

מבנים אלגבריים למדעי המחשב  
מערכי תרגול קורס 89-214

נובמבר 2018, גרסה 1.12

## תוכן העניינים

4	מבוא
5	1 תרגול ראשון
5	1.1 מבנים אלגבריים בסיסיים
7	1.2 חבורות אבליות
8	2 תרגול שני
9	2.1 תת-חבורות
10	2.2 חבורת אוילר
11	2.3 סדרים
12	3 תרגול שלישי
12	3.1 חבורות ציקליות
15	3.2 מכפלה ישרה של חבורות
16	4 תרגול רביעי
16	4.1 מבוא לחבורה הסימטרית
18	4.2 מחלקות
20	5 תרגול חמישי
20	5.1 מבוא לתורת המספרים
25	6 תרגול שישי
25	6.1 משפט לגראנז'
27	6.2 חישוב פונקציית אוילר
28	6.3 תת-חבורה הנוצרת על ידי תת-קבוצה
29	7 תרגול שביעי
29	7.1 סדר של איברים בחבורה הסימטרית
31	7.2 מערכת הצפנה RSA
32	8 תרגול שמיני
32	8.1 חבורות מוצגות סופית
33	8.2 החבורה הדיהדרלית
34	8.3 הומומורפיזמים
38	9 תרגול תשיעי
38	9.1 סימן של תמורה וחבורת החילופין
38	9.2 תת-חבורות נורמליות
40	9.3 חבורות מנה

<b>42</b>	<b>10 תרגול עשרי</b>
42 . . . . .	10.1 משפטי האיזומורפיזם של נתר .
<b>46</b>	<b>11 תרגול אחד עשר</b>
46 . . . . .	11.1 פעולת ההצמדה .
<b>50</b>	<b>12 תרגול שניים עשר</b>
50 . . . . .	12.1 אלגוריתם מילר-רבין לבדיקת ראשוניות
52 . . . . .	12.2 חבורות אבליות סופיות
<b>54</b>	<b>13 תרגול שלושה עשר</b>
54 . . . . .	13.1 שדות סופיים
57 . . . . .	13.2 בעיית הלוגריתם הבדיד ואלגוריתם דיפי-הלמן
<b>59</b>	<b>14 תרגול ארבעה עשר</b>
59 . . . . .	14.1 משוואת המחלקות
61 . . . . .	14.2 תת-חבורת הקומוטטור
<b>63</b>	<b>נספח: חבורות מוכרות</b>

## מבוא

כמה הערות טכניות לתחילת הקורס:

- דף הקורס נמצא באתר [www.math-wiki.com](http://www.math-wiki.com).
- שאלות בנוגע לחומר הלימודי מומלץ לשאול בדף השיחה באתר של הקורס.
- החומר בקובץ זה נאסף מכמה מקורות, ומבוסס בעיקרו על מערכי תרגול קודמים בקורסים מבנים אלגבריים למדעי המחשב ואלגברה מופשטת למתמטיקה.
- נשתדל לכתוב בגופן הזה כשהגדרות ומושגים חשובים מופיעים בפעם הראשונה. נוסיף בצד גם את השם באנגלית, שעשוי לעזור כשמחפשים חומר נוסף שאינו בעברית.
- נשמח לכל הערה על מסמך זה.

מחברים בשנת הלימודים תשע"ו: אבי אלון, תומר באואר וגיא בלשר  
מחברים בשנת הלימודים תשע"ז: תומר באואר, עמרי מרכוס ואלעד עטיא  
מחברים בשנת הלימודים תשע"ט: תומר באואר וגלעד פורת קורן

# 1 תרגול ראשון

## 1.1 מבנים אלגבריים בסיסיים

בהתאם לשם הקורס, כעת נכיר כמה מבנים אלגבריים. שדה הוא מבנה אלגברי שפוגשים כבר באלגברה לינארית. אנו נגדיר כמה מבנים יותר "פשוטים", כשהחשוב שבהם הוא חבורה. במרבית הקורס נתרכז בחקר חבורות. נסמן כמה קבוצות מוכרות של מספרים:

- $\mathbb{N} = \{1, 2, 3, \dots\}$  המספרים הטבעיים.

- $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$  המספרים השלמים (מגרמנית: Zahlen).

- $\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\} \right\}$  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.** פעולה בינארית על קבוצה  $S$  היא פונקציה דו־מקומית  $* : S \times S \rightarrow S$ . עבור  $a, b \in S$  כמעט תמיד במקום לרשום  $*(a, b)$  נשתמש בסימון  $a * b$ . חשוב לשים לב שהפעולה היא סגורה, כלומר תמונת הפונקציה  $a * b$  תמיד שייכת ל- $S$ .

**הגדרה 1.2.** אגודה (או חבורה למחצה) היא מערכת אלגברית  $(S, *)$  המורכבת מקבוצה  $S$  ופעולה בינארית קיבוצית על  $S$ . קיבוציות (או אסוציאטיביות) משמעה שלכל  $a, b, c \in S$  מתקיים  $(a * b) * c = a * (b * c)$ .

**דוגמה 1.3.** המערכת  $(\mathbb{N}, +)$  של מספרים טבעיים עם החיבור הרגיל היא אגודה.

**דוגמה 1.4.** המערכת  $(\mathbb{Z}, -)$  אינה אגודה, מפני שפעולת החיסור אינה קיבוצית. למשל  $(2 - 1) - 1 \neq 5 - (2 - 2)$ .

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

**הגדרה 1.6.** תהי  $(S, *)$  אגודה. איבר  $e \in S$  נקרא איבר יחידה אם לכל  $a \in S$  מתקיים  $a * e = e * a = a$ .

**הגדרה 1.7.** מונואיד (או יחידון)  $(M, *, e)$  הוא אגודה בעלת איבר יחידה  $e$ . כאשר הפעולה ואיבר היחידה ברורים מן ההקשר, פשוט נאמר כי  $M$  הוא מונואיד.

**1.8.** הערה (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  $e = e * f = f$ .

Left invertible הגדרה 1.9. 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  $a$ .

Left inverse באופן דומה, איבר  $a \in M$  יקרא הפיך מימין אם קיים איבר  $b \in M$  כך ש- $ab = e$ .

Right invertible במקרה זה  $b$  יקרא הופכי ימני של  $a$ .

Right inverse איבר יקרא הפיך אם קיים איבר  $b \in M$  כך ש- $ba = ab = e$ . במקרה זה  $b$  יקרא הופכי של  $a$ .

Invertible

Inverse

**תרגיל 1.10.** 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 הימניים וכל ההופכיים השמאליים של  $a$  שווים זה לזה. מכאן גם שההופכי הוא יחיד, ויסומן  $a^{-1}$ . שימו לב שאם איבר רק הפיך מימין ולא משמאל, אז יתכן שיש לו יותר מההופכי ימני אחד (וכנ"ל בהיפוך הכיוונים)!

Group **הגדרה 1.11.** חבורה  $(G, *, e)$  היא מונואיד שבו כל איבר הוא הפיך.

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.

כמו כן מתקיים: חבורה  $\Leftarrow$  מונואיד  $\Leftarrow$  אגודה.

**דוגמה 1.12.** המערכת  $(\mathbb{Z}, +)$  היא חבורה שאיבר היחידה בה הוא 0. בכתוב חיבורי מקובל לסמן את האיבר ההופכי של  $a$  בסימון  $-a$ . כתיב זה מתלכד עם המושג המוכר של מספר נגדי ביחס לחיבור.

**דוגמה 1.13.** 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 1.14.** יהי  $F$  שדה. המערכת  $(F, \cdot)$  עם פעולת הכפל של השדה היא מונואיד שאינו חבורה (מי לא הפיך?). איבר היחידה הוא 1.

**דוגמה 1.15.** 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?).

Trivial group

**דוגמה 1.16.** קבוצה בעלת איבר אחד ופעולה סגורה היא חבורה. לחבורה זו קוראים החבורה הטריוויאלית.

Group of units

**הגדרה 1.17.** יהי  $M$  מונואיד. אוסף האיברים ההפיכים במונואיד מהווה חבורה ביחס לפעולה המצומצמת, הנקראת חבורת האיברים ההפיכים של  $M$  ומסומנת  $U(M)$ .

למה  $U(M)$  חבורה בכלל? יהיו  $a, b \in M$  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. האוסף הזה מכיל את איבר היחידה, וכל איבר בו הוא הפיך.

הערה 1.18. מתקיים  $U(M) = M$  אם ורק אם  $M$  היא חבורה.

**הגדרה 1.19.** המערכת  $(M_n(\mathbb{R}), \cdot)$  של מטריצות ממשיות בגודל  $n \times n$  עם כפל מטריצות היא מונואיד. לחבורת ההפיכים שלו

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

General linear group

קוראים החבורה הליניארית הכללית (ממעלה  $n$ ) מעל  $\mathbb{R}$ .

**תרגיל 1.20** (אם יש זמן). 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  $X^X = \{f \mid X \rightarrow X\}$ . 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  $S_n$ , ובה כל איבר הפיך משמאל). 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.

Symmetry group on  $X$

## 1.2 חבורות אבליות

Abelian (or commutative) Abelian group

**הגדרה 1.21.** נאמר כי פעולה דו-מקומית  $\cdot: G \times G \rightarrow G$  היא אבלית (או חילופית) 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 1.22.** יהי  $F$  שדה. החבורה  $(GL_n(F), \cdot)$  אינה אבלית עבור  $n > 1$ .

**דוגמה 1.23.** מרחב וקטורי  $V$  יחד עם פעולת חיבור וקטורים הרגילה הוא חבורה אבלית.

**תרגיל 1.24.** תהי  $G$  חבורה. הוכיחו שאם לכל  $x \in G$  מתקיים  $x^2 = e$ , אזי  $G$  היא חבורה אבלית.

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

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

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

**הגדרה 1.25.** תהי  $G$  חבורה. נאמר ששני איברים  $a, b \in G$  מתחלפים אם  $ab = ba$ . נגדיר את המִרְכָּז של חבורה  $G$  להיות

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

דהיינו זהו האוסף של כל האיברים ב- $G$  שמתחלפים עם כל איברי  $G$ .

**דוגמה 1.26.** חבורה  $G$  היא אבלית אם ורק אם  $Z(G) = G$ . האם אתם יכולים להראות שבהנתן חבורה  $G$ , אז גם  $Z(G)$  היא חבורה?

הערה 1.27. 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 1.28 (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 אבלית,  $(F^*, \cdot, 1)$  היא חבורה אבלית וקיום חוק הפילוג (לכל  $a, b, c \in F$  מתקיים  $a(b + c) = ab + ac$ ).

Distributive law

## 2 תרגול שני

צורת רישום 2.1. יהי  $n$  מספר שלם. נסמן את הכפולות שלו ב- $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$ . למשל  $4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$ . זו חבורה אבלית לגבי פעולת החיבור.



**2.2 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  $10|5$ .

**2.3 משפט** (משפט החילוק, או חלוקה אוקלידית). לכל  $d \neq 0, n \in \mathbb{Z}$  קיימים יחידים  $q, r$  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).

**2.4 דוגמה**. נסתכל על אוסף מחלקות השקילות מודולו  $n$ ,  $\mathbb{Z}_n = \{[a] \mid a \in \mathbb{Z}\}$ . למשל  $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ . לפעמים מסמנים את מחלקת השקילות  $[a]$  בסימון  $\bar{a}$ , ולעיתים כאשר ההקשר ברור פשוט  $a$ .

חיבור וכפל מודולו  $n$  מוגדרים 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  $\mathbb{Z}_n^\circ = \mathbb{Z}_n \setminus \{[0]\}$ . האם  $(\mathbb{Z}_n^\circ, \cdot)$  חבורה? לא בהכרח. למשל עבור  $\mathbb{Z}_6^\circ$  נקבל כי  $[0] = [6] = [3] \cdot [2]$ . לפי ההגדרה  $\mathbb{Z}_6^\circ \ni [0]$ , ולכן  $(\mathbb{Z}_6^\circ, \cdot)$  אינה סגורה (כלומר אפילו לא אגודה). בהמשך נראה איך אפשר "להציל" את הכפל.

## 2.1 תת-חבורות

**2.5 הגדרה**. תהי  $G$  חבורה. תת-קבוצה  $H \subseteq G$  היא תת-חבורה, אם היא חבורה ביחס לאותה פעולה (באופן יותר מדויק, ביחס לפעולה המושרית מ- $G$ ). במקרה כזה נסמן  $H \leq G$ .

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

**2.7 דוגמה**. לכל  $n \in \mathbb{Z}$ ,  $n\mathbb{Z} \leq \mathbb{Z}$ . בהמשך נוכיח שאלו כל תת-חבורות של  $\mathbb{Z}$ .

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

**2.9 דוגמה**.  $(\mathbb{Z}_n, +)$  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. גם לא מדובר באותן פעולות, למרות שהסימון  $+$  זהה.

**דוגמה 2.10.**  $(GL_n(\mathbb{R}), \cdot)$  אינה תת-חבורה של  $(M_n(\mathbb{R}), +)$ , כי הפעולות בהן שונות. טענה 2.11 (קריטריון מקוצר לתת-חבורה - בהרצאה). תהי  $H \subseteq G$  תת-קבוצה. אזי  $H$  תת-חבורה של  $G$  אם ורק אם שני התנאים הבאים מתקיימים:

1.  $H \neq \emptyset$  (בדרך כלל הכי נוח להראות  $e \in H$ ).

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

**תרגיל 2.12.** יהי  $F$  שדה. נגדיר

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

Special linear group

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

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  $GL_n(F)$ .

□

**תרגיל 2.13.** תהי  $G$  חבורה. הוכיחו  $Z(G) \leq G$ , כלומר שהמרכז הוא תת-חבורה.

## 2.2 חבורת אוילר

Multiplicative group of integers modulo  $n$

**דוגמה 2.14.** נראה איך ניתן להציל את המקרה של הכפל מודולו  $n$ . נגדיר את חבורת אוילר להיות  $U_n = U(\mathbb{Z}_n)$  לגבי פעולת הכפל מודולו  $n$ . הן נקראות על שמו של לאונרד אוילר (Leonhard Euler).

נבנה את לוח הכפל של  $\mathbb{Z}_6$  (בהתעלם מ- $[0]$  שתמיד יתן במכפלה  $[0]$ ):

·	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 2.15. אם  $p$  הוא מספר ראשוני, אז  $U_p = \mathbb{Z}_p^*$ .

טענה 2.16 (בהרצאה בעתיד). יהי  $m \in \mathbb{Z}$ . אז  $[m] \in U_n$  אם ורק אם המחלק המשותף הגדול ביותר של  $n$  ו- $m$  הוא 1. כלומר, ההפיכים במונואיד  $(\mathbb{Z}_n, \cdot)$  הם כל האיברים הזרים ל- $n$ .

**דוגמה 2.17.**  $U_{12} = \{1, 5, 7, 11\}$

**דוגמה 2.18.** לא קיים ל-5 הופכי כפלי ב- $\mathbb{Z}_{10}$ , שכן אחרת 5 היה זר ל-10 וזו סתירה.

## 2.3 סדרים

**הגדרה 2.19.** תהי  $G$  חבורה. נגדיר את הסדר של  $G$  להיות עוצמתה כקבוצה. במילים יותר גשמיות, כמה איברים יש בחבורה. נסמן זאת  $|G|$ .

צורת רישום 2.20. 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 2.21.** 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 אינסופי. בפרט, בכל חבורה הסדר של איבר היחידה הוא 1, וזהו האיבר היחיד מסדר 1. סימון מקובל  $o(g) = n$  ולפעמים  $|g|$ .

**דוגמה 2.22.** בחבורה  $(\mathbb{Z}_6, +)$ ,  $o(2) = o(4) = 3$ ,  $o(3) = 2$ ,  $o(1) = o(5) = 6$ .

**דוגמה 2.23.** 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 2.24.** נסתכל על  $GL_2(\mathbb{R})$ , חבורת המטריצות ההפיכות מגודל  $2 \times 2$  מעל  $\mathbb{R}$ .

נחשב את הסדר של האיבר  $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ :

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

לכן  $o(b) = 3$

**תרגיל 2.25.** תהי  $G$  חבורה. הוכיחו שלכל  $a \in G$ ,  $o(a) = o(a^{-1})$ .

הוכחה. נחלק לשני מקרים:

מקרה 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- $a$  ו- $a^{-1}$  מתחלפים (הרי  $(ab)^n \neq a^n b^n$  באופן כללי). 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  $o(a) = o((a^{-1})^{-1}) \leq o(a^{-1})$ . לכן יש שוויון.

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

□

### 3 תרגול שלישי

#### 3.1 חבורות ציקליות

Subgroup  
generated by  $a$

**הגדרה 3.1.** 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 3.2.** לכל  $n \in \mathbb{Z}$  מתקיים  $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\} = n\mathbb{Z}$ .

**הגדרה 3.3.** 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).

Cyclic group

**דוגמה 3.4.** 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  $\mathbb{Z}$ .

**דוגמה 3.5.** 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. קל למצוא שניים (1 וגם  $9 \equiv -1$ ), האחרים (7, 3) דורשים לבניתיים בדיקה ידנית.

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

**3.7.** הערה. 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  $5 + 5 \equiv 0 \pmod{10}$ .

**דוגמה 3.8.** עבור  $a \in GL_3(\mathbb{C})$  נחשב את  $|\langle a \rangle|$  כאשר

$$a = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\langle a \rangle = \left\{ a^0 = I, a, a^2 = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \dots, a^n = \begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \dots \right.$$

$$\left. \dots, a^{-1} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, a^{-2} = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \dots, a^{-n}, \dots \right\}$$

$$= \left\{ \begin{pmatrix} 1 & 0 & k \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid k \in \mathbb{Z} \right\}$$

ולכן  $|\langle a \rangle| = \infty$  וזהו גם הסדר של  $a$ .

סענה 3.9. 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  $g_1 g_2 = g_2 g_1$ .  
 $G$  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 3.10.** לא כל חבורה אבלית היא ציקלית. למשל, נסתכל על  $U_8 = \{1, 3, 5, 7\}$ . זו אינה חבורה ציקלית, כי אין בחבורה הזו איבר מסדר 4 (כל האיברים שאינם 1 הם מסדר 2 כפי שבדקתם בתרגיל הבית).

**דוגמה 3.11.** קבוצת שורשי היחידה מסדר  $n$  מעל  $\mathbb{C}$  היא

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

זו תת-חבורה של  $\mathbb{C}^*$ . אם נסמן  $\omega_n = \operatorname{cis} \frac{2\pi}{n}$ , נקבל  $\Omega_n = \langle \omega_n \rangle$ . כלומר  $\Omega_n$  היא תת-חבורה ציקלית ונוצרת על ידי  $\omega_n$ . כדאי לציר את  $\Omega_4$  או  $\Omega_6$  כדי להבין למה החבורות נקראות ציקליות.

סענה 3.12. הוכיחו שאם  $G$  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. אם  $H = \{e\}$ , אז  $H = \langle e \rangle$  וסיימנו. מעתה נניח כי  $H$  לא טריוויאלית.

יהי  $0 \neq s \in \mathbb{Z}$  המספר המינימלי בערכו המוחלט כך ש- $a^s \in H$  (אפשר להבטיח ש- $s \in \mathbb{N}$  כי אם  $a^i \in H$ , אז גם  $a^{-i} \in H$  מסגירות להופכי). 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  $k = qs + r$  עם  $0 \leq r < s$ . 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 3.13.** תת־חבורות של  $(\mathbb{Z}, +)$  הן בדיוק  $(n\mathbb{Z}, +)$  עבור  $n \in \mathbb{N} \cup \{0\}$ .

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

הוכחה. נניח  $n | o(a)$ . לכן קיים  $k \in \mathbb{N}$  כך ש- $n = k \cdot o(a)$ . נחשב

$$a^n = a^{k \cdot o(a)} = (a^{o(a)})^k = e^k = e$$

כדרוש. מצד שני, אם  $a^n = e$ , אז  $o(a) \leq n$  ולפי משפט לפי משפט החילוק עם שארית, קיימים  $q$  ו- $r$  שעבורם  $n = q \cdot o(a) + r$  עם  $0 \leq r < o(a)$ . נחשב

$$e = a^n = a^{q \cdot o(a) + r} = (a^{o(a)})^q \cdot a^r = e^q \cdot a^r = a^r$$

אבל  $o(a)$  הוא המספר הטבעי  $i$  הקטן ביותר כך ש- $a^i = e$ , ולכן  $r = 0$ . כלומר  $n = q \cdot o(a)$ .  $\square$

Roots of unity

**תרגיל 3.15.** נסמן את קבוצת שורשי היחידה  $\Omega_\infty = \bigcup_{n=1}^{\infty} \Omega_n$ . הוכיחו:

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

Torsion group

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

פתרון.

1. נוכיח שהיא חבורה על ידי זה שנוכיח שהיא תת-חבורה של  $\mathbb{C}^*$ . תרגיל לבית: אוסף האיברים מסדר סופי של חבורה אבלית הוא תת-חבורה (ובמקרה זה נקרא תת-חבורת הפיתול). לפי הגדרת  $\Omega_\infty$ , 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  $\Omega_\infty$  הן סופיות. אך  $\Omega_\infty$  אינסופית, ולכן לא ייתכן שהיא שווה לאחת מהן.

