

מבוא לתורת החבורות
מערכי תרגול קורס 88-221

נובמבר 2016, גרסה 0.2

מבוא

נתחיל עם כמה דגשים:

- דף הקורס נמצא באתר www.math-wiki.com.
- שאלות בנוגע לחומר הלימודי מומלץ לשאול בדף השיחה באתר של הקורס.
- תרגילי בית כל שבוע עם חובת הגשה.
- יהיה בוחן. מתוכנן לתאריך 27.12.2016.

1 מבנים אלגבריים בסיסיים

1.1 הגדרה חבורה למחצה (semigroup) היא קבוצה לא ריקה S ומפעולה בינארית על S המקיימת קיבוציות (אסוציאטיביות, associativity). כלומר לכל $a, b, c \in S$ מתקיים $(a * b) * c = a * (b * c)$.

1.2 דוגמה \mathbb{Z} , מילים ושירשור מילים, קבוצה X עם הפעולה $a * b = b$.

1.3 דוגמה המערכת $(\mathbb{Z}, -)$ אינה חבורה למחצה, מפני שפעולת החיסור אינה קיבוצית. למשל $(5 - 2) - 1 \neq 5 - (2 - 1)$.

1.4 הגדרה תהי $(S, *)$ חבורה למחצה. איבר $e \in S$ נקרא איבר יחידה אם לכל $a \in S$ מתקיים $a * e = e * a = a$. חבורה למחצה שבה קיים איבר יחידה נקראת פונואיד (monoid, או יחידון).

1.5 דוגמה \mathbb{Z} , מטריצות ריבועיות מעל שדה, פונקציות על קבוצה X .

1.6 הערה. יהי M מונואיד. קל לראות כי איבר היחידה ב- M הוא יחיד.

1.7 דוגמה תהי X קבוצה כלשהי, ותהי $P(X)$ קבוצת החזקה שלה (זהו אוסף כל תתי הקבוצות של X). אזי $(P(X), \cap)$ היא מונואיד שבו איבר היחידה הוא X . מה קורה עבור $(P(X), \cup)$? (להמשך, נשים לב כי במונואיד זה לכל איבר a מתקיים $a^2 = a$).

1.8 הגדרה יהי $(M, *, e)$ מונואיד. איבר יקרא הפיך אם קיים איבר $b \in M$ כך ש- $ba = ab = e$. במקרה זה $a^{-1} = b$. יקרא הופכי של a .

1.9 תרגיל (אם יש זמן). אם $aba \in M$ הפיך במונואיד, הראו כי גם a, b הפיכים.

פתרון. יהי c ההופכי של aba . כלומר

$$abac = caba = e$$

לכן cab הוא הופכי שמאלי של a , ו- bac הופכי ימני של a . בפרט a הפיך ומתקיים גם $cab = bac$. לכן מתקיים גם

$$(aca)b = a(cab) = a(bac) = e = (cab)a = (bac)a = b(aca)$$

וניתן להסיק כי aca הופכי שמאלי וימני של b .

תרגיל 1.10. 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 (מהקורס מתמטיקה בדידה). מה יקרה אם נבחר את X להיות סופית?

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.

תרגיל 1.11 (ממבחן). הוכיחו כי לכל מונואיד (X, \cdot) הקבוצה $P_*(X)$ של כל תתי הקבוצות הלא ריקות של X מגדירה מונואיד ביחס לפעולת הכפל הטבעית:

$$A \bullet B = \{a \cdot b : a \in A, b \in B\}$$

ומצאו מי הם האיברים ההפיכים ב- $(P_*(X), \bullet)$.

פתרון. הקבוצה $P_*(X)$ אינה ריקה, לדוגמה היא מכילה את $\{e\}$ (כאשר e הוא איבר היחידה של X). הפעולה \bullet מוגדרת היטב וסגורה. קל לבדוק כי הפעולה קיבוצית בהתבסס על הקיבוציות של הפעולה ב- X . איבר היחידה ב- $(P_*(X), \bullet)$ הוא $\{e\}$.

האיברים ההפיכים במונואיד הן הקבוצות מהצורה $\{a\}$ עבור a הפיך ב- X (ההופכי הוא $\{a^{-1}\}$). אכן, נניח כי $A \in P_*(X)$ הפיך. לכן קיימת $B \in P_*(X)$ כך שלכל $a \in A, b \in B$ מתקיים $ab = e$. נראה כי $|B| = 1$. אחרת קיימים לפחות שני איברים $b_1, b_2 \in B$ ומתקיים $b_1 a = ab_1 = ab_2 = b_2 a = e$ ולכן מיחידות ההופכי של a נקבל $b_1 = b_2$. באופן סימטרי $|A| = 1$.

הגדרה 1.12. חבורה (group) $(G, *, e)$ היא מונואיד שבו כל איבר הוא הפיך.

מתקיים: חבורה \Leftarrow מונואיד \Leftarrow חבורה למחצה.

