

# מערך תרגיל קורס 89-214 סמסטר א' תשע"ו מבנים אלגבריים למדעי המחשב

אוקטובר 2015, גרסה 0.4

## מבוא

נתחיל עם כמה דגשים:

- דף הקורס נמצא באתר [www.math-wiki.com](http://www.math-wiki.com).
- שאלות בנוגע לחומר הלימודי מומלץ לשאול בדף השיחה באתר של הקורס.
- ישנה חובת הגשת תרגילים, אבל בודקים רק לחצי מהסטודנטים (ואולי יהיו בחנים שיתבססו על התרגילים).
- נשמח לכל הערה על מסמך זה.

## 1 מבוא לתורת המספרים

נסמן כמה קבוצות של מספרים:

- $\mathbb{N} = \{1, 2, 3, \dots\}$  המספרים הטבעיים.
- $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$  המספרים השלמים (מגרמנית: Zahlen).
- $\mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\} \right\}$  המספרים הרציונליים.
- $\mathbb{R}$  המספרים הממשיים.
- $\mathbb{C}$  המספרים המרוכבים.

מתקיים  $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ .

**הגדרה 1.1.** יהיו  $a, b$  מספרים שלמים. נאמר כי  $a$  פחלק את  $b$  אם קיים  $k \in \mathbb{Z}$  כך ש- $ka = b$ , ונסמן  $a|b$ . למשל  $5|10$ .

**משפט 1.2** (משפט החילוק, או חלוקה אוקלידית). לכל  $d \neq 0, n \in \mathbb{Z}$  קיימים  $q, r$  יחידים כך ש- $n = qd + r$  וגם  $0 \leq r < |d|$ .

המשפט לעיל מתאר "מה קורה" כאשר מחלקים את  $n$  ב- $d$ . הבחירה בשמות הפרמטרים במשפט מגיעה מלע"ז (מאנגלית?) quotient (מנה) ו-remainder (שארית).

**הגדרה 1.3**. בהנתן שני מספרים שלמים  $n, m$  המחלק המשותף המירבי (ממ"מ, greatest common divisor) שלהם מוגדר להיות המספר

$$\gcd(n, m) = \max \{d \in \mathbb{N} : d|n \wedge d|m\}$$

לעיתים נסמן  $(n, m)$ . למשל  $(6, 10) = 2$ . נאמר כי  $n, m$  זרים אם  $(n, m) = 1$ . למשל  $(2, 5) = 1$ .

הערה 1.4. אם  $d|a$  וגם  $d|b$ , אזי  $d$  מחלק כל צירוף לינארי של  $a$  ו- $b$ .

טענה 1.5. אם  $n = qm + r$ , אז  $(n, m) = (m, r)$ .

הוכחה. נסמן  $d = (n, m)$ , וצ"ל כי  $d = (m, r)$ . אנו יודעים כי  $d|n$  וגם  $d|m$ . אנו יכולים להציג את  $r$  כצירוף לינארי של  $n, m$ , ולכן  $d|r = n - qm$ . מכך קיבלנו  $d \leq (m, r)$ . כעת, לפי הגדרה  $(m, r)|r$  וגם  $(m, r)|m$ , ולכן  $(m, r)|n$  כי  $n$  הוא צירוף לינארי של  $m, r$ . אם ידוע כי  $(m, r)|m$  וגם  $(m, r)|n$ , אזי  $(m, r) \leq d$ . סך הכל קיבלנו כי  $d = (m, r)$ .  $\square$

**משפט 1.6** (אלגוריתם אוקלידס). "המתכון" למציאת פ"מ בעזרת שימוש חוזר בטענה 1.5 הוא אלגוריתם אוקלידס. ניתן להניח  $0 \leq m < n$ . אם  $m = 0$ , אזי  $(n, m) = n$ . אחרת נכתוב  $n = qm + r$  כאשר  $0 \leq r < m$  וגמשיך עם  $(n, m) = (m, r)$ . (הבינו לפה האלגוריתם חייב להעצר.)

**דוגמה 1.7**. נחשב את הממ"מ של 53 ו-47 בעזרת אלגוריתם אוקלידס

$$(53, 47) = [53 = 1 \cdot 47 + 6]$$

$$(47, 6) = [47 = 7 \cdot 6 + 5]$$

$$(6, 5) = 1$$

דוגמה נוספת עבור מספרים שאינם זרים:

$$(224, 63) = [224 = 3 \cdot 63 + 35]$$

$$(63, 35) = [63 = 1 \cdot 35 + 28]$$

$$(35, 28) = [35 = 1 \cdot 28 + 7]$$

$$(28, 7) = [28 = 4 \cdot 7 + 0]$$

$$(7, 0) = 7$$

**משפט 1.8** (אפיון הממ"מ כצירוף לינארי מזערי). מתקיים לכל מספרים שלמים  $a, b$  כי

$$(a, b) = \min_{u,v} \{au + bv \in \mathbb{N}\}$$

בפרט קיימים  $s, t \in \mathbb{Z}$  כך ש- $(a, b) = sa + tb$ .

הערה 1.9. מן המשפט קיבלנו כי  $(a, b) \in a\mathbb{Z} + b\mathbb{Z}$ .

**דוגמה 1.10.** כדי למצוא את המקדמים  $s, t$  כשמביעים את הממ"מ כצירוף לינארי כנ"ל נשתמש באלגוריתם אוקלידס המוכלל:

$$(234, 61) = [234=3 \cdot 61+51 \Rightarrow 51 = 234 - 3 \cdot 61]$$

$$(61, 51) = [61=1 \cdot 51+10 \Rightarrow 10 = 61 - 1 \cdot 51 = 61 - 1 \cdot (234 - 3 \cdot 61) = -1 \cdot 234 + 4 \cdot 61]$$

$$(51, 10) = [51=5 \cdot 10+1 \Rightarrow 1 = 51 - 5 \cdot 10 = 51 - 5 \cdot (-1 \cdot 234 + 4 \cdot 61) = 6 \cdot 234 - 23 \cdot 61]$$

$$(10, 1) = 1$$

$$\text{ולכן } (234, 61) = 1 = 6 \cdot 234 - 23 \cdot 61$$

**תרגיל 1.11.** יהיו  $a, b, c$  מספרים שלמים כך ש- $(a, b) = 1$  וגם  $a|bc$ . הראו כי  $a|c$ .

פתרון. לפי אפיון הממ"מ כצירוף לינארי, קיימים  $s, t$  כך ש- $1 = sa + tb$ . נכפיל ב- $c$  ונקבל  $c = sac + tbc$ . ברור כי  $a|sac$  ולפי הנתון גם  $a|tbc$ . לכן  $a|(sac + tbc)$ , כלומר  $a|c$ .

