

# תורת החבורות 88-218-01 תשפ"א

## הערות הרצאה 1

שלום!

אימייל: [mathzeta2@gmail.com](mailto:mathzeta2@gmail.com)

הערה 0.1. הסיכומים האלו הוקלדו במהלך ההרצאות. אין לראות בהם אלא טיוטה. בפרט, הם בטוח מכילים טעויות. הם גם לא כוללים את כל מה שנאמר במהלך ההרצאות, ולא מכסים את כל האתרים השונים שבהם נעזרנו להדגמות וחישובים. נשמח לשמוע על תיקונים ושיפורים.

**שאלה 0.2.** למה מתמטיקאים חוקרים מבנים אלגבריים?

- מעניין
- יפה
- שימושי
- חסכוני
- פיזיקה
- כימיה
- מדעי המחשב והנדסה
- היסטוריה - גלואה

### 0.1 הגדרות בסיסיות

סימונים

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

ואם צריך גם נסמן  $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$ .

**הגדרה 0.3.** תהי  $S$  קבוצה. פעולה בינארית על  $S$  היא פונקציה

$$*: S \times S \rightarrow S$$

ולרוב במקום לסמן  $*(a, b)$  להפעלה של הפעולה על  $a, b \in S$  נכתוב  $a * b$ . קבוצה עם פעולה בינארית עליה  $(S, *)$  נקראת מאגמה.

**דוגמה 0.4.** אתם כבר מכירים המון מאגמות:

•  $(\mathbb{R}, +)$

•  $(\mathbb{Z}, -)$

•  $(\mathbb{Z}, \cdot)$

•  $(\mathbb{Z}, *)$  כאשר  $x * y = 3x - y$  לכל  $x, y \in \mathbb{Z}$ .

•  $(\mathbb{R}^{3 \times 3}, \mu)$  כאשר  $\mu$  זו הפעולה של כפל מטריצות.

•  $(A^*, \cdot)$  כאשר  $A^*$  היא קבוצת כל המילים באותיות מהאלפבית  $A$  והפעולה היא שרשור של מילים.

**שאלה 0.5.** האם  $(\mathbb{N}, -)$  או  $(\mathbb{R}, :)$  הן מאגמות?

פתרון. לא! הרי  $3 - 5 = -2 \notin \mathbb{N}$ , ובאופן דומה אי אפשר לחלק באפס.

**הגדרה 0.6.** תהי  $(S, *)$  מאגמה. נאמר כי זו אגודה אם הפעולה היא קיבוצית (אסוציאטיבית). כלומר מתקיים

$$\forall a, b, c \in S : (a * b) * c = a * (b * c)$$

**דוגמה 0.7.** המאגמה  $(\mathbb{R}, +)$  היא אגודה, כי חיבור של מספרים ממשיים הוא קיבוצי. לעומת זאת  $(\mathbb{Z}, -)$  אינה אגודה, כי למשל

$$(3 - 2) - 1 = 0 \neq 2 = 3 - (2 - 1)$$

**הגדרה 0.8.** תהי  $(S, *)$  אגודה. נאמר שאיבר  $c \in S$  הוא יחידה ימנית אם לכל  $x \in S$  מתקיים  $x * c = x$ , ובאופן דומה נאמר כי איבר  $d \in S$  הוא יחידה שמאלית אם לכל  $x \in S$  מתקיים  $d * x = x$ .

נאמר שאיבר  $e \in S$  הוא איבר יחידה אם הוא יחידה מימין ומשמאל.

**דוגמה 0.9.** נתבונן במאגמה  $(\mathbb{Z}, R)$  כאשר  $R(a, b) = b$ . אפשר להוכיח שמדובר באגודה.

$$\forall a, b, c \in S : R(a, R(b, c)) = c = R(R(a, b), c)$$

כל איבר באגודה הזו הוא יחידה שמאלית. אבל אין בה אפילו יחידה ימנית אחת!

**דוגמה 0.10.** באגודה  $(\mathbb{R}, +)$  קיים איבר יחידה והוא 0 ואילו באגודה  $(\mathbb{R}, \cdot)$  איבר היחידה הוא 1. שימו לב שמדובר באותה קבוצה, אבל הפעולות הן שונות, ואפילו איברי היחידה הם שונים.

