מבנים אלגבריים למדעי המחשב
מערכי תרגול קורס 89-214

דצמבר 2022, גרסה 1.61

אוניברסיטת בר־אילן

סמסטר א׳ תשפ״ג

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.
- החומר בקובץ זה נאסף מכמה מקורות, ומבוסס בעיקרו על מערכי תרגול קודמים בקורסים מבנים אלגבריים למדעי המחשב ואלגברה מופשטת למתמטיקה.
- נשתדל לכתוב בגופן הזה כשהגדרות ומושגים חשובים מופיעים בפעם הראשונה. This font נוסיף בצד גם את השם באנגלית, שעשוי לעזור כשמחפשים חומר נוסף שאינו בעברית.
- נשמח לכל הערה על מסמך זה.

מחברים בשנת הלימודים תשע"ו: אבי אלון, תומר באואר וגיא בלשר
מחברים בשנת הלימודים תשע"ז: תומר באואר, עמרי מרכוס ואלעד עטייא
מחברים בשנת הלימודים תשע"ט: תומר באואר וגלעד פורת קורן
עידכונים בשנות הלימודים תש"ף–תשפ"ג: תומר באואר

1 תרגול ראשון

1.1 מבנים אלגבריים בסיסיים

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

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

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

Binary operation

הגדרה 1.1. פעולה בינארית על קבוצה S היא פונקציה דו־מקומית $* : S \times S \to S$. עבור $a, b \in S$ כמעט תמיד במקום לרשום $*(a, b)$ נשתמש בסימון $a * b$. חשוב לשים לב שהפעולה היא סגורה, כלומר תמונת הפונקציה $a * b$ תמיד שייכת ל-S.

Semigroup
Associative
Associativity

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

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

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

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

Identity element

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

Monoid

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

הערה 1.8 (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 1.9. יהי $(M,*,e)$ מונואיד. איבר $a \in M$ יקרא הפיך משמאל אם קיים איבר $b \in M$ כך ש-$ba = e$. במקרה זה b יקרא הופכי שמאלי של a.
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.

Left invertible
Left inverse
Right invertible
Right inverse
Invertible
Inverse

תרגיל 1.10. יהי $a \in M$ איבר הפיך משמאל ומימין. הראו ש-a הפיך וההופכי שלו הוא יחיד.

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

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

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

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

Group

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

1. סגירות הפעולה.
2. קיבוציות הפעולה.
3. קיום איבר יחידה.
4. כל איבר הוא הפיך.

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

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

דוגמה 1.13. יהי F שדה (למשל $\mathbb{Q}$, $\mathbb{R}$ או $\mathbb{C}$). אזי $(F,+,0)$ עם פעולת החיבור של השדה היא חבורה. באופן דומה גם $(M_{n,m}(F),+)$ (אוסף המטריצות בגודל $n \times m$ מעל F) עם פעולת חיבור מטריצות היא חבורה. איבר היחידה הוא מטריצת האפס.

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

דוגמה 1.15. יהי F שדה. נסמן $F^* = F \setminus \{0\}$. אזי $(F^*, \cdot, 1)$ היא חבורה. לעומת זאת, המערכת $(\mathbb{Z}^*, \cdot)$ עם הכפל הרגיל של מספרים שלמים היא רק מונואיד (מי הם האיברים ההפיכים בו?).

דוגמה 1.16. תהי X קבוצה כלשהי, ותהי $P(X)$ קבוצת החזקה שלה (זהו אוסף כל תת־הקבוצות של X). אזי $(P(X), \cap)$ היא מונואיד שבו איבר היחידה הוא X. מה קורה עבור $(P(X), \cup)$?

דוגמה 1.17. קבוצה בעלת איבר אחד ופעולה סגורה היא חבורה. לחבורה זו קוראים החבורה הטריוויאלית.

Trivial group

הגדרה 1.18. יהי M מונואיד. אוסף האיברים ההפיכים במונואיד מהווה חבורה ביחס לפעולה המצומצמת, הנקראת חבורת האיברים ההפיכים של M ומסומנת $U(M)$.

Group of units

למה $U(M)$ חבורה בכלל? יהיו $a, b \in M$ זוג איברים. אם a, b הם הפיכים, אזי גם $a \cdot b$ הוא הפיך במונואיד. אכן, האיבר ההופכי הוא $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. לכן אוסף כל האיברים ההפיכים במונואיד מהווה קבוצה סגורה ביחס לפעולה. האוסף הזה מכיל את איבר היחידה, וכל איבר בו הוא הפיך.

הערה 1.19. מתקיים $U(M) = M$ אם ורק אם M היא חבורה.

דוגמה 1.20. לפעמים עבור מונואיד אינסופי, כמו $M = (\mathbb{Z}, \cdot)$, חבורת ההפיכים שלו סופית, למשל כאן $U(M) = \{1, -1\}$.

הגדרה 1.21. המערכת $(M_n(\mathbb{R}), \cdot)$ של מטריצות ממשיות בגודל $n \times n$ עם כפל מטריצות היא מונואיד. לחבורת ההפיכים שלו

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

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

General linear group

תרגיל 1.22 (אם יש זמן)**.** האם קיים מונואיד שיש בו איבר הפיך מימין שאינו הפיך משמאל?

פתרון. כן. נבנה מונואיד כזה. תהא X קבוצה. נסתכל על קבוצת ההעתקות מ-X לעצמה המסומנת $X^X = \{f \mid X \to X\}$. 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 $X = \{1, \dots, n\}$ מקובל לסמן את חבורת הסימטריה שלה בסימון S_n, ובה כל איבר הפיך משמאל.)

Symmetry group on X

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.

1.2 חבורות אבליות

הגדרה 1.23. נאמר כי פעולה דו־מקומית $*: G \times G \to G$ היא אבלית (או חילופית) 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).

Abelian (or commutative)

Abelian group

דוגמה 1.24. יהי F שדה. החבורה $(GL_n(F), \cdot)$ אינה אבלית עבור $n > 1$.

דוגמה 1.25. מרחב וקטורי V יחד עם פעולת חיבור וקטורים הרגילה הוא חבורה אבלית.

תרגיל 1.26. תהי G חבורה. הוכיחו שאם לכל $x \in G$ מתקיים $x^2 = e$, אזי G היא חבורה אבלית.

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

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

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

הגדרה 1.27. תהי G חבורה. נאמר ששני איברים $a, b \in G$ מתחלפים אם $ab = ba$. נגדיר את המֶרְכָּז של חבורה G להיות

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

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

דוגמה 1.28. חבורה G היא אבלית אם ורק אם $Z(G) = G$. האם אתם יכולים להראות שבהנתן חבורה G, אז גם $Z(G)$ היא חבורה?

דוגמה 1.29. החבורה $GL_n(\mathbb{R})$ היא לא אבלית עבור $n > 1$, אבל קבוצת כל המטריצות האלכסוניות ב-$GL_n(\mathbb{R})$ היא חבורה אבלית ביחס לכפל מטריצות. האם חבורה זו שווה ל-$Z(GL_n(\mathbb{R}))$?

תרגיל 1.30. הוכיחו כי $Z(GL_n(\mathbb{R})) = \{\alpha I_n \,|\, \alpha \in \mathbb{R}^*\}$. כלומר, שהמרכז של החבורה $GL_n(\mathbb{R})$ הוא קבוצת המטריצות הסקלריות ההפיכות.

הערה 1.31. עבור קבוצה סופית אפשר להגדיר פעולה בעזרת לוח כפל. למשל, אם $S = \{a, b\}$ ונגדיר

$*$	a	b
a	a	a
b	b	b

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

הערה 1.32 (אם יש זמן). בקורס באלגברה לינארית כנראה ראיתם הגדרה של שדה $(F,+,\cdot,0,1)$ הכוללת רשימה ארוכה של דרישות. בעזרת ההגדרות שראינו נוכל לקצר אותה. נסמן $F^* = F\setminus\{0\}$. נאמר כי F הוא שדה אם $(F,+,0)$ היא חבורה אבלית, $(F^*,\cdot,1)$ היא חבורה אבלית וקיום חוק הפילוג (לכל $a,b,c\in F$ מתקיים $a(b+c)=ab+ac$). Distributive law

2 תרגול שני

הגדרה 2.1. 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 $-5|10$ וגם $n|\pm n$ לכל $n\neq 0$. Divides

משפט 2.2 (משפט החילוק, או חלוקה אוקלידית). לכל $n\in\mathbb{Z}$, $d\neq 0$ קיימים q,r יחידים כך ש-$n = qd+r$ וגם $0\le r<|d|$. Euclidean division

הגדרה 2.3. יהי n מספר טבעי. נאמר כי $a,b\in\mathbb{Z}$ הם שקולים מודולו n אם $n|a-b$. במילים אחרות, לשניהם יש את אותה שארית בחלוקה ב-n. 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". Congruent modulo n

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

טענה 2.4 (הוכחה לבית). שקילות מודולו n היא יחס שקילות (רפלקסיבי, סימטרי וטרנזיטיבי). חיבור וכפל מודולו n מוגדרים היטב.

דוגמה 2.5. נסתכל על אוסף מחלקות השקילות מודולו n, $\mathbb{Z}_n = \{[a] \mid a\in\mathbb{Z}\}$. למשל $\mathbb{Z}_4 = \{[0],[1],[2],[3]\}$. לפעמים מסמנים את מחלקת השקילות $[a]$ בסימון $\bar{a}$, ולעיתים כאשר ההקשר ברור פשוט a. Congruence class

נגדיר חיבור מודולו n לפי $[a]+[b] := [a+b]$ 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). באופן דומה נגדיר כפל מודולו n. אלו פעולות המוגדרות היטב. כלומר אם $a\equiv b, c\equiv d \pmod n$, אז $a+c\equiv b+d \pmod n$, וגם $ac\equiv bd \pmod n$.

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

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

2.1 תת־חבורות

הגדרה 2.6. תהי G חבורה. תת־קבוצה $H \subseteq G$ היא תת־חבורה, אם היא חבורה ביחס לאותה פעולה (באופן יותר מדויק, ביחס לפעולה המושרית מ-G). במקרה כזה נסמן $H \leq G$. Subgroup

דוגמה 2.7. לכל חבורה G יש שתי תת־חבורות באופן מיידי: $\{e\} \leq G$ (הנקראת תת־החבורה הטריוויאלית), ו-$G \leq G$. Trivial subgroup

צורת רישום 2.8. יהי n מספר שלם. נסמן את הכפולות שלו ב-$n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$. למשל $4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$. זו חבורה אבלית לגבי חיבור רגיל של שלמים.

דוגמה 2.9. לכל $n \in \mathbb{Z}$, $n\mathbb{Z} \leq \mathbb{Z}$. בהמשך נוכיח שאלו כל תת־החבורות של $\mathbb{Z}$.

דוגמה 2.10 (בתרגיל). $m\mathbb{Z} \leq n\mathbb{Z}$ אם ורק אם $n|m$.

דוגמה 2.11. $(\mathbb{Z}_n, +)$ <u>אינה</u> תת־חבורה של $(\mathbb{Z}, +)$ כי $\mathbb{Z}_n$ אינה מוכלת ב-$\mathbb{Z}$. האיברים ב-$\mathbb{Z}_n$ הם מחלקות שקילות, ואילו האיברים ב-$\mathbb{Z}$ הם מספרים. גם לא מדובר באותן פעולות, למרות שהסימון $+$ זהה.

דוגמה 2.12. $(GL_n(\mathbb{R}), \cdot)$ <u>אינה</u> תת־חבורה של $(M_n(\mathbb{R}), +)$, כי הפעולות בהן שונות.

טענה 2.13 (קריטריון מקוצר לתת־חבורה - בהרצאה). תהי $H \subseteq G$ תת־קבוצה. אזי H תת־חבורה של G אם ורק אם שני התנאים הבאים מתקיימים:

1. $H \neq \varnothing$ (בדרך כלל הכי נוח להראות $e \in H$).
2. לכל $h_1, h_2 \in H$, גם $h_1 \cdot h_2^{-1} \in H$.

תרגיל 2.14. יהי F שדה. נגדיר

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

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

הוכחה. ניעזר בקריטריון המקוצר לתת־חבורה.

1. ברור כי $SL_n(F)$ לא ריקה. הרי $I_n \in SL_n(F)$, כי $\det I_n = 1$.
2. נניח $A, B \in SL_n(F)$. צ"ל $AB^{-1} \in SL_n(F)$. אכן,

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

ולכן $AB^{-1} \in SL_n(F)$.

לפי הקריטריון המקוצר, $SL_n\left(F\right)$ היא תת־חבורה של $GL_n\left(F\right)$. $\square$

תרגיל 2.15. תהי G חבורה. הוכיחו $Z(G) \leq G$, כלומר שהמרכז הוא תת־חבורה.

הערה 2.16. מהתרגיל האחרון מסיקים כי אוסף המטריצות הסקלריות ההפיכות (בגודל $n \times n$) מעל שדה F הוא תת־חבורה של $GL_n(F)$. קל להראות שאוסף כל המטריצות האלכסוניות ההפיכות הוא תת־חבורה. האם תוכלו למצוא תת־חבורות אבליות של $GL_n(F)$ שלא מכילות אף איבר מרכזי, פרט למטריצת היחידה?

תרגיל 2.17 (לדלג)**.** תהי G חבורה, ויהיו $H, K \leq G$. נגדיר

$$HK = \{hk \,|\, h \in H, k \in K\}$$

הוכיחו: $HK = KH$ אם ורק אם $HK \leq G$.

פתרון. בכיוון אחד, נניח $HK = KH$, ונוכיח $HK \leq G$. ניעזר בקריטריון המקוצר:

1. מפני ש-$e \in H, K$, ברור כי $e = e \cdot e \in HK$.
2. נניח $x, y \in HK$, ונוכיח $x \cdot y^{-1} \in HK$. לפי ההנחה קיימים $h_1, h_2 \in H$ ו-$k_1, k_2 \in K$ שעבורם $x = h_1 k_1$ ו-$y = h_2 k_2$. לכן,

$$xy^{-1} = \left(h_1 k_1\right)\left(h_2 k_2\right)^{-1} = h_1 \underbrace{k_1 k_2^{-1}}_{k_3 \in K} h_2^{-1} = h_1 k_3 h_2^{-1}$$

נשים לב כי $k_3 h_2^{-1} \in KH = HK$, ולכן קיימים $h' \in H$ ו-$k' \in K$ שעבורם $k_3 h_2^{-1} = h' k'$. לכן,

$$xy^{-1} = h_1 k_3 h_2^{-1} = \underbrace{h_1 h'}_{\in H} k' \in HK$$

כדרוש.

בכיוון השני, נניח $HK \leq G$, ונוכיח $HK = KH$. עבור $X \subseteq G$, נסמן

$$X^{-1} = \left\{x^{-1} \,\middle|\, x \in X\right\}$$

מפני ש-$H, K, HK \leq G$ הן חבורות, אז הן סגורות להופכי. כלומר $H^{-1} = H$, $K^{-1} = K$ ו-$\left(HK\right)^{-1} = HK$. לכן $HK = \left(HK\right)^{-1} = K^{-1} H^{-1} = KH$.

2.2 סדרים

הגדרה 2.18. תהי G חבורה. נגדיר את הסדר של G להיות עוצמתה כקבוצה. במילים יותר גשמיות, כמה איברים יש בחבורה. נסמן זאת $|G|$. Order of a group

צורת רישום 2.19. בחבורה כפלית נסמן את החזקה החיובית $a^n = aa \dots a$ 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 2.20. 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 $|g|$. Order of an element

דוגמה 2.21. 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 2.22. נסתכל על $GL_2\left(\mathbb{R}\right)$, חבורת המטריצות ההפיכות מגודל 2×2 מעל $\mathbb{R}$. נחשב את הסדר של האיבר $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$:

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

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

לכן $o\left(b\right) = 3$.

תרגיל 2.23. תהי G חבורה. הוכיחו שלכל $a \in G$, $o\left(a\right) = o\left(a^{-1}\right)$.

פתרון. נחלק לשני מקרים:

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

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

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

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

2.3 חבורות ציקליות

Subgroup generated by a

הגדרה 2.24. 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 2.25. לכל $n \in \mathbb{Z}$ מתקיים $\langle n \rangle = \{kn \,|\, k \in \mathbb{Z}\} = n\mathbb{Z}$.