סעיף 1.12. תכונות של ממ"מ:

$$1. \text{ יהי } d = (n, m) \text{ ויהי } e \text{ כך ש-} e|m \text{ וגם } e|n, \text{ אזי } e|d.$$

$$2. (an, am) = |a|(n, m)$$

$$3. \text{ אם } p \text{ ראשוני וגם } p|ab, \text{ אזי } p|a \text{ או } p|b.$$

הוכחת התכונות. 1. קיימים  $s, t$  כך ש- $d = sn + tm$ . כיוון ש- $e|n, m$ , אז הוא מחלק גם את צירוף לינארי שלהם  $sn + tm$ , ז"א את  $d$ .

2. (חלק מתרגיל הבית)

3. אם  $p \nmid a$ , אז  $(p, a) = 1$ . לכן קיימים  $s, t$  כך ש- $sa + tp = 1$ . נכפיל את השויוון האחרון ב- $b$  ונקבל  $b = sab + tpb$ . ברור כי  $p$  מחלק את  $sa + tp$  (הרי  $p|ab$ ), ולכן  $p$  מחלק את  $b$ . כלומר  $p|b$ .

□

**הגדרה 1.13.** בהנתן שני מספרים שלמים  $n, m$  הכפולה המשותפת המזערית (כמ"מ, least common multiple) שלהם מוגדרת להיות

$$\text{lcm}(n, m) = \min \{d \in \mathbb{N} : n|d \wedge m|d\}$$

לעיתים נסמן  $[n, m]$ . למשל  $[6, 10] = 30$  ו- $[2, 5] = 10$ .

טענה 1.14. תכונות של כמ"מ:

1. אם  $m|a$  וגם  $n|a$ , אז  $[n, m]|a$ .

2.  $[n, m](n, m) = |nm|$ . למשל  $[6, 4](6, 4) = 12 \cdot 2 = 24 = 6 \cdot 4$ .

הוכחת התכונות. 1. יהיו  $q, r$  כך ש- $a = q[n, m] + r$  כאשר  $0 \leq r < [n, m]$ . מהנתון כי  $n, m|a$  ולפי הגדרה  $[n, m]|n, m$ , נובע כי  $n, m|r$ . אם  $r \neq 0$  אז סתירה למינימליות של  $[n, m]$ . לכן  $a = q[n, m]$ , כלומר  $[n, m]|a$ .

2. נראה דרך קלה לחישוב הממ"מ והכמ"מ בעזרת הפירוק של מספר למכפלת גורמים ראשוניים. נניח כי הפירוק הוא

$$n = \prod_{i=1}^{\infty} p_i^{\beta_i} = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \dots \quad m = \prod_{i=1}^{\infty} p_i^{\alpha_i} = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots$$

כאשר  $\alpha_i, \beta_i \geq 0$  (והם כמעט תמיד אפס כי המכפלה סופית). כעת צריך להשתכנע כי

$$(n, m) = \prod_{i=1}^{\infty} p_i^{\min(\alpha_i, \beta_i)} \quad [n, m] = \prod_{i=1}^{\infty} p_i^{\max(\alpha_i, \beta_i)}$$

ומפני שלכל שני מספרים  $\alpha, \beta$  מתקיים  $\alpha + \beta = \min(\alpha, \beta) + \max(\alpha, \beta)$ , אז  $[n, m](n, m) = |nm|$ .

□

**שאלה 1.15** (לבית). אפשר להגדיר ממ"מ ליותר מזוג מספרים. יהי  $d$  הממ"מ של המספרים  $n_1, \dots, n_k$ . הראו שקיימים מספרים שלמים  $s_1, \dots, s_k$  המקיימים  $s_1 n_1 + \dots + s_k n_k = d$ . רמז: אינדוקציה על  $k$ .

**הגדרה 1.16**. יהי  $n$  מספר טבעי. נאמר כי  $a, b \in \mathbb{Z}$  הם שקולים בשארית חלוקה  $n$ -ב אם  $a \equiv b \pmod{n}$ . כלומר קיים  $k \in \mathbb{Z}$  כך ש- $a = b + kn$ . נסמן יחס זה  $a \equiv b \pmod{n}$  ונקרא זאת " $a$  שקול ל- $b$  מודולו  $n$ ".

טענה 1.17 (הוכחה לבית). שקילות מודולו  $n$  היא יחס שקילות (רפלקסיבי, סימטרי וטרנזיטיבי). כפל וחיבור מודולו  $n$  מוגדרים היטב. כלומר אם  $a \equiv b, c \equiv d \pmod{n}$ , אז  $ac \equiv bd \pmod{n}$  וגם  $a + c \equiv b + d \pmod{n}$ .

1.18. ירושם  $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$  מוסף מחלקות השקילות מודולו  $n$  מקובל לסמן  $\{[a] : a \in \mathbb{Z}\}$ . למשל  $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ . לפעמים מסמנים את מחלקת השקילות  $[a]$  בסימון  $\bar{a}$ , ולעיתים כאשר ההקשר ברור פשוט  $a$ .

**תרגיל 1.19**. מצאו את הספרה האחרונה של  $333^{333}$ .

פתרון. נשים לב כי  $333^{333} = 3^{333} \cdot 111^{333}$  לכן

$$\begin{aligned} 111 &\equiv 1 \pmod{10} \Rightarrow 111^{333} \equiv 1^{333} \equiv 1 \pmod{10} \\ 3^{333} &= 3^{4 \cdot 83 + 1} = (3^4)^{83} \cdot 3 = 81^{83} \cdot 3 \equiv 1^{83} \cdot 3 \pmod{10} \\ 333^{333} &= 3^{333} \cdot 111^{333} \equiv 3 \pmod{10} \end{aligned}$$

ומכאן שהספרה האחרונה היא 3.

