מבנים אלגבריים למדעי המחשב
מערכי תרגול קורס 89-214

נובמבר 2016, גרסה 0.24

אוניברסיטת בר־אילן

סמסטר א׳ תשע״ז

תוכן העניינים

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 הגשה לתרגילי הבית.
- החומר בקובץ זה נאסף מכמה מקורות, ומבוסס בעיקרו על מערכי תרגול קודמים בקורסים מבנים אלגבריים למדעי המחשב ואלגברה מופשטת למתמטיקה.
- נשמח לכל הערה על מסמך זה.

מחברים בשנת הלימודים תשע"ו: אבי אלון, תומר באואר וגיא בלשר
מחברים בשנת הלימודים תשע"ז: תומר באואר, עמרי מרכוס ואלעד עטייא

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).
- $\mathbb{Q}=\left\{\frac{p}{q}:p\in\mathbb{Z},q\in\mathbb{Z}\backslash\{0\}\right\}$ 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-$b=ka$, ונסמן $a|b$. למשל $-5|10$.

משפט 1.2 (משפט החילוק, או חלוקה אוקלידית)**.** לכל $n\in\mathbb{Z}$,$d\neq0$ 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 המירבי (ממ"מ, greatest common divisor) שלהם מוגדר להיות המספר

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

לעיתים נסמן רק (n, m). למשל $2 = (6, 10)$. 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 $d \leq (m, r)$. 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 ממ"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 $0 \leq r < m$ ונמשיך עם $(n, m) = (m, r)$. (הבינו למה 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

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

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

דוגמה 1.9. כדי למצוא את המקדמים s,t כשמביעים את הממ"מ כצירוף לינארי כנ"ל נשתמש באלגוריתם אוקלידס המוכלל:

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

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

תרגיל 1.10. 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 $a|\left(sac+tbc\right)$, כלומר $a|c$.

טענה 1.11. תכונות של ממ"מ:

1. יהי $d=(n,m)$ ויהי e כך ש-$e|m$ וגם $e|n$, אזי $e|d$.
2. $(an,am)=|a|\left(n,m\right)$
3. אם p ראשוני וגם $p|ab$, אזי $p|a$ או $p|b$.

הוכחת התכונות.
1. קיימים s,t כך ש-$d=sn+tm$. כיוון ש-$e|n,m$, אז הוא מחלק גם את צירוף לינארי שלהם $sn+tm$, ז"א את d.
2. (חלק מתרגיל הבית.)
3. אם $p\nmid a$, אז $(p,a)=1$. לכן קיימים s,t כך ש-$sa+tp=1$. נכפיל את השיוויון האחרון ב-b ונקבל $sab+tpb=b$. ברור כי p מחלק את אגף שמאל (הרי $p|ab$), ולכן p מחלק את אגף ימין, כלומר $p|b$.

$\square$

הגדרה 1.12. בהנתן שני מספרים שלמים n,m הכפולה המשותפת המזערית (כמ"מ, least common multiple) שלהם מוגדרת להיות

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

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

טענה 1.13. תכונות של כמ"מ:

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

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

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 $r\neq 0$ זו 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

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

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

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

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

□

שאלה 1.14 (לבית)**.** אפשר להגדיר ממ"מ ליותר מזוג מספרים. יהי d הממ"מ של המספרים $n_1,\dots,n_k$. הראו שקיימים מספרים שלמים $s_1,\dots,s_k$ המקיימים $s_1n_1+\dots+s_kn_k=d$. רמז: אינדוקציה על k.

הגדרה 1.15. יהי n מספר טבעי. נאמר כי $a,b\in\mathbb{Z}$ הם שקולים בשארית חלוקה ב-n אם $n|a-b$. כלומר קיים $k\in\mathbb{Z}$ כך ש-$a=b+kn$. נסמן יחס זה $a\equiv b \pmod n$ ונקרא זאת "a שקול ל-b מודולו n".

טענה 1.16 (הוכחה לבית). שקילות מודולו n היא יחס שקילות (רפלקסיבי, סימטרי וטרנזיטיבי). כפל וחיבור מודולו n מוגדרים היטב. כלומר אם $a\equiv b, c\equiv d \pmod n$, אז $ac\equiv bd \pmod n$ וגם $a+c\equiv b+d \pmod n$.

צורת רישום 1.17. את אוסף מחלקות השקילות מודולו n מקובל לסמן $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}=\{[a]:a\in\mathbb{Z}\}$. למשל $\mathbb{Z}_4=\{[0],[1],[2],[3]\}$. לפעמים מסמנים את מחלקת השקילות $[a]$ בסימון $\overline{a}$, ולעיתים כאשר ההקשר ברור פשוט a.

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 $333^{333}=3^{333}\cdot 111^{333}$. לכן

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

ומכאן שהספרה האחרונה היא 3.

תרגיל 1.19 (אם יש זמן)**.** מצאו $0 \leq x \in \mathbb{Z}$ כך ש-$61x \equiv 1 \pmod{234}$.

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

משפט 1.20 (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 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

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

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

הוכחת היחידות של x מודולו nm תהיה בתרגיל הבית. $\square$

דוגמה 1.21. נמצא $x \in \mathbb{Z}$ כך ש-$x \equiv 1 \pmod{3}$ וגם $x \equiv 2 \pmod{5}$. ידוע כי $(5, 3) = 1$, ולכן $-1 \cdot 5 + 2 \cdot 3 = 1$. במקרה זה $n = 5, m = 3$ וכן $s = -1, t = 2$, ולפי משפט השאריות הסיני אפשר לבחור את $x = 1 \cdot (-5) + 2 \cdot 6 = 7$. אכן מתקיים $7 \equiv 1 \pmod{3}$ וגם $7 \equiv 2 \pmod{5}$.

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

משפט 1.22 (אם יש זמן)**.** תהא $\{m_1, \ldots, m_k\}$ קבוצת מספרים טבעיים הזרים בזוגות (כלומר כל זוג מספרים בקבוצה הוא זר). נסמן את מכפלתם ב-m. בהנתן קבוצה כלשהי של שאריות $\{a_i \,(\mathrm{mod} m_i) : 1 \leq i \leq k\}$, 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 1.23. נמצא $y \in \mathbb{Z}$ כך ש-ש-$y \equiv 1 \pmod{3}$, $y \equiv 2 \pmod{5}$ וגם $y \equiv 3 \pmod{7}$. נשים לב שהפתרון $y = 7$ מן הדוגמה הקודמת הוא נכון כדי כדי הוספה של $15 = 3 \cdot 5$ (כי $15 \equiv 0 \pmod{3}$ וגם $15 \equiv 0 \pmod{5}$). לכן את שתי המשוואות $y \equiv 1 \pmod{3}$, $y \equiv 2 \pmod{5}$ ניתן להחליף במשוואה אחת $y \equiv 7 \pmod{15}$. נשים לב כי $(15, 7) = 1$ ולכן אפשר להשתמש במשפט השאריות הסיני בגרסה לזוג משוואות. בדקו כי $y = 52$ מהווה פתרון.

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 $* : S \times S \to S$. 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 (אסוציטיביות, 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 יקרה 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 הימיניים 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. בכתיב 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 הטריוויאלית.

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

דוגמה 2.20. 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 $X^X = \{f : X \to X\}$. 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 $X = \{1, \ldots, n\}$ 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 שלם. נסמן את הכפולות שלו ב-$n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}$. למשל $4\mathbb{Z} = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$.