טענה 0.11. אם באגודה  $(S, *)$  יש יחידה ימנית  $c$  ויחידה שמאלית  $d$ , אז  $c = d$ . הוכחה. נסתכל על הביטוי

$$c = d * c = d$$

□

וסיימו

**מסקנה 0.12.** באגודה, אם קיים איבר יחידה, אז הוא יחיד.

**הגדרה 0.13.** אגודה  $(S, *)$  שקיים בה איבר יחידה  $e \in S$  נקראת מונואיד. במקום לרשום כי  $(S, *, e)$  הוא מונואיד נרשום כי  $S$  הוא מונואיד כשהקשר ברור.

**הגדרה 0.14.** יהי  $(M, *, e)$  מונואיד. איבר  $a \in M$  יקרא הפיך משמאל, אם קיים איבר  $b \in M$  כך ש- $b * a = e$ . באופן דומה  $a$  הפיך מימין אם קיים איבר  $c \in M$  כך ש- $a * c = e$ .

נאמר כי  $a$  הפיך אם הוא הפיך מימין ומשמאל.

**דוגמה 0.15.** במונואיד  $(\mathbb{Q}, +, 0)$  כל איבר הוא הפיך. לכל  $x \in \mathbb{Q}$  מתקיים כי  $-x$  הוא הופכי מימין ומשמאל של  $x$ . במונואיד  $(\mathbb{Q}, \cdot, 1)$  כל איבר ששונה מ-0 הוא הפיך.

טענה 0.16. יהי  $a \in M$  איבר הפיך משמאל ומימין. אזי  $a$  הפיך וההופכי שלו הוא יחיד. פתרון. יהי  $b$  הופכי שמאלי של  $a$  ויהי  $c$  הופכי ימני של  $a$ . נראה כי  $b = c$ .

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

לכן כל ההופכיים משמאל של  $a$  שווים לכל ההופכיים מימין של  $a$ . מכאן שההופכי של  $a$  הוא יחיד, ונוכל לתת לו סימון משל עצמו,  $a^{-1}$ .

$$a * a^{-1} = a^{-1} * a = e$$

הערה 0.17. יש מונואידים שבהם יש לאיבר יותר מהופכי שמאלי אחד, או יותר מהופכי ימני אחד. לפעמים אפילו אינסוף.

**הגדרה 0.18.** פונקציה  $f: X \rightarrow Y$  היא על אם לכל איבר  $y \in Y$  קיים  $x \in X$  כך ש- $f(x) = y$ . כלומר שלכל  $y \in Y$  קיימת תמונה קדומה ב- $X$ .

פונקציה  $f: X \rightarrow Y$  היא חח"ע אם לכל  $x_1, x_2 \in X$  התנאי  $f(x_1) = f(x_2)$  גורר ש- $x_1 = x_2$ .

**דוגמה 0.19.** תהי  $X$  קבוצה. נסמן ב- $X^X$  את אוסף הפונקציות מ- $X$  ל- $X$ .

$$|A^B| = |A|^{|B|}$$

הקבוצה  $X^X$  לגבי פעולת ההרכבה  $\circ$  של פונקציות היא מונואיד. איבר היחידה ב- $(X^X, \circ)$  הוא  $\text{id}_X$  פונקצית הזהות. מתי  $f \in X^X$  היא הפיכה משמאל? כלומר מתי קיימת  $g \in X^X$  כך ש- $g \circ f = \text{id}_X$ . תרגיל לבית: אם ורק אם  $f$  חח"ע. באופן דומה  $f \in X^X$  היא הפיכה מימין אם ורק אם  $f$  היא על. כלומר קיימת פונקציה  $g \in X^X$  ש- $f \circ g = \text{id}_X$ .

$$(f \circ g)(x) := f(g(x))$$

נציין שאם  $X$  היא סופית, אז  $f \in X^X$  היא חח"ע אם ורק אם  $f$  על. אם  $X$  היא אינסופית, אז ישנן פונקציות שהן הפיכות רק מצד אחד. דוגמה אחת: אם  $X = \mathbb{N}$ , אז לפונקציה  $f(x) = x + 1$  יש רק הופכיים משמאל (יש אינסוף כאלו). לעומת זאת לפונקציה  $f(x) = \lfloor \frac{x}{2} \rfloor$  יש הופכי רק מימין (ויש אינסוף כאלו).

**הגדרה 0.20.** מונואיד  $(G, *, e)$  שבו כל איבר הוא הפיך נקרא חבורה.

לפי ההגדרות לעיל, מה צריך כדי להוכיח שקבוצה עם פעולה בינארית היא חבורה?