**תרגיל 1.20** (אם יש זמן). מצאו  $x \in \mathbb{Z}$  כך ש- $61x \equiv 1 \pmod{234}$ .

פתרון. לפי הנתון, קיים  $k \in \mathbb{Z}$  כך ש- $61x + 234k \equiv 1$ . ז"א 1 הוא צירוף לינארי (מינימלי במקרה זה) של 61 ו-234. לפי איפיון ממ"מ קיבלנו כי  $(234, 61) = 1$ . כלומר  $k, x$  הם המקדמים מן המשפט של איפיון הממ"מ כצירוף לינארי מזערי. לפי תרגיל קודם  $1 = 6 \cdot 234 - 23 \cdot 61$ . לכן  $x \equiv -23 \pmod{234}$ , וכדי להבטיח כי  $x$  אינו שלילי נבחר  $x = 211$ .

**משפט 1.21** (משפט השאריות הסיני). אם  $n, m$  זרים, אזי לכל  $a, b \in \mathbb{Z}$  קיים  $x$  יחיד עד כדי שקילות מודולו  $nm$  כך ש- $x \equiv a \pmod{n}$ ,  $x \equiv b \pmod{m}$  (יחיד!).

הוכחה לא מלאה. מפני ש- $(n, m) = 1$ , אזי קיימים  $s, t \in \mathbb{Z}$  כך ש- $sn + tm = 1$ . כדי להוכיח קיום של  $x$  כמו במשפט נתבונן ב- $bsn + atm$ . מתקיים

$$\begin{aligned} bsn + atm &\equiv atm \equiv a \cdot 1 \equiv a \pmod{n} \\ bsn + atm &\equiv bsn \equiv b \cdot 1 \equiv b \pmod{m} \end{aligned}$$

ולכן  $x = bsn + atm$  הוא פתרון אפשרי. ברור כי גם  $x' = x + kmn$  לכל  $k \in \mathbb{Z}$  הוא פתרון תקף.

□ הוכחת היחידות של  $x$  מודולו  $nm$  תהיה בתרגיל הבית.

**דוגמה 1.22**. נמצא  $x \in \mathbb{Z}$  כך ש- $x \equiv 1 \pmod{3}$  וגם  $x \equiv 2 \pmod{5}$ . ידוע כי  $(5, 3) = 1$ , ולכן  $-1 \cdot 5 + 2 \cdot 3 = 1$ . במקרה זה  $n = 5, m = 3$  וכן  $s = -1, t = 2$ . לפי משפט השאריות הסיני אפשר לבחור את  $x = 1 \cdot (-5) + 2 \cdot 6 = 7$ . אכן מתקיים  $7 \equiv 1 \pmod{3}$  וגם  $7 \equiv 2 \pmod{5}$ .

משפט השאריות הסיני הוא יותר כללי. הנה גרסה שלו למערכת משוואות של שקילות מודולו:

**משפט 1.23** (אם יש זמן). תהא  $\{m_1, \dots, m_k\}$  קבוצת מספרים טבעיים הזרים זה לזה (כלומר כל זוג מספרים בקבוצה הוא זר). נסמן את מכפלתם ב- $m$ . בהנתן קבוצה כלשהי של שאריות  $\{a_i \pmod{m_i} : 1 \leq i \leq k\}$ , קיימת שארית יחידה  $x$  מודולו  $m$  המהווה פתרון למערכת המשוואות

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

**דוגמה 1.24.** נמצא  $y \in \mathbb{Z}$  כך ש- $y \equiv 1 \pmod{3}$ ,  $y \equiv 2 \pmod{5}$  וגם  $y \equiv 3 \pmod{7}$ . נשים לב שהפתרון  $y = 7$  מן הדוגמה הקודמת הוא נכון כדי כדי הוספה של  $3 \cdot 5 = 15$  (כי  $15 \equiv 0 \pmod{3}$  וגם  $15 \equiv 0 \pmod{5}$ ). לכן את שתי המשוואות  $y \equiv 1 \pmod{3}$ ,  $y \equiv 2 \pmod{5}$  ניתן להחליף במשוואה אחת  $y \equiv 7 \pmod{15}$ . נשים לב כי  $(15, 7) = 1$  ולכן אפשר להשתמש במשפט השאריות הסיני בגרסה לזוג משוואות. בדקו כי  $y = 52$  מהווה פתרון.

## 2 מבנים אלגבריים בסיסיים

בהתאם לשם הקורס, כעת נכיר כמה מבנים אלגבריים. מבנה אלגברי שמכירים כבר באלגברה לינארית הוא שדה. אנו נגדיר כמה מבנים יותר "פשוטים", כשהחשוב שבהם הוא חבורה. במרבית הקורס נתרכז בחקר חבורות.

**הגדרה 2.1.** תהי  $S$  קבוצה. פעולה בינארית (binary operation) על  $S$  היא פונקציה דו-מקומית  $: S \times S \rightarrow S$ . עבור  $a, b \in S$  כמעט תמיד במקום לרשום  $*(a, b)$  נשתמש בסימון  $a * b$ . מפני שתמונת הפונקציה  $a * b$  שייכת ל- $S$ , נאמר כי הפעולה היא סגורה.

**הגדרה 2.2.** אגודה (או חבורה למחצה, semigroup) היא מערכת אלגברית  $(S, *)$  המורכבת מקבוצה לא ריקה  $S$  ומפעולה בינארית על  $S$  המקיימת קיבוציות (אסוציאטיביות, associativity). כלומר לכל  $a, b, c \in S$  מתקיים  $(a * b) * c = a * (b * c)$ .

