

מערכי תרגול קורס 89-214 סמסטר א' תשע"ו מבנים אלגבריים למדעי המחשב

דצמבר 2015, גרסה 0.13

תוכן העניינים

2	מבוא
2	1 מבוא לתורת המספרים
6	2 מבנים אלגבריים בסיסיים
10	3 חבורת אוילר
10	4 תת-חבורות
11	5 סדר של איבר וסדר של חבורה
13	6 חבורות ציקליות
15	7 מכפלה קרטזית של חבורות
16	8 החבורה הסימטרית (על קצה המזלג)
18	9 מחלקות
22	10 חישוב פונקציית אוילר
24	11 תת-חבורה הנוצרת על ידי איברים
25	12 החבורה הדיהדרלית
26	13 נושאים נוספים בחבורה הסימטרית
28	14 שימוש בתורת החבורות: אלגוריתם RSA
30	15 הומומורפיזמים
33	16 תת-חבורות נורמליות
35	17 חבורות מנה
36	18 משפטי האיזומורפיזם של נתר

מבוא

כמה הערות טכניות לתחילת הקורס:

- דף הקורס נמצא באתר www.math-wiki.com.
- שאלות בנוגע לחומר הלימודי מומלץ לשאול בדף השיחה באתר של הקורס.
- ישנה חובת הגשת תרגילים, אבל בודקים רק לחצי מהסטודנטים.
- נשמח לכל הערה על מסמך זה.

1 מבוא לתורת המספרים

נסמן כמה קבוצות של מספרים:

- $\mathbb{N} = \{1, 2, 3, \dots\}$ המספרים הטבעיים.
- $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ המספרים השלמים (מגרמנית: Zahlen).
- $\mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\} \right\}$ 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 פחלק 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 $d \neq 0, n \in \mathbb{Z}$ קיימים q, r יחידים כך ש- $n = qd + r$ וגם $0 \leq r < |d|$.

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

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

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

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

1.4. הערה. 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 $d \leq (m, r)$. כעת, לפי הגדרה $(m, r)|r$ וגם $(m, r)|m$, ולכן $(m, r)|n$ כי n הוא צירוף לינארי של m, r . אם ידוע כי $(m, r)|m$ וגם $(m, r)|n$, אזי $(m, r) \leq d$. סך הכל קיבלנו כי $d = (m, r)$. \square

משפט 1.6 (אלגוריתם אוקלידס). "המתכון" למציאת פ"מ בעזרת שימוש חוזר בטענה 1.5 הוא אלגוריתם אוקלידס. ניתן להניח $0 \leq m < n$. אם $m = 0$, אזי $(n, m) = n$. אחרת נכתוב $n = qm + r$ כאשר $0 \leq r < m$ וגמשיך עם $(n, m) = (m, r)$. (הבינו לפה האלגוריתם חייב להעצר).

דוגמה 1.7. נחשב את הממ"מ של 53 ו-47 בעזרת אלגוריתם אוקלידס

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

דוגמה נוספת עבור מספרים שאינם זרים:

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

משפט 1.8 (אפיון הממ"מ כצירוף לינארי מזערי). מתקיים לכל מספרים שלמים a, b כי

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

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

הערה 1.9. מן המשפט קיבלנו כי $(a, b) \in a\mathbb{Z} + b\mathbb{Z}$.

דוגמה 1.10. כדי למצוא את המקדמים s, t כשמביעים את הממ"מ כצירוף לינארי כנ"ל נשתמש באלגוריתם אוקלידס המוכלל:

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

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

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- $1 = sa + tb$. נכפיל ב- c ונקבל $c = sac + tbc$. ברור כי $a|sac$ ולפי הנתון גם $a|tbc$. לכן $a|(sac + tbc)$, כלומר $a|c$.

טענה 1.12. תכונות של ממ"מ:

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

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

3. אם p ראשוני וגם $p|ab$, אזי $p|a$ או $p|b$.

הוכחת התכונות. 1. קיימים s, t כך ש- $d = sn + tm$. כיוון ש- $e|n, m$, אז הוא מחלק גם את צירוף לינארי שלהם $sn + tm$, ז"א את d .

2. (חלק מתרגיל הבית)

3. אם $p \nmid a$, אז $(p, a) = 1$. לכן קיימים s, t כך ש- $1 = sa + tp$. נכפיל את השויוון האחרון ב- b ונקבל $b = sab + tpb$. ברור כי p מחלק את אגף שמאל (הרי $p|ab$), ולכן p מחלק את אגף ימין, כלומר $p|b$.

□

הגדרה 1.13. בהנתן שני מספרים שלמים n, m הכפולה המשותפת המזערית (כמ"מ, least common multiple) שלהם מוגדרת להיות

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

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

טענה 1.14. תכונות של כמ"מ:

1. אם $m|a$ וגם $n|a$, אז $[n, m]|a$.

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

הוכחת התכונות. 1. יהיו q, r כך ש- $a = q[n, m] + r$ כאשר $0 \leq r < [n, m]$. מהנתון כי $n, m|a$ ולפי הגדרה $[n, m]|n, m$, נובע כי $n, m|r$. אם $r \neq 0$ אז סתירה למינימליות של $[n, m]$. לכן $a = q[n, m]$, כלומר $[n, m]|a$.

2. נראה דרך קלה לחישוב הממ"מ והכמ"מ בעזרת הפירוק של מספר למכפלת גורמים ראשוניים. נניח כי הפירוק הוא

$$n = \prod_{i=1}^{\infty} p_i^{\beta_i} = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \dots \quad m = \prod_{i=1}^{\infty} p_i^{\alpha_i} = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots$$

כאשר $\alpha_i, \beta_i \geq 0$ (והם כמעט תמיד אפס כי המכפלה סופית). כעת צריך להשתכנע כי

$$(n, m) = \prod_{i=1}^{\infty} p_i^{\min(\alpha_i, \beta_i)} \quad [n, m] = \prod_{i=1}^{\infty} p_i^{\max(\alpha_i, \beta_i)}$$

ומפני שלכל שני מספרים α, β מתקיים $\alpha + \beta = \min(\alpha, \beta) + \max(\alpha, \beta)$ אז $n, m = |nm|$.

□

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

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

טענה 1.17 (הוכחה לבית). שקילות מודולו n היא יחס שקילות (רפלקסיבי, סימטרי וטרנזיטיבי). כפל וחיבור מודולו n מוגדרים היטב. כלומר אם $a \equiv b, c \equiv d \pmod{n}$ אז $a + c \equiv b + d \pmod{n}$ וגם $ac \equiv bd \pmod{n}$.

צורת רישום 1.18. את אוסף מחלקות השקילות מודולו n מקובל לסמן $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. למשל $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$. $\{[a] : a \in \mathbb{Z}\}$ בסימון \bar{a} , ולעיתים כאשר ההקשר ברור פשוט a .

תרגיל 1.19. מצאו את הספרה האחרונה של 333^{333} .

פתרון. נשים לב כי $333^{333} = 3^{333} \cdot 111^{333}$ לכן

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

ומכאן שהספרה האחרונה היא 3.

תרגיל 1.20 (אם יש זמן). מצאו $x \in \mathbb{Z}$ כך ש- $61x \equiv 1 \pmod{234}$.

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

משפט 1.21 (משפט השאריות הסיני). אם n, m זרים, אזי לכל $a, b \in \mathbb{Z}$ קיים יחיד x כדל ש- $x \equiv a \pmod{n}$, $x \equiv b \pmod{m}$ (יחודי).

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

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

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

□ הוכחת היחידות של x מודולו nm תהיה בתרגיל הבית.

דוגמה 1.22. נמצא $x \in \mathbb{Z}$ כך ש- $x \equiv 1 \pmod{3}$ וגם $x \equiv 2 \pmod{5}$. ידוע כי $(5, 3) = 1$, ולכן $-1 \cdot 5 + 2 \cdot 3 = 1$. במקרה זה $n = 5, m = 3$ וכן $s = -1, t = 2$. לפי משפט השאריות הסיני אפשר לבחור את $x = 1 \cdot (-5) + 2 \cdot 6 = 7$. אכן מתקיים $7 \equiv 1 \pmod{3}$ וגם $7 \equiv 2 \pmod{5}$.