### 3.2 מכפלה ישרה של חבורות

בנייה חשובה של חבורות חדשות מחבורות קיימות. לתרגיל הבית, כולל מכפלות של יותר מזוג חבורות. תהינה  $(G, *)$  ו- $(H, \bullet)$  חבורות. הזכרו ממתטיקה בדידה בסימון

$$G \times H = \{(g, h) \mid g \in G, h \in H\}$$

טענה 3.16. נגדיר פעולה  $\odot$  על  $G \times H$  רכיב-רכיב, כלומר

$$(g_1, h_1) \odot (g_2, h_2) = (g_1 * g_2, h_1 \bullet h_2)$$

(External) Direct  
product

אז  $(G \times H, \odot)$  היא חבורה, הנקראת המכפלה הישרה (החיצונית) של  $G$  ו- $H$ . איבר היחידה ב- $G \times H$  הוא  $(e_G, e_H)$ .

דוגמה 3.17. נסתכל על  $U_8 \times \mathbb{Z}_3$ . נדגים את הפעולה:

$$(3, 2) \odot (5, 2) = (3 \cdot 5, 2 + 2) = (15, 4) = (7, 1)$$

$$(5, 1) \odot (7, 2) = (5 \cdot 7, 1 + 2) = (35, 3) = (3, 0)$$

האיבר הניטרלי הוא  $(1, 0)$ .

הערה 3.18. מעכשיו, במקום לסמן את הפעולה של  $G \times H$  ב- $\odot$ , נסמן אותה ב- $\cdot$  בשביל הנוחות.

**תרגיל 3.19.** האם  $\mathbb{Z}_n \times \mathbb{Z}_n$  ציקלית (עבור  $n \geq 2$ )?

פתרון. לא! נוכיח שהסדר של כל איבר  $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n$  הוא לכל היותר  $n$ : אכן,

$$(a, b)^n = (a, b) \cdot (a, b) \cdots (a, b) = (a + \cdots + a, b + \cdots + b) = (na, nb) = (0, 0)$$

כיוון שהסדר הוא המספר המינימלי  $m$  שעבורו  $(a, b)^m = (0, 0)$ , בהכרח  $m \leq n$ . כלומר, הסדר של כל איבר ב- $\mathbb{Z}_n \times \mathbb{Z}_n$  הוא לכל היותר  $n$ .

כעת, נסיק כי החבורה הזו אינה ציקלית: כזכור מבדידה,  $|\mathbb{Z}_n \times \mathbb{Z}_n| = n^2$ . אילו החבורה  $\mathbb{Z}_n \times \mathbb{Z}_n$  הייתה ציקלית, היה בה איבר מסדר  $n^2$ . אך אין כזה, ולכן החבורה אינה ציקלית.

הערה 3.20. התרגיל הקודם אומר שמכפלה של חבורות ציקליות אינה בהכרח ציקלית. לעומת זאת, מכפלה של חבורות אבליות נשארת אבלית.

## 4 תרגול רביעי

### 4.1 מבוא לחבורה הסימטרית

**הגדרה 4.1.** החבורה הסימטרית  $S_n$  היא

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

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.

Symmetric group

Permutation

הערה 4.2 (אם יש זמן). החבורה  $S_n$  היא בדיוק חבורת ההפיכים במונואיד  $X^X$  עם פעולת ההרכבה, כאשר  $X = \{1, 2, \dots, n\}$ .

**דוגמה 4.3.** ניקח לדוגמה את  $S_3$ . איבר  $\sigma \in S_3$  הוא מהצורה  $\sigma(1) = i, \sigma(2) = j, \sigma(3) = k$  ו- $i, j, k \in \{1, 2, 3\}$  שונים זה מזה. נסמן בקיצור

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

נכתוב במפורש את כל האיברים ב- $S_3$ :

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



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

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

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

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

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

**מסקנה 4.4.** 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 4.5. 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,  $|S_n| = n \cdot (n-1) \cdot \dots \cdot 1 = n!$ .

**הגדרה 4.6.** 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  $k$ .

Cycle

**דוגמה 4.7.** התמורה  $\sigma \in S_3$  שכתבנו בדוגמה 4.3 היא המחזור  $(1 2 3)$ . שימו לב שלא מדובר בתמורת הזהות!

**דוגמה 4.8.** ב- $S_5$ , המחזור  $(4 5 2)$  מציין את התמורה  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$ .

**משפט 4.9.** כל תמורה ניתנת לכתיבה כהרכבת מחזורים זרים, כאשר הכוונה ב"מחזורים זרים" היא מחזורים שאין להם מספר משותף שהם משנים את מיקומו.

Disjoint cycles

הערה 4.10. שימו לב שמחזורים זרים מתחלפים זה עם זה (מדוע?), ולכן חישובים עם מחזורים יהיו לעיתים קלים יותר מאשר חישובים עם התמורה כמטריצה.

**דוגמה 4.11.** 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  $\sigma^2$ . אפשר ללכת לפי ההגדרה, לעבור על כל מספר ולבדוק לאן  $\sigma^2$  תשלח אותו; אבל, כיוון שמחזורים זרים מתחלפים, נקבל

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

## 4.2 מחלקות

**הגדרה 4.12.** תהי  $G$  חבורה, ותהי  $H \leq G$  תת-חבורה. לכל  $g \in G$ , נגדיר:

Left coset

• המחלקה השמאלית של  $g$  לגבי  $H$  היא  $gH = \{gh \mid h \in H\} \subseteq G$

Right coset

• המחלקה הימנית של  $g$  לגבי  $H$  היא  $Hg = \{hg \mid h \in H\}$

את אוסף המחלקות השמאליות נסמן  $G/H$ .

**דוגמה 4.13.** ניקח את  $G = S_3$ , ונסתכל על תת-החבורה

$$H = \langle (1\ 2\ 3) \rangle = \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\}$$

המחלקות השמאליות של  $H$  ב- $G$ :

$$\begin{aligned} \text{id } H &= \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\} \\ (1\ 2) H &= \{(1\ 2), (2\ 3), (1\ 3)\} \\ (1\ 3) H &= \{(1\ 3), (1\ 2), (2\ 3)\} = (1\ 2) H \\ (2\ 3) H &= \{(2\ 3), (1\ 3), (1\ 2)\} = (1\ 2) H \\ (1\ 2\ 3) H &= \{(1\ 2\ 3), (1\ 3\ 2), \text{id}\} = \text{id } H \\ (1\ 3\ 2) H &= \{(1\ 3\ 2), \text{id}, (1\ 2\ 3)\} = \text{id } H \end{aligned}$$

לכן

$$S_3/H = \{\text{id } H, (1\ 2) H\}$$

**דוגמה 4.14.** ניקח את  $G = (\mathbb{Z}, +)$ , ונסתכל על המחלקות השמאליות של  $H = 5\mathbb{Z}$ :

$$\begin{aligned} 0 + H &= H = \{\dots, -10, -5, 0, 5, 10, \dots\} \\ 1 + H &= \{\dots, -9, -4, 1, 6, 11, \dots\} \\ 2 + H &= \{\dots, -8, -3, 2, 7, 12, \dots\} \\ 3 + H &= \{\dots, -7, -2, 3, 8, 13, \dots\} \\ 4 + H &= \{\dots, -6, -1, 4, 9, 14, \dots\} \\ 5 + H &= \{\dots, -5, 0, 5, 10, 15, \dots\} = H \\ 6 + H &= 1 + H \\ 7 + H &= 2 + H \end{aligned}$$

וכן הלאה. בסך הכל, יש חמש מחלקות שמאליות של  $5\mathbb{Z}$  ב- $\mathbb{Z}$ , וכן

$$\mathbb{Z}/5\mathbb{Z} = \{H, 1 + H, 2 + H, 3 + H, 4 + H\}$$

**דוגמה 4.15.** ניקח את  $G = (\mathbb{Z}_8, +)$ , ונסתכל על  $H = \langle 2 \rangle = \{0, 2, 4, 6\}$ . המחלקות השמאליות הן

$$0 + H = H, 1 + H = \{1, 3, 5, 7\}, 2 + H = H$$

ובאופן כללי,

$$a + H = \begin{cases} H, & \text{if } a \equiv 0 \pmod{2} \\ 1 + H, & \text{if } a \equiv 1 \pmod{2} \end{cases}$$

$$G = H \cup (1 + H) \text{ נשים לב ש-}$$

הערה 4.16. כפי שניתן לראות מהדוגמאות שהצגנו, המחלקות השמאליות (או הימניות) של  $H$  יוצרות חלוקה של  $G$ . נוסף על כך, יחס השוויון בין המחלקות הנוצרות על ידי שני איברים ב- $G$  הינו יחס שקילות.

כלומר עבור  $a, b \in G$  ותת-חבורה  $H \leq G$ , שוויון בין מחלקות  $aH = bH$  משרה יחס שקילות על  $H$  (שבו  $a$  ו- $b$  שקולים). נסכם זאת בעזרת המשפט הבא:

**משפט 4.17.** (בהרצאה). תהי  $G$  חבורה, ותהי  $H \leq G$  תת-חבורה. אזי  $a, b \in G$

$$1. aH = bH \text{ אם ורק אם: } b^{-1}a \in H, \text{ בפרט } aH = H \iff a \in H.$$

$$2. \text{ לכל שתי מחלקות } g_1H \text{ ו-} g_2H, \text{ מתקיים } g_1H = g_2H \text{ או } g_1H \cap g_2H = \emptyset.$$

$$3. \text{ מתקיים } |aH| = |bH| = |H| \text{ לכל } a, b \in G.$$

$$4. \text{ האיחוד של כל המחלקות הוא כל החבורה: } \bigcup_{gH \in G/H} gH = G, \text{ וזהו איחוד זר.}$$

הוכחה. (לבית) זה למעשה תרגיל ממתמטיקה בדידה. נוכיח רק את הסעיף הראשון:  
 $(\Leftarrow)$ : אם  $aH = bH$  אזי לכל  $h \in H, ah \in bH$ . בפרט עבור איבר היחידה  
 $a = ae \in bH$ . מכאן נובע שקיים  $h_0 \in H$  כך ש- $a = bh_0$ , לכן בהכרח  
 $b^{-1}a = h_0 \in H$ .

$(\Rightarrow)$ : נניח ש- $b^{-1}a \in H$ , אזי קיים  $h_0 \in H$  כך ש- $b^{-1}a = h_0$ . לכן  $a = bh_0$ .  
 עתה, לכל  $h \in H$  מתקיים ש- $ah = bh_0h \in bH$ , לכן  $aH \subseteq bH$ . אבל אם  
 $\square$   $bH = aH$ , אזי  $b = ah_0^{-1}$ , ונקבל באותו אופן ש- $bH \subseteq aH$ . לכן בהכרח  $bH = aH$ .

הערה 4.18 (בהרצאה). קיימת התאמה ח"ע ועל בין המחלקות השמאליות  $\{gH \mid g \in G\}$   
 לימניות  $\{Hg \mid g \in G\}$ , לפי  $(Hg \mapsto g^{-1}H)$ :

$$gH \mapsto (gH)^{-1} = \{(gh)^{-1} \mid h \in H\} = \{h^{-1}g^{-1} \mid h \in H\} = \{kg^{-1} \mid k \in H\} = Hg^{-1}$$

לכן מספר המחלקות השמאליות שווה למספר המחלקות הימניות.

**הגדרה 4.19.** נסמן את מספר המחלקות של  $H$  ב- $G$  בסימון  $[G : H]$ . מספר זה נקרא  
 האינדקס של  $H$  ב- $G$ .

**דוגמה 4.20.** על פי הדוגמאות שראינו:

$$1. [\mathbb{Z} : 5\mathbb{Z}] = 5$$

$$2. [S_3 : \langle (1\ 2\ 3) \rangle] = 2$$

$$3. [\mathbb{Z}_8 : \langle 2 \rangle] = 2$$

**תרגיל 4.21.** מצאו חבורה  $G$  ותת-חבורה  $H \leq G$ , כך ש- $[G : H] = \infty$ .

פתרון. תהי  $G = (\mathbb{Q}, +)$  ותת-חבורה  $H = \mathbb{Z}$ .

ניקח שני שברים  $\alpha_1, \alpha_2 \in \mathbb{Q}$  שונים בין 0 לבין 1, ונתבונן במחלקות שאיברים אלו  
 יוצרים. נקבל ש-

$$\{\alpha_1 + 0, \alpha_1 \pm 1, \alpha_1 \pm 2, \dots\} = \alpha_1 H \neq \alpha_2 H = \{\alpha_2 + 0, \alpha_2 \pm 1, \alpha_2 \pm 2, \dots\}$$

לכן, מספר המחלקות של  $H$  ב- $G$  הוא לפחות כמות המספרים ב- $\mathbb{Q}$  בין 0 לבין 1,  
 שהיא אינסופית.

## 5 תרגול חמישי

### 5.1 מבוא לתורת המספרים

**הגדרה 5.1.** בהנתן שני מספרים שלמים  $n, m$  המחלק המשותף המרבי (ממ"מ) 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 ו-5 הם זרים.

הערה 5.2. אם  $d|a$  וגם  $d|b$ , אזי  $d$  מחלק כל צירוף לינארי של  $a$  ו- $b$ .

טענה 5.3. 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  $d = (m, r)$ .  $\square$

Euclidean algorithm

**משפט 5.4** (אלגוריתם אוקלידס). "המתכוון" למציאת מ"מ בעזרת שימוש חוזר בטענה 5.3 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 5.5.** נחשב את המ"מ של 53 ו-47 בעזרת אלגוריתם אוקלידס

$$\begin{aligned} (53, 47) &= [53 = 1 \cdot 47 + 6] \\ (47, 6) &= [47 = 7 \cdot 6 + 5] \\ (6, 5) &= [6 = 1 \cdot 5 + 1] \\ (5, 1) &= 1 \end{aligned}$$

דוגמה נוספת עבור מספרים שאינם זרים:

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

כהערת אגב, מספר השלבים הרב ביותר באלגוריתם יתקבל עבור מספרים עוקבים בסדרת פיבונצ'י. היעילות של האלגוריתם היא  $\log_{\varphi} n$  כאשר  $\varphi$  הוא יחס הזהב.

**משפט 5.6** (איפיון המ"מ כצירוף לינארי מזערי). מתקיים לכל מספרים שלמים  $a, b \neq 0$  כי

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

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

**דוגמה 5.7.** כדי למצוא את המקדמים  $s, t$  כשמביעים את המ"מ כצירוף לינארי כנ"ל נשתמש באלגוריתם אוקלידס המורחב:

Extended Euclidean algorithm

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

ולכן  $(234, 61) = 1 = 6 \cdot 234 - 23 \cdot 61$ . מחישוב זה נקבל כי  $[234] \in U_{61}$ . נבצע מודולו 61 למשוואה האחרונה:

$$1 \equiv 6 \cdot 234 \equiv 6 \cdot 51 \pmod{61}$$

כלומר ההופכי של  $[51] = [234]$  בחבורה  $U_{61}$  הוא  $[6]$ . באופן דומה ההופכי של  $[61] \in U_{234}$  הוא  $[-23] = [211]$ .

**תרגיל 5.8.** 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 5.9. תכונות של ממ"מ:

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

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

3. אם  $p$  ראשוני וגם  $p|ab$ , אזי  $p|a$  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- $1 = sa + tp$ . נכפיל את השויון האחרון ב- $b$  ונקבל  $b = sab + tpb$ . ברור כי  $p$  מחלק את אגף שמאל (הרי  $p|ab$ ), ולכן  $p$  מחלק את אגף ימין, כלומר  $p|b$ .

□

Least common multiple

**הגדרה 5.10.** בהנתן שני מספרים שלמים  $n, m$  הכפולה המשותפת המזערית (כמ"מ) שלהם מוגדרת להיות

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

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

טענה 5.11. 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 5.12** (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  $k$ .

Congruent  
modulo  $n$

**הגדרה 5.13**. 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 יחס זה  $a \equiv b \pmod{n}$  ונקרא זאת "שקול ל- $b$  מודולו  $n$ ".

5.14 (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  $a + c \equiv b + d \pmod{n}$ .

**תרגיל 5.15**. 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.

**תרגיל 5.16** (אם יש זמן). מצאו  $0 \leq x \in \mathbb{Z}$  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  $x = 211$ .

Chinese  
remainder  
theorem

**משפט 5.17** (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 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 5.18**. 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  $s = -1, t = 2$ . ולפי 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 חפיפות (משוואות של שקילות מודולו):

**משפט 5.19** (אם יש זמן). תהא  $\{m_1, \dots, m_k\}$  קבוצת מספרים טבעיים הזרים בזוגות (כלומר כל זוג מספרים בקבוצה הוא זר). נסמן את מכפלתם ב- $m$ . בהנתן קבוצה כלשהי של שאריות  $\{a_i \pmod{m_i} \mid 1 \leq i \leq k\}$ , 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 5.20**. 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 עד 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.



**תרגיל 5.21.** תהי  $G$  חבורה, ויהי  $a \in G$  איבר מסדר  $n \in \mathbb{N}$ . 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 3.14,  $n|dt$ . 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 5.22.** תהי  $G$  חבורה ציקלית מסדר  $n$ . בעזרת התרגיל הקודם מצאו 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  $|U_n|$ .

## 6 תרגול שישי

### 6.1 משפט לגראנז'

**משפט 6.1** (לגראנז'). תהי  $G$  חבורה, ותהי  $H \leq G$  תת-חבורה. אז  $|G| = [G : H] \cdot |H|$ .

Lagrange's  
theorem

**מסקנה 6.2.** עבור חבורה סופית, הסדר של תת-חבורה מחלק את הסדר של החבורה:

$$\frac{|G|}{|H|} = [G : H]$$

בפרט, עבור  $a \in G$ , מפני ש- $\langle a \rangle \leq G$ , אז  $|\langle a \rangle| \mid |G|$ . לכן מפני ש- $o(a) = |\langle a \rangle|$ , הסדר של כל איבר בחבורה מחלק את הסדר של החבורה. לכן גם לכל  $a \in G$  מתקיים  $a^{|G|} = e$ .

**דוגמה 6.3.** עבור  $|\mathbb{Z}_{10}| = 10$ , הסדרים האפשריים של איברים ב- $\mathbb{Z}_{10}$  הם מהקבוצה  $\{1, 2, 5, 10\}$ .

**תרגיל 6.4.** האם לכל מספר  $m$  המחלק את סדר החבורה הסופית  $G$  בהכרח קיים איבר מסדר  $m$ ?

פתרון. לא בהכרח! דוגמה נגדית: נבחן את החבורה  $\mathbb{Z}_4 \times \mathbb{Z}_4$ .

סדר החבורה הינו 16 אבל לא קיים איבר מסדר 16. אילו היה קיים איבר כזה, אזי זו חבורה ציקלית, אבל הוכחנו שהחבורה  $\mathbb{Z}_n \times \mathbb{Z}_n$  אינה ציקלית עבור  $n > 1$ .

Euler's theorem  
Euler's totient  
function

**משפט 6.5** (משפט אוילר). פונקציית אוילר  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  מוגדרת לפי  $\varphi(n) = |U_n|$ . עבור כל  $a \in U_n$ , מתקיים  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

**דוגמה 6.6.**  $(3, 10) = 1$ , לכן  $3 \in U_{10}$ . מאחר ש- $U_{10} = \{1, 3, 7, 9\}$ , אזי  $\varphi(10) = 4$ .  $|U_{10}| = 4$ . אכן מתקיים:  $3^{\varphi(10)} = 3^4 = 81 \equiv 1 \pmod{10}$ .

Fermat's little  
theorem

**משפט 6.7** (המשפט הקטן של פרמה). זה מקרה פרטי של משפט אוילר: עבור ראשוני  $p$ ,  $a^{p-1} \equiv 1 \pmod{p}$  לכל  $a \in U_p$ . מתקיים ש- $o(g) \mid (p-1)$  ובפרט  $a^{p-1} \equiv 1 \pmod{p}$ .

**תרגיל 6.8.** חשב את שתי הספרות האחרונות של המספר  $909^{121}$ .

פתרון. נזכר ש- $\text{mod } n$  הינו יחס שקילות. מפני ש- $909 \equiv 9 \pmod{100}$ , אז נוכל לחשב  $9^{121}$ .

כיוון ש- $(9, 100) = 1$ , אזי על פי משפט אוילר:  $9^{\varphi(100)} = 9^{40} \equiv 1 \pmod{100}$ . מכאן ש- $9^{121} \equiv (9^{40})^3 \cdot 9 \equiv 1^3 \cdot 9 \equiv 9 \pmod{100}$ .

**דוגמה 6.9.** תהי  $G$  חבורה מסדר  $p$  ראשוני. יהי  $e \neq g \in G$ . לכן  $o(g) > 1$ . מצד שני  $o(g) \mid |G| = p$ . לכן בהכרח  $o(g) = p$ , מה שאומר ש- $G = \langle g \rangle$ . מאחר וזה נכון לכל  $e \neq g \in G$ , נסיק ש- $G$  נוצרת על ידי כל אחד מאיבריה שאינו איבר היחידה.

**טענה 6.10.** תהי  $G = \langle \alpha \rangle$  ציקלית מסדר  $n$ , ויהי  $m \mid n$ . אז ל- $G$  יש תת-חבורה ציקלית יחידה מסדר  $m$ .

הוכחה. נסמן  $H = \langle \alpha^{n/m} \rangle$ . זו תת-חבורה מסדר  $m$ , המוכיח קיום. תהי  $K$  תת-חבורה ציקלית נוספת מסדר  $m$ , ונניח  $K = \langle \beta \rangle$ . להוכחת היחידות נראה  $K = H$ . מאחר ש- $\alpha$  יוצר של  $G$ , קיים  $b \leq n$  כך ש- $\beta = \alpha^b$ . לכן לפי תרגיל 5.21,  $o(\beta) = \frac{n}{(n,b)}$ .