**דוגמה 2.3.** המערכת  $(\mathbb{N}, +)$  של מספרים טבעיים עם החיבור הרגיל היא אגודה.

**דוגמה 2.4.** המערכת  $(\mathbb{Z}, -)$  אינה אגודה, מפני שפעולת החיסור אינה קיבוצית. למשל  $(5 - 2) - 1 \neq 5 - (2 - 1)$ .

**צורת רישום 2.5.** לעיתים נקצר ונאמר כי  $S$  היא אגודה מבלי להזכיר במפורש את המערכת האלגברית. במקרים רבים הפעולה תסומן כמו כפל, דהיינו  $ab$  או  $a \cdot b$ , ובמקום לרשום מכפלה  $aa \dots a$  של  $n$  פעמים  $a$  נרשום  $a^n$ .

**הגדרה 2.6.** תהי  $(S, *)$  אגודה. איבר  $e \in S$  נקרא איבר יחידה אם לכל  $a \in S$  מתקיים  $a * e = e * a = a$ .

**הגדרה 2.7.** מונואיד (monoid, או יחידון)  $(M, *, e)$  הוא אגודה בעלת איבר יחידה  $e$ . כאשר הפעולה ואיבר היחידה ברורים מן ההקשר, פשוט נאמר כי  $M$  הוא מונואיד.

**הערה 2.8.** (בהרצאה). יהי  $(M, *, e)$  מונואיד עם איבר יחידה  $e$ . הוכיחו כי איבר היחידה הוא יחיד. הרי אם  $e, f \in M$  הם איברי יחידה, אז מתקיים  $e = e * f = f$ .

**הגדרה 2.9.** יהי  $(M, *, e)$  מונואיד. איבר  $a \in M$  יקרא הפיך משמאל אם קיים איבר  $b \in M$  כך ש- $ba = e$ . במקרה זה  $b$  יקרא הופכי שמאלי של  $a$ . באופן דומה, איבר  $a \in M$  יקרא הפיך ימין אם קיים איבר  $b \in M$  כך ש- $ab = e$ . במקרה זה  $b$  יקרא הופכי ימני של  $a$ . איבר יקרא הפיך אם קיים איבר  $b \in M$  כך ש- $ba = ab = e$ . במקרה זה  $b$  יקרא הופכי של  $a$ .

**תרגיל 2.10** (בהרצאה). יהי  $a \in M$  איבר הפיך משמאל ומימין. הראו ש- $a$  הפיך וההופכי שלו הוא יחיד.

פתרון. יהי  $b$  הופכי שמאלי כלשהו של  $a$  (קיים כזה כי  $a$  הפיך משמאל), ויהי  $c$  הופכי ימני כלשהו של  $a$  (הצדקה דומה). נראה כי  $b = c$  ונסיק שאיבר זה הוא הופכי של  $a$ . ודאו כי אתם יודעים להצדיק כל אחד מן המעברים הבאים:

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

לכן כל ההופכיים הימיניים וכל ההופכיים השמאליים של  $a$  שווים זה לזה. מכאן גם שההופכי הוא יחיד, ויסומן  $a^{-1}$ . שימו לב שאם איבר הוא רק הפיך מימין ולא משמאל, אזי יתכן שיש לו יותר מהופכי ימני אחד (וכנ"ל בהיפוך הכיוונים)!

**הגדרה 2.11** חבורה (group)  $(G, *, e)$  היא מונואיד שבו כל איבר הוא הפיך.

לפי ההגדרה לעיל על מנת להוכיח שמערכת אלגברית  $(G, *)$  היא חבורה צריך להראות כי הפעולה  $*$  היא סגורה, קיבוצית, שקיים איבר יחידה ושכל איבר הוא הפיך. כמו כן מתקיים: חבורה  $\Leftarrow$  מונואיד  $\Leftarrow$  אגודה.

**דוגמה 2.12** המערכת  $(\mathbb{Z}, +)$  היא חבורה שאיבר היחידה בה הוא 0. בכתיב חיבורי מקובל לסמן את האיבר ההופכי של  $a$  בסיומן  $-a$ . כתיב זה מתלכד עם המושג המוכר של מספר נגדי ביחס לחיבור.

**דוגמה 2.13** יהי  $F$  שדה (למשל  $\mathbb{Q}, \mathbb{R}$  או  $\mathbb{C}$ ). אזי  $(F, +, 0)$  עם פעולת החיבור של השדה היא חבורה. באופן דומה גם  $(M_{n,m}(F), +)$  (אוסף המטריצות בגודל  $n \times m$  מעל  $F$ ) עם פעולת חיבור מטריצות היא חבורה. איבר היחידה הוא מטריצת האפס.

**דוגמה 2.14** יהי  $F$  שדה. המערכת  $(F, \cdot)$  עם פעולת הכפל של השדה היא מונואיד שאינו חבורה (מי לא הפיך?). איבר היחידה הוא 1.

**דוגמה 2.15** יהי  $F$  שדה. נסמן  $F^* = F \setminus \{0\}$ . אזי  $(F^*, \cdot, 1)$  היא חבורה. לעומת זאת, המערכת  $(\mathbb{Z}^*, \cdot)$  עם הכפל הרגיל של מספרים שלמים היא רק מונואיד (מי הם האיברים ההפיכים בו?).

**דוגמה 2.16** קבוצה בעלת איבר אחד ופעולה סגורה היא חבורה. לחבורה זו קוראים החבורה הטריטיואלית.

**הגדרה 2.17** (חבורת האיברים ההפיכים). יהי  $M$  מונואיד ויהיו  $a, b \in M$  זוג איברים. אם  $a, b$  הם הפיכים, אזי גם  $a \cdot b$  הוא הפיך במונואיד. אכן, האיבר ההופכי הוא  $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ . לכן אוסף כל האיברים ההפיכים במונואיד מהווה קבוצה סגורה ביחס לפעולה. כמו כן האוסף הנ"ל מכיל את איבר היחידה, וכל איבר בו הוא הפיך. מסקנה מיידית היא שאוסף האיברים ההפיכים במונואיד מהווה חבורה ביחס לפעולה המצומצמת. נסמן חבורה זו ב- $U(M)$  (קיצור של Units).