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 $\mathbb{Z}_n = \{[0], [1], \ldots, [n - 1]\}$. 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 $[2]\,[3]=[6]=[0]$. 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 $[0]$):

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

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

הערה 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־החבורה הטריוויאלית), ו-$G\leq G$.

דוגמה 4.3. לכל $n \in \mathbb{Z}$, $n\mathbb{Z} \leq \mathbb{Z}$. בהמשך נוכיח שאלו כל תת־החבורות 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

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

הוכיחו כי $SL_n(F) \leq GL_n(F)$ היא תת־חבורה. קוראים לה החבורה הליניארית 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,

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

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 $\mathrm{Ord}(G)$.

צורת רישום 5.2. בחבורה כפלית נסמן את החזקה החיובית $a^n = aa\ldots a$ לכפל n פעמים. בחבורה חיבורית נסמן $na = a + \cdots + a$. 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 $(\mathbb{Z}_6,+)$, $o\left(2\right)=o\left(4\right)=3$, $o\left(3\right)=2$, $o\left(1\right)=o\left(5\right)=6$.

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 $o\left(7\right)$:

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

ולכן $o\left(7\right)=4$.

דוגמה 5.6. נסתכל על $\left(GL_2\left(\mathbb{R}\right),\cdot\right)$ – 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 $o\left(b\right)=3$.

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

הוכחה. נחלק לשני מקרים:

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

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

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

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

□

6 חבורות ציקליות

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

$$\langle a\rangle = \left\{a^k \middle| k \in \mathbb{Z}\right\}$$

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

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

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

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

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

טענה 6.7. 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 $|5| = 2 < 10 = |\mathbb{Z}_{10}|$, שהרי $5 + 5 \equiv 0 \pmod{10}$.

טענה 6.8. 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 $g_1g_2 = g_2g_1$. G ציקלית, ולכן קיימים i, j שעבורם $g_1 = a^i$ ו-$g_2 = a^j$. מכאן שמתקיים

$$g_1g_2 = a^ia^j = a^{i+j} = a^{j+i} = a^ja^i = g_2g_1$$

□

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

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

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

זו תת־חבורה של $\mathbb{C}^*$. 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 $k = qs + r$, $0 \leq r < s$. לכן,

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

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

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

מסקנה 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,

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

הוכחה. <u>היתכנות</u>: נשים לב כי

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

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

<u>מינימליות</u>: נניח $\left(a^d\right)^t = e$, כלומר $a^{dt} = e$. לפי טענה 6.13, $n|dt$. 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 $g_1 \in \Omega_m$, $g_2 \in \Omega_n$. נכתוב
$$g_1 = \text{cis}\frac{2\pi k}{m}, \qquad g_2 = \text{cis}\frac{2\pi \ell}{n}$$
לכן
$$\begin{aligned} g_1 g_2^{-1} &= \text{cis}\frac{2\pi k}{m}\left(\text{cis}\frac{2\pi\ell}{n}\right)^{-1} = \text{cis}\frac{2\pi k}{m}\text{cis}\left(-\frac{2\pi\ell}{n}\right) = \text{cis}\left(\frac{2\pi k}{m} - \frac{2\pi\ell}{n}\right) \\ &= \text{cis}\left(\frac{2\pi\left(kn - \ell m\right)}{mn}\right) \in \Omega_{mn} \subseteq \Omega_\infty \end{aligned}$$

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

3. נניח בשלילה $\Omega_\infty = \langle a \rangle$; לכן בהכרח $o\left(a\right) = \left|\Omega_\infty\right| = \aleph_0$. 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
$$G = \left\langle a^k \right\rangle \iff o\left(a^k\right) = n \iff \frac{n}{\left(k, n\right)} = n \iff \left(k, n\right) = 1$$
לכן, מספר האיברים היוצרים את G הוא $\left|U_n\right|$.

7 מכפלה קרטזית של חבורות

הגדרה 7.1. תהיינה $\left(G, *\right)$ ו-$\left(H, \bullet\right)$ חבורות. ניזכר ממתמטיקה בדידה כי
$$G \times H = \left\{\left(g, h\right) | g \in G, h \in H\right\}$$
נגדיר פעולה על $G \times H$ רכיב-רכיב, כלומר:
$$\left(g_1, h_1\right) \odot \left(g_2, h_2\right) = \left(g_1 * g_2, h_1 \bullet h_2\right)$$

טענה 7.2. $\left(G \times H, \odot\right)$ היא חבורה.

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

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

$$(3,2) \odot (5,2) = (3 \cdot 5, 2+2) = (15,4) = (7,1)$$
$$(5,1) \odot (7,2) = (5 \cdot 7, 1+2) = (35,3) = (3,0)$$

האיבר הניטרלי הוא $(1,0)$.

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,

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

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

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

הערה 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 $\cdot$ בשביל הנוחות.

8 החבורה הסימטרית (על קצה המזלג)

הגדרה 8.1. החבורה הסימטרית מדרגה n היא

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

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

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

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

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

נכתוב במפורש את האיברים ב-S_3:

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

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

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

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

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

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

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, $|S_n| = n \cdot (n-1) \cdot \dots \cdot 1 = n!$.

הגדרה 8.5. 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 $(a_1\ a_2\ \dots\ a_k)$. האורך של המחזור $(a_1\ a_2\ \dots\ a_k)$ הוא k.

דוגמה 8.6. 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 8.7. *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.

דוגמה 8.9. 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 $o(\sigma)$?

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

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

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

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

9 מחלקות

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

- מחלקה שמאלית – $gH = \{gh | h \in H\} \subseteq G$.
- מחלקה ימנית – $Hg = \{hg | h \in H\}$.

את אוסף המחלקות השמאליות נסמן G/H.

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

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

המחלקות השמאליות של H ב-G:

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

לכן

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

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

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

ובאופן כללי,

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

נשים לב ש: $G=H\bigcup 1+H$.

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 $H\le G$, יחס השוויון $aH=bH$ הינו יחס שקילות בין a ו b.

נסכם זאת בעזרת המשפט הבא:

משפט 9.6. תהי G חבורה, ותהי $H\le G$ תת־חבורה. $a,b\in G$ אזי

1. $aH=bH$ אם ורק אם: $b^{-1}a\in H$, בפרט $aH=H \iff a\in H$
2. לכל שתי מחלקות g_1H ו-g_2H, מתקיים $g_1H=g_2H$ או $g_1H\cap g_2H=\varnothing$.
3. מתקיים $|aH|=|bH|=|H|$.
4. האיחוד של כל המחלקות הוא כל G; $\bigcup\limits_{g\in G} gH=G$, 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 $a = bh_0 \in H$,

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 $b = ah_o^{-1}$, 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 $\{Hg : g \in G\}$, $(Hg \mapsto g^{-1}H)$.

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

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-

$\{\alpha_1,\, \pm1+\alpha_1,\, \pm2+\alpha_1, \dots\} = \alpha_1H \neq \alpha_2H = \{\alpha_2,\, \pm1+\alpha_2,\, \pm2+\alpha_2, \dots\}$

ולכן, מספר המחלקות של H ב-G הוא לפחות ככמות המספרים ב-$\mathbb{Q}$ בין 0 ל-1 שהיא אינסופית.