אבל  $o(\beta) = m \Leftrightarrow \frac{n}{(n,b)} = m$ . לכן  $(n,b) = \frac{n}{m}$ . לפי תכונת הממ"מ קיימים  $s, t \in \mathbb{Z}$  כך ש- $(n,b) = sn + tb$ . לכן

$$\alpha^{n/m} = \alpha^{(n,b)} = \alpha^{sn+tb} = (\alpha^n)^s (\alpha^b)^t = 1 \cdot \beta^t \in K$$

כלומר קיבלנו ש- $\alpha^{n/m} \in K$ , ולכן  $H \subseteq K$ . אבל על פי ההנחה  $|H| = |K|$ , לכן  $H = K$ . כדרוש.  $\square$

**תרגיל 6.11** (לדלג). כמה תת-חבורות לא טריוויאליות יש ב- $\mathbb{Z}_{30}$ ? (לא טריוויאלית פירושו לא כולל את  $\{0\}$  ואת  $\mathbb{Z}_{30}$ ).

על פי התרגיל, מאחר ומדובר בחבורה ציקלית, מספר תת-החבורות הוא כמספר המחלקים של המספר 30, כלומר:  $|\{1, 2, 3, 5, 6, 10, 15, 30\}| = 8$ . מאחר והסדרים 1 ו-30 מתאימים לתת-החבורות הטריוויאליות, נותרנו עם שש תת-חבורות לא טריוויאליות.

## 6.2 חישוב פונקציית אוילר

לצורך פתרון התרגיל הבא נפתח נוסחה נוחה לחישוב  $\varphi(n)$ . כלומר, בהנתן מספר שלם כלשהו, נוכל לחשב את מספר המספרים הקטנים ממנו בערך מוחלט וזרים לו. על פי המשפט היסודי של האריתמטיקה, כל מספר שלם ניתן לפרק למכפלת חזקות של מספרים ראשוניים (עד כדי סדר וסימן). נניח

$$n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$$

כעת נתבונן בנפרד בפונקציית אוילר של חזקה של מספר ראשוני כלשהו במכפלה, שאותם קל לחשב:

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k \left(1 - \frac{1}{p}\right)$$

ולכן, עבור מספר שלם כלשהו:

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}) = \varphi(p_1^{k_1}) \varphi(p_2^{k_2}) \dots \varphi(p_m^{k_m}) \\ &= p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) \end{aligned}$$

ולסיכום

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

**דוגמה 6.12.** נחשב את  $\varphi(60)$ :

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

**תרגיל 6.13.** חשבו את שתי הספרות האחרונות של  $80732767^{1999} + 2016$ .

פתרון. נפעיל mod100 ונקבל

$$\begin{aligned} 80732767^{1999} + 2016 &\equiv 67^{1999} + 16 = 67^{50 \cdot 40 - 1} + 16 = (67^{40})^{50} \cdot 67^{-1} + 16 \\ &= (67^{\varphi(100)})^{50} \cdot 67^{-1} + 16 \equiv (1)^{50} \cdot 67^{-1} + 16 = 67^{-1} + 16 \end{aligned}$$

כעת נותר למצוא את ההופכי של 67 בחבורה  $U_{100}$  (67 זר ל-100 ולכן נמצא ב- $U_{100}$ ). לצורך כך, נשתמש באלגוריתם של אוקלידס לצורך מציאת פתרון למשוואה  $67x = 1 \pmod{100}$ .

יש פתרון למשוואה אם ורק אם קיים  $k \in \mathbb{Z}$  כך ש- $100k + 67x = 1$ .

בעזרת אלגוריתם אוקלידס נמצא ביטוי של  $\gcd(100, 67)$  כצירוף לינארי של 67 ו-100:

$$\begin{aligned}(100, 67) &= [100 = 1 \cdot 67 + 33] \\(67, 33) &= [67 = 2 \cdot 33 + 1] \\(33, 1) &= 1\end{aligned}$$

ומהצבה לאחור נקבל:  $1 = 67 - 2 \cdot 33 = -2 \cdot 100 + 3 \cdot 67$ , ולכן  $x = 3$ , כלומר ההופכי של 67 הוא 3. לכן  $19 = 3 + 16 = 67^{-1} + 16$ . כלומר שתי הספרות האחרונות הם 19.

**תרגיל 6.14.** הוכיחו את הטענה הבאה: תהא  $G$  חבורה סופית, אזי  $G$  מסדר זוגי  $\Leftrightarrow$  קיים ב- $G$  איבר מסדר 2.  $(\Rightarrow)$ : על פי משפט לגראנז', הסדר של איבר מחלק את סדר החבורה ולכן סדר החבורה זוגי.

$(\Leftarrow)$ : לאיבר מסדר 2 תכונה יחודית - הוא הופכי לעצמו. נניח בשלילה שאין אף איבר ב- $G$  מסדר 2, כלומר שאין אף איבר שהופכי לעצמו, פרט לאיבר היחידה. אז ניתן לסדר את כל איברי החבורה בזוגות, כאשר כל איבר מזווג לאיבר ההופכי לו. ביחד עם איבר היחידה נקבל מספר אי זוגי של איברים ב- $G$  בסתירה להנחה.

**מסקנה 6.15.** לחבורה מסדר זוגי יש מספר אי זוגי של איברים מסדר 2.

### 6.3 תת-חבורה הנוצרת על ידי תת-קבוצה

**6.16 הגדרה.** תהי  $G$  חבורה ותהי  $S \subseteq G$  תת-קבוצה לא ריקה איברים ב- $G$  (שימו לב ש- $S$  אינה בהכרח תת-חבורה של  $G$ ).

Subgroup  
generated by  $S$   
 $S$  generates  $G$   
Finitely  
generated

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  $S$ . אם קיימת  $S$  סופית כך ש- $G = \langle S \rangle$ , נאמר כי  $G$  נוצרת סופית. 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. גם כל חבורה סופית נוצרת סופית.

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

$H \subseteq \mathbb{Z}$  ובפרט  $\mathbb{Z}$ , כיוון ש- $2 \in H$  אזי גם  $(-2) \in H$  ומכאן ש- $1 \in H$ . 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- $H = \mathbb{Z}$ .

**6.18 דוגמה.** אם ניקח  $\{4, 6\} \subseteq \mathbb{Z}$ , אז נקבל:  $\langle 4, 6 \rangle = \{4n + 6m \mid m, n \in \mathbb{Z}\}$ . נטען ש- $\langle 4, 6 \rangle = \gcd(4, 6) \cdot \mathbb{Z} = 2\mathbb{Z}$  (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 גם מתקיים  $2\mathbb{Z} \subseteq \langle 4, 6 \rangle$ .

**דוגמה 6.19.** 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:  $\langle a, b \rangle = \{a^i b^j \mid i, j \in \mathbb{Z}\}$ .

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:

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

הערה 6.20. 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  $A^{-1} = \{a^{-1} \mid a \in A\}$ . מילה היא סדרה סופית של אותיות מן האלפבית, ועבור  $x \in A$  מתקיים  $xx^{-1} = x^{-1}x = \varepsilon$ , כשהמילה הריקה  $\varepsilon$  מייצגת את איבר היחידה ב- $G$ .

## 7 תרגול שביעי

### 7.1 סדר של איברים בחבורה הסימטרית

טענה 7.1 (בתרגיל הבית). תהי  $G$  חבורה. יהיו  $a, b \in G$  כך ש- $ab = ba$  וגם  $\langle a \rangle \cap \langle b \rangle = e$  (כלומר החיתוך בין תת-החבורה הנוצרת על ידי  $a$  ותת-החבורה הנוצרת על ידי  $b$  היא טריוויאלית). אז

$$o(ab) = \text{lcm}(o(a), o(b))$$

**מסקנה 7.2.** סדר מכפלות מחזורים זרים ב- $S_n$  הוא הכפ"מ ( $\text{lcm}$ ) של אורכי המחזורים.

**דוגמה 7.3.** הסדר של (56) (193) הוא 6 והסדר של (56) (1234) הוא 4.

**תרגיל 7.4.** מצאו תת-חבורה מסדר 45 ב- $S_{15}$ .

פתרון. נמצא תמורה מסדר 45 ב- $S_{15}$ . נתבונן באיבר

$$\sigma = (1, 2, 3, 4, 5, 6, 7, 8, 9)(10, 11, 12, 13, 14)$$

$$o(\sigma) = [9, 5] = 45$$

ונשים לב כי  $o(\sigma) = 45$  כעת, מכיוון שסדר האיבר שווה לסדר תת-החבורה שאיבר זה יוצר, נסיק שתת-החבורה  $\langle \sigma \rangle$  עונה על הדרוש.

**שאלה 7.5.** האם קיים איבר מסדר 39 ב- $S_{15}$ ?

פתרון. לא. וזאת מכיוון שאיבר מסדר 39 לא יכול להתקבל כמכפלת מחזורים זרים ב- $S_{15}$ .

אמנם ניתן לקבל את הסדר 39 כמכפלת מחזורים זרים, האחד מאורך 13 והאחר מאורך 3, אבל  $13 + 3 = 16$  ולכן, זה בלתי אפשרי ב- $S_{15}$ .

**הגדרה 7.6.** מחזור מסדר 2 ב- $S_n$  נקרא חילוף.

טענה 7.7 (לדלג). כל מחזור  $(a_1, a_2, \dots, a_r)$  ניתן לרשום כמכפלת חילופים

$$(a_1, a_2, \dots, a_r) = (a_1, a_2) \cdot (a_2, a_3) \dots (a_{r-1}, a_r)$$

ולכן

$$S_n = \langle \{(i, j) \mid 1 \leq i, j \leq n\} \rangle$$

**תרגיל 7.8** (לדלג). כמה מחזורים מאורך  $2 \leq r \leq n$  יש בחבורה  $S_n$ ?

פתרון. זו שאלה קומבינטורית. בוחרים  $r$  מספרים מתוך  $n$  ויש  $\binom{n}{r}$  אפשרויות כאלה. כעת יש לסדר את  $r$  המספרים ב- $r!$  דרכים שונות. אבל ספרנו יותר מידי אפשרויות, כי יש  $r$  מחזורים זהים, שהרי

$$(a_1, \dots, a_r) = (a_2, \dots, a_r, a_1) = \dots = (a_r, a_1, \dots, a_{r-1})$$

לכן נחלק את המספר הכולל ב- $r$ . נקבל שמספר המחזורים מאורך  $r$  ב- $S_n$  הינו  $\binom{n}{r} \cdot (r-1)!$ .

**תרגיל 7.9.** מה הם הסדרים האפשריים לאיברי  $S_4$ ?

פתרון. ב- $S_4$  הסדרים האפשריים הם:

1. סדר 1 - רק איבר היחידה.
  2. סדר 2 - חילופים  $(i, j)$  או מכפלה של שני חילופים זרים, למשל (34) (12).
  3. סדר 3 - מחזורים מאורך 3, למשל (243).
  4. סדר 4 - מחזורים מאורך 4, למשל (2431).
- וזהו! כלומר הצלחנו למיין בצורה פשוטה ונוחה את כל הסדרים האפשריים ב- $S_4$ .

**תרגיל 7.10.** מה הם הסדרים האפשריים לאיברי  $S_5$ ?

פתרון. ב- $S_5$  הסדרים האפשריים הם:

1. סדר 1 - רק איבר היחידה.
  2. סדר 2 - חילופים  $(i, j)$  או מכפלה של שני חילופים זרים.
  3. סדר 3 - מחזורים מאורך 3.
  4. סדר 4 - מחזורים מאורך 4.
  5. סדר 5 - מחזורים מאורך 5.
  6. סדר 6 - מכפלה של חילוף ומחזור מאורך 3, למשל (54) (231).
- וזהו! שימו לב שב- $S_n$  יש איברים מסדר שגדול מ- $n$  עבור  $n \geq 5$ .

## 7.2 מערכת הצפנה RSA

RSA  
cryptosystem

דוגמה לשימוש בתורת החבורות הוא מערכת הצפנה RSA, המממשת שיטה להצפנה אסימטרית המובססת על רעיון המפתח הציבורי. נראה דוגמה להרצה של אלגוריתם RSA (על שם רון ריבסט, עדי שמיר ולאונרד אדלמן) הנלקחה מויקיפדיה.

**המטרה:** בוב מעוניין לשלוח לאליס הודעה באופן מוצפן.

**יצירת המפתחות:** אליס בוחרת שני מספרים ראשוניים  $p, q$  באופן אקראי (בפועל מאוד גדולים). היא מחשבת את המספרים  $n = pq$  ואת  $\varphi(n) = (p-1)(q-1)$ . בנוסף היא בוחרת מספר  $e > 1$  הזר ל- $\varphi(n)$  שנקרא המעריך להצפנה (בפועל  $65537 = 2^{16} + 1$  או מספר די קטן אחר). היא מוצאת הופכי כפלי  $d$  של  $e$  בחבורה  $U_{\varphi(n)}$  שיהווה את המפתח הסודי שלה. כלומר היא מוצאת מספר המקיים  $de \equiv 1 \pmod{\varphi(n)}$ , למשל על ידי אלגוריתם אוקלידס המורחב. זהו שלב שאין צורך לחזור עליו.

**הפצת המפתח הציבורי:** אליס שולחת באופן אמין, אך לא בהכרח מוצפן, את המפתח הציבורי  $(n, e)$  לבוב (או לעולם). את המפתח הסודי  $d$  היא שומרת בסוד לעצמה. גם זהו שלב שאין צורך לחזור עליו.

**הצפנה:** בוב ישלח הודעה  $M$  לאליס בצורת מספר  $m$  המקיים  $0 \leq m < n$ . הוא ישלח את ההודעה המוצפנת  $c \equiv m^e \pmod{n}$ . באופן נאיבי, יש מספר סופי של הודעות שונות שבוב יכול לשלוח.

**פענוח:** אליס תשחזר את ההודעה  $m$  בעזרת המפתח הסודי  $m \equiv c^d \equiv m^{ed} \pmod{n}$ .

**דוגמה 7.11.** נציג דוגמה עם מספרים קטנים מאוד. אליס תבחר למשל את  $p = 61$  ואת  $q = 53$  היא תחשב

$$n = pq = 3233 \quad \varphi(n) = (p-1)(q-1) = 3120$$

היא תבחר מעריך הצפנה  $e = 17$ , שאכן זר ל- $\varphi(n) = 3120$ . המפתח הסודי שלה הוא

$$d \equiv e^{-1} \equiv 2753 \pmod{3120}$$

וכדי לסיים את שני השלבים הראשונים באלגוריתם היא תפרסם את המפתח הציבורי שלה  $(n, e)$ .

נניח ובוב רוצה לשלוח את ההודעה  $m = 65$  לאליס. הוא יחשב את ההודעה המוצפנת

$$c \equiv m^{17} \equiv 2790 \pmod{3233}$$

וישלח את  $c$  לאליס. כעת אליס תפענח אותה על ידי חישוב

$$m \equiv 2790^{2753} \equiv 65 \pmod{3233}$$

החישובים בשלבי הביניים של חזקות מודולריות יכולים להעשות בשיטות יעילות מאוד הנעזרות במשפט השאריות הסיני, או על ידי חישוב חזקה בעזרת ריבועים (שיטה הנקראת גם העלאה בינארית בחזקה). למשל לחישוב  $m^{17}$  נשים לב שבסיס בינארי  $17 = 10001_2$ , ולכן במקום  $17 - 1 = 16$  הכפלות מודולריות נסתפק בחישוב:

$$\begin{aligned} m^1 &\equiv m \cdot 1 \equiv 65 \pmod{3233} \\ m^2 &\equiv (m)^2 \equiv 992 \pmod{3233} \\ m^4 &\equiv (m^2)^2 \equiv 1232 \pmod{3233} \\ m^8 &\equiv (m^4)^2 \equiv 1547 \pmod{3233} \\ m^{16} &\equiv (m^8)^2 \equiv 789 \pmod{3233} \\ m^{17} &\equiv m (m^8)^2 \equiv 2790 \pmod{3233} \end{aligned}$$

נשים לב שכאשר כפלנו ב- $m$  (שורה ראשונה ואחרונה) זה מקביל לסיביות הדלוקות ב- $10001_2$ , ואילו כאשר העלנו בריבוע, זה מקביל למספר הסיביות (פחות 1). בקיצור

$$m^k = \begin{cases} \left(m^{\lfloor \frac{k}{2} \rfloor}\right)^2 & k \text{ זוגי} \\ m \left(m^{\lfloor \frac{k}{2} \rfloor}\right)^2 & k \text{ אי זוגי} \end{cases}$$

כלומר כאשר נחשב  $m^k$  עבור  $k$  כלשהו נוכל להסתפק ב- $\lfloor \log_2 k \rfloor$  פעולות של העלאה בריבוע ולכל היותר ב- $\lfloor \log_2 k \rfloor$  הכפלות מודולריות, במקום  $k - 1$  הכפלות מודולריות ב- $m$ . בבית תדרשו לחישוב של  $2790^{2753}$  בעזרת שיטה זו.

הערה 7.12 (אזהרה!). יש לדעת שממש לא כדאי להשתמש בפונקציות קריפטוגרפיות שמיימשתם לבד לצרכים חשובים. ללא בחינה מדוקדקת על ידי מומחים בתחום לגבי רמת בטיחות ונכונות הקוד, ישנן התקפות רבות שאפשר לנצל לגבי מימושים שכאלו כמו בחירת פרמטרים לא בטוחים, יצירת מפתחות לא בטוחים, התקפת אדם בתווך, התקפת ערוץ צדדי ועוד ועוד.

## 8 תרגול שמיני

### 8.1 חבורות מוצגות סופית

Presentation

נראה דרך לכתובה של חבורות שנקראת "יצוג על ידי יוצרים ויחסים". בהנתן יצוג

$$G = \langle X \mid R \rangle$$

נאמר ש- $G$  נוצרת על ידי הקבוצה  $X$  של היוצרים עם קבוצת היחסים  $R$ . כלומר כל איבר בחבורה  $G$  ניתן לכתובה (לאו דווקא יחידה) כמילה סופית ביוצרים והופכיהם, ושכל אחד מן היחסים הוא מילה ששווה לאיבר היחידה.



**דוגמה 8.1.** יצוג של חבורה ציקלית מסדר  $n$  הוא

$$\mathbb{Z}_n \cong \langle x \mid x^n \rangle$$

כל איבר הוא חזקה של היוצר  $x$ , ושכאשר רואים את תת-המילה  $x^n$  אפשר להחליף אותה ביחידה. לנוחות, בדרך כלל קבוצת היחסים תכתב עם שיויונות, למשל  $x^n = e$ . באופן דומה, החבורה הציקלית האינסופית ניתנת ליצוג

$$\mathbb{Z} \cong \langle x \mid \emptyset \rangle$$

ובדרך כלל משמיטים את קבוצת היחסים אם היא ריקה. ודאו שאתם מבינים את ההבדל בין החבורות הלא איזומורפיות

$$\mathbb{Z} \times \mathbb{Z} \cong \langle x, y \mid xy = yx \rangle, \quad F_2 \cong \langle x, y \mid \emptyset \rangle$$

**הגדרה 8.2.** ראינו שחבורה שיש לה קבוצת יוצרים סופית נקראת חבורה נוצרת סופית. אם לחבורה יש יצוג שבו גם קבוצת היוצרים סופית וגם קבוצת היחסים סופית, נאמר שהחבורה מוצגת סופית.

Finitely  
presented

**דוגמה 8.3.** כל חבורה ציקלית היא מוצגת סופית, וראינו מה הם היצוגים המתאימים. כל חבורה סופית היא מוצגת סופית (זה לא טריוויאלי). נסו למצוא חבורה נוצרת סופית שאינה מוצגת סופית (זה לא כל כך קל).

## 8.2 החבורה הזיהדרלית

**הגדרה 8.4.** עבור מספר טבעי  $n$ , הקבוצה  $D_n$  של סיבובים ושיקופים המעתיקים מצולע משוכלל בין  $n$  צלעות על עצמו, היא החבורה הזיהדרלית פזרנה  $n$ , יחד עם הפעולת של הרכבת פונקציות.

Dihedral group

מיוונית, פירוש השם "די-הדרה" הוא שתי פאות, ומשה ירדן הציע במילונו את השם חבורת הפאתיים ל- $D_n$ .

אם  $\sigma$  הוא סיבוב ב- $\frac{2\pi}{n}$  ו- $\tau$  הוא שיקוף סביב ציר סימטריה כלשהו, אז יצוג סופי מקובל של  $D_n$  הוא

$$D_n = \langle \sigma, \tau \mid \sigma^n = \tau^2 = \text{id}, \sigma\tau = \tau\sigma^{-1} \rangle$$

הערה 8.5 (אם יש זמן). פונקציה  $\alpha : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  שהיא חח"ע ועל ושומרת מרחק (כלומר  $d(x, y) = d(\alpha(x), \alpha(y))$ ) נקראת איזומטריה. אוסף האיזומטריות עם הפעולה של הרכבת פונקציות הוא חבורה. תהי  $L \subseteq \mathbb{R}^2$  קבוצה כך שעבור איזומטריה  $\alpha$  מתקיים  $\alpha(L) = L$ . במקרה זה  $\alpha$  נקראת סימטריה של  $L$ . אוסף הסימטריות של  $L$  הוא תת-חבורה של האיזומטריות. החבורה  $D_n$  היא בדיוק אוסף הסימטריות של מצולע משוכלל בן  $n$  צלעות.