משפט השאריות הסיני הוא יותר כללי. הנה גרסה שלו למערכת משוואות של שקילות מודולו:

משפט 1.23 (אם יש זמן). תהא $\{m_1, \dots, m_k\}$ קבוצת מספרים טבעיים הזרים זה לזה (כלומר כל זוג מספרים בקבוצה הוא זר). נסמן את מכפלתם ב- m . בהנתן קבוצה כלשהי של שאריות $\{a_i \pmod{m_i} : 1 \leq i \leq k\}$, קיימת שארית יחידה x מודולו m המהווה פתרון למערכת המשוואות

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

דוגמה 1.24. נמצא $y \in \mathbb{Z}$ כך ש- $y \equiv 1 \pmod{3}$, $y \equiv 2 \pmod{5}$ וגם $y \equiv 3 \pmod{7}$. נשים לב שהפתרון $y = 7$ מן הדוגמה הקודמת הוא נכון כדי הוספה של $3 \cdot 5 = 15$ (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.

2 מבנים אלגבריים בסיסיים

בהתאם לשם הקורס, כעת נכיר כמה מבנים אלגבריים. מבנה אלגברי שמכירים כבר באלגברה לינארית הוא שדה. אנו נגדיר כמה מבנים יותר "פשוטים", כשהחשוב שבהם הוא חבורה. במרבית הקורס נתרכז בחקר חבורות.

הגדרה 2.1. תהי S קבוצה. פעולה בינארית (binary operation) על S היא פונקציה דו-מקומית $* : S \times S \rightarrow S$. עבור $a, b \in S$ כמעט תמיד במקום לרשום $*(a, b)$ נשתמש בסימון $a * b$. מפני שתמונת הפונקציה $a * b$ שייכת ל- S , נאמר כי הפעולה היא סגורה.

הגדרה 2.2. אגודה (או חבורה למחצה, semigroup) היא מערכת אלגברית $(S, *)$ המורכבת מקבוצה לא ריקה S ומפעולה בינארית על S המקיימת קיבוציות (אסוציאטיביות, associativity). כלומר לכל $a, b, c \in S$ מתקיים $(a * b) * c = a * (b * c)$.

דוגמה 2.3. המערכת $(\mathbb{N}, +)$ של מספרים טבעיים עם החיבור הרגיל היא אגודה.

דוגמה 2.4. המערכת $(\mathbb{Z}, -)$ אינה אגודה, מפני שפעולת החיסור אינה קיבוצית. למשל $(5 - 2) - 1 \neq 5 - (2 - 1)$.

צורת רישום 2.5. לעיתים נקצר ונאמר כי S היא אגודה מבלי להזכיר במפורש את המערכת האלגברית. במקרים רבים הפעולה תסומן כמו כפל, דהיינו ab או $a \cdot b$, ובמקום לרשום מכפלה $aa \dots a$ של n פעמים a נרשום a^n .

הגדרה 2.6. תהי $(S, *)$ אגודה. איבר $e \in S$ נקרא איבר יחידה אם לכל $a \in S$ מתקיים $a * e = e * a = a$.

הגדרה 2.7. מונואיד (monoid, או יחידון) $(M, *, e)$ הוא אגודה בעלת איבר יחידה e . כאשר הפעולה ואיבר היחידה ברורים מן ההקשר, פשוט נאמר כי M הוא מונואיד.

הערה 2.8 (בהרצאה). יהי $(M, *, e)$ מונואיד עם איבר יחידה e . הוכיחו כי איבר היחידה הוא יחיד. הרי אם $e, f \in M$ הם איברי יחידה, אז מתקיים $e = e * f = f$.

הגדרה 2.9. יהי $(M, *, e)$ מונואיד. איבר $a \in M$ יקרא הפיך משמאל אם קיים איבר $b \in M$ כך ש- $ba = e$. במקרה זה b יקרא הופכי שמאלי של a . באופן דומה, איבר $a \in M$ יקרא הפיך מימין אם קיים איבר $b \in M$ כך ש- $ab = e$. במקרה זה b יקרא הופכי ימני של a . איבר יקרא הפיך אם קיים איבר $b \in M$ כך ש- $ba = ab = e$. במקרה זה b יקרא הופכי של a .

תרגיל 2.10 (בהרצאה). יהי $a \in M$ איבר הפיך משמאל ומימין. הראו ש- a הפיך וההופכי שלו הוא יחיד.

פתרון. יהי b הופכי שמאלי כלשהו של a (קיים כזה כי a הפיך משמאל), ויהי c הופכי ימני כלשהו של a (הצדקה דומה). נראה כי $b = c$ ונסיק שאיבר זה הוא הופכי של a . ודאו כי אתם יודעים להצדיק כל אחד מן המעברים הבאים:

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

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

הגדרה 2.11. חבורה (group) $(G, *, e)$ היא מונואיד שבו כל איבר הוא הפיך.

לפי ההגדרה לעיל על מנת להוכיח שמערכת אלגברית $(G, *)$ היא חבורה צריך להראות כי הפעולה $*$ היא סגורה, קיבוצית, שקיים איבר יחידה ושכל איבר הוא הפיך. כמו כן מתקיים: חבורה \Leftarrow מונואיד \Leftarrow אגודה.

דוגמה 2.12. המערכת $(\mathbb{Z}, +)$ היא חבורה שאיבר היחידה בה הוא 0. בכתוב חיבורי מקובל לסמן את האיבר ההופכי של a בסימון $-a$. כתיב זה מתלכד עם המושג המוכר של מספר נגדי ביחס לחיבור.

דוגמה 2.13. יהי F שדה (למשל \mathbb{Q}, \mathbb{R} או \mathbb{C}). אזי $(F, +, 0)$ עם פעולת החיבור של השדה היא חבורה. באופן דומה גם $(M_{n,m}(F), +)$ (אוסף המטריצות בגודל $n \times m$ מעל F) עם פעולת חיבור מטריצות היא חבורה. איבר היחידה הוא מטריצת האפס.

דוגמה 2.14. יהי F שדה. המערכת (F, \cdot) עם פעולת הכפל של השדה היא מונואיד שאינו חבורה (מי לא הפיך?). איבר היחידה הוא 1.

דוגמה 2.15. יהי F שדה. נסמן $F^* = F \setminus \{0\}$. אזי $(F^*, \cdot, 1)$ היא חבורה. לעומת זאת, המערכת (\mathbb{Z}^*, \cdot) עם הכפל הרגיל של מספרים שלמים היא רק מונואיד (מי הם האיברים ההפיכים בו?).

דוגמה 2.16. קבוצה בעלת איבר אחד ופעולה סגורה היא חבורה. לחבורה זו קוראים החבורה הטריטיואלית.

הגדרה 2.17. (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 מיידיית היא שאוסף האיברים ההפיכים במונואיד מהווה חבורה ביחס לפעולה המצומצמת. נסמן חבורה זו ב- $U(M)$ (קיצור של Units).

הגדרה 2.18. המערכת $(M_n(\mathbb{R}), \cdot)$ של מטריצות ממשיות בגודל $n \times n$ עם כפל מטריצות היא מונואיד. לחבורת ההפיכים שלו

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

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

הגדרה 2.19. נאמר כי פעולה דו-מקומית $G \times G \rightarrow G : *$ 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 אָבֶל (Niels Henrik Abel).

דוגמה 2.20. יהי F שדה. החבורה $(GL_n(F), \cdot)$ אינה אבלית עבור $n > 1$.

דוגמה 2.21. מרחב וקטורי V יחד עם פעולת חיבור וקטורים הרגילה הוא חבורה אבלית.

הערה 2.22. עבור קבוצה סופית אפשר להגדיר פעולה בעזרת לוח כפל. למשל, אם $S = \{a, b\}$ ונגדיר

*	a	b
a	a	a
b	b	b

אזי $(S, *)$ היא אגודה כי הפעולה קיבוצית, אך היא אינה מונואיד כי אין בה איבר יחידה. נשים לב שהיא לא חילופית כי $a * b = a$, אבל $b * a = b$. בבית תתבקשו למצוא לוחות כפל עבור S כך שיתקבל מונואיד שאינו חבורה, שתתקבל חבורה וכו'.

הערה 2.23 (אם יש זמן). בקורס באלגברה לינארית כנראה ראיתם הגדרה של שדה $(F, +, \cdot, 0, 1)$ הכוללת רשימה ארוכה של דרישות. בעזרת ההגדרות שראינו נוכל לקצר אותה. נסמן $F^* = F \setminus \{0\}$. נאמר כי F הוא שדה אם $(F, +, 0)$ היא חבורה חילופית, $(F^*, \cdot, 1)$ היא חבורה חילופית וקיום חוק הפילוג (distributive law) לכל $a, b, c \in F$ מתקיים $a(b + c) = ab + ac$.

תרגיל 2.24. האם קיים מונואיד שיש בו איבר הפיך מימין שאינו הפיך משמאל?