• (סעיף 0) סגירות הפעולה (ואז  $G$  מאגמה)

1. קיבוציות הפעולה (ואז  $G$  אגודה)

2. קיום איבר יחידה (ואז  $G$  מונואיד)

3. כל איבר הוא הפיך (ואז  $G$  חבורה)

**דוגמה 0.21.** לגבי פעולה החיבור

$$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$$

מדובר בחבורות שאיבר היחידה בהן הוא 0.

**דוגמה 0.22.** יהי  $(F, +, \cdot, 0_F, 1_F)$  שדה (כמו  $\mathbb{R}$  או  $\mathbb{F}_2 = \{0, 1\}$ ). אז

$$(F, +, 0_F)$$

היא חבורה הנקראת החבורה החיבורית של השדה.

אילו  $(F, \cdot, 1_F)$  הוא רק מונואיד כי  $0_F$  אינו הפיך. נסמן  $F^* = F \setminus \{0_F\}$ . אז  $(F^*, \cdot, 1_F)$  היא כן חבורה הנקראת החבורה הכפלית של השדה.

**דוגמה 0.23.** קבוצה עם איבר אחד ופעולה בינארית סגורה היא חבורה. לחבורה הזו קוראים החבורה הטריטויאלית.

**תרגיל 0.24.** נתבונן בקבוצה  $\mathbb{Q} \cup \{\infty\}$  כאשר  $\infty$  הוא איבר חדש. נגדיר על הקבוצה הזו פעולה שלגבי שני מספרים רציונליים היא זהה לכפל של מספרים, ואילו

$$\infty \cdot 0 = 1 = 0 \cdot \infty$$

ולכל  $x \neq 0$  נגדיר  $\infty \cdot x = \infty = x \cdot \infty$ . הוכיחו שכל האקסיומות של חבורה פרט לקיבוציות מתקיימות למאגמה  $(\mathbb{Q} \cup \{\infty\}, \cdot)$ .

**הגדרה 0.25.** יהי  $M$  מונואיד. נסמן את אוסף האיברים ההפיכים במונואיד  $U(M)$ .

טענה 0.26. יהי  $M$  מונואיד. הקבוצה  $U(M)$  לגבי אותה פעולה היא חבורה. היא נקראת חבורת ההפיכים של  $M$ .

הוכחה. הסברנו כי  $e \in U(M)$ , כי הוא ההופכי של עצמו. לכל  $a, b \in U(M)$  צריך להראות סגירות, כלומר  $a \cdot b \in U(M)$ . נוכיח כי

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

(ההאיברים  $a^{-1}$  ו- $b^{-1}$  קיימים כי  $a, b$  הם הפיכים). אכן,

$$b^{-1} \cdot a^{-1} \cdot a \cdot b = b^{-1} \cdot e \cdot b = b^{-1} \cdot b = e$$

$$a \cdot b \cdot b^{-1} \cdot a^{-1} = \dots = e$$

ולכן  $a \cdot b$  הוא הפיך משמאל ומימין. בנוסף כל איבר ב- $U(M)$  הוא הפיך, והפעולה היא קיבוצית כי הפעולה ב- $M$  היא קיבוצית, ולכן  $U(M)$  חבורה.  $\square$

הערה 0.27. מתקיים  $U(M) = M$  אם ורק אם  $M$  חבורה.

**דוגמה 0.28.** יהי  $F$  שדה. אז אמרנו כי  $(F, \cdot)$  אינו חבורה, אבל

$$U(F, \cdot) = F^*$$

שימו לב כי  $U(\mathbb{Z}, +) = (\mathbb{Z}, +)$  ואילו  $U(\mathbb{Z}, \cdot) = \{1, -1\}$ .

