חבורה אבלית

<u>הגדרה</u>: חבורה $(G,*)$ תיקרא חבורה *קומוטטיבית* (או *אבלית*) אם לכל $a,b\in G$ מתקיים $a*b=b*a$.

<u>דוגמה</u>: $(S_n,\circ)$ אינה קומוטיטיבית (כפי שראינו), אך החבורות $(Z_n,+),(Z_n^*,\cdot),(Z,+)$ אכן קומוטיטיביות.

<u>טענה</u> (יחידות הניטרלי): בחבורה $(G,*)$ יש איבר ניטרלי יחיד.

<u>הוכחה</u>: נניח ש-$e,f\in G$ שניהם ניטרליים. אזי $ef=f$ שכן e נייטרלי, וגם $ef=e$ שכן f נייטרלי, ולכן $e=f$.

<u>טענה</u> (יחידות ההופכי): תהי $(G,*)$ חבורה ויהי $a\in G$ אזי $a^{-1}\in G$ יחיד.

<u>הוכחה</u>: נניח בשלילה כי יש ל-a שני הופכיים b,b'. אזי:

$$b'=b'e=b'(ab)=(b'a)b=eb=b$$

כאשר השיוויון השני מימין והשני משמאל נובעים מכך ש b,b' הפכיים ל-a .

<u>סימון</u>: תהי $(G,*)$ חבורה עם נייטרלי $e\in G$ ויהי $a\in G$. אזי נסמן

$$a^0=e,\quad a^1=a,\quad \forall n\geq 1: a^{n+1}=a*a^n$$

<u>דוגמה</u>: בחבורה $(Z_3^*,\cdot)$ (נקצר ונסמן למשל 2 במקום $[2]_3$) מתקיים

$$2^4=2\cdot 2\cdot 2\cdot 2\equiv 1\cdot 1\equiv 1\ (mod\ 3)$$

<u>דוגמה נוספת</u>: בחבורה $(Z_3,+)$ מתקיים

$$2^4=2+2+2+2=8\equiv 2\ (mod\ 3)$$

ולכן $[2]^4=[2]$.

בחבורה חיבורית, במקום חזקה כגון $[2]^4$ לפעמים נסמן $4\cdot[2]$.

<u>דוגמה שלישית</u>: בחבורה $(Z,+)$ מתקיים

$$2^4=2+2+2+2=8$$

<u>טענה</u>: תהי $(G,*)$ חבורה אבלית סופית $G=\{g_1,g_2,\dots g_r\}$ ויהי $a=g_1*g_2*\dots g_r$ אזי $a^2=e$.

<u>הוכחה</u>: לכל $1\leq i\leq r$ יש $1\leq k\leq r$ כך ש-g_k הופכי ל-g_i, ומקומוטטיביות הטענה נובעת.

<u>תזכורת</u> (משפט וילסון): יהי p ראשוני. אזי $(p-1)!\equiv -1\ (mod\ p)$.

<u>הוכחה</u> (כאשר חלק מן ההוכחה כתוב בשפה של חבורות): נתבונן בחבורה הכפלית Z_p^*. נסמן את איבריה כמספרים במקום כמחלקות שקילות. אזי מתקיים

$$\prod_{g\in Z_p^*} g \quad = \quad \prod_{g\in Z_p^*,\ g^2=e} g$$

מכפלת כל האיברים **מכפלת האיברים שהופכיים לעצמם**

אבל למדנו שהיחידים שהופכיים לעצמם במודולו p הם $1,-1\ (mod\ p)$ כלומר $1,p-1$.
ולכן

$$\prod_{g\in Z_p^*,\ g^2=e} g = 1\cdot(p-1) = p-1$$

האם בהוכחה זו יש יתרון על פני ההוכחה הקודמת? זה אותו דבר במילים אחרות, אבל ההתחלה מופשטת יותר עשויה להתאים גם לחבורות אחרות, ובלבד שיש לנו מידע על האיברים ההופכיים לעצמם.

<u>עוד דוגמאות לחבורות</u>:

1) חבורה מסדר 2: $(\{-1,1\},\cdot)$ (בדקו! 1 הוא הניטרלי, וכל איבר הופכי לעצמו)

2) חבורות מסדר 4:

א. $(Z_4,+)$. האם גם $(Z_4^*,\cdot)$ היא חבורה מסדר 4? לא, כי היא חבורה מסדר 2, וזהה לחבורה מדוגמה 1.

