

תרגול 1: אלגוריתם החלוקה של אוקלידס, חבורות ולא חבורות, טבלאות כפל, תרגילי הוכחה

משפט אוקלידס - חלוקה עם שארית:

בהנתן שני מספרים $a, b \in \mathbb{Z}$ כך ש $b \neq 0$, ניתן לחלק את a ב b עם שארית: כלומר קיימים $r, q \in \mathbb{Z}$ כך ש $0 \leq r < |b|$ ומתקיים $a = qb + r$. המספר r נקרא **השארית** (remainder) של החלוקה, והמספר q הוא **המנה** (quotient) של החלוקה.

דוגמאות: $7 = 3 \times 2 + 1$ (מנה 3, שארית 1). $7 = (-3) \times (-2) + 1$ (מנה -3, שארית 1).

תרגיל בית: הראו ש q, r נקבעים ביחידות.

הגדרה: יהיו $a, b \in \mathbb{Z}$. נאמר ש b מחלק את a אם קיים $c \in \mathbb{Z}$ כך ש $a = bc$. כלומר b מחלק את a ללא שארית.

הגדרה: בהנתן שני מספרים $0 \neq a, b \in \mathbb{Z}$ נגדיר את **המחלק המשותף הגדול ביותר** (הממג"ב) שלהם להיות המספר השלם הגדול ביותר שמחלק את שניהם. נסמן ע"י $\gcd(a, b)$ או (a, b) .
 $\gcd = \text{greatest common divisor}$.

הגדרה: בהנתן שני מספרים $a, b \in \mathbb{Z}$ שאינם שניהם 0, נגדיר את **הכפולה המשותפת הקטנה ביותר** (הכמק"ב) שלהם להיות המספר **הטבעי הקטן ביותר** שמתחלק בשניהם. נסמן ע"י $\text{lcm}(a, b)$. $\text{lcm} = \text{least common multiple}$.

הערה: לשם הנוחיות נגדיר בצורה דומה **כפולה משותפת ומחלק משותף** (כלומר לא בהכרח הגדולים ביותר או הקטנים ביותר).

דוגמא:

$$\gcd(6, 4) = 2, \gcd(6, 12) = 6, \text{lcm}(2, 3) = 6, \text{lcm}(2, 4) = 4$$

הגדרה: נאמר ש $a, b \in \mathbb{Z}$ הם זרים אם $\gcd(a, b) = 1$.

משפט (נקרא למשפט זה משפט ה-gcd): בהנתן שני מספרים $a, b \in \mathbb{Z}$, $0 \neq a, b$ קיימים

מספרים $u, v \in \mathbb{Z}$ כך ש $au + bv = \gcd(a, b)$.

הערה: במערכי התרגול נסמן משפטים חשובים או כאלה שמשמשים בהם בהמשך הקורס במסגרת אדומה.

דוגמא:

למשל, $\gcd(234, 61) = 1$ (כי 61 הוא מספר ראשוני) וניתן לחשב ש-
 $1 = 6 \cdot 234 + (-23) \cdot 61$. נראה בהמשך איך מוצאים את המקדמים -23, 6.

הוכחת בניה של משפט ה-gcd:

נזכר באלגוריתם החלוקה של אויקלידס: בהנתן שני שלמים a, b , נבצע סדרה של חלוקות עם שארית:

$$a = bq_1 + r_1$$

$$b = r_1q_2 + r_2$$

$$r_1 = r_2q_3 + r_3$$

⋮

$$r_{k-1} = r_kq_{k+1} + r_{k+1}$$

$$r_k = r_{k+1}q_{k+2}$$

(תרגיל בית: הסבירו מדוע סדרת החלוקות חייבת להסתיים בכך שהשארית האחרונה r_{k+2} היא

(0.)

נעת נראה ש $r_{k+1} = \gcd(a, b)$.

הוכיחו באינדוקציה את הטענה הבאה:

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \dots = \gcd(r_k, r_{k+1}) = r_{k+1}$$

(נראה את השלב הראשון: נסמן $d := \gcd(a, b)$. אזי

$$d \mid a, b \Rightarrow d \mid r_1 \Rightarrow d \mid b, r_1 \Rightarrow d \leq \gcd(b, r_1).$$

כעת ניתן להוכיח באינדוקציה (הפוכה) שניתן להציג את r_{k+1} כצירוף לינארי של r_k, r_{k-1} , כולל כצירוף לינארי של a, b .