Isometry

Symmetry

**דוגמה 8.6.** החבורה  $D_3$  נוצרת על ידי סיבוב  $\sigma$  של  $120^\circ$  ועל ידי שיקוף  $\tau$ , כך שמתקיימים היחסים הבאים בין היוצרים:  $\sigma^3 = \tau^2 = \text{id}$ ,  $\tau\sigma\tau = \sigma^{-1}$ . כלומר  $D_3 = \{\text{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$  (להדגים עם משולש מה עושה כל איבר, וכנ"ל עבור  $D_5$ ). מה לגבי האיבר  $\sigma\tau \in D_3$ ? הוא מופיע ברשימת האיברים תחת שם אחר, שכן

$$\begin{aligned}\tau\sigma\tau &= \sigma^{-1} \\ \sigma\tau &= \tau^{-1}\sigma^{-1} = \tau\sigma^2\end{aligned}$$

לכן  $\sigma\tau = \tau\sigma^2$ . כך גם הראנו כי  $D_3$  אינה אבלית.

סיכום 8.7. איברי  $D_n$  הם

$$\{\text{id}, \sigma, \sigma^2, \dots, \sigma^{n-1}, \tau, \tau\sigma, \tau\sigma^2, \dots, \tau\sigma^{n-1}\}$$

בפרט נקבל כי  $|D_n| = 2n$  ושעבור  $n > 2$  החבורה אינה אבלית כי  $\tau\sigma \neq \sigma\tau$ . (למי שכבר מכיר איזומורפיזמים ודאו שאתם מבינים כי  $D_3 \cong S_3$ , אבל עבור  $n > 3$  החבורות  $D_n$  ו- $S_n$  אינן איזומורפיות.)

### 8.3 הומומורפיזמים

**הגדרה 8.8.** תהינה  $(G, *)$ ,  $(H, \bullet)$  חבורות. העתקה  $f: G \rightarrow H$  תקרא הומומורפיזם של חבורות אם מתקיים

$$\forall x, y \in G, \quad f(x * y) = f(x) \bullet f(y)$$

נכין מילון קצר לסוגים שונים של הומומורפיזמים:

Group  
homomorphism

Monomorphism

1. הומומורפיזם שהוא חח"ע נקרא מונומורפיזם או שייכון. נאמר כי  $G$  משוכנת ב- $H$  אם קיים שייכון  $f: G \hookrightarrow H$ .

Epimorphism

2. הומומורפיזם שהוא על נקרא אפימורפיזם. נאמר כי  $H$  היא תמונה אפימורפית של  $G$  אם קיים אפימורפיזם  $f: G \twoheadrightarrow H$ .

Epimorphic

image

Isomorphism

3. הומומורפיזם שהוא חח"ע ועל נקרא איזומורפיזם. נאמר כי  $G$  ו- $H$  איזומורפיות אם קיים איזומורפיזם  $f: G \rightarrow H$ . נסמן זאת  $G \cong H$ .

Isomorphic

groups

Automorphism

4. איזומורפיזם  $f: G \rightarrow G$  נקרא אוטומורפיזם של  $G$ .

5. בכיתה נקצר את השמות של הומומורפיזם, מונומורפיזם, אפימורפיזם, איזומורפיזם ואוטומורפיזם להומ', מונו', אפי', איזו' ואוטו', בהתאמה.

8.9 הערה. העתקה  $f: G \rightarrow H$  היא איזומורפיזם אם ורק אם קיימת העתקה  $g: H \rightarrow G$  כך ש- $f \circ g = \text{id}_H$  וגם  $g \circ f = \text{id}_G$ .

אפשר להוכיח (נסו!) שההעתקה  $g$  הזו היא הומומורפיזם בעצמה. כלומר כדי להוכיח שהומומורפיזם  $f$  הוא איזומורפיזם מספיק למצוא העתקה הפוכה  $g = f^{-1}$ . אפשר גם לראות שאיזומורפיות היא תכונה רפלקסיבית, סימטרית וטרנזיטיבית (היא לא יחס שקילות כי מחלקת החבורות היא גדולה מכדי להיות קבוצה).

**תרגיל 8.10.** הנה רשימה של כמה העתקות בין חבורות. קבעו האם הן הומומורפיזמים, ואם כן מהו סוגן:

1.  $\varphi: \mathbb{R} \rightarrow \mathbb{R}^*$  המוגדרת לפי  $x \mapsto e^x$  היא מונומורפיזם. מה היה קורה אם היינו מחליפים למרוכבים?

2. יהי  $F$  שדה. אז  $\det: GL_n(F) \rightarrow F^*$  היא אפימורפיזם. הרי

$$\det(AB) = \det(A) \det(B)$$

וכדי להוכיח שההעתקה על אפשר להסתכל על מטריצה אלכסונית עם ערכים  $(x, 1, \dots, 1)$  באלכסון.

3.  $\varphi: \mathbb{R} \rightarrow \mathbb{R}^*$  המוגדרת לפי  $x \mapsto x$  אינה הומומורפיזם כלל.

4.  $\varphi: \mathbb{Z}_2 \rightarrow \Omega_2$  המוגדרת לפי  $1 \mapsto 1, 0 \mapsto -1$  היא איזומורפיזם. הראתם בתרגיל בית שכל החבורות מסדר 2 הן למעשה איזומורפיות.

העובדה שהעתקה  $f: G \rightarrow H$  היא הומומורפיזם גוררת כמה תכונות מאוד נוחות:

1.  $f(e_G) = e_H$

2.  $f(g^n) = f(g)^n$  לכל  $n \in \mathbb{Z}$

3.  $f(g^{-1}) = f(g)^{-1}$ , כמקרה פרטי של הסעיף הקודם.

Kernel

4. הגרעין של  $f$ , כלומר  $\ker f = \{g \in G \mid f(g) = e_H\}$ , הוא תת-חבורה נורמלית של  $G$  (בהמשך נסביר מה זה "תת-חבורה נורמלית").

Image

5. התמונה של  $f$ , כלומר  $\text{im } f = \{f(g) \mid g \in G\}$ , היא תת-חבורה של  $H$ .

6. אם  $G \cong H$ , אז  $|G| = |H|$ .

**דוגמה 8.11.** התכונות האלו של הומומורפיזמים מזכירות, ולא במקרה, מה שלומדים באלגברה לינארית. יהיו  $V, W$  מרחבים וקטוריים מעל שדה  $F$ . העתקה לינארית  $T: V \rightarrow W$  היא (גם) הומומורפיזם של חבורות. נניח  $\dim V = \dim W$ , האם בהכרח  $T$  איזומורפיזם?

8.12. הערה. ידוע שהעתקה לינארית נקבעת באופן יחיד על ידי תמונה של בסיס. באופן דומה, אם  $G = \langle S \rangle$ , אז תמונת הומומורפיזם  $f: G \rightarrow H$  נוצרת על ידי  $f(S)$ . שימו לב שלא כל קביעה של תמונה של קבוצת יוצרים (אפילו של יוצר אחד) תגדיר הומומורפיזם. למשל  $\varphi: \mathbb{Z}_n \rightarrow \mathbb{Z}$  המוגדרת לפי  $\varphi([1]) = 1$  אינה מגדירה הומומורפיזם ואינה מוגדרת היטב. מצד אחד

$$\varphi([n]) = \varphi([1] + \dots + [1]) \stackrel{?}{=} \varphi([1]) + \dots + \varphi([1]) = n$$

ומצד שני  $\varphi([n]) = 0$ . באופן כללי, יש לבדוק שכל היחסים שמתקיימים בין היוצרים, מתקיימים גם על תמונות היוצרים, כדי שיוגדר הומומורפיזם.

**תרגיל 8.13.** יהי  $f: G \rightarrow H$  הומומורפיזם. הוכיחו כי לכל  $g \in G$  מסדר סופי מתקיים  $|o(f(g))| \mid o(g)$ .

הוכחה. נסמן  $n = o(g)$ . לפי הגדרה  $g^n = e_G$ . נפעיל את  $f$  על המשוואה ונקבל

$$f(g^n) = f(g)^n = e_H = f(e_G)$$

ולכן  $|o(f(g))| \mid n$ . □

**תרגיל 8.14.** האם כל שתי חבורות מסדר 4 הן איזומורפיות?

פתרון. לא! נבחר  $G = \mathbb{Z}_2 \times \mathbb{Z}_2$  ואת  $H = \mathbb{Z}_4$ . נשים לב כי ב- $H$  יש איבר מסדר 4. אילו היה איזומורפיזם  $f: G \rightarrow H$ , אז הסדר של איבר מסדר 4, כמו  $1 \in H$ , היה מחלק את הסדר של המקור. בחבורה  $G$  כל האיברים מסדר 1 או 2, לכן הדבר לא יתכן, ולכן החבורות לא איזומורפיות.

בנוסף, איזומורפיזם שומר על סדר האיברים, ולכן בחבורות איזומורפיות הרשימות של סדרי האיברים בחבורות, הן שוות.

טענה 8.15 (לבית). יהי  $f: G \rightarrow H$  הומומורפיזם. הוכיחו שאם  $G$  אבלית, אז  $\text{im } f$  אבלית. הסיקו שאם  $G \cong H$ , אז  $G$  אבלית אם ורק אם  $H$  אבלית.

**תרגיל 8.16.** יהי  $f: G \rightarrow H$  הומומורפיזם. הוכיחו שאם  $G$  ציקלית, אז  $\text{im } f$  ציקלית.

הוכחה. נניח  $G = \langle a \rangle$ . נטען כי  $\text{im } f = \langle f(a) \rangle$ . יהי  $x \in \text{im } f$  איבר כלשהו. לכן יש איבר  $g \in G$  כך ש- $f(g) = x$  (כי  $\text{im } f$  היא תמונה אפימורפית של  $G$ ). מפני ש- $G$  ציקלית קיים  $k \in \mathbb{Z}$  כך ש- $g = a^k$ . לכן

$$x = f(g) = f(a^k) = f(a)^k$$

וקיבלנו כי  $x \in \langle f(a) \rangle$ , כלומר כל איבר בתמונה הוא חזקה של  $f(a)$ . הסיקו שכל החבורות הציקליות מסדר מסוים הן איזומורפיות. □

**תרגיל 8.17.** האם קיים איזומורפיזם  $f: S_3 \rightarrow \mathbb{Z}_6$ ?

פתרון. לא, כי  $S_3$  לא אבלית ואילו  $\mathbb{Z}_6$  כן.

**תרגיל 8.18.** האם קיים איזומורפיזם  $f: (\mathbb{Q}^+, \cdot) \rightarrow (\mathbb{Q}, +)$ ?

פתרון. לא. נניח בשלילה כי  $f$  הוא אכן איזומורפיזם. לכן  $f(a^2) = f(a) + f(a)$ . נסמן  $c = f(3)$ , ונשים לב כי  $c = \frac{c}{2} + \frac{c}{2}$ . מפני ש- $f$  היא על, אז יש מקור ל- $\frac{c}{2}$  ונסמן אותו  $f(x) = \frac{c}{2}$ .

קיבלנו אפוא את המשוואה

$$f(x^2) = f(x) + f(x) = c = f(3)$$

ומפני ש- $f$  היא חח"ע, קיבלנו  $x^2 = 3$ . אך זו סתירה כי  $\sqrt{3} \notin \mathbb{Q}$ .

**תרגיל 8.19.** האם קיים אפימורפיזם  $f: H \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_3$  כאשר  $H = \langle 5 \rangle \leq \mathbb{R}^*$ ?

פתרון. לא. נניח בשלילה שקיים  $f$  כזה. מפני ש- $H$  היא ציקלית, אז גם  $\text{im } f$  היא ציקלית. אבל  $f$  היא על, ולכן נקבל כי  $\text{im } f = \mathbb{Z}_3 \times \mathbb{Z}_3$ . אך זו סתירה כי החבורה  $\mathbb{Z}_3 \times \mathbb{Z}_3$  אינה ציקלית.

**תרגיל 8.20.** האם קיים מונומורפיזם  $f: GL_2(\mathbb{Q}) \rightarrow \mathbb{Q}^{10}$ ?

פתרון. לא. נניח בשלילה שקיים  $f$  כזה. נתבונן בצמצום  $\text{im } f$  של  $f: GL_2(\mathbb{Q}) \rightarrow \mathbb{Q}^{10}$ , שהוא איזומורפיזם (להדגיש כי זהו אפימורפיזם ומפני ש- $f$  חח"ע, אז  $\bar{f}$  היא איזומורפיזם). ידוע לנו כי  $\text{im } f \leq \mathbb{Q}^{10}$ , ולכן  $\text{im } f$  אבליית. כלומר גם  $GL_2(\mathbb{Q})$  אבליית, שזו סתירה.

**מסקנה.** יתכנו ארבע הפרכות ברצף.

**תרגיל 8.21.** מתי ההעתקה  $i: G \rightarrow G$  המוגדרת לפי  $i(g) = g^{-1}$  היא אוטומורפיזם?

פתרון. ברור שההעתקה הזו מחבורה לעצמה היא חח"ע ועל. כעת נשאר לבדוק שהיא שומרת על הפעולה (כלומר הומומורפיזם). יהיו  $g, h \in G$  ונשים לב כי

$$i(gh) = (gh)^{-1} = h^{-1}g^{-1} = i(h)i(g) = i(hg)$$

וזה יתקיים אם ורק אם  $gh = hg$ . כלומר  $i$  היא אוטומורפיזם אם ורק אם  $G$  אבליית. כהערת אגב, השם של ההעתקה נבחר כדי לסמן inversion.

Cayley's theorem

**תרגיל 8.22.** (משפט קיילי). תהי  $G$  חבורה. הוכיחו שקיים מונומורפיזם  $G \hookrightarrow S_G$ . תזכורת: האוסף  $S_X$  של הפונקציות ההפיכות ב- $X^X$  יחד עם פעולת ההרכבה נקרא חבורת הסימטריה על  $X$ .

הוכחה. לכל  $g \in G$  מוגדרת פונקציה חח"ע ועל  $l_g \in S_G$  לפי כפל משמאל  $l_g(a) = ga$ . נגדיר פונקציה  $\Phi: G \hookrightarrow S_G$  לפי  $\Phi(g) = l_g$ . תחילה נראה ש- $\Phi$  הומומורפיזם. כלומר צריך להוכיח שלכל  $g, h \in G$  מתקיים

$$l_g \circ l_h = l_{gh}$$

הפונקציות שוות אם ורק אם לכל  $a \in G$  הן יסכימו על תמונת  $a$ :

$$(l_g \circ l_h)(a) = l_g(l_h(a)) = l_g(ha) = gha = l_{gh}(a)$$

ולכן  $\Phi$  הומומורפיזם. כדי להראות שהוא חח"ע, נניח  $l_g = l_h$ . אז מתקיים

$$g = g \cdot e_G = l_g(e_G) = l_h(e_G) = h \cdot e_G = h$$

□

לכן  $g = h$ , ולכן  $G$  משוכנת ב- $S_G$ .

**מסקנה 8.23.** כל חבורה סופית  $G$  מסדר  $n$  איזומורפית לתת-חבורה של  $S_n$ .

**מסקנה 8.24.** יהי  $F$  שדה. כל חבורה סופית  $G$  מסדר  $n$  איזומורפית לתת-חבורה של  $GL_n(F)$ .

רמז להוכחה: הראו ש- $S_n$  איזומורפית לתת-חבורה של  $GL_n(F)$ .

אתגר: מצאו מונומורפיזם  $G \hookrightarrow GL_{n-1}(F)$  קודם נסו לשכן את  $S_n$  ב- $GL_{n-1}(F)$ .

**תרגיל 8.25.** (רשות). תהי  $G$  חבורה מסדר 6. הוכיחו שאם  $G$  אבליית, אז  $G \cong \mathbb{Z}_6$ , ושם  $G$  לא אבליית, אז  $G \cong S_3$ .

## 9 תרגול תשיעי

### 9.1 סימן של תמורה וחבורת החילופין

Sign הגדרה 9.1. יהי  $\sigma$  מחזור מאורך  $k$ , אזי הסימן שלו מוגדר להיות:

$$\text{sign}(\sigma) = (-1)^{k-1}$$

עבור תמורות  $\tau, \sigma \in S_n$  נגדיר

$$\text{sign}(\sigma\tau) = \text{sign}(\sigma)\text{sign}(\tau)$$

תכונה זו מאפשרת לחשב את הסימן של כל תמורה ב- $S_n$ . יש דרכים שקולות אחרות להגדיר סימן של תמורה.

Even permutation נקרא לתמורה שסימנה 1 בשם תמורה זוגית ולתמורה שסימנה -1 בשם תמורה אי זוגית.

Odd permutation

### 9.2 דוגמה (נקודה חשובה ומאוד מבלבלת)

1. החילוף (35) הוא תמורה אי זוגית.

2. התמורה הריקה היא תמורה זוגית.

3. מחזור מאורך אי זוגי הוא תמורה זוגית.

Alternating group

9.3 הגדרה חבורת החילופין (או חבורת התמורות הזוגיות)  $A_n$  היא תת-החבורה הבאה של  $S_n$ :

$$A_n = \{\sigma \in S_n \mid \text{sign}(\sigma) = 1\}$$

9.4 הערה הסדר של  $A_n$  הינו  $\frac{n!}{2}$ .

9.5 הגדרה  $A_3 = \{\text{id}, (123), (132)\}$

נשים לב כי  $A_3 = \langle (123) \rangle$  כלומר  $A_3$  ציקלית.

### 9.2 תת-חבורות נורמליות

Normal subgroup

9.6 הגדרה תת-חבורה  $H \leq G$  נקראת תת-חבורה נורמלית אם לכל  $g \in G$  מתקיים  $gH = Hg$ . במקרה זה נסמן  $H \triangleleft G$ .

9.7 משפט תהי תת-חבורה  $H \leq G$ . התנאים הבאים שקולים:

1.  $H \triangleleft G$

2. לכל  $g \in G$  מתקיים  $g^{-1}Hg = H$

3. לכל  $g \in G$  מתקיים  $g^{-1}Hg \subseteq H$

4.  $H$  היא גרעין של הומומורפיזם (שהתחום שלו הוא  $G$ ).

הוכחה חלקית. קל לראות כי סעיף 1 שקול לסעיף 2. ברור כי סעיף 2 גורר את סעיף 3, ובכיוון השני נשים לב כי אם  $g^{-1}Hg \subseteq H$  וגם  $gHg^{-1} \subseteq H$  נקבל כי

$$H = gg^{-1}Hg^{-1} \subseteq g^{-1}Hg \subseteq H$$

□ קל להוכיח שסעיף 4 גורר את האחרים, ובכיוון השני יש צורך בהגדרת חבורות מנה.

**דוגמה 9.8.** אם  $G$  חבורה אבלית, אז כל תת-חבורות שלה הן נורמליות. הרי אם  $h \in H \leq G$ , אז  $g^{-1}hg = h \in H$ . ההפך לא נכון. ברמת האיברים נורמליות לא שקולה לכך ש- $gh = hg$ !

**דוגמה 9.9.** מתקיים  $SL_n(F) \triangleleft GL_n(F)$ . אפשר לראות זאת לפי הצמדה. יהי  $A \in SL_n(F)$ , אז לכל  $g \in GL_n(F)$  מתקיים

$$\det(g^{-1}Ag) = \det(g^{-1}) \det(A) \det(g) = \det(g)^{-1} \cdot 1 \cdot \det(g) = 1$$

ולכן  $g^{-1}Ag \in SL_n(F)$ .

דרך אחרת להוכחה היא לשים לב כי  $SL_n(F)$  היא הגרעין של ההומומורפיזם  $\det: GL_n(F) \rightarrow F^*$ . אתגר: הסיקו מדוגמה זו כי  $A_n \triangleleft S_n$ .

**דוגמה 9.10.** עבור  $n \geq 3$ , תת-חבורה  $\langle \tau \rangle \leq D_n$  אינה נורמלית כי  $\langle \tau \rangle \neq \sigma \langle \tau \rangle \sigma$ .

9.11. תהי  $H \leq G$  תת-חבורה מאינדקס 2. אזי  $H \triangleleft G$ .

הוכחה. אנו יודעים כי יש רק שתי מחלקות שמאליות של  $H$  בתוך  $G$ , ורק שתי מחלקות ימניות. אחת מן המחלקות היא  $H$ . אם איבר  $a \notin H$ , אז המחלקה השמאלית האחרת היא  $aH$ , והמחלקה הימנית האחרת היא  $Ha$ . מכיוון ש- $G$  היא איחוד של המחלקות נקבל

$$H \cup aH = G = H \cup Ha$$

□ ומפני שהאיחוד בכל אגף הוא זר נקבל  $aH = Ha$ .

**מסקנה 9.12.** מתקיים  $\langle \sigma \rangle \triangleleft D_n$  כי לפי משפט לגראנז'  $2 \mid \frac{2n}{n} = 2$ .  $[D_n : \langle \sigma \rangle] = \frac{2n}{n} = 2$ .

9.13. אם  $K \leq H \leq G$  וגם  $K \triangleleft G$ , אז בוודאי  $K \triangleleft H$ . ההפך לא נכון. אם  $H \triangleleft G$  וגם  $K \triangleleft H$ , אז לא בהכרח  $K \triangleleft G$ ! למשל  $D_4 \triangleleft \langle \tau, \sigma^2 \rangle \triangleleft D_4$  לפי הטענה הקודמת, אבל ראינו כי  $\langle \tau \rangle$  לא נורמלית ב- $D_4$ .