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

ההפיכים משמאל הם הפונקציות החח"ע. ההפיכים מימין הם הפונקציות על (להזכיר את הטענות הרלוונטיות מבדידה). מה יקרה אם נבחר את X להיות סופית? (לעתיד: לחבורה $(U(X^X), \circ)$ קוראים חבורת הסימטריה על X ומסמנים S_X . אם $X = \{1, \dots, n\}$ מקובל לסמן את חבורת הסימטריה שלה בסימון S_n , ולכן כל איבר הפיך משמאל. עבור $n \geq 3$ זו חבורה לא אבלית.)

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.

צורת רישום 2.25. יהי n מספר טבעי. נסמן את הכפולות שלו ב- $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$. למשל $4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$.

דוגמה 2.26. נסתכל על אוסף מחלקות השקילות מודולו n , $\mathbb{Z}_n = \{[a] : a \in \mathbb{Z}\}$. כזכור חיבור וכפל מודולו n מוגדר היטב. למשל $[a] + [b] = [a + b]$ כאשר באגף שמאל הסימן $+$ הוא פעולה בינארית הפועלת על אוסף מחלקות השקילות (a הוא נציג של מחלקת שקילות אחת ו- b הוא נציג של מחלקת שקילות אחרת) ובאגף ימין זו פעולת החיבור הרגילה של מספרים (שלאחריה מסתכלים על מחלקת השקילות שבה $a + b$ נמצא). אפשר לראות כי $(\mathbb{Z}_n, +)$ היא חבורה אבלית. נבחר נציגים למחלקות השקילות $\{[0], [1], \dots, [n - 1]\}$. איבר היחידה הוא $[0]$ (הרי $[0] + [a] = [0 + a] = [a]$ לכל $[a]$). קיבוציות הפעולה והאבליות נובעת מקיבוציות והאבליות של פעולת החיבור הרגילה. האיבר ההופכי של $[a]$ הוא $[n - a]$.

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

3 חבורת אוילר

דוגמה 3.1. עדין ניתן להציל את המקרה של הכפל מודולו n . נגדיר את חבורת אוילר (Euler) להיות $U_n = U(\mathbb{Z}_n)$ לגבי פעולת הכפל. נבנה את לוח הכפל של \mathbb{Z}_6 (בהתעלם מ-0) שתמיד יתן במכפלה [0]:

·	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

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

הערה 3.2. אם p הוא מספר ראשוני, אז $U_p = \mathbb{Z}_p^*$ (למה?).

טענה 3.3 (הוכחה לבית). בדומה להערה האחרונה, נאפיין את האיברים ב- U_n . יהי $m \in \mathbb{Z}$ אז $[m] \in U_n$ אם ורק אם $(n, m) = 1$. כלומר, ההפיכים במונואיד (\mathbb{Z}_n, \cdot) הם כל האיברים הזרים ל- n .

דוגמה 3.4. $U_{12} = \{1, 5, 7, 11\}$

דוגמה 3.5. לא קיים ל-5 הופכי כפלי ב- \mathbb{Z}_{10} , שכן אחרת 5 היה זר ל-10 וזו סתירה.

טענה 3.6 (מההרצאה). 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 .

4 תת-חבורות

הגדרה 4.1. תהי G חבורה. תת-קבוצה $H \subseteq G$ היא תת-חבורה, אם היא מהווה חבורה ביחס לפעולה המושרית מ- G .

דוגמה 4.2. לכל חבורה G יש שתי תת-חבורות באופן מיידי: $\{e\} \leq G$ (הנקראת תת-חבורה הטריוויאלית), ו- $G \leq G$.

דוגמה 4.3. לכל $n \in \mathbb{Z}$, $n\mathbb{Z} \leq \mathbb{Z}$. בהמשך נוכיח שאלו כל תת-חבורות של \mathbb{Z} .

דוגמה 4.4 (בתרגיל). $m\mathbb{Z} \leq n\mathbb{Z}$ אם ורק אם $n|m$.

דוגמה 4.5 $(\mathbb{Z}_n, +)$ אינה תת-חבורה של $(\mathbb{Z}, +)$ - כי \mathbb{Z}_n אינה מוכלת ב- \mathbb{Z} : האיברים ב- \mathbb{Z}_n הם מחלקות שקילות, ואילו האיברים ב- \mathbb{Z} הם מספרים.

דוגמה 4.6 U_n אינה תת-חבורה כפלית של (\mathbb{Z}_n, \cdot) - כי (\mathbb{Z}_n, \cdot) אינה חבורה.

דוגמה 4.7 $(GL_n(\mathbb{R}), \cdot)$ אינה תת-חבורה של $(M_n(\mathbb{R}), +)$ - כי הפעולות בהן שונות.

טענה 4.8 (קריטריון מקוצר לתת-חבורה - מההרצאה). תהי $H \subseteq G$ תת-קבוצה. אזי H תת-חבורה של G אם ורק אם שני התנאים הבאים מתקיימים:

1. $e \in H$

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

תרגיל 4.9 יהי F שדה. נגדיר

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

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

הוכחה. ניעזר בקריטריון המקוצר לתת-חבורה.

1. ברור כי $I_n \in SL_n(F)$, כי $\det I_n = 1$.

2. נניח $A, B \in SL_n(F)$. צ"ל $AB^{-1} \in SL_n(F)$. אכן,

$$\det(AB^{-1}) = \det A \det B^{-1} = \frac{\det A}{\det B} = \frac{1}{1} = 1$$

ולכן $AB^{-1} \in SL_n(F)$.

לפי הקריטריון המקוצר, $SL_n(F)$ היא תת-חבורה של $GL_n(F)$.

□

5 סדר של איבר וסדר של חבורה

הגדרה 5.1 תהי G חבורה. נגדיר את הסדר (order) של G להיות עוצמתה כקבוצה. במילים יותר גשמיות, כמה איברים יש בחבורה. סימונים מקובלים: $|G|$ או $\text{Ord}(G)$.

5.2 רישוש. בחבורה כפלית נסמן את החזקה החיובית $a^n = aa \dots a$ לכפל n פעמים. בחבורה חיבורית נסמן $na = a + \dots + a$. חזקות שליליות הן חזקות חיוביות של ההופכי של a . מוסכם כי $a^0 = e$.

הגדרה 5.3. תהי (G, \cdot, e) חבורה ויהא איבר $g \in G$. הסדר של איבר הוא המספר הטבעי n הקטן ביותר כך שמתקיים $g^n = e$. אם אין n כזה, אומרים שהסדר של g הוא אינסוף. בפרט, בכל חבורה הסדר של איבר היחידה הוא 1, וזהו האיבר היחיד מסדר 1. סימון מקובל $o(g) = n$ ולפעמים $|g|$.

דוגמה 5.4. בחבורה $(\mathbb{Z}_6, +)$, $o(2) = o(4) = 3$, $o(3) = 2$, $o(1) = o(5) = 6$.

דוגמה 5.5. נסתכל על החבורה (U_{10}, \cdot) . נזכור כי $U_{10} = \{1, 3, 7, 9\}$ (כי אלו המספרים הזרים ל-10 וקטנים ממנו). נחשב את $o(7)$:

$$\begin{aligned} 7^2 &= 49 \equiv 9 \pmod{10} \\ 7^3 &= 7 \cdot 7^2 \equiv 7 \cdot 9 = 63 \equiv 3 \pmod{10} \\ 7^4 &= 7 \cdot 7^3 = 7 \cdot 3 = 21 \equiv 1 \pmod{10} \end{aligned}$$

ולכן $o(7) = 4$.

דוגמה 5.6. נסתכל על $(GL_2(\mathbb{R}), \cdot)$ - חבורת המטריצות ההפיכות מגודל 2×2 מעל \mathbb{R} . נחשב את הסדר של $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$:

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

לכן $o(b) = 3$.

תרגיל 5.7. תהי G חבורה. הוכיחו שלכל $a \in G$, $o(a) = o(a^{-1})$.

הוכחה. נחלק לשני מקרים:

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

$$e = e^n = (a^{-1}a)^n \stackrel{*}{=} (a^{-1})^n a^n = (a^{-1})^n e = (a^{-1})^n$$

כאשר המעבר $*$ מבוסס על כך ש- a ו- a^{-1} מתחלפים (באופן כללי, $(ab)^n \neq a^n b^n$). הוכחנו ש- $(a^{-1})^n = e$, ולכן $o(a^{-1}) \leq n = o(a)$. כעת, צריך להוכיח את אי-השוויון השני. אם נחליף את a ב- a^{-1} , נקבל $o(a) = o((a^{-1})^{-1}) < o(a^{-1})$. 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 $o(a) = o(a^{-1}) < \infty$.

