מבוא לתורת החבורות
מערכי תרגול קורס 88-211

דצמבר 2016, גרסה 0.6

אוניברסיטת בר־אילן סמסטר א' תשע"ז

תוכן העניינים

מבוא

נתחיל עם כמה דגשים:

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

1 מבנים אלגבריים בסיסיים

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

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

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

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

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

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

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

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

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

פתרון. יהי c ההופכי של aba. כלומר

$$abac = caba = e$$

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

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

וניתן להסיק כי aca הופכי שמאלי וימני של b.

תרגיל 1.10. האם קיים מונואיד שיש בו איבר הפיך מימין שאינו הפיך משמאל?

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

ההפיכים משמאל הם הפונקציות החח"ע. ההפיכים מימין הם הפונקציות על (מהקורס מתמטיקה בדידה). מה יקרה אם נבחר את X להיות סופית?

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

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

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

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

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

האיברים ההפיכים במונואיד הן הקבוצות מהצורה $\{a\}$ עבור a הפיך ב-X (ההופכי הוא $\{a^{-1}\}$). אכן, נניח כי $A \in P_*(X)$ הפיך. לכן קיימת $B \in P_*(X)$ כך שלכל $a \in A, b \in B$ מתקיים $ab = e$. נראה כי $|B| = 1$. אחרת קיימים לפחות שני איברים $b_1, b_2 \in B$ ומתקיים $b_1a = ab_1 = ab_2 = b_2a = e$, ולכן מיחידות ההופכי של a נקבל $b_1 = b_2$. באופן סימטרי $|A| = 1$.

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

מתקיים: חבורה $\Leftarrow$ מונואיד $\Leftarrow$ חבורה למחצה.

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

1. סגירות הפעולה.

2. קיבוציות הפעולה.

3. קיום איבר יחידה.

4. כל איבר הוא הפיך.

דוגמה 1.13. (עבור קבוצה סופית אחת הדרכים להגדיר פעולה בינארית היא בעזרת לוח כפל.) למשל, אם $S=\{a,b\}$ ונגדיר

$*$	a	b
a	a	b
b	b	a

אז קל לראות שמתקיימת סגירות, אסוציאטיביות, a הוא יחידה וb הוא ההופכי של עצמו.

למעשה, זוהי החבורה היחידה מגודל 2 (למה?).

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

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

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

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

דוגמה 1.18. נסתכל על אוסף מחלקות השקילות מודולו n, שמקובל לסמן $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}=\{[a]\,|\,a\in\mathbb{Z}\}$. למשל $\mathbb{Z}_4=\{[0],[1],[2],[3]\}$. לפעמים מסמנים את מחלקת השקילות $[a]$ בסימון $\bar{a}$, ולעיתים כאשר ברור ההקשר פשוט a. כזכור $[a]+[b]=[a+b]$ כאשר באגף שמאל הסימן $+$ הוא פעולה בינארית הפועלת על אוסף מחלקות השקילות (a הוא נציג של מחלקת שקילות אחת ו-b הוא נציג של מחלקת שקילות אחרת) ובאגף ימין זו פעולת החיבור הרגילה של מספרים (שלאחריה מסתכלים על מחלקת השקילות שבה $a+b$ נמצא).

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

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

הגדרה 1.19 (חבורת האיברים ההפיכים)**.** יהי M מונואיד ויהיו $a, b \in M$ זוג איברים. אם a, b הם הפיכים, אזי גם $a \cdot b$ הוא הפיך במונואיד. אכן, האיבר ההופכי הוא $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. לכן אוסף כל האיברים ההפיכים במונואיד מהווה קבוצה סגורה ביחס לפעולה. כמו כן האוסף הנ"ל מכיל את איבר היחידה, וכל איבר בו הוא הפיך. מסקנה מיידית היא שאוסף האיברים ההפיכים במונואיד מהווה חבורה ביחס לפעולה המצומצמת. נסמן חבורה זו ב-$U(M)$ (קיצור של Units).

הגדרה 1.20. המערכת $(M_n(\mathbb{R}), \cdot)$ של מטריצות ממשיות בגודל $n \times n$ עם כפל מטריצות היא מונואיד. לחבורת ההפיכים שלו

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

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

דוגמה 1.21. נגדיר את חבורת אוילר (Euler) להיות $U_n = U(\mathbb{Z}_n)$ לגבי פעולת הכפל. נבנה את לוח הכפל של $\mathbb{Z}_6$ (בהתעלם מ-$[0]$ שתמיד יתן במכפלה $[0]$):

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

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

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

טענה 1.23. בדומה להערה האחרונה, נאפיין את האיברים ב-U_n לכל n.
יהי $m \in \mathbb{Z}$. אז $[m] \in U_n$ אם ורק אם $(n, m) = 1$. כלומר, ההפיכים במונואיד $(\mathbb{Z}_n, \cdot)$ הם כל האיברים הזרים ל-n.

דוגמה 1.24. $U_{12} = \{1, 5, 7, 11\}$.

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

2 חבורה אבלית

הגדרה 2.1. נאמר כי פעולה דו־מקומית $* : G \times G \to G$ היא אבלית (או חילופית, commutative) אם לכל שני איברים $a, b \in G$ מתקיים $a * b = b * a$. אם $(G, *)$ חבורה והפעולה היא אבלית, נאמר כי G היא חבורה אבלית (או חילופית). המושג נקרא על שמו של נילס הנריק אָבֶּל (Niels Henrik Abel).

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

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

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

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

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

3 תת־חבורות

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

תכלס מה שצריך לבדוק:

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

דוגמה 3.2. נוכיח שקבוצת המטריצות

$$H = \left\{ \left(\begin{array}{ccc} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{array} \right) \middle| a, b, c \in \mathbb{R} \right\}$$

היא תת־חבורה של $GL_3(\mathbb{R})$:

- יחידה: ברור ש- $I_3 \in H$.
- $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix} \in H$ ולכן יש סגירות לכפל.
- אפשר לראות שיש הפיך לפי הדטרמיננטה, אבל זה לא מספיק! צריך גם להראות שהמטריצה ההופכית נמצאת ב-H בעצמה. אמנם,

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

לחבורה זאת ודומותיה (!) קוראים חבורת **הייזנברג**.

דוגמה 3.3. $SL_n(F) \leq GL_n(F)$.

דוגמה 3.4. עבור $a \in G$ תמיד אפשר לבנות תת־חבורה הנוצרת ע"י איבר $\langle a \rangle = \left\{ a^k \,\middle|\, k \in \mathbb{Z} \right\} \leq G$. למשל:

- $4 \in \mathbb{Z}$:

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

- $a = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in GL_3(\mathbb{R})$:

$$\begin{aligned} \langle a \rangle = \Bigg\{ a^0 = I, a, a^2 = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ldots, a^n = \begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ldots \\ \ldots, a^{-1} = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, a^{-2} = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ldots, a^{-n}, \ldots \Bigg\} \\ = \left\{ \begin{pmatrix} 1 & 0 & k \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \,\middle|\, k \in \mathbb{Z} \right\} \end{aligned}$$

4 מבוא לתורת המספרים

הגדרה 4.1. 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 $-5|10$.