**תרגיל 9.14.** תהי  $G$  חבורה. יהיו  $H, N \leq G$  תת-חבורות. נגדיר מכפלה של תת-חבורות להיות

$$HN = \{hn \mid h \in H, n \in N\}$$

הוכיחו כי אם  $N \triangleleft G$ , אז  $HN \leq G$ . אם בנוסף  $H \triangleleft G$ , אז  $HN \triangleleft G$ .

פתרון. חבורה היא סגורה להופכי, כלומר  $H^{-1} = H$ , וסגורה למכפלה ולכן  $HH = H$ . מפני ש- $G \triangleleft N$  נקבל כי לכל  $h \in H$  מתקיים  $hN = Nh$ , ולכן  $HN = NH$ . שימו לב שזה לא אומר שבהכרח  $nh = hn$ ! אלא שקיימים  $n' \in N$  וגם  $h' \in H$  כך ש- $nh = h'n'$ .

נשים לב כי  $HN \neq \emptyset$  כי  $e = e \cdot e \in HN$ . נוסיף הסבר (מיותר) עם האיברים של תת-החבורות בשורה השנייה, שבו נניח  $h_i \in H$  וגם  $n_i \in N$ . נבדוק סגירות למכפלה של  $HN$ :

$$HNHN = HHNN = HN$$

$$h_1n_1h_2n_2 = h_1h_2'n_1n_2 = h_3n_3$$

וסגירות להופכי

$$(HN)^{-1} = N^{-1}H^{-1} = NH = HN$$

$$(h_1n_1)^{-1} = n_1^{-1}h_1^{-1} = n_2h_2 = h_2'n_2'$$

ולכן  $HN \leq G$ .

אם בנוסף  $H \triangleleft G$ , אז לכל  $g \in G$  מתקיים  $g^{-1}Hg = H$  ולכן

$$g^{-1}HNg = g^{-1}Hgg^{-1}Ng = (g^{-1}Hg)(g^{-1}Ng) = HN$$

ולכן  $HN \triangleleft G$ . מה קורה אם לא  $N$  ולא  $H$  נורמליות ב- $G$ ?

**דוגמה 9.15.** הגדרנו בתרגיל בית את המִרְכָּז של חבורה  $G$  להיות

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

דהיינו זהו האוסף של כל האיברים ב- $G$  שמתחלפים עם כל איברי  $G$ . שימו לב שתמיד  $Z(G) \triangleleft G$  וכי  $Z(G)$  אבלי. האם תת-חבורה נורמלית היא בהכרח אבלי? כבר ראינו שלא, למשל עבור  $GL_2(\mathbb{R}) \triangleleft SL_2(\mathbb{R})$ .

### 9.3 חבורות מנה

נתבונן באוסף המחלקות השמאליות  $G/H = \{gH \mid g \in G\}$  של תת-חבורה  $H \leq G$ . אם (ורק אם)  $H \triangleleft G$ , אפשר להגדיר על אוסף זה את הפעולה הבאה כך שתקבל חבורה:

$$(aH)(bH) = aHHb = aHb = abH$$

כאשר בשיויונות בצדדים השתמשנו בנורמליות. פעולה זו מוגדרת היטב (ודאו!), ואיבר היחידה בחבורה זו הוא  $eH = H$ . החבורה  $G/H$  נקראת חבורת המנה של  $G$  ביחס ל- $H$ , ולעיתים נקרא זאת " $G$  מודולו  $H$ ". מקובל גם הסימון  $G/H$ .

Center

Quotient group,  
or factor group



**דוגמה 9.16.**  $\mathbb{Z}$  היא חבורה ציקלית, ובפרט אבלית. ברור כי  $n\mathbb{Z} \triangleleft \mathbb{Z}$ . נשים לב כי

$$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}$$

כלומר האיברים בחבורה זו הם מן הצורה  $k + n\mathbb{Z}$  כאשר  $0 \leq k \leq n-1$ . הפעולה היא

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) \pmod{n} + n\mathbb{Z}$$

אפשר לראות כי  $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$  לפי ההעתקה  $k + n\mathbb{Z} \mapsto k \pmod{n}$ . שימו לב כי  $\mathbb{Z}/n\mathbb{Z}$  אינה תת-חבורה של  $\mathbb{Z}$ , למשל כי האיברים שונים (או כי אין ב- $\mathbb{Z}$  איברים מסדר סופי, פרט לאיבר היחידה).

**דוגמה 9.17.** לכל חבורה  $G$  יש שתי תת-חבורות טריוויאליות  $\{e\}$  ו- $G$ , ושתיהן נורמליות. ברור כי  $[G : G] = 1$ , ולכן  $G/G \cong \{e\}$ . דרך אחרת לראות זאת היא לפי ההומומורפיזם הטריוויאלי  $f: G \rightarrow G$  המוגדר לפי  $e \mapsto g$ . ברור כי  $\ker f = G$ . מה לגבי  $G/\{e\}$ ? האיברים הם מן הצורה  $\{g\}$ . העתקת הזהות  $\text{id}: G \rightarrow G$  היא איזומורפיזם, שהגרעין שלו הוא  $\{e\}$ . אפשר גם לבנות איזומורפיזם  $f: G/\{e\} \rightarrow G$  לפי  $f: \{g\} \mapsto g$ . ודאו שאתם מבינים למה זה אכן איזומורפיזם.

**דוגמה 9.18.** תהי  $G = \mathbb{R} \times \mathbb{R}$ , ונתבונן ב- $G$   $H = \mathbb{R} \times \{0\}$ . האיברים בחבורת המנה הם

$$G/H = \{(a, b) + H \mid (a, b) \in G\} = \{\mathbb{R} \times \{b\}\}_{b \in \mathbb{R}}$$

כלומר אלו הם הישרים המקבילים לציר ה- $x$ .

הערה 9.19. עבור חבורה סופית  $G$  ותת-חבורה  $H \triangleleft G$  מתקיים כי

$$|G/H| = [G : H] = \frac{|G|}{|H|}$$

**תרגיל 9.20.** תהי  $G$  חבורה (לאו דווקא סופית), ותהי  $H \triangleleft G$  כך ש- $[G : H] = n < \infty$ . הוכיחו כי לכל  $a \in G$  מתקיים כי  $a^n \in H$ .

פתרון. נזכיר כי אחת מן המסקנות מלגראנז' היא שבחבורה סופית  $K$  מתקיים לכל  $k \in K$  כי  $k^{|K|} = e$ . יהי  $a \in G$ , אזי  $aH \in G/H$ . ידוע לנו כי  $|G/H| = n$ . ולכן

$$a^n H = (aH)^n = e_{G/H} H = H$$

כלומר קיבלנו  $a^n \in H$ .

**תרגיל 9.21.** תהי  $H \leq G$  תת-חבורה מאינדקס 2. הוכיחו כי  $G/H$  היא חבורה ואבלית.

פתרון. ראינו כבר שאם  $[G : H] = 2$ , אז  $H \triangleleft G$ . כמו כן  $[G : H] = 2$ . החבורה היחידה מסדר 2 (שהוא ראשוני), עד כדי איזומורפיזם, היא  $\mathbb{Z}_2$  שהיא אבלית. לכן  $G/H$  היא חבורה אבלית.

**תרגיל 9.22.** תהי  $G$  חבורה, ויהי  $T$  אוסף האיברים מסדר סופי ב- $G$ . בתרגיל בית הראתם שאם  $G$  אבלית, אז  $T \leq G$ . הוכיחו:

1. אם  $T \leq G$  (למשל אם  $G$  אבלית), אז  $T \triangleleft G$ .

2. בנוסף, בחבורת המנה  $G/T$  איבר היחידה הוא היחיד מסדר סופי.

פתרון. נתחיל עם הסעיף הראשון. יהי  $a \in T$ , ונניח  $o(a) = n$ . לכל  $g \in G$  מתקיים כי

$$(g^{-1}ag)^n = g^{-1}agg^{-1}ag \dots g^{-1}ag = g^{-1}a^n g = e$$

ולכן  $g^{-1}Tg \subseteq T$ . כלומר  $T \triangleleft G$ .

עבור הסעיף השני, נניח בשלילה כי קיים איבר  $xT \in G/T$  מסדר סופי  $e_{G/T} \neq xT$ .  $o(xT) = n$ . איבר היחידה הוא  $e_{G/T} = T$ , ולכן  $x \notin T$ . מתקיים  $(xT)^n = T$ , ונקבל כי  $x^n \in T$ . אם  $x^n \in T$  מסדר סופי, אז קיים  $m$  כך ש- $(x^n)^m = e$ . לכן  $x^{nm} = e$ , וקיבלנו כי  $x \in T$  שזו סתירה.

דוגמאות ל- $T \leq G$ : אם  $G$  חבורה סופית, אז  $T = G$ , וכבר ראינו  $G \triangleleft G$ , ואז  $G/T \cong \{e\}$ . אם  $G = \mathbb{C}^*$ , אז  $G/T = \Omega_\infty = \bigcup_n \Omega_n$ . כלומר כל מספר מרוכב לא אפסי עם ערך מוחלט השונה מ-1 הוא מסדר אינסופי.

## 10 תרגול עשרי

### 10.1 משפט האיזומורפיזם של נתר

**משפט 10.1** (משפט האיזומורפיזם הראשון). יהי הומומורפיזם  $f: G \rightarrow H$ . אז

$$G/\ker f \cong \text{im } f$$

בפרט, יהי אפימורפיזם  $\varphi: G \rightarrow H$ . אז  $G/\ker \varphi \cong H$ .

**תרגיל 10.2.** תהי  $G = \mathbb{R} \times \mathbb{R}$ , ותהי  $H = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = 3x\}$ . הוכיחו כי  $G/H \cong \mathbb{R}$ .

הוכחה. ראשית, נשים לב למשמעות הגיאומטרית:  $H$  היא ישר עם שיפוע 3 במישור. נגדיר  $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$  לפי  $f(x, y) = 3x - y$ . ודאו שזהו הומומורפיזם.  $f(\frac{x}{3}, 0) = x$  כמו כן,  $f$  אפימורפיזם, כי  $f(x, y) = 0$  אם ורק אם  $y = 3x$ .

$$\ker f = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid f(x, y) = 0\} = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid 3x - y = 0\} = H$$

□ לפי משפט האיזומורפיזם הראשון, נקבל את הדרוש.

**תרגיל 10.3.** נסמן  $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ . זו חבורה כפלית. הוכיחו כי  $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$ .

הוכחה. נגדיר  $f: \mathbb{R} \rightarrow \mathbb{T}$  לפי  $f(x) = e^{2\pi i x}$ . זהו הומומורפיזם, כי

$$f(x+y) = e^{2\pi i(x+y)} = e^{2\pi i x + 2\pi i y} = e^{2\pi i x} \cdot e^{2\pi i y} = f(x) f(y)$$

$f$  היא גם אפימורפיזם, כי כל  $z \in \mathbb{T}$  ניתן לכתוב כ- $e^{2\pi i x}$  עבור  $x \in \mathbb{R}$  כלשהו. נחשב את הגרעין:

$$\ker f = \{x \in \mathbb{R} \mid e^{2\pi i x} = 1\} = \mathbb{Z}$$

לפי משפט האיזומורפיזם הראשון, נקבל

$$\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$$

□

**תרגיל 10.4.** יהי הומומורפיזם  $f: \mathbb{Z}_{14} \rightarrow D_{10}$ . מה יכול להיות  $\ker f$ ?

פתרון. נסמן  $K = \ker f$ . מכיוון ש- $K \triangleleft \mathbb{Z}_{14}$ , אז  $|\mathbb{Z}_{14}/K| = 14/|K|$ . לכן  $|K| \in \{1, 2, 7, 14\}$ . נבדוק עבור כל מקרה.

אם  $|K| = 1$ , אז  $f$  הוא חח"ע וממשפט האיזומורפיזם הראשון נקבל  $\mathbb{Z}_{14}/K \cong \text{im } f$ . לכן  $\mathbb{Z}_{14} \cong \text{im } f \leq D_{10}$  ויודע לנו כי  $\text{im } f \leq D_{10}$  ולכן  $|\text{im } f| = 14$  אבל 14 אינו מחלק את 20, ולכן  $|K| \neq 1$ .

אם  $|K| = 2$ , אז בדומה לחישוב הקודם נקבל

$$|\text{im } f| = |\mathbb{Z}_{14}/K| = \frac{|\mathbb{Z}_{14}|}{|K|} = 7$$

שוב מפני ש-7 אינו מחלק את 20 נסיק כי  $|K| \neq 2$ .

אם  $|K| = 7$ , נראה כי קיים הומומורפיזם כזה. ניקח תת-חבורה  $H = \{\text{id}, \tau\}$  של  $D_{10}$  ונבנה אפימורפיזם  $\mathbb{Z}_{14} \rightarrow H \leq D_{10}$ . המספרים האי זוגיים ישלחו ל- $\tau$ , והזוגיים לאיבר היחידה. כמו כן, כיוון שהגרעין הוא מסדר ראשוני, אז  $K \cong \mathbb{Z}_7$ .

אם  $|K| = 14$ , אז נקבל  $K = \mathbb{Z}_{14}$ . תוצאה זאת מתקבלת עבור הומומורפיזם הטריוויאלי.

**תרגיל 10.5.** תהינה  $G_1$  ו- $G_2$  חבורות סופיות כך ש- $(|G_1|, |G_2|) = 1$ . מצאו את כל ההומומורפיזמים  $f: G_1 \rightarrow G_2$ .

פתרון. נניח כי  $f: G_1 \rightarrow G_2$  הומומורפיזם. לפי משפט האיזומורפיזם הראשון,

$$G_1/\ker f \cong \text{im } f \Rightarrow \frac{|G_1|}{|\ker f|} = |G_1/\ker f| = |\text{im } f| \Rightarrow |\text{im } f| \mid |G_1|$$

כמו כן,  $\text{im } f \leq G_2$ , ולכן, לפי משפט לגראנז',  $|\text{im } f| \mid |G_2|$ . אבל  $(|G_1|, |G_2|) = 1$ , ולכן  $|\text{im } f| = 1$  - כלומר  $f$  היא הומומורפיזם הטריוויאלי.

**תרגיל 10.6** (אם יש זמן). מצאו את כל התמונות האפימורפיות של  $D_4$  (עד כדי איזומורפיזם).

פתרון. לפי משפט האיזומורפיזם הראשון, כל תמונה אפימורפית של  $D_4$  איזומורפית למנה  $D_4/H$ , עבור  $H \triangleleft D_4$ . לכן מספיק לדעת מיהן כל תת־החבורות הנורמליות של  $D_4$ .

קודם כל, יש לנו את תת־החבורות הטריטיואליות  $D_4 \triangleleft D_4$ ,  $\{id\}$ ; לכן, קיבלנו את התמונות האפימורפיות  $D_4/\{id\} \cong D_4$  ו- $D_4/D_4 \cong \{id\}$ .  
 כעת, אנו יודעים כי  $\langle \sigma^2 \rangle \triangleleft D_4 = Z(D_4)$ . ננסה להבין מיהי  $D_4/\langle \sigma^2 \rangle$ . רעיון לניחוש: אנחנו יודעים, לפי לגראנז', כי זו חבורה מסדר 4. כמו כן, אפשר לבדוק שכל איבר  $x \in D_4/\langle \sigma^2 \rangle$  מקיים  $x^2 = e$ . לכן ננחש שזו  $\mathbb{Z}_2 \times \mathbb{Z}_2$  (ובהמשך נדע להגיד זאת בלי למצוא איזומורפיזם ממש). נגדיר  $f: D_4 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$  לפי  $f(\tau^i \sigma^j) = (i, j)$ . קל לבדוק שזהו אפימורפיזם עם גרעין  $\langle \sigma^2 \rangle$ , ולכן, לפי משפט האיזומורפיזם הראשון,

$$D_4/\langle \sigma^2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

נשים לב כי  $\langle \sigma \rangle \triangleleft D_4$ , כי זו תת־חבורה מאינדקס 2. אנחנו גם יודעים שכל החבורות מסדר 2 איזומורפיות זו לזו, ולכן

$$D_4/\langle \sigma \rangle \cong \mathbb{Z}_2$$

גם  $\langle \sigma^2, \tau \rangle, \langle \sigma^2, \tau \sigma \rangle \triangleleft D_4$  מאותו נימוק, וכן

$$D_4/\langle \sigma^2, \tau \rangle \cong D_4/\langle \sigma^2, \tau \sigma \rangle \cong \mathbb{Z}_2$$

צריך לבדוק האם יש עוד תת־חבורות נורמליות. נזכור שבתרגיל הבית מצאתם את כל תת־החבורות של  $D_4$ . לפי הרשימה שהכנתם, קל לראות שכתבנו את כל תת־החבורות מסדר 4, ואת  $\langle \sigma^2 \rangle$ . תת־החבורות היחידות שעוד לא הזכרנו הן מהצורה  $\langle \tau \sigma^i \rangle = \{id, \tau \sigma^i\}$  כדי שהיא תהיה נורמלית, צריך להתקיים

$$H \ni \tau (\tau \sigma^i) \tau^{-1} = \sigma^i \tau = \tau \sigma^{4-i}$$

לכן בהכרח  $i = 2$ . אבל אז

$$\sigma (\tau \sigma^2) \sigma^{-1} = (\sigma \tau) \sigma = \tau \sigma^{-1} \sigma = \tau \notin H$$

ולכן  $H \not\triangleleft D_4$ . מכאן שכתבנו את כל תת־החבורות הנורמליות של  $D_4$ , ולכן כל התמונות האפימורפיות של  $D_4$  הן  $D_4$ ,  $\mathbb{Z}_2 \times \mathbb{Z}_2$ , ו- $\mathbb{Z}_2$ .

**תרגיל 10.7**. תהי  $G$  חבורה. הוכיחו: אם  $G/Z(G)$  היא ציקלית, אזי  $G$  אבלי.

הוכחה.  $G/Z(G)$  ציקלית, ולכן קיים  $a \in G$  שעבורו  $G/Z(G) = \langle aZ(G) \rangle$ . כמו כן, אנחנו יודעים כי

$$G = \bigcup_{g \in G} gZ(G)$$

(כי כל חבורה היא איחוד המחלקות של תת-חבורה). כעת,  $gZ(G) \in G/Z(G)$ , ולכן קיים  $i$  שעבורו

$$gZ(G) = (aZ(G))^i = a^i Z(G)$$

(לפי הציקליות). אם כן, מתקיים

$$G = \bigcup_{i \in \mathbb{Z}} a^i Z(G)$$

כעת נראה ש- $G$  אבליה. יהיו  $g, h \in G$ . לכן קיימים  $i, j \in \mathbb{Z}$  שעבורם

$$g \in a^i Z(G), h \in a^j Z(G)$$

כלומר קיימים  $g', h' \in Z(G)$  שעבורם  $g = a^i g'$  ו- $h = a^j h'$ . לכן,

$$gh = a^i g' a^j h' = a^i a^j g' h' = a^j a^i h' g' = a^j h' a^i g' = hg$$

הוכחנו שלכל  $g, h \in G$  מתקיים  $gh = hg$ , ולכן  $G$  אבליה.  $\square$

**מסקנה 10.8.** אם  $G$  אבליה, אז מתקיים  $Z(G) = G$ , ומכאן ש- $G/Z(G) = \{e\}$ . כלומר, אם  $G/Z(G)$  ציקלית, אזי היא טריוויאלית.

**הגדרה 10.9.** תהי  $G$  חבורה, ויהי  $a \in G$ . האוטומורפיזם  $\gamma_a: G \rightarrow G$  המוגדר לפי  $\gamma_a(g) = aga^{-1}$  נקרא אוטומורפיזם פנימי. נסמן

$$\text{Inn}(G) = \{\gamma_a \mid a \in G\}$$

החבורה הזו נקראת חבורת האוטומורפיזמים הפנימיים של  $G$ .

**תרגיל 10.10.** הוכיחו כי  $\gamma_a \circ \gamma_b = \gamma_{ab}$ , וכי  $\gamma_a^{-1} = \gamma_{a^{-1}}$ . הסיקו כי  $\text{Inn}(G)$  היא חבורה עם פעולת ההרכבה.

הוכחה. לכל  $g \in G$  מתקיים

$$(\gamma_a \circ \gamma_b)(g) = \gamma_a(\gamma_b(g)) = a(bgb^{-1})a^{-1} = (ab)g(ab)^{-1} = \gamma_{ab}(g)$$

לכן הוכחנו את החלק הראשון. נשים לב כי  $\gamma_e = \text{id}_G$ , ולכן

$$\begin{cases} \gamma_a \circ \gamma_{a^{-1}} = \gamma_{aa^{-1}} = \gamma_e = \text{id}_G \\ \gamma_{a^{-1}} \circ \gamma_a = \gamma_{a^{-1}a} = \gamma_e = \text{id}_G \end{cases} \Rightarrow \gamma_a^{-1} = \gamma_{a^{-1}}$$

$\square$

**תרגיל 10.11.** הוכיחו כי לכל חבורה  $G$ ,

$$G/Z(G) \cong \text{Inn}(G)$$

הוכחה. נגדיר  $f: G \rightarrow \text{Inn}(G)$  לפי  $f(g) = \gamma_g$ . זהו הומומורפיזם, לפי התרגיל שהוכחנו. מובן שהוא על (לפי הגדרת  $\text{Inn}(G)$ ). נחשב את הגרעין:

$$\begin{aligned} \ker f &= \{g \in G \mid \gamma_g = \text{id}_G\} = \{g \in G \mid \forall h \in G : \gamma_g(h) = h\} \\ &= \{g \in G \mid \forall h \in G : ghg^{-1} = h\} = \{g \in G \mid \forall h \in G : gh = hg\} = Z(G) \end{aligned}$$

לפי משפט האיזומורפיזם הראשון, נקבל

$$G/Z(G) \cong \text{Inn}(G)$$

□

## 11 תרגול אחד עשר

### 11.1 פעולת ההצמדה

Conjugates

**11.1 הגדרה**. תהי  $G$  חבורה. אומרים שאיברים  $g$  ו- $h$  צמודים, אם קיים  $a \in G$  שעבורו  $h = aga^{-1}$ . זה מגדיר יחס שקילות על  $G$ , שבו מחלקת השקילות של כל איבר נקראת מחלקת הצמידות שלו.

