תורת החבורות
מערכי תרגול קורס 88-218

דצמבר 2019, גרסה 1.11

אוניברסיטת בר-אילן סמסטר א׳ תש״ף

תוכן העניינים

מבוא

נתחיל עם כמה הערות:

- דף הקורס נמצא באתר www.math-wiki.com.
- שאלות בנוגע לחומר הלימודי מומלץ לשאול בדף השיחה באתר של הקורס.
- יפורסמו תרגילי בית כל שבוע, ומתוכנן בוחן.
- החומר בקובץ זה נאסף מכמה מקורות, ומבוסס בעיקרו על מערכי תרגול קודמים בקורס אלגברה מופשטת למתמטיקה באוניברסיטת בר-אילן.
- נשמח לכל הערה על מסמך זה.

מחברים בשנת הלימודים תשע"ז: תומר באואר ושירה גילת
עדכונים בשנת הלימודים תשע"ח: תומר באואר

1 מבוא לתורת המספרים

נסמן כמה קבוצות של מספרים:

- $\mathbb{N}=\{1,2,3,\dots\}$ המספרים הטבעיים.
- $\mathbb{Z}=\{0,\pm1,\pm2,\pm3,\dots\}$ המספרים השלמים (מגרמנית: Zahlen).
- $\mathbb{Q}=\left\{\frac{p}{q}\,\middle|\,p\in\mathbb{Z},q\in\mathbb{Z}\setminus\{0\}\right\}$ המספרים הרציונליים.
- $\mathbb{R}$ המספרים הממשיים.
- $\mathbb{C}$ המספרים המרוכבים.

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

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

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

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

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

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

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

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

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

הוכחה. נסמן $d=(n,m)$, וצ"ל כי $d=(m,r)$. אנו יודעים כי $d|n$ וגם $d|m$. אנו יכולים להציג את r כצירוף לינארי של n,m, ולכן $d|r=n-qm$. מכך קיבלנו $d\le(m,r)$. 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 $(m,r)\le d$. סך הכל קיבלנו כי $d=(m,r)$. $\square$

הערה 1.6. תמיד מתקיים $(n,m)=(m,n)=(\pm n,\pm m)$.

משפט 1.7 (אלגוריתם אוקלידס)**.** "המתכון" למציאת ממ"מ בעזרת שימוש חוזר בטענה 1.5 הוא אלגוריתם אוקלידס. ניתן להניח $0 \leq m < n$ לפי ההערה הקודמת. 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 1.8. נחשב את הממ"מ של 53 ו-47 בעזרת אלגוריתם אוקלידס

$$\begin{aligned}(53,47) &= [53 = 1\cdot 47 + 6]\\ (47,6) &= [47 = 7\cdot 6 + 5]\\ (6,5) &= [6 = 1\cdot 5 + 1]\\ (5,1) &= [5 = 5\cdot 1 + 0]\\ (1,0) &= 1\end{aligned}$$

ואם יש זמן, 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 מספר עוקבים בסדרת פיבונצ'י.

משפט 1.9 (אפיון הממ"מ כצירוף לינארי מזערי)**.** לכל מספרים שלמים $a, b \neq 0$ מתקיים כי

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

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

הוכחה. נתבונן בקבוצה

$$S_{a,b} = \{ua + vb \,|\, u, v \in \mathbb{Z}\}$$

נשים לב כי $S_{a,b}$ אינה ריקה, כי למשל $\pm b \in S_{a,b}$. יהי d המספר הטבעי הקטן ביותר ב-S.

אנו רוצים להראות כי $d = (a,b)$. מפני ש-$d \in S_{a,b}$, אז קיימים $s, t \in \mathbb{Z}$ כך ש-$d = sa + tb$. נחלק את a ב-d עם שארית, ונקבל $a = qd + r$ כאשר $0 \leq r < d$. כעת מתקיים

$$r = a - qd = a - q(sa + tb) = (1 - qs)a + tb \in S_{a,b}$$

אבל אמרנו כי d הינו הטבעי הקטן ביותר ב-$S_{a,b}$, ולכן בהכרח $r = 0$. כלומר $d|a$, ובאופן דומה נקבל $d|b$. לכן מהגדרת הממ"מ נובע $d \leq (a,b)$. מצד שני, $(a,b)\,|a$ וגם

$(a,b)\,|b$, ולכן (a,b) מחלק גם כל צירוף לינארי של a ושל b. בפרט, $(a,b)\,|d$, ולכן $(a,b) \le d$. בסך הכל קיבלנו $(a,b) = d$.

הוכחה נוספת: ניתן להניח $a \ge b > 0$, וקל להוכיח ש-$\gcd(a,b) = \gcd(a-b,b)$. עבור $a = b = 1$ מתקיים כי

$$\gcd(a,b) = 1 = 1 \cdot 1 + 0 \cdot 1$$

ונניח שהטענה נכונה עבור כל $a + b < m$. נוכיח שהיא נכונה עבור $a + b = m$. אם $a = b$, אז

$$\gcd(a,b) = 1 \cdot a + 0 \cdot b = a$$

ואחרת $\gcd(a,b) = \gcd(a-b,b)$ והנחת האינדוקציה נכונה עבור $a-b, b$. לכן

$$\gcd(a,b) = s(a-b) + tb = sa + (t-s)b$$

צירוף לינארי כדרוש. $\square$

הערה 1.10 (לדלג). יהי $n \in \mathbb{Z}$. נסמן את הכפולות שלו ב-$n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$. למשל $4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$. מן המשפט האחרון נוכל להסיק כי $S_{a,b} = (a,b)\,\mathbb{Z}$, שכן לכל $x \in S_{a,b}$ מתקיים כי $(a,b)\,|x$.

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

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

מסקנה 1.12. אם p ראשוני וגם $p|bc$, אז $p|b$ או $p|c$.

פתרון. אם $p|b$, אז סיימנו. אחרת, $p \nmid b$ ולכן $(p,b) = 1$, ולפי התרגיל הקודם $p|c$.

דוגמה 1.13. 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 $(234,61) = 1 = 6\cdot 234 - 23\cdot 61$. כלומר $s = 6, t = -23$.

טענה 1.14. תכונות של ממ״מ:

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

ב. $(an,am)=|a|\,(n,m)$

הוכחה.

א. 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.

ב. (חלק מתרגיל הבית) $\square$

שאלה 1.15 (לבית). אפשר להגדיר ממ"מ ליותר מזוג מספרים. יהי d הממ"מ של המספרים $n_1,\ldots,n_k$. הראו שקיימים מספרים שלמים $s_1,\ldots,s_k$ המקיימים $s_1n_1+\cdots+s_kn_k=d$. רמז: אינדוקציה על k.

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

תרגיל 1.18. מצאו את הספרה האחרונה של 333^{333}.

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

$$3^{333}=3^{4\cdot 83+1}=\left(3^4\right)^{83}\cdot 3=81^{83}\cdot 3\equiv 1^{83}\cdot 3 \pmod{10}$$
$$333^{333}=3^{333}\equiv 3 \pmod{10}$$

ומכאן שהספרה האחרונה היא 3. בהמשך נגלה מדוע נבחר 3^4.

משפט 1.19 (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

$$bsn+atm\equiv atm\equiv a\cdot 1\equiv a \pmod n$$
$$bsn+atm\equiv bsn\equiv b\cdot 1\equiv b \pmod m$$

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 (לפחות אחד) המתאים לו מודולו nm. ישנם בסה"כ nm זוגות שונים (a,b) (מודולו x 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 1.20. 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 1.21 (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 $\{a_i \, (\mathrm{mod} m_i) \mid 1 \le i \le k\}$, 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 1.22. 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 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.

הגדרה 1.23 (לבית)**.** בהנתן שני מספרים שלמים n, m הכפולה המשותפת המזערית (כמ"מ, least common multiple) שלהם מוגדרת להיות

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

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

טענה 1.24. תכונות של כמ"מ:

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

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

2 מבנים אלגבריים בסיסיים

הגדרה 2.1. אגודה (semigroup, או חבורה למחצה) 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 2.2. $\mathbb{Z}$, מילים ושירשור מילים, קבוצה X עם הפעולה $a * b = b$.

דוגמה 2.3. המערכת $(\mathbb{Z}, -)$ אינה אגודה, מפני שפעולת החיסור אינה קיבוצית. למשל $(5-2)-1 \neq 5-(2-1)$.

הגדרה 2.4. תהי $(S, *)$ אגודה. איבר $e \in S$ נקרא איבר יחידה אם לכל $a \in S$ מתקיים $a * e = e * a = a$. אגודה שבה קיים איבר יחידה נקראת מונואיד (monoid, או יחידון).

דוגמה 2.5. $\mathbb{Z}$, מטריצות ריבועיות מעל שדה, פונקציות על קבוצה X. גם $(\mathbb{N}, \cdot)$ היא מונואיד, ואיבר היחידה שלה הוא 1. לעומת זאת, $(2\mathbb{N}, \cdot)$ היא אגודה שאינה מונואיד, כי אין בה איבר יחידה.

הערה 2.6. יהי M מונואיד. קל לראות כי איבר היחידה ב-M הוא יחיד.

דוגמה 2.7. תהי X קבוצה כלשהי, ותהי $P(X)$ קבוצת החזקה שלה (זהו אוסף כל תת־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 2.8. יהי $(M, *, e)$ מונואיד.
איבר יקרא הפיך אם קיים איבר $b \in M$ כך ש-$ba = ab = e$. במקרה זה $b = a^{-1}$ יקרא הופכי של a.

תרגיל 2.9 (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 2.10. 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 $X^X = \{f \colon X \to X\}$. ביחס לפעולת ההרכבה זהו מונואיד, ואיבר היחידה בו הוא העתקת הזהות id.

ההפיכים משמאל הם הפונקציות החח"ע. ההפיכים מימין הם הפונקציות על (לפי הקורס מתמטיקה בדידה. הוכחה לבית). 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 2.11 (ממבחן). הוכיחו כי לכל מונואיד $(X,\cdot)$ הקבוצה $P_*(X)$ של כל תת־הקבוצות הלא ריקות של X מגדירה מונואיד ביחס לפעולת הכפל הנקודתית:

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

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

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

א. סגירות הפעולה.

ב. קיבוציות הפעולה.

ג. קיום איבר יחידה.

ד. כל איבר הוא הפיך.

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

דוגמה 2.13. (עבור קבוצה סופית אחת הדרכים להגדיר פעולה בינארית היא בעזרת לוח כפל.) למשל, אם $S = \{a, b\}$ ונגדיר

$*$	a	b
a	a	b
b	b	a

אז קל לראות שמתקיימת סגירות, אסוציאטיביות, a הוא יחידה ו-b הוא ההופכי של עצמו.

למעשה, זוהי החבורה היחידה עם שני איברים (עד כדי שינוי שמות).

דוגמה 2.14. קבוצה בעלת איבר אחד ופעולה סגורה היא חבורה. לחבורה זו קוראים החבורה הטריוויאלית.

דוגמה 2.15. $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ חבורות ביחס לחיבור. מה קורה עם כפל? (כל שדה הוא חבורה חיבורית ומונואיד כפלי).

דוגמה 2.16. לכל $n \in \mathbb{Z}$ מתקיים כי $(n\mathbb{Z}, +)$ היא חבורה שאיבר היחידה בה הוא 0. בכתיב חיבורי מקובל לסמן את האיבר ההופכי של a בסימון $-a$. כתיב זה מתלכד עם המושג המוכר של מספר נגדי ביחס לחיבור.

דוגמה 2.17. נסתכל על אוסף מחלקות השקילות מודולו n, שמקובל לסמן $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{[a] \mid a \in \mathbb{Z}\}$. למשל $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$. לפעמים מסמנים את מחלקת השקילות $[a]$ בסימון $\overline{a}$, 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 $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$. 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 אגודה). בהמשך נראה איך אפשר "להציל" את הכפל.

הגדרה 2.18 (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).

הערה 2.19. מתקיים $U(M) = M$ אם ורק אם M היא חבורה.

הגדרה 2.20. המערכת $(M_n(\mathbb{R}), \cdot)$ של מטריצות ממשיות בגודל $n \times n$ עם כפל מטריצות היא מונואיד. לחבורת ההפיכים שלו

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

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

אתגר נסמן ב-$M_{\mathbb{N}}^\circ(F)$ את אוסף המטריצות האינסופיות מעל השדה F שבכל שורה ובכל עמודה יש להן רק מספר סופי של איברים ששונה מאפס. הוכיחו שפעולת הכפל הופכת את $M_{\mathbb{N}}^\circ(F)$ למונואיד שאינו חבורה (צריך להראות גם סגירות לפעולה!). הראו שבמקרה זה יש הבדל בין הפיכות משמאל להפיכות מימין.

3 חבורות אבליות

הגדרה 3.1. 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 3.2. יהי F שדה. החבורה $(GL_n(F), \cdot)$ אינה אבלית עבור $n > 1$.

דוגמה 3.3. מרחב וקטורי V יחד עם פעולת חיבור וקטורים הרגילה הוא חבורה אבלית.

תרגיל 3.4. 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. $\square$

הערה 3.5. אמנם אנחנו רגילים מהעבר שפעולות הן בדרך כלל חילופיות, אך יש פעולות משמעותיות מאוד שאינן חילופיות (כגון כפל מטריצות והרכבת פונקציות). אחת מהמטרות בתורת החבורות היא להבין את אותן פעולות. ככלל, הפעולות בהן נדון תהינה תמיד קיבוציות (חלק מהגדרת חבורה), אך לא בהכרח חילופיות.

הגדרה 3.6. תהי G חבורה. נאמר ששני איברים $a, b \in G$ מתחלפים אם $ab = ba$. נגדיר את המֶרְכָּז של חבורה G להיות

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

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

דוגמה 3.7. חבורה G היא אבלית אם ורק אם $Z(G) = G$. האם אתם יכולים להראות שבהנתן חבורה G, אז גם $Z(G)$ היא חבורה?

4 תת־חבורות

הגדרה 4.1. 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). במקרה כזה נסמן $H \leq G$.

בפועל מה שצריך לבדוק כדי להוכיח ש-$H \leq G$:

- תת־הקבוצה H לא ריקה (בדרך כלל קל להראות $e \in H$).
- סגירות לפעולה: לכל $a, b \in H$ מתקיים $ab \in H$.
- סגירות להופכי: לכל $a \in H$ מתקיים $a^{-1} \in H$.

דוגמה 4.2. נוכיח שקבוצת המטריצות

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

היא תת־חבורה של $GL_3(\mathbb{R})$.

- $H \neq \varnothing$ כי ברור ש- $I_3 \in H$ (שהיא איבר היחידה של G ולכן גם של H).
- יש סגירות לפעולה כי לכל זוג איברים

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

- אפשר לראות שהמטריצות ב-H הפיכות 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 4.3. $GL_n(F) \geq \{A \in GL_n(F) \,|\, \det A = 1\} = SL_n(F)$. קוראים לה החבורה הלינארית המיוחדת מדרגה n מעל F.

דוגמה 4.4. לכל חבורה G מתקיים כי $Z(G) \leq G$.

5 חבורת אוילר ומציאת הופכי

הגדרה 5.1. נגדיר את חבורת אוילר (Euler) להיות $U_n = U(\mathbb{Z}_n, \cdot)$ לגבי פעולת הכפל מודולו n.

דוגמה 5.2. 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.

טענה 5.3 (בהרצאה). 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.

יש לנו דרך למצוא את ההופכי של m: ראינו שקיימים s, t כך ש-$sn + tm = 1$. אם נחשב מודולו n נקבל $tm \equiv 1$ כלומר ש-$m^{-1} = t$ ב-$(\mathbb{Z}_n, \cdot)$. קיבלנו שההופכי הוא המקדם המתאים בצירוף של הממ"מ.

הערה 5.4. אם p הוא מספר ראשוני, אז $U_p = \mathbb{Z}_p^*$.

דוגמה 5.5. $U_{12} = \{1, 5, 7, 11\}$.

דוגמה 5.6. לא קיים ל-5 הופכי כפלי ב-$\mathbb{Z}_{10}$, שכן אחרת 5 היה זר ל-10 וזו סתירה.

תרגיל 5.7. מצאו $0 \le x \in \mathbb{Z}$ כך ש-$61x \equiv 1 \pmod{234}$.

פתרון. לפי הנתון, קיים $k \in \mathbb{Z}$ כך ש-$61x + 234k \equiv 1$. זאת אומרת ש-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. בדוגמה 1.13 ראינו כי $1 = 6 \cdot 234 - 23 \cdot 61$. לכן $x \equiv -23 \pmod{234}$ הוא ההופכי, וכדי להבטיח כי x אינו שלילי נבחר $x = 211$.