דוגמא: נפעיל את אלגוריתם הבניה עבור הדוגמא: $\gcd(234, 61) = 1$.

$$234 = 61 \times 3 + 51$$

$$61 = 51 \times 1 + 10$$

$$51 = 10 \times 5 + 1$$

$$10 = 1 \times 10$$

ואז נקבל:

$$\gcd(234, 61) = \gcd(61, 51) = \gcd(51, 10) = \gcd(5, 1) = 1$$

את הצירוף הלינארי המתאים נקבל כמו בהוכחה ע"י הצגת כל שארית כצירוף אלגברי מתאים של השאריות הקודמות:

$$1 = 51 - 10 \times 5$$

$$10 = 61 - 51 \times 1$$

$$51 = 234 - 61 \times 3$$

\Rightarrow

$$1 = 51 - 10 \times 5 = (234 - 61 \times 3) - (61 - 51 \times 1) \times 5 = (234 - 61 \times 3) - (61 - (234 - 61 \times 3) \times 1) \times 5 = 6 \times 234 + (-23) \times 61$$

הוכחת קיום של משפט ה gcd: נסמן ב- S את קבוצת כל הצירופים הלינאריים החיוביים של a

ו- b (שאלה: מדוע ה gcd תמיד חיובי?):

$$S = \{au + bv \mid au + bv > 0, u, v \in \mathbb{Z}\}$$

נשים לב ש- S אינה ריקה (למה?), ומכיוון שזו קבוצה של מספרים אי-שליליים, קיים איבר קטן ביותר $d > 0$. מהגדרת S קיימים x, y כך ש- $ax + by = d$. נראה ש- $d = \gcd(a, b)$, $d - r = a$ מחלק משותף מקסימלי של a ו- b .

ע"פ משפט החילוק ניתן למצוא מספרים שלמים q, r כך ש- $a = qd + r$, $0 \leq r < d$. למעשה:

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy)$$

נניח בשלילה ש- r שונה מ-0: נקבל ש- r היה איבר של S (כצירוף לינארי של a ו- b); בסתירה לכך ש- d הוא האיבר מינימלי ב- S (כי $r < d$). לכן $r = 0$ ולכן $a = qd$. כלומר $d \mid a$. באותו אופן מראים ש-

$d \mid b$, ולכן d מחלק משותף של a ו- b . נשאר להוכיח שהוא המחלק המשותף המקסימלי.

אם c מחלק משותף כלשהו של a ו- b , אז $c \mid (ax+by)$ ולכן $c \mid d$. נובע מכך ש- $c \leq d$ ולכן d גדול מכל מחלק משותף חיובי של a ו- b . מהגדרת \gcd מקבלים ש- $d = (a,b)$.

נשים לב שקיבלנו ש- d הוא האיבר המינימלי ב- S . □

תרגיל בית: (טענות נוספות על \gcd, lcm)

1. אם c מחלק משותף של $a, b \in \mathbb{Z}$ אזי c מחלק את $\gcd(a,b)$ (נובע ישירות מלמת בזו).

2. אם c מתחלק ב- $a, b \in \mathbb{Z}$ אזי c מתחלק ב- $lcm(a,b)$.

3. אם $a = \prod_{i=1}^m p_i^{\alpha_i}, b = \prod_{i=1}^m p_i^{\beta_i}$ הם הפירוקים לגורמים ראשוניים, אזי

$$\gcd(a,b) = \prod_{i=1}^m p_i^{\min(\alpha_i, \beta_i)}, lcm(a,b) = \prod_{i=1}^m p_i^{\max(\alpha_i, \beta_i)}$$

$$lcm(a,b) = \frac{ab}{\gcd(a,b)} \quad 4.$$

$$\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1 \quad 5.$$

6. אם $a \mid bc$ וגם $\gcd(a,b) = 1$ אזי $a \mid c$.

הגדרה: חבורה היא קבוצה G עם פעולה בינארית $\otimes : G \otimes G \rightarrow G$

המקיימת את 4 האקסיומות הבאות:

(1) **סגירות** (קשירות):

$$\forall a, b \in G \quad a \otimes b \in G$$

כלומר אם לוקחים שני איברים ומפעילים עליהם את פעולת הכפל הנ"ל אז התוצאה היא איבר בקבוצה (למעשה זה נובע ישירות מ *).

(2) **אסוציאטיביות** (קיבוציות):

$$\forall a, b, c \in G \quad (a \otimes b) \otimes c = a \otimes (b \otimes c)$$

כלומר עם הכללה באינדוקציה אנו יכולים לומר שסדר השמת הסוגרים עבור מספר איברים סופי אינו משנה.