משפט 4.2 (משפט החילוק, או חלוקה אוקלידית)**.** לכל $n \in \mathbb{Z}, d \neq 0$ קיימים q, r יחידים כך ש-$n = qd + r$ וגם $0 \leq r < |d|$.

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

הגדרה 4.3. בהנתן שני מספרים שלמים n, m המחלק המשותף המירבי (ממ"מ, greatest common divisor) שלהם מוגדר להיות המספר

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

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

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

טענה 4.5. אם $n = qm + r$, אזי $(n, m) = (m, r)$.

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

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

דוגמה 4.7. נחשב את הממ"מ של 53 ו-47 בעזרת אלגוריתם אוקלידס

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

דוגמה נוספת עבור מספרים שאינם זרים:

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

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

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

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

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

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

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

ולכן $(234,61)=1=6\cdot 234-23\cdot 61$.

תרגיל 4.11. יהיו a,b,c מספרים שלמים כך ש-$(a,b)=1$ וגם $a|bc$. הראו כי $a|c$.

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

טענה 4.12. 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-$sa+tp=1$. נכפיל את השוויון האחרון ב-b ונקבל $sab+tpb=b$. ברור כי p מחלק את אגף שמאל (הרי $p|ab$), ולכן p מחלק את אגף ימין, כלומר $p|b$.

$\square$

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

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

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

טענה 4.14. תכונות של כמ"מ:

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

שאלה 4.15 (לבית)**.** אפשר להגדיר ממ"מ ליותר מזוג מספרים. יהי d הממ"מ של המספרים $n_1,\dots,n_k$. הראו שקיימים מספרים שלמים $s_1,\dots,s_k$ המקיימים $s_1n_1+\cdots+s_kn_k=d$. רמז: אינדוקציה על k.

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

פתרון. בשיטה העשרונית, הספרה האחרונה של מספר N היא $N \pmod{10}$. נשים לב כי $333^{333}=3^{333}\cdot 111^{333}$. לכן

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

ומכאן שהספרה האחרונה היא 3.

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

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

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

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

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

דוגמה 4.18. נמצא $x\in\mathbb{Z}$ כך ש-$x\equiv 1 \pmod 3$ וגם $x\equiv 2 \pmod 5$. ידוע כי $(5,3)=1$, ולכן $-1\cdot 5+2\cdot 3=1$. במקרה זה $n=5, m=3$ וכן $s=-1, t=2$, 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 משוואות של שקילות מודולו:

משפט 4.19 (אם יש זמן). תהא $\{m_1,\ldots,m_k\}$ קבוצת מספרים טבעיים הזרים זה לזה (כלומר כל זוג מספרים בקבוצה הוא זר). נסמן את מכפלתם ב-m. בהנתן קבוצה כלשהי של שאריות $\{a_i \,(\mathrm{mod} m_i) : 1\le i\le k\}$, קיימת שארית יחידה x מודולו m המהווה פתרון למערכת המשוואות

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

דוגמה 4.20. נמצא $y\in\mathbb{Z}$ כך ש-ש-$y\equiv 1 \pmod 3$, $y\equiv 2 \pmod 5$ וגם $y\equiv 3 \pmod 7$. נשים לב שהפתרון $y=7$ מן הדוגמה הקודמת הוא נכון כדי כדי הוספה של $15=3\cdot 5$ (כי $15\equiv 0 \pmod 3$ וגם $15\equiv 0 \pmod 5$). לכן את שתי המשוואות $y\equiv 1 \pmod 3$, $y\equiv 2 \pmod 5$ ניתן להחליף במשוואה אחת $y\equiv 7 \pmod{15}$. נשים לב כי $(15,7)=1$ ולכן אפשר להשתמש במשפט השאריות הסיני בגרסה לזוג משוואות. בדקו כי $y=52$ מהווה פתרון.

5 חבורת אוילר ומציאת הופכי

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

יותר מזה, יש לנו דרך למצוא את ההופכי:

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

תרגיל 5.2. מצאו $0 \le x \in \mathbb{Z}$ כך ש-$61x \equiv 1 \pmod{234}$.

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

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

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

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

6 חבורות ציקליות

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

דוגמה 6.2.

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

- $n\mathbb{Z} = \langle n \rangle$.
- $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$.
- $U_{10} = \{3, 3^2 = 9, 3^3 = 7, 3^4 = 1\} = \langle 3 \rangle$.

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

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

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

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

אבל איך נזהה שחבורה היא ציקלית?

6.1 סדר של איבר

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

דוגמה 6.7.
- ב-U_6, $o(5) = 2$.
- ב-$(GL_2(\mathbb{R}), \cdot)$, נבחר את $b = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$. נראה ש-$o(b) = 3$ כי

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

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

שאלה 6.9. תהי חבורה $G \times H$, הוכח כי הסדר של איבר (g, h) הוא $[o(g), o(h)]$.

פתרון. נסמן $o(g) = n$ ו-$o(h) = m$. נראה שהסדר של איבר (g, h) הוא מחלק משותף של n, m:

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

ולכן בפרט, לפי הטענה האחרונה:

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

מה שאומר ש-$o(g, h)$ הוא מכפלה משותפת של m ו-n, ולכן $[n, m]|o(g, h)$.

מצד שני נשים לב כי

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

ולכן $o\left((g, h)\right)|[n, m]$.

משפט 6.10. הסדר של איבר x שווה לסדר תת־החבורה שהוא יוצר, כלומר ל-$|\langle x\rangle|$.
בפרט, אם G חבורה מסדר n. אז G היא ציקלית אמ"ם קיים איבר מסדר n.

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

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

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

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

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

- $A\neq\varnothing$ כי $e\in A$.
- סגירות לפעולה: יהיו $a,b\in A$. אז יש n,m טבעיים כך ש-$a^n=b^m=e$. אזי: $(ab)^{nm}=a^{nm}b^{nm}=(a^n)^m(b^m)^n=e^me^n=e$. (שימו לב לשימוש בחילופיות!)
- סגירות להופכי: יהי $a\in A$. יש n כך ש-$a^n=e$, אז $a\cdot a^{n-1}=e$ לכן $a^{-1}=a^{n-1}$ וכבר ראינו שיש סגירות לפעולה.

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

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

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

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

טענה 6.15. מספר תכונות של הסדר:

1. אם G חבורה ציקלית סופית מסדר n אז לכל $g\in G$ מתקיים $g^n=e$.
2. בחבורה סופית הסדר של כל איבר הוא סופי.

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

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

פתרון. נוכיח את הסעיף האחרון:

מקרה ראשון, נניח $o(a) = n$, מספיק להראות ש-$o(a^{-1}) \leq o(a)$ (כי $a = (a^{-1})^{-1}$).
אז $a^n = 1$. $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$. לכן $o(a^{-1}) \leq n$.

מקרה שני, נניח שהסדר של a אינסופי. אז גם הסדר של a^{-1} אינסופי, כי אם הוא היה איזשהו n, אז מהמקרה הראשון, היינו מקבלים ש-$o(a) = n$, בסתירה.

הערה 6.16. יהי $a \in G$. אזי $o(a) = |\langle a \rangle|$. במילים, הסדר של איבר הוא סדר תת־החבורה שהוא יוצר.