**דוגמה 0.29.** עבור קבוצה סופית אחת הדרכים להגדיר פעולה בינארית היא בעזרת לוח כפל. למשל, אם  $S = \{a, b\}$  ונגדיר

*	a	b
a	a	b
b	b	a

אז קל לראות שמתקיימת סגירות, קיבוציות,  $a$  הוא יחידה ו- $b$  הוא ההופכי של עצמו. למעשה, זוהי החבורה "היחידה" מסדר 2. האם אתם יכולים להוכיח זאת? למשל טבלת הכפל של  $U(\mathbb{Z}, \cdot)$  היא

·	1	-1
1	1	-1
-1	-1	1

**דוגמה 0.30.** נסמן ב- $M_n(\mathbb{R})$  את אוסף המטריצות הממשיות בגודל  $n \times n$ . למשל

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix} \in M_2(\mathbb{R})$$

לגבי פעולת חיבור מטריצות  $(M_n(\mathbb{R}), +)$  היא חבורה. מה לגבי  $(M_n(\mathbb{R}), \cdot)$  כפל מטריצות? יש סגירות, יש קיבוציות

$$(AB)C = A(BC)$$

קיים איבר יחידה (מטריצת הזהות  $I_n$ ), אבל לא כל איבר הוא הפיך. למעשה מגדירים חבורה חשובה מאוד בעזרת המונואיד  $(M_n(\mathbb{R}), \cdot)$ :

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

החבורה הלינארית הכללית מעל  $\mathbb{R}$  (מדרגה  $n$ ).

**אתגר** נסמן ב- $M_{\mathbb{N}}^{\circ}(F)$  את אוסף כל המטריצות האינסופיות שבכל שורה ועמודה שלהן יש רק מספר סופי של איברים שאינם 0. הוכיחו כי כפל מטריצות מוגדר כאן היטב, וכי  $(M_{\mathbb{N}}^{\circ}(F), \cdot)$  הוא מונואיד שאינו חבורה, ושיש בו איברים שהפיכים רק מצד אחד.

**הגדרה 0.31.** יהיו  $a, b \in S$  איברים במאגמה. נאמר כי  $a, b$  מתחלפים אם  $a * b = b * a$ .

**הגדרה 0.32.** נאמר שפעולה  $*: S \times S \rightarrow S$  היא חילופית אם כל זוג איברים ב- $S$  מתחלף. כאשר הפעולה חילופית נאמר על אגודה או מונואיד שהם חילופיים. לחבורה  $(G, *)$  עם פעולה חילופית קוראים חבורה אבליית.

**דוגמה 0.33.** החבורות  $(\mathbb{C}, +)$ ,  $(\mathbb{Z}, +)$  הן אבלייות, ואילו  $GL_5(\mathbb{R})$  אינה אבליית. החבורה הטריטוריאליית היא אבליית.

**דוגמה 0.34.** יהי  $V$  מרחב וקטורי. אז  $V$  יחד עם הפעולה של חיבור וקטורים הוא חבורה אבליית. איבר היחידה וקטור האפס.

**דוגמה 0.35.** תהי  $X$  קבוצה. ראינו כי  $(X^X, \circ)$  הוא מונואיד, ושהאיברים ההפיכים בו הן הפונקציות שהן חח"ע ועל. חבורת האיברים ההפיכים של המונואיד הזה יש שם מיוחד

$$S_X := U(X^X, \circ)$$

והיא נקראת החבורה הסימטרית על  $X$ .

אם במקרה  $X = \{1, \dots, n\}$ , נסמן  $S_n$  במקום  $S_{\{1, \dots, n\}}$ . כל איבר  $\sigma \in S_X$  של החבורה הסימטרית נקרא תמורה על  $X$ . למשל  $\sigma \in S_3$  היא פונקציה  $\sigma: \{1, 2, 3\} \rightarrow \{1, 2, 3\}$  שהיא חח"ע ועל. כלומר  $\sigma(1) = i, \sigma(2) = j, \sigma(3) = k$  כאשר  $\{i, j, k\} = \{1, 2, 3\}$ .

עבור  $n > 2$  החבורה  $S_n$  אינה אבליית.

**הגדרה 0.36.** יהי  $(G, *, e)$  איבר בחבורה, ויהי  $n$  מספר טבעי. אז החזקה ה- $n$  של  $a$  היא האיבר

$$a^n := \underbrace{a * a * \cdots * a}_n$$

ואם הפעולה של  $G$  מסומנת ב- $+$ , אז מקובל לסמן את החזקה בתור  $n \cdot a = a + \cdots + a$ .  
אז כדי להשלים את ההגדרה לכל חזקה שלמה, נגדיר  $a^0 = e$  וגם  $a^{-n} = (a^{-1})^n$ .

טענה 0.37. תכונות:

1. מתקיים  $(a * b)^{-1} = b^{-1} * a^{-1}$ .

2. מתקיים

$$(a_1 * a_2 * \cdots * a_{n-1} * a_n)^{-1} = a_n^{-1} * a_{n-1}^{-1} * \cdots * a_2^{-1} * a_1^{-1}$$

לפי אינדוקציה על הסעיף הקודם.