Conjugacy class

**11.2 דוגמה**. בחבורה אבלית  $G$ , אין שני איברים שונים הצמודים זה לזה; נניח כי  $g$  ו- $h$  צמודים. לכן, קיים  $a \in G$  שעבורו

$$h = aga^{-1} = gaa^{-1} = g$$

באופן כללי, אם  $G$  חבורה כלשהי אזי  $g \in Z(G)$  אם ורק אם מחלקת הצמידות של  $g$  היא  $\{g\}$ .

**11.3 תרגיל**. תהי  $G$  חבורה, ויהי  $g \in G$  מסדר סופי  $n$ . הוכיחו:

1. אם  $h \in G$  צמוד ל- $g$ , אזי  $o(h) = n$ .

2. אם אין עוד איברים ב- $G$  מסדר  $n$ , אזי  $g \in Z(G)$ .

הוכחה.

1.  $g$  ו- $h$  צמודים, ולכן קיים  $a \in G$  שעבורו  $h = aga^{-1}$ . נשים לב כי

$$h^n = (aga^{-1})^n = \underbrace{aga^{-1}aga^{-1} \dots aga^{-1}}_{n \text{ times}} = ag^n a^{-1} = aa^{-1} = e$$

זה מוכיח ש- $o(h) \leq n$ . מצד שני, אם  $o(h) = m$ , אזי

$$g^m = (a^{-1}ha)^m = a^{-1}h^m a = e$$

ולכן  $o(g) = n \leq m$ . בסך הכל,  $o(h) = m = n$ .

2. יהי  $h \in G$ . לפי הסעיף הראשון,  $o(hgh^{-1}) = n$ . אבל נתון ש- $g$  הוא האיבר היחיד מסדר  $n$  ב- $G$ , ולכן  $hgh^{-1} = g$ . נכפול ב- $h$  מימין, ונקבל ש- $hg = gh$ . הוכחנו שלכל  $h \in G$  מתקיים  $hg = gh$ , ולכן  $g \in Z(G)$ .

□

הערה 11.4. הכיוון ההפוך בכל סעיף אינו נכון. למשל, אפשר לקחת את  $\mathbb{Z}_4$ . שם  $o(1) = o(3) = 4$ , אבל הם לא צמודים; כמו כן, שניהם במרכז, ולכל אחד מהם יש איבר אחר מאותו סדר.

**דוגמה 11.5.** בחבורה  $D_3$ , האיבר  $\sigma$  צמוד לאיבר

$$\tau\sigma\tau^{-1} = \tau\sigma\tau = \sigma^2$$

אין עוד איברים צמודים להם, כי אין עוד איברים מסדר 3 ב- $D_3$ .

**תרגיל 11.6.** תהי  $\sigma \in S_n$ , ויהי מחזור  $(a_1, a_2, \dots, a_k) \in S_n$ . הוכיחו כי

$$\sigma(a_1, a_2, \dots, a_k)\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \dots, \sigma(a_k))$$

הוכחה. נסו לראות את הקשר לשיטת  $\text{decorate-sort-undecorate}$ , כשכאן המחזור ממוין לפי הסדר ש- $\sigma$  קובעת. נראה שהתמורות פועלות באותו אופן על  $\{1, 2, \dots, n\}$ . ראשית, נניח כי  $m = \sigma(a_i)$  עבור איזשהו  $1 \leq i \leq k$ . התמורה באגף ימין תשלח את  $m$  ל- $\sigma(a_{i+1})$ . נסתכל מה קורה באגף שמאל:

$$\begin{aligned} (\sigma(a_1, a_2, \dots, a_k)\sigma^{-1})(m) &= \sigma((a_1, a_2, \dots, a_k)(\sigma^{-1}(\sigma(a_i)))) \\ &= \sigma((a_1, a_2, \dots, a_k)(a_i)) = \sigma(a_{i+1}) \end{aligned}$$

ולכן התמורות פועלות אותו דבר על  $\sigma(a_1), \dots, \sigma(a_k)$ . כעת נניח כי  $m$  אינו מהצורה  $\sigma(a_i)$  לאף  $1 \leq i \leq k$ , ולכן התמורה באגף ימין תשלח אותו לעצמו. לגבי אגף שמאל: נשים לב כי  $\sigma^{-1}(m) \neq a_i$  לכל  $i$ , ולכן

$$(\sigma(a_1, a_2, \dots, a_k)\sigma^{-1})(m) = \sigma((a_1, a_2, \dots, a_k)(\sigma^{-1}(m))) = \sigma(\sigma^{-1}(m)) = m$$

□

מכאן ששתי התמורות הדרושות שוות.

**תרגיל 11.7.** נתונות ב- $S_6$  התמורות  $a = (1, 5, 3, 6)$ ,  $\sigma = (1, 3)(4, 5, 6)$  ו- $\tau = (2, 4, 5)$ . חשבו את:

1.  $\sigma a \sigma^{-1}$

2.  $\tau a \tau^{-1}$

פתרון. לפי הנוסחה מתרגיל 11.6,

$$\sigma a \sigma^{-1} = (3, 6, 1, 4)$$

$$\tau a \tau^{-1} = (1, 2, 3, 6)$$

**מסקנה 11.8** (לבית).  $S_n = \langle (1, 2), (1, 2, \dots, n) \rangle$ .

**הגדרה 11.9**. תהי  $\sigma \in S_n$  תמורה. נפרק אותה למכפלה של מחזורים זרים  $\sigma = \sigma_1 \sigma_2 \dots \sigma_k$ . נניח כי האורך של  $\sigma_i$  הוא  $r_i$ , וכי  $r_1 \geq r_2 \geq \dots \geq r_k$ . נגדיר את מבנה המחזורים של  $\sigma$  להיות ה- $k$ -יה הסדורה  $(r_1, r_2, \dots, r_k)$ .

Cycle type

**דוגמה 11.10**. מבנה המחזורים של  $(5, 6)(1, 2, 3)$  הוא  $(3, 2)$ ; מבנה המחזורים של  $(4, 2, 2)(1, 5)(4, 2, 3)$  גם הוא  $(3, 2)$ ; מבנה המחזורים של  $(7, 8)(5, 6)(1, 2, 3, 4)$  הוא  $(4, 2, 2)$ .

**מסקנה 11.11**. שתי תמורות צמודות ב- $S_n$  אם ורק אם יש להן אותו מבנה מחזורים. למשל, התמורה  $(5, 6)(1, 2, 3)$  צמודה ל- $(1, 5)(4, 2, 3)$  ב- $S_8$ , אבל הן לא צמודות לתמורה  $(7, 8)(5, 6)(1, 2, 3, 4)$  ב- $S_8$ .

הוכחה. (אם יש זמן, או רק לעבור על הרעיון)

$(\Leftarrow)$  תהיינה  $\sigma, \tau \in S_n$  שתי תמורות צמודות ב- $S_n$ . נכתוב  $\tau = \pi \sigma \pi^{-1}$ . נניח כי  $\sigma = \sigma_1 \sigma_2 \dots \sigma_k$  הפירוק של  $\sigma$  למכפלה של מחזורים זרים; לכן

$$\tau = \pi \sigma \pi^{-1} = \pi \sigma_1 \sigma_2 \dots \sigma_k \pi^{-1} = (\pi \sigma_1 \pi^{-1}) (\pi \sigma_2 \pi^{-1}) \dots (\pi \sigma_k \pi^{-1})$$

לפי התרגיל הקודם, כל תמורה מהצורה  $\pi \sigma_i \pi^{-1}$  היא מחזור; כמו כן, קל לבדוק כי כל שני מחזורים שונים כאלו זרים זה לזה (כי  $\sigma_1, \sigma_2, \dots, \sigma_k$  זרים זה לזה). לכן, קיבלנו פירוק של  $\tau$  למכפלה של מחזורים זרים, וכל אחד מהמחזורים האלו הוא מאותו האורך של המחזורים ב- $\sigma$ . מכאן נובע של- $\sigma$  ול- $\tau$  אותו מבנה מחזורים.

$(\Rightarrow)$  תהיינה  $\sigma, \tau \in S_n$  עם אותו מבנה מחזורים. נסמן  $\sigma = \sigma_1 \sigma_2 \dots \sigma_k$ ,  $\tau = \tau_1 \tau_2 \dots \tau_k$  כאשר  $\sigma_i = (a_{i,1}, a_{i,2}, \dots, a_{i,m_i})$  ו- $\tau_i = (b_{i,1}, b_{i,2}, \dots, b_{i,m_i})$ . הם מחזורים זרים וגם  $\tau_1, \dots, \tau_k$  הם מחזורים זרים. נגדיר תמורה  $\pi$  כך:  $\pi(a_{i,j}) = b_{i,j}$  וכל שאר האיברים נשלחים לעצמם. נשים לב כי

$$\begin{aligned} \pi \sigma_i \pi^{-1} &= \pi(a_{i,1}, a_{i,2}, \dots, a_{i,m_i}) \pi^{-1} = (\pi(a_{i,1}), \pi(a_{i,2}), \dots, \pi(a_{i,m_i})) = \\ &= (b_{i,1}, b_{i,2}, \dots, b_{i,m_i}) = \tau_i \end{aligned}$$

ולכן

$$\pi \sigma \pi^{-1} = \pi \sigma_1 \sigma_2 \dots \sigma_k \pi^{-1} = (\pi \sigma_1 \pi^{-1}) (\pi \sigma_2 \pi^{-1}) \dots (\pi \sigma_k \pi^{-1}) = \tau_1 \tau_2 \dots \tau_k = \tau$$

□

מכאן ש- $\sigma$  ו- $\tau$  צמודות ב- $S_n$ .

**מסקנה 11.12**. הוכיחו כי  $Z(S_n) = \{\text{id}\}$  לכל  $n \geq 3$ .



הוכחה. תהי  $a \in Z(S_n)$ , ונניח בשלילה כי  $a \neq \text{id}$ . תהי  $a \neq b \in S_n$  תמורה שונה מ- $a$  עם אותו מבנה מחזורים כמו של  $a$ . לפי התרגיל שפתרנו, קיימת  $\sigma \in S_n$  שעבורה  $\sigma a \sigma^{-1} = b$ , אבל  $a \in Z(S_n)$ , ולכן נקבל

$$b = \sigma a \sigma^{-1} = a \sigma \sigma^{-1} = a$$

בסתירה לבחירה של  $b$ . לכן בהכרח  $a = \text{id}$ , כלומר  $Z(S_n) = \{\text{id}\}$ .  $\square$

Partition

**11.13 הגדרה**. חלוקה של  $n$  היא סדרה לא עולה של מספרים טבעיים  $n_1 \geq \dots \geq n_k > 0$  כך ש- $n = n_1 + \dots + n_k$ . את מספר החלוקות של  $n$  מסמנים  $\rho(n)$ .

**11.14 מסקנה**. מספר מחלקות הצמידות ב- $S_n$  הוא  $\rho(n)$ .

**11.15 תרגיל**. כמה מחלקות צמידות יש ב- $S_5$ ?

פתרון. נייעזר במסקנה האחרונה, ונכתוב את 5 כסכומים של מספרים טבעיים:

$$\begin{aligned} 5 &= 5 \\ 5 &= 4 + 1 \\ 5 &= 3 + 2 \\ 5 &= 3 + 1 + 1 \\ 5 &= 2 + 2 + 1 \\ 5 &= 2 + 1 + 1 + 1 \\ 5 &= 1 + 1 + 1 + 1 + 1 \end{aligned}$$

ולכן  $\rho(5) = 7$ .

**11.16 תרגיל**. יהיו  $\sigma, \tau \in A_n$ , ונניח של- $\sigma$  ול- $\tau$  אותו מבנה מחזורים. האם  $\sigma$  ו- $\tau$  צמודות ב- $A_n$ ?

פתרון. לא! למשל, ניקח  $n = 3$ . אנחנו יודעים כי  $A_3$  היא חבורה מגודל 3, ולכן היא ציקלית, ובפרט אבליה. לפי הדוגמה שראינו בתחילת התרגול, נקבל כי כל איבר ב- $A_3$  צמוד רק לעצמו. בפרט,  $(1, 2, 3), (1, 3, 2) \in A_3$  אינם צמודים ב- $A_3$ . אבל הם צמודים ב- $S_3$ , כי יש להם אותו מבנה מחזורים.

Centralizer

**11.17 הגדרה** (מתרגילי הבית). תהי  $G$  חבורה. עבור איבר  $a \in G$  נגדיר את המרכז של  $a$  להיות

$$C_G(a) = \{g \in G \mid ga = ag\}$$

**11.18 תרגיל**. מצאו את  $C_{S_5}(\sigma)$  עבור  $\sigma = (1, 2, 5)$ .

פתרון. במילים אחרות, צריך למצוא את התמורות המתחלפות עם  $\sigma$ . תמורה  $\tau$  מתחלפת עם  $\sigma$  אם ורק אם  $\tau\sigma = \sigma\tau$  אם ורק אם  $\tau\sigma\tau^{-1} = \sigma$ , לכן, צריך למצוא אילו תמורות משאירות את  $\sigma$  במקום כשמצידיים בהן. יש שני סוגים של תמורות כאלו:

1. תמורות שזרות ל- $\sigma$  - יש רק אחת כזו, והיא  $(3, 4)$ .

2. תמורות שמזיזות את  $\sigma$  במעגל - id,  $(1, 2, 5)$  ו- $(1, 5, 2)$ .

כמובן, כל מכפלה של תמורות המתחלפות עם  $\sigma$  גם הוא מתחלף עם  $\sigma$ , ולכן מקבלים שהרשימה המלאה היא

$$\{\text{id}, (3, 4), (1, 2, 5), (1, 2, 5)(3, 4), (1, 5, 2), (1, 5, 2)(3, 4)\}$$

## 12 תרגול שניים עשר

### 12.1 אלגוריתם מילר-רבין לבדיקת ראשוניות

בפרק זה נציג אלגוריתם נפוץ לבדיקת ראשוניות של מספרים טבעיים. האלגוריתם המקורי הוא דטרמיניסטי ופותח בשנת 1976 על ידי מילר. בשנת 1980 הוצגה גרסה הסתברותית של האלגוריתם על ידי רבין. הגרסה ההסתברותית היא מהירה יחסית. היא תזזה כל מספר ראשוני בוודאות, אבל בהסתברות נמוכה, התלויה בכמות האיטרציה (חזרות) באלגוריתם היא תכריז גם על מספר פריק כראשוני.

בפועל, תוכנות לבדיקת ראשוניות של מספרים גדולים כמעט תמיד משתמשות בגרסאות של אלגוריתם מילר-רבין, או באלגוריתם Baillie-Pomerance-Selfridge-Wagstaff המכליל אותו. למשל בספריית OpenSSL האלגוריתם ממומש עם כמה שיפורים למהירות, בקובץ הזה.

אחד הרעיונות בבסיס האלגוריתם הוא שהמשפט הקטן של פרמה מבטיח שאם  $p$  ראשוני, אז  $a^{p-1} \equiv 1 \pmod{p}$  לכל  $a < p$ . מספר פריק  $N$  שעבורו כל  $a$  הזר ל- $N$  מקיים  $a^{N-1} \equiv 1 \pmod{N}$  נקרא מספר קרמייקל. קיימים אינסוף מספרי קרמייקל, אבל הם יחסית "נדירים". אלגוריתם מילר-רבין מצליח לזהות גם מספרים כאלו.

נניח כי  $N > 2$  ראשוני. נציג  $N-1 = 2^s \cdot M$  כאשר  $M$  אי זוגי. השורשים הריבועיים של 1 מודולו  $N$  הם רק  $\pm 1$  (שורשים של הפולינום  $x^2 + 1$  בשדה הסופי  $\mathbb{F}_N$ ). אם  $a^{N-1} \equiv 1 \pmod{N}$ , אז השורש הריבועי שלו  $a^{(N-1)/2}$  הוא  $\pm 1$ . כעת, אם  $(N-1)/2$  זוגי, נוכל להמשיך לקחת שורש ריבועי. אז בהכרח יתקיים  $a^M \equiv 1 \pmod{N}$  או  $a^{2^j M} \equiv -1 \pmod{N}$  עבור  $0 \leq j < s$  כלשהו. עבור  $N$  כללי, אם אחד מן השיויונות האלו מתקיים נאמר שהמספר  $a$  הוא עד חזק לראשוניות של  $N$ . עבור  $N$  פריק, אפשר להוכיח שלכל היותר רבע מן המספרים עד  $N-1$  הם עדים חזקים של  $N$ .

טענה 12.1 (אלגוריתם מילר-רבין). הקלט הוא מספר טבעי  $N > 3$ , ופרמטר  $k$  הקובע את דיוק המבחן.

הפלט הוא "פריק" אם  $N$  בטוח פריק, ואחרת "כנראה ראשוני" (כלומר  $N$  ראשוני או בהסתברות הנמוכה מבערך  $4^{-k}$  הוא פריק).

**לולאת עדים** נחזור בלולאה  $k$  פעמים על הבדיקה הבאה: נבחר מספר אקראי  $a \in [2, N-2]$  ונחשב  $x = a^M$ .

אם  $x$  שקול ל-1 או ל-1- מודולו  $N$ , אז  $a$  הוא עד חזק לראשוניות של  $N$ , ונוכל להמשיך לאיטרציה הבאה של בלולאת העדים מייד.

אחרת, נחזור בלולאה  $s - 1$  פעמים על הבדיקה הבאה:

$$x = x^2$$

אם  $x \equiv 1 \pmod{N}$ , נחזיר את הפלט "פריק".

אחרת, אם  $x \equiv -1 \pmod{N}$ , נעבור לאיטרציה הבאה של לולאת העדים.

אם לא יצאנו מהלולאה הפנימית, אז נחזיר "פריק", כי אז  $a^{2^j M}$  לא שקול ל-1- לאף  $0 \leq j < s$ .

רק במקרה שעברנו את כל  $k$  האיטרציות לעיל נחזיר "כנראה ראשוני".

**תרגיל 12.2** (רשות). כתבו בשפת אסמבלי פונקציה מהירה לחישוב מספר הפעמים ש- $N$  מתחלק ב-2. כלומר מצאו כמה אפסים רצופים יש בסוף ההצגה הבינארית של  $N$  כדי למצוא את  $s$ .

אם נשתמש בשיטת של העלאה בחזקה בעזרת ריבועים וחשבון מודולורי רגיל, אז סיבוכיות הזמן של האלגוריתם היא  $O(k \log^3 N)$ . אפשר לשפר את סיבוכיות הזמן על ידי שימוש באלגוריתמים מתוחכמים יותר. העובדה שניתן לבדוק את הראשוניות של  $N$  בזמן ריצה שהוא פולינומי ב- $\log N$  (למשל אלגוריתם AKS או הגרסה הדטרמיניסטית של מילר-רבין) מראה שזו בעיה שונה מפירוק מספרים לגורמים ראשוניים.

תחת הנחת רימן המוכללת, גרסה דטרמיניסטית לאלגוריתם מילר-רבין היא לבדוק האם כל מספר טבעי בקטע  $[2, \min(N - 1, [2 \ln^2 N])]$  הוא עד חזק לראשוניות של  $N$ . ישנם אלגוריתמים יותר יעילים למשימה זאת. עבור  $N$  קטן מספיק לבדוק בדרך כלל מספר די קטן של עדים.

**דוגמה 12.3**. נניח  $N = 221$  ו- $k = 2$ . נציג את  $2^2 \cdot 55 = 220 = N - 1$ . כלומר  $s = 2$  ו- $M = 55$ .

נבחר באופן אקראי (לפי ויקיפדיה האנגלית) את  $a = 174 \in [2, 219]$ . נחשב כי

$$a^M = a^{2^0 M} = 174^{55} \equiv 47 \pmod{N}$$

נשים לב כי 47 אינו  $\pm 1$  מודולו 221. לכן נבדוק

$$a^{2^1 M} = 174^{110} \equiv 220 \pmod{N}$$

ואכן  $220 \equiv -1 \pmod{221}$ . קיבלנו אפוא שאו ש-221 הוא ראשוני, או ש-174 הוא "עד שקרן" לראשוניות של 221. ננסה כעת עם מספר אקראי אחר  $a = 137$ . נחשב

$$a^{2^0 M} = 137^{55} \equiv 188 \pmod{N}$$

$$a^{2^1 M} = 137^{110} \equiv 205 \pmod{N}$$

בשני המקרים לא קיבלנו -1 מודולו 221, ולכן 137 מעיד על הפריקות של 221. לבסוף האלגוריתם יחזיר "פריק", ואכן  $221 = 13 \cdot 17$ .