לפי ההגדרה לעיל על מנת להוכיח שמערכת אלגברית היא חבורה צריך להראות:

1. סגירות הפעולה.
2. קיבוציות הפעולה.
3. קיום איבר יחידה.
4. כל איבר הוא הפיך.

דוגמה 1.13. (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, אסוציאטיביות, a הוא יחידה ו- b הוא ההופכי של עצמו. למעשה, זוהי החבורה היחידה מגודל 2 (למה?).

דוגמה 1.14. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ חבורות ביחס לחיבור. מה קורה עם כפל? (כל שדה הוא חבורה חיבורית ומונואיד כפלי).

דוגמה 1.15. יהי n מספר טבעי. נסמן את הכפולות שלו ב- $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$. למשל $4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$. לכל n המערכת $(n\mathbb{Z}, +)$ היא חבורה.

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

1.17. טענה. שקילות מודולו n היא יחס שקילות שמחלקות השקילות שלו מתאימות לשארית החלוקה של מספר ב- n . כפל וחיבור מודולו n מוגדרים היטב. כלומר אם $a \equiv b, c \equiv d \pmod{n}$, אז $ac \equiv bd \pmod{n}$ וגם $a + c \equiv b + d \pmod{n}$.

דוגמה 1.18. נסתכל על אוסף מחלקות השקילות מודולו n , שמקובל לסמן $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{[a] : a \in \mathbb{Z}\}$. למשל $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$. לפעמים מסמנים את מחלקת השקילות $[a]$ בסימון \bar{a} , ולעיתים כאשר ברור ההקשר פשוט a . כזכור $[a] + [b] = [a + b]$ 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 $[0] + [a] = [0 + a] = [a]$ (הרי $[0]$ איבר היחידה הוא $[0]$). $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$ לכל $[a]$. קיבוציות הפעולה והאבליות נובעות מהקיבוציות 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 $\mathbb{Z}_n^\circ = \mathbb{Z}_n \setminus \{[0]\}$. האם $(\mathbb{Z}_n^\circ, \cdot)$ חבורה? לא בהכרח. למשל עבור \mathbb{Z}_6° נקבל כי $[2][3] = [6] = [0]$ לפי ההגדרה $\mathbb{Z}_6^\circ \ni [0]$, ולכן הפעולה ב- $(\mathbb{Z}_n^\circ, \cdot)$ אינה בהכרח סגורה (כלומר אפילו לא חבורה למחצה). בהמשך נראה איך אפשר "להציל" את הכפל.

הגדרה 1.19 (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 1.20. 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 הליניארית הכללית (ממעלה n) מעל \mathbb{R} (General Linear group).

דוגמה 1.21. 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 1.22. אם p הוא מספר ראשוני, אז $U_p = \mathbb{Z}_p^*$.

1.23. בדומה להערה האחרונה, נאפיין את האיברים ב- U_n לכל 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 1.24. $U_{12} = \{1, 5, 7, 11\}$

דוגמה 1.25. לא קיים ל-5 הופכי כפלי ב- \mathbb{Z}_{10} , שכן אחרת 5 היה זר ל-10 וזו סתירה.

2 חבורה אבלית

הגדרה 2.1. 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 $a \cdot b = b \cdot a$. אם (G, \cdot) חבורה והפעולה היא אבלית, נאמר כי G היא חבורה אבלית (או חילופית). המושג נקרא על שמו של נילס הנריק אָבֶל (Niels Henrik Abel).

דוגמה 2.2. יהי F שדה. החבורה $(GL_n(F), \cdot)$ אינה אבלית עבור $n > 1$.

תרגיל 2.3. תהי G חבורה. הוכיחו שאם לכל $x \in G$ מתקיים $x^2 = 1$, אזי G היא חבורה אבלית.

הוכחה. מן הנתון מתקיים לכל $a, b \in G$ כי $(ab)^2 = a^2 = b^2 = 1$. לכן

$$abab = (ab)^2 = 1 = 1 \cdot 1 = a^2 \cdot b^2 = aabb$$

נכפיל את השיויון לעיל מצד שמאל בהופכי של a ומצד ימין בהופכי של b , ונקבל $ba = ab$. זה מתקיים לכל זוג איברים, ולכן G חבורה אבלית. \square

3 תת-חבורות

הגדרה 3.1. תהי G חבורה. תת-קבוצה $H \subseteq G$ נקראת תת-חבורה של G אם היא חבורה ביחס לאותה פעולה (באופן יותר מדויק, ביחס לפעולה המושרית מ- G). מסמנים $H \leq G$.

תכלס מה שצריך לבדוק:

- תת-קבוצה לא ריקה -או- $e \in H$.
- סגירות לכפל: לכל $a, b \in H$ מתקיים $ab \in H$.
- סגירות להופכי: לכל $a \in H$ מתקיים $a^{-1} \in H$.

דוגמה 3.2. נוכיח שקבוצת המטריצות

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\}$$

היא תת-חבורה של $GL_3(\mathbb{R})$:

• יחידה: ברור ש- $I_3 \in H$.

$$\text{ולכן } \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix} \in H \bullet$$

יש סגירות לכפל.

