הגדרה: תהי $(G,\cdot)$ — G קבוצה, $\cdot$ פעולה $G\times G\to G$

1) מוגדרות $\forall g_1,g_2\in G:\ g_1\cdot g_2\in G$

2) קיבוציות $(g_1\cdot g_2)g_3=g_1(g_2g_3)$

3) קיים ניטרלי $\exists e\in G:\forall g\in G\ \ ge=eg=g$

4) קיים הופכי $\forall g\exists h:\ gh=hg=e\ \ (h=g^{-1})$

(1–2: אגודה; 1–3: מונואיד; 1–4: חבורה)

דוגמאות:

1) $(\mathbb{Z},+)$ חבורה

2) $(\mathbb{N},+)$ אגודה

3) $(\mathbb{Z},\cdot)$ מונואיד

4) $\left(\{0,1\}^*=\bigcup_{n\in\mathbb{N}_0}\{0,1\}^n,\ \underbrace{/\!/}_{\text{שרשור מילים}}\right)$ מונואיד ניטרלי המילה הריקה ε

5) X קבוצה. נגדיר $a\cdot b=b$ $\forall a,b\in X$ אגודה

6) $(\mathbb{Z},-)$ פעולה מוגדרת בלבד. לא אגודה

7) $(2\mathbb{Z},+)$ חבורה

8) $(2\mathbb{N},\cdot)$ אגודה

9) $(P(X),\cap)$ מונואיד. $(e=\emptyset)$

10) $(P(X),\cup)$ מונואיד $(e=X)$

הערה: במונואיד זה מתקיים $A\cup A=A$ $\forall A\in P(X)$

הערה: יהי $(M\cdot e)$ מונואיד. $a\in M$
ואם קיימים $b_1,b_2\in M$ כך ש e , $b_2a=e$, $ab_1=e$
אז a הפיך ו- $b_1=b_2=a^{-1}$

הערה: כפל הפיכים הוא הפיך ואם a,b הפיכים $(ab)^{-1}=b^{-1}a^{-1}$

תרגיל:

יהי $(M\cdot e)$ מונואיד, $a,b\in M$ כך ש aba הפיך
הוכיחו כי a,b הפיכים (ab הפיך $\not\Rightarrow$ a,b הפיכים)

פתרון:

נתון שקיים c כך ש e $\quad a\underbrace{bac}_{b_2}=e \quad \underbrace{cab}_{b_1}a=e$

לכן $b_1=b_2$. a הפיך $a^{-1}abaa^{-1}=b$ גם הפיך
כפל של הפיכים

אבחנה:

תהי X קבוצה $(X^X\ \circ)$ מונואיד (id_X=ניטרלי)
תהי $f\in X^X$
1) מתי יש ל- f הפיך ימני? (כלומר $f\circ g=id$)
2) מתי יש הפיך שמאלי

פתרון:

(1) $\Longleftrightarrow$ f על
(2) $\Longleftrightarrow$ f חח"ע

מסקנה:

נתקן הפיכות מצד אחד בלבד

תרגיל:

$(M,\cdot e)$ מונואיד סופי. אם $a\in M$ הפיך מצד אחד אז a הפיך

פתרון:

יהי a הפיך מצד אחד. M סופי, קיימים $m<n$

כך ש $a^m=a^n$

נכפיל בהופכי החד-צדדי m פעמים ונקבל

$a^{n-m}=e \Rightarrow$ ההופכי של a a^{n-m-1}

תרגיל:

יהי $(X\cdot e)$ מונואיד. הקבוצה $P_*(X)=P(X)\setminus\phi$ היא מונואיד:

1) ביחס לכפל $A\cdot B=\{ab \mid a\in A, b\in B\}$

2) מצא מי הם האיברים ההפיכים ב-$(P_x(X)\cdot)$

פתרון:

1) סגירות: $A\cdot B\subseteq X$ ובנוסף ובנוסף $ab\in A\cdot B\neq\phi$ $\exists a\in A, b\in B$

אסוציאטיביות: נובע מאסוציאטיביות של $(X\cdot)$

נטרלי: $\{e\}$ $A\cdot\{e\}=A=\{e\}\cdot A$

2) מי הפיכים? נניח A הפיך, B ההופכי

$AB=\{ab \mid a\in A, b\in B\}=e$

$BA=\{ba \mid a\in A, b\in B\}=e$

טענה: כל $a\in A$ הפיך ב-X

a הפיך $\Leftarrow$ $ab_1=b_2a=e$ $\exists b_1,b_2\in B$

טענה: $|A|=1$

נניח $a_1,a_2\in A$ ו- $a_1\neq a_2$ והפיכים

קיים $b\in B$ כך e $a_1b=ba_1=e$ ולכל $a_2b\neq e$

כי יחידות b ההופכי של a_2 ⇐ $a_1=a_2$

בכיוון השני: לכל $a\in X$ הפיך מקיים כי $\{a\}$ הפיך ב- $(P_*(X)\cdot)$

ההופכי הוא $\{a^{-1}\}$

דוגמאות נוספות לחבורות:

1) $X=\{a,b\}$

	a	b
a	a	b
b	b	a

חבורה בשני איברים

$\mathbb{Z}_2=\{[0],[1]\}$ עם חיבור מודולו 2

2) ($\mathbb{Z}_n$ חיבור מודולו n) ניטרלי $[0]$. הנגדי $-[a]=[-a]$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\ \ \| \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad [n-a]$

3) $(n\mathbb{Z}\ +)$

4) ($\mathbb{Z}_n$ כפל מודולו n) לא חבורה. ל $[0]$ אין הופכי

$(\mathbb{Z}_n\setminus[0]\ \cdot)$ לא חבורה. למשל $[2]\cdot[3]=[0] \pmod 6$

⇐ $[2],[3]$ מחלקי אפס ולכן לא הפיכים

הערה: p ראשוני ⇔ $(\mathbb{Z}_p\setminus[0]\ \cdot)$ חבורה

הוכחה:

⇒ נב"ש p לא ראשוני ⇐ $\exists\, 1<a,b<p: p=ab$ ⇐ $[a][b]=[0]$

$\Downarrow$

$[0]$ אינו הפיך

⇐ סגירות/קיבוציות/נטרלי ($[1]$) ברור

הוכחה: יהא $[a]\neq[0]$
$\Downarrow$
a,p זרים ולכן $gcd(a,p)=1$
ולכן קיימים t,s כך ש $as+pt=1$
$\Leftarrow$ $[1]=[as+pt]=[a][s]+[p][t]=[a][s]$
$[p]=0$
$\Leftarrow$ $[a]^{-1}=[s]$ (החבורה חילופית (וקבוצתית))

מסקנה:
עבור p ראשוני $\mathbb{Z}_p$ שדה
שדה פירושו: $(F\ +)$ חבורה חילופית
$(F\ \cdot)$ חבורה חילופית
$0\cdot a=0$
+ פילוג ...

הגדרה: $(M\ \cdot)$ מונואיד. נגדיר $U(M)=\{a\in M \mid \text{הפיך } a\}$
אזי $(U(M)\ \cdot)$ חבורה. ונקראת חבורת ההפיכים של M

למשל:
1) $(\mathbb{Z}\ \cdot)$ מונואיד. חבורת ההפיכים $\{\pm1\}$
2) $(\mathbb{R}\ \cdot)$ מונואיד. $U(\mathbb{R})=\mathbb{R}^\times=\mathbb{R}\setminus\{0\}$
3) $(\mathbb{F}\ \cdot)$ מונואיד
$(\mathbb{F}^\times\cdot)$ כאשר $F^\times=\mathbb{F}\setminus\{0\}$. חבורת ההפיכים $(\mathbb{Z}_p^\times\ \cdot)$ חבורה
4) $(\mathbb{F}^{n\times n}\cdot)$ מונואיד $GL_n(\mathbb{F})=U(\mathbb{F}^{n\times n})=\{A\in\mathbb{F}^{n\times n} \mid \det A\neq0\}$
חבורת ההפיכים

הגדרה:
נסמן $M_N^0(\mathbb{F})$ אוסף המטריצות האינסופיות מעל שדה $\mathbb{F}$ שבכל
שורה ובכל עמודה יש מספר סופי של איברים שונים מ־0

הוכיחו שפעולת הכפל הופכת את $M^{o}_{\aleph_0}(\mathbb{F})$ למונואיד אבל לא חבורה.

הוכחה:

$i,j\in\mathbb{N}$ $\quad (AB)_{ij}=\sum_{k\in\mathbb{N}} A_{ik}B_{kj}$

סגירות:

$$(AB)_{11}=\sum_{k} A_{1k}B_{k1}$$
$$(AB)_{12}=\sum_{k} A_{1k}B_{k2}$$
$$(AB)_{13}=\sum_{k} A_{1k}B_{k3}$$
$$\vdots$$

יהי c כך ש $A_{1k}=0$ $\forall k>c$

נבחר N כך ש $B_{kj}=0$ $\forall k>N$

$$(AB)_{1N}=\sum_{k=1}^{c_1} A_{1k}B_{kN}=0$$
$$\vdots$$
$$=0$$

לא חבורה כי (0) לא הפיך

תרגיל המשך:

מצאו איבר הפיך מצד אחד בלבד

$$\begin{pmatrix} 1 & 1 & & & \\ & 1 & 1 & & \\ & & 1 & 1 & \\ & & & & \ddots \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & \ddots & & \\ & 1 & \ddots & \\ 0 & & 1 & \ddots \\ & & & 1 \end{pmatrix}=\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & \ddots & & \\ & 1 & \ddots & \\ 0 & & 1 & \ddots \\ & & & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & & & \\ & 1 & 1 & & \\ & & 1 & 1 & \\ & & & & \ddots \end{pmatrix}=\begin{pmatrix} 0 & 0 & 0 & 0 & \cdots \end{pmatrix}$$