**הגדרה 2.18.** המערכת  $(M_n(\mathbb{R}), \cdot)$  של מטריצות ממשיות בגודל  $n \times n$  עם כפל מטריצות היא מונואיד. לחבורת ההפיכים שלו

$$U(M_n(\mathbb{R})) = GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A \neq 0\}$$

קוראים החבורה הלינארית הכללית (ממעלה  $n$ ) מעל  $\mathbb{R}$  (General Linear group).

**הגדרה 2.19.** נאמר כי פעולה דו-מקומית  $\cdot : G \times G \rightarrow G$  היא אבלית (או חילופית, commutative) אם לכל שני איברים  $a, b \in G$  מתקיים  $a * b = b * a$ . אם  $(G, *)$  חבורה והפעולה היא אבלית, נאמר כי  $G$  היא חבורה אבלית (או חילופית). המושג נקרא על שמו של נילס הנריק אָבֶל (Niels Henrik Abel).

**דוגמה 2.20.** יהי  $F$  שדה. החבורה  $(GL_n(F), \cdot)$  אינה אבלית עבור  $n > 1$ .

**דוגמה 2.21.** מרחב וקטורי  $V$  יחד עם פעולת חיבור וקטורים הרגילה הוא חבורה אבלית.

הערה 2.22. עבור קבוצה סופית אפשר להגדיר פעולה בעזרת לוח כפל. למשל, אם  $S = \{a, b\}$  ונגדיר

*	a	b
a	a	a
b	b	b

אזי  $(S, *)$  היא אגודה כי הפעולה קיבוצית, אך היא אינה מונואיד כי אין בה איבר יחידה. נשים לב שהיא לא חילופית כי  $a * b = a$ , אבל  $b * a = b$ . בבית תתבקשו למצוא לוחות כפל עבור  $S$  כך שיתקבל מונואיד שאינו חבורה, שתתקבל חבורה וכו'.

הערה 2.23 (אם יש זמן). בקורס באלגברה לינארית כנראה ראיתם הגדרה של שדה  $(F, +, \cdot, 0, 1)$  הכוללת רשימה ארוכה של דרישות. בעזרת ההגדרות שראינו נוכל לקצר אותה. נסמן  $F^* = F \setminus \{0\}$ . נאמר כי  $F$  הוא שדה אם  $(F, +, 0)$  היא חבורה חילופית,  $(F^*, \cdot, 1)$  היא חבורה חילופית וקיום חוק הפילוג (distributive law), לכל  $a, b, c \in F$  מתקיים  $a(b + c) = ab + ac$ .

**תרגיל 2.24.** האם קיים מונואיד שיש בו איבר הפיך מימין שאינו הפיך משמאל?

פתרון. כן. נבנה מונואיד כזה. תהא  $X$  קבוצה. נסתכל על קבוצת ההעתקות מ- $X$  לעצמה המסומנת  $X^X = \{f : X \rightarrow X\}$ . ביחס לפעולת ההרכבה זהו מונואיד, ואיבר היחידה בו הוא העתקת הזהות.

ההפיכים משמאל הם הפונקציות החח"ע. ההפיכים מימין הם הפונקציות על (להזכיר את הטענות הרלוונטיות מבדידה). מה יקרה אם נבחר את  $X$  להיות סופית? (לעתיד: לחבורה  $(X^X, \circ)$  קוראים חבורת הסימטריה על  $X$  ומסמנים  $S_X$ . אם  $X = \{1, \dots, n\}$  מקובל לסמן את חבורת הסימטריה שלה בסימון  $S_n$ , ולכן כל איבר הפיך משמאל. עבור  $n \geq 3$  זו חבורה לא אבלית.)

אם ניקח למשל  $X = \mathbb{N}$  קל למצוא פונקציה על שאינה חח"ע. הפונקציה שנבחר היא  $d(n) = \max(1, n - 1)$ . לפונקציה זו יש הופכי מימין, למשל  $u(n) = n + 1$ , אבל אין לה הפיך משמאל.



צורת רישום 2.25. יהי  $n$  מספר טבעי. נסמן את הכפולות שלו ב- $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$ . למשל  $4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$ .

**דוגמה 2.26.** נסתכל על אוסף מחלקות השקילות מודולו  $n$ ,  $\mathbb{Z}_n = \{[a] : a \in \mathbb{Z}\}$ . כזכור חיבור וכפל מודולו  $n$  מוגדר היטב. למשל  $[a] + [b] = [a + b]$  כאשר באגף שמאל הסימן  $+$  הוא פעולה בינארית הפועלת על אוסף מחלקות השקילות ( $a$  הוא נציג של מחלקת שקילות אחת ו- $b$  הוא נציג של מחלקת שקילות אחרת) ובאגף ימין זו פעולת החיבור הרגילה של מספרים (שלאחריה מסתכלים על מחלקת השקילות שבה  $a + b$  נמצא).

אפשר לראות כי  $(\mathbb{Z}_n, +)$  היא חבורה אבלית. נבחר נציגים למחלקות השקילות  $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$ . איבר היחידה הוא  $[0]$  (הרי  $[0] + [a] = [0 + a] = [a]$ ) לכל  $[a]$ ). קיבוציות הפעולה והאבליות נובעת מקיבוציות והאבליות של פעולת החיבור הרגילה. האיבר ההופכי של  $[a]$  הוא  $[n-a]$ .

מה ניתן לומר לגבי  $(\mathbb{Z}_n, \cdot)$ ? ישנה סגירות, ישנה קיבוציות וישנו איבר יחידה  $[1]$ . אך זו לא חבורה כי ל- $[0]$  אין הופכי. נסמן  $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{[0]\}$ . האם  $(\mathbb{Z}_n^*, \cdot)$  חבורה? לא בהכרח. למשל עבור  $\mathbb{Z}_6^*$  נקבל כי  $[0] = [6] = [0] = [3] \cdot [2]$ . לפי ההגדרה  $[0] \notin \mathbb{Z}_6^*$ , ולכן  $(\mathbb{Z}_n^*, \cdot)$  אינה סגורה (כלומר אפילו לא אגודה).