(3) **קיום איבר יחידה** $e \in G$ כך ש: $\forall a \in G \quad e \otimes a = a \otimes e = a$

(4) **קיום הופכי:** $\forall a \in G \exists b \in G \quad a \otimes b = b \otimes a = e$

אם בנוסף לארבעת האחרונים מתקיים:

(5) **חילופיות:**

$$\forall a, b \in G \quad a \otimes b = b \otimes a$$

אז החבורה נקראת חבורה **חילופית או אבלית** (או **קומוטטיבית**).

אם מתקיים רק 1-3 (כלומר לא מובטח קיום הפכי) אז נקרא לקבוצה **מונואיד**. אם מתקיים 1-2 (כלומר לא מובטח קיום איבר יחידה) אזי נקרא לקבוצה **אגודה** (semigroup).

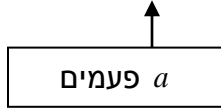
הערה: לעתים רבות נשמיט את סימן פעולת החבורה, ונרשום ישירות ab במקום $a \otimes b$. לעיתים גם משתמשים בסימון $a \cdot b$ אם רוצים להפריד בין האותיות.

הערה: כאשר מתייחסים לחבורה, מקובל לכתוב (G, \otimes, e) כדי לציין את הקבוצה, הפעולה, ואיבר היחידה.

דוגמאות: נבחן מספר דוגמאות של קבוצות ופעולות בינאריות עליהן, ונבחן האם מתקיימות האקסיומות 1-5 עבורן.

(1) $S = (\mathbb{N}, *)$ כאשר הפעולה * מוגדרת ע"י $a * b = b^a$.

סגירות: כיוון ש $a \in \mathbb{N}$ אזי $b^a = \underbrace{bb \cdots b}_a \in \mathbb{N}$



הפעולה אינה אסוציאטיבית: $2 * (3 * 2) = (2^3)^2 = 64 \neq 512 = 2^{(3^2)} = (2 * 3) * 2$.

האם יש ב S איבר יחידה? נניח בשלילה ש $e \in S$ הוא איבר יחידה. אזי

$$1 = 1^e = e * 1 = 1 * e = e^1 = e$$

אבל 1 אינה יחידה כיוון ש

$$1 * 2 = 2^1 = 2 \neq 1 = 1^2 = 2 * 1$$

1 היא יחידה שמאלית (כלומר לכל איבר $a \in \mathbb{N}$ מתקיים $a * 1 = a$).

כיוון שאין איבר יחידה, אין מה לבדוק את האקסיומה של קיום איבר הפכי.

(2) תהי X קבוצה. אזי $(P(X), \cup)$ היא מונואיד אבל, כאשר \emptyset היא היחידה, בקורס "מתמטיקה בדידה" ראינו סגירות, אסוציאטיביות וקומוטטיביות. $P(X)$ אינה חבורה, כי אין איבר הפכי לאף איבר שונה מ \emptyset (אם $A \cup B = \emptyset$ אזי $A = B = \emptyset$). $(P(X), \cap)$ גם היא מונואיד, כאשר X היא היחידה. לכל איבר $a \in P(X)$ בשני המונואידים מתקיים

$$a^2 = aa = \begin{cases} a \cap a = a \\ a \cup a = a \end{cases}$$

קוראים $a^2 = a$ קוראים **אידימפוטנטים**,

ויש להם חשיבות רבה. בחבורה האידימפוטנט היחיד הוא איבר היחידה.

(3) תהי X קבוצה לא ריקה. אזי $(P(X), \setminus)$ לא מקיימת אסוציאטיביות. כיוון ש $X \neq \emptyset$ נקח $a \in X$, ואת הקבוצה $\{a\} \in P(X)$, אזי $\{a\} \setminus \{a\} = \emptyset$ ולעומת זאת, $\{a\} \setminus (\emptyset \setminus \{a\}) = \{a\} \setminus \emptyset = \{a\} \neq \emptyset$. האם קיים איבר יחידה? לא. אם קיים איבר יחידה $E \in P(X)$, אזי $\emptyset = \emptyset \setminus E = E \setminus \emptyset = E$, כלומר בהכרח $E = \emptyset$, אבל \emptyset אינו איבר יחידה אם, כיוון ש $\emptyset \setminus X = \emptyset \neq X$. אבל \emptyset יחידה ימנית.