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 $a \in G$, $|a| = |\langle a\rangle|$ ו-$|G|\,|\,|\langle a\rangle|$ 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 $\varphi : \mathbb{N} \to \mathbb{N}$ מוגדרת לפי $\varphi(n) = |U_n|$.
עבור $a \in U_n$, $a^{\varphi(n)} = 1 \pmod n$.

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

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 $|a| \mid (p-1)$, ובפרט $a^{p-1} = 1 \pmod p$.

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

פתרון. נזכר ש $\bmod n$ 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: $9^{\varphi(100)} = 9^{40} = 1 \pmod{100}$.
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 : $\frac{n}{(d,n)} = \frac{12}{(8,12)} = \frac{12}{4} = 3$.
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 $n=\frac{n}{1}=\frac{n}{(d,n)}=|y|$. כלומר $G=\langle y\rangle$.

מכאן נסיק שבחבורה ציקלית , כל איבר שחזקתו זרה 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 $H=\left\langle\alpha^{n/m}\right\rangle$. זוהי תת־חבורה מסדר m. תהי K תת־חבורה ציקלית נוספת מסדר m, ונניח $K=\langle\beta\rangle$. 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 $m=|\beta|\Leftarrow m=\frac{n}{(n,b)}$. לכן $(n,b)=\frac{n}{m}$. לפי תכונת הממ"מ קיימים $s,t\in\mathbb{Z}$ כך ש $(n,b)=sn+tb$. לכן

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

כלומר קיבלנו ש-$\alpha^{n/m}\in K$, 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, מספר תת־החבורות הוא כמספר המחלקים של המספר 30, כלומר: $8=|\{1,2,3,5,6,10,15,30\}|$.

מאחר והסדרים 1 ו-30 מתאימים לתת־החבורות הטרוויאליות, נותרנו עם שש תת־חבורות לא טריוויאליות.

10 חישוב פונקציית אוילר

לצורך פתרון התרגיל הבא נפתח נוסחה נוחה לחישוב $\varphi\left(n\right)$, 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

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

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

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

ולכן, עבור מספר שלם כלשהו:

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

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 $\mathrm{mod}100$ ונקבל

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

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

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

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

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

לכן $67^{-1} + 13 = 3 + 13 = 16$. 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־החבורה 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 על ידי איבר אחד.

דוגמה 11.2. ניקח $\{2,3\} \subseteq \mathbb{Z}$ ואת $H = \langle 2,3\rangle$. 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-$(-2) + 3 = 1 \in H$. 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-$\langle 4,6\rangle = \gcd(4,6) \cdot \mathbb{Z} = 2\mathbb{Z}$ (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 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:

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

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:

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

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 120^0, המסומן באות σ, ושיקוף המסומן באות τ, על משולש שווה צלעות.

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

כעת נתאר במפורש את כל איברי D_3:

$$D_3=\left\{\mathrm{id},\sigma,\sigma^2,\tau,\tau\sigma,\tau\sigma^2\right\}$$

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

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

מסקנה 13.3. סדר מכפלות מחזורים זרים ב-S_n הוא הכמ"מ (lcm) של סדרי המחזורים.

דוגמה 13.4. הסדר של $(123)(56)$ 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 $(a_1, a_2, \ldots, a_r)$ 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:

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

תרגיל 13.9. כמה מחזורים מאורך $2 \le r \le n$ 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:

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

לכן נחלק את המספר הכולל ב-r 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:

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

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

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

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) A_n היא תת־החבורה הבאה של S_n:

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

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

הגדרה 13.16. $A_3 = \{\mathrm{id}, (123), (132)\}$.
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 רון 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 $65537 = 2^{16+1}$ או מספר די קטן אחר). היא מוצאת הופכי כפלי d של e בחבורה $U_{\varphi(n)}$ שיהווה את המפתח הסודי שלה. כלומר היא מוצאת מספר המקיים $de \equiv 1 \pmod{\varphi(n)}$, למשל על ידי אלגוריתם אוקלידס המורחב. זהו שלב שאין צורך לחזור עליו.

הפצת המפתח 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 שבוב 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

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

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 שבבסיס בינארי $17 = 10001_2$, ולכן במקום $17 - 1 = 16$ הכפלות מודלוריות נסתפק בחישוב:

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

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

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

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 מודלוריות 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 $f:G\to H$ תקרא הומומורפיזם של חבורות אם מתקיים

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

נכין מילון קצר לסוגים שונים של הומומורפיזמים:

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

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

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

1. $\varphi:\mathbb{R}\to\mathbb{R}^*$ המוגדרת לפי $x\mapsto e^x$ היא מונומורפיזם. מה היה קורה אם היינו מחליפים למרוכבים?
2. יהי F שדה. אז $\det:GL_n(F)\to F^*$ היא אפימורפיזם. הרי
$$\det(AB)=\det(A)\det(B)$$
וכדי להוכיח שההעתקה על אפשר להסתכל על מטריצה אלכסונית עם ערכים $(x,1,\dots,1)$ באלכסון.
3. $\varphi:\mathbb{R}\to\mathbb{R}^*$ המוגדרת לפי $x\mapsto x$ אינה הומומורפיזם כלל.
4. $\varphi:\mathbb{Z}_2\to\Omega_2$ המוגדרת לפי $0\mapsto 1$, $1\mapsto -1$ היא איזומורפיזם. הראתם בתרגיל בית שכל החבורות מסדר 2 הן למעשה איזומורפיות.

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

1. $f(e_G) = e_H$.
2. $f(g^n) = f(g)^n$ לכל $n \in \mathbb{Z}$.
3. $f(g^{-1}) = f(g)^{-1}$, כמקרה פרטי של הסעיף הקודם.
4. הגרעין של f, כלומר $\ker f = \{g \in G : f(g) = e_H\}$, הוא תת־חבורה נורמלית של G (בהמשך נסביר מה זה "תת־חבורה נורמלית").
5. התמונה של f, כלומר $\operatorname{im} f = \{f(g) : g \in G\}$, היא תת־חבורה של H.
6. אם $G \cong H$, אז $|G| = |H|$.

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

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

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

ולכן $o(f(g))|n$. $\square$

תרגיל 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 $f : G \to H$, 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 $f : G \to H$ 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 $f : G \to H$ 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 $f(a)$. הסיקו שכל החבורות הציקליות מסדר מסוים הן איזומורפיות. $\square$

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

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

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

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

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

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

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

מסקנה. יתכנו ארבע הפרכות ברצף.

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

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

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

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

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

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

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

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

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

טענה 16.6. 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 $aH = Ha$. $\square$

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

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

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

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

הוכיחו כי אם $N\lhd G$, אז $HN\le G$. אם בנוסף $H\lhd G$, אז $HN\lhd G$.

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

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

$$HNHN=HHNN=HN$$
$$h_1n_1h_2n_2=h_1h_2'n_1'n_2=h_3n_3$$

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 $HN\le G$.

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

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

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

דוגמה 16.10. הגדרנו בתרגיל בית את הַמֶּרְכָּז 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 $Z(G)\lhd G$ וכי $Z(G)$ אבלית. האם תת־חבורה נורמלית היא בהכרח אבלית? כבר ראינו שלא, למשל עבור $SL_2(\mathbb{R})\lhd GL_2(\mathbb{R})$.