תרגיל 6.17 (מההרצאה)**.** תהי G חבורה, ויהי $a \in G$. נניח $o(a) = n < \infty$. הוכיחו שלכל $d \leq n$ טבעי,

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

הוכחה (לדלג). <u>היתכנות</u>: נשים לב כי

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

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

<u>מינימליות</u>: נניח $\left(a^d\right)^t = e$, כלומר $a^{dt} = e$. לפי טענה 6.8, $n|dt$. לכן, גם $\frac{n}{(d,n)}\Big|\frac{dt}{(d,n)}$ (שניהם מספרים שלמים - מדוע?). מצד שני, $\left(\frac{n}{(d,n)}, \frac{d}{(d,n)}\right) = 1$.
לפי תרגיל 4.11, נקבל $\frac{n}{(d,n)}\Big|t$, כמו שרצינו. $\square$

תרגיל 6.18. תהי G חבורה ציקלית מסדר n. כמה איברים ב-G יוצרים (לבדם) את G?

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

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

לכן, מספר האיברים היוצרים את G הוא $|U_n|$. כלומר בדיוק $\varphi(n)$.

6.2 חבורת שורשי היחידה

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

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

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

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

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

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

פתרון.

1. נוכיח שהיא חבורה על ידי זה שנוכיח שהיא תת־חבורה של $\mathbb{C}^*$. ראינו בתרגיל 6.13 שתת־חבורת הפיתול של חבורה אבלית היא תת־חבורה. לפי הגדרת Ω_∞, רואים שהיא מכילה בדיוק את כל האיברים מסדר סופי של החבורה האבלית $\mathbb{C}^*$, ולכן חבורה.
באופן מפורש ולפי הגדרה: ברור כי $1 \in \Omega_\infty$, ולכן היא לא ריקה. יהיו $g_1, g_2 \in \Omega_\infty$. לכן קיימים m, n שעבורם $g_1 \in \Omega_m$, $g_2 \in \Omega_n$. נכתוב עבור $l, k \in \mathbb{Z}$ מתאימים:
$$g_1 = \operatorname{cis}\frac{2\pi k}{m}, \qquad g_2 = \operatorname{cis}\frac{2\pi l}{n}$$
לכן
$$\begin{aligned} g_1 g_2 &= \operatorname{cis}\frac{2\pi k}{m} \cdot \operatorname{cis}\frac{2\pi l}{n} = \operatorname{cis}\left(\frac{2\pi k}{m} + \frac{2\pi l}{n}\right) \\ &= \operatorname{cis}\left(\frac{2\pi\,(kn + lm)}{mn}\right) \in \Omega_{mn} \subseteq \Omega_\infty \end{aligned}$$
סגירות להופכי היא ברורה, שהרי אם $g \in \Omega_n$, אז גם $g^{-1} \in \Omega_n \subseteq \Omega_\infty$.
(אם יש זמן: לדבר שאיחוד של שרשרת חבורות, ובאופן כללי יותר, איחוד רשת של חבורות, היא חבורה.)

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

3. לפי הסעיף הקודם, כל תת־החבורות הציקליות של Ω_∞ הן סופיות. אך Ω_∞ אינסופית, ולכן לא ייתכן שהיא שווה לאחת מהן.

7 תת־חבורה הנוצרת על ידי איברים

הגדרה 7.1. תהי G חבורה ותהי $S \subseteq G$ תת־קבוצה לא ריקה איברים ב-G (שימו לב ש-S אינה בהכרח תת־חבורה של G).

תת־החבורה הנוצרת על ידי S הינה תת־החבורה המינימלית המכילה את S ונסמנה $\langle S\rangle$. אם $G = \langle S\rangle$ אז נאמר ש-G נוצרת על ידי S. עבור קבוצה סופית של איברים, נכתוב בקיצור $\langle x_1, \ldots, x_k\rangle$.

הגדרה זו מהווה הכללה להגדרה של חבורה ציקלית. חבורה היא ציקלית אם היא נוצרת על ידי איבר אחד.

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

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

דוגמה 7.3. אם ניקח $\{4,6\} \subseteq \mathbb{Z}$, אז נקבל: $\langle 4,6\rangle = \{4n + 6m : m, n \in \mathbb{Z}\}$.

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-$2|4m + 6n$ ולכן $\langle 4,6\rangle \subseteq 2\mathbb{Z}$.

($\supseteq$): יהי $2k \in 2\mathbb{Z}$. אזי $2k = 4(-k) + 6k \in \langle 4,6\rangle$. לכן מתקיים גם: $2\mathbb{Z} \subseteq \langle 4,6\rangle$.

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

בזכות החילופיות, ניתן לסדר את כל ה-a-ים יחד וכל ה-b-ים יחד. למשל

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

באופן כללי, בחבורה אבלית מתקיים:

$$\langle a_1, \ldots, a_n\rangle = \left\{a_1^{k_1} \ldots a_n^{k_n} \,\middle|\, \forall 1 \leq i \leq n, k_i \in \mathbb{Z}\right\}$$

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

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

מסקנה 7.7. כל חבורה סופית נוצרת סופית.

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

תרגיל 7.9. הוכיחו שהחבורות הבאות לא נוצרות סופית

1. חבורת שורשי היחידה Ω_∞.
2. $(M_3(\mathbb{R}),+)$
3. $(\mathbb{Q}^*,\cdot)$

פתרון.

1. בעוד ש-Ω_∞ היא אינסופית, נראה שכל תת־החבורה הנוצרת על ידי מספר סופי של איברים מ-Ω_∞ היא סופית. יהיו $a_1,\dots,a_k$ שורשי יחידה מסדרים $n_1,\dots,n_k$ בהתאמה. אז
$$\langle a_1,\dots,a_k\rangle=\left\{a_1^{i_1}\dots a_k^{i_k}:0\le i_j\le n_j,1\le j\le k\right\}$$
מפני ש-Ω_∞ היא אבלית. לכן יש מספר סופי (החסום מלמעלה במכפלה $n_1\cdots n_k$) של איברים ב-$\langle a_1,\dots,a_k\rangle$. לכן Ω_∞ אינה נוצרת סופית.

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

3. נניח בשלילה כי
$$\mathbb{Q}^*=\left\langle\frac{a_1}{b_1},\dots,\frac{a_n}{b_n}\right\rangle=\left\{\left(\frac{a_1}{b_1}\right)^{k_1}\dots\left(\frac{a_n}{b_n}\right)^{k_n}\,\middle|\,\forall 1\le i\le n,k_i\in\mathbb{Z}\right\}$$
אז קל לראות שהגורמים הראשוניים במכנה של כל איבר מוגבלים לקבוצת הגורמים הראשוניים שמופיעים בפירוק של המכפלה $b_1\cdots b_n$. אך זו קבוצה סופית, ולכן לא ניתן לקבל את כל השברים ב-$\mathbb{Q}^*$, כלומר סתירה.

