

פעולות בינאריות: תהא A קבוצה אזי $A \times A \rightarrow A$.

סימון: תהא A קבוצה ותהא $*$ פעולה בינארית על A אזי $a * b = *(a, b)$.

חבורה: תהא G קבוצה אזי $G \times G \rightarrow G : *$ עבורה קיים $e \in G$ עבורו

- אסוציאטיביות: לכל $a, b, c \in G$ מתקיים $a * (b * c) = (a * b) * c$.
- איבר יחידה: לכל $a \in G$ מתקיים $a * e = e * a = a$.
- איבר הופכי: לכל $a \in G$ קיים $b \in G$ עבורו $a * b = e = b * a$.

הגדרה: תהא X קבוצה אזי $f : X \rightarrow X$ הפיכה $S(X) = \{f : X \rightarrow X \mid f \text{ הפיכה}\}$.

חבורת התמורות: תהא X קבוצה אזי $(S(X), \circ)$.

טענה: תהא X קבוצה אזי חבורת התמורות הינה חבורה.

סימון: יהי $n \in \mathbb{N}$ אזי $S_n = S([n])$.

טענה: יהי $n \in \mathbb{N}$ אזי $|S_n| = n!$.

חבורת המטריצות: יהי \mathbb{F} שדה ויהי $n \in \mathbb{N}$ אזי $(GL_n(\mathbb{F}), \cdot)$.

טענה: יהי \mathbb{F} שדה ויהי $n \in \mathbb{N}$ אזי חבורת המטריצות הינה חבורה.

החבורות החיבוריות: יהי $\mathbb{F} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ אזי $(\mathbb{F}, +)$.

סימון: תהא $A \subseteq \mathbb{C}$ אזי $A^* = A \setminus \{0\}$.

החבורות הכפליות: יהי $\mathbb{F} \in \{\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*\}$ אזי (\mathbb{F}, \cdot) .

החבורה הטריטוראלית: יהי x אזי $(\{x\}, \text{Id})$.

הגדרה: יהי $n \in \mathbb{N}$ אזי $\sim_n \subseteq \mathbb{Z}^2$ המוגדרת $(x \sim_n y) \iff (n \mid (x - y))$.

סימון: יהי $n \in \mathbb{N}$ אזי $C_n = \mathbb{Z} / \sim_n$.

הגדרה: יהי $n \in \mathbb{N}$ אזי $C_n \times C_n \rightarrow C_n : +$ המוגדרת $[x]_{\sim_n} + [y]_{\sim_n} = [x + y]_{\sim_n}$.

חבורת שאריות החלוקה: יהי $n \in \mathbb{N}$ אזי $(C_n, +)$.

טענה: יהי $n \in \mathbb{N}$ אזי חבורת שאריות החלוקה הינה חבורה.

טענה: יהי $n \in \mathbb{N}$ אזי $|C_n| = n$.

חבורה אבלית/חילופית/קומוטטיבית: חבורה $(G, *)$ עבורה לכל $g, h \in G$ מתקיים $g * h = h * g$.

טענה: יהי $n \in \mathbb{N}_{\geq 3}$ אזי (S_n, \circ) אינה אבלית.

טענה: יהי $n \in \mathbb{N}_+$ אזי $(GL_n(\mathbb{F}), \cdot)$ אינה אבלית.

טענה: יהי $n \in \mathbb{N}_+$ אזי $(C_n, +)$ אבלית.

חבורה סופית: חבורה $(G, *)$ עבורה $|G| \in \mathbb{N}$.

חבורה אינסופית: חבורה $(G, *)$ עבורה $|G| \geq \aleph_0$.

סדר של חבורה: תהא $(G, *)$ חבורה סופית אזי $\text{ord}(G) = |G|$.

סדר של חבורה: תהא G חבורה אינסופית אזי $\text{ord}(G) = \infty$.

