

מערך תרגיל קורס 88-211 סמסטר א' תשע"ו אלגברה מופשטת

אוקטובר 2015, גרסה 0.3

מבוא

נתחיל עם כמה דגשים:

- דף הקורס נמצא באתר www.math-wiki.com.
- שאלות בנוגע לחומר הלימודי מומלץ לשאול בדף השיחה באתר של הקורס.
- חשוב לפתור את תרגילי הבית (אין חובת הגשה, אבל יהיו בחנים שיתבססו עליהם).
- נשמח לכל הערה על מסמך זה.

תרגול 1 מבנים אלגבריים בסיסיים

נפתח בהגדרות לכמה מבנים אלגבריים. מבנה אלגברי שמכירים כבר באלגברה לינארית הוא שדה. אנו נגדיר כמה מבנים יותר "פשוטים", כשהחשוב שבהם הוא חבורה. במרבית הקורס נתרכז בחקר חבורות.

הגדרה 1.1. תהי S קבוצה. פעולה בינארית (binary operation) על S היא פונקציה דו-מקומית $S \times S \rightarrow S$: $*$. עבור $a, b \in S$ כמעט תמיד במקום לרשום $(a, b) *$ נשתמש בסימון $a * b$. מפני שתמונת הפונקציה $a * b$ שייכת ל- S , נאמר כי הפעולה היא סגורה.

הגדרה 1.2. חבורה לפחצה (semigroup) היא מערכת אלגברית $(S, *)$ המורכבת מקבוצה לא ריקה S ומפעולה בינארית על S המקיימת קיבוציות (אסוציאטיביות, assoc-iativity). כלומר לכל $a, b, c \in S$ מתקיים $(a * b) * c = a * (b * c)$.

צורת רישום 1.3. לעיתים נקצר ונאמר כי S היא חבורה למחצה מבלי להזכיר במפורש את המערכת האלגברית. כנ"ל למבנים האלגבריים האחרים.

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

1.5. הערה. יהי M מונואיד. קל לראות כי איבר היחידה ב- M הוא יחיד. הרי אם $e, f \in M$ הם איברי יחידה, אז מתקיים $e = e * f = f$.

הגדרה 1.6. יהי $(M, *, e)$ מונואיד. איבר $a \in M$ יקרא הפיך משמאל אם קיים איבר $b \in M$ כך ש- $ba = e$. במקרה זה b יקרא הופכי שמאלי של a . באופן דומה, איבר $a \in M$ יקרא הפיך מימין אם קיים איבר $b \in M$ כך ש- $ab = e$. במקרה זה b יקרא הופכי ימני של a . איבר יקרא הפיך אם קיים איבר $b \in M$ כך ש- $ba = ab = e$. במקרה זה b יקרא הופכי של a .

תרגיל 1.7. 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)!

תרגיל 1.8 (אם יש זמן). אם $aba \in M$ הפיך במונואיד, הראו כי גם a, b הפיכים.

פתרון. יהי c ההופכי של aba . כלומר

$$abac = caba = e$$

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

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

וניתן להסיק כי aca הופכי שמאלי וימני של b .

הגדרה 1.9. חבורה (group) $(G, *, e)$ היא מונואיד שבו כל איבר הוא הפיך. מתקיים: חבורה \Leftarrow מונואיד \Leftarrow חבורה למחצה.

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

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

הערה 1.10. עבור קבוצה סופית אחת הדרכים להגדיר פעולה בינארית היא בעזרת לוח כפל. למשל, אם $S = \{a, b\}$ ונגדיר

| | | |
|---|---|---|
| * | a | b |
| a | b | b |
| b | b | a |

אז קל לראות שמתקיימת סגירות, אבל הפעולה אינה קיבוצית כי $(a*b)*b = b*b = a$, אבל $a*(b*b) = a*a = b$.
נסמן כמה קבוצות של מספרים:

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

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

דוגמה 1.11. המערכת $(\mathbb{N}, +)$ של מספרים טבעיים עם החיבור הרגיל של מספרים טבעיים היא חבורה למחצה.

דוגמה 1.12. תהי X קבוצה כלשהי, ותהי $P(X)$ קבוצת החזקה שלה (זהו אוסף כל תתי הקבוצות של X). אזי $(P(X), \cap)$ היא מונואיד שבו איבר היחידה הוא X . מה קורה עבור $(P(X), \cup)$? (להמשך, נשים לב כי במונואיד זה לכל איבר a מתקיים $a^2 = a$).