**דוגמה 2.27.** עדין ניתן להציל את המקרה של הכפל מודולו  $n$ . נגדיר את חבורת אוילר (Euler) להיות  $U_n = U(\mathbb{Z}_n)$  לגבי פעולת הכפל. נבנה את לוח הכפל של  $\mathbb{Z}_6$  (בהתעלם מ- $[0]$  שתמיד יתן במכפלה  $[0]$ ):

$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

האיברים ההפיכים הם אלו שמופיע עבורם 1 (הפעולה חילופית ולכן מספיק לבדוק רק עמודות או רק שורות). כלומר  $U_6 = \{[1], [5]\}$ . במקרה זה  $[5]$  הוא ההופכי של עצמו.

הערה 2.28. אם  $p$  הוא מספר ראשוני, אז  $U_p = \mathbb{Z}_p^*$  (למה?).

טענה 2.29 (הוכחה לבית). בדומה להערה האחרונה, נאפיין את האיברים ב- $U_n$ . יהי  $m \in \mathbb{Z}$  אז  $[m] \in U_n$  אם ורק אם  $(n, m) = 1$ . כלומר, ההפיכים במונואיד  $(\mathbb{Z}_n, \cdot)$  הם כל האיברים הזרים ל- $n$ .

**דוגמה 2.30.**  $U_{12} = \{1, 5, 7, 11\}$ .

**דוגמה 2.31.** לא קיים ל-5 הופכי כפלי ב- $\mathbb{Z}_{10}$ , שכן אחרת 5 היה זר ל-10 וזו סתירה.

### 3 תתי-חבורות, סדר של איבר וסדר של חבורה

טענה 3.1 (מההרצאה). יהי  $m \in \mathbb{Z}$  אז  $[m] \in U_n$  אם ורק אם  $(n, m) = 1$ . כלומר, ההפיכים במונואיד  $(\mathbb{Z}_n, \cdot)$  הם כל האיברים הזרים ל- $n$ .

## תתי-חבורות

**הגדרה 3.2.** תהי  $G$  חבורה. תת-קבוצה  $H \subseteq G$  היא תת-חבורה, אם היא מהווה חבורה ביחס לפעולה המושרית מ- $G$ .

**דוגמה 3.3.** לכל חבורה  $G$  יש שתי תתי-חבורות באופן מיידי:  $\{e\} \leq G$  (הנקראת תת-החבורה הטריוויאלית), ו- $G \leq G$ .

**דוגמה 3.4.** לכל  $n \in \mathbb{Z}$ ,  $n\mathbb{Z} \leq \mathbb{Z}$ . בהמשך נוכיח שאלו כל תתי-החבורות של  $\mathbb{Z}$ .

**דוגמה 3.5.** (בתרגיל.)  $m\mathbb{Z} \leq n\mathbb{Z}$  אם ורק אם  $n|m$ .

**דוגמה 3.6.**  $(\mathbb{Z}_n, +)$  אינה תת-חבורה של  $(\mathbb{Z}, +)$  - כי  $\mathbb{Z}_n$  אינה מוכלת ב- $\mathbb{Z}$ : האיברים ב- $\mathbb{Z}_n$  הם מחלקות שקילות, ואילו האיברים ב- $\mathbb{Z}$  הם מספרים.

**דוגמה 3.7.**  $U_n$  אינה תת-חבורה כפלית של  $(\mathbb{Z}_n, \cdot)$  - כי  $(\mathbb{Z}_n, \cdot)$  אינה חבורה.

**דוגמה 3.8.**  $(GL_n(\mathbb{R}), \cdot)$  אינה תת-חבורה של  $(M_n(\mathbb{R}), +)$  - כי הפעולות בהן שונות.

טענה 3.9 (קריטריון מקוצר לתת-חבורה - מההרצאה). תהי  $H \subseteq G$  תת-קבוצה. אזי  $H$  תת-חבורה של  $G$  אם ורק אם שני התנאים הבאים מתקיימים:

$$1. e \in H$$

$$2. \text{לכל } h_1, h_2 \in H \text{ גם } h_1 \cdot h_2^{-1} \in H$$

**תרגיל 3.10.** יהי  $F$  שדה. נגדיר

$$SL_n(F) = \{A \in GL_n(F) \mid \det A = 1\}$$

הוכיחו כי  $SL_n(F) \leq GL_n(F)$  היא תת-חבורה. קוראים לה החבורה הלינארית המיוחדת מדרגה  $n$ .

הוכחה. ניעזר בקריטריון המקוצר לתת-חבורה.

1. ברור כי  $I_n \in SL_n(F)$ , כי  $\det I_n = 1$ .

2. נניח  $A, B \in SL_n(F)$ . צ"ל  $AB^{-1} \in SL_n(F)$ . אכן,

$$\det(AB^{-1}) = \det A \det B^{-1} = \frac{\det A}{\det B} = \frac{1}{1} = 1$$

ולכן  $AB^{-1} \in SL_n(F)$ .

לפי הקריטריון המקוצר,  $SL_n(F)$  היא תת-חבורה של  $GL_n(F)$ .

□

### סדר של איבר וסדר של חבורה

**הגדרה 3.11.** תהי  $G$  חבורה. נגדיר את הסדר (order) של  $G$  להיות עוצמתה כקבוצה. במילים יותר גשמיות, כמה איברים יש בחבורה. סימונים מקובלים:  $|G|$  או  $\text{Ord}(G)$ .

**צורת רישוס 3.12.** בחבורה כפלית נסמן את החזקה החיובית  $a^n = aa \dots a$  לכפל  $n$  פעמים. בחבורה חיבורית נסמן  $na = a + \dots + a$ . חזקות שליליות הן חזקות חיוביות של ההופכי של  $a$ . מוסכם כי  $a^0 = e$ .

**הגדרה 3.13.** תהי  $(G, \cdot, e)$  חבורה ויהא איבר  $g \in G$ . הסדר של איבר הוא המספר הטבעי  $n$  הקטן ביותר כך שמתקיים  $g^n = e$ . אם אין  $n$  כזה, אומרים שהסדר של  $g$  הוא אינסוף. בפרט, בכל חבורה הסדר של איבר היחידה הוא 1, וזהו האיבר היחיד מסדר 1. סימון מקובל  $o(g) = n$  ולפעמים  $|g|$ .