ב. $G=Z_2XZ_2=\{(a,b)|a,b\in Z_2\}$, עם הפעולה

$$(a,b)*(c,d)=(a+c\ (mod\ 2),b+d\ (mod\ 2))$$

כלומר, $G=\{(0,0),(0,1),(1,0),(1,1)\}$

דוגמה: $(1,0)+(1,1)=(1+1,0+1)=(0,1)$.

<u>הסבר</u>: סגירות ואסוציאטיביות נובעים מכך ש-Z_2 חבורה חיבורית. ניטרלי $(0,0)$. הופכי של (a,b) הוא (a,b).

כיצד נוודא שהחבורות בשתי הדוגמאות הללו (א-ב) אינן בעצם אותה חבורה בשינוי שמות האיברים?

נשים לב כי בחבורה ב' כל איבר הפכי לעצמו ואילו בחבורה א' לא. לכן אלו שתי חבורות שונות מסדר 4.

<u>הכללה</u>: אם $G_1,G_2,\dots,G_n$ חבורות, אזי $G=G_1X\dots XG_n$ חבורה עם הפעולה * המוגדרת כך:

$$(g_1,\dots,g_n)*(g_1',\dots g_n')=(g_1g_1',\dots,g_ng_n')$$

שימו לב כי הפעולה בכל קואורדינטה (שלא סומנה כאן בשום סימון) היא הפעולה של החבורה המתאימה.

אז $e_G = (e_{G_1}, \dots, e_{G_n})$ ו-$(g_1, \dots, g_n)^{-1} = (g_1^{-1}, \dots, g_n^{-1})$ (וידוא הפרטים נשאר כתרגיל בית).

תכונות נוספות בחבורות

משפט "חוקי חזקות" בחבורה:

תהי $(G,*)$ חבורה, $a \in G$, $0 \le m,n \in Z$. אזי:

1. $a^m a^n = a^{m+n} = a^n a^m$ (משמיטים את הסימן $*$ כמו בכפל רגיל)
2. $(a^m)^n = a^{mn} = (a^n)^m$
3. אם $ab = ba$ אזי $(ab)^n = a^n b^n$

הוכחה של 1:

(שימו לב לטכניקה שבה מוכיחים טענה עבור 2 פרמטרים באינדוקציה על אחד מהם, כמו שעשינו בתרגול של GCD)

נקבע $m \ge 0$ ונוכיח כי לכל $n \ge 0$ מתקיים $a^m a^n = a^{m+n} = a^n a^m$, באינדוקציה על n.

בסיס האינדוקציה: עבור $n = 0$ נקבל

$$a^m a^0 = a^m e = a^m = e a^m = a^0 a^m$$

נניח נכונות, כלומר שעבור n כלשהו מתקיים

$$a^m a^n = a^{m+n} = a^n a^m$$

ונבדוק עבור $n+1$:

$$a^m a^{n+1} = a^m (a^n a) = (a^m a^n) a = a^{m+n} a = a^{m+n+1}$$

הגדרת חזקה/הנחת אינדוקציה/אסוציאטיביות/הגדרת חזקה

באגף השני מתקיים

$$a^{n+1} a^m = (a a^n) a^m = a (a^n a^m) = a a^{n+m} = a^{n+m+1}$$

הגדרת חזקה/הנחת אינדוקציה/אסוציאטיביות/הגדרת חזקה

ולכן לפי עקרון האינדוקציה, הטענה מתקיימת לכל n טבעי.

משפט "תכונות ההופכי" בחבורה:

תהי $(G,*)$ חבורה עם הניטרלי e, ויהיו $a, b, a_1, a_2, \dots, a_n \in G$. אזי:

1) $e^{-1} = e$. 2) $(a^{-1})^{-1} = a$. 3) $(ab)^{-1} = b^{-1} a^{-1}$ (הסדר משפיע!)

4) $(a_1 * a_2 * \dots * a_n)^{-1} = a_n^{-1} * \dots * a_1^{-1}$. 5) $(a^n)^{-1} = (a^{-1})^n$.

הוכחה:

1) $e * e = e$ ולכן $e^{-1} = e$.

2) נשים לב כי $(a^{-1})^{-1}$ הינו ההופכי (היחיד!) של (a^{-1}), כלומר, האיבר שאם נכפול אותו ב(a^{-1}) נקבל את e. אבל מתקיים גם $aa^{-1}=e$ ולכן מיחידות ההפכי $a=(a^{-1})^{-1}$.