□

6 חבורות ציקליות

6.1 הגדרה תהי G חבורה, ויהי $a \in G$. תת־החבורה הנוצרת על ידי a היא תת־החבורה

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

6.2 דוגמה עבור $n \in \mathbb{Z}$, $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\} = \langle n \rangle$.

6.3 הגדרה תהי G חבורה ויהי איבר $a \in G$. אם $G = \langle a \rangle$, אזי נאמר כי G נוצרת על ידי a ונקרא ל- G חבורה ציקלית (מעגלית).

6.4 דוגמה החבורה $(\mathbb{Z}, +)$ נוצרת על ידי 1, שכן כל מספר ניתן להצגה ככפולה (כחזקה) של 1. שימו לב כי יוצר של חבורה ציקלית לא חייב להיות יחיד, למשל גם -1 יוצר את \mathbb{Z} .

6.5 דוגמה החבורה $(\mathbb{Z}_n, +) = \langle 1 \rangle$ היא ציקלית. וודאו כי בחבורה $(\mathbb{Z}_2, +)$ יש רק יוצר אחד (נניח על ידי טבלת כפל). וודאו כי בחבורה $(\mathbb{Z}_{10}, +)$ יש ארבעה יוצרים. שניים די ברורים (1 וגם $-1 \equiv 9$), האחרים (3, 7) דורשים לבניתיים בדיקה ידנית.

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

6.7 טענה שימו לב כי הסדר של יוצר בחבורה ציקלית הוא סדר החבורה. כלומר אנחנו יודעים כי $5 \in (\mathbb{Z}_{10}, +)$ אינו יוצר כי הסדר שלו הוא $|\mathbb{Z}_{10}| = 10 > 2 = |5|$, שהרי $5 + 5 \equiv 0 \pmod{10}$.

6.8 טענה כל חבורה ציקלית היא אבלית.

הוכחה. תהי G חבורה ציקלית, ונניח כי $G = \langle a \rangle$. יהיו $g_1, g_2 \in G$. צ"ל $g_1 g_2 = g_2 g_1$. ציקלית, ולכן קיימים i, j שעבורם $g_1 = a^i$ ו- $g_2 = a^j$. מכאן שמתקיים

$$g_1 g_2 = a^i a^j = a^{i+j} = a^{j+i} = a^j a^i = g_2 g_1$$

□

6.9 דוגמה לא כל חבורה אבלית היא ציקלית. למשל, נסתכל על $U_8 = \{1, 3, 5, 7\}$. זו לא חבורה ציקלית, כי אין בחבורה הזו איבר מסדר 4 (כל האיברים שאינם 1 הם מסדר 2 - בדקו).

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

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

זו תת־חבורה של \mathbb{C}^* . יותר מכך: אם נסמן $\omega_n = \operatorname{cis} \frac{2\pi}{n}$, נקבל $\Omega_n = \langle \omega_n \rangle$, כלומר Ω_n היא חבורה ציקלית.

טענה 6.11. הוכיחו: אם G ציקלית, אז כל תת־חבורה של G היא ציקלית.

הוכחה. תהי $H \leq G$ תת־חבורה. נסמן $G = \langle a \rangle$. כל האיברים ב- G הם מהצורה a^i , ולכן גם כל האיברים ב- H הם מהצורה הזו. יהי $s \in \mathbb{N}$ המספר המינימלי שעבורו $a^s \in H$. נרצה להוכיח $H = \langle a^s \rangle$. אכן, יהי $k \in \mathbb{N}$ שעבורו $a^k \in H$. לפי משפט החילוק עם שארית, קיימים q ו- r שעבורם $0 \leq r < s, k = qs + r$, לכן,

$$a^k = a^{qs+r} = a^{qs} \cdot a^r = (a^s)^q \cdot a^r$$

במילים אחרות, $a^r = a^k \cdot (a^s)^{-q}$. אבל $a^s, a^k \in H$ ולכן גם $a^r \in H$ (סגירות לכפל ולהופכי).

אם $r \neq 0$, קיבלנו סתירה למינימליות של s - כי $a^r \in H$ וגם $0 < r < s$ (לפי בחירת r). לכן, $r = 0$. כלומר, $k = qs$, ומכאן $s | k$. לכן $a^k \in \langle a^s \rangle$, כדרוש. \square

מסקנה 6.12. תת־החבורות של $(\mathbb{Z}, +)$ הן בדיוק $(n\mathbb{Z}, +)$ עבור $n \in \mathbb{N} \cup \{0\}$.

טענה 6.13 (מההרצאה). תהי G חבורה, ויהי $a \in G$. אם $a^n = e$, אזי $o(a) | n$.

תרגיל 6.14. תהי G חבורה, ויהי $a \in G$. נניח $o(a) = n < \infty$. הוכיחו שלכל $d \leq n$ טבעי,

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

הוכחה. היתכנות: נשים לב כי

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

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

מינימליות: נניח $(a^d)^t = e$, כלומר $a^{dt} = e$. לפי טענה 6.13, $n | dt$. לכן, גם $\frac{n}{(d, n)} | \frac{dt}{(d, n)}$ (שניהם מספרים שלמים - מדוע?). מצד שני, $\left(\frac{n}{(d, n)}, \frac{d}{(d, n)} \right) = 1$.

לפי תרגיל שהוכחנו בתרגול הראשון, $\frac{n}{(d, n)} | t$, כמו שרצינו. \square

תרגיל 6.15 (אם יש זמן). נגדיר $\Omega_\infty = \bigcup_{n=1}^{\infty} \Omega_n$. הוכיחו:

1. Ω_∞ היא תת־חבורה של \mathbb{C}^* .

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

3. Ω_∞ אינה ציקלית.

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

פתרון.

1. ניעזר בקריטריון המקוצר. יהיו $g_1, g_2 \in \Omega_\infty$. לכן קיימים m, n שעבורם $g_1 \in \Omega_m, \Omega_n$. נכתוב

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

לכן

$$\begin{aligned} g_1 g_2^{-1} &= \text{cis} \frac{2\pi k}{m} \left(\text{cis} \frac{2\pi \ell}{n} \right)^{-1} = \text{cis} \frac{2\pi k}{m} \text{cis} \left(-\frac{2\pi \ell}{n} \right) = \text{cis} \left(\frac{2\pi k}{m} - \frac{2\pi \ell}{n} \right) = \\ &= \text{cis} \left(\frac{2\pi (kn - \ell m)}{mn} \right) \in \Omega_{mn} \subseteq \Omega_\infty \end{aligned}$$

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

3. נניח בשלילה $\Omega_\infty = \langle a \rangle$; לכן בהכרח $|\Omega_\infty| = \aleph_0$. אבל זה סותר את תוצאת סעיף ב'.

תרגיל 6.16 (אם יש זמן). תהי G חבורה ציקלית מסדר n . כמה איברים ב- G יוצרים את G ?

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

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

לכן, מספר האיברים היוצרים את G הוא $|U_n|$.

7 מכפלה קרטזית של חבורות

הגדרה 7.1. תהיינה $(G, *)$ ו- (H, \bullet) חבורות. נזכר ממתמטיקה בדידה כי

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

נגדיר פעולה על $G \times H$ רכיב-רכיב, כלומר:

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

סענה 7.2. $(G \times H, \odot)$ היא חבורה.

למשל, האיבר הניטרלי ב- $G \times H$ הוא (e_G, e_H) .

דוגמה 7.3. נסתכל על $U_8 \times \mathbb{Z}_3$. נדגים את הפעולה:

$$\begin{aligned}(3, 2) \odot (5, 2) &= (3 \cdot 5, 2 + 2) = (15, 4) = (7, 1) \\ (5, 1) \odot (7, 2) &= (5 \cdot 7, 1 + 2) = (35, 3) = (3, 0)\end{aligned}$$

האיבר הניטרלי הוא $(1, 0)$.

תרגיל 7.4. האם $\mathbb{Z}_n \times \mathbb{Z}_n$ ציקלית (עבור $n \geq 2$)?

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

$$(a, b)^n = (a, b) \odot (a, b) \odot \dots \odot (a, b) = (a + a + \dots + a, b + b + \dots + b) = (na, nb) = (0, 0)$$

כיוון שהסדר הוא המספר המינימלי m שעבורו $(a, b)^m = (0, 0)$, בהכרח $m \leq n$. כלומר, הסדר של כל איבר ב- $\mathbb{Z}_n \times \mathbb{Z}_n$ הוא לכל היותר n . כעת, נסיק כי החבורה הזו אינה ציקלית: כזכור מבדידה, $|\mathbb{Z}_n \times \mathbb{Z}_n| = n^2$. אילו החבורה $\mathbb{Z}_n \times \mathbb{Z}_n$ הייתה ציקלית, היה בה איבר מסדר n^2 ; אך אין כזה, ולכן החבורה אינה ציקלית.

