

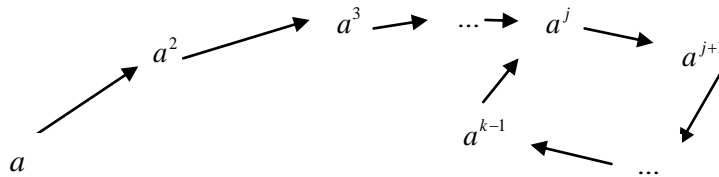
תרגול 2: איברים הפיכים במונואיד, חבורות אוילר, תת-חבורות

הגדרה: מונואיד M הוא בעל צמצום משמאל אם $\forall a, b, c \in M, ab = ac \Rightarrow b = c$. בצורה דומה מגדירים בעל צמצום מימין/בעל צמצום.

טענה: מונואיד סופי M בעל צמצום משמאל הוא חבורה.

הוכחה א: צ"ל שלכל איבר קיים איבר הפכי. יהי $a \in M$ נגדיר פונקציה $M \rightarrow M$ ע"י $l_a(x) = ax$ פונקצית הכפלה משמאל ב a . הפונקציה היא חח"ע בגלל צמצום משמאל ($l_a(x) = l_a(y) \Rightarrow ax = ay \Rightarrow x = y$), וכיוון שהמונואיד סופי נקבל שהפונקציה היא על (לפי עקרון שובר היונים).

הוכחה ב: כנ"ל צ"ל שלכל איבר קיים איבר הפכי. ניצור סדרה של חזקות a, a^2, a^3, a^4, \dots עבור איבר $a \in M, e \neq a$. כיוון שהמונואיד סופי, קיימות שתי חזקות $j < k$ כך ש $a^j = a^k$. נמחיש זאת בעזרת הציור הבא (כל חץ מייצג הכפלה ב a):



כעת $a^j e = a^j = a^{j+(k-j)} = a^j a^{k-j}$. לפי תכונת הצמצום, נקבל $e = a^{k-j}$. כעת כיוון ש $k > j$ נקבל $k - j \geq 1$, כיוון ש $e \neq a$ בהכרח $k - j \geq 2$. לכן נקבל ש $e = a^{k-j-1} a = a a^{k-j-1}$. כלומר $a^{-1} = a^{j-k-1}$.

תרגיל:

1. אם A אגודה סופית, אזי קיים $a \in A$ כך ש $a^2 = a$.
2. הראו שזה לאו דוקא נכון אם A אגודה אינסופית.
3. אם A חבורה אזי $a^2 = a \Rightarrow a = e$.

פתרון:

1. בדומה להוכחה ב' בתרגיל הקודם, נבנה סדרה של חזקות עבור $a \in A$: a, a^2, a^3, a^4, \dots . כיוון

שהאגודה סופית, נקבל שבהכרח קיימות שתי חזקות $j < k$ כך ש $a^j = a^k$. נטען שניתן להניח

שמתקיים $j \geq 2$, כיוון שלכל $t \geq 0$ מתקיים (באינדוקציה על t):

$$a^{k+t(k-j)} = a^k a^{t(k-j)} = a^k a^{k-j} a^{(t-1)(k-j)} = a^j a^{k-j} a^{(t-1)(k-j)} = a^k a^{(t-1)(k-j)} = \dots = a^k$$

ולכן ניתן להגדיל את k כרצוננו. כעת נשים לב ש $a^{j+i} = a^j a^i = a^k a^i = a^{k+i}$. נמצא i מתאים

כך שיתקיים: $2(j+i) = k+i$. מכאן ש $i = k - 2j$.

2. לדוגמא ב $(\mathbb{N}, +)$ הטענה לא מתקיימת. $2a = a \Rightarrow a = 0 \notin \mathbb{N}$.

3. מכפילים בהפכי של a בשני האגפים.

טענה: קבוצת האיברים ההפיכים $U(M)$ במונואיד M היא חבורה.

הוכחה: סגירות: אם a, b הפיכים, אזי $(ab)^{-1} = b^{-1}a^{-1}$ כלומר ab הפיך. קיום הפכי: שימו לב שלדעת

שאיבר הפיך זה לא מספיק, צריך גם להוכיח שההפכי שייך לקבוצה – כלומר במקרה זה יש להוכיח

שההפכי הפיך. שאר התכונות – תרגיל בית.

דוגמאות:

1. קבוצת הפונקציות $F = \{f : X \rightarrow X\}$ היא מונואיד עם פעולת ההרכבה, ואיבר היחידה היא

פונקצית הזהות. $U(F)$ היא קבוצת הפונקציות החח"ע ועל (ההפיכות) מ X ל X .