8 החבורה הסימטרית (על קצה המזלג)

הגדרה 8.1. החבורה הסימטרית מדרגה n היא

$$S_n = \{\sigma : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\} \,|\, \sigma \text{ is bijective}\}$$

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

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

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

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

נכתוב במפורש את האיברים ב-S_3:

1. $\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$.
2. $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.
3. $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.
4. $\sigma^2 = \sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.
5. $\sigma\tau = \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.
6. $\tau\sigma = \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

מסקנה 8.4. 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 8.5. הסדר הוא $|S_n| = n!$. אכן, מספר האפשרויות לבחור את $\sigma(1)$ הוא n; אחר כך, מספר האפשרויות לבחור את $\sigma(2)$ הוא $n-1$; כך ממשיכים, עד שמספר האפשרויות לבחור את $\sigma(n)$ הוא 1, האיבר האחרון שלא בחרנו. בסך הכל, $|S_n| = n \cdot (n-1) \cdots 1 = n!$.

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

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

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

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

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

$$1 \mapsto 4 \mapsto 1$$

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

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

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

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

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

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

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

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

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

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

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

8.1 סימן של תמורה

הגדרה 8.12. יהי σ מחזור מאורך k, אזי הסימן שלו מוגדר להיות:

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

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

$$\mathrm{sign}(\sigma\tau) = \mathrm{sign}(\sigma)\,\mathrm{sign}(\tau)$$

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

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

דוגמה 8.13. (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.

הגדרה 8.14. חבורת החילופין (חבורת התמורות הזוגיות) A_n היא תת־החבורה הבאה של S_n:

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

הערה 8.15. הסדר של A_n הינו $|A_n| = \frac{n!}{2}$.

דוגמה 8.16. $A_3 = \{\mathrm{id}, (123), (132)\}$.
נשים לב כי $A_3 = \langle (123) \rangle$ כלומר A_3 ציקלית.

9 מחלקות שמאליות וימניות

הגדרה 9.1. תהי G חבורה, ותהי $H \leq G$. לכל $a \in G$ נגדיר מחלקות (cosets):

1. המחלקה השמאלית של a ביחס ל-H היא הקבוצה $aH = \{ah \,|\, h \in H\}$.
2. המחלקה הימנית של a ביחס ל-H היא הקבוצה $Ha = \{ha \,|\, h \in H\}$.

את אוסף המחלקות השמאליות ביחס ל-H נסמן ב-G/H.
(למה זה בכלל מעניין להגדיר אוסף זה? בתרגול הבא נראה שכאשר H תת־חבורה "מספיק טובה" (נקראת נורמלית), אז אוסף המחלקות יחד עם פעולה שמושרית מ-G יוצרים חבורה.)

הערה 9.2. עבור איבר היחידה e תמיד מתקיים $eH = H = He$.
אם החבורה G היא אבלית, אז המחלקה השמאלית של a ביחס ל-H שווה למחלקה הימנית:

$$aH = \{ah \,|\, h \in H\} = \{ha \,|\, h \in H\} = Ha$$

דוגמה 9.3. ניקח את $G = (\mathbb{Z}, +)$, ונסתכל על המחלקות השמאליות של $H = 5\mathbb{Z}$:

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

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

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

תרגיל 9.4. תנו דוגמה לחבורה G, תת־חבורה H ואיבר $a \in G$ כך ש-$aH \neq Ha$.

פתרון. חייבים לבחור חבורה G שאינה אבלית. נבחר $G = S_3$, את $H = \langle (1\ 2) \rangle = \{\mathrm{id}, (1\ 2)\}$ ואת $a = (1\ 3)$. מתקיים

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

נמשיך ונחשב את G/H: המחלקות השמאליות הן

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

כלומר $G/H=\{H,(1\ 3)\, H,(2\ 3)\, H\}$. נשים לב שאיחוד כל המחלקות הוא G, וזהו איחוד זר.

דוגמה אחרת (אם יש זמן): נבחר $G=GL_2(\mathbb{Q})$, ותהי $H=\{\left(\begin{smallmatrix}1&n\\0&1\end{smallmatrix}\right):n\in\mathbb{Z}\}$ תת־חבורה של G. נבחר $g=\left(\begin{smallmatrix}5&0\\0&1\end{smallmatrix}\right)$, ונחשב

$$\begin{aligned}gH&=\left\{\begin{pmatrix}5&0\\0&1\end{pmatrix}\begin{pmatrix}1&n\\0&1\end{pmatrix}:n\in\mathbb{Z}\right\}=\left\{\begin{pmatrix}5&5n\\0&1\end{pmatrix}:n\in\mathbb{Z}\right\}\\Hg&=\left\{\begin{pmatrix}1&n\\0&1\end{pmatrix}\begin{pmatrix}5&0\\0&1\end{pmatrix}:n\in\mathbb{Z}\right\}=\left\{\begin{pmatrix}5&n\\0&1\end{pmatrix}:n\in\mathbb{Z}\right\}\end{aligned}$$

וקל לראות כי לא רק ש-$gH\neq Hg$, אלא גם $gH\subsetneq Hg$.

הערה 9.5. המחלקות הם חלוקה של G, דהיינו $G=\cup aH$ ושתי מחלקות aH,bH הן או שוות $aH=bH$ או זרות $aH\cap bH=\varnothing$.

ולכן עומד מאחוריהן יח"ש וG/H הוא בעצם קבוצת המנה.

מהו יחס השקילות?\מתי שתי מחלקות הן שוות?

$$\begin{aligned}aH=bH&\iff ab^{-1}\in H\\&\iff \exists h\in H\,,\ a=bh\end{aligned}$$

הגדרה 9.6. מספר המחלקות (השמאליות) של H ב-G נקרא האינדקס (השמאלי) של H ב-G ומסומן $[G:H]$. למעשה $|G/H|=[G:H]$.

ככל שהאינדקס קטן יותר, כך תת־החבורה H גדולה יותר. בפרט, $[G:H]=1$ אם ורק אם $H=G$.

הערה 9.7. ישנה התאמה חח"ע ועל בין מחלקות שמאליות של $H\leq G$ ובין מחלקות ימניות לפי $gH\mapsto Hg^{-1}$. ניתן להבין התאמה זאת מכך שכל חבורה סגורה להופכי: $H^{-1}=H$. נחשב

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

בפרט קיבלנו שמספר המחלקות השמאליות שווה למספר המחלקות הימניות. לכן אין הבדל בין האינדקס השמאלי לבין האינדקס הימני של תת־חבורה, ופשוט נקרא לו האינדקס. בתרגיל הבית תדרשו להתאמה $gH\mapsto Hg$.

תרגיל 9.8. מצאו חבורה G ותת־חבורה H כך ש-$[G:H]=\infty$.

פתרון. נביא שתי דוגמאות:

1. נבחר $G=\mathbb{Z}\times\mathbb{Z}$ ואת $H=\mathbb{Z}\times\{0\}$. יהיו $a,b\in\mathbb{Z}$ שונים. אז

$$(0,a)+H=\{(n,a):n\in\mathbb{Z}\}\neq\{(n,b):n\in\mathbb{Z}\}=(0,b)+H$$

ולכן $[G:H]=\aleph_0$.

2. נבחר $G=\mathbb{R}\times\mathbb{R}$ ואת $H=\mathbb{R}\times\{0\}$, ואז מתקיים $[G:H]=\aleph$. כנ"ל עם $K=\mathbb{Q}\times\{0\}\leq H$.