17 חבורות מנה

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

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

כאשר בשיוויונות 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 אבלית. ברור כי $n\mathbb{Z} \lhd \mathbb{Z}$. נשים לב כי

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

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 $f : G \to G$ המוגדר לפי $g \mapsto e$. ברור כי $\ker f = G$.

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

דוגמה 17.3. תהי $G = \mathbb{R} \times \mathbb{R}$, ונתבונן ב-$H = \mathbb{R} \times \{0\} \lhd G$. 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 $H \lhd G$ מתקיים כי

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

תרגיל 17.5. 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 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 $H \lhd G$. 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 $T \lhd G$.
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

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

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 $T = \Omega_\infty = \bigcup_n \Omega_n$. 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 $f : G \to H$. אז

$$G/_{\ker f} \cong \operatorname{im} f$$

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

תרגיל 18.2. תהי $G = \mathbb{R} \times \mathbb{R}$, ותהי $H = \{(x, y) \in \mathbb{R} \times \mathbb{R} | y = 3x\}$. הוכיחו כי $G/_H \cong \mathbb{R}$.

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

f אפימורפיזם, כי $f\left(\frac{x}{3}, 0\right) = x$. כמו כן,

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

לפי משפט האיזומורפיזם הראשון, נקבל את הדרוש. □

תרגיל 18.3. נסמן $\mathbb{T} = \{z \in \mathbb{C} || z| = 1\}$. זו חבורה כפלית. הוכיחו כי $\mathbb{R}/_{\mathbb{Z}} \cong \mathbb{T}$.

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

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

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

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

לפי משפט האיזומורפיזם הראשון, נקבל

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

$\square$

תרגיל 18.4. יהי הומומורפיזם $f : \mathbb{Z}_{14} \to D_{10}$. מה יכול להיות $\ker f$?

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

אם $|K| = 1$, אז f הוא חח"ע וממשפט האיזומורפיזם הראשון נקבל $\operatorname{im} f \cong \mathbb{Z}_{14}/K$. 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 18.5. תהיינה G_1 ו-G_2 חבורות סופיות כך ש-$(|G_1|, |G_2|) = 1$. מצאו את כל ההומומורפיזמים $f : G_1 \to G_2$.

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

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

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 היא ההומומורפיזם הטריוויאלי.

תרגיל 18.6. מצאו את כל התמונות האפימורפיות של D_4 (עד כדי איזומורפיזם).

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

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

כעת, אנו יודעים כי $Z\left(D_4\right)=\left\langle\sigma^2\right\rangle \lhd D_4$. ננסה להבין מיהי ${}^{D_4}\!/\!\left\langle\sigma^2\right\rangle$. רעיון לניחוש: אנחנו יודעים, לפי לגראנז', כי זו חבורה מסדר 4. כמו כן, אפשר לבדוק שכל איבר $x\in {}^{D_4}\!/\!\left\langle\sigma^2\right\rangle$ מקיים $x^2=e$. לכן ננחש שזו $\mathbb{Z}_2\times\mathbb{Z}_2$ (ובהמשך נדע להגיד זאת בלי למצוא איזומורפיזם ממש). נגדיר $f:D_4\to\mathbb{Z}_2\times\mathbb{Z}_2$ לפי $f\left(\tau^i\sigma^j\right)=(i,j)$. קל לבדוק שזהו אפימורפיזם עם גרעין $\left\langle\sigma^2\right\rangle$, ולכן, לפי משפט האיזומורפיזם הראשון,

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

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 $\left\langle\sigma^2,\tau\right\rangle,\left\langle\sigma^2,\tau\sigma\right\rangle\lhd D_4$ מאותו נימוק, וכן

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

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 $\left\langle\sigma^2\right\rangle$. תת־החבורות היחידות שעוד לא הזכרנו הן מהצורה $\left\langle\tau\sigma^i\right\rangle=\left\{\mathrm{id},\tau\sigma^i\right\}$. 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 $H\not\lhd D_4$. מכאן שכתבנו את כל תת־החבורות הנורמליות של D_4, ולכן כל התמונות האפימורפיות של D_4 הן $\{\mathrm{id}\},\mathbb{Z}_2,\mathbb{Z}_2\times\mathbb{Z}_2,D_4$.

תרגיל 18.7. תהי G חבורה. הוכיחו: אם ${}^{G}\!/\!{}_{Z(G)}$ היא ציקלית, אזי 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

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

(לפי הציקליות). אם כן, מתקיים

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

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

$$g\in a^iZ\left(G\right),h\in a^jZ\left(G\right)$$

כלומר קיימים $g',h'\in Z\left(G\right)$ שעבורם $g=a^ig'$ ו-$h=a^jh'$. לכן,

$$gh=a^ig'a^jh'=a^ia^jg'h'=a^ja^ih'g'=a^jh'a^ig'=hg$$

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

מסקנה 18.8. במבט לאחור, כיוון ש-G אבלית, מתקיים $Z\left(G\right)=G$, ומכאן ש-$G/Z(G)=\{e\}$. כלומר, אם $G/Z(G)$ ציקלית, אזי היא טריוויאלית.

הגדרה 18.9. תהי G חבורה, ויהי $a\in G$. אוטומורפיזם ההצמדה ב-a הוא האוטומורפיזם $\gamma_a:G\to G$ המוגדר על ידי $\gamma_a\left(g\right)=aga^{-1}$. נסמן

$$\operatorname{Inn}\left(G\right)=\left\{\gamma_a|a\in G\right\}$$

החבורה הזו נקראת חבורת האוטומורפיזמים הפנימיים של G.

תרגיל 18.10. הוכיחו כי $\gamma_a\circ\gamma_b=\gamma_{ab}$, וכי $\gamma_a^{-1}=\gamma_{a^{-1}}$. הסיקו כי $\operatorname{Inn}\left(G\right)$ היא חבורה עם פעולת ההרכבה.

הוכחה. לכל $g\in G$ מתקיים

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

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

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

$\square$

תרגיל 18.11. הוכיחו כי לכל חבורה G,

$$G/Z(G)\cong\operatorname{Inn}\left(G\right)$$

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

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

לפי משפט האיזומורפיזם הראשון, נקבל

$$G/Z(G)\cong\operatorname{Inn}\left(G\right)$$

$\square$

19 הצמדות

הגדרה 19.1. תהי G חבורה. אומרים שאיברים g ו-h צמודים, אם קיים $a \in G$ שעבורו $h = aga^{-1}$. זה מגדיר יחס שקילות על G, שבו מחלקת השקילות של כל איבר נקראת מחלקת הצמידות שלו.

דוגמה 19.2. בחבורה אבלית G, אין שני איברים שונים הצמודים זה לזה; נניח כי g ו-h צמודים. לכן, קיים $a \in G$ שעבורו

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

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

תרגיל 19.3. תהי G חבורה, ויהי $g \in G$ מסדר סופי n. הוכיחו:

1. אם $h \in G$ צמוד ל-g, אזי $o(h) = n$.
2. אם אין עוד איברים ב-G מסדר n, אזי $g \in Z(G)$.

הוכחה.

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

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

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

$$g^m = \left(a^{-1}ha\right)^m = a^{-1}h^ma = e$$

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

2. 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 $g \in Z(G)$.

□

הערה 19.4. הכיוון ההפוך בכל סעיף אינו נכון - למשל, אפשר לקחת את $\mathbb{Z}_4$. $o(1) = o(3) = 4$, אבל הם לא צמודים; כמו כן, שניהם במרכז, ולכל אחד מהם יש איבר אחר מאותו סדר.