6 חבורות ציקליות

הגדרה 6.1. תהי G חבורה, ויהי $a \in G$. תת־החבורה הנוצרת על ידי a היא $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$.

הגדרה 6.2. תהי G חבורה ויהי $a \in G$. אם $G = \langle a \rangle$ נאמר כי G חבורה ציקלית ושהיא נוצרת על ידי a. כלומר כל איבר ב-G הוא חזקה (חיובית או שלילית) של היוצר a.

דוגמה 6.3. רשימה של כמה תת־חבורות ציקליות:

א. $\mathbb{Z}$ נוצרת על ידי 1. שימו לב שהיוצר לא חייב להיות יחיד. למשל גם -1 הוא יוצר.

ב. $n\mathbb{Z} = \langle n \rangle$.

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

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

ה. עבור $a = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in GL_3(\mathbb{R})$,

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

7 סדר של חבורה וסדר של איבר

הגדרה 7.1. הסדר של חבורה G הוא עוצמתה כקבוצה, ומסומן $|G|$. במילים יותר גשמיות, כמה איברים יש בחבורה.

דוגמה 7.2. $|\mathbb{Z}| = \infty$, $|\mathbb{Z}_n| = n$.

הגדרה 7.3. פונקציית אוילר מוגדרת לפי $\varphi(n) = |U_n|$. לפי טענה 5.3 נסיק שהיא סופרת כמה מספרים קטנים וזרים ל-n:

$$\varphi(n) = |\{a \,|\, 0 \le a < n,\ (a,n) = 1\}|$$

דוגמה 7.4. 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, בתרגיל הבית תוכיחו כי $(a,b) = 1$ אם ורק אם $\varphi(ab) = \varphi(a)\varphi(b)$.

מכאן מתקבלת ההכללה: יהי $n = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ אז $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_n}\right)$.
למשל כדי לחשב את $|U_{60}|$, נזכר כי $60 = 2^2 \cdot 3 \cdot 5$ ולכן

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

הגדרה 7.5. יהי $a \in G$ איבר בחבורה. הסדר של a הוא $o(a) = \min\{n \in \mathbb{N} \,|\, a^n = e\}$. אם לא קיים כזה, נאמר שהסדר הוא אינסוף. בכל חבורה הסדר של איבר היחידה הוא 1, וזהו האיבר היחיד מסדר 1.

דוגמה 7.6. בחבורה U_6, $o(1) = 1, o(5) = 2$.

דוגמה 7.7. בחבורה $\mathbb{Z}_6$, $o(2) = o(4) = 3$, $o(3) = 2$, $o(1) = o(5) = 6$.

דוגמה 7.8. בחבורה $GL_2(\mathbb{R})$ 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 7.9. תהי G חבורה, ויהי $a \in G$. מתקיים $a^n = e$ אם ורק אם $o(a) \,|\, n$.

טענה 7.10. תהי G חבורה. יהיו $a, b \in G$ מסדר סופי 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 $o(ab) = [o(a), o(b)]$.

דוגמה 7.11. עבור $G = H_1 \times H_2$ והאיברים $a \in H_1$ ו-$b \in H_2$ הסדר של $(a, b) \in G$ הוא $[o(a), o(b)]$. הרי (a, e_2) מתחלף עם (e_1, b) ו-$\langle (a, e_2) \rangle \cap \langle (e_1, b) \rangle = \{e_G\} =$ (e_1, e_2).

הוכחה. נסמן $n = o(a)$ ו-$m = o(b)$. נראה ש-$o(ab)$ מחלק את $[n, m]$:

$$(ab)^{[n,m]} = a^{[n,m]} b^{[n,m]} = e \cdot e$$

כי $ab = ba$ ו-n, m מחלקים את $[n, m]$. לפי טענה 7.9 קיבלנו $o(ab) | [n, m]$.

מצד שני, כדי להוכיח מינימליות, אם $(ab)^t = e$, אז $a^t = b^{-t}$. לכן

$$a^t, b^{-t} \in \langle a \rangle \cap \langle b \rangle = e$$

כלומר $n | t$ וגם $m | t$, ולכן $[n, m] | t$. כלומר $o(ab) = [o(a), o(b)]$. $\square$

משפט 7.12. הסדר של איבר x שווה לסדר תת־החבורה שהוא יוצר, כלומר ל-$|\langle x \rangle|$.

בפרט, נניח G חבורה מסדר n, אז G היא ציקלית אם ורק אם קיים איבר מסדר n.

דוגמה 7.13. ב-U_8 קל לבדוק ש-$o(3) = o(5) = o(7) = 2$ ולכן החבורה אינה ציקלית.

תרגיל 7.14. האם $\mathbb{Z}_n \times \mathbb{Z}_n$ היא ציקלית?

פתרון. הסדר של החבורה הוא n^2. על מנת 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. כלומר $\mathbb{Z}_n \times \mathbb{Z}_n$ לא ציקלית עבור $n > 1$.

תרגיל 7.15. תהי G חבורה אבלית. הוכיחו שאוסף האיברים מסדר סופי, שנסמן T (עבור torsion), הוא תת־חבורה.

פתרון. נוכיח את התנאים הדרושים לתת־חבורה:

- $T \neq \varnothing$ כי $e \in T$, שהרי $o(e) = 1$.
- סגירות לפעולה: יהיו $a, b \in T$. אז יש n, m טבעיים כך ש-$a^n = b^m = e$. אזי: $(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = e^m e^n = e$. (שימו לב לשימוש בחילופיות!)
- סגירות להופכי: יהי $a \in T$. 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 7.16. 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 7.15. כמו כן, אם G סופית, נקבל כי $T = G$. באופן כללי, התשובה היא לא.

הנה דוגמה נגדית: נבחר את $GL_2(\mathbb{R})$, 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 7.17. מספר תכונות של הסדר:

א. בחבורה סופית הסדר של כל איבר הוא סופי.

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

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

ד. $o(a) = o(a^{-1})$.

פתרון. נוכיח את הסעיף האחרון, לפי שני מקרים:

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

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

כאשר המעבר $\star$ 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 $o(a^{-1}) \leq n = o\left(a\right)$.
כעת, צריך להוכיח את אי-השוויון השני. אם נחליף את a ב-a^{-1}, נקבל $o(a) = o\left((a^{-1})^{-1}\right) \leq o(a^{-1})$. 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 $o(a^{-1})=\infty$.

הערה 7.18. יהי $a\in G$. אזי $o\left(a\right)=\left|\left\langle a\right\rangle\right|$. במילים, הסדר של איבר הוא סדר תת־החבורה שהוא יוצר.

תרגיל 7.19 (מההרצאה). תהי G חבורה, ויהי $a\in G$. נניח $o\left(a\right)=n<\infty$. הוכיחו שלכל $d\le n$ טבעי,

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

הוכחה. תחילה נוכיח היתכנות: נשים לב כי

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

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

כעת נוכיח את המינימליות: נניח $\left(a^{d}\right)^{t}=e$, כלומר $a^{dt}=e$. לפי טענה 7.9, $n|dt$. לכן, גם $\dfrac{n}{(d,n)}\Big|\dfrac{dt}{(d,n)}$ (שניהם מספרים שלמים – מדוע?). מצד שני, $\left(\dfrac{n}{(d,n)},\dfrac{d}{(d,n)}\right)=1$.
לפי תרגיל 1.11 נקבל $\dfrac{n}{(d,n)}\Big|t$, כמו שרצינו. $\square$

תרגיל 7.20. 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 $\varphi(n)$.

8 תת־חבורה הנוצרת על ידי איברים

הגדרה 8.1. 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 8.2. ניקח $\{2,3\} \subseteq \mathbb{Z}$ ואת $H = \langle 2,3 \rangle$.
נוכיח $H = \mathbb{Z}$ בעזרת הכלה דו־כיוונית. 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 $\langle 1 \rangle \subseteq H$, כלומר $\mathbb{Z} \subseteq H$. נסיק $H = \mathbb{Z}$.

דוגמה 8.3. 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 8.4. 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: $\langle a,b \rangle = \{a^i b^j \mid i,j \in \mathbb{Z}\}$.
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:

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

דוגמה 8.5. 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 $A^{-1} = \{a^{-1} \mid a \in A\}$. מילה היא סדרה סופית של אותיות מן האלפבית, והמילה הריקה מייצגת את איבר היחידה ב-G. (אם יש זמן: להציג את F_n.)

הגדרה 8.6. חבורה G תקרא נוצרת סופית, אם קיימת לה קבוצת יוצרים סופית. כלומר קיימים מספר סופי של איברים $a_1, \ldots, a_n \in G$ כך ש-$G = \langle a_1, \ldots, a_n \rangle$.

מסקנה 8.7. כל חבורה סופית נוצרת סופית.

דוגמה 8.8. כל חבורה ציקלית נוצרת סופית (מהגדרה). לכן יש חבורות אינסופיות כמו $\mathbb{Z}$ שנוצרות סופית. האם יש עוד חבורות כאלו? כן, למשל $\mathbb{Z} \times \mathbb{Z} = \langle (1,0), (0,1) \rangle$. (אם יש זמן: גם F_2 נוצרת סופית על ידי שני איברים, אבל היא לא אבלית.)

8.1 חבורת שורשי היחידה

דוגמה 8.9. 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 8.10. נגדיר את קבוצת שורשי היחידה $\Omega_\infty = \bigcup_{n=1}^{\infty} \Omega_n$. הוכיחו:

א. Ω_∞ היא חבורה לגבי כפל. (איחוד חבורות הוא לא בהכרח חבורה!)

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

ג. Ω_∞ אינה ציקלית.

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

פתרון.

א. נוכיח שהיא חבורה על ידי זה שנוכיח שהיא תת־חבורה של $\mathbb{C}^*$. ראינו בתרגיל 7.15 שתת־חבורת הפיתול של חבורה אבלית היא תת־חבורה. לפי הגדרת Ω_∞, רואים שהיא מכילה בדיוק את כל האיברים מסדר סופי של החבורה האבלית $\mathbb{C}^*$, ולכן חבורה.
באופן מפורש ולפי הגדרה: ברור כי $1 \in \Omega_\infty$, ולכן היא לא ריקה. יהיו $g_1, g_2 \in \Omega_\infty$. לכן קיימים m, n שעבורם $g_1 \in \Omega_m$, $g_2 \in \Omega_n$. נכתוב עבור $l, k \in \mathbb{Z}$ מתאימים:

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

לכן

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

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.)

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

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

תרגיל 8.11. הוכיחו שהחבורות הבאות לא נוצרות סופית

א. חבורת שורשי היחידה Ω_∞.

ב. $(M_3(\mathbb{R}), +)$

ג. $(\mathbb{Q}^*, \cdot)$

פתרון.

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

$$\langle a_1,\ldots,a_k\rangle=\left\{a_1^{i_1}\ldots a_k^{i_k}\,\middle|\,0\le i_j\le n_j, 1\le j\le k\right\}$$

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

ב. 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.

ג. נניח בשלילה כי

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

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.

9 החבורה הסימטרית (על קצה המזלג)

הגדרה 9.1. החבורה הסימטרית מדרגה n היא

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

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 עם הפעולה של הרכבת פונקציות. איבר היחידה הוא פונקציית הזהות. כל איבר של S_n נקרא תמורה.

הערה 9.2 (אם יש זמן). החבורה S_n היא בדיוק חבורת ההפיכים במונואיד X^X עם פעולת ההרכבה, כאשר $X=\{1,2,\ldots,n\}$.

דוגמה 9.3. 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 כל האיברים ב-S_3:

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

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

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

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

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

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

מסקנה 9.4. 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 9.5. 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 9.6. 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 9.7. 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 9.8. כל תמורה ניתנת לכתיבה באופן יחיד כהרכבת מחזורים זרים, כאשר הכוונה ב"מחזורים זרים" היא מחזורים שאין לאף זוג מהם איבר משותף.

הערה 9.9. שימו לב שמחזורים זרים מתחלפים זה עם זה (מדוע?), ולכן חישובים עם מחזורים יהיו לעיתים קלים יותר מאשר חישובים עם התמורה עצמה.

דוגמה 9.10. 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

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

9.1 סדר של איברים בחבורה הסימטרית

תרגיל 9.11. יהי $\sigma \in S_n$ מחזור מאורך k. מצאו את $o\left(\sigma\right)$.

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

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

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

טענה 9.12 (תזכורת). תהי G חבורה. יהיו $a, b \in G$ כך ש-$ab = ba$ וגם $\langle a\rangle \cap \langle b\rangle = e$, אז $o\left(ab\right) = [o(a), o(b)]$.

מסקנה 9.13. סדר מכפלות מחזורים זרים ב-S_n הוא הכמ"מ (*lcm*) של אורכי המחזורים.

דוגמה 9.14. הסדר של $(56)\,(193)$ הוא 6 והסדר של $(56)\,(1234)$ הוא 4.

תרגיל 9.15. מצאו תת־חבורה מסדר 45 ב-S_{15}.

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

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

ונשים לב כי $o\left(\sigma\right) = [9, 5] = 45$.
כעת, מכיוון שסדר האיבר שווה לסדר תת־החבורה שאיבר זה יוצר, נסיק שתת־החבורה $\langle\sigma\rangle$ עונה על הדרוש.

שאלה 9.16. האם קיים איבר מסדר 39 ב-S_{15}?

פתרון. לא. זאת 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}.

9.2 הצגת מחזור כמכפלת חילופים

הגדרה 9.17. מחזור מסדר 2 ב-S_n נקרא חילוף.

טענה 9.18. כל מחזור $(a_1,a_2,\ldots,a_r)$ ניתן לרשום כמכפלת חילופים

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

לכן:

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

הסיקו ש-S_n גם נוצרת על ידי $\{(1,j)\,|\,j\in\{2,\ldots,n\}\}$. האם אפשר על ידי פחות איברים?

תרגיל 9.19. 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

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

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

תרגיל 9.20. מה הם הסדרים האפשריים לאיברי S_4?

פתרון. ב-S_4 הסדרים האפשריים הם:

א. סדר 1 - רק איבר היחידה.

ב. סדר 2 - חילופים (i,j) או מכפלה של שני חילופים זרים, למשל $(12)\,(34)$.

ג. סדר 3 - מחזורים מאורך 3, למשל (243).

ד. סדר 4 - מחזורים מאורך 4, למשל (2431).

וזהו! כלומר הצלחנו למיין בצורה פשוטה ונוחה את כל הסדרים האפשריים ב-S_4.

תרגיל 9.21. מה הם הסדרים האפשריים לאיברי S_5?

פתרון. ב-S_5 הסדרים האפשריים הם:

א. סדר 1 - רק איבר היחידה.

ב. סדר 2 - חילופים (i,j) או מכפלה של שני חילופים זרים.

ג. סדר 3 - מחזורים מאורך 3.

ד. סדר 4 - מחזורים מאורך 4.

ה. סדר 5 - מחזורים מאורך 5.

ו. סדר 6 - מכפלה של חילוף ומחזור מאורך 3, למשל $(54)\,(231)$.

וזהו! שימו לב שב-S_n יש איברים מסדר שגדול מ-n עבור $n \geq 5$.

10 מחלקות שמאליות וימניות

הגדרה 10.1. תהי G חבורה, ותהי $H \leq G$. לכל $a \in G$ נגדיר מחלקות (cosets):

א. המחלקה השמאלית של a ביחס ל-H היא הקבוצה $aH = \{ah \,|\, h \in H\}$.

ב. 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 את האוסף זה? בעתיד נראה שכאשר H תת־חבורה "מספיק טובה" (נקראת נורמלית), אז אוסף המחלקות יחד עם פעולה שמושרית מ-G יוצרים חבורה.)

הערה 10.2. עבור איבר היחידה $e \in G$ תמיד מתקיים $eH = H = He$.

אם החבורה G היא אבלית, אז המחלקה השמאלית של a ביחס ל-H שווה למחלקה הימנית:

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

תרגיל 10.3. תנו דוגמה לחבורה G, תת־חבורה H ואיבר $a \in G$ כך ש-$aH \neq Ha$.