**דוגמה 3.14.** בחבורה  $(\mathbb{Z}_6, +)$ ,  $o(2) = 3$ ,  $o(4) = 3$ ,  $o(3) = 2$ ,  $o(5) = 6$ ,  $o(1) = 6$ .

**דוגמה 3.15.** נסתכל על החבורה  $(U_{10}, \cdot)$ . נזכור כי  $U_{10} = \{1, 3, 7, 9\}$  (כי אלו המספרים הזרים ל-10 וקטנים ממנו). נחשב את  $o(7)$ :

$$\begin{aligned} 7^2 &= 49 \equiv 9 \pmod{10} \\ 7^3 &= 7 \cdot 7^2 \equiv 7 \cdot 9 = 63 \equiv 3 \pmod{10} \\ 7^4 &= 7 \cdot 7^3 = 7 \cdot 3 = 21 \equiv 1 \pmod{10} \end{aligned}$$

ולכן  $o(7) = 4$ .

**דוגמה 3.16.** נסתכל על  $(GL_2(\mathbb{R}), \cdot)$  - חבורת המטריצות ההפיכות מגודל  $2 \times 2$  מעל  $\mathbb{R}$ . נחשב את הסדר של  $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ :

$$\begin{aligned} b^2 &= \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \neq I \\ b^3 &= b \cdot b^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \end{aligned}$$

לכן  $o(b) = 3$ .

**תרגיל 3.17.** תהי  $G$  חבורה. הוכיחו שלכל  $a \in G$ ,  $o(a) = o(a^{-1})$ .

הוכחה. נחלק לשני מקרים:

עקרה 1. נניח  $o(a) = n < \infty$ . לכן  $a^n = e$ . ראשית,

$$e = e^n = (a^{-1}a)^n = (a^{-1})^n a^n = (a^{-1})^n e = (a^{-1})^n$$

כאשר המעבר  $*$  מבוסס על כך ש- $a^{-1}$  מתחלפים (באופן כללי,  $(ab)^n \neq a^n b^n$ ).

הוכחנו ש- $(a^{-1})^n = e$ , ולכן  $o(a^{-1}) \leq n = o(a)$ .

כעת, צריך להוכיח את אי-השוויון השני. אם נחליף את  $a$  ב- $a^{-1}$ , נקבל

$$o(a) = o\left((a^{-1})^{-1}\right) < o(a^{-1})$$

מקרה 2. נניח  $o(a) = \infty$ , ונניח בשלילה  $o(a^{-1}) < \infty$ . לפי המקרה הראשון,  $o(a^{-1}) < \infty$  וקיבלנו סתירה. לכן  $o(a^{-1}) < \infty$ .

□

**הגדרה 3.18.** תהי  $G$  חבורה, ויהי  $a \in G$ . תת-החבורה הנוצרת על ידי  $a$  היא תת-החבורה

$$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$$

**דוגמה 3.19.** עבור  $n \in \mathbb{Z}$ ,  $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\} = \langle n \rangle$ .

**הגדרה 3.20.** תהי  $G$  חבורה ויהי איבר  $a \in G$ . אם  $G = \langle a \rangle$ , אזי נאמר כי  $G$  נוצרת על ידי  $a$  ונקרא ל- $G$  חבורה ציקלית (מעגלית).

**דוגמה 3.21.** החבורה  $(\mathbb{Z}, +)$  נוצרת על ידי 1, שכן כל מספר ניתן להצגה ככפולה (כחזקה) של 1. שימו לב כי יוצר של חבורה ציקלית לא חייב להיות יחיד, למשל גם  $-1$  יוצר את  $\mathbb{Z}$  החיבורית.

**דוגמה 3.22.** החבורה  $(\mathbb{Z}_n, +) = \langle 1 \rangle$  היא ציקלית. וודאו כי בחבורה  $(\mathbb{Z}_2, +)$  יש רק יוצר אחד (נניח על ידי טבלת כפל). וודאו כי בחבורה  $(\mathbb{Z}_{10}, +)$  יש ארבעה יוצרים. שניים די ברורים (1 וגם  $-1 \equiv 9$ ), האחרים (3, 7) דורשים לבינתיים בדיקה ידנית.

**הערה 3.23.** יהי  $a \in G$ . אזי  $o(a) = |\langle a \rangle|$ . במילים, הסדר של איבר הוא גודל תת-החבורה שהוא יוצר.

**סענה 3.24.** שימו לב כי הסדר של יוצר בחבורה ציקלית הוא סדר החבורה. כלומר אנחנו יודעים כי  $5 \in (\mathbb{Z}_{10}, +)$  אינו יוצר כי הסדר שלו הוא  $|\mathbb{Z}_{10}| = 10 < 2 = |5|$ , שהרי  $5 + 5 \equiv 0 \pmod{10}$ .

**סענה 3.25.** כל חבורה ציקלית היא אבלית.

הוכחה. תהי  $G$  חבורה ציקלית, ונניח כי  $G = \langle a \rangle$ . יהיו  $g_1, g_2 \in G$ . צ"ל  $g_1 g_2 = g_2 g_1$ . ציקלית, ולכן קיימים  $i, j$  שעבורם  $g_1 = a^i$  ו- $g_2 = a^j$ . מכאן שמתקיים

$$g_1 g_2 = a^i a^j = a^{i+j} = a^{j+i} = a_j a_i = g_2 g_1$$

□

**דוגמה 3.26.** לא כל חבורה אבלית היא ציקלית. למשל, נסתכל על  $U_8 = \{1, 3, 5, 7\}$  זו לא חבורה ציקלית, כי אין בחבורה הזו איבר מסדר 4 (כל האיברים שאינם 1 הם מסדר 2 - בדקו).

