right) =: \phi(n)$$

משפט אוילר הוא משפט חשוב שקובע כי
לכל n טבעי אם a זר ל-n אז

$$a^{\phi(n)} \equiv 1 \mod n$$

ההוכחה לקחת בחשבון שמשפט לגרנז' שמן תת-חבורה a של חבורה כלשהי שקל לרבנים $\mod n$ הוא איבר ב- $\mathbb{Z}_n^*$, לכן חבורה זו היא $\phi(n) = |\mathbb{Z}_n^*|$.

משפט פרמה אומר שמשפט הקטן ביותר: יהי המספר p ו- a שאינו מתחלק ב-p.

$$a^{p-1} \equiv 1 \mod p$$

החשיבות הקריטית היא (משפט אוילר הוא $n = 744$) אשר הבסיס לקידוד RSA.