3. בפרט, לפי הסעיף הקודם  $(a^n)^{-1} = a^{-n}$  לכל  $n \in \mathbb{Z}$ .

4. לכל  $n, m \in \mathbb{Z}$  מתקיים  $a^n * a^m = a^{n+m}$ . איך מוכיחים דבר כזה? נניח  $n, m \in \mathbb{N}$  אז

$$a^n * a^m = \underbrace{a * a * \cdots * a}_n * \underbrace{a * a * \cdots * a}_m = \underbrace{a * a * \cdots * a}_{n+m} = a^{n+m}$$

אם  $n, m$  שניהם שליליים, אז נקבל את אותו דבר עבור  $a^{-1}$ . אם אחד מהם שלילי והשני חיובי, ובה"כ (בלי הגבלת הכלליות) נניח  $n \geq -m$ , נרשום

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

ואז נקבל

$$a^n * a^m = (a^{n+m} * a^{-m}) * a^m = a^{n+m} * (a^{-m} * a^m) = a^{n+m} * e = a^{n+m}$$

כאשר בשיויון לפני האחרון  $(a^m)^{-1} = a^{-m}$ .

5. לכל  $n, m \in \mathbb{Z}$  מתקיים  $(a^n)^m = a^{n \cdot m}$ . מוכיחים באינדוקציה (קצת יותר מסובכת) כמו בסעיף הקודם.

6. חזקות של אותו איבר, מתחלפות. כלומר  $a^n * a^m = a^m * a^n$  לכל  $n, m \in \mathbb{Z}$ .

הערה 0.38. כאשר אנחנו לא בחבורה אבלית, אז חזקות של האיבר  $ab$  הן לא בהכרח המכפלה של החזקות של  $a$  ושל  $b$ ! למעשה תוכיחו (בתרגול או בתרגיל הבית) כי  $(ab)^2 = a^2 b^2$  אם ורק אם  $a, b$  מתחלפים.

## 0.2 תת־חבורות

**הגדרה 0.39.** תהי  $G$  חבורה. תת־קבוצה  $H \subseteq G$  תקרא תת־חבורה של  $G$  אם  $H$  היא בעצמה חבורה לגבי הפעולה המצומצמת מ- $G$ . נסמן  $H \leq G$ .

**דוגמה 0.40.**  $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$  שרשרת של תת־חבורות לגבי פעולת החיבור.

**דוגמה 0.41.** כל תת־מרחב וקטורי הוא תת־חבורה לגבי הפעולה של חיבור וקטורים. ראו גם [Flip](#) מאת סימון טאת'ם.

**דוגמה 0.42.** תהי  $G$  חבורה. אז יש לה תת־חבורות שתמיד קיימות:  $G \leq G$  וגם  $\{e\} \leq G$  הנקראת תת־החבורה הטריוויאלית של  $G$ .

**שאלה 0.43.** אילו תכונות צריך לדרוש מתת־קבוצה  $H \subseteq G$  כדי שהיא תהיה ת"ח (תת־חבורה)?

פתרון. קיבוציות לא צריך לבדוק. הרי  $(a * b) * c = a * (b * c)$  מתקיים לכל שלשת איברים  $a, b, c \in G$ , אז בפרט זה מתקיים לאיברים של  $H$ . סגירות כן צריך לבדוק, כי ייתכן ש- $a, b \in H$ , אבל  $a * b \notin H$ . יחידה כן צריך לבדוק. נשים לב שהיחידה של  $H$  (אם היא ת"ח) חייבת להיות היחידה של  $G$ . הרי אם יש איבר  $e_H \in H$  שהוא איבר יחידה של  $H$ , אז הוא מקיים  $e_H * h = h$  לכל  $h \in H$ . מפני ש- $e_H, h \in G$  הם בעצמם איברים של  $G$ , נוכל לכפול מצד ימין ב- $h^{-1} \in G$  (ההופכי של  $h$  ב- $G$ ). נקבל

$$\begin{aligned} e_H * h &= h \\ e_H * h * h^{-1} &= h * h^{-1} \\ e_H &= e_H * e_G = e_G \end{aligned}$$

כאשר  $e_G$  הוא איבר היחידה של  $G$ . הופכי גם צריך לבדוק, וההופכי של איבר ב- $G$  נשאר אותו הופכי ב- $H$ . לסיכום: יש לבדוק  $e_G \in H$ , שיש סגירות לפעולה ויש סגירות להופכי.