דוגמה 1.13. המערכת $(\mathbb{Z}, +)$ היא חבורה שאיבר היחידה בה הוא 0. בכתוב חיבורי מקובל לסמן את האיבר ההופכי של a בסימון $-a$. כתיב זה מתלכד עם המושג המוכר של מספר נגדי ביחס לחיבור.

דוגמה 1.14. המערכת $(\mathbb{Z}, -)$ אינה אפילו חבורה למחצה, מפני שפעולת החיסור אינה קיבוצית. למשל $(2-1) - 1 \neq 5 - (2-2)$.

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

טענה 1.16. שקילות מודולו n היא יחס שקילות. כפל וחיבור מודולו n מוגדרים היטב. כלומר אם $a \equiv b, c \equiv d \pmod{n}$ אז $ac \equiv bd \pmod{n}$ וגם $a + c \equiv b + d \pmod{n}$.

דוגמה 1.17. נסתכל על אוסף מחלקות השקילות מודולו n , שמקובל לסמן $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{[a] : a \in \mathbb{Z}\}$. למשל $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$. לפעמים מסמנים את מחלקת השקילות $[a]$ בסימון \bar{a} , ולעיתים כאשר ברור ההקשר פשוט a . כזכור $[a] + [b] = [a + b]$ כאשר באגף שמאל הסימן $+$ הוא פעולה בינארית הפועלת על אוסף מחלקות השקילות (a הוא נציג של מחלקת שקילות אחת ו- b הוא נציג של מחלקת שקילות אחרת) ובאגף ימין זו פעולת החיבור הרגילה של מספרים (שלאחריה מסתכלים על מחלקת השקילות שבה $a + b$ נמצא).

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

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

דוגמה 1.18. יהי n מספר טבעי. נסמן את הכפולות שלו ב- $n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$. למשל $4\mathbb{Z} = \{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$. לכל n המערכת $(n\mathbb{Z}, +)$ היא חבורה.

דוגמה 1.19. 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 1.20. יהי F שדה. המערכת (F, \cdot) עם פעולת הכפל של השדה היא מונואיד שאינו חבורה (כי 0 לא הפיך). איבר היחידה הוא 1. גם המערכת $(M_n(F), \cdot)$ היא מונואיד ביחס לכפל מטריצות, שכן לא כל מטריצה היא הפיכה.

דוגמה 1.21. 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 (רק 1, -1 הפיכים).

הערה 1.22 (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. נאמר כי F הוא שדה אם $(F, +, 0)$ היא חבורה חילופית, $(F^*, \cdot, 1)$ היא חבורה חילופית וקיום חוק הפילוג (distributive law), לכל $a, b, c \in F$ מתקיים $a(b + c) = ab + ac$.

דוגמה 1.23. קבוצה בעלת איבר אחד ופעולה סגורה היא חבורה. לחבורה זו קוראים החבורה הטריטויאלית.

תרגיל 1.24. האם קיים מונואיד שיש בו איבר הפיך מימין שאינו הפיך משמאל?

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

ההפיכים משמאל הם הפונקציות החח"ע. ההפיכים מימין הם הפונקציות על (להזכיר את הטענות הרלוונטיות מבידידה). מה יקרה אם נבחר את X להיות סופית? אם ניקח למשל $X = \mathbb{N}$ קל למצוא פונקציה על שאינה חח"ע. הפונקציה שנבחר היא $d(n) = \max(1, n-1)$. לפונקציה זו יש הופכי מימין, למשל $u(n) = n+1$, אבל אין לה הפיך משמאל.

תרגיל 1.25. האם קיימת חבורה למחצה שבה יש איבר יחידה משמאל, אבל אין איבר יחידה מימין?

פתרון. כן, ראיתם את הדוגמה הזו בהרצאה. נתבונן ב- $S = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}$. קל לראות כי $e' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ הוא איבר יחידה משמאל.

נראה שאין איבר יחידה מימין. נניח בשלילה שקיים $u = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$ כך שלכל $s \in S$ מתקיים $su = s$. בפרט זה יתקיים עבור $s = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. נקבל כי $su = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, ולכן $x = 1$ וגם $y = b$. כיון שזה צריך להתקיים לכל $b \in \mathbb{R}$, קיבלנו סתירה לכך ש- u איבר יחידה מימין.