**דוגמה 12.4.** נניח  $N = 781$ . נציג את  $780 = 2^2 \cdot 195$ . אם נבחר באקראי (לפי ויקיפדיה העברית) את  $a = 5$ , נקבל כי

$$5^{195} \equiv 1 \pmod{N}$$

כלומר 5 הוא עד חזק לראשוניות של 781. כעת אם נבחר את  $a = 17$ , נקבל כי

$$17^{195} \equiv -1 \pmod{N}$$

ולכן גם 17 הוא עד חזק. אם נבדוק את  $a = 2$  נגלה כי  $2^{780} \equiv 243 \not\equiv \pm 1$ , ולכן 781 אינו ראשוני. אגב  $781 = 11 \cdot 71$ .

## 12.2 חבורות אבליות סופיות

12.5. תהי  $G$  חבורה אבלית מסדר  $p_1 p_2 \dots p_k$ , מכפלת ראשוניים שונים. אזי

$$G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \dots \times \mathbb{Z}_{p_k}$$

הוכחה באינדוקציה בעזרת הטענה (שראיתם בהרצאה) ש- $(n, m) = 1$  אם ורק אם  $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ . למשל אם  $G$  אבלית מסדר 154, אז  $G \cong \mathbb{Z}_2 \times \mathbb{Z}_7 \times \mathbb{Z}_{11}$ .

12.6. תהי  $G$  חבורה אבלית מסדר חזקה של ראשוני  $p^n$ . אזי קיימים מספרים טבעיים  $m_1, \dots, m_k$  כך ש- $m_1 + \dots + m_k = n$  ומתקיים  $G \cong \mathbb{Z}_{p^{m_1}} \times \mathbb{Z}_{p^{m_2}} \times \dots \times \mathbb{Z}_{p^{m_k}}$ .

למשל אם  $G$  אבלית מסדר  $27 = 3^3$ , אזי  $G$  איזומורפית לאחת מהחבורות הבאות:

$$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3, \mathbb{Z}_3 \times \mathbb{Z}_9, \mathbb{Z}_{27}$$

שקל לראות שהן לא איזומורפיות אחת לשניה (לפי סדרים של איברים למשל).

12.7. הערה (תזכורת מתרגול שעבר):

יהי  $n \in \mathbb{N}$ . נאמר כי סדרה לא עולה של מספרים טבעיים  $(s_i)_{i=1}^r$  היא חלוקה של  $n$  אם  $\sum_{i=1}^r s_i = n$ . נסמן את מספר החלוקות של  $n$  ב- $\rho(n)$ .

12.8. הגדרה. למשל  $\rho(4) = 5$ , כי  $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1 = 4$ .

12.9. טענה. מספר החבורות האבליות, עד כדי איזומורפיזם, מסדר  $p^n$  הוא  $\rho(n)$ .

12.10. טענה. לכל חבורה אבלית סופית  $G$  יש צורה קנונית

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \dots \times \mathbb{Z}_{d_r}$$

שבה  $d_i | d_{i+1}$  לכל  $1 \leq i \leq r-1$ .

12.11. טענה. כל חבורה אבלית מסדר  $p_1^{k_1} \dots p_n^{k_n}$  גם איזומורפית למכפלה של חבורות אבליות  $A_1 \times \dots \times A_n$  כאשר  $A_i$  היא מסדר  $p_i^{k_i}$ . פירוק כזה נקרא פירוק פרימרי.

למשל, אם  $G$  חבורה אבלית כך ש- $45 = 3^2 \cdot 5 = |G|$ , אז  $G$  איזומורפית ל- $\mathbb{Z}_9 \times \mathbb{Z}_5$  או ל- $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ .

**מסקנה 12.12.** מספר החבורות האבליות, עד כדי איזומורפיזם, מסדר  $p_1^{k_1} \dots p_n^{k_n}$  הוא  $\rho(k_1) \dots \rho(k_n)$ . למשל, מספר החבורות האבליות מסדר  $200 = 2^3 \cdot 5^2$  הוא  $\rho(3)\rho(2) = 3 \cdot 2 = 6$ . האם אתם יכולים למצוא את כולן?

**תרגיל 12.13.** הוכיחו כי  $\mathbb{Z}_{200} \times \mathbb{Z}_{20} \cong \mathbb{Z}_{100} \times \mathbb{Z}_{40}$ .

פתרון. אפשרות אחת היא להביא את החבורות להצגה בצורה קנונית, ולראות שההצגות הן זהות. אפשרות אחרת היא להעזר בטענה שאם  $(n, m) = 1$ , אז  $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$  לכן

$$\mathbb{Z}_{200} \times \mathbb{Z}_{20} \cong \mathbb{Z}_{25} \times \mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_4 \cong \mathbb{Z}_{25} \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_5 \cong \mathbb{Z}_{100} \times \mathbb{Z}_{40}$$

Exponent of a group

**הגדרה 12.14.** תהי  $G$  חבורה. נגדיר את האקספוננט (או, המעריך) של החבורה  $\exp(G)$  להיות המספר הטבעי הקטן ביותר  $n$  כך שלכל  $g \in G$  מתקיים  $g^n = e$ . אם לא קיים כזה, נאמר  $\exp(G) = \infty$ . קל לראות שהאקספוננט של  $G$  הוא הכפולה המשותפת המזערית (lcm) של סדרי האיברים שלה.

**תרגיל 12.15.** תנו דוגמא לחבורה לא ציקלית  $G$  עבורה  $\exp(G) = |G|$ .

פתרון. נבחר את  $G = S_3$ . אנחנו יודעים שיש בה איבר מסדר 1 (איבר היחידה), איברים מסדר 2 (החילופים) ואיברים מסדר 3 (מחזורים מאורך 3). לכן

$$\exp(S_3) = [1, 2, 3] = 6 = |S_3|$$

אם יש זמן הראו כי  $\exp(S_n) = [1, 2, \dots, n]$

**תרגיל 12.16.** הוכיחו שאם  $G$  חבורה אבלית סופית כך ש- $\exp(G) = |G|$ , אז  $G$  ציקלית.

פתרון. נניח וישנו פירוק  $\exp(G) = |G| = p_1^{k_1} \dots p_n^{k_n}$ . אנחנו יכולים לפרק את  $G$  לפירוק פרימרי  $A_1 \times \dots \times A_n$ , כאשר  $|A_i| = p_i^{k_i}$ . אנחנו יודעים מהו הסדר של איברים במכפלה ישרה (הכפולה המשותפת המזערית של הסדרים ברכיבים), ולכן הגורם  $p_i^{k_i}$  באקספוננט מגיע רק מאיברים שבהם ברכיב  $A_i$  בפירוק הפרימרי יש איבר לא אפסי. האפשרות היחידה שזה יקרה היא אם ורק אם  $A_i \cong \mathbb{Z}_{p_i^{k_i}}$  (אחרת האקספוננט יהיה

קטן יותר). ברור כי  $(p_i^{k_i}, p_j^{k_j}) = 1$  עבור  $i \neq j$ , ולכן נקבל כי

$$G \cong \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \dots \times \mathbb{Z}_{p_n^{k_n}} \cong \mathbb{Z}_{|G|}$$

ולכן  $G$  היא ציקלית.

**תרגיל 12.17.** הוכח או הפרד: קיימות 5 חבורות לא איזומורפיות מסדר 8.

פתרון. נכון. על פי טענה שראינו, מספר החבורות האבליות, עד כדי איזומורפיזם, מסדר  $p^n$  הוא  $\rho(n)$ , ולכן לחבורה מסדר  $2^3$  יש  $\rho(3) = 3$  חבורות אבליות. אלו הן

$$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

קיימות עוד שתי חבורות מסדר 8, שהן לא אבליות:  $D_4$  וחבורת הקוטרניונים.

Quaternion  
group

הערה 12.18 (על חבורת הקוטרניונים). המתמטיקאי האירי בן המאה ה-19, וויליאם המילטון, הוא האחראי על גילוי חבורת הקוטרניונים. רגע התגלית נקרא לימים "אקט של וונדליזם מתמטי".

בעודו מטייל עם אשתו ברחובות דבלין באירלנד, הבריק במוחו מבנה החבורה, ובתגובה נרגשת, חרט את המשוואה:  $i^2 = j^2 = k^2 = ijk$  על גשר ברום בדבלין. המשוואה נמצאת שם עד היום.

בדומה לחבורה הדיהדרלית, נוח לתאר את החבורה על ידי ארבעת היוצרים והיחסים ביניהם:

$$Q_8 = \langle -1, i, j, k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle$$

הדמיון למספרים המרוכבים אינו מקרי. בנסיון להכליל את שדה המרוכבים הדו מימדי למרחב תלת מימדי, הבין המילטון שיהיה עליו לעלות מימד נוסף - למרחב ארבע מימדי. זה גם מקור השם (קוטר פירושו ארבע בלטינית). שימוש נפוץ שלהם הוא לתיאור סיבוב במרחב כפי שמוסבר כאן.

קיים יצוג שקול וחסכוני יותר, על ידי שני יוצרים בלבד

$$\langle x, y \mid x^2 = y^2, y^{-1}xy = x^{-1} \rangle$$

## 13 תרגול שלושה עשר

### 13.1 שדות סופיים

Field **הגדרה 13.1.** שדה הוא מבנה אלגברי הכולל קבוצה  $F$  עם שתי פעולות בינאריות, להן אפשר לקרוא "חיבור" ו"כפל" ושני קבועים, שאותם נסמן  $0_F$  ו- $1_F$ , המקיים את התכונות הבאות:

1. המבנה  $(F, +, 0_F)$  הוא חבורה חיבורית אבלית.

2. המבנה  $(F^*, \cdot, 1_F)$  הוא חבורה כפלית אבלית.

3. מתקיים חוק הפילוג (דיסטריבוטיביות הכפל מעל החיבור): לכל  $a, b, c \in F$  מתקיים  $a(b + c) = ab + ac$ .

Field order **הגדרה 13.2.** סדר השדה הינו מספר האיברים בשדה.

Field  
isomorphism

**הגדרה 13.3.** איזומורפיזם של שדות הוא העתקה חח"ע ועל בין שני שדות ששומרת על שתי הפעולות.

13.4. הערה. הסדר של שדות סופיים הוא תמיד חזקה של מספר ראשוני. כמו כן, עבור כל חזקה של ראשוני קיים שדה סופי יחיד עד כדי איזומורפיזם של שדות מסדר זה. לא נוכיח טענות אלו.

13.5. טענה. לכל מספר ראשוני  $p$ ,  $\mathbb{F}_p = (\mathbb{Z}_p, +(\text{mod } p), \cdot(\text{mod } p))$  הוא שדה סופי מסדר  $p$ . האם אתם יכולים להראות שכל שדה סופי אחר מסדר  $p$  הוא איזומורפי ל- $\mathbb{F}_p$ ?

Characteristic

**הגדרה 13.6.** המאפיין של שדה  $F$ , שסימונו  $\text{char}(F)$ , הינו המספר המינימלי המקיים:  $1_F + 1_F + \dots + 1_F = 0_F$ . כלומר הסדר של  $1_F$  בחבורה החיבורית של השדה (בתחבורה הכפלית זהו איבר היחידה).

13.7. הערה. עבור שדה סופי  $\mathbb{F}_q$ , סדר השדה הוא תמיד חזקה של מספר ראשוני, כלומר מתקיים  $q = p^n$  עבור  $p$  ראשוני כלשהו. המאפיין של השדה הזה הוא בהכרח  $p$ .

13.8. הערה. אם הסדר של  $1_F$  הוא אינסופי, מגדירים  $\text{char}(F) = 0$ . למשל השדות  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  הם ממאפיין אפס. כל שדה סופי הוא בהכרח עם מאפיין חיובי, מה לגבי ההפך?

13.9. טענה. החבורה הכפלית של השדה,  $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0_F\}$  היא ציקלית מסדר  $q - 1$ .

**דוגמה 13.10.**  $\mathbb{F}_{13}^* = \{1_F, 2, \dots, 12\}$  חבורה ציקלית מסדר 12, כלומר  $\mathbb{F}_{13}^* \cong \mathbb{Z}_{12}$ .

Subfield  
Field extension

**הגדרה 13.11.** יהי  $E$  שדה. תת-קבוצה (לא ריקה)  $F \subseteq E$ , שהיא שדה ביחס לפעולות המושרות נקראת תת-שדה. במקרה זה גם נאמר כי  $E/F$  הוא הרחבת שדות. נגדיר את הדרגה של  $E/F$  להיות המימד של  $E$  כמרחב וקטורי מעל  $F$ .

**דוגמה 13.12.**  $\mathbb{C}/\mathbb{R}$  היא הרחבת שדות מדרגה 2, ואילו  $\mathbb{R}/\mathbb{Q}$  היא הרחבת שדות מדרגה אינסופית. שימו לב ש- $\mathbb{Q}/\mathbb{F}_{13}$  היא לא הרחבת שדות כי לא מדובר באותן פעולות (ואפשר להוסיף שגם שלא מדובר בתת-קבוצה).

13.13. טענה. אם  $E/F$  היא הרחבת שדות סופיים, אז  $|E| = |F|^r$ . כלומר  $r = \log_{|F|} |E|$ , ולמשל אם  $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$  הרחבת שדות, אז  $r = n/m$ .

הוכחה. החבורה החיבורית של  $E$  היא למעשה מרחב וקטורי מעל  $F$  ממימד  $r = [E : F] < \infty$ . יהי  $\{x_1, x_2, \dots, x_r\}$  בסיס של  $E$  מעל  $F$ . אז כל איבר ב- $E$  ניתן לכתוב בדיוק בדרך אחת כצירוף לינארי (מעל  $F$ ) של  $\{x_1, x_2, \dots, x_r\}$ . לכן מספר האיברים ב- $E$  שווה למספר הצירופים הלינאריים השונים (מעל  $F$ ) של  $\{x_1, x_2, \dots, x_r\}$ . אבל יש  $|F|^r$  צירופים שונים כאלו, ולכן  $|E| = |F|^r$ .  $\square$

13.14. הערה (הרחבת שדות סופיים). הרחבה של  $\mathbb{F}_p$  מדרגה  $n \in \mathbb{N}$  מתבצעת על ידי הוספת שורש  $\alpha \notin \mathbb{F}_p$  של פולינום אי פריק ממעלה  $n$  מעל  $\mathbb{F}_p$  (כלומר שהמקדמים הם מהשדה הזה).

התוצאה של הרחבה זו  $\mathbb{F}_p(\alpha)$  היא שדה סופי מסדר  $q = p^n$  שניתן לסמן אותה על ידי  $\mathbb{F}_q$ . כל ההרחבות מאותו מימד איזומורפיות ולכן הזהות הספציפית של  $\alpha$  אינה חשובה (עד כדי איזומורפיזם).

**דוגמה 13.15.** השדה  $K = \mathbb{F}_3(i) = \mathbb{F}_9$  כאשר  $i$  הוא שורש הפולינום  $x^2 + 1$  הוא הרחבה של השדה  $\mathbb{F}_3$ . קל לבדוק האם פולינומים ממעלה 2 או 3 הם אי פריקים מעל שדה על ידי זה שנראה שאין להם שורשים מעל השדה.

כיצד נראים איברים בשדה החדש?  $K = \{a + ib \mid a, b \in \mathbb{F}_3\}$ . סדר השדה:  $3^2 = 9$ .

זו לא תהיה הרחבה מעל  $\mathbb{F}_5$  מכיוון שהפולינום הזה מתפצל מעל  $\mathbb{F}_5$ :  $x^2 + 1 = (x + 2)(x - 2)$  (זכרו שהחישובים הם מודולו 5). כלומר שני השורשים 2, 3 שייכים כבר ל- $\mathbb{F}_5$  לכן סיפוחם לא מרחיב את השדה הקיים.

**תרגיל 13.16.** לאילו שדות סופיים  $\mathbb{F}_q$  יש איבר  $x$  המקיים  $x^4 = -1$ ?

פתרון. נשים לב שאפס אינו מקיים את המשוואה, ולכן אנו מחפשים את הפתרון בחבורה הכפלית  $\mathbb{F}_q^*$ .

אם  $x^4 = -1$  אז  $x^8 = (-1)^2 = 1$ , ולכן מתקיים  $8 \mid o(x)$ . מנגד, אם המאפיין של השדה איננו 2, אז  $x^4 \neq 1$  כי  $1 \neq -1$  לכן  $4 \nmid o(x)$ . במקרה זה בהכרח  $o(x) = 8$ . אם כן, נדרוש שב- $\mathbb{F}_q^*$  יהיה איבר  $x$  מסדר 8, ואז הוא יקיים את המשוואה. מכיוון שסדר איבר מחלק את סדר החבורה (לגראנז'), נסיק שהסדר של  $\mathbb{F}_q^*$  מתחלק ב-8, ואז מפני ש- $\mathbb{F}_q^*$  ציקלית, אז גם קיים איבר מסדר 8.

בהתחשב בכך שסדרי השדות הסופיים האפשריים הם מהצורה  $p^n$  עבור  $p$  ראשוני, אנו מחפשים מקרים בהם  $8 \mid |\mathbb{F}_q^*| = |\mathbb{F}_q| - 1 = p^n - 1$ .

כלומר  $p^n \equiv 1 \pmod{8}$ . במקרה זה, פתרונות אפשריים הם השדות מסדרים: 17, 25, 41, 9, וכן הלאה. שימו לב שלא מופיע ברשימה 33 למרות ש- $33 \equiv 1 \pmod{8}$ . הסיבה היא שאין שדה מסדר 33 כיוון ש-33 אינו חזקה של מספר ראשוני.

כעת נחזור ונטפל במקרה הייחודי בו השדה ממאפיין 2. במקרה זה מתקיים  $-1 = 1$ , ולכן  $x^4 = 1$ . אכן האיבר 1 מקיים את השוויון ולכן שדה ממאפיין 2 עונה על הדרישה בתרגיל.

לסיכום, השדות המבוקשים הם שדות ממאפיין 2 או מסדר המקיים  $q = p^n \equiv 1 \pmod{8}$ .

**הערה 13.17.** שימו לב שבעוד שהפולינום  $T(x) = x^4 + 1$  אינו פריק מעל  $\mathbb{Q}$ , הוא פריק מעל כל שדה סופי.

בשדות ממאפיין 2 נשים לב ש- $T(x) = (x + 1)^4$ . בשדות סופיים ממאפיין אחר, לפחות אחד מהאיברים  $-1, 2, -2$  הוא ריבוע כי מכפלה של שני לא ריבועים היא ריבוע (אפשר לראות זאת לפי חזקות של היוצר בחבורה הכפלית). אז נחלק למקרים: אם  $-1 = a^2$ , אז  $T(x) = (x^2 + a)(x^2 - a)$ ; אם  $2 = a^2$ , אז  $T(x) = (x^2 + ax + 1)(x^2 - ax + 1)$  ואם  $-2 = a^2$ , אז  $T(x) = (x^2 + ax - 1)(x^2 - ax - 1)$ .

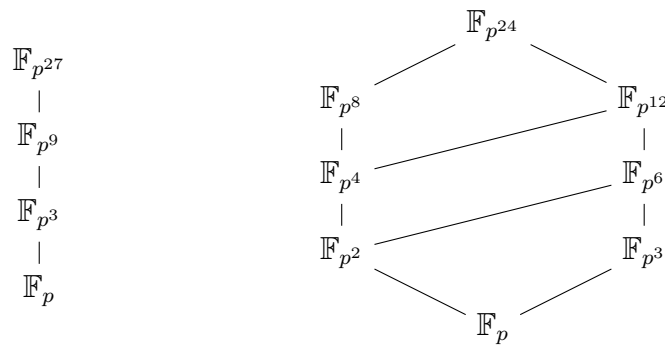
**תרגיל 13.18.** בשדה  $\mathbb{F}_q$  מתקיים  $a^q = a$  לכל  $a \in \mathbb{F}_q$  וגם  $x^q - x = \prod_{a \in \mathbb{F}_q} (x - a)$ .



הוכחה. אם  $a = 0_{\mathbb{F}_q}$  זה ברור. אחרת,  $a \in \mathbb{F}_q^*$ , ואנו יודעים שזו חבורה מסדר  $q - 1$ . לפי מסקנה ממשפט לגראנז' נקבל  $a^{q-1} = 1_{\mathbb{F}_q}$ . נכפול ב- $a$  ונקבל  $a^q = a$ . המשמעות היא שכל איברי  $\mathbb{F}_q$  הם שורשים של הפולינום  $x^q - x$ , ולכן המכפלה  $\prod_{a \in \mathbb{F}_q} (x - a)$  מחלקת אותו. מפני שהדרגות של שני הפולינומים האלו שוות, ושניהם מתוקנים (כלומר המקדם של המונום עם המעלה הגבוהה ביותר הוא 1), בהכרח הם שווים.  $\square$

**תרגיל 13.19.** הוכיחו כי  $\mathbb{F}_q$  משוכן ב- $\mathbb{F}_{q'}$  אם ורק אם  $q' = q^r$  עבור  $r$  כלשהו. בפרט, עבור  $p$  ראשוני,  $\mathbb{F}_{p^n}$  הוא תת-שדה של  $\mathbb{F}_{p^m}$  אם ורק אם  $n|m$ .