סימון: תהא $(G, *)$ חבורה אזי $\text{ord}(G) = o(G)$.

תת־חבורה: תהא $(G, *)$ חבורה ותהא $H \subseteq G$ אזי $(H, *|_{H \times H})$ עבורה

- סגירות לכפל: לכל $a, b \in H$ מתקיים $a * b \in H$.
- סגירות להופכי: לכל $a \in H$ מתקיים $a^{-1} \in H$.
- איבר יחידה: יהי e איבר היחידה של G אזי $e \in H$.

סימון: תהא $(G, *)$ חבורה ותהא $H \subseteq G$ עבורה $(H, *|_{H \times H})$ תת־חבורה אזי $H \leq G$.

למה: תהא $(G, *)$ חבורה ותהא $H \in \mathcal{P}(G) \setminus \{\emptyset\}$ אזי $H \leq G \iff (a * b^{-1} \in H \mid a, b \in H)$ (לכל $a, b \in H$ מתקיים $a * b^{-1} \in H$).

סימון: תהא $(G, *)$ חבורה ותהינה $A, B \subseteq G$ אזי $A * B = \{a * b \mid (a \in A) \wedge (b \in B)\}$.

סימון: תהא $(G, *)$ חבורה תהא $H \subseteq G$ ויהי $g \in G$ אזי $g * H = \{g * h \mid h \in H\}$.

טענה: יהי $n \in \mathbb{N}$ אזי $(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$.

טענה: יהי $n \in \mathbb{N}$ ויהי \mathbb{F} שדה אזי $(SL_n(\mathbb{F}), \cdot) \leq (GL_n(\mathbb{F}), \cdot)$.

סימון: יהי $n \in \mathbb{N}$ אזי $R_n = \{z \in \mathbb{C} \mid z^n = 1\}$.

טענה: יהי $n \in \mathbb{N}$ אזי $(R_n, \cdot) \leq (\mathbb{C}^*, \cdot)$.

טענה: תהא $(G, *)$ חבורה אזי $G \leq G$.

טענה: תהא $(G, *)$ חבורה אזי $\{e\} \leq G$.

הערה: מכאן והלאה כאשר ברור מהי הפעולה של החבורה נסמנה על ידי הקבוצה בלבד.

טענה: תהא $(G, *)$ חבורה אזי קיים יחיד $e \in G$ עבורו $a * e = e * a = a$ לכל $a \in G$.

טענה: תהא $(G, *)$ חבורה ויהי $a \in G$ אזי קיים יחיד $b \in G$ עבורו $a * b = e = b * a$.

סימון: תהא $(G, *)$ חבורה יהי $a \in G$ ויהי $b \in G$ איבר הופכי ל- a אזי $a^{-1} = b$.

טענה: תהא $(G, *)$ חבורה ויהיו $a, b \in G$ אזי $(a * b)^{-1} = b^{-1} * a^{-1}$.

טענה: תהא $(G, *)$ חבורה ויהי $a \in G$ אזי $(a^{-1})^{-1} = a$.

מסקנה כלל צמצום משמאל: תהא $(G, *)$ חבורה ויהי $a, b, c \in G$ עבורם $a * b = a * c$ אזי $b = c$.

מסקנה כלל צמצום מימין: תהא $(G, *)$ חבורה ויהי $a, b, c \in G$ עבורם $b * a = c * a$ אזי $b = c$.

סימון: תהא $(G, *)$ חבורה ויהי $g \in G$ אזי $g^0 = e$.

הגדרה: תהא $(G, *)$ חבורה יהי $n \in \mathbb{N}_+$ ויהי $g \in G$ אזי $g^n = g * g^{n-1}$.

סימון: תהא G חבורה יהי $n \in \mathbb{N}$ ויהי $g \in G$ אזי $g^{-n} = (g^n)^{-1}$.

טענה: תהא G חבורה יהי $n \in \mathbb{N}$ ויהי $g \in G$ אזי $g^{-n} = (g^{-1})^n$.