Cyclic group

הגדרה 2.26. 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 2.27. 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 2.28. החבורה $(\mathbb{Z}_n, +) = \langle 1 \rangle$ היא ציקלית. וודאו כי בחבורה $(\mathbb{Z}_2, +)$ יש רק יוצר אחד (נניח על ידי טבלת כפל). וודאו כי בחבורה $(\mathbb{Z}_{10}, +)$ יש ארבעה יוצרים. קל למצוא שניים (1 וגם $9 \equiv -1$), האחרים $(3, 7)$ דורשים לבינתיים בדיקה ידנית.

טענה 2.29. יהי $a \in G$. אזי $o\,(a) = |\langle a \rangle|$. במילים, הסדר של איבר הוא סדר תת־החבורה שהוא יוצר.

הערה 2.30. 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 $5 + 5 \equiv 0 \pmod{10}$.

דוגמה 2.31. עבור $a \in GL_3(\mathbb{C})$ נחשב את $|\langle a \rangle|$ כאשר

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

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

טענה 2.32. כל חבורה ציקלית היא אבלית.

הוכחה. תהי G חבורה ציקלית, ונניח כי $G = \langle a \rangle$. צריך להוכיח שכל $g_1, g_2 \in G$ מתחלפים. מפני ש-G ציקלית, קיימים i, j שעבורם $g_1 = a^i$ ו-$g_2 = a^j$. מכאן שמתקיים

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

כלומר $g_1 g_2 = g_2 g_1$, כדרוש. $\square$

הערה 2.33. לא כל חבורה אבלית היא ציקלית. נסו למצוא דוגמאות כאלו.

3 תרגול שלישי

3.1 המשך ציקליות וסדרים

טענה 3.1. הוכיחו שאם G ציקלית, אז כל תת־חבורה של G היא ציקלית.

הוכחה. תהי $H \leq G$ תת־חבורה. נסמן $G = \langle a \rangle$. כל האיברים ב-G הם מהצורה a^i, ולכן גם כל האיברים ב-H הם מהצורה הזו. אם $H = \{e\}$, אז $H = \langle e \rangle$ וסיימנו. מעתה נניח כי H לא טריוויאלית.

יהי $0 \neq s \in \mathbb{Z}$ המספר המינימלי בערכו המוחלט כך ש-$a^s \in H$. אפשר להניח ש-$s \in \mathbb{N}$ כי אם $a^i \in H$, אז גם $a^{-i} \in H$ מסגירות להופכי. נרצה להוכיח $H = \langle a^s \rangle$. ההכלה בכיוון $\supseteq$ ברורה, הרי $\langle a^s \rangle$ זו תת־החבורה הקטנה ביותר שמכילה את a^s, והנחנו כי $a^s \in H$, אז H מכילה את $\langle a^s \rangle$.

לכיוון השני, יהי $h \in H$. כלומר קיים $k \in \mathbb{Z}$ שעבורו $h = a^k$ כי $h \in G$. לפי משפט החילוק עם שארית, קיימים q ו-r שעבורם $k = qs + r$ עם $0 \leq r < s$. לכן,

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

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

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

מסקנה 3.2. תת־החבורות של $(\mathbb{Z}, +)$ הן בדיוק $(n\mathbb{Z}, +)$ עבור $n \in \mathbb{N} \cup \{0\}$.

טענה 3.3. תהי G חבורה, ויהי $a \in G$. מתקיים $a^n = e$ אם ורק אם $o\left(a\right)|n$.

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

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

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

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

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

n-th roots of unity

דוגמה 3.4 (לדלג)**.** 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 $\mathbb{C}^*$. אם נסמן $\omega_n = \operatorname{cis}\frac{2\pi}{n}$, נקבל $\Omega_n = \langle \omega_n \rangle$. כלומר Ω_n היא תת־חבורה ציקלית ונוצרת על ידי ω_n. כדאי לצייר את Ω_4 או Ω_6 כדי להבין למה החבורות נקראות ציקליות.

Roots of unity

תרגיל 3.5 (לדלג)**.** נסמן את קבוצת שורשי היחידה $\Omega_\infty = \bigcup_{n=1}^{\infty} \Omega_n$. הוכיחו:

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

Torsion group

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

פתרון.

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

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

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

3.2 מכפלה ישרה של חבורות

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

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

טענה 3.6. נגדיר פעולה $\odot$ על $G \times H$ רכיב-רכיב, כלומר

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

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

(External) Direct product

דוגמה 3.7. נסתכל על $\mathbb{C}^* \times \mathbb{Z}_8$. נדגים את הפעולה:

$$(-i,2) \odot (i,7) = (-i \cdot i, 2+7) = (1,1)$$
$$(5+3i,1) \odot (2,2) = ((5+3i)\cdot 2, 1+2) = (10+6i,3)$$

האיבר היחידה בחבורה זו הוא $(1,0)$.

הערה 3.8. מעכשיו, במקום לסמן את הפעולה של $G \times H$ ב-$\odot$, נסמן אותה $\cdot$ בשביל הנוחות.

תרגיל 3.9. האם $\mathbb{Z}_n \times \mathbb{Z}_n$ ציקלית (עבור $n \ge 2$)?

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

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

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

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

הערה 3.10. התרגיל הקודם אומר שמכפלה של חבורות ציקליות אינה בהכרח ציקלית. לעומת זאת, מכפלה של חבורות אבליות נשארת אבלית.

3.3 מבוא לחבורה הסימטרית

הגדרה 3.11. החבורה הסימטרית מדרגה n היא Symmetric group

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

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. Permutation

הערה 3.12 (אם יש זמן). החבורה S_n היא בדיוק חבורת ההפיכים במונואיד X^X עם פעולת ההרכבה, כאשר $X = \{1,2,\ldots,n\}$.

דוגמה 3.13. ניקח לדוגמה את S_3. איבר $\sigma \in S_3$ הוא מהצורה $\sigma(1) = i$, $\sigma(2) = j$ ו-$\sigma(3) = k$, כאשר $i,j,k \in \{1,2,3\}$ שונים זה מזה. נסמן בקיצור

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

נכתוב במפורש את כל האיברים ב-S_3:

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

מסקנה 3.14. נשים לב ש-S_3 אינה אבלית, כי $\sigma\tau \neq \tau\sigma$. מכאן גם קל לראות ש-$S_n$ אינה ציקלית לכל $n \geq 3$, כי היא לא אבלית.

הערה 3.15. הסדר הוא $|S_n| = n!$. אכן, מספר האפשרויות לבחור את $\sigma(1)$ הוא n. אחר כך, מספר האפשרויות לבחור את $\sigma(2)$ הוא $n-1$. כך ממשיכים, עד שמספר האפשרויות לבחור את $\sigma(n)$ הוא 1, האיבר האחרון שלא בחרנו. בסך הכל, $|S_n| = n\cdot(n-1)\cdots 1 = n!$.

Cycle

Length of a cycle

הגדרה 3.16. 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 3.17. התמורה $\sigma \in S_3$ שכתבנו בדוגמה 3.13 היא המחזור $(1\ 2\ 3)$. שימו לב שלא מדובר בתמורת הזהות!

דוגמה 3.18. ב-S_5, המחזור $(4\ 5\ 2)$ מציין את התמורה $\begin{pmatrix}1&2&3&4&5\\1&4&3&5&2\end{pmatrix}$.

Disjoint cycles

משפט 3.19. כל תמורה ניתנת לכתיבה כהרכבת מחזורים זרים, כאשר הכוונה ב"מחזורים זרים" היא מחזורים שאין להם מספר משותף שהם משנים את מיקומו.

הערה 3.20. שימו לב שמחזורים זרים מתחלפים זה עם זה (מדוע?), ולכן חישובים עם מחזורים יהיו לעיתים קלים יותר מאשר חישובים עם התמורה כמטריצה.

דוגמה 3.21. 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 תשלח σ^2 אותו; אבל, כיוון שמחזורים זרים מתחלפים, נקבל

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

4 תרגול רביעי

4.1 הומומורפיזמים

הגדרה 4.1. תהינה $(G,*)$, $(H,\bullet)$ חבורות. העתקה $f\colon G\to H$ תקרא הומומורפיזם של חבורות אם מתקיים

Group homomorphism

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

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 $f\colon G\hookrightarrow H$. (Monomorphism)
2. הומומורפיזם שהוא על נקרא אפימורפיזם. נאמר כי H היא תמונה אפימורפית של G אם קיים אפימורפיזם $f\colon G\twoheadrightarrow H$. (Epimorphism, Epimorphic image)
3. הומומורפיזם שהוא חח"ע ועל נקרא איזומורפיזם. נאמר כי G ו-H איזומורפיות אם קיים איזומורפיזם $f\colon G\to H$. נסמן זאת $G\cong H$. (Isomorphism, Isomorphic groups)
4. איזומורפיזם $f\colon G\to G$ נקרא אוטומורפיזם של G. (Automorphism)
5. בכיתה נקצר את השמות של הומומורפיזם, מונומורפיזם, אפימורפיזם, איזומורפיזם ואוטומורפיזם להומ', מונו', אפי', איזו' ואוטו', בהתאמה.

הערה 4.2. הומומורפיזם $f\colon G\to H$ הוא איזומורפיזם אם ורק אם קיימת העתקה $g\colon H\to G$ כך ש-$f\circ g=\mathrm{id}_H$ וגם $g\circ f=\mathrm{id}_G$.
אפשר להוכיח (נסו!) שההעתקה g הזו היא הומומורפיזם בעצמה. כלומר כדי להוכיח שהומומורפיזם f הוא איזומורפיזם מספיק למצוא העתקה הפוכה $g=f^{-1}$. אפשר גם לראות שאיזומורפיות היא תכונה רפלקסיבית, סימטרית וטרנזיטיבית (היא לא יחס שקילות כי מחלקת החבורות היא גדולה מכדי להיות קבוצה).

תרגיל 4.3. הנה רשימה של כמה העתקות בין חבורות. קבעו האם הן הומומורפיזמים, ואם כן מהו סוגן:

1. $\varphi\colon\mathbb{R}\to\mathbb{R}^*$ המוגדרת לפי $x\mapsto e^x$ היא מונומורפיזם. מה היה קורה אם היינו מחליפים למרוכבים?
2. יהי F שדה. אז $\det\colon GL_n(F)\to F^*$ 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. $\varphi\colon \mathbb{R} \to \mathbb{R}^*$ המוגדרת לפי $x \mapsto x$ אינה הומומורפיזם כלל, אפילו אם נקבע $\varphi(0) = 1$.

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

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

1. $f(e_G) = e_H$.

2. $f(g^{-1}) = f(g)^{-1}$.

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

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

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

6. אם $G \cong H$, אז $|G| = |H|$.

דוגמה 4.4 (לדלג). התכונות האלו של הומומורפיזמים מזכירות, ולא במקרה, מה שלומדים באלגברה לינארית. יהיו V, W מרחבים וקטוריים מעל שדה F. העתקה לינארית $T\colon V \to W$ היא (גם) הומומורפיזם של חבורות. נניח $\dim V = \dim W$, האם בהכרח T איזומורפיזם?

הערה 4.5 (לדלג). ידוע שהעתקה לינארית נקבעת באופן יחיד על ידי תמונה של בסיס. באופן דומה, אם $G = \langle S \rangle$, אז תמונת הומומורפיזם $f\colon G \to H$ נוצרת על ידי $f(S)$.

שימו לב שלא כל קביעה של תמונה של קבוצת יוצרים (אפילו של יוצר אחד) תגדיר הומומורפיזם. למשל $\varphi\colon \mathbb{Z}_n \to \mathbb{Z}$ המוגדרת לפי $\varphi([1]) = 1$ אינה מגדירה הומומורפיזם ואינה מוגדרת היטב. מצד אחד

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

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

תרגיל 4.6. יהי $f\colon G \to H$ הומומורפיזם. הוכיחו כי לכל $g \in G$ מסדר סופי מתקיים $o(f(g)) | o(g)$.

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

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

ולכן לפי טענה 3.3 נסיק $o(f(g)) | n$. $\square$

תרגיל 4.7. האם כל שתי חבורות מסדר 4 הן איזומורפיות?

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

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

טענה 4.8 (לבית). יהי $f\colon G \to H$ הומומורפיזם. הוכיחו שאם G אבלית, אז $\operatorname{im} f$ אבלית. הסיקו שאם $H \cong G$, אז G אבלית אם ורק אם H אבלית.

תרגיל 4.9. יהי $f\colon G \to H$ הומומורפיזם. הוכיחו שאם G ציקלית, אז $\operatorname{im} f$ ציקלית.

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

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

וקיבלנו כי $x \in \langle f(a) \rangle$, כלומר כל איבר בתמונה הוא חזקה של $f(a)$. □

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

משפט 4.10. כל חבורה ציקלית איזומורפית או ל-$\mathbb{Z}_n$ או ל-$\mathbb{Z}$.

דוגמה 4.11. $n\mathbb{Z} \cong \mathbb{Z}$ ו-$U_{10} \cong \Omega_4 \cong \mathbb{Z}_4$ (למי שפגש את חבורת אוילר).

תרגיל 4.12. האם קיים איזומורפיזם $f\colon S_3 \to \mathbb{Z}_6$?

פתרון. לא, כי S_3 לא ציקלית (היא אפילו לא אבלית) ואילו $\mathbb{Z}_6$ ציקלית.

תרגיל 4.13. האם קיים איזומורפיזם $f\colon (\mathbb{Q}^+, \cdot) \to (\mathbb{Q}, +)$?

פתרון. לא. נניח בשלילה כי f הוא איזומורפיזם, ובפרט $f(a^2) = f(a) + f(a)$ לכל $a \in \mathbb{Q}^+$. 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 4.14. האם קיים אפימורפיזם $f\colon H \to \mathbb{Z}_3 \times \mathbb{Z}_3$ כאשר $H = \langle 5 \rangle \leq \mathbb{R}^*$?

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

תרגיל 4.15. האם קיים מונומורפיזם $f\colon GL_2(\mathbb{Q}) \to \mathbb{Q}^8$?

פתרון. לא. נניח בשלילה שקיים f כזה. נתבונן בצמצום $\overline{f}\colon GL_2(\mathbb{Q}) \to \operatorname{im} f$, שהוא איזומורפיזם (להדגיש כי זהו אפימורפיזם ומפני ש-f חח"ע, אז $\overline{f}$ היא איזומורפיזם). ידוע לנו כי $\operatorname{im} f \le \mathbb{Q}^8$, ולכן $\operatorname{im} f$ אבלית. כלומר גם $GL_2(\mathbb{Q})$ אבלית, שזו סתירה.

מסקנה. יתכנו ארבע הפרכות ברצף.

תרגיל 4.16. מתי ההעתקה $i\colon G \to G$ המוגדרת לפי $i(g) = g^{-1}$ היא אוטומורפיזם?

פתרון. ברור שההעתקה הזו מחבורה לעצמה היא חח"ע ועל. נשאר לבדוק מה קורה אם i שומרת על הפעולה (כלומר היא 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.

4.2 סימן של תמורה וחבורת החילופין

Transposition

הגדרה 4.17. מחזור מאורך 2 ב-S_n נקרא חילוף.

טענה 4.18. כל מחזור $(a_1, a_2, \ldots, a_r)$ ניתן לרשום כמכפלת חילופים

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

תרגיל 4.19 (לדלג)**.** 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, שהרי

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

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

Sign

הגדרה 4.20. יהי σ מחזור מאורך k, אזי הסימן שלו מוגדר להיות:

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

וכדי לחשב את הסימן של כל תמורה ב-S_n, נרחיב את הפונקציה כך שלכל $\tau,\sigma\in S_n$ יתקיים

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

שימו לב שלא הוכחנו שזה מוגדר היטב! יש דרכים שקולות אחרות להגדיר סימן של תמורה, למשל לפי זוגיות מספר החילופים.

Even permutation
Odd permutation

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

דוגמה 4.21. זה חשוב לדעת לחשב סימן של תמורה, אבל זה קצת מבלבל:

1. החילוף (35) הוא תמורה אי זוגית. התמורה $(49)(35)$ היא זוגית.
2. מחזור מאורך אי זוגי הוא תמורה זוגית, למשל (34158).
3. תמורת הזהות היא תמורה זוגית.