הסבר אחר: נשים לב שישנם אינסוף איברי יחידה משמאל (הם האיברים מהצורה $\begin{pmatrix} 1 & y \\ 0 & 0 \end{pmatrix}$), ולכן אין יחידה מימין. כי אם היה איבר יחידה מימין, הוא היה שווה לכל אחד מאיברי היחידה משמאל, אך יש אינסוף איברי יחידה שונים משמאל.

תרגיל 1.26 (ממבחן). הוכיחו כי לכל מונואיד (X, \cdot) הקבוצה $P_*(X)$ של כל תתי הקבוצות הלא ריקות של X מגדירה מונואיד ביחס לפעולת הכפל הטבעית:

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

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

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

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

הגדרה 1.27 (חבורת האיברים ההפיכים). יהי M מונואיד ויהיו $a, b \in M$ זוג איברים. אם a, b הם הפיכים, אזי גם $a \cdot b$ הוא הפיך במונואיד. אכן, האיבר ההופכי הוא $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. לכן אוסף כל האיברים ההפיכים במונואיד מהווה קבוצה סגורה ביחס לפעולה. כמו כן האוסף הנ"ל מכיל את איבר היחידה, וכל איבר בו הוא הפיך. מסקנה מיידית היא שאוסף האיברים ההפיכים במונואיד מהווה חבורה ביחס לפעולה המצומצמת. נסמן חבורה זו ב- $U(M)$ (קיצור של Units).

הגדרה 1.28. המערכת $(M_n(\mathbb{R}), \cdot)$ של מטריצות ממשיות בגודל $n \times n$ עם כפל מטריצות היא מונואיד. לחבורת ההפיכים שלו

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

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

הגדרה 1.29. נאמר כי פעולה דו-מקומית $G \times G \rightarrow G$ היא אבליית (או חילופית, commutative) אם לכל שני איברים $a, b \in G$ מתקיים $a * b = b * a$. אם $(G, *)$ חבורה והפעולה היא אבליית, נאמר כי G היא חבורה אבליית (או חילופית). המושג נקרא על שמו של נילס הנריק אָבֶל (Niels Henrik Abel).

דוגמה 1.30. יהי F שדה. החבורה $(GL_n(F), \cdot)$ אינה אבליית עבור $n > 1$.

דוגמה 1.31. מרחב וקטורי V יחד עם פעולת חיבור וקטורים הרגילה הוא חבורה אבליית.

תרגיל 1.32. תהי G חבורה. הוכיחו שאם לכל $x \in G$ מתקיים $x^2 = 1$, אזי G היא חבורה אבליית.

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

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

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

הגדרה 1.33. תהי X קבוצה. 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 . עבור $n \geq 3$ חבורה לא אבליית.

דוגמה 1.34. עדין ניתן להציל את המקרה של הכפל מודולו n . נגדיר את חבורת אוילר (Euler) להיות $U_n = U(\mathbb{Z}_n)$ לגבי פעולת הכפל. נבנה את לוח הכפל של \mathbb{Z}_6 (בהתעלם מ- $[0]$ שתמיד יתן במכפלה $[0]$):

| | | | | | |
|---|---|---|---|---|---|
| · | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 |
| 2 | 2 | 4 | 0 | 2 | 4 |
| 3 | 3 | 0 | 3 | 0 | 3 |
| 4 | 4 | 2 | 0 | 4 | 2 |
| 5 | 5 | 4 | 3 | 2 | 1 |

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

הערה 1.35. אם p הוא מספר ראשוני, אז $U_p = \mathbb{Z}_p^*$ (למה?).

סענה 1.36. בדומה להערה האחרונה, נאפיין את האיברים ב- U_n לכל n .

יהי $m \in \mathbb{Z}$ אז $[m] \in U_n$ אם ורק אם $(n, m) = 1$. כלומר, ההפיכים במונואיד (\mathbb{Z}_n, \cdot) הם כל האיברים הזרים ל- n .