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

$$(1\ 3)\, H = \{(1\ 3) \cdot \mathrm{id} = (1\ 3)\,, (1\ 3)\,(1\ 2) = (1\ 2\ 3)\}$$
$$H\,(1\ 3) = \{\mathrm{id} \cdot (1\ 3) = (1\ 3)\,, (1\ 2)\,(1\ 3) = (1\ 3\ 2)\}$$

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 $H = \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \mid n \in \mathbb{Z}\}$ תת־חבורה של G. נבחר $g = \left(\begin{smallmatrix} 5 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, ונחשב

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

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

דוגמה 10.4. 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-$\mathbb{Z}$, וכך

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

הערה 10.5. כפי שניתן לראות מהדוגמאות לעיל, המחלקות השמאליות (או הימניות) של תת־חבורה $H \leq G$ יוצרות חלוקה של G. למעשה הן מחלקות השקילות של יחס השקילות הבא על G:

$$a \sim_H b \iff aH = bH$$

כלומר $a \sim_H b$ אם ורק אם קיים $h \in H$ כך ש-$a = bh$, וזה נכון אם ורק אם $b^{-1}a \in H$. נסכם זאת במשפט הבא.

משפט 10.6 (בהרצאה)**.** תהי G חבורה, תהי $H \le G$ תת־חבורה ויהיו $a, b \in G$. אז

א. $aH = bH$ אם ורק אם $b^{-1}a \in H$. בפרט $aH = H$ אם ורק אם $a \in H$.

ב. לכל זוג מחלקות aH ו-bH, או ש-$aH = bH$ או שהן זרות $aH \cap bH = \varnothing$.

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

הגדרה 10.7. מספר המחלקות (השמאליות) של H ב-G נקרא האינדקס (השמאלי) של H ב-G ומסומן $[G : H]$. כלומר $[G : H] = |G/H|$.

הערה 10.8. האינדקס $[G : H]$ הוא מדד לגודל תת־החבורה. ככל שהאינדקס קטן יותר, כך תת־החבורה H גדולה יותר. בפרט, $[G : H] = 1$ אם ורק אם $H = G$.

דוגמה 10.9. על פי הדוגמאות שראינו:

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

ב. $[\mathbb{Z} : 5\mathbb{Z}] = 5$

ג. $[G : \{e\}] = |G|$

הערה 10.10. ישנה התאמה חח"ע ועל בין מחלקות שמאליות של $H \le G$ ובין מחלקות ימניות לפי $gH \mapsto Hg^{-1}$. ניתן להבין התאמה זאת מכך שכל חבורה סגורה להופכי: $H^{-1} = H$. נחשב

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

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

פתרון. נביא שתי דוגמאות:

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

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

ולכן $[G : H] = \aleph_0$.

ב. נבחר $G = \mathbb{R}$ ואת $H = \mathbb{Q}$, ואז מתקיים $[G : H] = \aleph$, כי העוצמה של aH היא $\aleph_0$, ואיחוד כל המחלקות הוא G שהיא מעוצמה $\aleph$.

11 משפט לגראנז' ושימושים

משפט 11.1 (משפט לגראנז'). תהי G חבורה סופית ותהי $H \leq G$. אז $|H| \mid |G|$.

מסקנה 11.2. מכיוון שאנו יודעים כי $o(a) = |\langle a\rangle|$ לכל $a \in G$, נקבל שהסדר של כל איבר מחלק את סדר החבורה.

הערה 11.3. מהוכחת המשפט נקבל $|G| = [G : H] \cdot |H|$. המסקנה הזו נכונה גם לחבורות אינסופיות בחשבון עוצמות, והיא שקולה לאקסיומת הבחירה.

תרגיל 11.4. תהא G חבורה מסדר 8. הוכיחו:

א. אם G היא ציקלית, אז קיימת תת־חבורה של G מסדר 4 (למה ברור כי תת־החבורה ציקלית?).

ב. אם G לא אבלית, אז עדין קיימת תת־חבורה ציקלית של G מסדר 4 (כאן הציקליות של תת־החבורה לא ברורה מיידית).

ג. 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.

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

ב. 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.

ג. 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 11.5 (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 $k \in \{0, 1, 2, \dots, t\}$. 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 11.6. 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.

נסיק מתרגיל זה שבחבורה מסדר זוגי יש מספר אי זוגי של איברים מסדר 2.

מסקנה 11.7. 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 11.8 (משפט אוילר 2)**.** לכל $a \in U_n$ מתקיים $a^{\varphi(n)} \equiv 1 \pmod n$.

דוגמה 11.9. 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 11.10. מצאו את שתי הספרות האחרונות של $8821811^{4039} + 2019$.

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

$$8821811^{4039} + 2019 \equiv 11^{4039} + 19 \pmod{100}$$

אנו יודעים כי $\varphi(100) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 40$, 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

$$8821811^{4039} + 2020 \equiv 11^{-1} + 19 \equiv 10 \pmod{100}$$

ולכן שתי הספרות האחרונות הן 10.

שאלה 11.11. ראינו מסקנה ממשפט לגראנז': בחבורה סופית G מתקיים לכל איבר $g \in G$ כי $o(g) \mid |G|$. האם הכיוון ההפוך נכון?
כלומר, אם G חבורה סופית והמספר $m \in \mathbb{N}$ מחלק את $|G|$, האם בהכרח קיים ב-G איבר מסדר m?

פתרון. לא בהכרח! דוגמה נגדית: נבחן את החבורה $\mathbb{Z}_4 \times \mathbb{Z}_4$.
סדר החבורה הינו 16 אבל אין בה איבר מסדר 8 או 16. ראינו כבר שהסדר המרבי בחבורה הזאת הוא לכל היותר 4. בנוסף, אילו היה קיים איבר מסדר 16, אזי היא ציקלית, אבל הוכחנו שהחבורה $\mathbb{Z}_n \times \mathbb{Z}_n$ אינה ציקלית עבור $n > 1$.

הערה 11.12. נעיר שבחבורה **ציקלית** $G = \langle a \rangle$ מסדר $n \in \mathbb{N}$ זה כן מתקיים בעזרת נוסחת הקסם שראינו $o(a^t) = \frac{n}{(n,t)}$.

12 פעולה של חבורה על קבוצה

ההבדל הבסיסי בין קבוצה לחבורה היא קיומה של פעולה על קבוצה. אנחנו מכירים מקרים בהם ניתן להפעיל פעולה על (g,x) (כאשר g איבר בחבורה ו-x איבר בקבוצה) ולקבל איבר אחר בקבוצה. למשל, אם $G = \mathbb{F}$ שדה ו-$X = V$ מרחב וקטורי מעל השדה, אז למרות שלא ניתן להכפיל את איברי V זה בזה, נוכל להכפיל איבר ב-$\mathbb{F}$ באיבר של V ולקבל איבר של V. זהו הכפל בסקלר בשדה.

הגדרה 12.1. פעולה של חבורה G על קבוצה X היא פעולה בינארית $G \times X \to X$ שנסמנה לפי $(g,x) \mapsto g * x$, המקיימת:

א. $(gh) * x = g * (h * x)$ לכל $g,h \in G$ ו-$x \in X$.

ב. $e * x = x$ לכל $x \in X$.

הגדרה 12.2 (הגדרה שקולה). פעולה של חבורה G על קבוצה X היא הומומורפיזם $\varphi\colon G \to S_X$. כלומר לכל g נתאים פונקציה חח"ע ועל $\varphi(g)\colon X \to X$ ומתקיים $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$.

דוגמה 12.3. כנראה ראיתם כבר בהרצאה.

א. פעולת הכפל משמאל של חבורה על עצמה (זו הפעולה שנראה בהוכחת משפט קיילי). מתי כפל מימין הוא לא פעולה?

ב. פעולת ההצמדה של חבורה על עצמה. זו "דוגמה קלאסית" וחשובה שנתעסק בה.

ג. הפעולה של S_n על $F[x_1,\dots,x_n]$ בתמורה על האינדקסים של המשתנים.

ד. הפעולה של $GL_n(F)$ על F^n.

הגדרה 12.4. פעולה של חבורה על קבוצה נקראת נאמנה אם האיבר היחידי שפועל טריוויאלית הוא איבר היחידה.
באופן שקול, פעולה היא נאמנה אם לכל $g \neq h \in G$ קיים $x \in X$ כך ש-$g * x \neq h * x$. בהצגה כהומומורפיזם $\varphi\colon G \to S_X$, למעשה דורשים חח"ע.

דוגמה 12.5. מהדוגמאות הקודמות:

א. נאמנה תמיד.

ב. תלוי... אם יש איבר $e \neq x \in Z(G)$, אז הוא פועל טריוויאלית.

ג. נאמנה.

ד. נאמנה.

הגדרה 12.6. בהנתן פעולה של G על X, המסלול של איבר $x \in X$ היא תת־הקבוצה

$$\mathrm{orb}(x) = G * x = \{g * x \mid g \in G\}$$

דוגמה 12.7. עבור פעולת הכפל משמאל $\mathrm{orb}(x) = Gx = G$.

דוגמה 12.8. עבור הפעולה של S_4 על פולינומים, נחשב את המסלול של הפולינום $f = x_1x_2 + x_3x_4$:

$$\mathrm{orb}(f) = \{f, x_1x_3 + x_2x_4, x_1x_4 + x_2x_3\}$$

דוגמה 12.9. עבור פעולת ההצמדה, $\mathrm{orb}(g) = \mathrm{conj}(g)$ נקראת *מחלקת צמידות* של g.
בחבורה אבלית G, אין שני איברים שונים הצמודים זה לזה. הרי אם g ו-h צמודים בחבורה אבלית, אז קיים $a \in G$ שעבורו

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

באופן כללי בחבורה כלשהי G, מתקיים $g \in Z\left(G\right)$ אם ורק אם $\mathrm{conj}(g) = \{g\}$.

תרגיל 12.10. תהי G חבורה, ויהי $g \in G$ מסדר סופי n. הוכיחו:

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

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

פתרון.

א. g ו-h צמודים, ולכן קיים $a \in G$ שעבורו $h = aga^{-1}$. לפי תרגיל מהשיעורי בית

$$o(h) = o(aga^{-1}) = o(a^{-1}ag) = o(g)$$

ב. יהי $h \in G$. לפי הסעיף הראשון, $o\left(hgh^{-1}\right) = n$. 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 $g \in Z\left(G\right)$.

הערה 12.11. הכיוון ההפוך בכל סעיף אינו נכון - למשל, בחבורה $\mathbb{Z}_4$ מתקיים $o\left(1\right) = o\left(3\right) = 4$, אבל הם לא צמודים. כמו כן, שניהם במרכז, ולכל אחד מהם יש איבר אחר מאותו סדר.

דוגמה 12.12. בחבורה S_3, האיבר $\sigma = \left(1\ 2\ 3\right)$ צמוד לאיבר

$$\left(1\ 2\right)\left(1\ 2\ 3\right)\left(1\ 2\right)^{-1} = \left(2\ 3\right)\left(1\ 2\right) = \left(1\ 3\ 2\right) = \sigma^2$$

אין עוד איברים צמודים להם, כי אלו כל האיברים מסדר 3 ב-S_3.

טענה 12.13 (לבית). תהי $\sigma \in S_n$, ויהי מחזור $\left(a_1, a_2, \ldots, a_k\right) \in S_n$. הוכיחו כי

$$\sigma\left(a_1, a_2, \ldots, a_k\right)\sigma^{-1} = \left(\sigma\left(a_1\right), \sigma\left(a_2\right), \ldots, \sigma\left(a_k\right)\right)$$

תרגיל 12.14. בחבורה S_6 נתונות התמורות $\mu = \left(1, 5, 3, 6\right)$, $\sigma = \left(1, 3\right)\left(4, 5, 6\right)$ ו-$\tau = \left(1, 4, 5\right)$. חשבו את $\sigma\mu\sigma^{-1}$ ואת $\tau\sigma\tau^{-1}$.

פתרון. לפי הנוסחה מהטענה הקודמת,

$$\begin{aligned}\sigma\mu\sigma^{-1} &= (3, 6, 1, 4)\\ \tau\sigma\tau^{-1} &= \left(\tau(13)\tau^{-1}\right)\left(\tau(456)\tau^{-1}\right) = (43)(516)\end{aligned}$$

הגדרה 12.15. תהי $\sigma \in S_n$ תמורה ונציג אותה כמכפלה של מחזורים זרים $\sigma = \sigma_1\sigma_2\ldots\sigma_k$. נניח כי האורך של σ_i הוא r_i, וכי $r_1 \geq r_2 \geq \cdots \geq r_k$. נגדיר את מבנה המחזורים של σ להיות ה-k-יה הסדורה $\left(r_1, r_2, \ldots, r_k\right)$.

דוגמה 12.16. מבנה המחזורים של $\left(1, 2, 3\right)\left(5, 6\right)$ הוא $\left(3, 2\right)$; מבנה המחזורים של $\left(4, 2, 3\right)\left(1, 5\right)$ גם הוא $\left(3, 2\right)$; מבנה המחזורים של $\left(1, 2, 3, 4\right)\left(5, 6\right)\left(7, 8\right)$ הוא $\left(4, 2, 2\right)$.

טענה 12.17. שתי תמורות ב-S_n הן צמודות אם ורק אם יש להן אותו מבנה מחזורים.

דוגמה 12.18. התמורה $\left(1, 2, 3\right)\left(5, 6\right)$ צמודה ל-$\left(4, 2, 3\right)\left(1, 5\right)$ ב-S_8, אבל הן לא צמודות לתמורה $\left(1, 2, 3, 4\right)\left(5, 6\right)\left(7, 8\right)$.

הגדרה 12.19. חלוקה של n היא סדרה לא עולה של מספרים טבעיים $n_1 \geq \cdots \geq n_k > 0$ כך ש-$n = n_1 + \cdots + n_k$. נסמן ב-$p(n)$ את מספר החלוקות של n.

מסקנה 12.20. מספר מחלקות הצמידות ב-S_n הוא $p(n)$.

דוגמה 12.21. נחשב כמה מחלקות צמידות יש ב-S_5. נמצא את החלוקות של 5:

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

ולכן $p(5) = 7$. בעזרת המסקנה האחרונה נסיק שישנן 7 מחלקות צמידות ב-S_5.

13 משוואת המחלקות

טענה 13.1 (משוואת המחלקות). כל פעולה מגדירה יחס שקילות: $x \sim y$ אם קיים $g \in G$ כך ש-$g * x = y$. מחלקות השקילות הן בדיוק המסלולים של הפעולה. בפרט,

$$\begin{aligned}
X &= \bigcup \mathrm{orb}(x)\\
|X| &= |\mathrm{Fix}(X)| + \sum |\mathrm{orb}(x_i)|
\end{aligned}$$

כאשר $\mathrm{Fix}(X)$ הוא אוסף נקודות השבת (Fixed points). שימו לב שהסכימה היא על נציגים של המסלולים.

הערה 13.2. עבור פעולת ההצמדה של S_4 על עצמה נקבל:

$$S_4 = \mathrm{orb}\left(\mathrm{id}\right) \cup \mathrm{orb}\left((**)\right) \cup \mathrm{orb}\left((***)\right) \cup \mathrm{orb}\left((****)\right) \cup \mathrm{orb}\left((**)(**)\right)$$

טענה 13.3. ניסוח של הטענה הקודמת עבור פעולת ההצמדה:

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G),\, \mathrm{rep.}} |\mathrm{conj}(x_i)|$$

הגדרה 13.4. יהי $x \in X$. המייצב של x הוא תת־החבורה

$$\mathrm{stab}(x) = \{g \in G \mid g * x = x\}$$

ודאו שברור למה זו תת־חבורה. סימון מקובל אחר הוא G_x.

דוגמה 13.5.

א. עבור פעולת ההצמדה, $\mathrm{stab}(x) = C_G(x)$ הוא המְרַכֵּז של x.

ב. עבור פעולת הכפל משמאל, $\mathrm{stab}(x) = \{e\}$.

ג. עבור הפעולה של S_4 על $F[x_1, x_2, x_3, x_4]$,

$$\mathrm{stab}(x_1 + x_2) = \{\mathrm{id}, (12), (34), (12)(34)\}$$

משפט 13.6. לכל $x \in X$ מתקיים $|\mathrm{orb}(x)| = [G : \mathrm{stab}(x)]$. אם G סופית, אז

$$|\mathrm{orb}(x)| = \frac{|G|}{|\mathrm{stab}(x)|}$$

כמסקנה, $|\mathrm{orb}(x)|$ מחלק את הסדר של G (אפילו שהוא לא בהכרח מוכל שם!). בפרט, $|\mathrm{conj}(x)|$ מחלק את הסדר של G (אפילו שהיא לא תת־חבורה).

דוגמה 13.7. נתבונן בפעולה של S_3 על $F[x_1, x_2, x_3]$. נחשב את המייצב של $f = x_1x_2 + x_1x_3$.