Alternating group

הגדרה 4.22. חבורת החילופין (או חבורת התמורות הזוגיות) A_n היא תת־החבורה הבאה של S_n:

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

הערה 4.23. הסדר של A_n הינו $|A_n|=\frac{n!}{2}$. דרך אחרת להוכיח ש-A_n היא תת־חבורה (ואפילו נורמלית) ב-S_n היא לשים לב ש-$A_n=\ker(\operatorname{sign})$, כי הסימן הוא הומומורפיזם.

דוגמה 4.24. $A_3=\{\mathrm{id},(123),(132)\}$. נשים לב כי $A_3=\langle(123)\rangle$, כלומר A_3 ציקלית.

5 תרגול חמישי

5.1 משפט קיילי

Cayley's theorem

משפט 5.1 (משפט קיילי). תהי G חבורה. אז קיים שיכון $G\hookrightarrow S_G$.

הוכחה (בהרצאה). נזכר כי S_X הוא קבוצת הפונקציות ההפיכות ב-X^X יחד עם פעולת ההרכבה, ונקרא חבורת הסימטריה על X. לכל $g\in G$ נתאים פונקציה חח"ע ועל $l_g\in S_G$ לפי כפל משמאל $l_g(a)=ga$. נגדיר פונקציה $\Phi\colon G\hookrightarrow S_G$ לפי $\Phi(g)=l_g$. תחילה נראה ש-Φ הומומורפיזם. כלומר מוכיחים שלכל $g,h\in G$ מתקיים

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

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

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

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

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

לכן $g=h$, ולכן G משוכנת ב-S_G. □

דוגמה 5.2. נבחר $G=S_3$ ונבנה שיכון $S_6 \hookrightarrow G$. נסמן את איברי החבורה שרירותית

$$\{1=\mathrm{id},2=(1\;2\;3)\,,3=(1\;3\;2)\,,4=(1\;2)\,,5=(2\;3)\,,6=(1\;3)\}$$

לכל איבר $g\in G$ נראה לאן כפל משמאל ב-g שולח את כל איברי החבורה - תמורה זו היא התמונה של g ב-S_6. למשל, נחשב את התמונה של $g=(1\;2\;3)$:

$(1\;2\;3)\cdot\mathrm{id}=(1\;2\;3)$, כלומר $1\mapsto 2$, ולכן $l_g(1)=2$.

$(1\;2\;3)\,(1\;2\;3)=(1\;3\;2)$, כלומר $2\mapsto 3$, ולכן $l_g(2)=3$.

$(1\;2\;3)\,(1\;3\;2)=\mathrm{id}$, כלומר $3\mapsto 1$, ולכן $l_g(3)=1$.

$(1\;2\;3)\,(1\;2)=(1\;3)$, כלומר $4\mapsto 6$, ולכן $l_g(4)=6$.

$(1\;2\;3)\,(2\;3)=(1\;2)$, כלומר $5\mapsto 4$, ולכן $l_g(5)=4$.

$(1\;2\;3)\,(1\;3)=(2\;3)$, כלומר $6\mapsto 5$, ולכן $l_g(6)=5$.

ובסך הכל $g\mapsto(1\;2\;3)\,(4\;6\;5)$ לפי המספור שבחרנו. האם תוכלו להראות כי תמונת $(1\;2)$ היא $(1\;4)\,(2\;5)\,(3\;6)$? שימו לב לבזבזנות במשפט קיילי, הרי אנחנו יודעים שיש שיכון $S_3\hookrightarrow S_3$!

מסקנה 5.3. כל חבורה סופית G מסדר n איזומורפית לתת־חבורה של S_n.

מסקנה 5.4. יהי F שדה. כל חבורה סופית G מסדר n איזומורפית לתת־חבורה של $GL_n(F)$.

רמז להוכחה: הראו ש-S_n איזומורפית לתת־חבורה של $GL_n(F)$.
אתגר: מצאו מונומורפיזם $G\hookrightarrow GL_{n-1}(F)$. קודם נסו לשכן את S_n ב-$GL_{n-1}(F)$.

תרגיל 5.5 (רשות). תהי G חבורה מסדר 6. הוכיחו שאם G אבלית, אז $G\cong\mathbb{Z}_6$, ושאם G לא אבלית, אז $G\cong S_3$.

5.2 מחלקות

הגדרה 5.6. תהי G חבורה, ותהי $H\le G$ תת־חבורה. לכל $g\in G$, נגדיר:

- המחלקה השמאלית של g לגבי H היא $gH=\{gh\,|\,h\in H\}\subseteq G$. Left coset
- המחלקה הימנית של g לגבי H היא $Hg=\{hg\,|\,h\in H\}$. Right coset

את אוסף המחלקות השמאליות נסמן G/H.

דוגמה 5.7. 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 5.8. 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 5.9 (אם יש זמן)**.** 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-$G = H \cup (1 + H)$.

הערה 5.10. כפי שניתן לראות מהדוגמאות שהצגנו, המחלקות השמאליות (או הימניות) של תת־חבורה $H \leq G$ יוצרות חלוקה של G. נוסף על כך, היחס

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

של שוויון בין המחלקות של שני איברים $a, b \in G$ הינו יחס שקילות על G. נסכם זאת בעזרת המשפט הבא:

משפט 5.11 (בהרצאה)**.** תהי G חבורה, תהי $H \leq G$ תת־חבורה ויהיו $a, b \in G$. אז

1. $aH = bH$ אם ורק אם $b^{-1}a \in H$. בפרט $aH = H$ אם ורק אם $a \in H$.
2. לכל שתי מחלקות aH ו-bH, מתקיים $aH = bH$ או $aH \cap bH = \varnothing$.
3. האיחוד של כל המחלקות הוא כל החבורה: $\bigcup_{gH \in G/H} gH = G$, וזהו איחוד זר.

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

הערה 5.12 (בהרצאה). קיימת התאמה חח"ע ועל בין המחלקות השמאליות $\{gH \mid g \in G\}$ לימניות $\{Hg \mid g \in G\}$, לפי $(Hg \mapsto g^{-1}H)$:

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

לכן מספר המחלקות השמאליות שווה למספר המחלקות הימניות.

הגדרה 5.13. נסמן את מספר המחלקות של H ב-G בסימון $[G : H]$. מספר זה נקרא האינדקס של H ב-G.

Index of a subgroup

דוגמה 5.14. על פי הדוגמאות שראינו:

1. $[\mathbb{Z} : 5\mathbb{Z}] = 5$
2. $[S_3 : \langle(1\ 2\ 3)\rangle] = 2$
3. $[\mathbb{Z}_8 : \langle 2\rangle] = 2$

הערה 5.15. האינדקס $[G : H]$ הוא מדד לגודל תת־החבורה. ככל שהאינדקס קטן יותר, כך תת־החבורה H גדולה יותר. מקרי הקיצון הם $[G : G] = 1$ ו-$[G : \{e\}] = |G|$.

תרגיל 5.16. מצאו חבורה G ותת־חבורה $H \leq G$, כך ש-$[G : H] = \infty$.

פתרון. תמיד אפשר לבחור חבורה אינסופית G ובתור H את תת־החבורה הטריוויאלית. ננסה לבחור משהו יותר מעניין. תהי $G = (\mathbb{Q}, +)$ ותת־חבורה $H = \mathbb{Z}$.
ניקח שני שברים $\alpha_1, \alpha_2 \in \mathbb{Q}$ שונים בין 0 לבין 1, ונתבונן במחלקות שאיברים אלו יוצרים. נקבל ש-

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

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

5.3 משפט לגראנז'

טענה 5.17. תהי G חבורה ותהי $H \leq G$ תת־חבורה. מתקיים $|aH| = |H|$ לכל $a \in G$.
מפני שמחלקות הן למעשה מחלקות שקילות של יחס על G, אז מייד נקבל את המשפט החשוב הבא.

משפט 5.18 (לגראנז'). תהי G חבורה ותהי $H \leq G$ תת־חבורה. אז $|G| = [G : H] \cdot |H|$.

Lagrange's theorem

מסקנה 5.19. עבור חבורה סופית, הסדר של תת־חבורה מחלק את הסדר של החבורה:

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

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

דוגמה 5.20. עבור $|\mathbb{Z}_{10}| = 10$, הסדרים האפשריים של איברים ב-$\mathbb{Z}_{10}$ הם מהקבוצה $\{1, 2, 5, 10\}$.

תרגיל 5.21. אם G חבורה סופית והמספר $m \in \mathbb{N}$ מחלק את $|G|$, האם בהכרח קיים ב-G איבר מסדר m?

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

דוגמה 5.22. תהי G חבורה מסדר p ראשוני. יהי $e \neq g \in G$. לכן $o(g) > 1$.
מצד שני $o(g) \,\big|\, |G| = p$. לכן בהכרח $o(g) = p$, מה שאומר ש-$G = \langle g \rangle$. מאחר וזה נכון לכל $e \neq g \in G$, נסיק ש-G נוצרת על ידי כל אחד מאיבריה שאינו איבר היחידה.

תרגיל 5.23. תהי G חבורה סופית. הוכיחו כי G מסדר זוגי אם ורק אם קיים ב-G איבר מסדר 2.

פתרון. אם קיים איבר מסדר 2, אז לפי משפט לגראנז', הסדר של איבר מחלק את סדר החבורה ולכן סדר החבורה זוגי.
אם G מסדר זוגי, נשים לב שלאיבר מסדר 2 תכונה יחודית - הוא הופכי לעצמו. נניח בשלילה שאין אף איבר ב-G מסדר 2, כלומר שאין אף איבר שהופכי לעצמו, פרט לאיבר היחידה. אז ניתן לסדר את כל איברי החבורה בזוגות, כאשר כל איבר מזווג לאיבר ההופכי לו (השונה ממנו). יחד עם איבר היחידה נקבל מספר אי זוגי של איברים ב-G, בסתירה להנחה.

מסקנה 5.24. לחבורה מסדר זוגי יש מספר אי זוגי של איברים מסדר 2.

6 תרגול שישי

6.1 מבוא לתורת המספרים

הגדרה 6.1. בהנתן שני מספרים שלמים n, m המחלק המשותף המרבי (ממ"מ) שלהם מוגדר להיות המספר

Greatest common divisor

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

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

Coprime

הערה 6.2. אם $d|a$ וגם $d|b$, אזי d מחלק כל צירוף לינארי $ua + vb$ של a ו-b.

טענה 6.3. אם $n = qm + r$, אז $(n, m) = (m, r)$.

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

משפט 6.4 (אלגוריתם אוקלידס)**.** "המתכון" למציאת ממ"מ בעזרת שימוש חוזר בטענה 6.3 הוא אלגוריתם אוקלידס. ניתן להניח $0 \leq m < n$. אם $m = 0$, אזי $(n, m) = n$. אחרת נכתוב $n = qm + r$ כאשר $0 \leq r < m$ ונמשיך עם $(n, m) = (m, r)$. (הבינו למה האלגוריתם חייב להעצר.)

Euclidean algorithm

דוגמה 6.5. נחשב את הממ"מ של 53 ו-47 בעזרת אלגוריתם אוקלידס

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

ואם יש זמן, דוגמה נוספת עבור מספרים שאינם זרים:

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

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

משפט 6.6 (איפיון הממ"מ כצירוף לינארי מזערי)**.** לכל זוג מספרים שלמים a, b שלא שניהם 0 מתקיים
$$(a, b) = \min\{ua + vb \in \mathbb{N} \mid u, v \in \mathbb{Z}\}$$
בפרט קיימים $s, t \in \mathbb{Z}$ כך ש-$(a, b) = sa + tb$ (הנקראת זהות בֶּזוּ).

תרגיל 6.7. יהיו a, b, c מספרים שלמים כך ש-$(a, b) = 1$ וגם $a|bc$. הראו כי $a|c$.

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

מסקנה 6.8. אם p ראשוני וגם $p|bc$, אז $p|b$ או $p|c$.

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

דוגמה 6.9. כדי למצוא את המקדמים s, t כשמביעים את הממ"מ כצירוף לינארי מזערי נשתמש באלגוריתם אוקלידס המורחב. בכל שלב נביע את השארית באלגוריתם אוקלידס כצירוף לינארי, ונעדכן את הצירוף הלינארי עד שנגיע לממ"מ:

Extended Euclidean algorithm

$$\begin{aligned}
(234, 61) &= [{\scriptstyle 234=3\cdot61+51} \Rightarrow 51 = 234 - 3 \cdot 61] \\
(61, 51) &= [{\scriptstyle 61=1\cdot51+10} \Rightarrow 10 = 61 - 1 \cdot 51 = 61 - 1 \cdot (234 - 3 \cdot 61) = -1 \cdot 234 + 4 \cdot 61] \\
(51, 10) &= [{\scriptstyle 51=5\cdot10+1} \Rightarrow 1 = 51 - 5 \cdot 10 = 51 - 5 \cdot (-1 \cdot 234 + 4 \cdot 61) = 6 \cdot 234 - 23 \cdot 61] \\
(10, 1) &= 1
\end{aligned}$$

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

טענה 6.10. תכונות של ממ"מ:

1. יהי $d = (n, m)$ ויהי e כך ש-$e|m$ וגם $e|n$, אזי $e|d$.
2. $(an, am) = |a|\,(n, m)$ לכל $a \neq 0$.

הוכחה.

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.) □

הגדרה 6.11. בהנתן שני מספרים שלמים n, m הכפולה המשותפת המזערית (כמ"מ) שלהם מוגדרת להיות

Least common multiple

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

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

טענה 6.12. תכונות של כמ"מ:

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

הוכחה.

1. יהיו q,r כך ש-$a = q\,[n,m] + r$ כאשר $0 \le r < [n,m]$. 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

$$|n| = \prod_{i=1}^{k} p_i^{\beta_i} = p_1^{\beta_1}p_2^{\beta_2}\dots p_k^{\beta_k} \qquad |m| = \prod_{i=1}^{k} p_i^{\alpha_i} = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$$

כאשר p_i ראשוניים שונים ו-$\alpha_i,\beta_i \ge 0$ (מתירים 0 כדי שנשתמש באותם ראשוניים ובאותו סדר). כעת צריך להשתכנע כי

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

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

שאלה 6.13 (לדלג). 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.

תרגיל 6.14. תהי G חבורה, ויהי $a\in G$ איבר מסדר סופי n. הוכיחו שלכל d שלם,

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

הוכחה. הטענה היא דרך לחשב את הסדר של כל חזקה של איבר, בהנתן חישוב ממ"מ. תחילה נוכיח היתכנות לסדר: נשים לב כי

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

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

להוכחת המינימליות של הסדר נניח $\left(a^d\right)^t = e$ עבור $t\in\mathbb{N}$. לכן $a^{dt}=e$, ולפי טענה 3.3, נסיק $n|dt$. לכן $\frac{n}{(d,n)}\Big|\frac{dt}{(d,n)}$, וכאמור מדובר במספרים שלמים. מצד שני, ברור כי $\left(\frac{n}{(d,n)},\frac{d}{(d,n)}\right) = 1$, למשל לפי טענה 6.10. לפי תרגיל 6.7 נקבל $\frac{n}{(d,n)}\Big|t$, כמו שרצינו. □

7 תרגול שביעי

7.1 חישוב סדר של איבר

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

$$o\left(ab\right)=[o(a),o(b)]$$

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

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

כי $ab=ba$ ו-n,m מחלקים את $[n,m]$. לפי טענה 3.3 קיבלנו $o(ab)|[n,m]$.
מצד שני, כדי להוכיח מינימליות, אם $(ab)^t=e$, אז $a^t=b^{-t}$. לכן

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

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

טענה 7.2 (אם יש זמן). תהי $G=\langle\alpha\rangle$ ציקלית מסדר n, ויהי $m|n$. אז ל-G יש תת־חבורה ציקלית יחידה מסדר m.