• אפשר לראות שיש הפיך לפי הדטרמיננטה, אבל זה לא מספיק! צריך גם להראות שהמטריצה ההופכית נמצאת ב- H בעצמה. אמנם,

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \in H$$

לחבורה זאת ודומותיה (!) קוראים חבורת הייזנברג.

דוגמה 3.3. $SL_n(F) \leq GL_n(F)$.

דוגמה 3.4. עבור $a \in G$ תמיד אפשר לבנות תת-חבורה הנוצרת ע"י איבר $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\} \leq G$ למשל:

• $4 \in \mathbb{Z}$

$$\langle 4 \rangle = \{4k \mid k \in \mathbb{Z}\} = 4\mathbb{Z}$$

• $a = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in GL_3(\mathbb{R})$

$$\begin{aligned} \langle a \rangle &= \left\{ a^0 = I, a, a^2 = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \dots, a^n = \begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \dots \right. \\ &\quad \left. \dots, a^{-1} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, a^{-2} = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \dots, a^{-n}, \dots \right\} \\ &= \left\{ \begin{pmatrix} 1 & 0 & k \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid k \in \mathbb{Z} \right\} \end{aligned}$$

4 מבוא לתורת המספרים

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

4.2 משפט (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 quotient (מנה) ו-remainder (שארית).

4.3 הגדרה 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 רק (n, m) . למשל $(6, 10) = 2$. נאמר כי n, m זרים אם $(n, m) = 1$. למשל $(2, 5) = 1$.

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

4.5 טענה 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 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

4.6 משפט (אלגוריתם אוקלידס). "המתכון" למציאת מ"מ בעזרת שימוש חוזר בטענה 4.5 הוא אלגוריתם אוקלידס. ניתן להניח $0 \leq m < n$. אם $m = 0$, אזי $(n, m) = n$. אחרת נכתוב $n = qm + r$ כאשר $0 \leq r < m$ ונמשיך עם $(n, m) = (m, r)$. (הבינו למה האלגוריתם חייב להעצר).

4.7 דוגמה 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:

$$\begin{aligned}(224, 63) &= [224 = 3 \cdot 63 + 35] \\ (63, 35) &= [63 = 1 \cdot 35 + 28] \\ (35, 28) &= [35 = 1 \cdot 28 + 7] \\ (28, 7) &= [28 = 4 \cdot 7 + 0] \\ (7, 0) &= 7\end{aligned}$$

משפט 4.8 (אפיון הממ"מ כצירוף לינארי מזערי). מתקיים לכל מספרים שלמים a, b כי

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

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

הערה 4.9. מן המשפט קיבלנו כי $(a, b) \in a\mathbb{Z} + b\mathbb{Z}$.

דוגמה 4.10. כדי למצוא את המקדמים s, t כשמביעים את הממ"מ כצירוף לינארי כנ"ל נשתמש באלגוריתם אוקלידס המורחב:

$$\begin{aligned}(234, 61) &= [234=3 \cdot 61+51 \Rightarrow 51 = 234 - 3 \cdot 61] \\ (61, 51) &= [61=1 \cdot 51+10 \Rightarrow 10 = 61 - 1 \cdot 51 = 61 - 1 \cdot (234 - 3 \cdot 61) = -1 \cdot 234 + 4 \cdot 61] \\ (51, 10) &= [51=5 \cdot 10+1 \Rightarrow 1 = 51 - 5 \cdot 10 = 51 - 5 \cdot (-1 \cdot 234 + 4 \cdot 61) = 6 \cdot 234 - 23 \cdot 61] \\ (10, 1) &= 1\end{aligned}$$

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

תרגיל 4.11. 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 $a|c$.

טענה 4.12. 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 השויון האחרון ב- b ונקבל $sab + tpb = b$. ברור כי p מחלק את אגף שמאל (הרי $p|ab$), ולכן p מחלק את אגף ימין, כלומר $p|b$.

□

הגדרה 4.13 (לבית). בהנתן שני מספרים שלמים n, m הכפולה המשותפת המזערית (כמ"מ, least common multiple) שלהם מוגדרת להיות

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

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

טענה 4.14. תכונות של כמ"מ:

1. אם $m|a$ וגם $n|a$, אז $[n, m]|a$.

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

שאלה 4.15 (לבית). אפשר להגדיר כמ"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 .

תרגיל 4.16. מצאו את הספרה האחרונה של 333^{333} .

פתרון. בשיטה העשרונית, הספרה האחרונה של מספר N היא $N \pmod{10}$. 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.

משפט 4.17 (משפט השאריות הסיני). אם n, m זרים, אזי לכל $a, b \in \mathbb{Z}$ קיים x יחיד עד כדי שקילות מודולו nm כך ש- $x \equiv a \pmod{n}$, $x \equiv b \pmod{m}$ (יחודי!).