**דוגמה 3.27.** קבוצת שורשי היחידה מסדר  $n$  מעל  $\mathbb{C}$  היא

$$\Omega_n = \{z \in \mathbb{C} \mid z^n = 1\} = \left\{ \text{cis} \frac{2\pi k}{n} \mid k = 0, 1, \dots, n-1 \right\}$$

זו תת-חבורה של  $\mathbb{C}^*$ . יותר מכך: אם נסמן  $\omega_n = \text{cis} \frac{2\pi}{n}$ , נקבל  $\Omega_n = \langle \omega_n \rangle$ , כלומר  $\Omega_n$  היא חבורה ציקלית.

טענה 3.28. הוכיחו: אם  $G$  ציקלית, אז כל תת-חבורה של  $G$  היא ציקלית.

הוכחה. תהי  $H \leq G$  תת-חבורה. נסמן  $G = \langle a \rangle$ . כל האיברים ב- $G$  הם מהצורה  $a^i$ , ולכן גם כל האיברים ב- $H$  הם מהצורה הזו.  
יהי  $s \in \mathbb{N}$  המספר המינימלי שעבורו  $a^s \in H$ . נרצה להוכיח  $H = \langle a^s \rangle$ . אכן, יהי  $k \in \mathbb{N}$  שעבורו  $a^k \in H$ . לפי משפט החילוק עם שארית, קיימים  $q$  ו- $r$  שעבורם  $0 \leq r < s, k = qs + r$ , לכן,

$$a^k = a^{qs+r} = a^{qs} \cdot a^r = (a^s)^q \cdot a^r$$

במילים אחרות,  $a^r = a^k \cdot (a^s)^{-q}$ . אבל  $a^s, a^k \in H$  ולכן גם  $a^r \in H$  (סגירות לכפל ולהופכי).

אם  $r \neq 0$ , קיבלנו סתירה למינימליות של  $s$  - כי  $a^r \in H$  וגם  $0 < r < s$  (לפי בחירת  $r$ ). לכן,  $r = 0$ . כלומר,  $k = qs$ , ומכאן  $s|k$ . לכן  $a^k \in \langle a^s \rangle$ , כדרוש.  $\square$

**מסקנה 3.29.** תתי-החבורות של  $(\mathbb{Z}, +)$  הן בדיוק  $(n\mathbb{Z}, +)$  עבור  $n \in \mathbb{N} \cup \{0\}$ .

טענה 3.30 (מההרצאה). תהי  $G$  חבורה, ויהי  $a \in G$ . אם  $a^n = e$ , אזי  $o(a) | n$ .

**תרגיל 3.31.** תהי  $G$  חבורה, ויהי  $a \in G$ . נניח  $o(a) = n < \infty$ . הוכיחו שלכל  $d \leq n$ , טבעי,

$$o(a^d) = \frac{n}{(d, n)} = \frac{o(a)}{(d, o(a))}$$

הוכחה. היתכנות: נשים לב כי

$$(a^d)^{\frac{n}{(d, n)}} = (a^n)^{\frac{d}{(d, n)}} = e$$

(הפעולות שעשינו חוקיות, כי  $\frac{d}{(d, n)} \in \mathbb{Z}$ ).

מינימליות: נניח  $(a^d)^t = e$ , כלומר  $a^{dt} = e$ . לפי טענה 3.30,  $n | dt$ . לכן, גם  $\frac{n}{(d, n)} \mid \frac{dt}{(d, n)}$  (שניהם מספרים שלמים - מדוע?). מצד שני,  $\left(\frac{n}{(d, n)}, \frac{d}{(d, n)}\right) = 1$ .

לפי תרגיל שהוכחנו בתרגול הראשון,  $\frac{n}{(d, n)} \mid t$ , כמו שרצינו.  $\square$

**תרגיל 3.32** (אם יש זמן). נגדיר  $\Omega_\infty = \bigcup_{n=1}^{\infty} \Omega_n$ . הוכיחו:

1.  $\Omega_\infty$  היא תת-חבורה של  $\mathbb{C}^*$ .

2. לכל  $x \in \Omega_\infty, o(x) < \infty$  (כלומר: כל איבר ב- $\Omega_\infty$  הוא מסדר סופי).

3.  $\Omega_\infty$  אינה ציקלית.

לחבורה כזו, שבה כל איבר הוא מסדר סופי, קוראים חבורה מפותלת.

פתרון.

1. ניעזר בקריטריון המקוצר. יהיו  $g_1, g_2 \in \Omega_\infty$ . לכן קיימים  $m, n$  שעבורם  $g_1 \in \Omega_m, \Omega_n$ . נכתוב

$$g_1 = \text{cis} \frac{2\pi k}{m}, \quad g_2 = \text{cis} \frac{2\pi \ell}{n}$$

לכן

$$\begin{aligned} g_1 g_2^{-1} &= \text{cis} \frac{2\pi k}{m} \left( \text{cis} \frac{2\pi \ell}{n} \right)^{-1} = \text{cis} \frac{2\pi k}{m} \text{cis} \left( -\frac{2\pi \ell}{n} \right) = \text{cis} \left( \frac{2\pi k}{m} - \frac{2\pi \ell}{n} \right) = \\ &= \text{cis} \left( \frac{2\pi (kn - \ell m)}{mn} \right) \in \Omega_{mn} \subseteq \Omega_\infty \end{aligned}$$

2. לכל  $x \in \Omega_\infty$  קיים  $n$  שעבורו  $x \in \Omega_n$ ; לכן,  $o(x) \leq n$ .

3. נניח בשלילה  $\Omega_\infty = \langle a \rangle$ ; לכן בהכרח  $|\Omega_\infty| = \aleph_0$ . אבל זה סותר את תוצאת סעיף ב'.

**תרגיל 3.33** (אם יש זמן). תהי  $G$  חבורה ציקלית מסדר  $n$ . כמה איברים ב- $G$  יוצרים את  $G$ ?

פתרון. נניח כי  $G = \langle a \rangle$ . אזי

$$G = \langle a^k \rangle \iff o(a^k) = n \iff \frac{n}{(k, n)} = n \iff (k, n) = 1$$

לכן, מספר האיברים היוצרים את  $G$  הוא  $|U_n|$ .