דוגמה 19.5. בחבורה D_3, האיבר σ צמוד לאיבר

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

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

תרגיל 19.6. תהי $\sigma \in S_n$, ויהי מחזור $(a_1, a_2, \ldots, a_k) \in S_n$. הוכיחו כי

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

הוכחה. נראה שהתמורות האלו פועלות באותו אופן על $\{1, 2, \ldots, n\}$. ראשית, נניח כי $m = \sigma (a_i)$ עבור איזשהו $1 \le i \le k$. התמורה באגף ימין תשלח את m ל-$\sigma (a_{i+1})$. נסתכל מה קורה באגף שמאל:

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

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

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

מכאן ששתי התמורות הדרושות שוות. □

תרגיל 19.7. נתונות ב-S_6 התמורות $a = (1,5,3,6)$, $\sigma = (1,3)(4,5,6)$ ו-$\tau = (2,4,5)$. חשבו את:

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

פתרון. לפי הנוסחה הנ"ל,

$$\begin{aligned}\sigma a \sigma^{-1} &= (3,6,1,4) \\ \tau a \tau^{-1} &= (1,2,3,6)\end{aligned}$$

מסקנה 19.8 (לבית). $S_n = \langle (1,2), (1,2,\ldots,n) \rangle$.

הגדרה 19.9. תהי $\sigma \in S_n$ תמורה. נפרק אותה למכפלה של מחזורים זרים $\sigma = \sigma_1 \sigma_2 \ldots \sigma_k$. נניח כי האורך של σ_i הוא r_i, וכי $r_1 \ge r_2 \ge \cdots \ge r_k$. נגדיר את מבנה המחזורים של σ להיות ה-k-יה הסדורה $(r_1, r_2, \ldots, r_k)$.

דוגמה 19.10. מבנה המחזורים של $(1,2,3)(5,6)$ הוא $(3,2)$; מבנה המחזורים של $(4,2,3)(1,5)$ גם הוא $(3,2)$; מבנה המחזורים של $(1,2,3,4)(5,6)(7,8)$ הוא $(4,2,2)$.

מסקנה 19.11. שתי תמורות צמודות ב-S_n אם ורק אם יש להן אותו מבנה מחזורים. למשל, התמורה $(1,2,3)(5,6)$ צמודה ל-$(4,2,3)(1,5)$ ב-S_8, אבל הן לא צמודות לתמורה $(1,2,3,4)(5,6)(7,8)$ ב-S_8.

הוכחה. (אם יש זמן; אם אין זמן - לעבור רק על הרעיון)
$\boxed{\Leftarrow}$ תהיינה $\sigma,\tau\in S_n$ שתי תמורות צמודות ב-S_n. נכתוב $\tau=\pi\sigma\pi^{-1}$. נניח כי $\sigma=\sigma_1\sigma_2\dots\sigma_k$ הפירוק של σ למכפלה של מחזורים זרים; לכן

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

לפי התרגיל הקודם, כל תמורה מהצורה $\pi\sigma_i\pi^{-1}$ היא מחזור; כמו כן, קל לבדוק כי כל שני מחזורים שונים כאלו זרים זה לזה (כי $\sigma_1,\sigma_2,\dots,\sigma_k$ זרים זה לזה). לכן, קיבלנו פירוק של τ למכפלה של מחזורים זרים, וכל אחד מהמחזורים האלו הוא מאותו האורך של המחזורים ב-σ. מכאן נובע של-σ ול-τ אותו מבנה מחזורים.
$\boxed{\Rightarrow}$ תהיינה $\sigma,\tau\in S_n$ עם אותו מבנה מחזורים. נסמן $\sigma=\sigma_1\sigma_2\dots\sigma_k$, $\tau=\tau_1\tau_2\dots\tau_k$, כאשר $\sigma_i=(a_{i,1},a_{i,2},\dots,a_{i,m_i})$ ו-$\tau_i=(b_{i,1},b_{i,2},\dots,b_{i,m_i})$, $\sigma_1,\sigma_2,\dots,\sigma_k$ הם מחזורים זרים וגם $\tau_1,\dots,\tau_k$ הם מחזורים זרים. נגדיר תמורה π כך: $\pi(a_{i,j})=b_{i,j}$, וכל שאר האיברים נשלחים לעצמם. נשים לב כי

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

ולכן

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

מכאן ש-σ ו-τ צמודות ב-S_n. $\square$

מסקנה 19.12. הוכיחו כי $Z(S_n)=\{\mathrm{id}\}$ לכל $n\geq 3$.

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

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

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

הגדרה 19.13. חלוקה של n היא סדרה לא עולה של מספרים טבעיים $n_1\geq\dots\geq n_k>0$ כך ש-$n=n_1+\dots+n_k$. את מספר החלוקות של n מסמנים $\rho(n)$.

מסקנה 19.14. מספר מחלקות הצמידות ב-S_n הוא $\rho(n)$.

תרגיל 19.15. כמה מחלקות צמידות יש ב-S_5?

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

$$5 = 5$$
$$5 = 4 + 1$$
$$5 = 3 + 2$$
$$5 = 3 + 1 + 1$$
$$5 = 2 + 2 + 1$$
$$5 = 2 + 1 + 1 + 1$$
$$5 = 1 + 1 + 1 + 1 + 1$$

ולכן $\rho(5) = 7$.

תרגיל 19.16. יהיו $\sigma, \tau \in A_n$, ונניח של-σ ול-τ אותו מבנה מחזורים. האם σ ו-τ צמודות ב-A_n?

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

הגדרה 19.17 (מתרגילי הבית)**.** תהי G חבורה. עבור איבר $a \in G$ נגדיר את הִמְרַכֵּז של a להיות

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

תרגיל 19.18. מצאו את $C_{S_5}(\sigma)$ עבור $\sigma = (1,2,5)$.

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

1. תמורות שזרות ל-σ - יש רק אחת כזו, והיא $(3,4)$.
2. תמורות שמזיזות את σ במעגל - id, $(1,2,5)$ ו-$(1,5,2)$.

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

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

20 חבורות אבליות סופיות

טענה 20.1. תהי G חבורה אבלית מסדר $p_1p_2\dots p_k$ (מכפלת ראשוניים שונים). אזי

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

למשל אם G אבלית מסדר 154, אז $G\cong\mathbb{Z}_2\times\mathbb{Z}_7\times\mathbb{Z}_{11}$.

טענה 20.2. תהי G חבורה אבלית מסדר חזקה של ראשוני p^n. אזי קיימים מספרים טבעיים $m_1,\dots,m_k$ 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 G איזומורפית לאחת מהחבורות הבאות:

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

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

הערה 20.3. (תזכורת מתרגול שעבר):

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

הגדרה 20.4. למשל $\rho(4)=5$, כי $4=3+1=2+2=2+1+1=1+1+1+1=4$.

טענה 20.5. מספר החבורות האבליות, עד כדי איזומורפיזם, מסדר p^n הוא $\rho(n)$.

סיכום 20.6. כל חבורה אבלית מסדר $p_1^{k_1}\dots p_n^{k_n}$ איזומורפית למכפלה של חבורות אבליות $A_1\times\dots A_n$ כאשר A_i היא מסדר $p_i^{k_i}$. פירוק כזה נקרא פירוק פרימרי.