חבורת המכפלה: תהיינה $(H, \otimes), (G, *)$, חבורות נגדיר $(g, h) \cdot (g', h') = (g * g', h \otimes h')$ לכל $g, g' \in G$ ולכל $h, h' \in H$ אזי $(G \times H, \cdot)$.

טענה: תהיינה $(H, \otimes), (G, *)$, חבורות אזי חבורת המכפלה הינה חבורה.

טענה: תהיינה $(H, \otimes), (G, *)$, חבורות אזי $(H, \otimes) \leq (G \times H, \cdot) \iff (H, \otimes) \leq (H, \otimes)$.

טענה: תהא $(G, *)$ חבורה ותהיינה $H, K \leq G$ אזי $(HK = KH) \iff (H * K \leq G)$.

טענה: תהא $(G, *)$ חבורה ותהיינה $H, K \leq G$ אזי $(H \cap K \in \{H, K\}) \iff (H \cup K \leq G)$.

הגדרה: תהא X קבוצה ותהא $Y \subseteq X$ אזי $\text{Stab}(Y) = \{\pi \in S(X) \mid \forall y \in Y. \pi(y) = y\}$.

טענה: תהא X קבוצה ותהא $Y \subseteq X$ אזי $\text{Stab}(Y) \leq S(X)$.

מסקנה: תהא G חבורה ותהא $\{H_i\}_{i \in I} \subseteq \mathcal{P}(G)$ באשר $H_i \leq G$ לכל $i \in I$ אזי $\bigcap_{i \in I} H_i \leq G$.

הגדרה: תהא G חבורה ותהא $X \subseteq G$ אזי $\mathcal{F}(X) = \{H \leq G \mid X \subseteq H\}$.

החבורה שנוצרת על ידי תת-קבוצה: תהא G חבורה ותהא $X \subseteq G$ אזי $\langle X \rangle = \bigcap_{H \in \mathcal{F}(X)} H$.

למה: תהא G חבורה ותהא $X \subseteq G$ אזי $\langle X \rangle \leq G$.

טענה מינימליות החבורה הנוצרת: תהא G חבורה תהא $X \subseteq G$ ותהא $H \leq G$ עבורה $X \subseteq H$ אזי $\langle X \rangle \subseteq H$.

קבוצת יוצרים של חבורה: תהא G חבורה אזי $X \subseteq G$ עבורה $\langle X \rangle = G$.

חבורה נוצרת סופית (נ"ס): חבורה G עבורה קיימת קבוצת יוצרים סופית.

חבורה ציקלית: חבורה G עבורה קיים $g \in G$ המקיים $\langle g \rangle = G$.

למה: תהא G חבורה ויהי $g \in G$ אזי $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$.

טענה: תהא G חבורה יהיו $n, m \in \mathbb{Z}$ ויהי $g \in G$ אזי $g^{n+m} = g^n * g^m$.

טענה: תהא G חבורה יהיו $n, m \in \mathbb{Z}$ ויהי $g \in G$ אזי $(g^n)^m = g^{n \cdot m}$.

למה: תהא G חבורה אזי $(G \text{ ציקלית}) \iff (G \text{ קיים } g \in G \text{ עבורו } G = \{g^k \mid k \in \mathbb{Z}\})$.

מסקנה: תהא G חבורה ציקלית אזי G אבלית.

סדר של איבר: תהא G חבורה ויהי $g \in G$ אזי $\text{ord}(g) = \text{ord}(\langle g \rangle)$.

טענה: תהא G חבורה ויהי $g \in G$ אזי $\text{ord}(g) = \min \{n \in \mathbb{N}_+ \mid g^n = e\}$.

הערה: תהא G חבורה ויהי $g \in G$ עבורו $\text{ord}(g)$ לא קיים אזי $\text{ord}(g) = \infty$.