הוכחה. נסמן $H=\left\langle\alpha^{n/m}\right\rangle$. זו תת־חבורה מסדר m, ומכאן שיש קיום. תהי K תת־חבורה ציקלית נוספת מסדר m, ונניח $K=\langle\beta\rangle$. להוכחת היחידות נראה $K=H$.
מאחר ש-α יוצר של G, קיים $b\leq n$ כך ש-$\beta=\alpha^b$. לכן לפי תרגיל 6.14, $o(\beta)=\frac{n}{(n,b)}$.
אבל $o(\beta)=m$ גורר כי $m=\frac{n}{(n,b)}$. לכן $(n,b)=\frac{n}{m}$. לפי תכונת הממ"מ קיימים $s,t\in\mathbb{Z}$ כך ש- $(n,b)=sn+tb$. לכן

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

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

תרגיל 7.3. כמה תת־חבורות שונות יש ל-$\mathbb{Z}_{30}$?

פתרון. לפי הטענה הקודמת, מאחר ומדובר בחבורה ציקלית, מספר תת־החבורות הוא כמספר המחלקים של המספר 30, כלומר: $|\{1,2,3,5,6,10,15,30\}|=8$. הסדרים 1 ו-30 מתאימים לתת־החבורות הטרוויאליות.

מסקנה 7.4 (של טענה 7.1)**.** סדר מכפלות מחזורים זרים ב-S_n הוא הכמ"מ (lcm) של אורכי המחזורים.

דוגמה 7.5. הסדר של $(56)\,(193)$ הוא 6 והסדר של $(56)\,(1234)$ הוא 4.

תרגיל 7.6. מצאו תת־חבורה מסדר 45 ב-S_{15}.

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

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

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

שאלה 7.7. 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}.

תרגיל 7.8 (אם יש זמן)**.** 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 $(12)\,(34)$.
3. סדר 3 - מחזורים מאורך 3, למשל (243).
4. סדר 4 - מחזורים מאורך 4, למשל (2431).

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

תרגיל 7.9 (אם יש זמן)**.** מה הם הסדרים האפשריים לאיברי S_5?

פתרון. ב-S_5 הסדרים האפשריים הם:

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

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

7.2 משפט השאריות הסיני

Chinese remainder theorem

משפט 7.10 (לדלג, משפט השאריות הסיני (סן-צו)). 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. □

דוגמה 7.11 (לדלג). נמצא $x \in \mathbb{Z}$ כך ש-$x \equiv 1 \pmod{3}$ וגם $x \equiv 2 \pmod{5}$. ידוע כי $(5, 3) = 1$, ולכן $-1 \cdot 5 + 2 \cdot 3 = 1$. במקרה זה $n = 5, m = 3$ וכן $s = -1, t = 2$, ולפי משפט השאריות הסיני אפשר לבחור את $x = 1 \cdot (-5) + 2 \cdot 6 = 7$. אכן מתקיים $7 \equiv 1 \pmod{3}$ וגם $7 \equiv 2 \pmod{5}$.

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

משפט 7.12 (לדלג). תהא $\{m_1, \ldots, m_k\}$ קבוצת מספרים טבעיים הזרים בזוגות (כלומר כל זוג מספרים בקבוצה הוא זר). נסמן את מכפלתם ב-m. בהינתן קבוצה כלשהי של שאריות $\{a_i \,(\mathrm{mod} m_i) \,|\, 1 \le i \le k\}$, קיימת שארית יחידה x מודולו m המהווה פתרון למערכת המשוואות

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

דוגמה 7.13 (לדלג). נמצא $y \in \mathbb{Z}$ כך ש-ש-$y \equiv 1 \pmod{3}$, $y \equiv 2 \pmod{5}$ וגם $y \equiv 3 \pmod{7}$. נשים לב שהפתרון $y = 7$ מן הדוגמה הקודמת הוא נכון עד כדי הוספה של 15 ($3 \cdot 5 = 15$ (כי $15 \equiv 0 \pmod{3}$ וגם $15 \equiv 0 \pmod{5}$). לכן את שתי המשוואות $y \equiv 1 \pmod{3}$, $y \equiv 2 \pmod{5}$ ניתן להחליף במשוואה אחת $y \equiv 7 \pmod{15}$. נשים לב כי $(15, 7) = 1$ ולכן אפשר להשתמש במשפט השאריות הסיני בגרסה לזוג משוואות. בדקו כי $y = 52$ מהווה פתרון.

7.3 חבורת אוילר

Multiplicative group of integers modulo n

הגדרה 7.14. המונואיד הכפלי $(\mathbb{Z}_n, \cdot)$ הוא לא חבורה עבור $n > 1$. כדי להציל את המצב, נגדיר את חבורת אוילר להיות $U_n = U(\mathbb{Z}_n)$ לגבי פעולת הכפל מודולו n. הן נקראות על שמו של לאונרד אוילֶר (Leonhard Euler).

דוגמה 7.15. נבנה את לוח הכפל של $\mathbb{Z}_6$ (בהתעלם מ-$[0]$ שתמיד יתן במכפלה $[0]$):

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

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

טענה 7.16 (בהרצאה). יהי $m \in \mathbb{Z}$. אז $[m] \in U_n$ אם ורק אם המחלק המשותף הגדול ביותר של n ו-m הוא 1. כלומר, ההפיכים במונואיד $(\mathbb{Z}_n, \cdot)$ הם כל האיברים הזרים ל-n.

דוגמה 7.17. נתבונן בחבורה $(U_{10}, \cdot)$. לפי הטענה $U_{10} = \{1, 3, 7, 9\}$ (כי אלו המספרים הזרים ל-10 וקטנים ממנו). נראה כי $o(7) = 4$:

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

הערה 7.18. אם p הוא מספר ראשוני, אז $U_p = \mathbb{Z}_p^*$.

דוגמה 7.19. לא קיים ל-5 הופכי כפלי ב-$\mathbb{Z}_{10}$, שכן אחרת 5 היה זר ל-10 וזו סתירה.

תרגיל 7.20. מצאו $0 \le x \in \mathbb{Z}$ כך ש-$61x \equiv 1 \pmod{234}$.

פתרון. ראינו כי $(234, 61) = 1$. נרצה למצוא $k \in \mathbb{Z}$ כך ש-$61x + 234k = 1$. כלומר 1 הוא צירוף לינארי (מינימלי במקרה זה) של 61 ו-234. כלומר k, x הם המקדמים ממשפט איפיון הממ"מ כצירוף לינארי מזערי. לפי הדוגמה הקודמת $1 = 6\cdot 234 - 23\cdot 61$. לכן $x \equiv -23 \pmod{234}$, וכדי להבטיח כי x אינו שלילי נבחר $x = 211$.

מחישוב זה גם קיבלנו $[234] \in U_{61}$. נבצע מודולו 61 למשוואה האחרונה:

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

ומכאן שההופכי של $[51] = [234]$ בחבורה U_{61} הוא $[6]$.

7.4 חישוב פונקציית אוילר

ממשפט לגראנז' עבור החבורה U_n נסיק את המשפט החשוב הבא:

Euler's theorem
Euler's totient function

משפט 7.21 (משפט אוילר)**.** פונקציית אוילר $\varphi\colon \mathbb{N}\to\mathbb{N}$ מוגדרת לפי $\varphi(n)=|U_n|$. עבור כל $a\in U_n$ מתקיים $a^{\varphi(n)}=1 \pmod n$.

דוגמה 7.22. $(3,10)=1$, לכן $3\in U_{10}$. מאחר ש-$U_{10}=\{1,3,7,9\}$, אזי $\varphi(10)=|U_{10}|=4$. אכן מתקיים: $3^{\varphi(10)}=3^4=81=1 \pmod{10}$.

תרגיל 7.23. מצאו את הספרה האחרונה של 333^{333}.

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

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

ומכאן שהספרה האחרונה היא 3.

תרגיל 7.24. תהי G חבורה ציקלית מסדר n. בעזרת תרגיל 6.14 מצאו כמה איברים ב-G יוצרים את G.

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

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

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

Fermat's little theorem

משפט 7.25 (המשפט הקטן של פרמה)**.** זה מקרה פרטי של משפט אוילר: עבור p ראשוני, $|U_p|=p-1$. לכן לכל $a\in U_p$ מתקיים ש-$o(a)|(p-1)$, ובפרט $a^{p-1}=1 \pmod p$.

תרגיל 7.26. נניח וגילו לנו כי $\varphi(100)=40$. חשבו את שתי הספרות האחרונות של המספר 909^{121}.

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

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

איך מחשבים את $\varphi(n)$ למספרים גדולים חוץ מ-100? נפתח נוסחה נוחה שבהנתן פירוק מספר טבעי, נוכל לחשב את מספר המספרים הקטנים ממנו בערך מוחלט וזרים לו.

על פי המשפט היסודי של האריתמטיקה, כל מספר שלם ניתן לפרק למכפלת חזקות של מספרים ראשוניים (עד כדי סדר וסימן). נניח

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

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

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

נזכר במשפט השאריות הסיני או בטענה שלא הוכחה בהרצאה, לפיו אם $(a,b)=1$, אז $\varphi(ab)=\varphi(a)\varphi(b)$. לכן, עבור מספר שלם נקבל

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

ולסיכום

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

דוגמה 7.27. כדי לחשב את $|U_{60}|$, נזכר כי $60=2^2\cdot3\cdot5$ ולכן

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

תרגיל 7.28 (לדלג). חשבו את שתי הספרות האחרונות של $8921467^{1999}+2023$.

פתרון. קל לחשב $\varphi(100)=100\cdot\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=40$. נפעיל $\mathrm{mod}100$ ונקבל

$$\begin{aligned}8921467^{1999}+2023&\equiv67^{1999}+23=67^{50\cdot40-1}+23=\left(67^{40}\right)^{50}\cdot67^{-1}+23\\&=\left(67^{\varphi(100)}\right)^{50}\cdot67^{-1}+23\equiv\left(1\right)^{50}\cdot67^{-1}+23=67^{-1}+23\end{aligned}$$

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 המורחב נציג את $\gcd\left(100,67\right)$ כצירוף לינארי של 67 ו-100:

$$\begin{aligned}(100,67)&=[100=1\cdot67+33]\\(67,33)&=[67=2\cdot33+1]\\(33,1)&=1\end{aligned}$$

ומהצבה לאחור נקבל: $1=67-2\cdot33=-2\cdot100+3\cdot67$, ולכן $x=3$, כלומר ההופכי של 67 הוא 3.

לכן $67^{-1}+23=3+23=26$. כלומר שתי הספרות האחרונות הן 26.

8 תרגול שמיני

8.1 מערכת הצפנה RSA

דוגמה לשימוש מעשי בתורת החבורות הוא מערכת ההצפנה RSA (על שם רון ריבסט, עדי שמיר ולאונרד אדלמן), שמממשת שיטה להצפנה אסימטרית, ובבסיסה מפתח ציבורי. נראה גם דוגמה להרצה של אלגוריתם RSA הנלקחה מויקיפדיה. RSA cryptosystem

טענה 8.1. יהיו p, q ראשוניים שונים, ונסמן $n = pq$. אז חישוב $\varphi(n)$ קשה כמו פירוק n לגורמים ראשוניים.

הוכחה. אם ידוע הפירוק $n = pq$, אז קל לחשב $\varphi(n) = (p-1)(q-1)$. בכיוון השני, נניח כי n ו-$\varphi(n)$ ידועים. נזכר כי מתקיים

$$\begin{aligned} \varphi(n) &= pq - p - q + 1 = n + 1 - (p+q) \\ p + q &= n + 1 - \varphi(n) \end{aligned}$$

במשוואה האחרונה נעזר בחישוב המקדמים של הפולינום הריבועי ששורשיו הם p, q:

$$(x-p)(x-q) = x^2 - (p+q)x + pq = x^2 + (\varphi(n) - n - 1)x + n$$

כעת, מפני ש-n ו-$\varphi(n)$ ידועים לנו, בעזרת נוסחת השורשים נחשב

$$p, q = \frac{-(\varphi(n) - n - 1) \pm \sqrt{(\varphi(n) - n - 1)^2 - 4n}}{2}$$

ואלו פעולות מהירות. $\square$

המטרה: בוב מעוניין לשלוח לאליס הודעה באופן מוצפן.

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

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

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

פענוח: אליס תשחזר מ-c את ההודעה m בעזרת המפתח הסודי

$$c^d \equiv m^{ed} \equiv m \pmod n$$

דוגמה 8.2. נציג דוגמה עם מספרים קטנים מאוד. אליס תגריל למשל את $p = 61$ ו-$q = 53$. היא תחשב

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

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

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

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

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

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

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

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

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

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

נשים לב שכאשר כפלנו ב-m (שורה ראשונה ואחרונה) זה מקביל לסיביות הדלוקות ב-10001_2, ואילו כאשר העלנו בריבוע, זה מקביל למספר הסיביות. בקיצור עשינו שימוש רקורסיבי בהבחנה הפשוטה

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

כך כאשר נחשב m^k עבור k כלשהו, נוכל להסתפק ב-$\lfloor \log_2 k \rfloor$ פעולות של העלאה בריבוע ולכל היותר ב-$\lfloor \log_2 k \rfloor$ הכפלות מודולריות, במקום $k-1$ הכפלות מודולריות בגרסה נאיבית. נסו בבית לחשב את $2790^{2753} \pmod{3233}$ בעזרת שיטה זו.

הערה 8.3 (אזהרה!). יש לדעת שממש לא כדאי להשתמש בפונקציות קריפטוגרפיות שמימשתם לבד לצרכים חשובים. ללא בחינה מדוקדקת על ידי מומחים בתחום לגבי רמת בטיחות ונכונות הקוד, ישנן התקפות רבות שאפשר לנצל לגבי מימושים שכאלו כמו בחירת פרמטרים לא בטוחים, יצירת מפתחות לא בטוחים, התקפת אדם בתווך, התקפת ערוץ צדדי ועוד ועוד.

תרגיל 8.4 (אם יש זמן). מספר ראשוני p נקרא ראשוני בטוח אם הוא מן הצורה $p = 2q+1$ כאשר גם q ראשוני. בוב רוצה לשלוח לאליס מסר מוצפן עם RSA. אליס מצאה ראשוני בטוח $p = 2q+1$, ופרסמה את המפתח הציבורי שלה

$$n = pq = 60031, \ \ e = 4761$$

בוב שלח לה את ההודעה המוצפנת $c \equiv m^e \equiv 19033 \pmod{60031}$. מצאו את ההודעה m שבוב שלח, ובפתרון הסבירו למה קל למצוא את $\varphi(n)$.

פתרון. בחירת הראשוניים של אליס לא הייתה טובה, כי אפשר לפרק את n בעזרת פתרון המשוואה הריבועית הבאה במשתנה q:

$$n = pq = (2q+1)q = 2q^2 + q = 60031$$

שיש לה שני פתרונות $\frac{-1\pm 693}{4} = \frac{-1\pm\sqrt{1+4\cdot 2\cdot 60031}}{2\cdot 2}$ שרק אחד מהם $q = 173$ הוא מספר טבעי, ומכאן ש-$p = 347$. לכן $\varphi(n) = (p-1)(q-1) = 59512$.

כדי למצוא את ההודעה שבוב שלח, תחילה נחשב את d. נריץ את אלגוריתם אוקלידס המורחב

$$\begin{aligned}(\varphi(n), e) = (59512, 4761) &= [59512 = 12\cdot 4761 + 2380]\\ (4761, 2380) &= [4761 = 2\cdot 2380 + 1]\\ (2380, 1) &= 1\end{aligned}$$

ולחישוב המקדמים

$$\begin{aligned}1 &= 1\cdot 4761 - 2\cdot 2380\\ &= 1\cdot 4761 - 2\cdot(59512 - 12\cdot 4761)\\ &= -2\cdot 59512 + 25\cdot 4761\end{aligned}$$

ולכן $d \equiv e^{-1} \equiv 25 \pmod{59512}$. כדי למצוא את ההודעה נחשב את החזקה c^d בעזרת ריבועים. נזכר כי $25 = 11001_2$. לכן

$$c^d = c^{25} = c\cdot c^{24} = c(c^{12})^2 = c((c^6)^2)^2 = c(((c^3)^2)^2)^2 = c(((c\cdot(c)^2)^2)^2)^2$$

ובהצבה מהסוגריים הפנימיים ביותר נקבל

$$\begin{aligned} c\cdot 1 = c^1 &= 19033 \pmod{60031}\\ (c^1)^2 = c^2 &= 19033^2 \equiv 28035 \pmod{60031}\\ c\cdot c^2 = c^3 &= 19033\cdot 28035 \equiv 34627 \pmod{60031}\\ (c\cdot c^2)^2 = c^6 &= 34627^2 \equiv 29966 \pmod{60031}\\ ((c\cdot c^2)^2)^2 = c^{12} &= 29966^2 \equiv 17458 \pmod{60031}\\ (((c\cdot c^2)^2)^2)^2 = c^{24} &= 17458^2 \equiv 4377 \pmod{60031}\\ c(((c\cdot c^2)^2)^2)^2 = c^{25} &= 19033\cdot 4377 \equiv 44444 \pmod{60031} \end{aligned}$$

ולכן ההודעה היא $m \equiv c^d \equiv 44444$.