הערה 7.5. התרגיל הקודם אומר שמכפלה של חבורות ציקליות אינה בהכרח ציקלית. לעומת זאת, מכפלה של חבורות אבליות תישאר אבלית (תוכיחו בבית).

הערה 7.6. מעכשיו, במקום לסמן את הפעולה של $G \times H$ ב- \odot , נסמן אותה ב- \cdot בשביל הנוחות.

8 החבורה הסימטרית (על קצה המזלג)

הגדרה 8.1. החבורה הסימטרית S_n היא

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

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

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

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

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

נכתוב במפורש את האיברים ב- S_3 :

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

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

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

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

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

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

נשים לב ש- S_3 אינה אבלית, כי $\sigma\tau \neq \tau\sigma$.

הערה 8.4. נשים לב כי $|S_n| = n!$. אכן, מספר האפשרויות לבחור את $\sigma(1)$ הוא n ; אחר כך, מספר האפשרויות לבחור את $\sigma(2)$ הוא $n-1$; כך ממשיכים, עד שמספר האפשרויות לבחור את $\sigma(n)$ הוא 1 - האיבר האחרון שלא בחרנו. בסך הכל, $|S_n| = n \cdot (n-1) \cdot \dots \cdot 1 = n!$

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

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

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

הערה 8.8. שימו לב שמחזורים זרים מתחלפים זה עם זה (מדוע?), ולכן חישובים עם מחזורים יהיו לעיתים קלים יותר מאשר חישובים עם התמורה עצמה.

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

$$1 \mapsto 4 \mapsto 1$$

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

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

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

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

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

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

תרגיל 8.10. יהי $\sigma \in S_n$ מחזור מאורך k . מהו σ^k ?

פתרון. נסמן $\sigma = (a_1\ a_2\ \dots\ a_k)$ בנוכח כי $\sigma^k = \text{id}$. ראשית, ברור כי $\sigma^k = \text{id}$: לכל a_i מתקיים

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

ולכל $m \neq a_i$, $\sigma^k(m) = m$ (כי $\sigma(m) = m$).

נותר להוכיח מינימליות; אבל אם $\ell < k$, אפשר להשתכנע כי $\sigma^\ell(a_1) = a_{\ell+1} \neq a_1$, כלומר $\sigma^\ell \neq \text{id}$.

9 מחלקות

הגדרה 9.1. תהי G חבורה, ותהי $H \leq G$ תת-חבורה. לכל $g \in G$, נגדיר:

• $gH = \{gh | h \in H\} \subseteq G$ - מחלקה שמאלית

• $Hg = \{hg | h \in H\}$ - מחלקה ימנית

את אוסף המחלקות השמאליות נסמן G/H .

דוגמה 9.2. ניקח את $G = S_3$, ונסתכל על תת-החבורה

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

המחלקות השמאליות של H ב- G :

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

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

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

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

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

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

לכן

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

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

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

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

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

דוגמה 9.4. ניקח את $G = (\mathbb{Z}_8, +)$, ונסתכל על $H = \langle 2 \rangle = \{0, 2, 4, 6\}$. המחלקות השמאליות הן

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

ובאופן כללי,

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

נשים לב ש: $G = H \cup 1 + H$.

הערה 9.5. כפי שניתן לראות מהדוגמאות שהצגנו, המחלקות השמאליות (או הימניות) של H יוצרות חלוקה של G . נוסף על כך, יחס השוויון בין המחלקות הנוצרות ע"י שני איברים ב G הינו יחס שקילות.

כלומר עבור $a, b \in G$ ותת-חבורה $H \leq G$, יחס השוויון $aH = bH$ הינו יחס שקילות בין a ו b .

נסכם זאת בעזרת המשפט הבא:

משפט 9.6. תהי G חבורה, ותהי $H \leq G$ תת-חבורה. אזי

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

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

$$3. \quad \text{מתקיים } |aH| = |bH| = |H|.$$

$$4. \quad \text{האיחוד של כל המחלקות הוא כל } G; \bigcup_{g \in G} gH = G, \text{ וזהו איחוד זר.}$$

הוכחה. נוכיח את 1:

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

הערה 9.7. קיימת התאמה חח"ע ועל בין המחלקות השמאליות $\{gH : g \in G\}$ לימניות $\{Hg : g \in G\}$.
 $(Hg \mapsto g^{-1}H)$, $\{Hg : g \in G\}$
 $gH \mapsto (gH)^{-1} = \{(gh)^{-1} : h \in H\} = \{h^{-1}g^{-1} : h \in H\} = \{kg^{-1} : k \in H\} = Hg^{-1}$
 לכן מס' המחלקות השמאליות = מספר המחלקות הימניות.

הגדרה 9.8. נסמן את מספר המחלקות של H ב- G בסימון $[G : H]$. מספר זה נקרא האינדקס של H ב- G .

דוגמה 9.9. על פי הדוגמאות שראינו:

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

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

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

תרגיל 9.10. מצאו חבורה G ותת-חבורה $H \leq G$, כך ש- $[G : H] = \infty$.

פתרון. תהי $G = (\mathbb{Q}, +)$ ותת-חבורה $H = \mathbb{Z}$.
 ניקח שני שברים שונים מ \mathbb{Q} בין 0 ל 1: α_1, α_2 , ונתבונן במחלקות שאיברים אלו יוצרים. נקבל ש:
 $\{\alpha_1, \pm 1 + \alpha_1, \pm 2 + \alpha_1, \dots\} = \alpha_1 H \neq \alpha_2 H = \{\alpha_2, \pm 1 + \alpha_2, \pm 2 + \alpha_2, \dots\}$
 ולכן,
 מספר המחלקות של H ב- G הוא לפחות כמספר המספרים ב \mathbb{Q} בין 0 ל 1 שווה ∞ .

משפט 9.11 (לגרנז'). תהי G חבורה, ותהי $H \leq G$ תת-חבורה. אז $|G| = [G : H] \cdot |H|$.

מסקנה 9.12. עבור חבורה סופית, הסדר של תת-חבורה מחלק את הסדר של החבורה:

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

בפרט, עבור $a \in G$, $|a| = |G| \cdot |a|^{-1}$ כי $|\langle a \rangle| \leq G$. לכן הסדר של כל איבר בחבורה מחלק את הסדר של החבורה. במילים אחרות, לכל $a \in G$ מתקיים $a^{|G|} = e$.

דוגמה 9.13. עבור $|\mathbb{Z}_{10}| = 10$, הסדרים האפשריים של איברים ב \mathbb{Z}_{10} הם מהקבוצה $\{1, 2, 5, 10\}$.

תרגיל 9.14. האם לכל מספר m המחלק את סדר החבורה הסופית G בהכרח קיים איבר מסדר m ?

פתרון. לא בהכרח! דוגמה נגדית: נבחן את החבורה $\mathbb{Z}_4 \times \mathbb{Z}_4$. סדר החבורה הינו 16 אבל לא קיים איבר מסדר 16. אילו היה קיים איבר כזה, אזי זו חבורה ציקלית, אבל הוכחנו שהחבורה $\mathbb{Z}_n \times \mathbb{Z}_n$ אינה ציקלית עבור $n > 1$.

משפט 9.15 (משפט אוילר). פונקציית אוילר $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ פוגדרת לפי $\varphi(n) = |U_n|$. עבור $a \in U_n$, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

דוגמה 9.16. $(3, 10) = 1$, לכן $3 \in U_{10}$. מאחר ש- $U_{10} = \{1, 3, 7, 9\}$, אזי $\varphi(10) = |U_{10}| = 4$.
 אך מתקיים: $3^{\varphi(10)} = 3^4 = 81 \equiv 1 \pmod{10}$.

משפט 9.17. המשפט הקטן של פרמה (כמקרה פרטי של משפט אוילר): עבור p ראשוני מתקיים $|U_p| = p - 1$, לכן לכל $a \in U_p$ מתקיים ש $a^{p-1} \equiv 1 \pmod{p}$.

תרגיל 9.18. חשב את שתי הספרות האחרונות של המספר 909^{121} .

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

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

דוגמה 9.19. תהי G חבורה מסדר p ראשוני. יהי $e \neq g \in G$. לכן $|g| > 1$. מצד שני $|g| \mid |G| = p$, לכן בהכרח $|g| = p$, מה שאומר ש: $G = \langle g \rangle$. מאחר וזה נכון לכל $e \neq g \in G$, נסיק ש- G נוצרת ע"י כל אחד מאיבריה שאינו היחידה.