10 משפט לגראנז' ושימושים

משפט 10.1 (משפט לגראנז'). תהי G חבורה ו-$H\leq G$. אז $|G|=[G:H]\,|H|$.

הערה 10.2. המשפט נכון עבור חשבון עוצמות. במקרה שהחבורה G היא סופית נקבל $[G:H]=\frac{|G|}{|H|}$, כלומר הסדר של תת־החבורה H מחלק את סדר החבורה G.
בפרט, מכיוון ואנו יודעים כי $o(a)=|\langle a\rangle|$ לכל $a\in G$, נקבל שהסדר של כל איבר מחלק את סדר החבורה.

תרגיל 10.3. תהא G חבורה מסדר 8. הוכיחו:

1. אם G היא ציקלית, אז קיימת תת־חבורה של G מסדר 4 (למה ברור כי תת־החבורה ציקלית?).
2. אם G לא אבלית, אז קיימת תת־חבורה ציקלית של G מסדר 4 (כאן הציקליות של תת־החבורה לא ברורה מיידית).
3. מצאו דוגמה נגדית לסעיף הקודם אם G אבלית.

פתרון. אם יש זמן בכיתה, נוכל לספר שיש בדיוק חמש חבורות מסדר 8 עד כדי איזומורפיזם (ואפילו מכל סדר p^3 עבור p ראשוני). בפתרון לא נשתמש במיון זה.

1. נניח $G=\langle g\rangle$ ציקלית מסדר 8 עם יוצר g. אזי קיימת תת־החבורה הציקלית שנוצרת על ידי $\langle g^2\rangle=\{e,g^2,g^4,g^6\}$.

2. תהא G חבורה לא אבלית. לפי משפט לגראנז', הסדר של כל איבר בחבורה סופית מחלק את סדר החבורה. לכן הסדרים האפשריים היחידים בחבורה מסדר 8 הם 1, 2, 4 או 8 (לא בהכרח כל הסדרים משתתפים).
יש רק איבר אחד מסדר 1 והוא איבר היחידה. לא ייתכן כי כל שאר האיברים הם מסדר 2, שכן לפי תרגיל שראינו נקבל כי G אבלית. אין בחבורה איבר מסדר 8, שכן אז היא תהיה ציקלית, וכל חבורה ציקלית היא אבלית. מכאן קיים איבר, נאמר $a \in G$, שהוא מסדר 4. הסדר של איבר הוא הסדר של תת־החבורה הציקלית $\{e, a, a^2, a^3\}$ שהוא יוצר.

3. במקרה זה G לא יכולה להיות ציקלית. נבחר את $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. אפשר לבדוק שהסדר של כל איבר בחבורה זו הוא 2, פרט לאיבר היחידה. לכן אין לה תת־חבורה ציקלית מסדר 4.

תרגיל 10.4 (אם יש זמן)**.** הכלילו את התרגיל האחרון: תהא G חבורה לא אבלית מסדר 2^t עבור $t > 2$. אזי קיימת ב-G תת־חבורה ציקלית מסדר 4.

פתרון. באופן דומה לשאלה האחרונה, הסדרים האפשריים היחידים בחבורה מסדר 2^t (כאשר $t > 2$) הם רק מן הצורה 2^k עבור $k \in \{0, 1, 2, \ldots, t\}$. ישנו רק איבר אחד מסדר 1. הסדר של כל שאר האיברים לא יכול להיות 2, כי אז G אבלית. אין איבר מסדר 2^t, שכן אז החבורה ציקלית ולכן אבלית. לכן קיים איבר, נאמר $a \in G$, כך ש-$o(a) = 2^k > 2$.

נתבונן בתת־החבורה $\langle a \rangle$ ונבחר את האיבר a^{k-2}. מתקיים

$$o(a^{2^{k-2}}) = \frac{2^k}{(2^k, 2^{k-2})} = 4$$

וקיבלנו שזהו האיבר שיוצר את תת־החבורה הציקלית הדרושה מסדר 4.

תרגיל 10.5. הוכיחו שחבורה סופית היא מסדר זוגי אם ורק אם קיים בה איבר מסדר 2.

פתרון. הכיוון $(\Rightarrow)$ הוא לפי לגראנז', שכן הסדר של האיבר מסדר 2 מחלק את סדר החבורה.

את הכיוון $(\Leftarrow)$ עשיתם בתרגיל בית.

כמסקנה מהתרגיל האחרון קיבלנו שבחבורה מסדר זוגי יש מספר אי זוגי של איברים מסדר 2.

מסקנה 10.6. נזכר בטענה ש-$o(a)|m$ אם ורק אם $a^m = e$. כעת אפשר להסיק שלכל איבר a בחבורה סופית G מתקיים $a^{|G|} = e$.

משפט 10.7 (משפט אוילר 2)**.** לכל $a \in U_n$ מתקיים $a^{\varphi(n)} \equiv 1 \pmod n$.

דוגמה 10.8. יהי p מספר ראשוני, ויהי $a \in U_p$. מתקיים $\varphi(p) = p - 1$ ולכן $a^{p-1} \equiv 1 \pmod p$. זהו למעשה משפט פרמה הקטן.

(הערה אם יש זמן: פונקציית קרמייקל (Carmichael) $\lambda(n)$ מוגדרת להיות המספר הטבעי m הקטן ביותר כך ש-$a^m \equiv 1 \pmod n$ לכל a שזר ל-n. ממשפט לגראנז' נקבל $\lambda(n)|\varphi(n)$. נסו למצוא דרך לחשב את $\lambda(n)$, ומתי $\lambda(n) \neq \varphi(n)$.)

תרגיל 10.9. מצאו את שתי הספרות האחרונות של $88211^{4039} + 2015$.

פתרון. אנו נדרשים למצוא את הביטוי מודולו 100, כלומר מספיק לחשב את

$$88211^{4039} + 2015 \equiv 11^{4039} + 15 \pmod{100}$$

אנו יודעים כי $\varphi(100) = 40$, ולפי משפט אוילר נקבל

$$11^{4039} \equiv 11^{100 \cdot 40} 11^{39} \equiv 11^{-1} \pmod{100}$$

ואנו יודעים כי יש הופכי כפלי ל-11 מודולו 100 מפני שהם זרים. אנו מחפשים פתרון למשוואה $11x \equiv 1 \pmod{100}$ שקיים אם ורק אם קיים $k \in \mathbb{Z}$ כך ש-$100k + 11x = 1$. אפשר למצוא פתרון למשוואה בעזרת אלגוריתם אוקלידס המורחב. נביע את $(100, 11)$ כצירוף לינארי שלהם:

$$(100, 11) \overset{100 = 9 \cdot 11 + 1}{=} (11, 1) = 1$$

כלומר $1 = 1 \cdot 100 - 9 \cdot 11$, ולכן $k = -9 \equiv 91 \pmod{100}$. קיבלנו

$$88211^{4039} + 2015 \equiv 11^{-1} + 15 \equiv 6 \pmod{100}$$

ולכן שתי הספרות האחרונות הן 06.

שאלה 10.10. ראינו מסקנה ממשפט לגרנז: עבור חבורה סופית G ואיבר $g \in G$ מתקיים $o(g)\,|\,|G|$. האם הכיוון ההפוך נכון?