2. קבוצת כל המטריצות $M_n(F)$ מגודל $n \times n$ מעל שדה F , היא מונואיד עם פעולת כפל מטריצות

ומטריצת הזהות היא איבר היחידה. מתקיים $U(M_n(F)) = GL_n(F)$.

חבורת אוילר:

חשיבות מיוחדת יש לקבוצת האיברים ההפיכים ב $(\mathbb{Z}_n, *, 1)$ אשר לפי הסימונים הנ"ל תסומן ב-

$$U(\mathbb{Z}_n, *)$$

הגדרה: נקרא לחבורות מהצורה $U((\mathbb{Z}_n, *, 1))$ חבורות אוילר, ונסמן ב U_n או ב $Euler(n)$.

דוגמא: נחשב את החבורה U_6 . נבנה תחילה את לוח הכפל של \mathbb{Z}_6 :

*	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

(השמטנו את 0 מהטבלה כי הכפל בו תמיד 0). רואים ש $U_6 = \{1, 5\}$. ההפכי של 1 הוא 1, וההפכי של 5 הוא 5.

טענה: איבר $a \in (\mathbb{Z}_n, *, 1)$ הפיך (כפלית) אם ורק אם $\gcd(a, n) = 1$.

הוכחה:

$\gcd(a, n) = 1$ אם ורק אם (לפי למת בזו) קיימים u, v שלמים כך ש $au + nv = 1$ לכן כאשר נעבור ל $\text{mod } n$, נקבל $au \equiv 1 \pmod{n}$, כלומר a הפיך.

תרגיל בית:

ניתן להוכיח את הכיוון \Rightarrow גם בצורה "אלגברית יותר": הראו שהקבוצה $\{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$ הוא מונואיד (כפלי) בעל צמצום, ולכן ע"פ טענה שהראינו קודם, נקבל שהקבוצה הנ"ל היא חבורה, ובפרט כל האיברים המקיימים $\gcd(a, n) = 1$ הם הפיכים.

מסקנה: $U_n = \{a \in \mathbb{Z}_n \mid 1 \leq a \leq n-1, \gcd(a, n) = 1\}$.

דוגמאות: $U_{14} = \{1, 3, 5, 9, 11, 13\}$, $U_{12} = \{1, 5, 7, 11\}$.

אם p ראשוני, אזי $U_p = \mathbb{Z}_p^*$, זאת כיוון שכל $1 \leq a < p$ הוא זר ל p .

תרגיל: האם ל 5 קיים הפיך כפלי ב \mathbb{Z}_{10} ?

פתרון: לא. כיוון ש 5 אינו זר ל 10.

הגדרה: פונקציית אוילר $\varphi(n)$, היא פונקציה המחזירה את מספר האיברים בחבורה U_n (כלומר מספר הטבעיים הקטנים ל n וזרים לו). לדוגמא, $\varphi(p) = p - 1$ עבור p ראשוני, $\varphi(12) = 4$, $\varphi(14) = 6$.

תרגיל בית: חשבו את $\varphi(pq)$ כאשר p, q ראשוניים (טפלו גם במקרה $p = q$).

תתי חבורות:

תת חבורה: תהי $(G, *, e)$ חבורה אז תת קבוצה $H \subseteq G$ תקרא תת חבורה של G אם H חבורה ביחס לפעולה $*$. מסמנים $H \leq G$.

טרמינולוגיה: קוראים לחבורה $\{e\}$ החבורה הטריוויאלית. כאשר אומרים תתי-החבורות הטריוויאליות של חבורה G , מתכוונים ל- $\{e\}, G$.

דוגמאות לת"ח

$$1. (\mathbb{Z}, +, 0) \leq (\mathbb{Q}, +, 0)$$

2. האם: $\mathbb{Z}_3 \leq \mathbb{Z}_6$? תשובה: לא!! כי פעולת החבורה היא שונה. למה אנחנו מתכוונים בפעולות שונות? שימו לב ש 2 הוא ההפכי של 1 ב- \mathbb{Z}_3 , אבל ב \mathbb{Z}_6 זה לא נכון. בצורה דומה $\mathbb{Z}_n \not\leq \mathbb{Z}$.

3. קבוצת כל החזקות של איבר מסוים בחבורה היא ת"ח. כלומר אם G חבורה, ו- $x \in G$ אזי $\{x^n \mid n \in \mathbb{Z}\} \leq G$. קבוצת כל החזקות החיוביות היא אגודה, קבוצת כל החזקות הלא-שליליות היא מונואיד.