8.2 בעיית הלוגריתם הבדיד ואלגוריתם דיפי-הלמן

Discrete logarithm problem (DLP)

בעיה 8.5 (בעיית הלוגריתם הבדיד)**.** תהי G חבורה. יהי $g \in G$ ונניח $h = g^x$. המשימה היא למצוא את x בהנתן h. 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 8.6. 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 8.7. 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 $x = hg^{-1} \pmod{n}$.

Baby-step giant-step

טענה 8.8 (צעדי גמד וצעדי ענק). נציג התקפה על בעיית הלוגריתם הבדיד שמראה שיש לבחור פרמטרים גדולים מהמצופה מהתקפה כוחנית נאיבית. ההבחנה החשובה של ההתקפה היא שלמספרים דו־ספרתיים יש שתי ספרות.

הקלט לבעיה, כמו מקודם, הוא חבורה ציקלית $G = \langle g\rangle$ מסדר n ואיבר $h = g^x$. הפלט הוא $0 \le x < n$. נסמן $m = \lceil\sqrt{n}\rceil$, ונשים לב כי $x = im + j$ עבור $0 \le i, j < m$ כלשהם. כלומר הצגנו את x בבסיס m. לכן

$$h = g^x = g^{im+j} = (g^m)^i g^j$$

נתחיל עם בניית טבלה שבה לכל $0 \le j < m$ נוסיף את הערך g^j (צעדי הגמד, בפועל כדאי לאחסן בטבלת גיבוב לפי g^j). לאחר מכן נחשב את g^{-m} בעזרת אלגוריתם אוקלידס המורחב, ונאתחל משתנה $\alpha \leftarrow h$. בלולאה על $0 \le i < m$ נבדוק האם α שייך לטבלה: אם כן וקיים j כך ש-$\alpha = g^j$ נחזיר את התשובה $x = im + j$, ואם לא נמשיך עם $\alpha \leftarrow \alpha g^{-m}$ (צעדי הענק) לאיטרציה הבאה בלולאה.

ניתן כמובן לבחור ערך שונה עבור m כדי לאזן באופן שונה את סיבוכיות הזמן והמקום. כך נקבל שלאלגוריתם הזה יש סיבוכיות מקום של $O(m)$ עבור הטבלה וסיבוכיות זמן של $O(\frac{n}{m})$ עבור הלולאה שבה רצים על $0 \le i < \frac{n}{m}$. אפשר גם לבחור בגרסה שבה מאחסנים בטבלה את צעדי הענק, ורצים על צעדי הגמד.

דוגמה 8.9. נתון לנו כי 101 ראשוני, שהחבורה $G = U_{101}$ היא ציקלית ושהאיבר $g = 7$ הוא יוצר שלה. לכן קל לחשב $n = o(7) = |G| = \varphi(101) = 100$. נרצה למצוא x כך ש-$h = 88 \equiv 7^x \pmod{101}$.

נסמן $m = \lceil \sqrt{100} \rceil = 10$. נחשב את כל החזקות g^j עבור $0 \le j < m$:

j	0	1	2	3	4	5	6	7	8	9
7^j	1	7	49	40	78	41	85	90	24	67

כמו כן נחשב $7^{-1} \equiv 29 \pmod{101}$ לפי אלגוריתם אוקלידס המורחב, ואז בעזרת חישוב עם ריבועים נמצא את $g^{-m} = 7^{-10} \equiv 29^{10} \equiv 14 \pmod{101}$.

נאתחל $\alpha \leftarrow 88$. עבור $i = 0$, נשים לב כי α לא נמצא בשורה השנייה בטבלה. נחשב $\alpha \leftarrow 14\alpha = 20$ ונמשיך עם $i = 1$. גם עכשיו α לא נמצא בשורה השנייה בטבלה. נחשב $\alpha \leftarrow 14\alpha = 78$ ונמשיך עם $i = 2$. נשים לב כי עבור $j = 4$ מצאנו כי α מופיע בטבלה. לכן $x = 10 \cdot 2 + 4 = 24$ ותוכלו בבית לוודא כי $88 \equiv 7^{24} \pmod{101}$.

הטבלה שחישבנו פעם אחת שימושית לכל הרצה נוספת ואינה ספציפית ל-h.

Diffie-Hellman key exchange

טענה 8.10 (פרוטוקול דיפי-הלמן). תהי חבורה ציקלית $G = \langle g \rangle$ מסדר n, הידועה לכל. מקובל לבחור את U_p עבור p ראשוני גדול מאוד (יותר מאלף ספרות בינאריות) או תת־חבורה של עקום אליפטי.

לכל משתמש ברשת יש מפתח פרטי סודי, שהוא מספר טבעי $a \in [2, n-1]$ ומפתח ציבורי g^a. איך שני משתמשים, אליס ובוב, יתאמו ביניהם סוד משותף?

1. אליס מגרילה מפתח פרטי a ובוב מגריל b. אז אליס שולחת לבוב את המפתח הציבורי שלה g^a והוא שולח לה את g^b.
2. אליס מחשבת את $\left(g^b\right)^a$, שהרי יש לה את g^b ואת a, ובוב מחשב את $(g^a)^b$.

כעת הם יכולים להשתמש בסוד המשותף $g^{ab} = \left(g^b\right)^a = (g^a)^b$ כדי להצפין הודעות, למשל כמפתח להצפנה סימטרית.

הערה 8.11. 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 למניעת התקפה זו.

דוגמה 8.12. נריץ את האלגוריתם עם מספרים קטנים (באדיבות ויקיפדיה). יהי $p = 23$. נבחר יוצר $U_{23} = \langle 5 \rangle$.

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

9 תרגול תשיעי

9.1 אלגוריתם מילר-רבין לבדיקת ראשוניות

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

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

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

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 $a^{N-1} \equiv 1 \pmod{N}$, אז השורש הריבועי שלו $a^{(N-1)/2}$ הוא ± 1. כעת, אם $(N-1)/2$ זוגי, נוכל להמשיך לקחת שורש ריבועי. אז בהכרח יתקיים $a^M \equiv 1 \pmod{N}$ או $a^{2^j M} \equiv -1 \pmod{N}$ עבור $0 \leq j < s$ 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. Strong witness

טענה 9.1 (אלגוריתם מילר-רבין). הקלט הוא מספר אי זוגי $N > 9$, ופרמטר k הקובע את דיוק המבחן. Miller-Rabin primality test

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

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

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

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

נחשב $x \leftarrow x^2$.

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

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

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

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

תרגיל 9.2 (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 השערת 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 9.3. 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 או 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 9.4. 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. אכן $781 = 11 \cdot 71$.

9.2 תת־חבורות נורמליות

הגדרה 9.5. תת־חבורה $H \leq G$ נקראת תת־חבורה נורמלית אם לכל $g \in G$ מתקיים $gH = Hg$. במקרה זה נסמן $H \lhd G$. Normal subgroup

משפט 9.6. תהי תת־חבורה $H \leq G$. התנאים הבאים שקולים:

1. $H \lhd G$.
2. לכל $g \in G$ מתקיים $gHg^{-1} = H$.
3. לכל $g \in G$ מתקיים $gHg^{-1} \subseteq H$.
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 $gHg^{-1} \subseteq H$ וגם $g^{-1}Hg \subseteq H$ נקבל כי

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

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

דוגמה 9.7. אם G חבורה אבלית, אז כל תת־החבורות שלה הן נורמליות. הרי אם $h \in H \leq G$, אז $g^{-1}hg = h \in H$. ההפך לא נכון. ברמת האיברים נורמליות **לא** שקולה לכך ש-$gh = hg$!

דוגמה 9.8. מתקיים $SL_n(F) \lhd GL_n(F)$. אפשר לראות זאת לפי הצמדה. יהי $A \in SL_n(F)$, אז לכל $g \in GL_n(F)$ מתקיים

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

ולכן $g^{-1}Ag \in SL_n(F)$.
דרך אחרת להוכחה היא לשים לב כי $SL_n(F)$ היא הגרעין של ההומומורפיזם $\det\colon GL_n(F) \to F^*$. אתגר: הסיקו מדוגמה זו כי $A_n \lhd S_n$.

דוגמה 9.9. תת־החבורה $S_n \leq \langle(1\ 2)\rangle$ אינה נורמלית כי $(2\ 3)\ \langle(1\ 2)\rangle \neq \langle(1\ 2)\rangle\ (2\ 3)$.

טענה 9.10. תהי $H \leq G$ תת־חבורה מאינדקס 2. אזי $H \lhd G$.

הוכחה. למי ששכח $[G:H] = |G/H| = 2$. אנו יודעים כי יש רק שתי מחלקות שמאליות של H בתוך G, ורק שתי מחלקות ימניות. אחת מן המחלקות (מכל צד) היא $H = eH = He$. מכיוון ש-G היא איחוד של המחלקות של H, אז המחלקה השמאלית והמחלקה הימנית האחרת היא ההפרש $G \setminus H$.

אם $a \in H$, אז $aH = H = Ha$, ואם $a \notin H$, אז בהכרח $aH = G \setminus H = Ha$.
כלומר לכל $a \in G$ מתקיים $aH = Ha$, ולכן $H \lhd G$. □

מסקנה 9.11. מתקיים $\langle\sigma\rangle \lhd D_n$ כי לפי משפט לגראנז' $[D_n : \langle\sigma\rangle] = \frac{2n}{n} = 2$.
זו גם דרך אחרת לראות למה $A_n \lhd S_n$, שהרי $[S_n : A_n] = 2$.

הערה 9.12. אם $G \leq H \leq K$ 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 $D_4 \rhd \langle\tau, \sigma^2\rangle \rhd \langle\tau\rangle$ לפי הטענה הקודמת, אבל ראינו כי $\langle\tau\rangle$ לא נורמלית ב-D_4. נסו למצוא הפרכה דומה ב-S_4.

תרגיל 9.13. תהי G חבורה. יהיו $H, N \leq G$ תת־חבורות. נגדיר מכפלה של תת־חבורות להיות

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

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

פתרון. חבורה היא סגורה להופכי, כלומר $H^{-1} = H$, 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 $nh = hn$! אלא שקיימים $n' \in N$ וגם $h' \in H$ כך ש-$nh = h'n'$.

נשים לב כי $HN \neq \varnothing$ שהרי $e = e \cdot e \in HN$. 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:

$$HNHN = HHNN = HN$$
$$h_1 n_1 h_2 n_2 = h_1 h_2' n_1' n_2 = h_3 n_3$$

וסגירות להופכי

$$(HN)^{-1} = N^{-1}H^{-1} = NH = HN$$
$$(h_1 n_1)^{-1} = n_1^{-1} h_1^{-1} = n_2 h_2 = h_2' n_2'$$

ולכן $HN \leq G$.

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 9.14. הגדרנו בתרגיל בית את הַמֶּרְכָּז של חבורה G להיות Center

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

דהיינו זהו האוסף של כל האיברים ב-G שמתחלפים עם כל איברי G. שימו לב שתמיד $Z(G) \lhd G$ ובנוסף $Z(G)$ אבלית. הבינו למה כל תת־חבורה $K \leq Z(G)$ היא נורמלית לא רק ב-$Z(G)$, אלא גם ב-G. האם תת־חבורה נורמלית היא בהכרח אבלית? כבר ראינו שלא, למשל עבור $SL_2(\mathbb{R}) \lhd GL_2(\mathbb{R})$.

10 תרגול עשירי

10.1 חבורות מנה

נתבונן באוסף המחלקות השמאליות $\{gH \,|\, g \in G\} = {}^{G}\!/_{H}$ של תת־חבורה $H \leq G$. אפשר להגדיר על אוסף זה את הפעולה הבאה:

$$(aH)\,(bH) \coloneqq abH \in {}^{G}\!/_{H}$$

פעולה זו מוגדרת היטב (ודאו!) אם ורק אם $H \lhd G$. במקרה כזה, איבר היחידה בחבורה זו הוא $eH = H$ והחבורה ${}^{G}\!/_{H}$ נקראת חבורת המנה של G ביחס ל-H, ולעיתים נקרא זאת "G מודולו H". מקובל גם הסימון G/H. Quotient group, or factor group

דוגמה 10.1. $\mathbb{Z}$ 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 $k + n\mathbb{Z} \mapsto k \pmod{n}$. שימו לב כי ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ אינה תת־חבורה של $\mathbb{Z}$, למשל כי האיברים שונים (או כי אין ב-$\mathbb{Z}$ איברים מסדר סופי, פרט לאיבר היחידה).

דוגמה 10.2. לכל חבורה G יש את תת־החבורות $\{e\}$ ו-G. ברור כי $[G:G] = 1$, כלומר יש רק איבר אחד בחבורה ${}^{G}\!/_{G} = \{G\}$. בפרט, יש איזומורפיזם ${}^{G}\!/_{G} \cong \{e\}$. למה G היא תת־חבורה נורמלית? למשל כי ההומומורפיזם הטריוויאלי $f\colon G \to G$ המוגדר לפי $g \mapsto e$ מקיים $\ker f = G$.

האיברים בחבורה ${}^{G}\!/_{\{e\}}$ הם מן הצורה $g\,\{e\} = \{g\}$. ישנו איזומורפיזם $f\colon {}^{G}\!/_{\{e\}} \to G$ לפי $g\,\{e\} \mapsto g$. ודאו שאתם מבינים למה זה אכן איזומורפיזם. גם כאן קל לראות שהגרעין של העתקת הזהות $\mathrm{id}\colon G \to G$ הוא $\{e\}$, ולכן מדובר בתת־חבורה נורמלית של G.

דוגמה 10.3. תהי $G=\mathbb{R}\times\mathbb{R}$, ונתבונן ב-$H=\mathbb{R}\times\{0\}\lhd G$. האיברים בחבורת המנה הם

$$^{G}/_{H}=\{(a,b)+H\,|\,(a,b)\in G\}=\{(0,b)+H\,|\,b\in\mathbb{R}\}=\{\mathbb{R}\times\{b\}\,|\,b\in\mathbb{R}\}$$

כלומר אלו הם הישרים המקבילים לציר ה-x.

הערה 10.4. עבור חבורה סופית G ותת־חבורה $H\lhd G$ מתקיים כי

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

תרגיל 10.5. 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

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

כלומר קיבלנו $a^n\in H$.

תרגיל 10.6. תהי $H\leq G$ תת־חבורה מאינדקס 2. הוכיחו כי $^{G}/_{H}$ היא חבורה ואבלית.

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

1. אם $T\leq G$ (למשל אם G אבלית), אז $T\lhd G$.
2. בנוסף, בחבורת המנה G/T איבר היחידה הוא היחיד מסדר סופי.

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

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

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.

10.2 משפטי האיזומורפיזמים של נתר

שלושת משפטי האיזומורפיזמים של נתר לחבורות הם משפטים יסודיים המקשרים בין הומומורפיזמים, חבורות מנה ותת־חבורות נורמליות. יש משפטים דומים למבנים אלגבריים אחרים, כולל הכללות בתחום של אלגברה אוניברסלית. בתרגול נעסוק רק במשפט האיזומורפיזמים הראשון, שהוא העיקרי והשימושי מבין משפטי האיזומורפיזמים (את האחרים מוכיחים בעזרתו). למעשה, הוא כה שימושי שכאשר נרצה להוכיח איזומורפיזם בין חבורת מנה לחבורה אחרת, כמעט תמיד נשתמש בו.

First isomorphism theorem

משפט 10.8 (משפט האיזומורפיזמים הראשון)**.** יהי הומומורפיזם $f\colon G \to H$. אז

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

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

תרגיל 10.9. תהי $G = \mathbb{R} \times \mathbb{R}$, ותהי $H = \{(x,y) \in \mathbb{R}\times\mathbb{R} \mid y = 3x\}$. הוכיחו כי $G/H \cong \mathbb{R}$.