3) עלינו להראות כי ההופכי של ab הינו $b^{-1}a^{-1}$. נראה שאכן בהכפלה שלהם, משני הצדדים, נקבל את e.

$$(ab)\left(b^{(-1)}a^{-1}\right)=\left(a(bb^{-1})a^{-1}\right)=aea^{-1}=aa^{-1}=e$$

$$\left(b^{(-1)}a^{-1}\right)(ab)=\left(b^{-1}(a^{-1}a)b\right)=b^{-1}eb=b^{-1}b=e$$

כאשר השיוויון הראשון נובע מכמה הפעלות של האסוציאטיביות, השני מהגדרת הופכי, והשלישי מהגדרת ניטרלי.

4) נובע מתכונה 3) באינדוקציה על n. נשאר כתרגיל בית.

5) מקרה פרטי של 4) כאשר $a_1=a_2=\cdots a_n=a$.

<u>חוק הצמצום בחבורה</u>: תהי $(G,*)$ חבורה ויהיו $g,h,f\in G$. אזי:

1. (צמצום שמאלי) אם $gh=gf$ אזי $h=f$.

2. (צמצום ימני) אם $hg=fg$ אזי $h=f$.

<u>הוכחה</u>:

1. לפי הגדרת חבורה קיים g^{-1}. נכפול בו משמאל ונקבל

$$g^{-1}(gh)=g^{-1}(gf)\rightarrow(g^{-1}g)h=(g^{-1}gf)\rightarrow eh=ef\rightarrow h=f$$

הוכחת 2 זהה, רק שנכפיל מימין. השלימו בבית.

<u>טענה</u>: אם G חבורה סופית ו-$g\in G$ אזי קיים n טבעי כך ש-$g^n=e$.

<u>דיון</u>: האם זה נכון לחבורה אינסופית? לא. למשל $(Z,+)$, אם ניקח $g=2$ אז $2+2+\cdots+2$ לעולם לא ייתן 0.

<u>הוכחה</u>: נתבונן באוסף .... g^1,g^2,g^3 מסופיות G נובע כי קיימים $m,n\in N$ כך שמתקיים

$$g^m=g^{n+m}\rightarrow g^m\cdot e=g^m\cdot g^n\rightarrow e=g^n$$

כאשרה המעבר האחרון נובע מכלל הצמצום.

העובדה שבחבורה לכל איבר יש הופכי מקילה עלינו בפתרון משוואות ליניאריות. בניגוד למה שלמדנו על שקילות ליניארית באופן כללי, שאז רק לפעמים ש פתרון למשוואה

$ax\equiv b\ (mod\ m)$ (רק כאשר $(a,m)|b$), בחבורות זה לא קורה, ויש פתרון לכל שקילות ליניארית.

(היעדר הפתרון (לעיתים) בשקילויות נבע מכך שעבדנו עם $(Z_n,\cdot)$. בחבורות אנו עובדים עם $(Z_n^*,\cdot)$ ואז יש פתרון לכל שקילות לינארית.)

טענה- פתרון שקילות ליניארית בחבורות:
תהי G חבורה, ויהיו $g,h\in G$. אזי:

1. למשוואה $gx=h$ יש פתרון יחיד ב-G, $x=g^{-1}h$.

2. למשוואה $xg=h$ יש פתרון יחיד ב-G, $x=hg^{-1}$.

הוכחת 1. x פתרון, שכן

$$gx=g(g^{-1}h)=(gg^{-1})h=eh=h.$$

נראה שזהו פתרון יחיד- יהי $y\in G$ פתרון למשוואה $gx=h$. אזי $gx=gy \leftarrow x=y$ (חוק הצמצום).

תת חבורה

אינטואיציה: תת חבורה היא תת קבוצה של חבורה, שהיא בעצמה חבורה.

לדוגמה: $G=(Z_6,+)=\{[0],[1],[2],[3],[4],[5]\}$

אזי $S=\{[0],[2],[4]\}$ הינה תת-חבורה של G, אבל $S'=\{[0],[1],[2],[4]\}$ אינה תת-חבורה, שכן ל-$[1]$ אין איבר הפכי (כלומר נגדי כי זו חבורה חיבורית).

כדי שתת-החבורה תהיה אכן חבורה, נצטרך סגירות לפעולה ולהופכי.

הגדרה: תהי $(G,*)$ חבורה. תהי $S\subseteq G$ תת קבוצה לא ריקה של G המקיימת:

1) סגירות לפעולה - לכל $s,t\in S$ גם $s*t\in S$

2) סגירות להופכי- לכל $s\in S$ גם $s^{-1}\in S$

אז S נקראת תת-חבורה של G, ומסמנים $S\leq G$.

טענה: אם S תת חבורה של $(G,*)$ אז S עצמה חבורה עם הפעולה $*$.

הוכחה: נראה את קיום האקסיומות:

1) סגירות- מההגדרה. 2) אסוציאטיביות- תורשתית מ-G.