הוכחה. 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.

כדי להראות יחידות של x מודולו nm נשתמש בטיעון קומבינטורי. לכל זוג (a, b) יש x (לפחות אחד) המתאים לו מודולו nm . ישנם בסה"כ nm זוגות שונים (a, b) (מודולו nm), וכן רק nm ערכים אפשריים ל- x (מודולו nm). ההתאמה הזו היא פונקציה חח"ע בין קבוצות סופיות שוות עוצמה, ולכן ההתאמה היא גם על. דרך אחרת: אם קיים מספר y המקיים את הטענה, אז $n|x - y$ וגם $m|x - y$. מהנתון $(n, m) = 1$ נקבל כי $nm|x - y$ ולכן $x \equiv y \pmod{nm}$ (בהמשך נראה גם $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$). \square

דוגמה 4.18. 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 4.19 (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 4.20. 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 $15 = 3 \cdot 5$ (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.

5 חבורת אוילר ומציאת הופכי

טענה 5.1. יהי $a \in \mathbb{Z}_n$, אזי $a \in U_n$ (כלומר שהוא הפיך כפלית) אם ורק אם $(a, n) = 1$.
לכן $U_n = \{1 \leq a < n \mid (a, n) = 1\}$.

יותר מזה, יש לנו דרך למצוא את ההופכי:

ראינו שקיימים s, t כך ש $sa + tn = 1$. אם נחשב מודולו n נקבל $sa \equiv 1$ כלומר $a^{-1} = s$ ב- \mathbb{Z}_n . כלומר ההופכי הוא המקדם המתאים בצירוף של הממ"מ.

תרגיל 5.2. 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 $x = 211$.

הגדרה 5.3. סדר של חבורה הוא מספר האיברים בחבורה ומסומן: $|G|$.
לדוגמא: $|\mathbb{Z}| = \infty, |\mathbb{Z}_n| = n$.

דוגמה 5.4. פונקציית אוילר מוגדרת לפי $\varphi(n) = |U_n|$.
עבור p ראשוני, אנחנו כבר יודעים ש- $\varphi(p) = p - 1$.
ניתן להראות (בהרצאה) כי לכל ראשוני p ולכל k טבעי, $\varphi(p^k) = p^k - p^{k-1}$, כמו כן, אם $(a, b) = 1$ אזי $\varphi(ab) = \varphi(a)\varphi(b)$.
מכאן מתקבלת ההכללה: יהי $n = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ אזי $\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right)$.
למשל:

$$\varphi(60) = 60 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 16$$

6 חבורות ציקליות

הגדרה 6.1. תהי G חבורה ויהי $a \in G$. אם כל איבר ב- G הוא חזקה (חיובית או שלילית) של a אז נאמר ש- G נוצרת על ידי a . במקרה זה נאמר כי G חבורה ציקלית.
סימון: $G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$.

דוגמה 6.2.

• \mathbb{Z} נוצרת ע"י 1. שימו לב שהיוצר לא חייב להיות יחיד. למשל במקרה שלנו גם -1 הוא יוצר.

$$\bullet n\mathbb{Z} = \langle n \rangle$$

$$\bullet \mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$$

$$\bullet U_{10} = \{3, 3^2 = 9, 3^3 = 7, 3^4 = 1\} = \langle 3 \rangle$$

אם מצאנו ב"רחוב" חבורה ציקלית, אז הסדר שלה נותן לנו את כל המידע שצריך עליה:

משפט 6.3. כל חבורה ציקלית איזומורפית או ל- \mathbb{Z}_n או ל- \mathbb{Z} .

$$\bullet \text{דוגמה 6.4. } n\mathbb{Z} \cong \mathbb{Z}$$

$$\bullet \text{דוגמה 6.5. } U_{10} \cong \mathbb{Z}_4$$

אבל איך נזהה שחבורה היא ציקלית?

6.1 סדר של איבר

הגדרה 6.6. יהי $a \in G$, הסדר של a הוא: $o(a) = \min\{n \in \mathbb{N} : a^n = 1\}$. אם לא קיים כזה, נאמר שהסדר הוא אינסוף.

$$\bullet \text{דוגמה 6.7. } o(5) = 2, \text{ ב-} U_6$$

\bullet ב- $(GL_2(\mathbb{R}), \cdot)$, נבחר את $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. נראה ש- $o(b) = 3$ כי

$$b^1 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \neq I_2, \quad b^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \neq I_2, \quad b^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

טענה 6.8. תהי G חבורה, ויהי $a \in G$. מתקיים $a^n = e$ אם ורק אם $o(a) | n$.