הוכחה. נתחיל בדוגמאות של סריג תת-השדות של  $\mathbb{F}_{p^{24}}$  ושל  $\mathbb{F}_{p^{27}}$ :



בכיוון אחד, נניח כי  $\mathbb{F}_q$  הוא תת-שדה של  $\mathbb{F}_{q'}$ . אזי  $\mathbb{F}_{q'}$  מרחב וקטורי מעל  $\mathbb{F}_q$ , וראינו בטענה 13.13 ש- $q' = q^r$  עבור  $r$  כלשהו. בכיוון השני, נניח  $q' = q^r$ , ונראה כי ל- $\mathbb{F}_{q'}$  יש תת-שדה מסדר  $q$ . מתקיים

$$\begin{aligned} x^{q'} - x &= x(x^{q^r-1} - 1) = x(x^{q-1} - 1)(x^{q^{r-1}-q} + x^{q^{r-2}-q} + \dots + x^q + 1) = \\ &= (x^q - x)(x^{q^{r-1}-q} + x^{q^{r-2}-q} + \dots + x^q + 1) \end{aligned}$$

ולכן ישנו חילוק פולינומים  $(x^q - x) | (x^{q'} - x)$ . לפי התרגיל הקודם, הפולינום  $x^{q'} - x$  מתפצל לגורמים לינאריים שונים מעל  $\mathbb{F}_{q'}$ , ולכן גם  $x^q - x$  מתפצל לגורמים לינאריים שונים. כלומר בקבוצה  $K = \{x \in \mathbb{F}_{q'} \mid x^q = x\}$  יש בדיוק  $q$  איברים שונים, וזה יהיה תת-שדה הדרוש של  $\mathbb{F}_{q'}$ . מספיק להראות סגירות לכפל וחיבור: אם  $x, y \in K$ , אז  $x^q = x$  וגם  $y^q = y$ . נניח  $q = p^n$ , ולכן

$$\begin{aligned} (x + y)^q &= (x + y)^{p^n} = x^{p^n} + y^{p^n} = x^q + y^q = x + y \\ (xy)^q &= x^q y^q = xy \end{aligned}$$

$\square$  וקיבלנו  $x + y, xy \in K$  כלומר  $K$  תת-שדה של  $\mathbb{F}_{q'}$  מסדר  $q$ .

### 13.2 בעיית הלוגריתם הבדיד ואלגוריתם דיפי-הלמן

**13.20 בעיה** (בעיית הלוגריתם הבדיד). תהי  $G$  חבורה. יהי  $g \in G$  ו- $x \in \mathbb{N}$ . המשימה היא למצוא את  $x$  בהנתן  $h = g^x$ . מסמנים את הפתרון ב- $\log_g h$ . מסתבר שבחבורות

Discrete  
logarithm  
problem (DLP)

מתאימות, אפילו אם ניתן לממש את הפעולה בחבורה באופן יעיל מאוד, עדין קשה מאוד (סיבוכיות זמן ריצה שהיא לפחות תת-מעריכית) למצוא את  $x$ .

הערה 13.21. שימו לב שבעיית הלוגריתם הבדיד עוסקת למעשה רק בחבורה הציקלית  $\langle g \rangle$ . למרות שכל החבורות הציקליות מאותו סדר הן איזומורפיות, דרך ההצגה של החבורה תקבע את הקושי של פתרון הבעיה. בעיית הלוגריתם הבדיד היא הבעיה הקשה בבסיס של בניות קריפטוגרפיות רבות, כמו החלפת מפתחות, הצפנה, חתימות דיגיטליות ופונקציות גיבוב קריפטוגרפיות.

**דוגמה 13.22.** דוגמה למה החבורה החיבורית  $\mathbb{Z}_n$  היא לא בחירה טובה לבעיית הלוגריתם הבדיד. נניח  $\mathbb{Z}_n = \langle g \rangle$ . שימו לב שאם  $g = 1$  הבעיה היא טריוויאלית! הרי  $x \cdot 1 \equiv x \pmod{n}$ . שימו לב כי ה- $x$  באגף שמאל הוא מספר טבעי, ואילו באגף ימין זה איבר של  $\mathbb{Z}_n$ .

התכונה הספציפית של  $\mathbb{Z}_n$ , שכפל וחיבור מודולו  $n$  מוגדרים היטב, היא מה שמנצלים לפתרון מהיר. נניח  $g \neq 1$ . בהנתן  $h \in \mathbb{Z}_n$  אנו רוצים למצוא  $x$  כך ש- $x \cdot g \equiv h \pmod{n}$ . ידוע לנו כי  $(g, n) = 1$ , ולכן קיים הופכי כפלי  $g^{-1}$ , שאותו ניתן לחשב בעזרת אלגוריתם אוקלידס ביעילות. לכן הפתרון הוא  $x = hg^{-1} \pmod{n}$ .

Diffie-Hellman  
key exchange

טענה 13.23 (פרוטוקול דיפי-הלמן). תהי חבורה ציקלית  $G = \langle g \rangle$  מסדר  $n$ , הידועה לכל. מקובל לבחור את  $U_p$  עבור  $p$  ראשוני גדול מאוד (יותר מאלף ספרות בינאריות). לכל משתמש ברשת יש מפתח פרטי סודי, מספר טבעי  $a \in [2, n-1]$  ומפתח ציבורי  $g^a \pmod{n}$ . איך שני משתמשים, אליס ובוב, יתאמו ביניהן מפתח הצפנה שיהיה ידוע רק להם?

1. אליס שולחת לבוב את המפתח הציבורי שלה  $g^a \pmod{n}$ .
2. בוב מחשב את מפתח ההצפנה המשותף שלהם  $(g^a)^b \pmod{n}$ , ואת מפתח הפענוח  $(g^a)^{-b} \pmod{n}$ .
3. אותו תהליך קורה בכיוון ההפוך שבו אליס מחשבת את  $(g^b)^a \pmod{n}$  ואת  $(g^b)^{-a} \pmod{n}$ .
4. כעת שני הצדדים יכולים להצפין הודעות עם  $g^{ab} \pmod{n}$ .

הערה 13.24. בתהליך המפתח הסודי של אליס ובוב לא שודר, וסודיותו לא נפגעה. האלגוריתם הוא סימטרי, כלומר ניתן לחשב ממפתח ההצפנה את מפתח הפענוח ולהפך. יש לפחות מתקפה ברורה אחת והיא שתוקף יכול להתחזות בדרך לאליס או לבוב (או לשניהם), ולכן בפועל משתמשים בפרוטוקולים יותר מתוחכמים יותר למניעת התקפה זו.

**דוגמה 13.25.** נריץ את האלגוריתם עם מספרים קטנים (באדיבות ויקיפדיה). יהי  $p = 23$ . נבחר יוצר  $U_{23} = \langle 5 \rangle$ . אליס בחרה  $a = 6$ , ולכן תשלח לבוב את  $5^6 \equiv 8 \pmod{23}$ . בוב בחר  $b = 15$ , ולכן ישלח לאליס את  $5^{15} \equiv 19 \pmod{23}$ . כעת אליס תחשב  $19^6 \equiv 2 \pmod{23}$ , ובוב יחשב  $8^{15} \equiv 2 \pmod{23}$ .

## 14 תרגול ארבעה עשר

### 14.1 משוואת המחלקות

לפני שנציג את משוואת המחלקות נזכיר שלושה מושגים.

Center

**הגדרה 14.1.** המרכז של חבורה  $G$  הוא הקבוצה

$$Z(G) = \{x \in G \mid xy = yx, \forall y \in G\}$$

וכמו כן, ראינו ש- $Z(G)$  תת-חבורה נורמלית של  $G$ .

Centralizer

**הגדרה 14.2.** תהי  $G$  חבורה. לכל  $x \in G$ , המרכז של  $x$  הוא הקבוצה

$$C_G(x) = \{y \in G \mid xy = yx\}$$

וכמו כן, ראינו ש- $C_G(x)$  תת-חבורה של  $G$ .

Conjugacy class

**הגדרה 14.3.** תהי  $G$  חבורה. יהי  $x \in G$ . נגדיר את מחלקת הצמידות של  $x$  להיות הקבוצה

$$\text{conj}(x) = \{gxg^{-1} \mid g \in G\}$$

הערה 14.4. לכל  $x \in G$  מתקיים

$$[G : C_G(x)] = |\text{conj}(x)|$$

**תרגיל 14.5.** מצא את מספר התמורות ב- $S_n$  המתחלפות עם  $\beta = (12)(34)$ , כלומר כל התמורות  $\gamma \in S_n$  המקיימות  $\beta\gamma = \gamma\beta$ .

פתרון.

$$|C_{S_n}(\beta)| = \frac{|S_n|}{|\text{conj}(\beta)|} = \frac{n!}{\frac{1}{2} \binom{n}{2} \binom{n-2}{2}} = 8(n-4)!$$

למשל, ב- $S_4$  יש 8 תמורות כאלו.

**תרגיל 14.6.** תהי  $G$  חבורה סופית כך ש- $n = [G : Z(G)]$ . הראה כי מחלקת צמידות ב- $G$  מכילה לכל היותר  $n$  איברים.

פתרון. לכל  $x \in G$  מתקיים  $Z(G) \leq C_G(x)$ . לכן

$$n = [G : Z(G)] \geq [G : C_G(x)] = |\text{conj}(x)|$$

Class equation

**משפט 14.7** (משוואת המחלקות). תהי  $G$  חבורה סופית. אזי

$$|G| = \sum_{x \text{ rep.}} |\text{conj}(x)| = |Z(G)| + \sum_{x \notin Z(G) \text{ rep.}} \frac{|G|}{|C_G(x)|}$$

הסבר לסכימה: סוכמים את גודל כל מחלקות הצמידות על ידי בחירת נציג מכל מחלקת צמידות וחישוב גודל מחלקת הצמידות שהוא יוצר.

**תרגיל 14.8.** רשום את משוואת המחלקות עבור  $S_3$  ו- $\mathbb{Z}_6$ .

פתרון. נתחיל ממשוואת המחלקות של  $\mathbb{Z}_6$ . חבורת זו אבליית ולכן מחלקת הצמידות של כל איבר כוללת איבר אחד בלבד. לכן משוואת המחלקות של  $\mathbb{Z}_6$  הינה  $6 = 1 + 1 + 1 + 1 + 1 + 1$ .

קעת נציג את המשוואת המחלקות של  $S_3$ : מחלקת צמידות ב- $S_n$  מורכבת מכל התמורות בעלות מבנה מחזורים זהה. כלומר נקבל  $6 = 3 + 2 + 1$ . פירוט החישוב:

$$|\text{conj}(\text{id})| = 1 \bullet$$

$$|\text{conj}(\text{---})| = 3 \bullet$$

$$|\text{conj}(\text{---})| = 2 \bullet$$

$p$ -group

**הגדרה 14.9.** יהי  $p$  ראשוני. חבורה  $G$  תקרא חבורת- $p$ , אם הסדר של כל איבר בה הוא חזקה של  $p$ . הראו שאם  $G$  סופית, אז  $G$  חבורת- $p$  אם ורק אם  $|G| = p^n$  עבור איזשהו  $n \in \mathbb{N}$ .

**תרגיל 14.10.** הוכיחו שהמרכז של חבורת- $p$  אינו טריוויאלי.

פתרון. תהי  $G$  חבורת- $p$ . על פי משוואת המחלקות מתקיים

$$|Z(G)| = p^n - \sum \frac{p^n}{|C_G(x_i)|} = p^n - \sum \frac{p^n}{p^{r_i}} = p^n - \sum p^{n-r_i}$$

נשים לב שאגף ימין של המשוואה מתחלק ב- $p$  ולכן באגף שמאל  $p$  מחלק את הסדר של  $Z(G)$ . מכאן נובע ש- $Z(G)$  לא יכול להיות טריוויאלי.

**תרגיל 14.11.** מיינו את החבורות מסדר  $p^2$  על ידי זה שתראו שהן חייבות להיות אבליות.

פתרון. לפי התרגיל הקודם אנו יודעים שהמרכז לא טריוויאלי, לכן לפי לגראנז':  $|Z(G)| \in \{p, p^2\}$ . נזכר שחבורה אבליית פירושה בין היתר הוא ש- $Z(G) = G$ , כלומר שמרכז החבורה מתלכד עם החבורה כולה. לכן עלינו להוכיח שבהכרח  $|Z(G)| = p^2$ .

נניח בשלילה שלא. כלומר ש- $|Z(G)| = p$ . כלומר תת-חבורה זו מסדר ראשוני וכן ציקלית. לכן נציגה על ידי יוצר:  $|Z(G)| = \langle a \rangle$ . נבחר  $b \in G \setminus Z(G)$ . קעת נתבונן בתת-חבורה הנוצרת על ידי האיברים  $a$  ו- $b$ . ברור כי  $|\langle a, b \rangle| > p$ , ולכן לפי לגראנז',  $|\langle a, b \rangle| = p^2$ . כלומר  $\langle a, b \rangle$  היא כל  $G$ .

על מנת להראות שחבורה הנוצרת על ידי שני יוצרים אלו היא אבליית, נראה שהיוצרים שלה מתחלפים, כלומר:  $ab = ba$ .

אכן זה נובע מכך ש- $a \in Z(G)$ . לכן בהכרח  $G = Z(G)$ . (בדרך אחרת: הראו כי  $G/Z(G)$  היא ציקלית, ולכן  $G$  אבליית.)

לפי משפט מיון חבורות אבליות, נקבל שכל חבורה מסדר  $p^2$  איזומורפית או ל- $\mathbb{Z}_{p^2}$  או ל- $\mathbb{Z}_p \times \mathbb{Z}_p$ .

## 14.2 תת-חבורת הקומוטטור

**הגדרה 14.12.** תהא  $G$  חבורה. הקומוטטור של זוג איברים  $a, b \in G$  הוא האיבר  
 $[a, b] = aba^{-1}b^{-1}$ .

הערה 14.13.  $a, b$  מתחלפים אם ורק אם  $[a, b] = e$ . באופן כללי,  $ab = [a, b]ba$ .

**הגדרה 14.14.** תת-חבורת הקומוטטור (נקראת גם תת-חבורת הנגזרת) הינה:

Commutator subgroup (or derived subgroup)

$$G' = [G, G] = \langle \{[g, h] \mid g, h \in G\} \rangle$$

כלומר תת-החבורה הנוצרת על ידי כל הקומוטטורים של  $G$ .

הערה 14.15.  $G$  אבליית אם ורק אם  $G' = \{e\}$ .  
 למעשה, תת-חבורת הקומוטטור "מודדת" עד כמה החבורה  $G$  אבליית.

הערה 14.16.  $[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b, a]$ .

הערה 14.17. אם  $H \leq G$  אז  $H' \leq G'$ .

הערה 14.18.  $G' \triangleleft G$ . למשל לפי זה ש- $[gag^{-1}, gbg^{-1}] = g[a, b]g^{-1}$ .  
 תת-חבורת הקומוטטור מקיימת למעשה תנאי חזק הרבה יותר מנורמליות. לכל הומומורפיזם  $f: G \rightarrow H$  מתקיים

$$f([a, b]) = [f(a), f(b)]$$

להוכחת הנורמליות של  $G'$  מספיק להראות שתנאי זה מתקיים לכל אוטומורפיזם פנימי של  $G$ .

**הגדרה 14.19.** חבורה  $G$  תקרא חבורה פשוטה אם ל- $G$  אין תת-חבורות נורמליות לא טריוויאליות.

Simple group

**דוגמה 14.20.** החבורה  $A_n$  עבור  $n \geq 5$  פשוטה. חבורה אבליית (לאו דווקא סופית) היא פשוטה אם היא איזומורפית ל- $\mathbb{Z}_p$  עבור ראשוני  $p$ .

**הגדרה 14.21.** חבורה  $G$  נקראת פושלפת אם  $G = G'$ .

Perfect

**מסקנה 14.22.** אם  $G$  חבורה פשוטה לא אבליית, אז היא פושלפת.

הוכחה. מתקיים  $G' \triangleleft G$  לפי ההערה הקודמת. מכיוון ש- $G$  פשוטה, אין לה תת-חבורות נורמליות למעט החבורות הטריוויאליות  $G$  ו- $\{e\}$ . מכיוון ש- $G$  לא אבליית,  $G' \neq \{e\}$ . לכן בהכרח  $G' = G$ .  
 $\square$

**דוגמה 14.23.** עבור  $n \geq 5$ , מתקיים  $A'_n = A_n$ . אבל  $\mathbb{Z}_5$  למשל היא פשוטה ולא מושלמת, כי היא אבליית.

**משפט 14.24.** הפנה  $G/G'$ , שנקראת האבליניזציה של  $G$ , היא הפנה האבליית הגדולה ביותר של  $G$ . כלומר:

Abelinization

1. לכל חבורה  $G$ , המנה  $G/G'$  אבליית.

2. לכל  $N \triangleleft G$  מתקיים ש- $G/N$  אבליית אם ורק אם  $G' \leq N$  (כלומר  $G/N$  איזומורפית למנה של  $G/G'$ ).

**דוגמה 14.25.** אם  $A$  אבליית, אז  $A/G' \cong A$ .

**דוגמה 14.26.** תהי  $D_4 = \langle \sigma, \tau \rangle$ . ראינו ש- $Z(D_4) = \{e, \sigma^2\}$ . כמו כן, המנה  $|D_4/Z(D_4)| = 4$ . תת-חבורה זו אבליית (מכיוון שהסדר שלה הוא  $p^2$ ) לפי תרגיל 14.11.

לכן, לפי תכונת המקסימליות של האבליניזציה,  $D'_4 \leq Z(D_4)$ . החבורה  $D_4$  לא אבליית ולכן  $D'_4 \neq \{e\}$ . לכן  $D'_4 = Z(D_4)$ .

**תרגיל 14.27.** מצא את  $S'_n$  עבור  $n \geq 5$ .

פתרון. יהי  $[a, b] = aba^{-1}b^{-1} \in S_n$ . נשים לב כי  $\text{sign}(a) = \text{sign}(a^{-1})$ . לכן

$$\text{sign}([a, b]) = \text{sign}(a) \text{sign}(b) \text{sign}(a^{-1}) \text{sign}(b^{-1}) = \text{sign}(a)^2 \text{sign}(b)^2 = 1$$

כלומר קומוטטור הוא תמורה זוגית. גם כל מכפלה של קומוטטורים היא תמורה זוגית, ולכן  $S'_n \leq A_n$ .

נזכר כי  $A_n \leq S_n$ . לכן, על פי הערה שהצגנו קודם,  $A'_n \leq S'_n$ . מצד שני, ראינו שעבור  $n \geq 5$  מתקיים  $A'_n = A_n$ . כלומר קיבלנו  $S'_n = A_n$ . בדרך אחרת,  $S_n/A_n \cong \mathbb{Z}_2$ . כלומר המנה אבליית. לכן, לפי מקסימליות האבליניזציה, נקבל  $S'_n = A_n$ .

## א' נספח: חבורות מוכרות

כאשר חבורה היא מספיק "מפורסמת" אפשר לכתוב את הסימון לקבוצת האיברים שלה מבלי לכתוב את הפעולה. הנה רשימה לא ממצה לכמה חבורות מוכרות שכאלו:

- $(G, \cdot)$  או  $(G, *)$ , חבורה כלשהי עם פעולה כלשהי. איבר היחידה מסומן  $e$ .
  - $(\mathbb{Z}, +)$ , המספרים השלמים עם חיבור רגיל. איבר היחידה מסומן 0.
  - $(n\mathbb{Z}, +)$ , הכפולות של  $n \in \mathbb{Z}$  עם חיבור רגיל. איבר היחידה מסומן 0.
  - $(\mathbb{Z}_n, +)$ , מחלקות שקילות של חלוקה בשארית  $n$  עם חיבור מודולו  $n$ . איבר היחידה מסומן 0 או  $[0]$ .
  - $(U_n, \cdot)$ , חבורת אוילר עם כפל מודולו  $n$ . איבר היחידה מסומן 1 או  $[1]$ .
  - $(\Omega_n, \cdot)$ , חבורת שורשי היחידה מסדר  $n$  עם כפל רגיל. איבר היחידה מסומן 1.
  - $(F, +)$ , החבורה החיבורית של שדה  $F$  עם החיבור בשדה. איבר היחידה מסומן 0.
  - $(F^*, +)$ , החבורה הכפלית של שדה  $F$  עם הכפל בשדה. איבר היחידה מסומן 1.
  - $(M_n(F), +)$ , מטריצות בגודל  $n \times n$  מעל שדה  $F$  עם חיבור מטריצות. איבר היחידה מסומן 0 או  $0_n$ .
  - $(GL_n(F), \cdot)$ , החבורה הלינארית הכללית מעל  $F$  מדרגה  $n$  עם כפל מטריצות. האיברים הם מטריצות הפיכות בגודל  $n \times n$  מעל שדה  $F$ . איבר היחידה מסומן  $I$  או  $I_n$ .
  - $(SL_n(F), \cdot)$ , החבורה הלינארית המיוחדת מעל  $F$  מדרגה  $n$  עם כפל מטריצות. האיברים הם מטריצות בגודל  $n \times n$  עם דטרמיננטה 1 מעל שדה  $F$ . איבר היחידה מסומן  $I$  או  $I_n$ .
  - $(S_n, \cdot)$ , החבורה הסימטרית עם הרכבת פונקציות. איבר היחידה מסומן id.
  - $(A_n, \cdot)$ , חבורה החילופין (או חבורת התמורות הזוגיות) עם הרכבת פונקציות. איבר היחידה מסומן id.
  - $(D_n, \cdot)$ , החבורה הדיהדרלית עם הרכבת פונקציות. איבר היחידה מסומן id.
  - $(Q_8, \cdot)$ , חבורת הקוטרניונים. איבר היחידה מסומן 1.
- שימו לב שאם פעולה מסומנת  $\cdot$  כמו כפל, במקרים רבים נשמיט את סימון הפעולה. לעיתים כדי להדגיש למי שייך איבר היחידה נרשום  $e_G$  במקום  $e$ , או למשל  $0_F$  במקום 0 עבור איבר היחידה בחבורה החיבורית של שדה  $F$ .