3) קיום נייטרלי- $S\neq\phi$ ולכן יש $s\in S$. מסגירות להופכי, גם $s^{-1}\in S$ ומסגירות לפעולה נובע כי $e=ss^{-1}\in S$. 4) קיום הופכי- מההגדרה.

תת חבורות שתמיד קיימות: לכל חבורה G, $\{e\}\leq G$ וגם $G\leq G$. (תת חבורות טריוויאליות)

תת חבורה ששונה מ-G נקראת "תת חבורה proper".

<u>דוגמאות לתת-חבורות:</u>

1) $(Z,+) \leq (R,+)$ 2) $(Z,+)$ אינה תת-חבורה של $(R,\cdot)$, כי זו לא אותה פעולה.

3) עבור $n \in N$ נגדיר $nZ = \{nk \mid k \in Z\}$, לדוגמה: $3Z = \{\dots -3,0,3,6,9,\dots\}$.

אזי $(nZ,+) \leq (Z,+)$. למה?

1. אם $a,b \in nZ$ אזי $a = nk, b = nl$ ולכן $a + b = n(k+l) \in nZ$.

2. אם $a = nk \in nZ$ אזי $-a = n(-k) \in nZ$. (שימו לב שבחבורה חיבורית סגירות להפכי היא בעצם סגירות לנגדי.)

4) יהי $0 \neq a \in Q$. אזי $(\{a^n | n \in Z\},\cdot) \leq (Q,\cdot)$. (בידקו את הפרטים!)

<u>מבחני תת-חבורה:</u>

1) מבחן ראשון: תהי $(G,*)$ חבורה. $S \subseteq G$ תת-חבורה אם"ם מתקיים

א. $e \in S$

ב. לכל $s,t \in S$ גם $st^{-1} \in S$.

<u>הוכחה</u>: $(\leftarrow)$ ברור.

$(\rightarrow)$ נראה כי S מקיימת את תנאי החבורה.

2. סגירות להופכי- יהי $s \in S$. משום שגם $e \in S$ נובע שגם $es^{-1} \in S$ ולכן $s^{-1} \in S$.

1. סגירות לפעולה- יהיו $s,t \in S$. אזי $t^{-1} \in S$ לפי השורה הקודמת, ולכן $st = s(t^{-1})^{-1} \in S$.

2) מבחן שני: מבחן לתת חבורה <u>סופית</u>:

<u>משפט</u>: תהי H תת קבוצה סופית לא ריקה של חבורה G. אזי:

$H \leq G \leftrightarrow H$ סגורה תחת הפעולה של G (כלומר, כאן מספיק תנאי הסגירות לפעולה, ולא דרוש גם סגירות להופכי.)

<u>הוכחה</u>: $(\leftarrow)$ ברור.

$(\rightarrow)$ עלינו להראות כי לכל $h \in H$ מתקיים כי $h^{-1} \in H$.

יהי $h \in H$. מהסגירות נובע כי $h, h^2, h^3, \dots \in H$. אבל H סופית, ולכן יש $m,n \in N$ כך ש-

$h^n = h^{n+m}$ ולכן $e = h^m$ (בגלל חוק הצמצום מחבורה G!) ולכן h^{m-1} הוא ההופכי של h (ב-G) ומתקיים $h^{-1} = h^{m-1} \in H$.

<u>חיתוך של תתי חבורות</u>:

אינטואיציה: חיתוך של תתי חבורות יישאר חבורה, בעוד שאיחוד תתי חבורות לא.

למשל $3Z \cap 5Z = 15Z$ (כפולות 3 וגם כפולות $5 =$ כפולות 15) חבורה, אבל $(3Z) \cup (5Z)$ אינה תת חבורה, שכן $3,5 \in (3Z) \cup (5Z)$ אבל $3 + 5 = 8 \notin (3Z) \cup (5Z)$.

<u>משפט</u>: תהי $\{S_i\}_{i\in I}$ משפחה של תת חבורות של G (אולי משפחה אינסופית) אז

$$\bigcap_{i\in I} S_i \leq G$$

<u>הוכחה</u>: נראה לפי המבחן הראשון.

א. לכל $i \in I$ הניטרלי $e \in S_i$, ולכן $e \in \bigcap_{i\in I} S_i$.

ב. יהיו $a, b \in \bigcap_{i\in I} S_i$ אזי לכל $i \in I$ מתקיים $ab^{-1} \in S_i$ ולכן $ab^{-1} \in \bigcap_{i\in I} S_i$.

ולכן לפי המבחן הראשון $\bigcap_{i\in I} S_i \leq G$.