כלומר, אם $|G| = n$ ו-$k|n$ אז האם יש איבר $a \in G$ מסדר k? **לא!**

<u>דוגמא נגדית</u> היא $G = \mathbb{Z}_4 \times \mathbb{Z}_4$, אמנם $|G| = 16$ ו-$8|16$ אבל אין איבר מסדר 8!

הערה 10.11. נעיר שבחבורה **ציקלית** סופית $G = \langle a \rangle$ זה **כן** מתקיים בעזרת נוסחת הקסם שראינו $o(a^t) = \dfrac{n}{(n,t)}$ (כאשר n זה סדר החבורה).

11 חבורות מוצגות סופית

בהרצאה ראיתם דרך לכתיבה 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 לכתיבה (לאו דווקא יחידה) כמילה סופית ביוצרים והופכיהם, ושכל אחד מן היחסים הוא מילה ששווה לאיבר היחידה.

דוגמה 11.1. 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 שיוויונות, למשל $x^n = e$.
באופן דומה, החבורה הציקלית האינסופית ניתנת ליצוג

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

ובדרך כלל משמיטים את קבוצת היחסים אם היא ריקה.

ודאו שאתם מבינים את ההבדל בין החבורות הלא איזומורפיות

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

הגדרה 11.2. 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 11.3. 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).

11.1 החבורה הדיהדרלית

הגדרה 11.4. עבור מספר טבעי n, הקבוצה D_n של סיבובים ושיקופים המעתיקים מצולע משוכלל בין n צלעות על עצמו, היא *החבורה הדיהדרלית* מדרגה n, יחד עם הפעולת של הרכבת פונקציות.

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

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

$$D_n = \left\langle \sigma, \tau \;\middle|\; \sigma^n = \tau^2 = \mathrm{id}, \sigma\tau = \tau\sigma^{-1} \right\rangle$$

הערה 11.5 (אם יש זמן). פונקציה $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ 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 α מתקיים $\alpha(L) = L$. במקרה זה α 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.

דוגמה 11.6. החבורה D_3 נוצרת על ידי סיבוב σ של $120°$ ועל ידי שיקוף τ, כך שמתקיימים היחסים הבאים בין היוצרים: $\sigma^3 = \tau^2 = \mathrm{id}$, $\tau\sigma\tau = \sigma^{-1}$. כלומר $D_3 = \{\mathrm{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ (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

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

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

סיכום 11.7. איברי D_n הם

$$\{\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{n-1}\}$$

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.)

12 תת־חבורות נורמליות

הגדרה 12.1. תת־חבורה $H \leq G$ נקראת תת־חבורה נורמלית אם לכל $g \in G$ מתקיים $gH = Hg$. במקרה זה נסמן $H \lhd G$.

משפט 12.2. תהי תת־חבורה $H \leq G$. התנאים הבאים שקולים:

1. $H \lhd G$.
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

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

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

דוגמה 12.3. אם G חבורה אבלית, אז כל תת־החבורות שלה הן נורמליות. הרי אם $h \in H \le G$, אז $g^{-1}hg = h \in H$. ההפך לא נכון. ברמת האיברים נורמליות **לא** שקולה לכך ש-$gh = hg$! זה אומר ש- $gh = h'g$ (חילופיות עם "מס מעבר").

דוגמה 12.4. מתקיים $SL_n(F) \lhd GL_n(F)$. 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 $\det : GL_n(F) \to F^*$.

דוגמה 12.5. $H = \langle (1\ 2) \rangle \le S_3$ אינה תת־חבורה נורמלית, כי כבר ראינו $H \neq (1\ 3)\, H$ $(1\ 3)\, H$.

דוגמה 12.6. עבור $n \ge 3$, תת־החבורה $\langle \tau \rangle \le D_n$ אינה נורמלית כי $\sigma \langle \tau \rangle \neq \langle \tau \rangle \sigma$.

טענה 12.7. תהי $H \le G$ תת־חבורה מאינדקס 2. אזי $H \lhd G$.

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 $aH = Ha$. $\square$

מסקנה 12.8. מתקיים $\langle \sigma \rangle \lhd D_n$ כי לפי משפט לגראנז' $[D_n : \langle \sigma \rangle] = \frac{2n}{n} = 2$. באופן דומה, $A_n \lhd S_n$ כי

$$[S_n : A_n] = \frac{n!}{n!/2} = 2$$

הערה 12.9. אם $K \le H \le G$ וגם $K \lhd G$, אז בוודאי $K \lhd H$. ההפך לא נכון. אם $K \lhd H$ וגם $H \lhd G$, אז לא בהכרח $K \lhd G$! למשל $\langle \tau \rangle \lhd \langle \tau, \sigma^2 \rangle \lhd D_4$ לפי הטענה הקודמת, אבל ראינו כי $\langle \tau \rangle$ לא נורמלית ב-D_4.

תרגיל 12.10 (לבית). לכל חבורה מסדר 8 יש תת־חבורה נורמלית לא טריוויאלית (מצאו תת־חבורה מאינדקס 2).

13 הומומורפיזמים

הגדרה 13.1. תהינה $(G,*)$, $(H,\bullet)$ חבורות. העתקה $f:G\to H$ 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:

1. הומומורפיזם שהוא חח"ע נקרא מונומורפיזם או שיכון. נאמר כי G משוכנת ב-H אם קיים שיכון $f:G\hookrightarrow H$.
2. הומומורפיזם שהוא על נקרא אפימורפיזם. נאמר כי H היא תמונה אפימורפית של G אם קיים אפימורפיזם $f:G\twoheadrightarrow H$.
3. הומומורפיזם שהוא חח"ע ועל נקרא איזומורפיזם. נאמר כי G ו-H איזומורפיות אם קיים איזומורפיזם $f:G\to H$. נסמן זאת $G\cong H$.
4. איזומורפיזם $f:G\to G$ נקרא אוטומורפיזם של G.
5. בכיתה נקצר את השמות של הומומורפיזם, מונומורפיזם, אפימורפיזם, איזומורפיזם ואוטומורפיזם להומ', מונו', אפי', איזו' ואוטו', בהתאמה.

הערה 13.2. העתקה $f:G\to H$ היא איזומורפיזם אם ורק אם קיימת העתקה $g:H\to G$ כך ש-$f\circ g=\mathrm{id}_H$ וגם $g\circ f=\mathrm{id}_G$.
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 שאיזומורפיזם הוא יחס שקילות.

תרגיל 13.3. הנה רשימה של כמה העתקות בין חבורות. קבעו האם הן הומומורפיזמים, ואם כן מהו סוגן:

1. $\varphi:\mathbb{R}\to\mathbb{R}^*$ המוגדרת לפי $x\mapsto e^x$ היא מונומורפיזם. מה היה קורה אם היינו מחליפים למרוכבים?
2. יהי F שדה. אז $\det:GL_n(F)\to F^*$ 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. $\varphi:\mathbb{R}\to\mathbb{R}^*$ המוגדרת לפי $x\mapsto x$ אינה הומומורפיזם כלל.

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

העובדה שהעתקה $f:G\to H$ היא הומומורפיזם גוררת אחריה 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.