שאלה 6.9. תהי חבורה $G \times H$, הוכח כי הסדר של איבר (g, h) הוא $[o(g), o(h)]$. פתרון. נסמן $o(g) = n$ ו- $o(h) = m$. נראה שהסדר של איבר (g, h) הוא מחלק משותף של n, m :

$$(g, h)^{o(g,h)} = (g^{o(g,h)}, h^{o(g,h)}) = (e_G, e_H)$$

ולכן בפרט, לפי הטענה האחרונה:

$$n | o(g, h) \Leftarrow g^{o(g,h)} = e$$

$$m | o(g, h) \Leftarrow h^{o(g,h)} = e$$

מה שאומר ש- $o(g, h)$ הוא מכפלה משותפת של m ו- n , ולכן $[n, m] | o(g, h)$ מצד שני נשים לב כי

$$(g, h)^{[n,m]} = (g^{[n,m]}, h^{[n,m]}) = (g^{nk}, h^{mk'}) = (e_G, e_H) = e_{G \times H}$$

ולכן $o((g, h)) | [n, m]$

משפט 6.10. הסדר של איבר x שווה לסדר תת-החבורה שהוא יוצר (כלומר $\langle x \rangle$).
 בפרט, אם G חבורה מסדר n . אז G היא ציקלית אם"ס קיים איבר מסדר n .

דוגמה 6.11. ב- U_8 קל לבדוק ש $o(3) = o(5) = o(7) = 2$ ולכן החבורה אינה ציקלית.

תרגיל 6.12. האם $\mathbb{Z}_n \times \mathbb{Z}_n$ היא ציקלית?

פתרון. הסדר של החבורה הוא n^2 . ע"מ שהיא תהיה ציקלית יש למצוא איבר שהסדר שלו הוא n^2 . אולם לכל $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n$ מתקיים: $n(a, b) = (na, nb) = (0, 0)$ ולכן הסדר של כל איבר קטן או שווה ל- n .

תרגיל 6.13. תהי G חבורה אבלית. הוכיחו שאוסף האיברים מסדר סופי הוא תת-חבורה.

פתרון. נסמן את האוסף הנ"ל ב- A . נוכיח את התנאים הדרושים:

- $e \in A$ כי $A \neq \emptyset$.

- סגירות לפעולה: יהיו $a, b \in A$. אז יש n, m טבעיים כך ש $a^n = b^m = e$. אזי: $(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = e^m e^n = e$ (שימו לב לשימוש בחילופיות!).

- סגירות להופכי: יהי $a \in A$. יש n כך ש $a^n = e$, אז $a \cdot a^{n-1} = e$ לכן $a^{-1} = a^{n-1}$ וכבר ראינו שיש סגירות לפעולה.

תרגיל 6.14. תהי G חבורה ויהיו $a, b \in G$ מסדר סופי. האם גם ab בהכרח מסדר סופי?

פתרון. אם G אבלית, אז ראינו שזה נכון בתרגיל 6.13. באופן כללי, לא. נמצא דוגמה נגדית: נבחר את $(GL_2(\mathbb{R}), \cdot)$, ונתבונן באיברים

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

ניתן לבדוק שמתקיים: $a^4 = b^3 = I$. אולם $ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ אינו מסדר סופי כי

$$(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

טענה 6.15. מספר תכונות של הסדר:

1. אם G חבורה ציקלית סופית מסדר n אז לכל $g \in G$ מתקיים $g^n = e$.

2. בתבורה סופית הסדר של כל איבר הוא סופי.

3. $o(a^i) \leq o(a)$. למעשה $o(a^i) | o(a)$ (בהמשך).

4. $o(a) = o(a^{-1})$.

פתרון. נוכיח את הסעיף האחרון:

מקרה ראשון, נניח $o(a) = n$, מספיק להראות ש $o(a^{-1}) \leq o(a)$ (כי $(a^{-1})^{-1} = a$).
 אז $a^n = 1$. $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$. לכן $o(a^{-1}) \leq n$.
 מקרה שני, נניח שהסדר של a אינסופי. אז גם הסדר של a^{-1} אינסופי, כי אם הוא היה איזשהו n , אז מהמקרה הראשון, היינו מקבלים ש $o(a) = n$, בסתירה.
 הערה 6.16. יהי $a \in G$. אזי $o(a) = |\langle a \rangle|$. במילים, הסדר של איבר הוא סדר תת-החבורה שהוא יוצר.

תרגיל 6.17 (מההרצאה). 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 (לדגל). 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 6.8, $n | dt$. לכן, גם $\frac{n}{(d, n)} | \frac{dt}{(d, n)}$ (שניהם מספרים שלמים - מדוע?). מצד שני, $\left(\frac{n}{(d, n)}, \frac{d}{(d, n)}\right) = 1$. לפי תרגיל 4.11, נקבל $\frac{n}{(d, n)} | t$, כמו שרצינו. \square

תרגיל 6.18. תהי G חבורה ציקלית מסדר n . כמה איברים ב- G יוצרים (לבדם) 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 $|U_n|$. כלומר בדיוק $\varphi(n)$.