טענה 9.20. תהי $G = \langle x \rangle$ חבורה ציקלית מסדר n ויהי $y = x^d$ כאשר $d > 0$, אזי $|y| = \frac{n}{(d,n)}$ (ראה תרגיל 6.14 עבור ההוכחה).

דוגמה 9.21. $(\mathbb{Z}_{12}, +)$, חבורה ציקלית מסדר 12 הנוצרת ע"י $x = 1$. אם ניקח $y = x^8 = 8$, אזי נקבל: $\frac{12}{(8,12)} = \frac{12}{4} = 3$. מצד שני, על מנת לחשב את הסדר של y , נבדוק מהי תת-החבורה הנוצרת ע"י y :
 $\langle 8 \rangle = \{0, 8, 4\} \leq (\mathbb{Z}_{12}, +)$
 ואכן $|y| = |8| = |\langle 8 \rangle| = 3$.

מסקנה 9.22. בסימונים שלעיל, אם $(n, d) = 1$ אזי $\frac{n}{1} = n$. כלומר $|y| = \frac{n}{(d,n)} = \frac{n}{1} = n$.
 $G = \langle y \rangle$

מכאן נסיק שבחבורה ציקלית, כל איבר שחזקתו זהה למספר איברי החבורה - יוצר את החבורה.

לכן מספר היוצרים בחבורה ציקלית מסדר n הוא כמספר המספרים השלמים הזרים ל- n . כלומר מספר היוצרים הוא בדיוק $\varphi(n)$ (פונקציית אוילר).

טענה 9.23. תהי $G = \langle \alpha \rangle$ ציקלית מסדר n ויהי $m|n$. אזי ל G יש תת-חבורה ציקלית יחידה מסדר m .

הוכחה. נסמן $H = \langle \alpha^{n/m} \rangle$. זוהי תת-חבורה מסדר m . תהי K תת-חבורה ציקלית נוספת מסדר m : אז $K = \langle \beta \rangle$. נרצה להוכיח ש: $K = H$.

מאחר ש α יוצר של G , קיים $b \in \mathbb{Z}$ כך ש: $\beta = \alpha^b$, לכן על פי הטענה הקודמת, $|\beta| = \frac{n}{(n,b)}$.

אבל $|\beta| = m \Leftrightarrow \frac{n}{(n,b)} = m \Leftrightarrow (n,b) = \frac{n}{m} \Leftrightarrow m|n$. לפי תכונת ה gcd קיימים $s, t \in \mathbb{Z}$ כך ש $(n,b) = sn + tb$. לכן:

$\alpha^{n/m} = \alpha^{(n,b)} = \alpha^{sn+tb} = (\alpha^n)^s (\alpha^b)^t = 1 \cdot \beta^t \in K$
 $\alpha^{n/m} \in K$, לכן $H \subseteq K$, אבל על פי ההנחה $|H| = |K|$, לכן $H = K$, כדרוש. \square

תרגיל 9.24. כמה תת-חבורות לא טריוויאליות יש ב- \mathbb{Z}_{30} ? (לא טריוויאלית פירושו לא כולל את $\{0\}$ ואת \mathbb{Z}_{30})

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

10 חישוב פונקציית אוילר

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

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

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

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

ולכן, עבור מספר שלם כלשהו:

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

ולסיכום

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

דוגמה 10.1. נחשב את $\varphi(60)$:

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

תרגיל 10.2. חשבו את שתי הספרות האחרונות של $80732767^{1999} + 2013$.

פתרון. נפעיל mod100 ונקבל

$$\begin{aligned}80732767^{1999} + 2013 &\equiv 67^{1999} + 13 = 67^{50 \cdot 40 - 1} + 13 = (67^{40})^{50} \cdot 67^{-1} + 13 \\ &= (67^{\varphi(100)})^{50} \cdot 67^{-1} + 13 \equiv (1)^{50} \cdot 67^{-1} + 13 = 67^{-1} + 13\end{aligned}$$

כעת נותר למצוא את ההופכי של 67 בחבורה U_{100} . (67 זר ל-100 ולכן נמצא ב- U_{100})

לצורך כך, נשתמש באלגוריתם של אוקלידס לצורך מציאת פתרון למשוואה $67x = 1 \pmod{100}$.

יש פתרון למשוואה אם $k \in \mathbb{Z}$ כך ש $100k + 67x = 1$.
נבעזרת אלגוריתם אוקלידס נמצא ביטוי של $\gcd(100, 67)$ כצירוף לינארי של 67 ו-100.

$$(100, 67) = [100 = 1 \cdot 67 + 33]$$

$$(67, 33) = [67 = 2 \cdot 33 + 1]$$

$$(33, 1) = 1$$

ומהצבה לאחור נקבל: $1 = 67 - 2 \cdot 33 = -2 \cdot 100 + 3 \cdot 67$, ולכן $x = 3$, כלומר ההופכי של 67 הוא 3.

לכן $67^{-1} + 13 = 3 + 13 = 16$. כלומר שתי הספרות האחרונות הם 16.

תרגיל 10.3. הוכיחו את הטענה הבאה: תהא G חבורה סופית, אזי G מסדר זוגי \Leftrightarrow קיים ב G איבר מסדר 2.
 (\Rightarrow) : על פי משפט לגרנז', הסדר של איבר מחלק את סדר החבורה ולכן סדר החבורה זוגי.
 (\Leftarrow) : לאיבר מסדר 2 תכונה יחודית - הוא הופכי לעצמו. נניח בשלילה שאין אף איבר ב G מסדר שני, כלומר שאין אף איבר שהופכי לעצמו (למעט איבר היחידה כמובן).
אזי, ניתן לסדר את כל איברי החבורה - זוגות זוגות, כאשר כל איבר מזווג לאיבר ההופכי לו. ביחד עם איבר היחידה נקבל מספר אי זוגי של איברים ב G בסתירה להנחה.

מסקנה 10.4. לחבורה מסדר זוגי יש מספר אי זוגי של איברים מסדר 2.

11 תת-חבורה הנוצרת על ידי איברים

הגדרה 11.1. תהי G חבורה ותהי $A \subseteq G$ תת-קבוצה לא ריקה איברים ב G (שימו לב ש A אינה בהכרח תת-חבורה של G).
תת-חבורה נוצרת ע"י A הינה תת-החבורה המינימלית המכילה את A ונסמנה $\langle A \rangle$.

אם $G = \langle A \rangle$ אז נאמר ש G נוצרת ע"י A .
עבור קבוצה סופית של איברים, נכתוב $\langle x_1, \dots, x_k \rangle$.
נשים לב שעבור קבוצה סופית של יוצרים, הגדרה זו מהווה הכללה לכתיבה של חבורה ציקלית הנוצרת ע"י איבר אחד.

דוגמה 11.2. אם ניקח $\{2, 3\} \subseteq \mathbb{Z}$ אז $\langle 2, 3 \rangle = H$. נוכיח ש- $H = \mathbb{Z}$.
 H תת-חבורה של \mathbb{Z} ובפרט $H \subseteq \mathbb{Z}$. נראה שגם $\mathbb{Z} \subseteq H$, ומזה נסיק שוויון.
כיוון ש- $2 \in H$ אזי גם $-2 \in H$ ומכאן ש- $1 = (-2) + 3 \in H$. כלומר איבר היחידה שהוא כידוע היוצר של כל \mathbb{Z} , מוכל ב H .
לכן נקבל: $1 \in H \Rightarrow \mathbb{Z} = \langle 1 \rangle \subseteq H$. כלומר $\mathbb{Z} \subseteq H$, ומכאן נובע השוויון $H = \mathbb{Z}$.

דוגמה 11.3. אם ניקח $\{4, 6\} \subseteq \mathbb{Z}$ אזי נקבל: $\langle 4, 6 \rangle = \{4n + 6m : m, n \in \mathbb{Z}\}$.
נטען ש- $2\mathbb{Z} = \gcd(4, 6) \cdot \mathbb{Z} = \langle 4, 6 \rangle$ (כלומר תת-חבורה של השלמים המכילה רק את המספרים הזוגיים).
נוכיח ע"י 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 11.4. במקרה שהחבורה אבלית, קל יותר לתאר את תת-החבורה הנוצרת. למשל אם ניקח שני יוצרים $a, b \in G$ נקבל: $\langle a, b \rangle = \{a^i b^j : i, j \in \mathbb{Z}\}$.