מפני ש-$f = x_1(x_2+x_3)$ קל לראות ש-$\mathrm{id}, (23)$ מייצבים את f. לכן $|\mathrm{stab}(f)| \geq 2$. קל לחשב את המסלול

$$\mathrm{orb}(f) = \{f, x_2(x_1 + x_3), x_3(x_1 + x_2)\}$$

כלומר יש בו שלושה איברים. לכן $|\mathrm{stab}(f)| = \dfrac{|S_3|}{|\mathrm{orb}(x)|} = \dfrac{6}{3} = 2$, ולכן $\mathrm{stab}(f) = \{\mathrm{id}, (23)\}$.

תרגיל 13.8. כמה איברים ב-S_n מתחלפים עם $(12)(34)$?

פתרון. זה שקול לשאול כמה איברים $\sigma \in S_n$ מקיימים $\sigma(12)(34)\sigma^{-1} = (12)(34)$. או במילים אחרות: כמה איברים יש במייצב של $(12)(34)$ ביחס לפעולת ההצמדה.

לפי המשפט, נבדוק את הגודל של המסלול. כידוע, האיברים הצמודים ל-$(12)(34)$ הם כל התמורות מאותו מבנה מחזורים.

דהיינו, כל המכפלות של 2 חילופים זרים: $\frac{1}{2}\binom{n}{2}\binom{n-2}{2}$.

לכן הגודל של המייצב הוא

$$\frac{n!}{\frac{1}{2}\binom{n}{2}\binom{n-2}{2}} = 8(n-4)!$$

תרגיל 13.9. נתון שהחבורה

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a, b, c \in \mathbb{Z}_3 \right\}$$

פועלת על קבוצה X מגודל 218. הוכיחו שיש לפעולה נקודת שבת. כלומר שקיים $x \in X$ כך ש-$\mathrm{orb}(x) = \{x\}$.

פתרון. נשים לב ש-$|G| = 3^3 = 27$.

נקח נציגים של המסלולים $x_1, \ldots, x_k$, אזי $X = \operatorname{orb}(x_1) \cup \cdots \cup \operatorname{orb}(x_k)$.

מהמשפט נקבל ש-$|\operatorname{orb}(x_i)|$ מחלק את 27. לכן הגודל של המסלולים השונים יכול להיות רק מ-$\{1, 3, 9, 27\}$.

נניח בשלילה שלא קיים איבר $x \in X$ כך ש-$|\operatorname{orb}(x)| = 1$. אזי גדלי המסלולים האפשריים הם $\{3, 9, 27\}$. אז

$$|X| = 218 = (3+\cdots+3)+(9+\cdots+9)+(27+\cdots+27) = 3\alpha+9\beta+27\gamma = 3(\alpha+3\beta+9\gamma)$$

קיבלנו ש$3|218$ וזו סתירה!

הגדרה 13.10. יהי p ראשוני. חבורה G תקרא חבורת-p, אם הסדר של כל איבר בה הוא חזקה של p.

תרגיל 13.11. הראו שאם G סופית, אז G חבורת-p אם ורק אם $|G| = p^n$ עבור איזשהו $n \in \mathbb{N}$.

תרגיל 13.12. נסו להכליל את מה שעשינו בתרגיל קודם: אם G חבורת-p סופית הפועלת על קבוצה X כך ש-$p \nmid |X|$, אז קיימת ב-X נקודת שבת.

תרגיל 13.13. הוכיחו שהמרכז של חבורת-p אינו טריוויאלי.

פתרון (רק אם לא נעשה בהרצאה). 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 (כי $r_i \neq n$) ולכן באגף שמאל p מחלק את הסדר של $Z(G)$. מכאן נובע ש-$Z(G)$ לא יכול להיות טריוויאלי.

13.1 טרנזיטיביות והלמה של ברנסייד

הגדרה 13.14. אומרים שהפעולה של G על X היא טרנזיטיבית אם לכל שני איברים $x_1, x_2 \in X$ קיים $g \in G$ כך ש-$g * x_1 = x_2$.

זה בעצם אומר ש-$\operatorname{orb}(x) = X$ (ודאו למה זה שקול!).

דוגמה 13.15.

א. הצמדה היא בדרך כלל לא טרנזיטיבית (בגלל היחידה, גם להראות ב-S_n).

ב. הפעולה של S_n על $\{1, 2, \ldots, n\}$ היא טרנזיטיבית.

ג. (לדלג) הפעולה של S_4 על תת־החבורה הנורמלית

$$V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$$

היא לא טרנזיטיבית.

ד. הפעולה של S_n על $F[x_1,\dots,x_n]$ היא לא טרנזיטיבית.
הפעולה הנ"ל על תת־הקבוצה $\{x_1,x_2,\dots,x_n\}$ היא טרנזיטיבית.

ה. תהי Y קבוצת בת לפחות 2 איברים. S_n פועלת על Y^n על ידי תמורה על האינדקסים. זו פעולה לא טרנזיטיבית כי למשל $(1,2,\dots) \nrightarrow (1,1,\dots,1)$.

טענה **13.16.** אם חבורה סופית G פועלת טרנזיטיבית על קבוצה סופית X, אז $|X|$ מחלק את $|G|$. הרי לפי המשפט $|G| \mid |\mathrm{orb}(x)| = |X|$.

הגדרה 13.17. יהי $g \in G$. נסמן $X^g = \{x \in X \mid g * x = x\}$ עבור קבוצת נקודות השבת של g.

למה 13.18 (הלמה שאינה של ברנסייד). תהי G חבורה הפועלת על קבוצה X. נסמן ב-k את מספר המסלולים. אז מתקיים (גם בחשבון עוצמות)

$$k\,|G| = \sum_{g\in G} |X^g|$$

בחבורה סופית אפשר לפרש זאת שמספר המסלולים הוא ממוצע גודל קבוצות השבת:

$$k = \frac{1}{|G|}\sum_{g\in G} |X^g|$$

תרגיל 13.19. תהי G חבורה סופית (לא טריוויאלית) הפועלת טרנזיטיבית על קבוצה X (מגודל לפחות 2). הוכיחו כי קיים $g \in G$ כך ש-$X^g = \varnothing$.

פתרון. כיוון שהפעולה טרנזיטיבית, אז $\mathrm{orb}(x) = X$ לכל $x \in X$. יש בעצם רק מסלול אחד (דהיינו $k = 1$). לפי הלמה של ברנסייד $\frac{1}{|G|}\sum_{g\in G}|X^g| = 1$. כלומר $|G| = \sum_{g\in G}|X^g|$.
מפני ש-$|X^e| = |X| > 1$, אז בהכרח אחת מהקבוצות X^g האחרות חייבת להיות מגודל אפס.

תרגיל 13.20. רוצים לקשט את הרחוב בדגלים. כל דגל הוא מלבן המחולק ל-6 פסים אותם אפשר לצבוע בצבעים שונים מתוך 4 צבעים.
אנחנו נחשיב שני דגלים (צבועים) להיות זהים אם הם צבועים בדיוק אותו דבר או במהופך (כך שאם הופכים את אחד הדגלים זה נראה בדיוק אותו דבר). כמה דגלים שונים אפשר ליצור?

פתרון. נתחיל מלחשוב על כל הדגלים בתור איברים של $X = (\mathbb{Z}_4)^6$ (כאשר המספרים $0,1,2,3$ מייצגים את שמות הצבעים).
שימו לב שכרגע ב-X יש איברים שונים שמייצגים את אותו דגל, כמו $(0,1,1,2,2,3) \sim (3,2,2,1,1,0)$.

S_6 פועלת על X לפי תמורה על הקואורדינטות. נסתכל ספציפית על התמורה $\sigma = (16)(25)(34)$ ועל הפעולה של $\langle \sigma \rangle$ על X. נשים לב ששני איברים של X מייצגים את אותו דגל אם ורק אם הם באותו מסלול.

לכן השאלה כמה דגלים שונים יש שקולה לשאלה כמה מסלולים שונים יש בפעולה של החבורה $\langle \sigma \rangle$ על X. כדי להשתמש בלמה של ברנסייד, צריך לחשב את $\left| X^{\mathrm{id}} \right|$ ו-$|X^{\sigma}|$. ברור ש-$\left| X^{\mathrm{id}} \right| = |X| = 4^6$.

עבור σ, האיברים ב-X^{σ} הם בעצם נקודות השבת (הוקטורים שלא מושפעים). אלו הם האיברים שמספיק לבחור עבורם את הצביעה של 3 הקואורדינטות הראשונות, ולכן $|X^{\sigma}| = 4^3$. לפי הלמה של ברנסייד יש $k = \frac{1}{2}\left(4^3 + 4^6\right) = 2080$ דגלים שונים.

14 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 14.1. 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 14.2. 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 14.3. 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).

14.1 החבורה הדיהדרלית

הגדרה 14.4. עבור מספר טבעי n, הקבוצה D_n של סיבובים ושיקופים המעתיקים מצולע משוכלל בן n צלעות על עצמו, יחד עם הרכבת פונקציות נקראת החבורה הדיהדרלית מדרגה n. הפעולה של D_n על קודקודי המצולע המשוכלל היא נאמנה וטרנזיטיבית.

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

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 14.5 (אם יש זמן). פונקציה $\alpha\colon \mathbb{R}^2 \to \mathbb{R}^2$ 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 14.6. 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

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

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

סיכום 14.7. איברי D_n הם

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

בפרט נקבל כי $|D_n| = 2n$ ושעבור $n > 2$ החבורה אינה אבלית כי $\sigma\tau \neq \tau\sigma$. (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.)

15 הומומורפיזמים

הגדרה 15.1. תהינה $(G, *)$, $(H, \bullet)$ חבורות. העתקה $f\colon G \to H$ 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:

א. הומומורפיזם שהוא חח"ע נקרא מונומורפיזם או שיכון. נאמר כי G משוכנת ב-H אם קיים שיכון $f\colon G \hookrightarrow H$.

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

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

ד. איזומורפיזם $f\colon G \to G$ נקרא אוטומורפיזם של G.

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

הערה 15.2. הומומורפיזם $f\colon G \to H$ הוא איזומורפיזם אם ורק אם קיימת העתקה $g\colon H \to G$ 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 שאיזומורפיות היא תכונה רפלקסיבית, סימטרית וטרנזיטיבית (היא לא יחס שקילות כי מחלקת החבורות היא גדולה מכדי להיות קבוצה).

תרגיל 15.3. הנה רשימה של כמה העתקות בין חבורות. קבעו האם הן הומומורפיזמים, ואם כן מהו סוגן:

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

ב. יהי F שדה. אז $\det\colon GL_n(F) \to F^*$ היא אפימורפיזם. הרי

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

וכדי להוכיח שההעתקה על, לכל $\alpha \in F^*$ נסתכל על מטריצה אלכסונית עם ערכים $(\alpha, 1, \ldots, 1)$ באלכסון.

ג. $\varphi\colon \mathbb{R} \to \mathbb{R}^*$ המוגדרת לפי $x \mapsto x$ אינה הומומורפיזם כלל.

ד. $\varphi\colon \mathbb{Z}_2 \to U_3$ המוגדרת לפי $0 \mapsto 1$, $1 \mapsto 2$ היא איזומורפיזם. הראתם בתרגיל בית שכל החבורות מסדר 2 הן למעשה איזומורפיות.

העובדה שהעתקה $f\colon G \to H$ היא הומומורפיזם גוררת אחריה כמה תכונות מאוד נוחות:

א. $f(e_G) = e_H$.

ב. $f(g^{-1}) = f(g)^{-1}$.

ג. $f(g^n) = f(g)^n$ לכל $n \in \mathbb{Z}$. הסעיפים הקודמים הם מקרה פרטי.

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

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

ו. אם $G \cong H$, אז $|G| = |H|$.

תרגיל 15.4. יהי $f\colon G \to H$ 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 $o(f(g))|n$. □

תרגיל 15.5. 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 $f\colon G \to H$, 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 15.6 (לבית). יהי $f\colon G \to H$ הומומורפיזם. הוכיחו שאם G אבלית, אז $\operatorname{im} f$ אבלית. הסיקו שאם $G \cong H$, אז G אבלית אם ורק אם H אבלית.

תרגיל 15.7. יהי $f\colon G \to H$ 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-$f(g) = x$ (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 $f(a)$. □

מהתרגיל הקודם ניתן להסיק שכל החבורות הציקליות מסדר מסוים הן איזומורפיות. אם מצאנו ב"רחוב" חבורה ציקלית, אז הסדר שלה הוא כל המידע שצריך לדעת עליה, עד כדי איזומורפיזם:

משפט 15.8. כל חבורה ציקלית איזומורפית או ל-$\mathbb{Z}_n$ או ל-$\mathbb{Z}$.

דוגמה 15.9. $n\mathbb{Z}\cong\mathbb{Z}$ ו-$U_{10}\cong\Omega_4\cong\mathbb{Z}_4$.

תרגיל 15.10. האם קיים איזומורפיזם $f\colon S_3\to\mathbb{Z}_6$?

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

תרגיל 15.11. האם קיים איזומורפיזם $f\colon(\mathbb{Q}^+,\cdot)\to(\mathbb{Q},+)$?

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 15.12. האם קיים אפימורפיזם $f\colon H\to\mathbb{Z}_3\times\mathbb{Z}_3$ 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 15.13. האם קיים מונומורפיזם $f\colon GL_2(\mathbb{Q})\to\mathbb{Q}^{16}$?

פתרון. לא. נניח בשלילה שקיים f כזה. נתבונן בצמצום $\overline{f}\colon GL_2(\mathbb{Q})\to\operatorname{im} f$, שהוא איזומורפיזם (להדגיש כי $\overline{f}$ אפימורפיזם ומפני ש-f חח"ע, אז $\overline{f}$ הוא איזומורפיזם). ידוע לנו כי $\operatorname{im} f\leq\mathbb{Q}^{16}$, ולכן $\operatorname{im} f$ אבלית. כלומר גם $GL_2(\mathbb{Q})$ אבלית, שזו סתירה.

מסקנה. יתכנו ארבע הפרכות ברצף.

תרגיל 15.14. מתי ההעתקה $i\colon G\to G$ 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.

16 תת־חבורות נורמליות

הגדרה 16.1. תת־חבורה $H \leq G$ נקראת תת־חבורה נורמלית אם לכל $g \in G$ מתקיים $gH = Hg$. במקרה זה נסמן $H \lhd G$.

משפט 16.2. 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 הסעיפים האחרים, ובכיוון השני יש צורך בהגדרת חבורת מנה. שקילויות נוספות: כל מחלקה שמאלית היא גם מחלקה ימנית, כל מחלקה ימנית היא גם מחלקה שמאלית, כל מחלקה שמאלית מוכלת במחלקה ימנית, כל מחלקה ימנית מוכלת במחלקה שמאלית, ועוד ועוד. □

דוגמה 16.3. אם G חבורה אבלית, אז כל תת־החבורות 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-$gh = hg$! זה אומר ש- $gh = h'g$ (חילופיות עם "מס מעבר").

דוגמה 16.4. 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 $\det\colon GL_n(F) \to F^*$.

דוגמה 16.5. $H = \langle (1\ 2) \rangle \leq S_3$ אינה תת־חבורה נורמלית, כי כבר ראינו $(1\ 3)\,H \neq H\,(1\ 3)$.

דוגמה 16.6. עבור $n \geq 3$, תת־החבורה $\langle \tau \rangle \leq D_n$ אינה נורמלית כי $\sigma \langle \tau \rangle \neq \langle \tau \rangle \sigma$.

טענה 16.7. תהי $H \leq G$ 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 $aH = Ha$ לכל $a \in G$. $\square$

מסקנה 16.8. מתקיים $\langle\sigma\rangle \lhd D_n$ כי לפי משפט לגראנז' $[D_n : \langle\sigma\rangle] = \frac{2n}{n} = 2$.

תרגיל 16.9. תהי G חבורה, ונתון שיש איבר $g \in G$ שבמחלקת הצמידות שלו יש שני איברים בדיוק. הוכיחו כי ל-G יש תת־חבורה נורמלית לא טריוויאלית.

פתרון. לפי משפט 13.6 נקבל $[G : \mathrm{stab}(g)] = 2$, ולכן המייצב של g (לגבי פעולת ההצמדה) הוא תת־החבורה הנורמלית המבוקשת.

הערה 16.10. אם $G \leq H \leq K$ וגם $K \lhd G$, אז בוודאי $K \lhd H$. ההפך לא נכון. אם $H \lhd K$ 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 16.11 (לבית). לכל חבורה מסדר 8 יש תת־חבורה נורמלית לא טריוויאלית (מצאו תת־חבורה מאינדקס 2).

תרגיל 16.12. תהי G חבורה ותהי $H \lhd G$ תת־חבורה נורמלית. הוכיחו כי G פועלת על ידי הצמדה על H, ושהפעולה לא בהכרח נאמנה.