6.2 חבורת שורשי היחידה

דוגמה 6.19. קבוצת שורשי היחידה מסדר n מעל \mathbb{C} היא

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

זו תת-חבורה של \mathbb{C}^* . אם נסמן $\omega_n = \text{cis} \frac{2\pi}{n}$, נקבל $\langle \omega_n \rangle = \Omega_n$. כלומר Ω_n היא תת-חבורה ציקלית ונוצרת על ידי ω_n . מפני ש- Ω_n מסדר n וציקלית, אז בהכרח $\Omega_n \cong \mathbb{Z}_n$.

תרגיל 6.20. נגדיר את קבוצת שורשי היחידה $\Omega_\infty = \bigcup_{n=1}^{\infty} \Omega_n$. הוכיחו:

- Ω_∞ היא חבורה לגבי כפל. (איחוד חבורות הוא לא בהכרח חבורה!)
- לכל $x \in \Omega_\infty$, $o(x) < \infty$ (כלומר: כל איבר ב- Ω_∞ הוא מסדר סופי).
- Ω_∞ אינה ציקלית.

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

פתרון.

1. נוכיח שהיא חבורה על ידי זה שנוכיח שהיא תת-חבורה של \mathbb{C}^* . ראינו בתרגיל 6.13 שתת-חבורת הפיתול של חבורה אבלית היא תת-חבורה. לפי הגדרת Ω_∞ , רואים שהיא מכילה בדיוק את כל האיברים מסדר סופי של החבורה האבלית \mathbb{C}^* , ולכן חבורה.

באופן מפורש ולפי הגדרה: ברור כי $1 \in \Omega_\infty$, ולכן היא לא ריקה. יהיו $g_1, g_2 \in \Omega_\infty$. לכן קיימים m, n שעבורם $g_1 \in \Omega_m, g_2 \in \Omega_n$. נכתוב עבור $l, k \in \mathbb{Z}$ מתאימים:

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

לכן

$$\begin{aligned} g_1 g_2 &= \text{cis} \frac{2\pi k}{m} \cdot \text{cis} \frac{2\pi l}{n} = \text{cis} \left(\frac{2\pi k}{m} + \frac{2\pi l}{n} \right) \\ &= \text{cis} \left(\frac{2\pi (kn + lm)}{mn} \right) \in \Omega_{mn} \subseteq \Omega_\infty \end{aligned}$$

סגירות להופכי היא ברורה, שהרי אם $g \in \Omega_n$, אז גם $g^{-1} \in \Omega_n \subseteq \Omega_\infty$. (אם יש זמן: לדבר שאיחוד של שרשרת חבורות, ובאופן כללי יותר, איחוד רשת של חבורות, היא חבורה.)

2. לכל $x \in \Omega_\infty$ קיים n שעבורו $x \in \Omega_n$. לכן, $o(x) \leq n$.
3. לפי הסעיף הקודם, כל תת-החבורות הציקליות של Ω_∞ הן סופיות. אך Ω_∞ אינסופית, ולכן לא ייתכן שהיא שווה לאחת מהן.

7 תת-חבורה הנוצרת על ידי איברים

7.1 הגדרה תהי G חבורה ותהי $S \subseteq G$ תת-קבוצה לא ריקה איברים ב- G (שימו לב ש- S אינה בהכרח תת-חבורה של G).
תת-החבורה הנוצרת על ידי S הינה תת-החבורה המינימלית המכילה את S ונסמנה $\langle S \rangle$. אם $G = \langle S \rangle$ אז נאמר ש- G נוצרת על ידי S . עבור קבוצה סופית של איברים, נכתוב בקיצור $\langle x_1, \dots, x_k \rangle$.
הגדרה זו מהווה הכללה להגדרה של חבורה ציקלית. חבורה היא ציקלית אם היא נוצרת על ידי איבר אחד.

7.2 דוגמה ניקח $\{2, 3\} \subseteq \mathbb{Z}$ ואת $H = \langle 2, 3 \rangle$. נוכיח בעזרת הכלה דו-כיוונית ש- $H = \mathbb{Z}$.

H תת-חבורה של \mathbb{Z} , ובפרט $H \subseteq \mathbb{Z}$. כיוון ש- $2 \in H$ אזי גם $-2 \in H$ ומכאן $1 \in H = (-2) + 3$. כלומר איבר היחידה, שהוא יוצר של \mathbb{Z} , מוכל ב- H . לכן $\mathbb{Z} = \langle 1 \rangle \subseteq H$, כלומר $\mathbb{Z} \subseteq H$. קיבלנו ש- $H = \mathbb{Z}$.

7.3 דוגמה אם ניקח $\{4, 6\} \subseteq \mathbb{Z}$, אז נקבל: $\langle 4, 6 \rangle = \{4n + 6m : m, n \in \mathbb{Z}\}$.
נטען ש- $2\mathbb{Z} = \gcd(4, 6) \cdot \mathbb{Z} = \langle 4, 6 \rangle$ (כלומר תת-חבורה של השלמים המכילה רק את המספרים הזוגיים). נוכיח על ידי הכלה דו כיוונית,
 (\subseteq) : ברור ש- $2 \mid 4m + 6n$ ולכן $\langle 4, 6 \rangle \subseteq 2\mathbb{Z}$.
 (\supseteq) : יהי $2k \in 2\mathbb{Z}$. אזי $2k = 4(-k) + 6k \in \langle 4, 6 \rangle$. לכן מתקיים גם: $2\mathbb{Z} \subseteq \langle 4, 6 \rangle$.