למשל, אם G חבורה אבלית כך ש-$|G|=45=3^2\cdot5$, אז G איזומורפית ל-$\mathbb{Z}_9\times\mathbb{Z}_5$ או ל-$\mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_5$.

טענה 20.7. מספר החבורות האבליות, עד כדי איזומורפיזם, מסדר $p_1^{k_1}\dots p_n^{k_n}$ הוא $\rho(k_1)\dots\rho(k_n)$.

למשל, מספר החבורות האבליות מסדר $200=2^3\cdot5^2$ הוא $\rho(3)\rho(2)=3\cdot2=6$.
האם אתם יכולים למצוא את כולן?

תרגיל 20.8. הוכיחו כי $\mathbb{Z}_{200}\times\mathbb{Z}_{20}\cong\mathbb{Z}_{100}\times\mathbb{Z}_{40}$.

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

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

הגדרה 20.9. תהי G חבורה. נגדיר את האקספוננט של החבורה $\exp(G)$ להיות המספר הטבעי הקטן ביותר n כך שלכל $g\in G$ מתקיים $g^n=e$. אם לא קיים כזה, נאמר $\exp(G)=\infty$.

קל לראות שהאקספוננט של G הוא הכפולה המשותפת המזערית (lcm) של סדרי האיברים שלה.

תרגיל 20.10. 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 $\exp(S_n) = [1, 2, \ldots, n]$.

תרגיל 20.11. הוכיחו שאם G חבורה אבלית סופית כך ש-$\exp(G) = |G|$, אז G ציקלית.

פתרון. נניח וישנו פירוק $\exp(G) = p_1^{k_1} \ldots p_n^{k_n} = |G|$. 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 קרטזית (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.

תרגיל 20.12. הוכח או הפרך: קיימות 5 חבורות לא איזומורפיות מסדר 8.

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

אלו הן:

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

וקיימות עוד שתי חבורות לא אבליות מסדר 8: D_4 וחבורת הקווטרניונים.

על חבורת הקווטרניונים: המתמטיקאי האירי בן המאה ה-19, וויליאם המילטון, הוא האחראי על גילוי חבורת הקווטרניונים.

רגע התגלית נקרא לימים "אקט של וונדליזם מתמטי".

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

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

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

הדמיון למספרים המרוכבים אינו מקרי. בנסיון להכליל את שדה המרוכבים הדו מימדי למרחב תלת מימדי, הבין המילטון שיהיה עליו לעלות מימד נוסף - למרחב הארבע-מימדי. זה מקור השם (קווטר פירושו ארבע).

קיימת הצגה שקולה וחסכונית יותר, על ידי 2 יוצרים בלבד:

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

21 משוואת המחלקה

לפני שנציג את משוואת המחלקה נזכיר שלושה מושגים.

הגדרה 21.1. המרכז (center) של חבורה G הוא הקבוצה:

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

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

הגדרה 21.2. תהי G חבורה. לכל $x\in G$, המְרַכֵּז (centralizer) של x הוא הקבוצה:

$$C_{G}\left(x\right):=\left\{y\in G:xy=yx\right\}$$

וכמו כן, ראינו ש-$C_{G}\left(x\right)$ תת־חבורה של G.

הגדרה 21.3. תהי G חבורה. יהי $x\in G$. נגדיר את מחלקת הצמידות של x להיות הקבוצה

$$\operatorname{conj}\left(x\right)=\left\{gxg^{-1}|g\in G\right\}$$

כאשר הסימון מקורו במילה conjugation שפירושה באנגלית הצמדה.

הערה 21.4. לכל $x\in G$ מתקיים:

$$\left[G:C_{G}\left(x\right)\right]=\left|\operatorname{conj}\left(x\right)\right|$$

תרגיל 21.5. מצא את מספר התמורות ב-S_n המתחלפות עם $\beta=\left(12\right)\left(34\right)$, כלומר כל התמורות $\gamma\in S_n$ המקיימות $\beta\gamma=\gamma\beta$.

פתרון. $\left|C_{S_n}\left(\beta\right)\right|=\frac{\left|S_n\right|}{\operatorname{conj}\left(\beta\right)}=\frac{n!}{\frac{1}{2}\binom{n}{2}\binom{n-2}{2}}=8\left(n-4\right)!$. לדוגמא: ב-$S_4$ יש 8 תמורות כאלו.

תרגיל 21.6. תהי G חבורה סופית כך ש-$\left[G:Z\left(G\right)\right]=n$. הראה כי מחלקת צמידות ב-G מכילה לכל היותר n איברים.

פתרון. לכל $x\in G$ מתקיים $Z\left(G\right)\leq C_{G}\left(x\right)$. לכן:

$$n=\left[G:Z\left(G\right)\right]\geq\left[G:C_{G}\left(x\right)\right]=\left|\operatorname{conj}\left(x\right)\right|$$

משפט 21.7 (משוואת המחלקות)**.** תהי G חבורה סופית. אזי:

$$|G|=\sum_{x\text{ rep.}}\left|\operatorname{conj}\left(x\right)\right|=\left|Z\left(G\right)\right|+\sum_{x\notin Z(G)\text{ rep.}}\frac{|G|}{\left|C_{G}(x)\right|}$$

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

תרגיל 21.8. רשום את משוואת המחלקות עבור S_3 ו-$\mathbb{Z}_6$.

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

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

- $|\operatorname{conj}(id)| = 1$.
- $|\operatorname{conj}(--)| = 3$.
- $|\operatorname{conj}(---)| = 2$.

תרגיל 21.9. הראה שמרכז של חבורת-p אינו טריוויאלי. (כאשר חבורת p, הינה חבורה סופית המקיימת $|G| = p^n$ עבור איזשהו $n \in \mathbb{N}$).

פתרון. על פי משוואת המחלקות:

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

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

תרגיל 21.10. מיינו את החבורות מסדר p^2 על ידי זה שתראו שהן חייבות להיות אבליות.

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

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

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

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

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

22 תת־חבורת הקומוטטור

הגדרה 22.1. תהא G חבורה. הקומוטטור של זוג איברים $a,b\in G$ הוא האיבר $[a,b]=aba^{-1}b^{-1}$.

הערה 22.2. a,b מתחלפים אם ורק אם $[a,b]=e$. באופן כללי, $ab=[a,b]\,ba$.

הגדרה 22.3. תת־חבורת הקומוטטור (נקראת גם תת־חבורת הנגזרת) הינה:

$$G'=[G,G]=\langle [g,h]:g,h\in G\rangle$$

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

הערה 22.4. G אבלית אם ורק אם $G'=\{e\}$.
למעשה, תת־חבורת הקומוטטור "מודדת" עד כמה החבורה G אבלית.

הערה 22.5. $[a,b]^{-1}=\left(aba^{-1}b^{-1}\right)^{-1}=bab^{-1}a^{-1}=[b,a]$.

הערה 22.6. אם $H\leq G$ אז $H'\leq G'$.

הערה 22.7. $G'\lhd G$. למשל לפי זה ש-$g\,[a,b]\,g^{-1}=\left[gag^{-1},gbg^{-1}\right]$.
תת־חבורת הקומוטטור מקיימת למעשה תנאי חזק הרבה יותר מנורמליות. לכל הומומורפיזם $f:G\to H$ מתקיים

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

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

הגדרה 22.8. חבורה G תקרא חבורה פשוטה אם ל-G אין תת־חבורות נורמליות לא טריוויאליות.