פתרון. ראינו ש-G פועלת על עצמה על ידי הצמדה. נשאר להוכיח סגירות ב-H. לכל $g \in G$ נשים לב שלפי ההגדרה של תת־חבורה נורמלית $ghg^{-1} \in H$ לכל $h \in H$.

להפרכה שהפעולה בהכרח נאמנה, נבחר את $\langle\sigma\rangle \lhd D_{20}$ שבה הצמדה על ידי $\sigma \in \mathrm{id}$ היא טריוויאלית.

תרגיל 16.13. תהי G חבורת-p סופית, ותהי $H \lhd G$ תת־חבורה נורמלית מסדר p. הוכיחו כי $H \subseteq Z(G)$.

פתרון. מכיוון ש-H היא נורמלית, אז היא סגורה להצמדה. לכן לכל $x \in H$ מתקיים $\mathrm{conj}(x) \subseteq H$ ולכן $|\mathrm{conj}(x)| \leq p$. אך מכיוון שלכל $x \neq e$ מתקיים $e \notin \mathrm{conj}(x)$, אז $|\mathrm{conj}(x)| \leq p - 1$.

אבל ראינו שמחלקת הצמידות מחלקת את p^n שהוא סדר החבורה, ולכן בהכרח $|\mathrm{conj}(x)| = 1$ לכל $x \in H$. לכן $x \in Z(G)$, וקיבלנו ש-$H \subseteq Z(G)$.

17 חבורת החילופין

הגדרה 17.1 (שקולה). יהי σ מחזור מאורך k, אזי הסימן שלו מוגדר להיות:

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

עבור תמורות $\tau, \sigma \in S_n$ נרחיב את ההגדרה

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

וזה מאפשר לחשב את הסימן של כל תמורה ב-S_n. שימו לב שלא הראנו שהסימן מוגדר היטב! יש דרכים שקולות אחרות להגדיר סימן של תמורה.

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

דוגמה 17.2. זה חשוב לדעת לחשב סימן של תמורה, אבל זה קצת מבלבל:

א. החילוף (35) הוא תמורה אי זוגית. התמורה $(49)(35)$ היא זוגית.

ב. מחזור מאורך אי זוגי הוא תמורה זוגית, למשל (34158).

ג. תמורת הזהות היא תמורה זוגית.

הגדרה 17.3. חבורת החילופין (חבורת התמורות הזוגיות) A_n היא תת־החבורה הבאה של S_n:

$$A_n = \{\sigma \in S_n \,|\, \operatorname{sign}(\sigma) = 1\}$$

הערה 17.4. הסדר של A_n הינו $|A_n| = \frac{n!}{2}$. הראו זאת בעזרת ההעתקה $f\colon A_n \to S_n \setminus A_n$ המוגדרת לפי $f(\sigma) = (12)\,\sigma$. יש להוכיח כי f מוגדרת היטב והפיכה.

מכאן נסיק ש-$A_n \lhd S_n$ כי $[S_n : A_n] = \frac{n!}{n!/2} = 2$. דרך אחרת להראות ש-$A_n$ נורמלית ב-S_n היא לשים לב ש-$A_n = \ker(\operatorname{sign})$.

דוגמה 17.5. $A_3 = \langle(123)\rangle = \{\mathrm{id}, (123), (132)\}$. כלומר A_3 ציקלית. עבור $n > 3$ החבורה A_n אינה אבלית.

טענה 17.6. ראינו שב-S_n שני איברים הם צמודים אם ורק אם הם מאותו מבנה מחזורים. זה לא נכון עבור A_n! למשל (123) ו-(213) הם מאותו מבנה מחזורים, אבל לא צמודים ב-A_3 שהרי היא אבלית. האם אתם יכולים למצוא איברים מאותו מבנה מחזורים ב-A_4 (שאינה אבלית) שאינם צמודים?

ראיתם בהרצאה כי קבוצת החילופים (ij) עבור $i, j \in \{1, \ldots, n\}$ יוצרים את S_n. כעת נראה כמה קבוצות יוצרים עבור A_n. נתבסס בתרגילים הבאים על רשימות של קית' קונרד.

תרגיל 17.7. לכל $n \geq 3$, הוכיחו שכל תמורה זוגית היא מכפלה של מחזורים מאורך 3. הסיקו שקבוצת המחזורים מאורך 3 יוצרת את A_n.

פתרון. איבר היחידה מקיים $\mathrm{id} = (123)^0 = (123)^3$, ולכן הוא מכפלה של מחזורים מאורך 3. עבור $\mathrm{id} \neq \sigma \in A_n$ נכתוב אותה כמכפלת חילופים (לא בהכרח זרים): $\sigma = \tau_1 \ldots \tau_k$. מפני ש-$\sigma \in A_n$, אז k זוגי. אפשר להניח בלי הגבלת הכלליות ש-τ_i, τ_{i+1} הם שונים. אם $\tau_i = (ab)$ ו-$\tau_{i+1} = (ac)$ כאשר $b \neq c$, אז

$$\tau_i\tau_{i+1} = (ab)\,(ac) = (acb)$$

הוא מחזור מאורך 3. אחרת τ_i, τ_{i+1} הם זרים, נניח $\tau_i = (ab)$ ו-$\tau_{i+1} = (cd)$ עבור a, b, c, d שונים, אז

$$\tau_i \tau_{i+1} = (ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)$$

שזו מכפלה של שני מחזורים מאורך 3. בסך הכל כל $\sigma \in A_n$ היא מכפלה של מחזורים מאורך 3, ולכן זו קבוצת יוצרים.

תרגיל 17.8. לכל $n \geq 3$ הוכיחו שקבוצת המחזורים מהצורה $(1ij)$ יוצרת את A_n.

פתרון. זו טענה דומה לכך שקבוצת החילופים מהצורה $(1i)$ יוצרת את S_n.

אם (abc) הוא מחזור מאורך 3 שאינו כולל את 1, אז $(abc) = (1ab)(1bc)$. בעזרת התרגיל הקודם סיימנו.

תרגיל 17.9. לכל $n \geq 3$ הוכיחו שקבוצת המחזורים מהצורה $(12i)$ יוצרת את A_n.

פתרון. עבור $n = 3$ כבר ראינו ש-$A_3 = \langle (123) \rangle$. נניח $n \geq 4$, ולפי התרגיל הקודם, מספיק לנו להראות שכל מחזור מהצורה $(1ij)$ הוא מכפלה של מחזורים מהצורה $(12i)$.

נשים לב כי $(12i)^{-1} = (1i2)$. כלומר כל מחזור מאורך 3 הכולל את 1 ואת 2 נוצר על ידי מחזורים מהצורה $(12i)$. נניח $(1ij)$ הוא מחזור שכולל את 1, אבל לא את 2. אז

$$(1ij) = (1j2)(12i)(1j2)^{-1} = (12j)(12j)(12i)(12j)$$

וסיימנו. נסו להוכיח שקבוצת המחזורים מהצורה $(i, i+1, i+2)$ יוצרת את A_n. זו טענה המקבילה לכך שקבוצת החילופים מהצורה $(i, i+1)$ יוצרת את S_n (הם מתאימים להיות היוצרים בהצגת קוקסטר של S_n).

18 חבורות מנה

הגדרה 18.1. נוכל להגדיר על G/H מבנה של חבורה לפי $(aH)(bH) = abH$ אם ורק אם H היא תת־חבורה נורמלית. במקרה זה, זוהי חבורת המנה של G ביחס ל-H.

איבר היחידה הוא המחלקה $eH = H$ כי $(aH)H = (Ha)H = aH$. מכאן שאפשר "למצוא" את H בהנתן G/H בעזרת ההטלה הטבעית $\pi\colon G \to G/H$ המוגדרת לפי $\pi(g) = gH$. אז $\ker \pi = H$.

דוגמה 18.2.

א. כבר (כמעט) השתכנענו כי

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, n-1+n\mathbb{Z}\} \cong \mathbb{Z}_n$$

ב. $G/\{e\} \cong G$, $G/G \cong \{e\}$. מי הם האיזומורפיזמים המתאימים?

ג. $\langle\sigma\rangle \lhd D_n$ ראינו שהיא מאינדקס 2 ולכן $\mathbb{Z}_2 \cong {}^{D_n}/_{\langle\sigma\rangle} = \{\langle\sigma\rangle, \langle\sigma\rangle\tau\}$. אכן, $\langle\sigma\rangle\tau\langle\sigma\rangle\tau = \langle\sigma\rangle\tau\tau = \langle\sigma\rangle$.

ד. $H = \mathbb{R}\times\{0\} \lhd \mathbb{R}^2$ 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.

ה. $H = \langle(1,1)\rangle \lhd \mathbb{Z}_4\times\mathbb{Z}_4$ 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 18.3. אם G אבלית ו-$H \le G$ אזי G/H חבורה אבלית. מה לגבי הכיוון ההפוך?

פתרון. קודם כל נעיר שמכיוון ש-G אבלית, אז H בהכרח נורמלית. לכן 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 18.4. אם G ציקלית ו-$H \le G$ אז G/H ציקלית. מה לגבי הכיוון ההפוך?

תרגיל 18.5. 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 $|G/H| = n$. לכן

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

כלומר קיבלנו $a^n \in H$.

תרגיל 18.6. 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 $x^{|N|} = e$ גורר ש-$x\in N$.

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

א. אם $T \leq G$ (למשל אם G אבלית), אז $T \lhd G$.

ב. 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

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

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 $T = \Omega_\infty = \bigcup_n \Omega_n$. בפרט כל מספר מרוכב לא אפסי עם ערך מוחלט השונה מ-1 הוא מסדר אינסופי.

תרגיל 18.8. תהי G חבורה. הוכיחו שאם $G/Z(G)$ היא ציקלית, אז G אבלית.

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 אבלית. 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 אבלית. $\square$

מסקנה 18.9. אם G לא אבלית, אז $G/Z(G)$ לא ציקלית (ובפרט לא טריוויאלית). בפרט, למרכז אין אינדקס ראשוני (למה?).

מסקנה 18.10. אם G חבורת-p מסדר p^n לא אבלית, אז $|Z(G)| \neq 1, p^{n-1}, p^n$.

19 משפטי האיזומורפיזם של נתר

19.1 משפט האיזומורפיזם הראשון

משפט 19.1 (משפט האיזומורפיזם הראשון)**.** יהי הומומורפיזם $f\colon G\to H$. אז

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

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

דוגמה 19.2. ראינו ש-$\det\colon GL_n(\mathbb{R})\to\mathbb{R}^*$ הוא אפימורפיזם.
הגרעין הוא בדיוק $SL_n(\mathbb{R})$ ולכן $GL_n(\mathbb{R})/SL_n(\mathbb{R})\cong\mathbb{R}^*$.

תרגיל 19.3. 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 $f\colon\mathbb{R}\times\mathbb{R}\to\mathbb{R}$ 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. □

תרגיל 19.4. נסמן $\mathbb{T}=\{z\in\mathbb{C}\,|\,|z|=1\}$. זו חבורה כפלית. הוכיחו כי $\mathbb{R}/_{\mathbb{Z}}\cong\mathbb{T}$.

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

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

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

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

לפי משפט האיזומורפיזם הראשון, נקבל

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

□

תרגיל 19.5. יהי הומומורפיזם $f\colon\mathbb{Z}_{14}\to D_{10}$. מה יכול להיות $\ker f$?

פתרון. נסמן $K = \ker f$. מכיוון ש-$K \lhd \mathbb{Z}_{14}$, אז $|K| \mid |\mathbb{Z}_{14}| = 14$. 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 $|\operatorname{im} f| \mid |D_{10}| = 20$. 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 19.6. תהיינה G_1 ו-G_2 חבורות סופיות כך ש-$(|G_1|, |G_2|) = 1$. מצאו את כל ההומומורפיזמים $f\colon G_1 \to G_2$.

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

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

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

תרגיל 19.7. 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 $D_4, \{\mathrm{id}\} \lhd D_4$; 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 $f\colon D_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ 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 $\{\mathrm{id}\}, \mathbb{Z}_2, \mathbb{Z}_2\times\mathbb{Z}_2, D_4$.

19.2 משפט ההתאמה ושאר משפטי האיזומורפיזם

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

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

ובמובלע: $N\cap H \lhd H$, $NH \le G$ ו-$N \lhd NH$.

דוגמה 19.9. ניקח $H = 15\mathbb{Z} \le \mathbb{Z}$ ו-$N = 6\mathbb{Z}$. אזי

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

ולכן

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

משפט 19.10. תהי G חבורה ו-$K \lhd G$ תת־חבורה נורמלית. אז

א. (משפט ההתאמה) כל תת־החבורות (הנורמליות) של G/K הן מהצורה H/K עבור תת־חבורה (נורמלית) $H \leq G$ המכילה את K.

ב. (משפט האיזומורפיזם השלישי) תהי $H \leq K$ תת־חבורה נורמלית של G אזי $\left.{}^{G/K}\middle/_{H/K}\right. \cong G/H$.

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

הגדרה 19.11. חבורה תקרא חבורה פשוטה אם אין לה תת־חבורות נורמליות לא טריוויאליות.

דוגמה 19.12. יהי p ראשוני. אז $\mathbb{Z}_p$ היא פשוטה. נסו להוכיח שכל חבורה אבלית פשוטה (לאו דווקא סופית) היא מן הצורה הזו.

מסקנה 19.13. מנה של חבורה ביחס לתת־חבורה נורמלית מקסימלית היא פשוטה.

דוגמה 19.14. תת־החבורות של $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$ הן $m\mathbb{Z}/n\mathbb{Z} \cong m\mathbb{Z}_n$ עבור $m|n$.

דוגמה 19.15. $8\mathbb{Z} \leq 2\mathbb{Z}$ אז

$$\left.{}^{\mathbb{Z}/8\mathbb{Z}}\middle/_{2\mathbb{Z}/8\mathbb{Z}}\right. \cong \left.{}^{\mathbb{Z}}\middle/_{2\mathbb{Z}}\right.$$

תרגיל 19.16. תהי $N \lhd G$ מאינדקס ראשוני p, ותהי $K \leq G$. הוכיחו כי או $K \subseteq N$ או ש-$G = NK$ ו- $[K : K \cap N] = p$.

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

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

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

20 משפט קיילי

למעשה כל פעולה של חבורה G על קבוצה X מגדירה הומומורפיזם

$$f : G \to S_X$$

כאשר כל איבר $g \in G$ נשלח לפונקציה שהוא עושה על X, כלומר $f(g)(x) = g * x$.

עובדה 20.1. אם הפעולה נאמנה אז זהו שיכון.

יש לנו פעולה נאמנה של חבורה על עצמה בהיכון: כפל משמאל. מכאן מקבלים את המשפט החשוב הבא.

משפט 20.2 (משפט קיילי). לכל חבורה G יש שיכון

$$G \hookrightarrow S_G$$

דוגמה 20.3. לחבורה $G = D_3$ נמצא שיכון $G \hookrightarrow S_6$. נסמן שרירותית

$$\left\{1 = \mathrm{id}, 2 = \sigma, 3 = \sigma^2, 4 = \tau, 5 = \tau\sigma, 6 = \tau\sigma^2\right\}$$

את איברי החבורה. כעת צריך לבדוק איך כפל משמאל באיבר קבוע פועל על כל האיברים. זו תמורה והיא התמונה ב-S_6 של האיבר הקבוע. למעשה מספיק לבדוק תמונה של קבוצת יוצרים. למשל, נחשב את התמונה של σ בשיכון קיילי:
$\sigma \cdot \mathrm{id} = \sigma$ ולכן σ שולח $1 \mapsto 2$,
$\sigma\sigma = \sigma^2$ ולכן σ שולח $2 \mapsto 3$,
$\sigma\sigma^2 = \mathrm{id}$ ולכן σ שולח $3 \mapsto 1$,
$\sigma\tau = \tau\sigma^2$ ולכן σ שולח $4 \mapsto 6$,
$\sigma\tau\sigma = \tau$ ולכן σ שולח $5 \mapsto 4$,
$\sigma\tau\sigma^2 = \tau\sigma$ ולכן σ שולח $6 \mapsto 5$,
ובסך הכל $\sigma \mapsto (123)(465)$ לפי המספור שבחרנו. האם תוכלו להראות כי תמונת τ היא $(1\ 4)\ (2\ 5)\ (3\ 6)$? שימו לב לבזבזנות במשפט קיילי, הרי אנחנו יודעים שיש שיכון $D_3 \hookrightarrow S_3$!