כלומר בזכות החילופיות, ניתן לסדר את כל ה- a -ים יחד וכל ה- b -ים יחד. נדגים לאיבר הנוצר על ידי a ו- b : $abaaab^{-1}bbba^{-1} = a^3b^3$. באופן כללי, בחבורה אבלית מתקיים:

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

דוגמה 11.5. נוח לעיתים לחשוב על איברי $\langle A \rangle$ בתור קבוצת מילים שניתן לכתוב באמצעות האותיות בקבוצה (היוצרים ב A). נסביר: נגדיר את הא"ב שלנו להיות $A \cup A^{-1}$ כאשר $A^{-1} = \{a^{-1} : a \in A\}$. כעת, מילה היא סדרה סופית של אותיות מה-א"ב. המילה הריקה מייצגת כאן את איבר היחידה ב G .

12 החבורה הדיהדרלית

נציג חבורה חשובה נוספת שמקורה גאומטרי: החבורה הדיהדרלית.

הגדרה 12.1. עבור מספר טבעי n , הקבוצה D_n של סיבובים ושיקופים המעתיקים מצולע משוכלל בין n צלעות על עצמו, היא החבורה הדיהדרלית, יחד עם פעולת ההרכבה. אם σ הוא סיבוב ב $\frac{2\pi}{n}$ ו- τ הוא שיקוף סביב ציר סימטריה כלשהו, אז:

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

צורת תיאור זו נקראת תיאור חבורה על ידי יוצרים ויחסים.

דוגמה 12.2. החבורה D_3 כוללת איברים המייצגים את כל הקומבינציות של סיבוב של 120° , המסומן באות σ , ושיקוף המסומן באות τ , על משולש שווה צלעות.

$$D_3 = \langle \sigma, \tau : \sigma^3 = \tau^2 = \text{id}, \sigma\tau = \tau\sigma^2 \rangle$$

כעת נתאר במפורש את כל איברי D_3

$$D_3 = \{\text{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$$

הערה 12.3. שימו לב שאמנם האיבר $\sigma\tau$ לא מופיע בתאור ששת האיברים אך על פי היחס שהוגדר $\sigma\tau = \tau\sigma^2$, לכן האיבר נמצא בחבורה, אך מתואר בכתיבה שונה.

הערה 12.4. בהמשך להערה הקודמת, נשים לב ש $\sigma\tau$ ו $\tau\sigma$ הם שני איברים שונים זה מזה (גזור משולש שווה צלעות, סמן את קודקודיו, ואז: פעם אחת שקף את המשולש ואח"כ סובב, ובפעם השניה סובב ואח"כ שקף ותיווכח שהמצב הסופי שבו מונח המושלש שונה בשני המקרים).

כלומר: החבורה D_3 אינה אבלית, ובאופן כללי, כל D_n אינה אבלית עבור $n \geq 3$.

הערה 12.5. סדר החבורה D_3 הינו 6. לכל n , הסדר של D_n הינו $2n$.

13 נושאים נוספים בחבורה הסימטרית

13.1 סדר של איברים בחבורה הסימטרית

נחזור לחקור את החבורה הסימטרית S_n .

הערה 13.1. תזכורת: עבור מחזור σ מאורך k מתקיים: $o(\sigma) = k$.

טענה 13.2. (מופיעה כתרגיל בית בדף עבודה מס' 5)

תהי G חבורה. יהי $a, b \in G$ כך ש $ab = ba$ וגם $\langle a \rangle \cap \langle b \rangle = e$ (כלומר החיתוך בין תת-החבורה הציקלית הנוצרת ע"י a ותת-החבורה הציקלית הנוצרת ע"י b היא טריוויאלית). אז

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

מסקנה 13.3. סדר מכפלות מחזורים זרים ב S_n הוא ה lcm (הכפ"ט) של סדרי המחזורים.

דוגמה 13.4. הסדר של $(56)(123)$ הוא 6 והסדר של $(56)(1234)$ הוא 4.

תרגיל 13.5. 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 $o(\sigma) = [9, 5] = 45$

כעת, מכיוון שסדר האיבר שווה לסדר תת-החבורה שאיבר זה יוצר, נסיק שתת-החבורה $\langle \sigma \rangle$ עונה על הדרוש.

שאלה 13.6. האם קיים איבר מסדר 39 ב- S_{15} ?

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

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

13.2 הצגת מחזור כמכפלת חילופים

הגדרה 13.7. מחזור מסדר 2 ב- S_n נקרא חילוף.

טענה 13.8. כל מחזור (a_1, a_2, \dots, a_r) ניתן לרשום כמכפלת חילופים

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

לכן:

$$S_n = \langle (i, j) : 1 \leq i, j \leq n \rangle$$

תרגיל 13.9. 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, נסביר:

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

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

תרגיל 13.10. מה הם הסדרים האפשריים לאיברי S_4 ?

פתרון. ב- S_4 הסדרים האפשריים הם:

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

תרגיל 13.11. מה הם הסדרים האפשריים לאיברי S_5 ?

1. סדר 1 - רק איבר היחידה.
2. סדר 2 - חילופים (i, j) או מכפלה של שני חילופים זרים.
3. סדר 3 - מחזורים מאורך 3.
4. סדר 4 - מחזורים מאורך 4.
5. סדר 5 - מחזורים מאורך 5.
6. סדר 6 - מכפלה של חילוף ומחזור מאורך 3, למשל (54) (231).

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

13.3 סימן של תמורה וחבורת החילופין (חבורת התמורות הזוגיות)

הגדרה 13.12. יהי σ מחזור מאורך k , אזי הסימן שלו הוא:

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

ועבור התמורות $\tau, \sigma \in S_n$ מתקיים:

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

תכונה זו מאפשרת לחשב את הסימן של כל תמורה ב- S_n . נקרא לתמורה שסימנה 1 בשם תמורה זוגית ולתמורה שסימנה 0 בשם תמורה אי זוגית.

דוגמה 13.13. (נקודה חשובה ומאוד מבלבלת)

1. החילוף (35) הוא תמורה אי זוגית.
2. התמורה הריקה היא תמורה זוגית.
3. מחזור מאורך אי זוגי הוא תמורה זוגית.

הגדרה 13.14. חבורת החילופין (חבורת התמורות הזוגיות) היא תת-החבורה הבאה של S_n :

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

הערה 13.15. הסדר של A_n הינו $\frac{n!}{2}$.

הגדרה 13.16. $A_3 = \{\text{id}, (123), (132)\}$. נשים לב כי $A_3 = \langle (123) \rangle$ כלומר A_3 ציקלית.

14 שימוש בתורת החבורות: אלגוריתם RSA

נראה דוגמה להרצה של אלגוריתם RSA (על שם רוני ריבסט, עדי שמיר ולאונרד אדלמן) הנלקחה מויקיפדיה. אלגוריתם RSA מממש שיטה להצפנה אסימטרית המובססת על רעיון המפתח הפומבי.

המטרה: בוב מעוניין לשלוח לאליס הודעה באופן מוצפן.

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

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

הצפנה: בוב ישלח הודעה M לאליס בצורת מספר m המקיים $0 \leq m < n$ וגם $\gcd(n, m) = 1$. כלומר יש רק $\varphi(n) + 1$ סוגי הודעות שונות שבווב יכול לשלוח. הוא ישלח את ההודעה המוצפנת $c \equiv m^e \pmod{n}$.

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

דוגמה 14.1. נציג דוגמה עם מספרים קטנים מאוד. אליס תבחר למשל את $p = 61$ ואת $q = 53$ היא תחשב

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

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

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

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

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

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

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

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

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

$$m^1 \equiv m \cdot 1 \equiv 65 \pmod{3233}$$

$$m^2 \equiv (m)^2 \equiv 992 \pmod{3233}$$

$$m^4 \equiv (m^2)^2 \equiv 1232 \pmod{3233}$$

$$m^8 \equiv (m^4)^2 \equiv 1547 \pmod{3233}$$

$$m^{16} \equiv (m^8)^2 \equiv 789 \pmod{3233}$$

$$m^{17} \equiv m (m^8)^2 \equiv 2790 \pmod{3233}$$

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

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

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

הערה 14.2 (אזהרה!). יש לדעת שלא כדאי להשתמש לצרכים חשובים בפונקציות קריפטוגרפיות שמימשתם לבד. ללא בחינה מדוקדקת על ידי מומחים בתחום לגבי רמת בטיחות ונכונות הקוד, ישנן התקפות רבות שאפשר לנצל לגבי מימושים שכאלו, כגון בחירת מפתחות לא ראויה. בנוסף יש התקפות לגבי הפרוטוקול בו משתמשים כגון התקפת אדם באמצע והתקפת ערוץ צדדי.