טענה: יהי $n \in \mathbb{N}_+$ ויהי $i \in \mathbb{Z}_n$ אזי $\langle i \rangle = \mathbb{Z}_n \iff \langle i, n \rangle$ (זרים).

טענה: תהא G חבורה ציקלית ותהא $H \leq G$ אזי H ציקלית.

קוסט ימני: תהא G חבורה תהא $H \leq G$ ויהי $g \in G$ אזי $H * g$.

קוסט שמאלי: תהא G חבורה תהא $H \leq G$ ויהי $g \in G$ אזי $g * H$.

נציג של קוסט ימני: תהא G חבורה ויהי Hg קוסט ימני אזי g .

נציג של קוסט שמאלי: תהא G חבורה ויהי gH קוסט שמאלי אזי g .

מסקנה: תהא G חבורה אבלית תהא $H \leq G$ ויהי $g \in G$ אזי $Hg = gH$.

מסקנה: תהא G חבורה תהא $H \leq G$ ויהי $g \in G$ אזי $(gH)^{-1} = Hg^{-1}$.

טענה: תהא G חבורה תהא $H \leq G$ ויהי $g \in G$ אזי $(gH = H) \iff (g \in H)$.

טענה: תהא G חבורה תהא $H \leq G$ ויהי $g \in G$ אזי $(Hg = H) \iff (g \in H)$.

סימון: תהא G חבורה ותהא $H \leq G$ אזי $G/H = \{gH \mid g \in G\}$.

סימון: תהא G חבורה ותהא $H \leq G$ אזי $H \backslash G = \{Hg \mid g \in G\}$.

משפט: תהא G חבורה ותהא $H \leq G$ אזי G/H חלוקה של G .

טענה: תהא G חבורה תהא $H \leq G$ ויהיו $g_1, g_2 \in G$ אזי $(g_1H = g_2H) \iff (g_2^{-1}g_1 \in H)$.

הקוסט הטריוואלית: תהא G חבורה ותהא $H \leq G$ אזי eH .

אינדקס של תת-חבורה בחבורה: תהא G חבורה ותהא $H \leq G$ אזי $[G : H] = |G/H|$.

טענה: תהא G חבורה ותהא $H \leq G$ אזי $[G : H] = |H \backslash G|$.

טענה: תהא G חבורה סופית ותהא $H \leq G$ אזי $\text{ord}(G) = \text{ord}(H) \cdot [G : H]$.

משפט לגראנז': תהא G חבורה סופית ותהא $H \leq G$ אזי $\text{ord}(H) \mid \text{ord}(G)$.

מסקנה: תהא G חבורה סופית ויהי $g \in G$ אזי $\text{ord}(g) \mid \text{ord}(G)$.

טענה: תהא G חבורה תהא $H \leq G$ ותהא $K \leq H$ אזי $[G : K] = [G : H] \cdot [H : K]$.

מסקנה: יהי $p \in \mathbb{P}$ תהא G חבורה סופית באשר $\text{ord}(G) = p$ אזי לכל $g \in G \setminus \{e\}$ מתקיים $G = \langle g \rangle$.

מסקנה: יהי $p \in \mathbb{P}$ תהא G חבורה סופית באשר $\text{ord}(G) = p$ אזי G ציקלית.

מסקנה משפט פרמה הקטן: יהי $p \in \mathbb{P}$ ויהי $n \in \mathbb{N}$ באשר $\text{gcd}(n, p) = 1$ אזי $n^{p-1} \equiv 1 \pmod{p}$.

למה: תהא G חבורה ותהיינה $H, K \leq G$ חבורות סופיות אזי $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$.

טענה: יהיו $p, q \in \mathbb{P}$ באשר $p > q$ ותהא G חבורה באשר $|G| = pq$ אזי לכל $H, K \leq G$ באשר $\text{ord}(H) = p$ וכן $\text{ord}(K) = p$ מתקיים $K = H$.