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

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

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

לפי משפט האיזומורפיזמים הראשון, נקבל את הדרוש. □

תרגיל 10.10. נסמן $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$. הראו שזו חבורה כפלית וכי $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$.

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

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

ברור כי $\operatorname{im} f \subseteq \mathbb{T}$. כל $z \in \mathbb{T}$ ניתן לכתוב כ-$e^{2\pi i x}$ עבור $x \in \mathbb{R}$ כלשהו, ולכן $\operatorname{im} f = \mathbb{T}$, מה שמראה שהיא תת־חבורה של $\mathbb{C}^*$. נחשב את הגרעין:

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

לפי משפט האיזומורפיזמים הראשון, נקבל $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$. □

תרגיל 10.11. תהיינה G_1 ו-G_2 חבורות סופיות כך ש-$(|G_1|, |G_2|) = 1$. מצאו את כל ההומומורפיזמים $f\colon G_1 \to G_2$.

פתרון. נניח כי $f\colon G_1 \to G_2$ הומומורפיזם. לפי משפט האיזומורפיזמים 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, $\operatorname{im} f \le G_2$, 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 10.12. יהי הומומורפיזם $f\colon \mathbb{Z}_{14} \to \mathbb{Z}_{20}$. 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 האיזומורפיזמים הראשון נקבל $\mathbb{Z}_{14}/K \cong \operatorname{im} f$. לכן $\mathbb{Z}_{14} \cong \operatorname{im} f$. ידוע לנו כי $\operatorname{im} f \leq \mathbb{Z}_{20}$ ולכן $|\operatorname{im} f| \mid |\mathbb{Z}_{20}| = 20$. 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 $H = 10\mathbb{Z}_{20}$ (יש שרק תת־חבורה אחת מסדר 2) של $\mathbb{Z}_{20}$, ונבנה אפימורפיזם $\mathbb{Z}_{14} \to H \leq \mathbb{Z}_{20}$. המספרים האי זוגיים ישלחו ל-10, והזוגיים ל-0. כמו כן, כיוון שהגרעין הוא מסדר ראשוני, אז $K \cong \mathbb{Z}_7$.

אם $|K| = 14$, אז נקבל $K = \mathbb{Z}_{14}$. זה מתקבל רק עבור ההומומורפיזם הטריוויאלי.

תרגיל 10.13. 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

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

(לפי הציקליות). אם כן, מתקיים

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

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

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

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

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

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

מסקנה 10.14. אנחנו יודעים כי G אבלית אם ורק אם $Z(G)=G$. לכן אם $G/Z(G)$ ציקלית, אז היא טריוויאלית, כי במקרה כזה נקבל $G/Z(G)=G/G=\{G\}$.

הגדרה 10.15. תהי G חבורה, ויהי $a\in G$. האוטומורפיזם $\gamma_a\colon G\to G$ המוגדר לפי $\gamma_a(g)=aga^{-1}$ נקרא אוטומורפיזם פנימי. נסמן

Inner automorphism

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

החבורה הזו נקראת חבורת האוטומורפיזמים הפנימיים של G.

Inner automorphism group

תרגיל 10.16. הוכיחו כי $\gamma_a\circ\gamma_b=\gamma_{ab}$, וכי $\gamma_a^{-1}=\gamma_{a^{-1}}$. הסיקו כי $\operatorname{Inn}(G)$ היא חבורה עם פעולת ההרכבה.

הוכחה. לכל $g\in G$ מתקיים

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

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

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

שמוכיח שההופכי של אוטומורפיזם פנימי הוא אוטומורפיזם פנימי. $\square$

תרגיל 10.17. הוכיחו כי לכל חבורה G,

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

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

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

לפי משפט האיזומורפיזמים הראשון, נקבל $G/Z(G)\cong\operatorname{Inn}(G)$. כמסקנה מתרגיל 10.13 נסיק כי אם $\operatorname{Inn}(G)$ ציקלית, אז היא טריוויאלית. $\square$

11 תרגול אחד עשר

11.1 מבוא לקודים לינאריים

תורת הקידוד מראה כיצד ניתן להעביר הודעות בתוך רועש ולוודא שלא נפלו בהן שגיאות, בהתאם לסיכוי לשגיאה ולעיתים גם לתקן שגיאות.

אצלנו תמיד נרצה להעביר הודעות שהן איברים של $\mathbb{Z}_2^k$, כלומר וקטורים באורך קבוע של k סיביות. לכל הודעה מסוג אחר נצטרך להתאים וקטור (או יותר) ב-$\mathbb{Z}_2^k$. המקודד שלנו יתאים לכל איבר של $\mathbb{Z}_2^k$ איבר של $\mathbb{Z}_2^n$, כמובן כאשר $n\geq k$.

הגדרה 11.1. קוד הוא תת־קבוצה של $\mathbb{Z}_2^n$. כל איבר שלו נקרא מילת קוד, ובקיצור מילה.

Code
Codeword

הגדרה 11.2. קוד שהוא מרחב האפסים של מטריצה $H \in M_{k,n}(\mathbb{Z}_2)$ נקרא קוד לינארי.

Linear Code

טענה 11.3. קוד $C \subseteq \mathbb{Z}_2^n$ הוא לינארי אם ורק אם C הוא תת־חבורה של $\mathbb{Z}_2^n$. אם C הוא קוד לינארי, אז כל איבר הוא ההופכי של עצמו ואיבר היחידה הוא וקטור האפס. אגב, עבור p ראשוני, כל תת־חבורה של $\mathbb{Z}_p^n$ היא מרחב וקטורי.

בהרצאה ראיתם דרך נוחה להגדיר קודים לינאריים המאפשרים גם פיענוח יעיל. נסמן ב-I_d מטריצת יחידה בגודל $d \times d$. לכל מטריצה $A \in M_{n-k,k}(\mathbb{Z}_2)$ נגדיר שתי מטריצות בלוקים

$$G = \begin{pmatrix} I_k \\ A \end{pmatrix} \in M_{n,k}(\mathbb{Z}_2) \qquad\qquad H = \begin{pmatrix} A & I_{n-k} \end{pmatrix} \in M_{n-k,n}(\mathbb{Z}_2)$$

כאשר G מצורה כזו נקראת מטריצה יוצרת תקנית של הקוד ו-H נקראת מטריצת בדיקת זוגיות קנונית של הקוד. נקודד וקטור $x \in \mathbb{Z}_2^k$ לוקטור $Gx \in \mathbb{Z}_2^n$. כלומר הקוד שלנו הוא $C = \left\{ Gx \;\middle|\; x \in \mathbb{Z}_2^k \right\}$. שימו לב שהוקטור Gx מתחיל בוקטור x בתוספת $n-k$ סיביות של יתירות. המטריצה H תבדוק את תקינות המילה: מתקיים $v \in C$ אם ורק אם $Hv = 0$. בכתיב מטריצות זה אומר ש-$HG = 0$.

Standard generator matrix
Canonical pairty-check matrix

דוגמה 11.4. נתבונן במטריצה יוצרת תקנית

$$G = \begin{pmatrix} I_k \\ 1 \cdots 1 \end{pmatrix}$$

מטריצה זו מגדירה קוד המוסיף סיבית זוגיות. בפיענוח הקוד נקבל אפס אם ורק אם ב-Gx יש מספר זוגי של אחדות. שימו לב שהקוד הזה לא יצליח לזהות שגיאה בודדת (אבל הוא מוסיף רק סיבית בודדת).

הערה 11.5. מפני שהקידוד שלנו הוא חח"ע, לכל וקטור $x \in \mathbb{Z}_2^k$ יש וקטור יתירות u יחיד כך ש-$\left(\begin{smallmatrix} x \\ u \end{smallmatrix}\right) \in C$. לכן אם אנחנו יודעים שאירעו שגיאות רק בחלק של היתירות, תמיד נוכל לזהות אותן. כעת נראה כמה שגיאות יכולות להפוך מילת קוד אחת לאחרת, וכמה שגיאות לא יאפשרו לנו פיענוח יחיד.

הגדרה 11.6. משקל המינג של וקטור $v \in \mathbb{Z}_2^n$ הוא מספר האחדות שבו. מרחק המינג $d(u,v)$ בין שני וקטורים $u, v \in \mathbb{Z}_2^n$ הוא מספר השורות השונות ביניהם. מפני שאנחנו עובדים מעל השדה $\mathbb{Z}_2$ ניתן לחשב את $d(u,v)$ על ידי חישוב משקל המינג של $u - v$.

Hamming weight
Hamming distance

דוגמה 11.7. מרחק המינג של (1100) מ-(0111) הוא

$$d((1100),(0111)) = 3$$

וזה בדיוק משקל המינג של $(1100) - (0111) = (1011)$.

Distance

הגדרה 11.8. המרחק $d_{\min}$ של קוד הוא המרחק המינימלי בין שתי מילות קוד שונות.

טענה 11.9. בקוד לינארי המרחק $d_{\min}$ שווה למשקל המינימלי של מילות קוד שאינן וקטור האפס.

טענה 11.10. יהי C קוד לינארי עם מרחק $d_{\min}$. אם $d_{\min} \geq 2d+1$, אז C יצליח לזהות $2d$ שגיאות ולתקן d שגיאות.

בפרט, קוד מסוגל לזהות לפחות שגיאה אחת אם ורק אם אין ב-H עמודת אפסים.

תרגיל 11.11. תהי מטריצה

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

חשבו את $d_{\min}$ של הקוד שהוא מרחב האפסים של H, והסבירו כמה שגיאות ניתן לזהות וכמה ניתן לתקן.

פתרון. אם נסכום את העמודות הראשונה, השנייה והרביעית נקבל 0. כלומר יש וקטור v ששייך למרחב האפסים של H (ולכן הוא מילת קוד) שהוא

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

לכן $d_{\min} \leq 3$, כי המשקל של v הוא 3, וכאמור v הוא מילת קוד. בהרצאה ראיתם מסקנה לטענה הקודמת לפיה $d_{\min} \geq 3$ אם ורק אם אין ב-H עמודת אפסים ואין בה עמודות זהות. זה בדיוק המצב אצלנו ולכן $d_{\min} = 3$. לפי הטענה נסיק כי ניתן לזהות עד שתי שגיאות ולתקן עד שגיאה אחת.

כיצד מתקנים שגיאה? נניח ואירעה שגיאה אחת בדיוק במילת קוד v. כלומר סיבית אחת שונה במילה שקיבלנו, נניח הסיבית במקום i, ובמקום לקבל את v קיבלנו את $v + e_i$. נכפיל ב-H ונקבל

$$H(v + e_i) = 0 + He_i = C_i(H)$$

שהיא העמודה ה-i של H. כך נגלה שהשגיאה אירעה בסיבית i של v. אילו היו כמה עמודות זהות ב-H, אז לא נוכל לדעת היכן השגיאה אירעה, ולכן גם לא נוכל לתקן אותה. התיקון עצמו הוא ברור: להחזיר $v = (v + e_i) + e_i$.

דוגמה 11.12. נבחר את המטריצה $A = \left(\begin{smallmatrix}1&0&1\\0&1&0\end{smallmatrix}\right)$. לכן

$$G = \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\\1&0&1\\0&1&0\end{pmatrix} \qquad\qquad H = \begin{pmatrix}1&0&1&1&0\\0&1&0&0&1\end{pmatrix}$$

נרצה לשלוח את ההודעה $x = 011$. נקודד אותה למילת הקוד

$$v = Gx = \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\\1&0&1\\0&1&0\end{pmatrix}\begin{pmatrix}0\\1\\1\end{pmatrix} = \begin{pmatrix}0\\1\\1\\1\\1\end{pmatrix}$$

וברור כי $Hv = \left(\begin{smallmatrix}0\\0\end{smallmatrix}\right)$, שהרי מדובר במטריצת בדיקת הזוגיות של קוד לינארי. במקרה זה $d_{\min} = 2$ כי אין ב-H עמודת אפסים, אבל יש שתי עמודות זהות. כלומר ניתן לזהות שגיאה אחת, אבל לא לתקן שגיאות. נניח שאירעה שגיאה ונתקבלה המילה $v' = 11111$. נבדוק כי

$$Hv' = \begin{pmatrix}1&0&1&1&0\\0&1&0&0&1\end{pmatrix}\begin{pmatrix}1\\1\\1\\1\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} \neq \begin{pmatrix}0\\0\end{pmatrix}$$

ולכן נסיק כי אירעה שגיאה, אך לא נוכל לתקן אותה, כי יש שתי עמודות $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$ ב-H. אילו נעשו שתי שגיאות (או יותר), יתכן והיינו מקבלים $Hv' = 0$, ולא נוכל לזהות שבכלל אירעה שגיאה.

12 תרגול שניים עשר

12.1 קודים פולינומיים

נתחיל בקצת רקע מתורת החוגים:

הגדרה 12.1. חוג $(R, +, \cdot, 0, 1)$ הוא מבנה אלגברי המקיים: Ring

1. $(R, +, 0)$ הוא חבורה אבלית. נקראת החבורה החיבורית של החוג.

2. $(R, \cdot, 1)$ הוא מונואיד.

3. מתקיים חוג הפילוג (משמאל ומימין). כלומר לכל $a, b, c \in R$ מתקיים

$$(a+b)c = ac + bc, \qquad a(b+c) = ab + ac$$

כאשר ההקשר ברור, נכתוב רק R במקום $(R, +, \cdot, 0, 1)$.

דוגמה 12.2. כל שדה $(F, +, \cdot, 0, 1)$ כמו $\mathbb{R}$ או $\mathbb{C}$ הוא דוגמה לחוג. שדה הוא דוגמה לחוג חילופי, כלומר שפעולת הכפל בחוג היא חילופית. ישנם חוגים לא חילופיים כמו $M_2(\mathbb{Q})$ עם חיבור וכפל מטריצות, שהוא בוודאי אינו שדה. ישנם חוגים חילופיים שאינם שדות (כי לא כל האיברים הפיכים), כמו $\mathbb{Z}$ עם חיבור וכפל רגילים, או חוג הפולינומים הממשיים במשתנה אחד $\mathbb{R}[t]$ עם חיבור וכפל של פולינומים.

אפשר להגדיר הומומורפיזם של חוגים $\varphi \colon R \to S$ בדיוק כמו שמצפים. לגרעין של הומומורפיזם של חוגים קוראים אידאל (דו־צדדי), שדומה בתפקידו לתת־חבורות נורמליות בחבורות. דרך שקולה להגדיר אידאל: נאמר כי $I \subseteq R$ הוא אידאל אם הוא תת־חבורה חיבורית ולכל $r \in R$ ו-$i \in I$ מתקיים $ri, ir \in I$. במקרה כזה נסמן $I \lhd R$. אידאל נקרא ראשי אם הוא מן הצורה $\langle r \rangle = \{arb \mid a, b \in R\}$ עבור איזשהו $r \in R$. אידאלים מאפשרים להגדיר חוג מנה: (Two-sided) Ideal

הגדרה 12.3. יהי $I \lhd R$ אידאל. חוג המנה של R ביחס ל-I הוא הקבוצה Quotient ring

$$R/I = \{a + I \mid a \in R\}$$

עם פעולות החיבור $(a+I)+(b+I) = (a+b)+I$ והכפל $(a+I)(b+I) = ab+I$. איבר האפס הוא $0_R + I = I$ ואיבר היחידה הוא $1_R + I$.

כעת נראה שיטת קידוד בעזרת חוג הפולינומים $\mathbb{Z}_2[x]$. כל איבר $f(x)$ בחוג הוא מן הצורה

$$f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$$

עבור $a_i \in \mathbb{Z}_2$. המעלה של f, המסומנת $\deg f$, היא החזקה n הכי גבוהה של x עבורה $a_n \neq 0$. Degree

טענה 12.4 (חלוקה אוקלידית לפולינומים). יהי F שדה ויהיו $f(x), g(x) \in F[x]$. אז קיימים פולינומים יחידים $q(x), r(x) \in F[x]$ כך ש-$\deg r(x) < \deg g(x)$ ומתקיים $f(x) = q(x)g(x) + r(x)$.

מכאן גם קצרה הדרך לחישוב ממ"מ של פולינומים עם אלגוריתם אוקלידס.