אם $H \leq G$, יש פעולה של G על הקבוצה G/H לפי כפל משמאל ($g{*}xH = gxH$). כלומר יש הומומורפיזם $G \to S_{G/H}$ שהגרעין שלו הוא הליבה $\mathrm{Core}(H)$. מכאן נקבל:

משפט 20.4 (העידון של משפט קיילי). אם $H \leq G$ תת־חבורה מאינדקס n אז יש הומומורפיזם $G \to S_n$ המוגדר לפי הפעולה על המחלקות השמאליות לפי כפל משמאל

$$x \mapsto (l_x \colon gH \mapsto xgH)$$

בפרט, אם G פשוטה אז יש **שיכון** $G \hookrightarrow S_n$.

תרגיל 20.5. יהי $n \geq 5$ ותהי $H \leq A_n$ תת־חבורה נאותה (כלומר $H \neq A_n$). הוכיחו כי $[A_n \colon H] \geq n$.

פתרון. נסמן $m = [A_n \colon H] > 1$.
לפי משפט העידון של משפט קיילי יש הומומורפיזם לא טריוויאלי $A_n \to S_m$.
ראיתם בהרצאה ש-A_n היא פשוטה עבור $n \geq 5$ ולכן זהו בעצם שיכון $A_n \hookrightarrow S_m$
ולכן $\frac{n!}{2} \mid m!$ מה שגורר $n \leq m$.

דוגמה 20.6. לחבורה A_6 אין תת־חבורות מסדרים $72, 90, 120, 180$.

תרגיל 20.7. תהי $H \leq G$ תת־חבורה מאינדקס m. הוכיחו כי יש תת־חבורה נורמלית $N \lhd G$ כך ש-$N \subseteq H$ וגם $[G \colon N] \mid m!$.

פתרון. נתבונן בפעולה של G על קבוצת המנה $G/H=\{x_1H,x_2H,\dots,x_mH\}$ של כפל משמאל. אזי יש הומומורפיזם $f\colon G\to S_n$. נסמן את הגרעין

$$N=\ker(f)=\{g\in G\mid g(x_iH)=x_iH\}\subset H$$

והוא מוכל ב-H כי האיברים שם בפרט צריכים לקיים $gH=H$. לפי תרגיל בשיעורי בית (ודאו את הפרטים) G משרה פעולה נאמנה של G/N על G/H (ניתן גם לוודא ישירות שהפעולה $(gN)(xH)=gxH$ מוגדרת כמו שצריך). לכן יש גם מונומורפיזם $G/N\to S_m$, ולכן $[G:N]=|G/N|\mid m!$.

תרגיל 20.8. תהי G חבורה סופית ו-p המספר הראשוני הכי קטן שמחלק את $|G|$. תהי $H\le G$ תת־חבורה מאינדקס p. הוכיחו כי זו תת־חבורה נורמלית.

פתרון. לפי התרגיל הקודם יש תת־חבורה נורמלית $N\subseteq H$ כך ש-$[G:N]\mid p!$ כלומר אפשר לרשום $k\,[G:N]=p!$.

לפי כפליות האינדקס מתקיים $[G:N]=[G:H]\,[H:N]$ (מסקנה ממשפט לגראנז'), ולכן

$$k\,[G:H]\,[H:N]=p!$$
$$kp\frac{|H|}{|N|}=p!$$
$$k\,|H|=|N|\,(p-1)!$$

ל-$|H|$ אין מחלקים ראשוניים הקטנים מ-p (אחרת זו סתירה למינימליות של p) ולכן $\gcd\left(|H|,(p-1)!\right)=1$. לכן $|H|\mid|N|$, מה שגורר $H=N$. כלומר $|H|$ נורמלית.

תרגיל 20.9. תהי G חבורה מסדר $2m$, כאשר m הוא מספר אי-זוגי. הוכיחו כי ל-G יש תת־חבורה נורמלית מסדר m.

פתרון. לפי משפט קיילי יש שיכון $\varphi\colon G\hookrightarrow S_{2m}$. נתבונן בתת־חבורה הנורמלית $\varphi(G)\cap A_{2m}\lhd\varphi(G)$ (הנורמלית לפי משפט האיזומורפיזם השני).

אם נראה $\varphi(G)\nsubseteq A_{2m}$ (כלומר שיש בתמונה תמורה אי-זוגית), אז $\varphi(G)A_{2m}=S_{2m}$ ולפי משפט האיזומורפיזם השני:

$$S_{2m}/A_{2m}\cong\varphi(G)/\varphi(G)\cap A_{2m}$$

מה שאומר ש-$\varphi(G)\cap A_{2m}$ מאינדקס 2 ב-$\varphi(G)$, ולכן מסדר $\frac{2m}{2}=m$ כדרוש.

אז למה יש בתמונה תמורה אי-זוגית? ל-G יש איבר a מסדר 2 (הוכחתם את זה, ובכיתה ראיתם את משפט קושי), שנסמן אותו $\varphi(a)=\sigma$.

φ שיכון ולכן σ מסדר 2 בדיוק. לכן σ הוא מכפלה של חילופים זרים. נזכר שבפעולה של חבורה על ידי כפל משמאל לאף איבר אין נקודות שבת, ולכן σ פועל לא טריוויאלית על כל האיברים בחבורה. כלומר שצריך לסדר את כל $2m$ האיברים בחילופים. זה מכריח שיש בדיוק m חילופים - כמות אי-זוגית. לכן התמורה σ היא אי-זוגית.

21 משפטי סילו

משפט 21.1 (משפט קושי)**.** תהא G חבורה סופית ויהי p מספר ראשוני. אם $p \mid |G|$ אזי קיים ב-G איבר מסדר p.

אם p^k מחלק את הסדר G, אז לא בהכרח קיים איבר מסדר p^k. כעת נראה מה קורה לגבי תת־חבורות.

הגדרה 21.2. תהי G חבורה סופית. נרשום את הסדר שלה באופן $|G| = p^t m$ עבור $p \nmid m$. תת־חבורה $H \leq G$ מסדר p^t נקראת תת־חבורה p-סילו של G.

דוגמה 21.3. נמצא תת־חבורת 2-סילו של S_3: כיוון ש-$|S_3| = 6$, אז תת־חבורת 2-סילו שלה היא מסדר 2. יש 3 תת־חבורות כאלה: $\langle(23)\rangle, \langle(13)\rangle, \langle(12)\rangle$.

נשים לב שהראינו כעת שתת־חבורה p-סילו לא בהכרח יחידה! בנוסף גם הראינו שתת־חבורה p-סילו לא בהכרח תת־חבורה נורמלית.

דוגמה 21.4. נמצא תת־חבורה 3-סילו של S_3: כיוון ש-$|S_3| = 6$, אז תת־חבורה 3-סילו היא מסדר 3. יש רק תת־חבורה אחת כזאת, $A_3 = \langle(123)\rangle$, והיא נורמלית.

משפט 21.5 (משפט סילו I)**.** לחבורה סופית G קיימת תת־חבורה p-סילו לכל p ראשוני. בהרצאה ראיתם יותר: אם $p^i \mid |G|$ אז יש ל-G תת־חבורה מסדר p^i.

משפט 21.6 (משפט סילו II)**.** תהי G חבורה. אז

א. כל תת־חבורות p-סילו של חבורה סופית צמודות זו לזו. וכל תת־החבורות הצמודות לתת־חבורה p-סילו הן גם תת־חבורה p-סילו.

ב. כל תת־חבורת-p של G מוכלת בתת־חבורה p-סילו כלשהי.

מסקנה 21.7. תהי H היא תת־חבורה p-סילו של G. היא יחידה אם ורק אם היא נורמלית.

משפט 21.8 (משפט סילו III)**.** נסמן ב-n_p את מספר תת־חבורות p-סילו של G. אז

א. $n_p \mid |G|$

ב. $n_p \equiv 1 \pmod p$

שימו לב שמשני התנאים מקבלים שאם $|G| = p^n m$ כאשר $p \nmid m$, אז $n_p \mid m$ (כי הוא זר ל-p).

תרגיל 21.9. הוכיחו כי כל חבורה מסדר 45 איננה פשוטה.

פתרון. נחשב $45 = 5 \cdot 3^2$. לפי משפט סילו III מתקיים $n_3 \mid 5$ וגם $n_5 \equiv 1 \pmod 5$. המספר היחידי שמקיים זאת הוא $n_5 = 1$. לכן תת־חבורת 5-סילו היא נורמלית. היא מסדר 5 ולכן לא טריוויאלית.

תרגיל 21.10. תהי G חבורה מסדר אי זוגי. הוכיחו שאם $|G| < 21$, אז G אבלית. קצת יותר קשה, אבל נסו למצוא חבורה לא אבלית מסדר 21.

תרגיל 21.11. תהי G חבורה לא אבלית מסדר 21. כמה תת־חבורות סילו יש לה מכל סוג?

פתרון. נחשב $21 = 3 \cdot 7$. לפי משפט סילו III מתקיים $n_7 | 3$ וגם $n_7 \equiv 1 \pmod 7$. לכן $n_7 = 1$.

עבור n_3 מתקיים $n_3 \mid 7$ וגם $n_3 \equiv 1 \pmod 3$. לכן $n_3 \in \{1,7\}$. כדי לבדוק מי מהאופציות נכונה נספור איברים בטבלה הבאה:

כמות האיברים	סדר האיברים
1	1
?	3
$6 = 7 - 1$	7
0	21

נשים לב שתת־חבורה 3-סילו ב-G היא מסדר 3. נשארו לנו $21 - 6 - 1 = 14$ איברים, ולכן ברור שאין רק תת־חבורה 3-סילו אחת. כלומר בהכרח $n_3 = 7$.

תזכורת. $[G : N(H)]$ שווה למספר תת־החבורות (השונות!) הצמודות ל-H.

מסקנה 21.12. תהי P תת־חבורה p-סילו. ראינו שכל תת־החבורות הצמודות ל-P הן בדיוק כל תת־חבורות ה-p-סילו. לכן $n_p = [G : N(P)]$.

תרגיל 21.13. הוכיחו שכל חבורה מסדר 224 אינה פשוטה.

פתרון. נניח בשלילה ש-G פשוטה מסדר $224 = 2^5 \cdot 7$. לפי משפט סילו III נקבל $n_2 \in \{1,7\}$. אבל מכיוון שאנחנו מניחים שהחבורה פשוטה אז בהכרח $n_2 = 7$.

תהי Q תת־חבורה 2-סילו. לפי הטענה שהבאנו לעיל, $[G : N(Q)] = 7$, ולכן לפי העידון של משפט קיילי יש הומומורפיזם $G \to S_7$. אבל הנחנו ש-G פשוטה ולכן זהו שיכון $G \hookrightarrow S_7$. מה שאומר ש-$|G| \mid |S_7|$. אבל $224 \nmid 7!$, וקיבלנו סתירה!

טענה 21.14. תהיינה H_1, H_2 תת־חבורות שונות מסדר p. אז $H_1 \cap H_2 = \{e\}$.
(כי אם יש איבר אחר בחיתוך הוא בהכרח מסדר p ויוצר את שתיהן.)

תרגיל 21.15. אם $|G| = p^2 q$ עבור p, q ראשוניים שונים, אזי G אינה פשוטה.

פתרון. נניח בשלילה שהיא פשוטה. לפי משפט סילו III נקבל $n_p = q$ ו-$n_q \in \{p, p^2\}$.
נשים לב שמכך ש-$n_p = q$ נקבל ש-$q \equiv 1 \pmod p$, מה שמכריח כי $q > p$.

זה גורר שלא ייתכן ש-$n_q = p$, כי אז $p \equiv 1 \pmod q$, ונקבל $q > p$. לכן $n_q = p^2$.

כעת, תהי Q תת־חבורה q-סילו. שימו לב שהיא מסדר q ויש בה $q - 1$ איברים מסדר q (חוץ מהיחידה). מכיוון שיש p^2 תת־חבורות כאלו והן נחתכות טריוויאלית (לפי הטענה הקודמת), אזי יש $p^2(q-1)$ איברים מסדר q ב-G. כלומר נשארו לנו p^2 איברים - מספיק רק בשביל תת־חבורה p-סילו אחת בלבד! וזו סתירה.

דוגמה 21.16. כל חבורה מסדר $99 = 3^2 \cdot 11$ היא לא פשוטה.

22 אוטומורפיזמים

הגדרה 22.1. תהי G חבורה. אוסף האוטומורפיזמים $\mathrm{Aut}(G)$ של G ביחס לפעולה של הרכבת פונקציות הוא חבורה הנקראת חבורת האוטומורפיזמים של G. איבר היחידה הוא העתקת הזהות $\mathrm{id}\colon G \to G$.

דוגמה 22.2. כמה דוגמאות שהוכחו בהרצאה:

א. $\mathrm{Aut}(\mathbb{Z}_n) \cong U_n$.

ב. יהי p ראשוני. אז $\mathrm{Aut}(\mathbb{Z}_p^n) \cong GL_n(\mathbb{F}_p)$, כאשר $\mathbb{F}_p$ הוא השדה הסופי מסדר p.

תרגיל 22.3. תהי $V = \mathbb{Z}_2 \times \mathbb{Z}_2$. הוכיחו $S_3 \cong \mathrm{Aut}(V)$.

פתרון. נשים לב כי $|V| = 4$. כל אוטומורפיזם $\varphi \in \mathrm{Aut}(V)$ יעביר את איבר היחידה של V לעצמו, ויבצע תמורה על הקבוצה $\{x, y, z\}$ של שלושת האיברים הלא טריוויאלים של V. לכן אפשר לזהות את $\mathrm{Aut}(V)$ כתת־קבוצה של $S_{\{x,y,z\}}$, שכמובן איזומורפית ל-S_3.

נשאר להראות שכל תמורה של $S_{\{x,y,z\}}$ היא אכן הומומורפיזם. כל שני איברים מתוך $\{x, y, z\}$ יוצרים את V, והמכפלה שלהם היא האיבר השלישי. נניח כי x, y הם היוצרים, וכך נוכל להתאים לכל תמורה איזומורפיזם. יש שלוש אפשרויות לאן לשלוח את x, ואז 2 אפשרויות לאן לשלוח את y, ונשארים עם אפשרות יחידה עבור z. כך נקבל כל תמורה, וההרכבת תמורות תבטיח שמדובר בחבורה.

למעשה הוכחנו $S_3 \cong GL_2(\mathbb{Z}_2)$.

תרגיל 22.4. תהינה G, H חבורות. אז קיים שיכון

$$\Phi\colon\ \mathrm{Aut}(G) \times \mathrm{Aut}(H) \hookrightarrow \mathrm{Aut}(G \times H)$$

פתרון. לאורך התרגיל נסמן איברים $\varphi_G, \psi_G \in \mathrm{Aut}(G)$, $\varphi_H, \psi_H \in \mathrm{Aut}(H)$, $g \in G$ ו-$h \in H$. מסתבר ש"הניסיון הראשון" יעבוד: נשלח את (φ_G, φ_H) להעתקה $\varphi_G \times \varphi_H$, המוגדרת לפי

$$(\varphi_G \times \varphi_H)\,(g, h) = (\varphi_G(g), \varphi_H(h)) \in G \times H$$

קודם יש להראות כי אכן $\varphi_G \times \varphi_H \in \mathrm{Aut}(G \times H)$. כלומר שזה הומומורפיזם חח"ע ועל. לא נראה זאת כאן.

כעת נראה כי Φ הוא הומומורפיזם. לפי הגדרה

$$\Phi\,(\varphi_G \circ \psi_G, \varphi_H \circ \psi_H) = (\varphi_G \circ \psi_G) \times (\varphi_H \circ \psi_H)$$
$$\Phi\,(\varphi_G, \varphi_H) \circ \Phi\,(\psi_G, \psi_H) = (\varphi_G \times \varphi_H) \circ (\psi_G \times \psi_H)$$

כדי להוכיח שהפונקציות האלו שוות, נבדוק האם הן מסכימות על כל האיברים. אכן

$$\begin{aligned}(\varphi_G\times\varphi_H)\circ(\psi_G\times\psi_H)(g,h)&=(\varphi_G\times\varphi_H)(\psi_G(g),\psi_H(h))\\&=((\varphi_G\circ\psi_G)(g),(\varphi_H\circ\psi_H)(h))\\&=((\varphi_G\circ\psi_G)\times(\varphi_H\circ\psi_H))(g,h)\end{aligned}$$

ולכן Φ הוא הומומורפיזם. חח"ע של Φ נובעת מחח"ע בכל רכיב.

הערה 22.5. אגב, אם $(|G|,|H|)=1$, אז Φ הוא איזומורפיזם (ההוכחה לא קשה, אבל קצת ארוכה). נסו למצוא בעזרת זה את $\mathrm{Aut}(\mathbb{Z}_n^r)$.