15 הומומורפיזמים

הגדרה 15.1. תהינה $(G, *)$, (H, \bullet) חבורות. העתקה $f : G \rightarrow H$ תקרא הומומורפיזם של חבורות אם מתקיים

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

נכין מילון קצר לסוגים שונים של הומומורפיזמים:

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

הערה 15.2. העתקה $f : G \rightarrow H$ היא איזומורפיזם אם ורק אם קיימת העתקה $g : H \rightarrow G$ כך ש- $f \circ g = \text{id}_H$ וגם $g \circ f = \text{id}_G$. אפשר להוכיח (נסו!) שההעתקה g הזו היא הומומורפיזם בעצמה. כלומר כדי להוכיח שהומומורפיזם f הוא איזומורפיזם מספיק למצוא העתקה הפוכה $g = f^{-1}$. אפשר גם לראות שאיזומורפיזם הוא יחס שקילות.

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

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

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

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

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

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

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

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

1. $f(e_G) = e_H$

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

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

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

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

6. אם $G \cong H$, אז $|G| = |H|$.

תרגיל 15.4. יהי $f : G \rightarrow H$ הומומורפיזם. הוכיחו כי לכל $g \in G$ מסדר סופי מתקיים $o(f(g)) \mid o(g)$.

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

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

ולכן $o(f(g)) \mid n$. □

תרגיל 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 $f: G \rightarrow H$, 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 $f: G \rightarrow H$ הומומורפיזם. הוכיחו שאם G אבלית, אז $\text{im } f$ אבלית. הסיקו שאם $G \cong H$, אז G אבלית אם ורק אם H אבלית.

תרגיל 15.7. יהי $f: G \rightarrow H$ הומומורפיזם. הוכיחו שאם G ציקלית, אז $\text{im } f$ ציקלית.

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

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

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

תרגיל 15.8. האם קיים איזומורפיזם $f: S_3 \rightarrow \mathbb{Z}_6$?

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

תרגיל 15.9. האם קיים איזומורפיזם $f: (\mathbb{Q}^+, \cdot) \rightarrow (\mathbb{Q}, +)$?

פתרון. לא. נניח בשלילה כי 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 15.10. האם קיים אפימורפיזם $f: H \rightarrow \mathbb{Z}_3 \times \mathbb{Z}_3$ כאשר $H = \langle 5 \rangle \leq \mathbb{R}^*$?

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

תרגיל 15.11. האם קיים מונומורפיזם $f: GL_2(\mathbb{Q}) \rightarrow \mathbb{Q}^{10}$?

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

מסקנה. יתכנו ארבע הפרכות ברצף.

תרגיל 15.12. מתי ההעתקה $i : G \rightarrow G$ המוגדרת לפי $i(g) = g^{-1}$ היא אוטומורפיזם?

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

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

וזה יתקיים אם ורק אם $gh = hg$. כלומר i היא אוטומורפיזם אם ורק אם G 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 $H \triangleleft G$.

משפט 16.2. תהי תת-חבורה $H \leq G$. התנאים הבאים שקולים:

1. $H \triangleleft G$

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

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

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

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

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

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

דוגמה 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!

דוגמה 16.4. מתקיים $SL_n(F) \triangleleft GL_n(F)$. אפשר לראות זאת לפי הצמדה. יהי $A \in SL_n(F)$, אז לכל $g \in GL_n(F)$ מתקיים

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

ולכן $g^{-1}Ag \in SL_n(F)$. דרך אחרת להוכחה היא לשים לב כי $SL_n(F)$ היא הגרעין של ההומומורפיזם \det .

אתגר: הוכיחו בעזרת דוגמה זו כי $A_n \triangleleft S_n$.

דוגמה 16.5. $\langle \tau \rangle \leq D_3$ אינה נורמלית כי $\sigma \langle \tau \rangle \neq \langle \tau \rangle \sigma$.

16.6. סענה. $H \leq G$ תת-חבורה מאינדקס 2. אזי $H \triangleleft G$.

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

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

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

מסקנה 16.7. מתקיים $\langle \sigma \rangle \triangleleft D_n$ כי לפי משפט לגראנז' $2 \mid \frac{2n}{n} = [D_n : \langle \sigma \rangle]$.

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

תרגיל 16.9. תהי G חבורה. יהיו $H, N \leq G$ תת-חבורות. נגדיר מכפלה של תת-חבורות להיות

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

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

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

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

$$HNHN = HHNN = HN$$

$$h_1n_1h_2n_2 = h_1h_2n_1n_2 = h_3n_3$$

וסגירות להופכי

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

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

ולכן $HN \leq G$.

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

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

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

דוגמה 16.10. הגדרנו בתרגיל בית את המִרְפָּז 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 . שימו לב שתמיד $Z(G) \triangleleft G$ וכי $Z(G)$ אבלי. האם תת-חבורה נורמלית היא בהכרח אבלי? כבר ראינו שלא, למשל עבור $GL_2(\mathbb{R}) \triangleleft SL_2(\mathbb{R})$.

17 חבורות מנה

נתבונן באוסף המחלקות השמאליות $G/H = \{gH : g \in G\}$. אם (ורק אם) $H \triangleleft G$ אפשר להגדיר על אוסף זה את הפעולה הבאה שיחד איתה נקבל חבורה:

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

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

דוגמה 17.1. \mathbb{Z} היא חבורה ציקלית, ובפרט אבלי. ברור כי $n\mathbb{Z} \triangleleft \mathbb{Z}$. נשים לב כי

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

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

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

אפשר לראות כי $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ לפי ההעתקה $k + n\mathbb{Z} \mapsto k \pmod{n}$.

דוגמה 17.2. לכל חבורה G יש שתי תת-חבורות טריוויאליות $\{e\}$ ו- G , ושתיהן נורמליות. ברור כי $[G : G] = 1$, ולכן $G/G \cong \{e\}$. דרך אחרת לראות זאת היא לפי ההומומורפיזם הטריוויאלי $f : G \rightarrow G$ המוגדר לפי $f : g \mapsto e$. ברור כי $\ker f = G$.

מה לגבי $G/\{e\}$? האיברים הם מן הצורה $g\{e\} = \{g\}$. העתקת הזהות $\text{id} : G \rightarrow G$ היא איזומורפיזם, שהגרעין שלו הוא $\{e\}$. אפשר גם לבנות איזומורפיזם $f : G/\{e\} \rightarrow G$ לפי $f : g\{e\} \mapsto g$. ודאו שאתם מבינים למה זה אכן איזומורפיזם.

דוגמה 17.3. תהי $G = \mathbb{R} \times \mathbb{R}$, ונתבונן ב- G $H = \mathbb{R} \times \{0\}$. האיברים בחבורת המנה הם

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

כלומר אלו הם הישרים המקבילים לציר ה- x .

הערה 17.4. עבור חבורה סופית G ותת-חבורה $H \triangleleft G$ מתקיים כי

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

תרגיל 17.5. תהי G חבורה (לאו דווקא סופית), ותהי $H \triangleleft G$ כך ש- $[G : H] = n < \infty$. הוכיחו כי לכל $a \in G$ מתקיים כי $a^n \in H$.

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

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

כלומר קיבלנו $a^n \in H$.

תרגיל 17.6. תהי $H \leq G$ תת-חבורה מאינדקס 2. הוכיחו כי G/H היא חבורה אבלית.

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

תרגיל 17.7. תהי G חבורה, ויהי T אוסף האיברים מסדר סופי ב- G . בתרגיל בית הראתם שאם G אבלית, אז $T \leq G$. הוכיחו:

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

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

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

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

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

עבור הסעיף השני, נניח בשלילה כי קיים איבר $xT \in G/T$ ש- $e_{G/T} \neq xT$ 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 $G \triangleleft G$, ואז $G/T \cong \{e\}$. אם $G = \mathbb{C}^*$, אז $T = \Omega_\infty = \bigcup_n \Omega_n$. כלומר כל מספר מרוכב לא אפסי עם ערך מוחלט השונה מ-1 הוא מסדר אינסופי.

18 משפטי האיזומורפיזם של נתר

משפט 18.1 (משפט האיזומורפיזם הראשון). יהי הומומורפיזם $f : G \rightarrow H$. אז

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

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

תרגיל 18.2. יהי הומומורפיזם $f : \mathbb{Z}_{14} \rightarrow D_{10}$. מה יכול להיות $\ker f$?

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

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

ושוב מפני ש-7 אינו מחלק את 20 נסיק כי $|K| \neq 2$.
 אם $|K| = 7$, נראה כי קיים הומומורפיזם כזה. ניקח תת-חבורה $H = \{\text{id}, \tau\}$ (כל תת-חבורה מסדר 2 תתאים) של D_{10} , ונבנה אפימורפיזם $\mathbb{Z}_{14} \rightarrow H \leq D_{10}$.
 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.