דוגמה 22.9. החבורה A_n עבור $n\geq 5$ פשוטה. חבורה אבלית (לאו דווקא סופית) היא פשוטה אם היא איזומורפית ל-$\mathbb{Z}_p$ עבור p ראשוני.

הגדרה 22.10. חבורה G נקראת מושלמת (perfect) אם $G=G'$.

מסקנה 22.11. 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 22.12. עבור $n\geq 5$, מתקיים $A_n^{'}=A_n$. אבל $\mathbb{Z}_5$ למשל היא פשוטה ולא מושלמת, כי היא אבלית.

משפט 22.13. המנה G/G', שנקראת האבליניזציה של G, היא המנה האבלית הגדולה ביותר של G. כלומר:

1. לכל חבורה G, המנה G/G' אבלית.

2. לכל $G \triangleleft N$ מתקיים ש G/N אבלית אם ורק אם $G' \leq N$ (כלומר G/N איזומורפית לתת־חבורה של G/G').

הערה 22.14. אם A אבלית, אז $A/G' \cong A$.

דוגמה 22.15. $D_4 = \langle \sigma, \tau \rangle$. 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 לפי תרגיל 21.10.
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 22.16. מצא את S_n' עבור $n \geq 5$.

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

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

כלומר קומוטטור הוא תמורה זוגית. גם כל מכפלה של קומוטטורים היא תמורה זוגית, ולכן $S_n' \leq A_n$.
נזכר כי $A_n \leq S_n$. לכן, על פי הערה שהצגנו קודם, $A_n' \leq S_n'$. מצד שני, ראינו שעבור $n \geq 5$ מתקיים $A_n' = A_n$. כלומר קיבלנו $S_n' = A_n$. בדרך אחרת, $S_n/A_n \cong \mathbb{Z}_2$ כלומר המנה אבלית. לכן, לפי מקסימליות האבליניזציה, נקבל $S_n' = A_n$.

23 שדות סופיים

הגדרה 23.1. שדה הוא מבנה אלגברי הכולל קבוצה F עם **שתי** פעולות בינאריות, להן אפשר לקרוא "חיבור" ו"כפל" ושני קבועים, שאותם נסמן 0_F ו-1_F, המקיים את התכונות הבאות:

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

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

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

הגדרה 23.2. סדר השדה הינו מספר האיברים בשדה.

הגדרה 23.3. איזומורפיזם של שדות הוא העתקה חח"ע ועל בין שני שדות ששומרת על שתי הפעולות.

הערה 23.4. הסדר של שדות סופיים הוא תמיד חזקה של מספר ראשוני. כמו כן, עבור כל חזקה של ראשוני קיים שדה סופי יחיד עד כדי איזומורפיזם של שדות מסדר זה. לא נוכיח טענות אלו.

טענה 23.5. לכל מספר ראשוני p, $\mathbb{F}_p = (\mathbb{Z}_p, +(\mathrm{mod} p), \cdot(\mathrm{mod} p))$ הוא שדה סופי מסדר p. האם אתם יכולים להראות שכל שדה סופי אחר מסדר p הוא איזומורפי ל-$\mathbb{F}_p$?

הגדרה 23.6. המאפיין של שדה F, שסימונו $\mathrm{char}(F)$, הינו המספר המינימלי המקיים: $1_F + 1_F + \cdots + 1_F = 0_F$. כלומר הסדר של 1_F בחבורה החיבורית של השדה (בחבורה הכפלית זהו איבר היחידה).

הערה 23.7. עבור שדה סופי $\mathbb{F}_q$, סדר השדה הוא תמיד חזקה של מספר ראשוני, כלומר מתקיים $q = p^n$ עבור p ראשוני כלשהו. לכן המאפיין של שדה סופי הוא בהכרח p.

הערה 23.8. אם הסדר של 1_F הוא אינסופי, מגדירים $\mathrm{char}(F) = 0$. למשל השדות $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ הם ממאפיין אפס. כל שדה סופי הוא בהכרח עם מאפיין חיובי.

טענה 23.9. החבורה הכפלית של השדה, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0_F\}$ היא ציקלית מסדר $q-1$.

דוגמה 23.10. $\mathbb{F}_{13}^* = \{1_F, 2, \ldots, 12\}$ חבורה ציקלית מסדר 12, כלומר $\mathbb{F}_{13}^* \cong \mathbb{Z}_{12}$.

הגדרה 23.11. יהי E שדה. תת־קבוצה (לא ריקה) $F \subseteq E$, שהיא שדה ביחס לפעולות המושרות נקראת תת־שדה. במקרה זה גם נאמר כי E/F הוא הרחבת שדות. נגדיר את הדרגה של E/F להיות המימד של E כמרחב וקטורי מעל F.

דוגמה 23.12. $\mathbb{C}/\mathbb{R}$ היא הרחבת שדות מדרגה 2, ואילו $\mathbb{R}/\mathbb{Q}$ היא הרחבת שדות מדרגה אינסופית. שימו לב ש-$\mathbb{Q}/\mathbb{F}_{13}$ היא לא הרחבת שדות כי לא מדובר באותן פעולות (ואפשר לומר גם שלא מדובר בתת־קבוצה).

טענה 23.13. אם E/F היא הרחבת שדות סופיים, אז $|E| = |F|^r$. כלומר $r = \log_{|F|}|E|$, ולמשל אם $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ הרחבת שדות, אז $r = n/m$.

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

הערה 23.14 (הרחבת שדות סופיים). הרחבה של $\mathbb{F}_p$ מדרגה $n \in \mathbb{N}$ מתבצעת על ידי הוספת שורש $\alpha \notin \mathbb{F}_p$ של פולינום אי פריק ממעלה n מעל $\mathbb{F}_p$ (כלומר שהמקדמים הם מהשדה הזה).

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

דוגמה 23.15. השדה $K = \mathbb{F}_3(i) = \mathbb{F}_9$ כאשר i הוא שורש הפולינום x^2+1 הוא הרחבה של השדה $\mathbb{F}_3$. קל לבדוק האם פולינומים ממעלה 2 או 3 הם אי פריקים מעל שדה על ידי זה שנראה שאין להם שורשים מעל השדה.

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

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

תרגיל 23.16. לאילו שדות סופיים $\mathbb{F}_q$ יש איבר x המקיים $x^4=-1$?

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

אם $x^4=-1$ אז $x^8=(-1)^2=1$, ולכן מתקיים $o(x) \mid 8$. מנגד, אם המאפיין של השדה איננו 2, אז $x^4 \neq 1$ כי $-1 \neq 1$ לכן $o(x) \nmid 4$.

הפתרון הוא $o(x)=8$. אם כן, נדרוש שב-$\mathbb{F}_q^*$ יהיה איבר x מסדר 8, ואז הוא יקיים את המשוואה. מכיוון שסדר איבר מחלק את סדר החבורה (לגרנז'), נסיק שהסדר של $\mathbb{F}_q^*$ מתחלק ב 8.

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

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

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

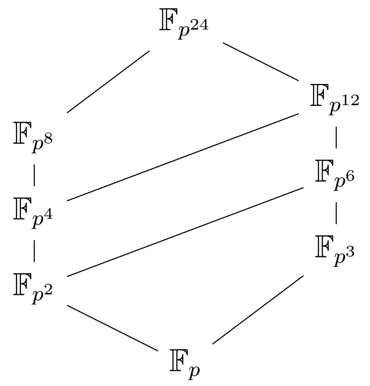
לסיכום, השדות האפשריים הם שדות ממאפיין 2 או מסדר המקיים $q=p^n \equiv 1$ $\mathrm{mod}\ 8$.