**הגדרה 0.44.** תהי  $G$  חבורה. נגדיר את המֶרְכֶּז של  $G$  להיות

$$Z(G) = \{g \in G \mid \forall h \in G, gh = hg\}$$

כלומר זהו אוסף כל האיברים של  $G$  שמתחלפים עם כל האיברים של  $G$ .

הערה 0.45. מתקיים  $Z(G) = G$  אם ורק אם  $G$  אבלית.

**תרגיל 0.46.** לכל חבורה  $G$  מתקיים  $Z(G) \leq G$ .

פתרון. ברור כי  $e \in Z(G)$  כי מתקיים  $eh = he$  לכל  $h \in G$ . לכן  $Z(G) \neq \emptyset$  לכל חבורה.



עבור סגירות לפעולה, יהיו  $a, b \in Z(G)$ . צריך להוכיח  $ab \in Z(G)$ . איך מוכיחים דבר כזה? צריך להוכיח ש- $ab$  מתחלף עם כל איבר של  $G$ . לכל  $h \in G$  מתקיים

$$(ab)h = a(bh) = a(hb) = (ah)b = (ha)b = h(ab)$$

וקיבלנו כי  $ab$  מתחלף עם  $h$ .  
עבור סגירות להופכי צריך לבדוק שלכל  $a \in Z(G)$  מתקיים  $a^{-1} \in Z(G)$ : לכל  $h \in G$  נבדוק

$$\begin{aligned} ah &= ha & / \cdot a^{-1} \square a^{-1} \\ a^{-1}aha^{-1} &= a^{-1}haa^{-1} \\ eha^{-1} &= a^{-1}he \\ ha^{-1} &= a^{-1}h \end{aligned}$$

ולכן  $a^{-1}$  מתחלף עם  $h$ . בדרך אחרת

$$a^{-1}h = (h^{-1}a)^{-1} = (ah^{-1})^{-1} = ha^{-1}$$

ולכן  $Z(G) \leq G$  היא אכן תת-חבורה.

**תרגיל 0.47** (קצת קשה לבית). הוכיחו כי  $Z(GL_n(\mathbb{R}))$  היא אוסף המטריצות הסקלריות, כלומר מטריצות מן הצורה

$$\alpha I_n = \begin{pmatrix} \alpha & & \\ & \ddots & \\ & & \alpha \end{pmatrix}$$

כאשר  $\alpha \neq 0$ .

**תרגיל 0.48** (לבית). הוכיחו כי בחבורה  $G = GL_2(\mathbb{R})$  אוסף המטריצות

$$H = \left\{ \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\}$$

מהווה תת-חבורה.

**דוגמה 0.49**. יהי  $F$  שדה. אז  $(F^*, \cdot)$  אינה תת-חבורה של  $(F, +)$  כי הפעולות הן שונות. באופן דומה גם  $GL_n(F)$  אינה תת-חבורה של  $(M_n(F), +)$ .

**הגדרה 0.50**. תהי  $G$  חבורה ויהי  $a \in G$  חבורה. תת-החבורה הציקלית הנוצרת על ידי  $a$  היא

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

הערה 0.51. אפשר לראות כי  $\langle a \rangle$  היא אכן תת-חבורה לכל איבר  $a \in G$ . מתקיים  $a^0 = e \in \langle a \rangle$ . לכל  $a^k, a^t \in \langle a \rangle$  יש סגירות לפעולה:  $a^k \cdot a^t = a^{k+t} \in \langle a \rangle$  ויש סגירות להופכי:  $(a^k)^{-1} = a^{-k} \in \langle a \rangle$ .  
תת-החבורה  $\langle a \rangle$  היא תת-החבורה הקטנה ביותר של  $G$  המכילה את  $a$ . במילים אחרות, אם  $H \leq G$  וגם  $a \in H$ , אז  $\langle a \rangle \subseteq H$ .

**דוגמה 0.52.** נתבונן בחבורה  $\mathbb{Z}$ . יהי מספר שלם  $n \in \mathbb{Z}$ . אז אוסף הכפולות של  $n$ :

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$$

הוא שווה לתת-החבורה  $\langle n \rangle$ . בהמשך הקורס נראה שאלו הן כל תת-החבורות של  $\mathbb{Z}$ .