4. הגרעין של f, כלומר $\ker f=\{g\in G: f(g)=e_H\}$, הוא תת־חבורה **נורמלית** של G.

5. התמונה של f, כלומר $\operatorname{im} f=\{f(g): g\in G\}$, היא תת־חבורה של H.

6. אם $G\cong H$, אז $|G|=|H|$.

תרגיל 13.4. יהי $f:G\to H$ הומומורפיזם. הוכיחו כי לכל $g\in G$ מסדר סופי מתקיים $o(f(g))|o(g)$.

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 $o(f(g))|n$. $\square$

תרגיל 13.5. 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 $f:G\to H$, אז הסדר של האיבר מסדר 4 היה מחלק את הסדר של המקור שלו. בחבורה G כל האיברים מסדר 1 או 2, לכן הדבר לא יתכן, ולכן החבורות לא איזומורפיות.

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

טענה 13.6 (לבית). יהי $f:G\to H$ הומומורפיזם. הוכיחו שאם G אבלית, אז $\operatorname{im} f$ אבלית. הסיקו שאם $G\cong H$, אז G אבלית אם ורק אם H אבלית.

תרגיל 13.7. יהי $f:G\to H$ הומומורפיזם. הוכיחו שאם G ציקלית, אז $\operatorname{im} f$ ציקלית.

הוכחה. נניח $G = \langle a \rangle$. נטען כי $\operatorname{im} f = \langle f(a) \rangle$. יהי $x \in \operatorname{im} f$ איבר כלשהו. לכן יש איבר $g \in G$ כך ש-$x = f(g)$ (כי $\operatorname{im} f$ 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. $\square$

תרגיל 13.8. האם קיים איזומורפיזם $f : S_3 \to \mathbb{Z}_6$?

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

תרגיל 13.9. האם קיים איזומורפיזם $f : (\mathbb{Q}^+, \cdot) \to (\mathbb{Q}, +)$?

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

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

תרגיל 13.11. האם קיים מונומורפיזם $f : GL_2(\mathbb{Q}) \to \mathbb{Q}^{10}$?

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

מסקנה. יתכנו ארבע הפרכות ברצף.

תרגיל 13.12. מתי ההעתקה $i : G \to G$ 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 אבלית.
כהערת אגב, השם של ההעתקה נבחר כדי לסמן inversion.

14 חבורות מנה

הגדרה 14.1. נוכל להגדיר על G/H מבנה של חבורה ע"י $(Ha)(Hb) = Hab$ אם ורק אם H היא תת־חבורה נורמלית. במקרה זה, זוהי חבורת המנה.
איבר היחידה הוא המחלקה H כי $(Ha)H = H(Ha) = Ha$.

דוגמה 14.2.
1. כבר (כמעט) השתכנענו ש-$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, n-1+n\mathbb{Z}\} \cong$ $\mathbb{Z}_n$.
2. $G/G \cong \{e\}$, $G/\{e\} \cong G$.
3. $\langle\sigma\rangle \lhd D_n$ ראינו שזה מאינדקס 2 ולכן $\{\langle\sigma\rangle, \langle\sigma\rangle\tau\} = {}^{D_n}/_{\langle\sigma\rangle} \cong \mathbb{Z}_2$. אמנם: $\langle\sigma\rangle\tau\langle\sigma\rangle\tau = \langle\sigma\rangle\tau\tau = \langle\sigma\rangle$.
4. $H = \mathbb{R}\times\{0\} \lhd \mathbb{R}^2$ נתאר את המנה
$$^{\mathbb{R}^2}/_H = \left\{(a,b)+H \,\middle|\, (a,b)\in\mathbb{R}^2\right\} = \{(0,b)+H \mid b\in\mathbb{R}\} = \{\mathbb{R}\times\{b\}\} \cong \mathbb{R}$$
אלו אוסף ישרים המקבילים לציר ה-x.
5. $H = \langle(1,1)\rangle \lhd \mathbb{Z}_4\times\mathbb{Z}_4$ נתאר את המנה
$$^{\mathbb{Z}_4\times\mathbb{Z}_4}/_H = \left\{(a,b)+H \,\middle|\, (a,b)\in\mathbb{Z}_4^2\right\} = \{(a',0)+H \mid a'=0,1,2,3\} \cong \mathbb{Z}_4$$

תרגיל 14.3. אם G אבלית ו$H \le G$ אזי G/H חבורה אבלית. מה לגבי הכיוון ההפוך?

פתרון. קודם כל נעיר שמכיוון שG אבלית H בהכרח נורמלית ולכן המנה היא באמת חבורה.
צריך להוכיח $HaHb = HbHa$, ובאמת $HaHb = Hab = Hba = HbHa$ כי G אבלית.
הכיוון ההפוך לא נכון. עבור $\langle\sigma\rangle \lhd D_n$ ראינו שהמנה $\mathbb{Z}_2$ היא אבלית, וגם תת־החבורה הנורמלית $\langle\sigma\rangle$ אבלית, אבל D_n לא אבלית.

תרגיל 14.4. אם G ציקלית ו-$H \le G$ אז G/H ציקלית. מה לגבי הכיוון ההפוך?

תרגיל 14.5. תהי G חבורה (לאו דווקא סופית), ותהי $H \lhd G$ 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 G מתקיים לכל $g\in G$ כי $g^{|G|} = e$.
יהי $a\in G$, אזי $aH \in G/H$. ידוע לנו כי $|G/H| = n$. ולכן
$$a^nH = (aH)^n = e_{G/H} = H$$
כלומר קיבלנו $a^n \in H$.

תרגיל 14.6. תהי G חבורה סופית ו-$N \lhd G$ המקיימת $\gcd(|N|, [G\colon N]) = 1$.
הוכיחו כי N מכילה כל איבר של G מסדר המחלק את $|N|$. כלומר $x \in N \Longleftarrow x^{|N|} = e$.

פתרון. יהי $x \in G$ כך ש-$x^{|N|} = e$.
מכיוון ו-$\gcd(|N|, [G\colon N]) = 1$ ניתן לרשום $1 = s|N| + r[G\colon N]$ ואז

$$x = x^1 = x^{s|N| + r[G\colon N]} = x^{r[G\colon N]} \in N$$

לפי התרגיל הקודם.

תרגיל 14.7. 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 $T \lhd G$.
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

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

ולכן $g^{-1}Tg \subseteq T$. כלומר $T \lhd G$.
עבור הסעיף השני, נניח בשלילה כי קיים איבר $e_{G/T} \neq xT \in G/T$ מסדר סופי $o(xT) = n$. איבר היחידה הוא $e_{G/T} = T$, ולכן $x \notin T$. מתקיים $(xT)^n = T$, ונקבל כי $x^n \in T$. אם x^n 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 $G \lhd G$, ואז $G/T \cong \{e\}$. אם $G = \mathbb{C}^*$, אז $T = \Omega_\infty = \bigcup_n \Omega_n$. כלומר כל מספר מרוכב לא אפסי עם ערך מוחלט השונה מ-1 הוא מסדר אינסופי.

15 משפטי האיזומורפיזם של נתר

משפט 15.1 (משפט האיזומורפיזם הראשון)**.** יהי הומומורפיזם $f: G \to H$. אז

$$G/_{\ker f} \cong \operatorname{im} f$$
$$(Kerf)g \mapsto f(g)$$

בפרט, יהי אפימורפיזם $\varphi: G \to H$. אז $G/_{\ker \varphi} \cong H$.