הגדרה 22.6. תהי G חבורה, ויהי $a\in G$. האוטומורפיזם $\gamma_a\colon G\to G$ המוגדר לפי $\gamma_a(g)=aga^{-1}$ נקרא אוטומורפיזם פנימי. נסמן

$$\mathrm{Inn}(G)=\{\gamma_a\,|\,a\in G\}$$

החבורה הזו נקראת חבורת האוטומורפיזמים הפנימיים של G.

תרגיל 22.7. הוכיחו כי $\gamma_a\circ\gamma_b=\gamma_{ab}$, וכי $\gamma_a^{-1}=\gamma_{a^{-1}}$. הסיקו כי $\mathrm{Inn}(G)$ היא אכן חבורה עם פעולת ההרכבה.

הוכחה. לכל $g\in G$ מתקיים

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

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

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

□

תרגיל 22.8 (בהרצאה)**.** הוכיחו כי לכל חבורה G,

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

הוכחה. נגדיר $f\colon G\to\mathrm{Inn}(G)$ לפי $f(g)=\gamma_g$. זהו הומומורפיזם, לפי תרגיל 22.7. מובן שהוא על (לפי הגדרת $\mathrm{Inn}(G)$). נחשב את הגרעין:

$$\begin{aligned}\ker f&=\{g\in G\,|\,\gamma_g=\mathrm{id}_G\}=\{g\in G\,|\,\forall h\in G:\gamma_g(h)=h\}\\&=\left\{g\in G\,\middle|\,\forall h\in G:ghg^{-1}=h\right\}=\{g\in G\,|\,\forall h\in G:gh=hg\}=Z(G)\end{aligned}$$

לפי משפט האיזומורפיזם הראשון, נקבל $G/Z(G)\cong\mathrm{Inn}(G)$. □

טענה 22.9 (בהרצאה). לכל חבורה G מתקיים $\mathrm{Inn}(G)\lhd\mathrm{Aut}(G)$.

תרגיל 22.10. חשבו את $|\mathrm{Inn}(H)|$ עבור חבורת הייזנברג

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a, b, c \in \mathbb{Z}_3 \right\}$$

פתרון. נחשב את $|Z(H)|$. לפי משפט לגראנז' האפשרויות הן $1, 3, 9, 27$.
$|Z(H)| \neq 1$ כי לחבורות-p יש מרכז לא טריוויאלי.
$|Z(H)| \neq 27$ כי זו לא חבורה אבלית.
$|Z(H)| \neq 9$ כי אז המנה $H/Z(H)$ היא מסדר 3. אז היא בהכרח ציקלית וזה גורר (כפי הוכחנו בעבר) ש-H אבלית. לכן $|Z(H)| = 3$ ונקבל $|\mathrm{Inn}(H)| = \frac{27}{3} = 9$.

23 משפט N/C

נסתכל על חבורה G הפועלת על עצמה על ידי הצמדה. אם N תת־חבורה נורמלית, אז היא סגורה להצמדה ולכן G פועלת גם על N.

אם $H \leq G$ לא נורמלית אז פעולת ההצמדה לא שומרת על H. כדי לתקן את זה נסתכל על האיברים ב-G שאם נצמיד בהם **כן** נשמור על H:

הגדרה 23.1. המנרמל של תת־חבורה H ב-G הוא תת־החבורה

$$N_G(H) = \left\{ g \in G \,\middle|\, gHg^{-1} = H \right\}$$

מכיוון שהמנרמל הוא תת־חבורה והוא פועל על H, אז השגנו פעולה של חבורה על H.

זה נותן לנו הומומורפיזם $N_G(H) \to S_H$ (כמו שראינו במשפט קיילי). אבל למעשה, האיברים של המנרמל פועלים על ידי הצמדה, כך שהם לא סתם פונקציה על H - אלא אוטומורפיזמים! כך שקיבלנו הומומורפיזם $N_G(H) \to \mathrm{Aut}(H)$ שהגרעין שלו הוא $C_G(H)$.

משפט 23.2 (משפט N/C)**.** תהי $H \leq G$ תת־חבורה. אז קיים שיכון

$$N_G(H) / C_G(H) \hookrightarrow \mathrm{Aut}(H)$$

דוגמה 23.3. אם נבחר $H = G$, אז נסיק מהמשפט $G/Z(G) \cong \mathrm{Inn}\,(G)$, כפי שראינו.

תרגיל 23.4. תהי G חבורה ו-$K \lhd G$ סופית. הוכיחו כי $C_G(K)$ מאינדקס סופי.

פתרון. מכיוון ו-K נורמלית, אז $N_G(K) = G$. לכן לפי משפט N/C יש שיכון $G/C_G(K) \hookrightarrow \mathrm{Aut}(K)$.

מפני ש-K סופית, אז גם $\mathrm{Aut}(K)$ סופית. לכן $G/C_G(K)$ סופית, מה שאומר שהאינדקס של $C_G(K)$ סופי.

תרגיל 23.5. תהי חבורה G מסדר mp כאשר p ראשוני, $(m,p)=1$ וגם $(m,p-1)=1$.
הוכיחו שאם P תת־חבורה p-סילו של G נורמלית, אז $P\subseteq Z(G)$.

פתרון. הרעיון הוא להראות ש-$C(P)=G$. לפי משפט N/C יש שיכון

$$ {}^{N(P)}/_{C(P)} \hookrightarrow \mathrm{Aut}(P) $$

P נורמלית ולכן $N(P)=G$. בנוסף P היא מסדר ראשוני p (כי m זר ל-p), ולכן $P\cong\mathbb{Z}_p$. אז נקבל

$$ \mathrm{Aut}(P)\cong\mathrm{Aut}(\mathbb{Z}_p)\cong U_p $$

כלומר קיבלנו $G/C(P)\hookrightarrow U_p$, ולפי משפט לגראנז' $p-1 \mid |G/C(P)| = \dfrac{mp}{|C(P)|}$.
אבל m ו-p זרים ל-$p-1$, ולכן בהכרח $|C(P)|=mp$. מכאן ש-$C(P)=G$, כדרוש.

24 מכפלות ישרות וישרות למחצה

הכרתם את המכפלה הישרה החיצונית $G=A\times B$ עבור חבורות A,B (שבאו מ"בחוץ").
נשים לב שאפשר לזהות $A\cong A\times\{e_B\}$ ו-$B\cong\{e_A\}\times B$ וכך לחשוב על A,B כתת־חבורות של G (שבאו מ"בפנים"). יש להן כמה תכונות טובות:

- $A,B\lhd G$
- $A\cap B=\{e_G\}$
- $G=AB$ (כי $(a,b)=(a,e)(e,b)$).
- כל האיברים של A מתחלפים עם כל האיברים של B.

כעת, אם נתונה לנו G בתחפושת (חבורה שאיזומורפית ל-G) איך נוכל לזהות שזה במקור מכפלה ישרה? כלומר איך מזהים מכפלה "מבפנים"?

הגדרה 24.1. תהי G חבורה ו-$A,B\le G$ תת־חבורות. אם מתקיים:

- $A,B\lhd G$
- $A\cap B=\{e_G\}$
- $G=AB$

אז אומרים ש-G היא מכפלה ישרה פנימית של A,B.

משפט 24.2. אם G היא מכפלה פנימית ישרה של A,B אז $G\cong A\times B$.

בפרט נובע שאברי A,B מתחלפים זה עם זה.
זה אומר שכדי לדעת את לוח הכפל של כל החבורה כל מה שצריך לדעת זה את A,B. כי אז מכפלה של איברים כלליים היא פשוט $(a_1b_1)(a_2b_2)=(a_1a_2)(b_1b_2)$.

תרגיל 24.3. הוכיחו כי $D_{2n} \cong D_n \times \mathbb{Z}_2$ כאשר n אי-זוגי.

פתרון. בעצם עלינו למצוא ב-D_{2n} תת־חבורה נורמלית שאיזומורפית ל-D_n ותת־חבורה נורמלית שאיזומורפית ל-$\mathbb{Z}_2$ שמקיימות את כל הדרוש.

נתחיל בלחפש תת־חבורה שדומה ל-D_n. שיקוף כבר יש לנו, והוא τ. בשביל סיבוב מסדר n נקח את σ^2. אזי אפשר לבדוק ש-$A = \langle \sigma^2, \tau \rangle$ היא החבורה הדרושה.

עבור $\mathbb{Z}_2$ זו צריכה להיות תת־חבורה מסדר 2 שתשלים את A. נקח לשם כך את $B = \langle \sigma^n \rangle$.

כעת נבדוק שהכל מתקיים:

- A נורמלית כי היא מאינדקס 2.
- B נורמלית מבדיקה ישירה (או מכך שהיא מוכלת במרכז).
- רואים כי $A \cap B = \{\mathrm{id}\}$ לפי ההצגה הקנונית של איברים כ-$\tau^i\sigma^j$.
- $D_{2n} = AB$ כי היוצרים של D_{2n} נמצאים ב-AB: באופן מיידי עבור $\tau = \tau \cdot \mathrm{id}$, ועבור σ,

$$\sigma = \underbrace{\left(\sigma^2\right)^{\frac{n+1}{2}}}_{\in A}\underbrace{\left(\sigma^n\right)}_{\in B}$$

שימו לב שפה השתמשנו בכך ש-n אי-זוגי.

לכן לפי המשפט על מכפלה ישרה, $D_{2n} \cong A \times B \cong D_n \times \mathbb{Z}_2$.

טענה 24.4. יהיו m,n טבעיים. אז $(m,n)=1$ אם ורק אם $\mathbb{Z}_{mn} \cong \mathbb{Z}_n \times \mathbb{Z}_m$.

אין לנו זמן לדבר על מכפלה ישרה למחצה חיצונית!

מה קורה כאשר בבניה של מכפלה ישרה פנימית נוותר על הדרישה ש-B נורמלית?

הגדרה 24.5. תהי G חבורה ו-$K,Q \le G$ תת־חבורות. אם מתקיים:

- $K \lhd G$ (חשוב!)
- $K \cap Q = \{e\}$
- $G = KQ$

אזי G נקראת מכפלה ישרה למחצה (פנימית) של K ב-Q (שימו לב לסדר!) ומסמנים

$$G = K \rtimes Q$$

הערה 24.6. הסימן $\rtimes$ הוא מעין שילוב של הסימן $\times$ עם $\lhd$, שמופנה לתת־חבורה הנורמלית. איך זה מלמד אותנו על המבנה של G? נכפול שני איברים כללים:

$$(k_1q_1)(k_2q_2) = k_1\underbrace{\left(q_1k_2q_1^{-1}\right)}_{\in K}q_1q_2$$

כלומר שאפשר לשחזר את G מ-K,Q והפעולה של Q על K. לכן לפעמים מסמנים (וכך בונים מכפלה חיצונית) $G = K \rtimes_\varphi Q$ כאשר φ היא פעולה של Q על K.

תרגיל 24.7. הראו ש-$\mathbb{Z}_6$ ו-S_3 הן מכפלות ישרות למחצה של תת־חבורה נורמלית מסדר 3 בתת־חבורה מסדר 2. הראו ש-S_3 אינה מכפלה ישרה למחצה של תת־חבורה נורמלית מסדר 2 בתת־חבורה מסדר 3.

פתרון. $\mathbb{Z}_6 = \langle 2\rangle \rtimes \langle 3\rangle$ ו-$S_3 = \langle(123)\rangle \rtimes \langle(12)\rangle$.
ל-S_3 אין תת־חבורה נורמלית מסדר 2, ולכן ברור שהיא לא מכפלה ישרה למחצה עם תת־חבורה נורמלית מסדר כזה.

25 חבורות אבליות נוצרות סופית

הרעיון בגדול הוא שכל חבורה אבלית נוצרת סופית היא מכפלה ישרה (סופית) של חבורות ציקליות. אנו נתמקד בחבורות סופיות. נראה איך אפשר לפרוט את הרעיון הזה לספירת מספר החבורות האבליות מסדר נתון, מציאת איברים מסדר מסוים וכו'.

משפט 25.1 (מיון חבורות אבליות נוצרות סופית)**.** תהי G *חבורה אבלית נוצרת סופית.* *אזי יש לה צורה קנונית*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_s}$$

שבה $d_i | d_{i+1}$ *לכל* $1 \le i \le s-1$. *למספר* $r \ge 0$ *קוראים הדרגה של* G.

הערה 25.2. חבורה אבלית נוצרת סופית היא סופית אם ורק אם $r = 0$. כדי להציג את G בצורה הקנונית שלה בדרך כלל עושים שימוש חוזר בטענות המוכרות $H \times K \cong K \times H$ לכל זוג חבורות H, K וש-$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ אם ורק אם $(n, m) = 1$.

תרגיל 25.3. הוכיחו כי $\mathbb{Z}_{200} \times \mathbb{Z}_{20} \cong \mathbb{Z}_{100} \times \mathbb{Z}_{40}$.

פתרון. נראה שלשתי החבורות אותה צורה קנונית (שהיא יחידה), ולכן הן איזומורפיות. הצורה הקנונית של החבורה באגף שמאל היא כמובן $\mathbb{Z}_{20} \times \mathbb{Z}_{200}$. עבור החבורה באגף ימין נמצא את הצורה הקנונית:

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

מה שעשינו בתרגיל האחרון היה לפרק ככל שניתן חבורה למכפלה של חבורות ציקליות מסדר חזקת ראשוני. ננסה להבין כיצד נראות חבורות-p אבליות סופיות.

טענה 25.4. *יהי* p *ראשוני, ותהי* G *חבורה אבלית מסדר* p^n. *אז בצורה הקנונית שלה מופיעות רק חבורות ציקליות מסדר חזקת* p. *כלומר קיימים מספרים טבעיים* $m_1, \ldots, m_k$ *כך ש-*$m_1 + \cdots + m_k = n$ *ומתקיים* $G \cong \mathbb{Z}_{p^{m_1}} \times \mathbb{Z}_{p^{m_2}} \times \cdots \times \mathbb{Z}_{p^{m_k}}$.
למשל אם G אבלית מסדר $27 = 3^3$, אזי היא איזומורפית לאחת מהחבורות הבאות:

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

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

הגדרה 25.5. יהי $n \in \mathbb{N}$. נאמר כי סדרה $m_1 \geq m_2 \geq \cdots \geq m_r$ לא עולה של מספרים טבעיים היא חלוקה של n אם $\sum_{i=1}^{r} m_i = n$. נסמן את מספר החלוקות של n ב-$\rho(n)$.

דוגמה 25.6. $\rho(4) = 5$, כי $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$.

טענה 25.7. מספר החבורות האבליות, עד כדי איזומורפיזם, מסדר p^n הוא $\rho(n)$.

טענה 25.8. כל חבורה אבלית מסדר $p_1^{k_1} \dots p_n^{k_n}$ גם איזומורפית למכפלה של חבורות אבליות $H_1 \times \cdots \times H_n$ כאשר H_i היא מסדר $p_i^{k_i}$. פירוק כזה נקרא פירוק פרימרי.

למשל, אם G חבורה אבלית כך ש-$|G| = 45 = 3^2 \cdot 5$, 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 25.9. מספר החבורות האבליות, עד כדי איזומורפיזם, מסדר $p_1^{k_1} \dots p_n^{k_n}$ הוא $\rho(k_1) \dots \rho(k_n)$.

דוגמה 25.10. מספר החבורות האבליות מסדר $2^3 \cdot 5^2 = 200$ הוא $\rho(3)\rho(2) = 3 \cdot 2 = 6$. האם אתם יכולים למצוא את כולן? מה היא הצורה הקנונית של כל אחת?

הגדרה 25.11. תהי G חבורה. נגדיר את האקספוננט של החבורה $\exp(G)$ (או המעריך) 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 25.12. 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 25.13. הוכיחו שאם G חבורה אבלית סופית כך ש-$\exp(G) = |G|$, אז G ציקלית.

פתרון. נניח וישנו פירוק $\exp(G) = p_1^{k_1} \dots p_n^{k_n} = |G|$. אנחנו יכולים לפרק את G לפירוק פרימרי $A_1 \times \cdots \times A_n$, 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 $\left(p_i^{k_i}, p_j^{k_j}\right) = 1$ עבור $i \neq j$, ולכן נקבל כי

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

ולכן G היא ציקלית.

26 תת־חבורת הקומוטטורים

הגדרה 26.1. תהא G חבורה. הקומוטטור של זוג איברים $a, b \in G$ הוא האיבר

$$[a,b] = aba^{-1}b^{-1}$$

הערה 26.2. a, b מתחלפים אם ורק אם $[a,b] = e$. באופן כללי, $ab = [a,b]\,ba$.

הגדרה 26.3. תת־חבורת הקומוטטורים (נקראת גם תת־חבורת הנגזרת) הינה:

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

כלומר תת־החבורה הנוצרת על ידי כל הקומוטטורים של G.