תרגיל 23.17. בשדה $\mathbb{F}_q$ מתקיים $a^q=a$ לכל $a\in\mathbb{F}_q$ וגם $x^q-x=\prod_{a\in\mathbb{F}_q}(x-a)$.

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

תרגיל 23.18. הוכיחו כי $\mathbb{F}_q$ משוכן ב-$\mathbb{F}_{q'}$ אם ורק אם $q'=q^r$ עבור r כלשהו. בפרט, עבור p ראשוני, $\mathbb{F}_{p^n}$ הוא תת־שדה של $\mathbb{F}_{p^m}$ אם ורק אם $n|m$.

הוכחה. נתחיל בדוגמה של סריג תת־השדות של $\mathbb{F}_{p^{24}}$:



בכיוון אחד, נניח כי $\mathbb{F}_q$ הוא תת־שדה של $\mathbb{F}_{q'}$. אזי $\mathbb{F}_{q'}$ מרחב וקטורי מעל $\mathbb{F}_q$, וראינו בטענה 23.13 ש-$q' = q^r$ עבור r כלשהו.

בכיוון השני, נניח $q' = q^r$, ונראה כי ל-$\mathbb{F}_{q'}$ יש תת־שדה מסדר q. מתקיים

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

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

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

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

24 בעיית הלוגריתם הבדיד ואלגוריתם דיפי-הלמן

בעיה 24.1 (בעיית הלוגריתם הבדיד, DLP)**.** תהי G חבורה. יהי $g \in G$ ו-$x \in \mathbb{N}$. המשימה היא למצוא את x בהנתן $h = g^x$. מסמנים את הפתרון ב-$\log_g h$. מסתבר שבחבורות מתאימות, אפילו אם ניתן לממש את הפעולה בחבורה באופן יעיל מאוד, עדין קשה מאוד (סיבוכיות זמן ריצה שהיא לפחות תת־מעריכית) למצוא את x.

הערה 24.2. שימו לב שבעיית הלוגריתם הבדיד עוסקת למעשה רק בחבורה הציקלית $\langle g \rangle$. למרות שכל החבורות הציקליות מאותו סדר הן איזומורפיות, דרך ההצגה של החבורה תקבע את הקושי של פתרון הבעיה. בעיית הלוגריתם הבדיד היא הבעיה הקשה בבסיס של בניות קריפטוגרפיות רבות, כמו החלפת מפתחות, הצפנה, חתימות דיגיטליות ופונקציות גיבוב קריפטוגרפיות.

דוגמה 24.3. דוגמה למה החבורה החיבורית $\mathbb{Z}_n$ היא לא בחירה טובה לבעיית הלוגריתם הבדיד. נניח $\mathbb{Z}_n = \langle g \rangle$. שימו לב שאם $g = 1$ הבעיה היא טריוויאלית! הרי $x \cdot 1 \equiv x \pmod{n}$. שימו לב כי ה-$x$ באגף שמאל הוא מספר טבעי, ואילו באגף ימין זה איבר של $\mathbb{Z}_n$.

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

טענה 24.4 (אלגוריתם דיפי-הלמן). תהי חבורה ציקלית $G = \langle g \rangle$ מסדר n, הידועה לכל. מקובל לבחור את U_p עבור p ראשוני גדול מאוד (יותר מאלף ספרות בינאריות).

לכל משתמש ברשת יש מפתח פרטי סודי, מספר טבעי $a \in [2, n-1]$ ומפתח ציבורי $g^a \pmod{n}$. איך שני משתמשים, אליס ובוב, יתאמו בינהן מפתח הצפנה שיהיה ידוע רק להם?

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

הערה 24.5. בתהליך המפתח הסודי של אליס ובוב לא שודר, וסודיותו לא נפגעה. האלגוריתם הוא סימטרי, כלומר ניתן לחשב ממפתח ההצפנה את מפתח הפענוח ולהפך. יש לפחות מתקפה ברורה אחת והיא שתוקף יכול להתחזות בדרך לאליס או לבוב (או לשניהם), ולכן בפועל משתמשים בפרוטוקולים יותר מתוחכמים יותר למניעת התקפה זו.

דוגמה 24.6. נריץ את האלגוריתם עם מספרים קטנים (באדיבות ויקיפדיה). יהי $p = 23$. נבחר יוצר $U_{23} = \langle 5 \rangle$.

אליס בחרה $a = 6$, ולכן תשלח לבוב את $5^6 \equiv 8 \pmod{23}$. בוב בחר $b = 15$, ולכן ישלח לאליס את $5^{15} \equiv 19 \pmod{23}$. כעת אליס תחשב $19^6 \equiv 2 \pmod{23}$, ובוב יחשב $8^{15} \equiv 2 \pmod{23}$.

25 אלגוריתם מילר-רבין לבדיקת ראשוניות

בפרק זה נציג אלגוריתם נפוץ לבדיקת ראשוניות של מספרים טבעיים. האלגוריתם המקורי הוא דטרמיניסטי ופותח בשנת 1976 על ידי מילר. בשנת 1980 הוצגה גרסה הסתברותית של האלגוריתם על ידי רבין. הגרסה ההסתברותית היא מהירה יחסית.

היא תזהה כל מספר ראשוני, אבל בהסתברות נמוכה (התלויה במספר האיטרציות באלגוריתם) היא תכריז גם על מספק פריק כראשוני.

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

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

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

טענה 25.1 (אלגוריתם מילר-רבין). הקלט הוא מספר טבעי $N > 3$, ופרמטר k הקובע את דיוק המבחן.

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

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

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

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

נחשב $x = x^2$.

אם $x \equiv 1 \,(\mathrm{mod} N)$, נחזיר את הפלט "פריק".

אחרת, אם $x \equiv -1 \,(\mathrm{mod} N)$, נעבור לאיטרציה הבאה של לולאת העדים.

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

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

תרגיל 25.2 (רשות). כתבו בשפת אסמבלי פונקציה מהירה לחישוב מספר הפעמים ש-N מתחלק ב-2. כלומר מצאו כמה אפסים רצופים יש בסוף ההצגה הבינארית של N כדי למצוא את s.

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

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

דוגמה 25.3. נניח $N = 221$ ו-$k = 2$. נציג את $N - 1 = 220 = 2^2 \cdot 55$. כלומר $s = 2$ ו-$M = 55$.

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

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

נשים לב כי 47 אינו ± 1 מודולו 211. לכן נבדוק

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

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

$$a^{2^0 M} = 137^{55} \equiv 188 \pmod N$$
$$a^{2^1 M} = 137^{110} \equiv 205 \pmod N$$

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

דוגמה 25.4. נניח $N = 781$. נציג את $N - 1 = 780 = 2^2 \cdot 195$. אם נבחר באקראי (לפי ויקיפדיה העברית) את $a = 5$, נקבל כי

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

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

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

ולכן גם 17 הוא עד חזק. אם נבדוק את $a = 2$ נגלה כי $2^{780} \equiv 243 \neq \pm 1$, ולכן 781 אינו ראשוני. אגב $781 = 11 \cdot 71$.