7.4 דוגמה בדומה לדוגמה האחרונה, במקרה שהחבורה אבלית, קל יותר לתאר את תת-החבורה הנוצרת על ידי קבוצת איברים. למשל אם ניקח שני יוצרים $a, b \in G$ נקבל: $\langle a, b \rangle = \{a^i b^j : i, j \in \mathbb{Z}\}$.
בזכות החילופיות, ניתן לסדר את כל ה- a -ים יחד וכל ה- b -ים יחד. למשל

$$abaaab^{-1}bbba^{-1}a = a^4b^3$$

באופן כללי, בחבורה אבלית מתקיים:

$$\langle a_1, \dots, a_n \rangle = \{a_1^{k_1} \dots a_n^{k_n} : \forall 1 \leq i \leq n, k_i \in \mathbb{Z}\}$$

דוגמה 7.5. נוח לעיתים לחשוב על איברי $\langle A \rangle$ בתור קבוצת "המילים" שניתן לכתוב באמצעות האותיות בקבוצה A . מגדירים את האלפבית שלנו להיות $A \cup A^{-1}$ כאשר $A^{-1} = \{a^{-1} : a \in A\}$. מילה היא סדרה סופית של אותיות מן האלפבית, והמילה הריקה מייצגת את איבר היחידה ב- G .

הגדרה 7.6. חבורה G תקרא נוצרת סופית, אם קיימת לה קבוצת יוצרים סופית. כלומר קיימים מספר סופי של איברים $a_1, \dots, a_n \in G$ כך ש- $\langle a_1, \dots, a_n \rangle = G$.

מסקנה 7.7. כל חבורה סופית נוצרת סופית.

דוגמה 7.8. כל חבורה ציקלית נוצרת סופית (מהגדרה). לכן יש חבורות אינסופיות כמו \mathbb{Z} שנוצרות סופית. האם יש עוד חבורות כאלו? כן, למשל $\mathbb{Z} \times \mathbb{Z} = \langle (1, 0), (0, 1) \rangle$.

תרגיל 7.9. הוכיחו שהחבורות הבאות לא נוצרות סופית

1. חבורת שורשי היחידה Ω_∞ .

2. $(M_3(\mathbb{R}), +)$.

3. (\mathbb{Q}^*, \cdot) .

פתרון.

1. בעוד ש- Ω_∞ היא אינסופית, נראה שכל תת-החבורה הנוצרת על ידי מספר סופי של איברים מ- Ω_∞ היא סופית. יהיו a_1, \dots, a_k שורשי יחידה מסדרים n_1, \dots, n_k בהתאמה. אז

$$\langle a_1, \dots, a_k \rangle = \{a_1^{i_1} \dots a_k^{i_k} : 0 \leq i_j \leq n_j, 1 \leq j \leq k\}$$

מפני ש- Ω_∞ היא אבלית. לכן יש מספר סופי (החסום מלמעלה במכפלה $n_1 \dots n_k$) של איברים ב- $\langle a_1, \dots, a_k \rangle$. לכן Ω_∞ אינה נוצרת סופית.

2. אפשר להוכיח זאת בעזרת שיקולי עוצמה. כל חבורה נוצרת סופית היא סופית או בת מנייה (אוסף המילים הסופיות על אלפבית סופי הוא בן מנייה), ואילו $M_3(\mathbb{R})$ אינה בת מנייה.

3. נניח בשלילה כי

$$\mathbb{Q}^* = \left\langle \frac{a_1}{b_1}, \dots, \frac{a_n}{b_n} \right\rangle = \left\{ \left(\frac{a_1}{b_1} \right)^{k_1} \dots \left(\frac{a_n}{b_n} \right)^{k_n} : \forall 1 \leq i \leq n, k_i \in \mathbb{Z} \right\}$$

אז קל לראות שהגורמים הראשוניים במכנה של כל איבר מוגבלים לקבוצת הגורמים הראשוניים שמופיעים בפירוק של המכפלה $b_1 \dots b_n$. אך זו קבוצה סופית, ולכן לא ניתן לקבל את כל השברים ב- \mathbb{Q}^* , כלומר סתירה.

8 החבורה הסימטרית (על קצה המזלג)

8.1 הגדרה. החבורה הסימטרית מזרקה n היא

$$S_n = \{\sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\} \mid \sigma \text{ is bijective}\}$$

זהו אוסף כל ההעתקות החח"ע ועל מהקבוצה $\{1, 2, \dots, n\}$ לעצמה, ובמילים אחרות – אוסף כל שינויי הסדר של המספרים $\{1, 2, \dots, n\}$. S_n היא חבורה, כאשר הפעולה היא הרכבת פונקציות. איבר היחידה הוא פונקציית הזהות. כל איבר של S_n נקרא תמורה.