דוגמה 15.2. ראינו ש-$\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ הוא אפימורפיזם.
הגרעין הוא בדיוק $\mathrm{SL}_n(\mathbb{R})$ ולכן $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^*$.

תרגיל 15.3. תהי $G = \mathbb{R} \times \mathbb{R}$, ותהי $H = \{(x,y) \in \mathbb{R} \times \mathbb{R} \,|\, y = 3x\}$. הוכיחו כי $G/H \cong \mathbb{R}$.

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

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

לפי משפט האיזומורפיזם הראשון, נקבל את הדרוש. $\square$

תרגיל 15.4. נסמן $\mathbb{T} = \{z \in \mathbb{C} \,|\, |z| = 1\}$. זו חבורה כפלית. הוכיחו כי $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$.

הוכחה. נגדיר $f : \mathbb{R} \to \mathbb{T}$ 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:

$$\ker f = \left\{x \in \mathbb{R} \,\middle|\, e^{2\pi i x} = 1\right\} = \mathbb{Z}$$

לפי משפט האיזומורפיזם הראשון, נקבל

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

$\square$

תרגיל 15.5. יהי הומומורפיזם $f : \mathbb{Z}_{14} \to D_{10}$. מה יכול להיות $\ker f$?

פתרון. נסמן $K = \ker f$. מכיוון ש-$K \lhd \mathbb{Z}_{14}$, אז $|K| \,|\, |\mathbb{Z}_{14}| = 14$. לכן $|K| \in \{1,2,7,14\}$. נבדוק עבור כל מקרה.
אם $|K| = 1$, אז f הוא חח"ע וממשפט האיזומורפיזם הראשון נקבל $\mathbb{Z}_{14}/K \cong \operatorname{im} f$. לכן $\operatorname{im} f \cong \mathbb{Z}_{14}$. ידוע לנו כי $\operatorname{im} f \leq D_{10}$ ולכן $|\operatorname{im} f| \,|\, |D_{10}| = 20$. אבל 14 אינו מחלק את 20, ולכן $|K| \neq 1$.
אם $|K| = 2$, אז בדומה לחישוב הקודם נקבל

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

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

אם $|K| = 7$, נראה כי קיים הומומורפיזם כזה. ניקח תת־חבורה $H = \{\mathrm{id}, \tau\}$ (כל תת־חבורה מסדר 2 תתאים) של D_{10}, ונבנה אפימורפיזם $\mathbb{Z}_{14} \to H \leq D_{10}$. המספרים האי זוגיים ישלחו ל-τ, 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 ההומומורפיזם הטריוויאלי.

תרגיל 15.6. תהיינה G_1 ו-G_2 חבורות סופיות כך ש-$(|G_1|, |G_2|) = 1$. מצאו את כל ההומומורפיזמים $f : G_1 \to G_2$.

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

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

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

תרגיל 15.7. 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 איזשהו $H \lhd D_4$. לכן מספיק לדעת מיהן כל תת־החבורות הנורמליות של D_4.

קודם כל, יש לנו את תת־החבורות הטריוויאליות $D_4 \lhd D_4, \{\mathrm{id}\}$; לכן, קיבלנו את התמונות האפימורפיות $D_4/\{\mathrm{id}\} \cong D_4$ ו-$D_4/D_4 \cong \{\mathrm{id}\}$.

כעת, אנו יודעים כי $Z(D_4) = \langle \sigma^2 \rangle \lhd D_4$. 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 $f : D_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ 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 $\langle \sigma \rangle \lhd D_4$, 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 $\langle \sigma^2, \tau \rangle, \langle \sigma^2, \tau\sigma \rangle \lhd D_4$ 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 $\langle\tau\sigma^i\rangle=\{\mathrm{id},\tau\sigma^i\}$. כדי שהיא תהיה נורמלית, צריך להתקיים

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

לכן בהכרח $i=2$. אבל אז

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

ולכן $H\ntriangleleft D_4$. מכאן שכתבנו את כל תת־החבורות הנורמליות של D_4, ולכן כל התמונות האפימורפיות של D_4 הן $\{\mathrm{id}\}\,,\mathbb{Z}_2,\mathbb{Z}_2\times\mathbb{Z}_2,D_4$.

המטרה של שאר משפטי האיזומורפיזם הם לתאר את תת־החבורות של המנה G/N, אחרי זה נשאל על תת־החבורות הנורמליות ואז על המנות. נראה שכל הזמן יש קשר לתת־חבורות, תת־חבורות נורמליות ומנות של G.

משפט 15.8 (משפט האיזומורפיזם השני). תהי G חבורה, $H\leq G$ ו-$N\lhd G$, אזי

$$^{NH}\!/_{N}\cong{}^{H}\!/_{N\cap H}$$

ובמובלע: $H \lhd N\cap H$,$NH \lhd N$.

דוגמה 15.9. ניקח $H=15\mathbb{Z}\leq\mathbb{Z}$ ו-$N=6\mathbb{Z}$. אזי

$$\begin{aligned}&"NH"=N+H=(6,15)\mathbb{Z}=3\mathbb{Z}\\&N\cap H=[6,15]\mathbb{Z}=30\mathbb{Z}\end{aligned}$$

ולכן

$$^{3\mathbb{Z}}\!/_{6\mathbb{Z}}\cong{}^{15\mathbb{Z}}\!/_{30\mathbb{Z}}$$

משפט 15.10. תהי G חבורה ו-$K\lhd G$ תת־חבורה נורמלית.

1. כל תת־החבורות (הנורמליות) של G/K הן מהצורה H/K עבור תת־חבורה (נורמלית) $H\leq G$ המכילה את K.
2. (משפט האיזומורפיזם השלישי) תהי $K\leq H$ תת־חבורה נורמלית של G אזי $^{G/K}\!/_{H/K}\cong G/H$.

בפרט $[G:K]=[G:N][N:K]$ (כפליות האינדקס).

דוגמה 15.11. $4\mathbb{Z} \leq 2\mathbb{Z}$ אז

$$\mathbb{Z}/4\mathbb{Z}\big/_{2\mathbb{Z}/4\mathbb{Z}} \cong \mathbb{Z}\big/_{2\mathbb{Z}}$$

תרגיל 15.12. תהי $N \lhd G$ מאינדקס ראשוני p, ותהי $K \leq G$. הוכיחו כי או $K \subseteq N$ או ש-$G = NK$ ו- $[K\colon K \cap N] = p$.

פתרון. נתבונן ב-$N \leq NK \leq G$. מכפליות האינדקס נקבל $[NK\colon N] \mid [G\colon N] = p$ ולכן $[NK\colon N] = 1, p$.

אם $[NK : N] = p$ אז אין ברירה ו-1 $[G : KN] = 1$ מה שאומר $G = NK$. בנוסף ממשפט האיזו' השני $[K : K \cap N] = [NK : N] = p$.

אם $[NK : N] = 1$ אז לפי משפט האיזו' השני $[K : K \cap N] = 1$ מה שאומר ש-$K \subseteq N$.