4. יהי Ω_n אוסף הפתרונות של המשוואה $z^n = 1$ ב \mathbb{C} . אזי $\Omega_n \leq \mathbb{C}^*$. נראה זאת: נניח ש $a, b \in \Omega_n$, אז $a^n = b^n = 1$. אזי $(ab)^n = a^n b^n = 1$ (בגלל האבלייות של \mathbb{C}^*). עבור $a \in \Omega_n$ ניקח את $a^{-1} \in \mathbb{C}^*$. אזי $(a^{-1})^n = (a^n)^{-1} = 1$ ולכן $a^{-1} \in \Omega_n$. נשים לב ש $\Omega_n = \{cis(\frac{2\pi k}{n}) \mid 0 \leq k \leq n-1\}$, כאשר $cis(\alpha)$ הוא סימון מקוצר ל $cis(\alpha) = \cos(\alpha) + i \sin(\alpha)$

$$(לדוגמא: $cis(30) = \cos(30) + i \sin(30) = \frac{\sqrt{3}}{2} + \frac{1}{2}i$)$$

$$\left(\text{cis}\left(\frac{2\pi k}{n}\right) \right)^n = \text{cis}(2\pi k) = 1 \text{ ולכן } \text{cis}(\alpha)\text{cis}(\beta) = \text{cis}(\alpha + \beta) \text{ ש זאת כיוון ש}$$

ל Ω_n קוראים חבורת שורשי- n של היחידה.

קריטריונים לבדיקה האם תת-קבוצה היא ת"ח:

משפט קיצור הדרך 1:

תהי H תת קבוצה לא ריקה של G . אז $H \leq G$ אם ורק אם:

$$\forall a, b \in H, ab \in H \quad (1)$$

$$\forall a \in H, a^{-1} \in H \quad (2)$$

משפט קיצור הדרך 2:

תהי H תת קבוצה לא ריקה של G . אז $H \leq G$ אם ורק אם:

$$\forall a, b \in H, ab^{-1} \in H$$

תרגיל: הראו שהתת-חבורות היחידות של \mathbb{Z} הן מהצורה $n\mathbb{Z}$.

פתרון: תחילה נראה שמתקיים $n\mathbb{Z} \leq \mathbb{Z}$. ע"פ משפט קיצור הדרך מספיק להראות שלכל $a, b \in n\mathbb{Z}$

מתקיים $a - b \in n\mathbb{Z}$ (שימו לב לשינוי הקריטריון לכתוב החיבורי). כיוון ש $a, b \in n\mathbb{Z}$ אזי קיימים

$$a', b' \in \mathbb{Z} \text{ כך ש- } a = na', b = nb' \text{ . לכן } a - b = na' - nb' = n(a' - b') \in n\mathbb{Z} \text{ . כנדרש.}$$

כעת, האם יש ל \mathbb{Z} ת"ח מצורה שונה? תהי $H \leq \mathbb{Z}$, $\{0\} \neq H$, וניקח את $0 < n \in H$ המינימלי, ונטען ש

$$H = n\mathbb{Z} \text{ . יהי } k \in H \text{ ונחלק את } n \text{ ב } k \text{ חלוקה עם שארית: } k = nq + r, 0 \leq r < n \text{ ואז נקבל}$$

$$k - nq = r \in H \text{ וזה יכול להיות רק אם } r = 0 \text{ (אחרת סתירה למינימליות נ). בצורה דומה ניתן להראות}$$

$$\text{שכל ת"ח של } n\mathbb{Z} \text{ הם מהצורה } m\mathbb{Z} \text{ כאשר } n|m \text{ .}$$

הערה: אם $A, B \leq G$ וגם $A \subseteq B$ אזי בוודאי שגם $A \leq B$ (אין צורך להוכיח זאת, זה נובע ישירות

מהגדרה, הרבה סטודנטים מנסים להוכיח זאת בעזרת משפטי קיצור הדרך).

תרגיל: אם G חבורה סופית ו- H תת-קבוצה של G אזי $H \leq G$ אם ורק אם $H \neq \emptyset$ וגם

$$x, y \in H \Rightarrow xy \in H$$

הוכחה: כיוון \leq ברור. בכיוון השני, מספיק לפי משפט קיצור הדרך להראות $\forall a \in H, a^{-1} \in H$. יהי

$$e \neq a \in H \text{ (אם } H = \{e\} \text{ אזי סיימנו). לפי התנאי, מתקיים } a \in H \Rightarrow a^2 = aa \in H \text{ , ובאינדוקציה רואים}$$

שכל החזקות החיוביות של a הן ב H . אבל החבורה היא סופית, ולכן בסדרה $a, a^2, a^3, \dots, a^n, \dots$ קיימים $i < j$ כך ש $a^i = a^j$ ונקבל $a^{j-i} = e$, ומכאן נקבל ש- $a^{-1} = a^{j-i-1} \Leftarrow aa^{j-i-1} = a^{j-i-1}a = e$.