4) נקח את קבוצת הנקודות $C = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ (זהו מעגל היחידה). נגדיר פעולה על הנקודות במעגל $(x, y) * (z, w) = (xz - yw, xw + yz)$. נבדוק שהפעולה הזאת

אכן מגדירה חבורה, ובנוסף היא חבורה אבלית:

סגירות: צריך להראות שהנקודה $(xz - yw, xw + yz)$ אכן שייכת למעגל.

$$\begin{aligned} (xz - yw)^2 + (xw + yz)^2 &= x^2 z^2 - 2xyzw + y^2 w^2 + x^2 w^2 + 2xyzw + y^2 z^2 = \\ &= x^2 z^2 + y^2 w^2 + x^2 w^2 + y^2 z^2 = (x^2 + y^2)z^2 + (x^2 + y^2)w^2 = z^2 + w^2 = 1 \end{aligned}$$

אסוציאטיביות: נקח 3 נקודות על המעגל, $(x, y), (z, w), (s, t) \in C$.

$$\begin{aligned} [(x, y) * (z, w)] * (s, t) &= (xz - yw, xw + yz) * (s, t) = \\ &= ((xz - yw)s - (xw + yz)t, (xz - yw)t + (xw + yz)s) = \\ &= (sxz - syw - txw - tyz, txz - tyw + sxw + syz) \\ (x, y) * [(z, w) * (s, t)] &= (x, y) * (sz - tw, tz + sw) = \\ &= (x(sz - tw) - y(tz + sw), x(tz + sw) + y(sz - tw)) = \\ &= (sxz - txw - tyz - syw, txz + sxw + syz - tyw) \end{aligned}$$

איבר יחידה: $e = (1, 0)$

$$(1, 0) * (x, y) = (1 \cdot x - 0 \cdot y, 1 \cdot y + 0 \cdot x) = (x, y)$$

$$(x, y) * (1, 0) = (x \cdot 1 - y \cdot 0, x \cdot 0 + y \cdot 1) = (x, y)$$

הפכי: $(x, y)^{-1} = (x, -y)$

$$(x, y) * (x, -y) = (x^2 + y^2, -xy + xy) = (1, 0)$$

$$(x, -y) * (x, y) = (x^2 + y^2, xy - xy) = (1, 0)$$

מי זאת החבורה הזאת: ניתן לראות אותה באופן גיאומטרי כסכום הזוויות של הוקטורים $(x, y), (z, w) \in C$, או לחלופין, לזהות את הנקודה (x, y) עם הנקודה $x + iy \in \mathbb{C}$ ואז הפעולה "המסובכת" הנ"ל היא פשוט כפל של מספרים מרוכבים.

הגדרה: סדר של חבורה הוא העוצמה של הקבוצה של החבורה.

טבלאות כפל:

כל חבורה סופית מוגדרת לחלוטין ע"י טבלת הכפל המתאימה לפעולה הבינארית של החבורה. נראה כעת דוגמא: נשווה את טבלאות הכפל של החבורה \mathbb{Z}_4 (חיבור של המספרים $\{0, 1, 2, 3\}$

מודולו 4) והחבורה $\mathbb{Z}_2 \times \mathbb{Z}_2$ (מכפלה קרטזית של שני עותקים של \mathbb{Z}_2) עם הפעולה

(למעשה זה מ"ו ממימד 2 מעל השדה \mathbb{Z}_2). חבורה זאת נקראת גם **חבורת קליין**. איבר היחידה הוא $(0,0)$. טבלאות הכפל של שתי החבורות הן:

\mathbb{Z}_4	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_2 \times \mathbb{Z}_2$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

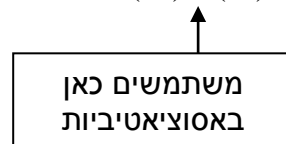
נשים לב ששתי הטבלאות סימטריות כי החבורות אבליות. שתי החבורות הן שונות! רואים זאת ע"י ההבדל בין האלכסונים. בחבורת קליין כל איבר הפכי לעצמו, וזה לא המצב בחבורה מודולו 4. בחבורות לא אבליות קוראים את הטבלה עמודה*שורה ($row * column$). נשים לב שכל עמודה וכל שורה בטבלת הכפל היא **תמורה** של האיברים.

תרגיל בית: נסו לבנות טבלת כפל לחבורה כלשהיא מסדר 3, והראו שהיא חייבת להיות אבלית.