הוכחה. אם $(n, m) = 1$, אזי קיימים $s, t \in \mathbb{Z}$ כך ש- $sn + tm = 1$. לכן $[tm] = [1]$ ולכן $tm \equiv 1 \pmod{n}$. וראינו שכפל מודולו n מוגדר היטב, כלומר $[t][m] = [tm]$. בכיוון השני אם $[m] \in U_n$, אז קיים $b \in \mathbb{Z}$ כך ש- $[b][m] = [1]$. לכן $bm \equiv 1 \pmod{n}$, ולכן $n|1 - bm$. כלומר קיים $k \in \mathbb{Z}$ כך ש- $kn = 1 - bm$. לאחר העבר אגף נקבל $kn + bm = 1$, כלומר 1 הוא צירוף לינארי (מינימלי) של n ושל m , ולכן $(n, m) = 1$. \square

דוגמה 1.37. $U_{12} = \{1, 5, 7, 11\}$

דוגמה 1.38. לא קיים ל-5 הופכי כפלי ב- \mathbb{Z}_{10} , שכן אחרת 5 היה זר ל-10 וזו סתירה.

תרגול 2 מבוא לתורת המספרים

הגדרה 2.1. יהיו a, b מספרים שלמים. נאמר כי a פחלק את b אם קיים $k \in \mathbb{Z}$ כך ש- $ka = b$, ונסמן $a|b$. למשל $5|10$.

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

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

הגדרה 2.3. בהנתן שני מספרים שלמים n, m , המחלק המשותף המירבי (ממ"מ, greatest common divisor) שלהם מוגדר להיות המספר

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

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

הערה 2.4. אם $d|a$ וגם $d|b$, אזי d מחלק כל צירוף לינארי של a ו- b .

סענה 2.5. אם $n = qm + r$, אז $(n, m) = (m, r)$.

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

משפט 2.6 (אלגוריתם אוקלידס). "המתכוון" למציאת מ"מ בעזרת שימוש חוזר בטענה 2.5 הוא אלגוריתם אוקלידס. ניתן להניח $0 \leq m < n$. אם $m = 0$, אזי $(n, m) = n$. אחרת נכתוב $n = qm + r$ כאשר $0 \leq r < m$ וגמשיך עם $(n, m) = (m, r)$. (הבינו לפה האלגוריתם חייב להעצר).

דוגמה 2.7. נחשב את המ"מ של 53 ו-47 בעזרת אלגוריתם אוקלידס

$$(53, 47) = [53 = 1 \cdot 47 + 6]$$

$$(47, 6) = [47 = 7 \cdot 6 + 5]$$

$$(6, 5) = 1$$

דוגמה נוספת עבור מספרים שאינם זרים:

$$(224, 63) = [224 = 3 \cdot 63 + 35]$$

$$(63, 35) = [63 = 1 \cdot 35 + 28]$$

$$(35, 28) = [35 = 1 \cdot 28 + 7]$$

$$(28, 7) = [28 = 4 \cdot 7 + 0]$$

$$(7, 0) = 7$$

משפט 2.8 (אפיון המ"מ כצירוף לינארי מזערי). מתקיים לכל מספרים שלמים a, b כי

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

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

הערה 2.9. מן המשפט קיבלנו כי $(a, b) \in a\mathbb{Z} + b\mathbb{Z}$.

דוגמה 2.10. כדי למצוא את המקדמים s, t כשמביעים את המ"מ כצירוף לינארי כנ"ל נשתמש באלגוריתם אוקלידס המוכלל:

$$(234, 61) = [234 = 3 \cdot 61 + 51 \Rightarrow 51 = 234 - 3 \cdot 61]$$

$$(61, 51) = [61 = 1 \cdot 51 + 10 \Rightarrow 10 = 61 - 1 \cdot 51 = 61 - 1 \cdot (234 - 3 \cdot 61) = -1 \cdot 234 + 4 \cdot 61]$$

$$(51, 10) = [51 = 5 \cdot 10 + 1 \Rightarrow 1 = 51 - 5 \cdot 10 = 51 - 5 \cdot (-1 \cdot 234 + 4 \cdot 61) = 6 \cdot 234 - 23 \cdot 61]$$

$$(10, 1) = 1$$

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

תרגיל 2.11. יהיו a, b, c מספרים שלמים כך ש- $(a, b) = 1$ וגם $a|bc$. הראו כי $a|c$.