כל וקטור ב-$\mathbb{Z}_2^{n+1}$ נציג על ידי פולינום שמעלתו היא לכל היותר n, שמקדמיו הם רכיבי הוקטור לפי סדר. למשל את 011001 נייצג עם הפולינום $x^4 + x^3 + 1$. להגדרת קוד פולינומי נבחר $g(x) \in \mathbb{Z}_2[x]$ ממעלה m הנקרא הפולינום היוצר של הקוד. Polynomial code

נניח שנרצה לשלוח את הוקטור שמתאים לפולינום $f(x)$. אז נכפול אותו ב-x^m ונבצע חילוק עם שארית של $f(x) \cdot x^m$ ב-$g(x)$. לכן קיימים פולינומים $q(x), r(x) \in \mathbb{Z}_2[x]$ כך שמתקיים

$$f(x) \cdot x^m = q(x)g(x) + r(x)$$

וגם $\deg r(x) < \deg g(x)$. מילת הקוד שנשלח היא הוקטור שמתאים ל-$f(x) \cdot x^m -$ $r(x)$.

כלומר מילה $v \in \mathbb{Z}_2[x]$ היא מילת קוד אם ורק אם $g(x)|v$ אם ורק אם $v \in \langle g(x) \rangle$ (שייכת לאידאל הנוצר על ידי $g(x)$).

הערה 12.5. קוד פולינומי הוא קוד לינארי (שאפשר להבטיח לגביו יותר תכונות). קוד זה מוסיף m סיביות של יתירות. בפועל לא שולחים פולינום $f(x)$ כללי, אלא מגבילים את המעלה שלו עד k נתון.

דוגמה 12.6. נבחר $g(x) = x^3 + x^2 + x$ ונקודד את הוקטור 1101. הוקטור הזה מתאים לפולינום $f(x) = x^3 + x^2 + 1$. נבצע חלוקת פולינומים ונקבל

$$f(x) \cdot x^3 = x^6 + x^5 + x^3 = (x^3 + x)g(x) + x^2$$

כלומר השארית היא $r(x) = x^2$. נשלח את וקטור המקדמים של

$$f(x) \cdot x^3 - r(x) = x^6 + x^5 + x^3 + x^2$$

שהוא 1101100. פולינום זה בודאי מתחלק ב-$g(x)$, לפי בנייתו, ולכן הוא מילת קוד "חוקית".

נניח והתקבל הוקטור 1001110. האם הוא מילת קוד? הפולינום המתאים לו הוא $x^6 + x^3 + x^2 + x$, ושארית החלוקה שלו ב-$g(x)$ היא $x^2 + x$, ולכן זו אינה מילת קוד "חוקית".

הגדרה 12.7. קוד נקרא ציקלי אם לכל מילת קוד $(a_1, a_2, \ldots, a_n) \in \mathbb{Z}_2^n$ גם ההסטה המעגלית שלה $(a_n, a_1, a_2, \ldots, a_{n-1})$ היא מילת קוד. Cyclic code

תרגיל 12.8. האם הקוד הבא עם מטריצה יוצרת תקנית

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

הוא ציקלי?

פתרון. ההודעות ב-$\mathbb{Z}_2^3$ יקודדו למילות הקוד הבאות

$$\begin{aligned} (000) &\mapsto (000000) & (001) &\mapsto (001001) \\ (100) &\mapsto (100111) & (101) &\mapsto (101110) \\ (010) &\mapsto (010011) & (011) &\mapsto (011010) \\ (110) &\mapsto (110100) & (111) &\mapsto (111101) \end{aligned}$$

נשים לב כי (100111) שייך לקוד, אבל (110011) לא, ולכן הקוד לא ציקלי.

טענה 12.9. הקוד הפולינומי המתקבל מ-$g(x)$ הוא ציקלי אם ורק אם הפולינום $g(x)$ מחלק את x^n-1 (אם ורק אם הקוד הוא אידאל בחוג $\mathbb{Z}_2[x]/\langle x^n-1\rangle$).

דוגמה 12.10. הפולינום $x^{15}-1\in\mathbb{Z}_2[x]$ מתפרק למכפלה הבאה של פולינומים אי פריקים:

$$x^{15}-1=(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

נבחר את הפולינום

$$g(x)=(x^4+x+1)(x^4+x^3+x^2+x+1)=x^8+x^7+x^6+x^4+1$$

והוא ייצר קוד ציקלי $C\subseteq\mathbb{Z}_2^{15}$ עם מרחק מינימלי 5. וקטור המקדמים של הפולינום $g(x)$ הוא (111010001). לפי הסטות מעגליות שלו, נסמן מטריצה $M\in M_{15,7}(\mathbb{Z}_2)$:

$$M=\begin{pmatrix} x^6g(x)\\ x^5g(x)\\ x^4g(x)\\ x^3g(x)\\ x^2g(x)\\ xg(x)\\ g(x)\end{pmatrix}^T=\begin{pmatrix} 1&1&1&0&1&0&0&0&1&0&0&0&0&0&0\\ 0&1&1&1&0&1&0&0&0&1&0&0&0&0&0\\ 0&0&1&1&1&0&1&0&0&0&1&0&0&0&0\\ 0&0&0&1&1&1&0&1&0&0&0&1&0&0&0\\ 0&0&0&0&1&1&1&0&1&0&0&0&1&0&0\\ 0&0&0&0&0&1&1&1&0&1&0&0&0&1&0\\ 0&0&0&0&0&0&1&1&1&0&1&0&0&0&1\end{pmatrix}^T$$

שהיא מטריצה יוצרת של הקוד C. בעזרת דירוג גאוס של M^T אפשר למצוא מטריצה יוצרת תקנית G, וממנה את מטריצת בדיקת הזוגיות הקנונית H.

13 תרגול שלושה עשר

13.1 פעולת ההצמדה

הגדרה 13.1. 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. Conjugates Conjugacy class

דוגמה 13.2. 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 13.3. 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 $n \le m$ $o(g) =$. 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 $g \in Z(G)$. $\square$

הערה 13.4. הכיוון ההפוך בכל סעיף אינו נכון. למשל, אפשר לקחת את $\mathbb{Z}_4$. שם $o(1) = o(3) = 4$, אבל הם לא צמודים; כמו כן, שניהם במרכז, ולכל אחד מהם יש איבר אחר מאותו סדר.

דוגמה 13.5. בחבורה D_3, האיבר σ צמוד לאיבר $\tau\sigma\tau^{-1} = \tau\sigma\tau = \sigma^2$. אין עוד איברים שצמודים אליהם, כי אין עוד איברים מסדר 3 ב-D_3.

תרגיל 13.6. תהי $\sigma \in S_n$, ויהי מחזור $(a_1, a_2, \dots, a_k) \in S_n$. הוכיחו כי

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

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

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

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

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

מכאן ששתי התמורות הדרושות שוות. □

תרגיל 13.7. נתונות ב-S_6 התמורות $a = (1, 5, 3, 6)$, $\sigma = (1, 3)(4, 5, 6)$ ו-$\tau = (2, 4, 5)$. חשבו את:

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

פתרון. לפי הנוסחה מתרגיל 13.6,

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

מסקנה 13.8 (לבית). $S_n = \langle (1, 2), (1, 2, \ldots, n) \rangle$.

הגדרה 13.9. 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 $r_1 \geq r_2 \geq \cdots \geq r_k$. נגדיר את מבנה המחזורים של σ להיות ה-k-יה הסדורה $(r_1, r_2, \ldots, r_k)$. Cycle type

דוגמה 13.10. מבנה המחזורים של $(1, 2, 3)(5, 6)$ הוא $(3, 2)$; מבנה המחזורים של $(1, 5)(4, 2, 3)$ גם הוא $(3, 2)$; מבנה המחזורים של $(1, 2, 3, 4)(5, 6)(7, 8)$ הוא $(4, 2, 2)$.

מסקנה 13.11. שתי תמורות צמודות ב-S_n אם ורק אם יש להן אותו מבנה מחזורים. למשל, התמורה $(1, 2, 3)(5, 6)$ צמודה ל-$(1, 5)(4, 2, 3)$ ב-S_8, אבל הן לא צמודות לתמורה $(1, 2, 3, 4)(5, 6)(7, 8)$ ב-S_8.

הוכחה. (אם יש זמן, או חלק מתרגיל הבית)
($\Leftarrow$) תהיינה $\sigma, \tau \in S_n$ שתי תמורות צמודות ב-S_n. נכתוב $\tau = \pi \sigma \pi^{-1}$. נניח כי $\sigma = \sigma_1 \sigma_2 \ldots \sigma_k$ הפירוק של σ למכפלה של מחזורים זרים; לכן

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

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 $\sigma_1,\sigma_2,\ldots,\sigma_k$ 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.

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

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

ולכן

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

מכאן ש-σ ו-τ צמודות ב-S_n. $\square$

מסקנה 13.12. 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 13.13. חלוקה של n היא סדרה לא עולה של מספרים טבעיים $n_1\geq\cdots\geq n_k>0$ כך ש-$n=n_1+\cdots+n_k$. את מספר החלוקות של n מסמנים $\rho(n)$. Partition

מסקנה 13.14. מספר מחלקות הצמידות ב-S_n הוא $\rho(n)$.

תרגיל 13.15. כמה מחלקות צמידות יש ב-S_5?

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

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

ולכן $\rho(5)=7$.

תרגיל 13.16. 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, $(1,2,3),(1,3,2)\in A_3$ אינם צמודים ב-A_3. אבל הם צמודים ב-S_3, כי יש להם אותו מבנה מחזורים.

הגדרה 13.17 (מתרגילי הבית)**.** תהי G חבורה. עבור איבר $a\in G$ נגדיר את הַמְּרַכֵּז של a להיות Centralizer

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

תרגיל 13.18. 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 $\tau\sigma\tau^{-1}=\sigma$. 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 מתחלפת עם σ, ולכן הרשימה המלאה היא

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

14 תרגול ארבעה עשר

14.1 תת־חבורה הנוצרת על ידי תת־קבוצה

הגדרה 14.1. תהי G חבורה ותהי $S\subseteq G$ תת־קבוצה לא ריקה איברים ב-G (שימו לב ש-S אינה בהכרח תת־חבורה של G).

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

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

דוגמה 14.2. ניקח $\{2,3\}\subseteq\mathbb{Z}$ ואת $H=\langle 2,3\rangle$. נוכיח בעזרת הכלה דו־כיוונית ש-$\mathbb{Z}=H$.

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

דוגמה 14.3. אם ניקח $\{4,6\} \subseteq \mathbb{Z}$, אז נקבל: $\langle 4,6\rangle = \{4n+6m \,|\, m,n\in\mathbb{Z}\}$.
נטען ש-$\langle 4,6\rangle = \gcd(4,6)\cdot\mathbb{Z} = 2\mathbb{Z}$ (כלומר תת־חבורה של השלמים המכילה רק את המספרים הזוגיים). נוכיח על ידי הכלה דו כיוונית,
($\subseteq$): ברור ש-$2|4m+6n$ ולכן $\langle 4,6\rangle \subseteq 2\mathbb{Z}$.
($\supseteq$): יהי $2k\in 2\mathbb{Z}$. אזי $2k = 4(-k)+6k \in \langle 4,6\rangle$. לכן גם מתקיים $2\mathbb{Z}\subseteq\langle 4,6\rangle$.

דוגמה 14.4. בדומה לדוגמה האחרונה, במקרה שהחבורה אבלית, קל יותר לתאר את תת־החבורה הנוצרת על ידי קבוצת איברים. למשל אם ניקח שני יוצרים $a,b\in G$ נקבל: $\langle a,b\rangle = \{a^ib^j \,|\, i,j\in\mathbb{Z}\}$.
בזכות החילופיות, ניתן לסדר את כל ה-a-ים יחד וכל ה-b-ים יחד. למשל

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

באופן כללי, בחבורה אבלית מתקיים:

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

הערה 14.5. נוח לעיתים לחשוב על איברי $\langle A\rangle$ בתור קבוצת "המילים" שניתן לכתוב באמצעות האותיות בקבוצה A. מגדירים את האלפבית שלנו להיות $A\cup A^{-1}$ כאשר $A^{-1} = \{a^{-1}\,|\,a\in A\}$. מילה היא סדרה סופית של אותיות מן האלפבית, ועבור $x\in A$ מתקיים $xx^{-1} = x^{-1}x = \varepsilon$, כשהמילה הריקה ε מייצגת את איבר היחידה ב-G.

14.2 חבורות אבליות סופיות

טענה 14.6. תהי G חבורה אבלית מסדר $p_1p_2\ldots p_k$, מכפלת ראשוניים שונים. אזי

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

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

טענה 14.7. תהי G חבורה אבלית מסדר חזקה של ראשוני p^n. אזי קיימים מספרים טבעיים $m_1,\ldots,m_k$ כך ש-$m_1+\cdots+m_k=n$ ומתקיים $G\cong\mathbb{Z}_{p^{m_1}}\times\mathbb{Z}_{p^{m_2}}\times\cdots\times\mathbb{Z}_{p^{m_k}}$.
למשל אם G אבלית מסדר $27=3^3$, אזי 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 14.8. (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 14.9. למשל $\rho(4)=5$, כי $4 = 1+1+1+1 = 2+1+1 = 2+2 = 3+1 = 4$.

טענה 14.10. מספר החבורות האבליות, עד כדי איזומורפיזם, מסדר p^n הוא $\rho(n)$.

טענה 14.11. לכל חבורה אבלית סופית G יש צורה קנונית

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

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

Primary decomposition

טענה 14.12. כל חבורה אבלית מסדר $p_1^{k_1} \dots p_n^{k_n}$ גם 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-$|G| = 45 = 3^2 \cdot 5$, אז G איזומורפית ל-$\mathbb{Z}_9 \times \mathbb{Z}_5$ או ל-$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

מסקנה 14.13. 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 $2^3 \cdot 5^2 = 200$ הוא $6 = 3 \cdot 2 = \rho(3)\rho(2)$. האם אתם יכולים למצוא את כולן?

תרגיל 14.14. הוכיחו כי $\mathbb{Z}_{200} \times \mathbb{Z}_{20} \cong \mathbb{Z}_{100} \times \mathbb{Z}_{40}$.

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

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

Exponent of a group

הגדרה 14.15. תהי G חבורה. נגדיר את האקספוננט (או, המעריך) של החבורה $\exp(G)$ להיות המספר הטבעי הקטן ביותר n כך שלכל $g \in G$ מתקיים $g^n = e$. אם לא קיים כזה, נאמר $\exp(G) = \infty$.

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

תרגיל 14.16. תנו דוגמא לחבורה לא ציקלית G עבורה $\exp(G) = |G|$.

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

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

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

תרגיל 14.17. הוכיחו שאם G חבורה אבלית סופית כך ש-$\exp(G) = |G|$, אז G ציקלית.

פתרון. נניח וישנו פירוק $|G| = p_1^{k_1} \dots p_n^{k_n} = \exp(G)$. אנחנו יכולים לפרק את G לפירוק פרימרי $A_1 \times \cdots \times A_n$, כאשר $|A_i| = p_i^{k_i}$. אנחנו יודעים מהו הסדר של איברים במכפלה ישרה (הכפולה המשותפת המזערית של הסדרים ברכיבים), ולכן הגורם $p_i^{k_i}$ באקספוננט מגיע רק מאיברים שבהם ברכיב A_i בפירוק הפרימרי יש איבר לא אפסי. האפשרות היחידה שזה יקרה היא אם ורק אם $A_i \cong \mathbb{Z}_{p_i^{k_i}}$ (אחרת האקספוננט יהיה קטן יותר). ברור כי $\left(p_i^{k_i}, p_j^{k_j}\right) = 1$ עבור $i \neq j$, ולכן נקבל כי

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

ולכן G היא ציקלית.

תרגיל 14.18. 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

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

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

הערה 14.19 (על חבורת הקווטרניונים). המתמטיקאי האירי בן המאה ה-19, ויליאם המילטון, הוא האחראי על גילוי (חבורת) הקווטרניונים. רגע התגלית נקרא לימים "אקט של ונדליזם מתמטי". Quaternion group

בתאריך 16 באוקטובר 1843 בעודו מטייל עם אשתו ברחובות דבלין באירלנד, הבריק במוחו מבנה החבורה, ובתגובה נרגשת חרט את המשוואה $i^2 = j^2 = k^2 = ijk = -1$ על גשר בְּרוּם. שלט עם המשוואה נמצא שם עד היום.