הערה 8.2 (אם יש זמן). החבורה S_n היא בדיוק חבורת ההפיכים במונואיד X^X עם פעולת ההרכבה, כאשר $X = \{1, 2, \dots, n\}$.

8.3 דוגמה. ניקח לדוגמה את S_3 . איבר $\sigma \in S_3$ הוא מהצורה $\sigma(1) = i, \sigma(2) = j, \sigma(3) = k$, כאשר $i, j, k \in \{1, 2, 3\}$ שונים זה מזה. נסמן בקיצור

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ i & j & k \end{pmatrix}$$

נכתוב במפורש את האיברים ב- S_3 :

$$1. \text{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$2. \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$3. \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$4. \sigma^2 = \sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$5. \sigma\tau = \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$6. \tau\sigma = \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

8.4 מסקנה. נשים לב ש- S_3 אינה אבלית, כי $\sigma\tau \neq \tau\sigma$. מכאן גם קל לראות ש- S_n אינה ציקלית לכל $n \geq 3$, כי היא לא אבלית.

הערה 8.5. הסדר הוא $|S_n| = n!$. אכן, מספר האפשרויות לבחור את $\sigma(1)$ הוא n ; אחר כך, מספר האפשרויות לבחור את $\sigma(2)$ הוא $n-1$; כך ממשיכים, עד שמספר האפשרויות לבחור את $\sigma(n)$ הוא 1, האיבר האחרון שלא בחרנו. בסך הכל, $|S_n| = n \cdot (n-1) \cdot \dots \cdot 1 = n!$.

8.6 הגדרה. מחזור (או עגיל) ב- S_n הוא תמורה המציינת מעגל אחד של החלפות של מספרים שונים: $a_1 \mapsto a_2 \mapsto a_3 \mapsto \dots \mapsto a_k \mapsto a_1$ (ושאר המספרים נשלחים לעצמם). כותבים את התמורה הזו בקיצור $(a_1 a_2 \dots a_k)$. האורך של המחזור $(a_1 a_2 \dots a_k)$ הוא k .

8.7 דוגמה. ב- S_5 , המחזור $(4 5 2)$ מציין את התמורה $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$.

8.8 משפט. כל תמורה ניתנת לכתיבה באופן יחיד כהרכבת מחזורים זרים, כאשר הכוונה ב"מחזורים זרים" היא מחזורים שאין לאף זוג מהם איבר משותף.

הערה 8.9. שימו לב שמחזורים זרים מתחלפים זה עם זה (מדוע?), ולכן חישובים עם מחזורים יהיו לעיתים קלים יותר מאשר חישובים עם התמורה עצמה.

8.10 דוגמה. נסתכל על התמורה הבאה ב- S_7 : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 3 & 1 & 5 & 2 & 6 \end{pmatrix}$. כדי לכתוב אותה כמכפלת מחזורים זרים, לוקחים מספר, ומתחילים לעבור על המחזור המתחיל בו. למשל:

$$1 \mapsto 4 \mapsto 1$$

אז בכתיבה על ידי מחזורים יהיה לנו את המחזור $(1 4)$. כעת ממשיכים כך, ומתחילים ממספר אחר:

$$2 \mapsto 7 \mapsto 6 \mapsto 2$$

אז נקבל את המחזור $(2 7 6)$ בכתיבה. נשים לב ששאר המספרים הולכים לעצמם, כלומר $3 \mapsto 3, 5 \mapsto 5$, ולכן

$$\sigma = (1 4)(2 7 6)$$

נחשב את σ^2 . אפשר ללכת לפי ההגדרה, לעבור על כל מספר ולבדוק לאן σ^2 תשלח אותו; אבל, כיוון שמחזורים זרים מתחלפים, נקבל

$$\sigma^2 = ((1 4)(2 7 6))^2 = (1 4)^2 (2 7 6)^2 = (2 6 7)$$

8.11 תרגיל. יהי $\sigma \in S_n$ מחזור מאורך k . מהו $o(\sigma)$?

פתרון. נסמן $\sigma = (a_0 a_1 \dots a_{k-1})$. נוכיח כי $o(\sigma) = k$.

מתקיים ש- $\sigma^k(a_0) = a_{i \bmod k}$ (שימו לב, האינדקס מודולו k מאפשר לנו לעבוד בטווח $\{0, 1, \dots, k-1\}$). ראשית, ברור כי $\sigma^k = \text{id}$: לכל מתקיים

$$\sigma^k(a_i) = \sigma^{k-1}(a_{i+1}) = \dots = \sigma(a_{i-1}) = a_i$$

ולכל $m \neq a_i$, $\sigma^k(m) = m$ (כי $\sigma(m) = m$). נותר להוכיח מינימליות. אבל אם $l < k$, אז $\sigma^l(a_0) = a_l \neq a_0$, כלומר $\sigma^l \neq \text{id}$.