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

טענה 2.12. תכונות של מ"מ:

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

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

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

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

2. (חלק מתרגיל הבית)

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

□

הגדרה 2.13. בהנתן שני מספרים שלמים n, m הכפולה המשותפת המזערית (כמ"מ, least common multiple) שלהם מוגדרת להיות

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

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

טענה 2.14. תכונות של כמ"מ:

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

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

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

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

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

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

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

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

□

שאלה 2.15 (לבית). אפשר להגדיר מע"מ ליותר מזוג מספרים. יהי d המע"מ של המספרים n_1, \dots, n_k . הראו שקיימים מספרים שלמים s_1, \dots, s_k המקיימים $s_1 n_1 + \dots + s_k n_k = d$. רמז: אינדוקציה על k .

תרגיל 2.16. מצאו את הספרה האחרונה של 333^{333} .

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

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

ומכאן שהספרה האחרונה היא 3.

תרגיל 2.17 (אם יש זמן). מצאו $x \in \mathbb{Z}$ כך $0 \leq x < 234$ ו- $61x \equiv 1 \pmod{234}$.

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

משפט 2.18 (משפט השאריות הסיני). אם n, m זרים, אזי לכל $a, b \in \mathbb{Z}$ קיים x יחיד עד כדי שקילות מודולו nm כך ש- $x \equiv a \pmod{n}$, $x \equiv b \pmod{m}$ (יחיד!).

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

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

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

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

דוגמה 2.19. נמצא $x \in \mathbb{Z}$ כך ש- $x \equiv 1 \pmod{3}$ וגם $x \equiv 2 \pmod{5}$. ידוע כי $(5, 3) = 1$, ולכן $-1 \cdot 5 + 2 \cdot 3 = 1$. במקרה זה $n = 5, m = 3$ וכן $s = -1, t = 2$, ולפי משפט השאריות הסיני אפשר לבחור את $x = 1 \cdot (-5) + 2 \cdot 6 = 7$. אכן מתקיים $7 \equiv 1 \pmod{3}$ וגם $7 \equiv 2 \pmod{5}$.

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

משפט 2.20 (אם יש זמן). תהא $\{m_1, \dots, m_k\}$ קבוצת מספרים טבעיים הזרים זה לזה (כלומר כל זוג מספרים בקבוצה הוא זר). נסמן את מכפלתם ב- m . בהנתן קבוצה כלשהי של שאריות $\{a_i \pmod{m_i} : 1 \leq i \leq k\}$, קיימת שארית יחידה x מודולו m המהווה פתרון למערכת המשוואות

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

דוגמה 2.21. נמצא $y \in \mathbb{Z}$ כך ש- $y \equiv 1 \pmod{3}$, $y \equiv 2 \pmod{5}$ וגם $y \equiv 3 \pmod{7}$. נשים לב שהפתרון $y = 7$ מן הדוגמה הקודמת הוא נכון כדי כדי הוספה של $3 \cdot 5 = 15$ (כי $15 \equiv 0 \pmod{3}$ וגם $15 \equiv 0 \pmod{5}$). לכן את שתי המשוואות $y \equiv 1 \pmod{3}$, $y \equiv 2 \pmod{5}$ ניתן להחליף במשוואה אחת $y \equiv 7 \pmod{15}$. נשים לב כי $(15, 7) = 1$ ולכן אפשר להשתמש במשפט השאריות הסיני בגרסה לזוג משוואות. בדקו כי $y = 52$ מהווה פתרון.

תרגול 3 סדר של איבר, סדר של חבורה ותת-חבורות

הגדרה 3.1. תהא G חבורה. נגדיר את הסדר (order) של G להיות עוצמתה כקבוצה. במילים יותר גשמיות, כמה איברים יש בחבורה. סימונים מקובלים: $|G|$ או $\text{Ord}(G)$.

הגדרה 3.2. תהא (G, \cdot, e) חבורה ויהא איבר $g \in G$. הסדר של איבר הוא המספר הטבעי n הקטן ביותר כך שמתקיים $g^n = e$. בפרט, בכל חבורה הסדר של איבר היחידה הוא 1, וזהו האיבר היחיד מסדר 1. סימון מקובל $o(g) = n$ ולפעמים $|g|$.

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

תרגול 4

תרגול 5 מחלקות

5.1 החבורה הדיהדרלית

הגדרה 5.1. החבורה הדיהדרלית (מילולית: שתי פאות) היא חבורת הסיבובים והשיקופים של מצולע משוכלל בן n צלעות. משה ירדן הציע במילונו את השם חבורת הפאתיים.