טענה: תהי G חבורה אז לכל $a \in G$ קיים איבר הפכי יחיד נסמן אותו ב: a^{-1} .

טענה: תהי G חבורה אז קיים איבר יחידה יחיד ב G נסמן אותו ב: e .

הערה: במונואיד M (ובפרט בחבורה) מתקיים שאם איבר $a \in M$ הפיך מימין (כלומר קיים $b \in M$ כך ש $ab = e$), וגם הפיך משמאל (כלומר קיים $c \in M$ כך ש $ca = e$) אזי בהכרח a הפיך ומתקיים $b = c = a^{-1}$. מוכיחים זאת ע"י $b = c = a^{-1}$.



תרגיל: יהי M מונואיד. הראו שאם $a, b \in M$ הפיכים, אזי ab הפיך.

פתרון: $(ab)^{-1} = b^{-1}a^{-1}$, רואים זאת ע"י $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$, ואותו

דבר בהכפלה מהכיוון השני. שימו לב: אנחנו השתמשנו כאן באסוציאטיביות של החבורה. ללא אסוציאטיביות, לא היינו יכולים להוכיח תרגיל זה.

הגדרה: יהי $x \in G$ איבר בחבורה, אזי נגדיר חזקה של איבר ע"י $x^n := x^{n-1} \otimes x = x \otimes \dots \otimes x$.
 כאשר $x^1 := x$ ו- $x^0 = e$.

הערה: יהי $a \in G$ איבר בחבורה, אזי $a^{m+n} = a^m a^n$ וגם $(a^m)^n = a^{mn}$. שימו לב שלא בהכרח מתקיים $(ab)^n = a^n b^n$, כיוון שלא בהכרח מתקיים $ab = ba$.

כתיב חיבורי לעומת כתיב כפלי

נשים לב שבחבורה בה הפעולה היא "חיבורית" (+) זה פחות נוח להשתמש בסימון כגון x^n , כיוון שלפי הגדרה $x^n = x + x + \dots + x$ כאשר הסכום מתבצע n פעמים. הרבה יותר נוח להשתמש בסימון nx , ולכן נביא להלן מילון שבו נחליף את הסימונים המקובלים עבור חבורות בסימונים המקובלים עבור חבורות חיבוריות:

הפעולה	חבורה "כפלית"	חבורה "חיבורית"
כפל בחבורה	ab	$a + b$
איבר יחידה/ניטרלי/אדיש	1 או e	0
איבר הפכי	a^{-1}	$-a$
חזקה של איבר	a^n	na
כפל בהפכי	ab^{-1}	$a - b$

בהמשך הקורס נרחיב את הטבלה הזאת עם עוד מספר פעולות.

הגדרה: נאמר ששני איברים $a, b \in G$ בחבורה **מתחלפים** אם $ab = ba$.
טענה: חבורה G היא חבורה אבליית אם ורק אם כל שני איברים בה מתחלפים.

תרגיל: אם $(G, *)$ חבורה ולכל $x \in G$ מתקיים $x^2 = e$ אז G חבורה אבלית.

הוכחה:

$$\forall x, y \in G$$

$$xx = e \rightarrow x = x^{-1}$$

$$(xy)^2 = e$$

$$xyxy = e$$

$$xy = y^{-1}x^{-1} = yx$$

□

תרגיל: תהי $(G, *)$ חבורה. הוכח שלמשוואה:

$$xax = b$$

יש פתרון אם ab הוא ריבוע (כלומר קיים $t \in G$ המקיים $t^2 = ab$)

הוכחה:

כיוון א' (קל): נתון ל $xax = b$ יש פתרון צ"ל: קיים $t^2 = ab$.

לפי הנתון מתקיים:

$$\exists c \in G \quad cac = b$$

נכפיל את שני הצדדים ב a משמאל ונקבל:

$$acac = ab$$

$$(ac)^2 = ab \rightarrow ac = t, t^2 = ab$$

כיוון ב': נתון $\exists t \in G \quad t^2 = ab$ צ"ל: למשוואה $xax = b$ קיים פתרון ב G . נעזר בכיוון א': אנחנו

כבר יודעים שאם קיים פתרון x אז בהכרח מתקיים $t=ax$. לכן "ננחש" שהפתרון הוא $x = a^{-1}t$:

$$\begin{aligned} xax &= (a^{-1}t)a(a^{-1}t) = a^{-1}taa^{-1}t = \\ &= a^{-1}t^2 = a^{-1}ab = b \end{aligned}$$

□