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

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

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

יצוג שקול וחסכוני יותר, עם שני יוצרים בלבד, הוא $\langle x, y \,|\, x^2 = y^2, y^{-1}xy = x^{-1} \rangle$.

15 תרגול חמישה עשר

15.1 שדות סופיים

הגדרה 15.1. 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: Field

1. המבנה $(F,+,0_F)$ הוא חבורה חיבורית אבלית.
2. המבנה $(F^*,\cdot,1_F)$ הוא חבורה כפלית אבלית.
3. מתקיים חוק הפילוג (דיסטריביוטיביות הכפל מעל החיבור): לכל $a,b,c\in F$ מתקיים $a(b+c)=ab+ac$.

Field order

הגדרה 15.2. סדר השדה הינו מספר האיברים בשדה.

Field isomorphism

הגדרה 15.3. איזומורפיזם של שדות הוא העתקה חח"ע ועל בין שני שדות ששומרת על שתי הפעולות.

הערה 15.4. 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 15.5. 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-$\mathbb{F}_p$?

Characteristic

הגדרה 15.6. 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 15.7. עבור שדה סופי $\mathbb{F}_q$, סדר השדה הוא תמיד חזקה של מספר ראשוני, כלומר מתקיים $q=p^n$ עבור p ראשוני כלשהו. המאפיין של השדה הזה הוא בהכרח p.

הערה 15.8. 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, מה לגבי ההפך?

טענה 15.9. החבורה הכפלית של השדה, $\mathbb{F}_q^*=\mathbb{F}_q\setminus\{0_F\}$ היא ציקלית מסדר $q-1$.

דוגמה 15.10. $\mathbb{F}_{13}^*=\{1_F,2,\dots,12\}$ חבורה ציקלית מסדר 12, כלומר $\mathbb{F}_{13}^*\cong\mathbb{Z}_{12}$.

Subfield

Field extension

הגדרה 15.11. 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 15.12. $\mathbb{C}/\mathbb{R}$ היא הרחבת שדות מדרגה 2, ואילו $\mathbb{R}/\mathbb{Q}$ היא הרחבת שדות מדרגה אינסופית. שימו לב ש-$\mathbb{Q}/\mathbb{F}_{13}$ היא לא הרחבת שדות כי לא מדובר באותן פעולות (ואפשר להוסיף שגם שלא מדובר בתת־קבוצה).

טענה 15.13. 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 $\{x_1, x_2, \dots, x_r\}$ בסיס של E מעל F. אז כל איבר ב-E ניתן לכתוב בדיוק בדרך אחת כצירוף לינארי (מעל F) של $\{x_1, x_2, \dots, x_r\}$. לכן מספר האיברים ב-E שווה למספר הצירופים הלינאריים השונים (מעל F) של $\{x_1, x_2, \dots, x_r\}$. אבל יש $|F|^r$ צירופים שונים כאלו, ולכן $|E| = |F|^r$. □

הערה 15.14 (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 15.15. 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 15.16. 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 $o(x) \nmid 4$. במקרה זה בהכרח $o(x) = 8$.

אם כן, נדרוש שב-$\mathbb{F}_q^*$ יהיה איבר x מסדר 8, ואז הוא יקיים את המשוואה. מכיוון שסדר איבר מחלק את סדר החבורה (לגראנז'), נסיק שהסדר של $\mathbb{F}_q^*$ מתחלק ב-8, ואז מפני ש-$\mathbb{F}_q^*$ ציקלית, אז גם קיים איבר מסדר 8.

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

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 המבוקשים הם שדות ממאפיין 2 או מסדר המקיים $q = p^n \equiv 1 \mod 8$.

הערה 15.17. שימו לב שבעוד שהפולינום $T(x)=x^4+1$ אינו פריק מעל $\mathbb{Q}$, הוא פריק מעל כל שדה סופי.

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

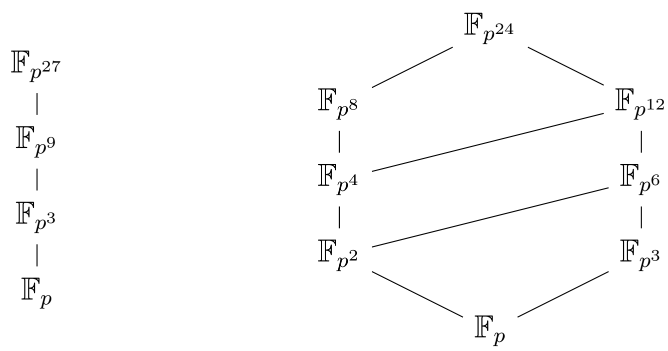
תרגיל 15.18. הוכיחו שבשדה $\mathbb{F}_q$ מתקיים $a^q=a$ לכל $a\in\mathbb{F}_q$ וגם

$$x^q-x=\prod_{a\in\mathbb{F}_q}(x-a)$$

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

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



בכיוון אחד, נניח כי $\mathbb{F}_q$ הוא תת־שדה של $\mathbb{F}_{q'}$. אזי $\mathbb{F}_{q'}$ מרחב וקטורי מעל $\mathbb{F}_q$, וראינו בטענה 15.13 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

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

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 $K = \{x \in \mathbb{F}_{q'} \mid x^q = x\}$ 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. $\square$

16 תרגול חמישה עשר

16.1 חבורות מוצגות סופית

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

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

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

דוגמה 16.1. יצוג של חבורה ציקלית מסדר n הוא $\mathbb{Z}_n \cong \langle x \mid x^n \rangle$. כל איבר הוא חזקה של היוצר x, ושכאשר רואים את תת־המילה x^n אפשר להחליף אותה ביחידה. לנוחות, בדרך כלל קבוצת היחסים תכתב עם שיוויונות, למשל $x^n = e$. באופן דומה, החבורה הציקלית האינסופית ניתנת ליצוג

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

ובדרך כלל משמיטים את קבוצת היחסים אם היא ריקה.

ודאו שאתם מבינים את ההבדל בין החבורות הלא איזומורפיות

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

הגדרה 16.2. ראינו שחבורה שיש לה קבוצת יוצרים סופית נקראת חבורה נוצרת סופית. אם לחבורה יש יצוג שבו גם קבוצת היוצרים סופית וגם קבוצת היחסים סופית, נאמר שהחבורה מוצגת סופית. Finitely presented

דוגמה 16.3. כל חבורה ציקלית היא מוצגת סופית, וראינו מה הם היצוגים המתאימים. כל חבורה סופית היא מוצגת סופית (זה לא טריוויאלי). נסו למצוא חבורה נוצרת סופית שאינה מוצגת סופית (זה לא כל כך קל).

16.2 החבורה הדיהדרלית

הגדרה 16.4. עבור מספר טבעי n, הקבוצה D_n של סיבובים ושיקופים המעתיקים מצולע משוכלל בן n צלעות על עצמו, היא החבורה הדיהדרלית מדרגה n, יחד עם הפעולת של הרכבת פונקציות. Dihedral group

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

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

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

הערה 16.5 (אם יש זמן). פונקציה $\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ שהיא חח"ע ועל ושומרת מרחק (כלומר $d(x,y) = d(\alpha(x), \alpha(y))$) נקראת איזומטריה. אוסף האיזומטריות עם הפעולה של הרכבת פונקציות הוא חבורה. תהי $L \subseteq \mathbb{R}^2$ קבוצה כך שעבור איזומטריה α מתקיים $\alpha(L) = L$. במקרה זה α נקראת סימטריה של L. אוסף הסימטריות של L הוא תת־חבורה של האיזומטריות. החבורה D_n היא בדיוק אוסף הסימטריות של מצולע משוכלל בן n צלעות. Isometry Symmetry

דוגמה 16.6. החבורה D_3 נוצרת על ידי סיבוב σ של 120° ועל ידי שיקוף τ, כך שמתקיימים היחסים הבאים בין היוצרים: $\sigma^3 = \tau^2 = \mathrm{id}$, $\tau\sigma\tau = \sigma^{-1}$. כלומר $D_3 = \{\mathrm{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ (להדגים עם משולש מה עושה כל איבר, וכנ"ל עבור D_5).

מה לגבי האיבר $\sigma\tau \in D_3$? הוא מופיע ברשימת האיברים תחת שם אחר, שכן

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

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

סיכום 16.7. איברי D_n הם

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

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

תרגיל 16.8. מצאו את כל התמונות האפימורפיות של D_4 (עד כדי איזומורפיזם).

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

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

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

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

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

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

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

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

לכן בהכרח $i = 2$. אבל אז

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

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

16.3 משוואת המחלקות

לפני שנציג את משוואת המחלקות נזכיר שלושה מושגים.

הגדרה 16.9. המרכז של חבורה G הוא הקבוצה Center

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

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

הגדרה 16.10. תהי G חבורה. לכל $x \in G$, המְרַכֵּז של x הוא הקבוצה Centralizer

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

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

Conjugacy class

הגדרה 16.11. תהי G חבורה. יהי $x \in G$. נגדיר את מחלקת הצמידות של x להיות הקבוצה

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

הערה 16.12. לכל $x \in G$ מתקיים

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

תרגיל 16.13. מצא את מספר התמורות ב-S_n המתחלפות עם $\beta = (12)(34)$, כלומר כל התמורות $\gamma \in S_n$ המקיימות $\beta\gamma = \gamma\beta$.

פתרון.

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

למשל, ב-S_4 יש 8 תמורות כאלו.

תרגיל 16.14. תהי G חבורה סופית כך ש-$n = [G : Z(G)]$. הראה כי מחלקת צמידות ב-G מכילה לכל היותר n איברים.

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

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

Class equation

משפט 16.15 (משוואת המחלקות). תהי G חבורה סופית. אזי

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

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

תרגיל 16.16. 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:

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

הגדרה 16.17. יהי p ראשוני. חבורה G תקרא חבורת-p, אם הסדר של כל איבר בה הוא חזקה של p. הראו שאם G סופית, אז G חבורת-p אם ורק אם $|G| = p^n$ עבור איזשהו $n \in \mathbb{N}$. p-group

תרגיל 16.18. הוכיחו שהמרכז של חבורת-p אינו טריוויאלי.

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

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

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

תרגיל 16.19. מיינו את החבורות מסדר p^2 על ידי זה שתראו שהן חייבות להיות אבליות.

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

נניח בשלילה שלא. כלומר ש-$|Z(G)| = p$. כלומר תת־חבורה זו מסדר ראשוני וכן ציקלית. לכן נציגה על ידי יוצר: $\langle a \rangle = |Z(G)|$. 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 לגראנז', $|\langle a, b \rangle| = p^2$. כלומר $\langle a, b \rangle$ היא כל G.

על מנת להראות שחבורה הנוצרת על ידי שני יוצרים אלו היא 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-$\mathbb{Z}_p \times \mathbb{Z}_p$.

16.4 תת־חבורת הקומוטטורים

הגדרה 16.20. תהא G חבורה. הקומוטטור של זוג איברים $a, b \in G$ הוא האיבר $[a, b] = aba^{-1}b^{-1}$. Commutator

הערה 16.21. a, b מתחלפים אם ורק אם $[a, b] = e$. באופן כללי, $ab = [a, b]\, ba$.

הגדרה 16.22. תת־חבורת הקומוטטורים (נקראת גם תת־חבורת הנגזרת) הינה: Commutator subgroup (or derived subgroup)

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

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

הערה 16.23. G אבלית אם ורק אם $G' = \{e\}$.

למעשה, תת־חבורת הקומוטטורים "מודדת" עד כמה החבורה G אבלית.

הערה 16.24. $[a,b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b,a]$.

הערה 16.25. אם $H \leq G$ אז $H' \leq G'$.

הערה 16.26. $G' \lhd G$. למשל לפי זה ש-$g\,[a,b]\,g^{-1} = [gag^{-1}, gbg^{-1}]$.
תת־חבורת הקומוטטורים מקיימת למעשה תנאי חזק הרבה יותר מנורמליות. לכל הומומורפיזם $f\colon G \to H$ מתקיים

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

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

הגדרה 16.27. חבורה G תקרא חבורה פשוטה אם ל-G אין תת־חבורות נורמליות לא טריוויאליות. Simple group

דוגמה 16.28. 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 16.29. חבורה G נקראת מושלמת אם $G = G'$. Perfect

מסקנה 16.30. 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 16.31. עבור $n \geq 5$, מתקיים $A_n' = A_n$. אבל $\mathbb{Z}_5$ למשל היא פשוטה ולא מושלמת, כי היא אבלית.

משפט 16.32. המנה G/G', שנקראת האבליניזציה של G, היא המנה האבלית הגדולה ביותר של G. כלומר: Abelinization

1. לכל חבורה G, המנה G/G' אבלית.
2. לכל $N \lhd G$ מתקיים ש-G/N אבלית אם ורק אם $G' \leq N$ (כלומר G/N איזומורפית למנה של G/G').

דוגמה 16.33. אם A אבלית, אז $A/G' \cong A$.

דוגמה 16.34. תהי $D_4 = \langle \sigma, \tau \rangle$. ראינו ש-$G \lhd Z(D_4) = \{e, \sigma^2\}$.
כמו כן, המנה $|D_4/Z(D_4)| = 4$. תת־חבורה זו אבלית (מכיוון שהסדר שלה הוא p^2 לפי תרגיל 16.19).
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 16.35. מצאו את S_n' עבור $n \geq 5$.

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

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

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 $S_n'=A_n$.

א' נספח: חבורות מוכרות

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

- $(G,\cdot)$ או $(G,*)$, חבורה כלשהי עם פעולה כלשהי. איבר היחידה מסומן e.
- $(\mathbb{Z},+)$, המספרים השלמים עם חיבור רגיל. איבר היחידה מסומן 0.
- $(n\mathbb{Z},+)$, הכפולות של $n\in\mathbb{Z}$ עם חיבור רגיל. איבר היחידה מסומן 0.
- $(\mathbb{Z}_n,+)$, מחלקות שקילות של חלוקה בשארית ב-n עם חיבור מודולו n. איבר היחידה מסומן 0 או $[0]$.
- $(U_n,\cdot)$, חבורת אוילר עם כפל מודולו n. איבר היחידה מסומן 1 או $[1]$.
- $(\Omega_n,\cdot)$, חבורת שורשי היחידה מסדר n עם כפל רגיל. איבר היחידה מסומן 1.
- $(F,+)$, החבורה החיבורית של שדה F עם החיבור בשדה. איבר היחידה מסומן 0.
- $(F^*,\cdot)$, החבורה הכפלית של שדה F עם הכפל בשדה. איבר היחידה מסומן 1.
- $(M_n(F),+)$, מטריצות בגודל $n\times n$ מעל שדה F עם חיבור מטריצות. איבר היחידה מסומן 0 או 0_n.
- $(GL_n(F),\cdot)$, החבורה הלינארית הכללית מעל F מדרגה n עם כפל מטריצות. האיברים הם מטריצות הפיכות בגודל $n\times n$ מעל שדה F. איבר היחידה מסומן I או I_n.
- $(SL_n(F),\cdot)$, החבורה הלינארית המיוחדת מעל F מדרגה n עם כפל מטריצות. האיברים הם מטריצות בגודל $n\times n$ עם דטרמיננטה 1 מעל שדה F. איבר היחידה מסומן I או I_n.
- $(S_n,\cdot)$, החבורה הסימטרית עם הרכבת פונקציות. איבר היחידה מסומן id.
- $(A_n,\cdot)$, חבורה החילופין (או חבורת התמורות הזוגיות) עם הרכבת פונקציות. איבר היחידה מסומן id.
- $(D_n,\cdot)$, החבורה הדיהדרלית עם הרכבת פונקציות. איבר היחידה מסומן id.
- $(Q_8,\cdot)$, חבורת הקווטרניונים. איבר היחידה מסומן 1.

שימו לב שאם פעולה מסומנת $\cdot$ כמו כפל, אז במקרים רבים נשמיט את סימון הפעולה. לעיתים כדי להדגיש למי שייך איבר היחידה נרשום e_G במקום e, או למשל 0_F במקום 0 עבור איבר היחידה בחבורה החיבורית של שדה F.