הערה 5.2 (אם יש זמן). פונקציה $\alpha : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ שהיא חח"ע ועל ושומרת מרחק (כלומר $d(x, y) = d(\alpha(x), \alpha(y))$) נקראת איזומטריה. אוסף האיזומטריות עם הפעולה של הרכבת פונקציות הוא חבורה. תהי $L \subseteq \mathbb{R}^2$ קבוצה כך שעבור איזומטריה α מתקיים

$\alpha(L) = L$ במקרה זה α נקראת סימטריה של L . אוסף הסימטריות של L הוא תת-חבורה של האיזומטריות. החבורה D_n היא בדיוק אוסף הסימטריות של מצולע משוכלל בן n צלעות.

דוגמה 5.3. החבורה D_3 נוצרת על ידי סיבוב σ של 120° ועל ידי שיקוף τ , כך שמתקיימים היחסים הבאים בין היוצרים: $\sigma^3 = \tau^2 = \text{id}$, $\tau\sigma\tau = \sigma^{-1}$. כלומר $D_3 = \{\text{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$. (להדגים עם משולש מה עושה כל איבר, כנ"ל עבור D_5). מה לגבי האיבר $\sigma\tau \in D_3$? הוא מופיע ברשימת האיברים תחת שם אחר, שכן

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

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

סיכום 5.4. החבורה D_n נוצרת על ידי סיבוב σ של $\frac{360^\circ}{n}$ ועל ידי שיקוף τ עם היחסים שנביע בכתוב המקוצר הבא:

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

ונקבל שהאיברים הם $\{\text{id}, \sigma, \sigma^2, \dots, \sigma^{n-1}, \tau, \tau\sigma, \tau\sigma^2, \dots, \tau\sigma^{n-1}\}$. בפרט נקבל כי $|D_n| = 2n$ ושעבור $n > 2$ החבורה אינה אבלית כי $\tau\sigma \neq \sigma\tau$. (למי שכבר מכיר איזומורפיזמים ודאו שאתם מבינים כי $D_3 \cong S_3$, אבל עבור $n > 3$ החבורות D_n ו- S_n אינן איזומורפיות).

5.2 מחלקות שמאליות וימניות

הגדרה 5.5. תהי G חבורה, ותהי $H \leq G$. לכל $a \in G$ נגדיר מחלקות (cosets):

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

2. המחלקה הימנית של a ביחס ל- H היא הקבוצה $Ha = \{ha \mid h \in H\}$.

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

הערה 5.6. עבור איבר היחידה e תמיד מתקיים $eH = H = He$. אם החבורה G היא אבלית, אז המחלקה השמאלית של a ביחס ל- H שווה למחלקה הימנית:

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

דוגמה 5.7. 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

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

תרגיל 5.8. תנו דוגמה לחבורה G , תת-חבורה H ואיבר $a \in G$ כך ש- $aH \neq Ha$.

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

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

אפשר להזכר מההרצאה שמחלקות הן למעשה מחלקות שקילות. במקרה זה המחלקות השמאליות הן

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

כלומר $G/H = \{H, (1\ 3)H, (2\ 3)H\}$. נשים לב שאיחוד כל המחלקות הוא G , וזהו איחוד זר. כלומר שתי מחלקות aH, bH הן או שוות $aH = bH$ או זרות $aH \cap bH = \emptyset$. דוגמה אחרת (אם יש זמן): נבחר $G = GL_2(\mathbb{Q})$, ותהי $H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\}$ תת-חבורה של G . נבחר $g = \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}$, ונחשב

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

וקל לראות כי לא רק ש- $gH \neq Hg$, אלא גם $gH \not\subseteq Hg$.

הגדרה 5.9. מספר המחלקות (השמאליות) של H ב- G נקרא האינדקס (השמאלי) של H ב- G ומסומן $[G : H]$.
 ככל שהאינדקס קטן יותר, כך תת-חבורה H גדולה יותר. בפרט, $[G : H] = 1$ אם ורק אם $H = G$.

הערה 5.10. ישנה התאמה חח"ע ועל בין מחלקות שמאליות של $H \leq G$ ובין מחלקות ימניות לפי $gH \mapsto Hg^{-1}$. ניתן להבין התאמה זאת מכך שכל חבורה סגורה להופכי: $H^{-1} = H$ נחשב.

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

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

תרגיל 5.11. מצאו חבורה G ותת-חבורה H כך ש- $[G : H] = \infty$.