הערה 26.4. G אבלית אם ורק אם $G' = \{e\}$.
למעשה, תת־חבורת הקומוטטורים "מודדת" עד כמה החבורה G אבלית.

הערה 26.5. $[a,b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b,a]$.
אבל מכפלה של קומוטטורים היא לא בהכרח קומוטטור!

הערה 26.6. אם $H \leq G$ אז $H' \leq G'$.

הערה 26.7. $G' \lhd G$. למשל לפי זה ש-$g\,[a,b]\,g^{-1} = [gag^{-1}, gbg^{-1}]$ ואינדוקציה.
תת־חבורת הקומוטטורים מקיימת למעשה תנאי חזק הרבה יותר מנורמליות: לכל הומומורפיזם $f \colon G \to H$ מתקיים

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

ולכן G' היא תת־חבורה אופיינית במלואה. להוכחת הנורמליות של G' מספיק להראות שתנאי זה מתקיים לכל אוטומורפיזם פנימי של G.

הגדרה 26.8. חבורה G נקראת מושלמת אם $G = G'$.

מסקנה 26.9. אם G חבורה פשוטה לא אבלית, אז היא מושלמת.

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

דוגמה 26.10. עבור $n \geq 5$, מתקיים $A_n' = A_n$. אבל $\mathbb{Z}_5$ למשל היא פשוטה ולא מושלמת, כי היא אבלית.

משפט 26.11. המנה G/G', שנקראת האבליניזציה של G, היא המנה האבלית הגדולה ביותר של G. כלומר:

א. לכל חבורה G, המנה G/G' אבלית.

ב. לכל $G \triangleright N$ מתקיים ש-${}^{G}/_{N}$ אבלית אם ורק אם $G' \leq N$ (כלומר ${}^{G}/_{N}$ איזומורפית למנה של ${}^{G}/_{G'}$. הראו זאת לפי משפט האיזומורפיזם השלישי).

דוגמה 26.12. אם A אבלית, אז $A \cong {}^{A}/_{G'}$.

תרגיל 26.13. הראו שכל חבורת-p סופית אינה מושלמת.

דוגמה 26.14. תהי $D_4 = \langle \sigma, \tau \rangle$. ראינו ש-$\{e, \sigma^2\} = Z(D_4) \triangleleft G$.
כמו כן, המנה $|{}^{D_4}/_{Z(D_4)}| = 4$. תת־חבורה זו אבלית מכיוון שהסדר שלה הוא p^2.
לכן, לפי תכונת המקסימליות של האבליניזציה, $D_4' \leq Z(D_4)$. החבורה D_4 לא אבלית ולכן $D_4' \neq \{e\}$. לכן $D_4' = Z(D_4)$.

תרגיל 26.15. מצא את S_n' עבור $n \geq 5$.

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

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

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 אבלית. לכן, לפי מקסימליות האבליניזציה, נקבל $S_n' = A_n$.

הערה 26.16. הטענה בתרגיל נכונה גם עבור S_3 ו-S_4, אך משיקולים שונים. עבור $n = 3$, מתקיים $S_3' \triangleleft A_3$, ומפני ש-$S_3' \neq \{\mathrm{id}\}$ כי S_3 לא אבלית, נקבל $S_3' = A_3$. עבור $n = 4$, צריך לשים לב למשל ש-$(234) = [(24), (123)]$.

תרגיל 26.17. תהי G חבורה מסדר 28. הוכיחו:

א. יש לה תת־חבורה נורמלית $P \triangleleft G$ מסדר 7.

ב. אם G לא אבלית, אז $|G'| = 7$.

ג. אם G לא אבלית, אז $|\mathrm{Inn}(G)| = 14$. הניחו שקיימת תת־חבורה נורמלית $N \triangleleft G$ מסדר 2.

פתרון. נחשב $28 = 2^2 \cdot 7$.

א. לפי משפט סילו III מתקיים $n_7 | 4$ וגם $n_7 \equiv 1 \pmod 7$. לכן $n_7 = 1$, ויש תת־חבורה 7-סילו P יחידה, ולכן היא נורמלית. ברור ש-$|P| = 7$.

ב. נסתכל על $P \triangleleft G$. המנה ${}^{G}/_{P}$ היא מסדר 4, ולכן אבלית. כלומר $G' \leq P$. נתון ש-G לא אבלית, ולכן $G' \neq \{e\}$. מפני ש-$P \cong \mathbb{Z}_7$ פשוטה, אז בהכרח $G' = P$, ולכן גם $|G'| = 7$.

ג. ראינו כי $G/Z(G) \cong \mathrm{Inn}(G)$, ולכן מספיק למצוא את הסדר של $Z(G)$. האפשרויות לסדר הן $|Z(G)| \in \{1,2,4,7,14\}$ כי G לא אבלית. אם $Z(G) = 4$ או $Z(G) = 14$, אז המנה $G/Z(G)$ ציקלית, ולפי טענה שראינו, אז G אבלית - סתירה לנתון.

אין צורך בהנחה "שבמקרה" קיימת תת־חבורה נורמלית מסדר 2, כי לכל חבורה מסדר 28 יש כזאת, אבל זה מקל על הפתרון. מפני שתת־חבורה נורמלית היא איחוד של מחלקות צמידות, ונתון $|N| = 2$, אז בהכרח $N \subseteq Z(G)$. לכן $|Z(G)| \neq 1$. לכן גם $2\,|\,|Z(G)|$, ונקבל $|Z(G)| \neq 7$. נשאר רק $|Z(G)| = 2$.

דרך אחרת, היא להסתכל על תת־חבורה 2-סילו Q, ולשים לב כי $P \cap Q = \{e\}$, וגם $PQ = G$. לכן קיים $\varphi\colon Q \to \mathrm{Aut}(P)$ כך ש-$G \cong P \rtimes_\varphi Q$. שמים לב ש-$\mathrm{Aut}(P) \cong U_7 \cong \mathbb{Z}_6$, ואז ממיינים את כל ארבע החבורות מסדר 28.

27 סדרות נורמליות וסדרות הרכב

הגדרה 27.1. תהי G חבורה. סדרה תת־נורמלית של G היא סדרה של תת־חבורות נורמליות

$$\{e\} = G_n \lhd \cdots \lhd G_2 \lhd G_1 = G$$

וחשוב לשים לב שכל תת־חבורה היא נורמלית בזו שאחריה, ולאו דווקא נורמלית ב-G. לחבורות המנה G_i/G_{i+1} קוראים הגורמים (או המנות) של הסדרה.

דוגמה 27.2. לכל חבורה G יש סדרה תת־נורמלית $\{e\} \lhd G$, והגורם היחיד שלה הוא $G/\{e\} \cong G$.

דוגמה 27.3. הסדרה $\{\mathrm{id}\} \lhd \langle(123)\rangle \lhd S_3$ היא תת־נורמלית. הגורמים הם $S_3/\langle(123)\rangle \cong \mathbb{Z}_2$ ו-$\langle(123)\rangle/\{\mathrm{id}\} \cong \mathbb{Z}_3$.

הגדרה 27.4. תהי $\{e\} = G_n \lhd \cdots \lhd G_2 \lhd G_1 = G$ סדרה תת־נורמלית. עידון של הסדרה הוא סדרה נורמלית שבה יש את אותן תת־חבורות ומוסיפים תת־חבורות נוספות כמו G_i^*:

$$\{e\} = G_n \lhd \cdots \lhd G_{i+1} \lhd G_i^* \lhd G_i \lhd \cdots \lhd G_2 \lhd G_1 = G$$

כאשר הגורמים החדשים $G_i/G_i^* \neq \{e\}$ ו-$G_i^*/G_{i+1} \neq \{e\}$ אינם טריוויאלים.

הגדרה 27.5. סדרה תת־נורמלית שאין לה עידונים נקראת סדרת הרכב.

טענה 27.6. סדרה תת־נורמלית היא סדרת הרכב אם ורק אם כל הגורמים של הסדרה הם פשוטים (כלומר המנות הן חבורות פשוטות).

דוגמה 27.7. תהי $G = \mathbb{Z}_2 \times \mathbb{Z}_4$. הסדרה $\{0\} \times \{0\} \lhd \mathbb{Z}_2 \times \{0\} \lhd G$ היא תת־נורמלית, אך לא סדרת הרכב. העידון שלה

$$\{0\} \times \{0\} \lhd \mathbb{Z}_2 \times \{0\} \lhd \mathbb{Z}_2 \times \langle 2 \rangle \lhd G$$

הוא כבר סדרת הרכב.

דוגמה 27.8. הסדרה $S_n \rhd A_n \rhd \{\mathrm{id}\}$ עבור $n \geq 5$ היא סדרת הרכב, כי כל הגורמים פשוטים.

דוגמה 27.9. הסדרה $S_4 \rhd A_4 \rhd \{\mathrm{id}\}$ היא לא סדרת הרכב, כי ניתן לעדן אותה עם חבורת הארבעה של קליין V_4 לסדרה הנורמלית $S_4 \rhd A_4 \rhd V_4 \rhd \{\mathrm{id}\}$. אך זו עדין לא סדרת הרכב. ניתן לעדן שוב ולקבל את סדרת ההרכב

$$\{\mathrm{id}\} \lhd \langle (12)\,(34) \rangle \lhd V_4 \lhd A_4 \lhd S_4$$

שקל לבדוק שכל הגורמים בה איזומורפיים ל-$\mathbb{Z}_2$ או $\mathbb{Z}_3$, ולכן פשוטים.

משפט 27.10 (ז'ורדן-הולדר)**.** כל סדרות ההרכב של חבורה G הן מאותו אורך, ועם אותן מנות עד כדי סדר.

דוגמה 27.11. לחבורה $\mathbb{Z}_{12}$ יש סדרות הרכב

$$0 \lhd \langle 6 \rangle \lhd \langle 2 \rangle \lhd \mathbb{Z}_{12}$$
$$0 \lhd \langle 6 \rangle \lhd \langle 3 \rangle \lhd \mathbb{Z}_{12}$$
$$0 \lhd \langle 4 \rangle \lhd \langle 2 \rangle \lhd \mathbb{Z}_{12}$$

המנות איזומורפיות (עד כדי סדר) ל-$\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3$.

28 חבורות פתירות

הגדרה 28.1. חבורה תקרא פתירה אם קיימת לה סדרה תת־נורמלית (ולאו דווקא סדרת הרכב) שכל הגורמים בה אבליים.

דוגמה 28.2.

א. כל חבורה אבלית G היא פתירה, כי בסדרה התת־נורמלית $G \rhd \{e\}$ כל הגורמים אבליים (שזה רק $G/\{e\} \cong G$).

ב. החבורות הדיהדרליות פתירות, שכן בסדרה התת־נורמלית $D_n \rhd \langle \sigma \rangle \rhd \{\mathrm{id}\}$ הגורמים איזומורפיים ל-$\mathbb{Z}_2$ ו-$\mathbb{Z}_n$, בהתאמה, שהם אבליים.

ג. החבורות S_n ו-A_n אינן פתירות עבור $n \geq 5$.

תרגיל 28.3. הראו שחבורת הייזנברג $H(\mathbb{Z}_p)$ היא פתירה.

פתרון. ראינו שהחבורה הזו לא אבלית, ושמתקיים $|H(\mathbb{Z}_p)| = p^3$. כמו כן ראינו שהמרכז שלה $Z = Z(H(\mathbb{Z}_p))$ הוא מסדר p. לכן $|H(\mathbb{Z}_p)/Z| = p^2$ היא חבורה מסדר p^2, שהוכחתם שהן תמיד אבליות. אז קיימת סדרה נורמלית $H(\mathbb{Z}_p) \rhd Z \rhd \{e\}$ שבה כל הגורמים אבליים, ולכן החבורה פתירה.

הוכיחו שחבורת הייזנברג פתירה מעל כל שדה, ולא רק מעל $\mathbb{Z}_p$.

משפט 28.4 (בהרצאה)**.** כל חבורת-p היא פתירה.

טענה 28.5. תהא G חבורה מסדר pq, עבור p,q ראשוניים. אזי G פתירה.

הוכחה. אם $p=q$, אז $|G|=p^2$. לכן G אבלית, ולכן פתירה.

אם $p\neq q$, אז נניח בלי הגבלת הכלליות ש-$p>q$. לפי משפט סילו III מתקיים $n_q|p$ וגם $n_q\equiv 1 \pmod q$. אבל הנחנו $q>p$, ולכן $n_q=1$. לכן קיימת תת־חבורה q-סילו Q יחידה ל-G, והיא נורמלית. נתבונן בסדרה הנורמלית $G\rhd Q\rhd\{e\}$. אז $|{}^{G}\!/\!_{Q}|=p$, ולכן ${}^{G}\!/\!_{Q}\cong\mathbb{Z}_p$ אבלית. כמו כן ${}^{Q}\!/\!_{\{e\}}\cong Q\cong\mathbb{Z}_q$. כל הגורמים בסדרה אבליים, ולכן G פתירה. $\square$

תרגיל 28.6. הוכיחו שכל חבורה G מסדר 1089 היא פתירה.

פתרון. נחשב $1089=3^2\cdot 11^2$. לפי משפט סילו III נקבל $n_{11}|3^2$ וגם $n_{11}\equiv 1 \pmod{11}$. לכן $n_{11}=1$. תהי Q תת־חבורה 11-סילו של G. היא נורמלית ומתקיים $|Q|=11^2$, ולכן אבלית. כמו כן $|{}^{G}\!/\!_{Q}|=3^2$, ולכן גם ${}^{G}\!/\!_{Q}$ אבלית. בסדרה הנורמלית $G\rhd Q\rhd\{e\}$ כל הגורמים אבליים, ולכן G פתירה.

משפט 28.7 (בהרצאה)**.** תהי $G\rhd N$. החבורה G פתירה אם ורק אם N, ${}^{G}\!/\!_{N}$ פתירות.

דוגמה 28.8. כל חבורה מסדר $11979=3^2\cdot 11^3$ היא פתירה. כמו בתרגיל 28.6 מוכיחים $n_{11}=1$, ומסתכלים על הסדרה $G\rhd Q\rhd\{e\}$. תת־החבורה Q היא לא בהכרח אבלית, אבל היא פתירה כי היא חבורת-11.

הגדרה 28.9. תהי G חבורה. נגדיר באופן רקורסיבי את סדרת תת־חבורות הנגזרת שלה. תהי $G^{(0)}=G$, ועבור $n>0$ תהי $G^{(n)}=\left[G^{(n-1)},G^{(n-1)}\right]$. למשל $G^{(1)}=G'$.

מסקנה 28.10. לכל $k\in\mathbb{N}$ מתקיים $G\rhd G^{(k)}$ ובפרט $G^{(k-1)}\rhd G^{(k)}$.

משפט 28.11. חבורה G היא פתירה אם ורק אם קיים $t\in\mathbb{N}$ כך ש-$G^{(t)}=\{e\}$. המינימלי מבין ה-t נקרא דרגת הפתירות של G.

דוגמה 28.12. תהי $G=D_3$. אז $G^{(1)}=G'=\langle\sigma\rangle$ ו-$G^{(2)}=\{\mathrm{id}\}$. אזי G פתירה.

דוגמה 28.13. דרך נוספת להראות ש-S_n עבור $n\geq 5$ אינה פתירה. לכל $t\geq 1$ מתקיים $(S_n)^{(t)}=A_n\neq\{\mathrm{id}\}$.

תרגיל 28.14. הוכיחו כי לכל חבורה פתירה לא טריוויאלית יש תת־חבורה נורמלית אבלית שאינה $\{e\}$.

פתרון. החבורה פתירה ולכן יש t מינימלי כך ש-$G^{(t)}=\{e\}$.
זה אומר שתת־החבורה $G^{(t-1)}$ היא אבלית (כי הנגזרת שלה טריוויאלית).
והיא גם נורמלית ולא טריוויאלית (מהמינימליות של t).

שאלה 28.15. יהי $t\in\mathbb{N}$. נסו למצוא חבורה מדרגת פתירות t.

תרגיל 28.16 (לבית)**.** אם $|G|=pq$ כאשר p,q ראשוניים, כך ש- $p\not\equiv 1 \pmod q$, אזי G ציקלית.

תרגיל 28.17 (לבית)**.** מיינו את החבורות מסדר pq, כאשר p,q ראשוניים שונים המקיימים $p\equiv 1 \pmod q$.

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 ב-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.
- $(F^*,\cdot)$, 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 הקווטרניונים. איבר היחידה מסומן 1.

שימו לב שאם פעולה מסומנת $\cdot$ כמו כפל, אז 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.