פתרון. נביא שתי דוגמאות:

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

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

$$[G : H] = \aleph_0 \text{ ולכן}$$

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

$$K = \mathbb{Q} \times \{0\} \leq H$$

5.3 משפט לגראנז' ושימושים

משפט 5.12 (משפט לגראנז'). תהי G חבורה ו- $H \leq G$. אז $|G| = [G : H] |H|$.

הערה 5.13. המשפט נכון עבור חשבון עוצמות. במקרה שהחבורה G היא סופית נקבל $[G : H] = \frac{|G|}{|H|}$, כלומר הסדר של תת-חבורה H מחלק את סדר החבורה G . אנו יודעים כי $o(a) = |\langle a \rangle|$ לכל $a \in G$, ולכן הסדר של כל איבר מחלק את סדר החבורה.

טענה 5.14. תהיינה $K \leq H \leq G$ שרשרת תת-חבורות של חבורה סופית. אזי $[G : K] = [G : H][H : K]$. אתגר: הוכיחו זאת ללא ההנחה ש- G סופית, אלא רק שהאינדקסים של H ב- G ושל K ב- H הם סופיים.

הערה 5.15. נזכר בטענה ש- $o(a) \mid m$ אם ורק אם $a^m = e$. כעת אפשר להסיק שלכל איבר a בחבורה סופית G מתקיים $a^{|G|} = e$.

תרגיל 5.16. תהא G חבורה מסדר 8. הוכיחו:

1. אם G היא ציקלית, אז קיימת תת-חבורה של G מסדר 4 (למה ברור כי תת-חבורה ציקלית?).

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

3. מצאו דוגמה נגדית לסעיף הקודם אם G אבלית.

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

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

2. תהא G חבורה לא אבלית. לפי משפט לגראנז', הסדר של כל איבר בחבורה סופית מחלק את סדר החבורה. לכן הסדרים האפשריים היחידים בחבורה מסדר 8 הם 1, 2, 4 או 8 (לא בהכרח כל הסדרים משתתפים).

יש רק איבר אחד מסדר 1 והוא איבר היחידה. לא ייתכן כי כל שאר האיברים הם מסדר 2, שכן לפי תרגיל שראינו נקבל כי G אבלית. אין בחבורה איבר מסדר 8, שכן אז היא תהיה ציקלית, וכל חבורה ציקלית היא אבלית. מכאן קיים איבר, נאמר $a \in G$, שהוא מסדר 4. הסדר של איבר הוא הסדר של תת־החבורה הציקלית $\{e, a, a^2, a^3\}$ שהוא יוצר.

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

תרגיל 5.17 (אם יש זמן). הכלילו את התרגיל האחרון: תהא G חבורה לא אבלית מסדר 2^t עבור $t > 2$. אזי קיימת ב- G תת־חבורה ציקלית מסדר 4.

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

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

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

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

תרגיל 5.18. הוכיחו שחבורה סופית היא מסדר זוגי אם ורק אם קיים בה איבר מסדר 2.

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

הכיוון (\Leftarrow) לא הרבה יותר מסובך. אם אין איברים מסדר 2, אז ניתן להצמיד כל איבר להופכי שלו (שהוא איבר ששונה ממנו), ויחד עם איבר היחידה נקבל מספר אי זוגי של איברים.

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

משפט 5.19 (משפט אוילר 2). לכל $a \in U_n$ מתקיים $a^{\varphi(n)} \equiv 1 \pmod{n}$.

דוגמה 5.20. יהי p מספר ראשוני, ויהי $a \in U_p$. מתקיים $\varphi(p) = p - 1$ ולכן $a^{p-1} \equiv 1 \pmod{p}$. זהו למעשה משפט פרמה הקטן. (העשרה אם יש זמן: פונקציית קרמייקל (Carmichael) $\lambda(n)$ מוגדרת להיות המספר הטבעי m הקטן ביותר כך ש- $a^m \equiv 1 \pmod{n}$ לכל a שזר ל- n . ממשפט לגראנז' נקבל $\lambda(n) | \varphi(n)$. נסו למצוא דרך לחשב את $\lambda(n)$, ומתי $\lambda(n) \neq \varphi(n)$.)

תרגיל 5.21. מצאו את שתי הספרות האחרונות של $88211^{4039} + 2015$.

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

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

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

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

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

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

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

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

ולכן שתי הספרות האחרונות הן 06.