

מופשטת 1 - תרגול 3

28 באוקטובר 2015

תתי חבורות

הגדרה 0.1 תהי $(G, *)$ חבורה. אם $H \subseteq G$ ו- $H \neq \emptyset$ כך ש- $(H, *)$ היא גם חבורה, נאמר ש- H תת חבורה של G , ונסמן $H \leq G$.

דוגמאות: 1. $4\mathbb{Z} \leq 2\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$

2. $\mathbb{Q}^* \leq \mathbb{R}^*$

3. נשים לב ש- \mathbb{Z}_n אינה תת חבורה של \mathbb{Z} כי זאת לא אותה פעולה.

4. $SL_n(F) \leq GL_n(F)$

תרגיל: יהי $\Omega_n = \left\{ cis\left(\frac{2\pi k}{n}\right) : 0 \leq k \leq n-1 \right\}$ אוסף הפתרונות של המשוואה

$z^n = 1$ ב- \mathbb{C} . למשל אם $n = 4$ אז $\Omega_4 = \{1, i, -1, -i\}$.

הוכיחו:

1. $\Omega_n \leq (\mathbb{C}^*, \cdot)$

2. אם $m|n$ אז $\Omega_m \leq \Omega_n$

פתרון: 1. קודם כל, $\Omega_n \neq \emptyset$ כי לכל $n \in \mathbb{N}$ $1 \in \Omega_n$. כעת, יהיו $a, b \in \Omega_n$, אזי מתקיים: $a^n = b^n = 1$. לכן: $a^{-n} = (a^n)^{-1} = 1^{-1} = 1$, לכן יש סגירות להופכי. כמו כן, \mathbb{C} אבלי, ולכן $(ab)^n = a^n b^n = 1 \cdot 1 = 1$, לכן יש סגירות לכפל.

2. מספיק להראות את ההכלה $\Omega_m \subseteq \Omega_n$. ובכן, נתון ש- $m|n$, לכן יש k כך ש- $n = mk$. יהי $a \in \Omega_m$, כלומר $a^m = 1$. צריך להראות: $a^n = 1$.

$a^n = a^{km} = (a^m)^k = 1^k = 1$

תרגיל: הוכיחו שחיתוך של תתי חבורות הוא תת חבורה.

פתרון: יהיו $H_1, H_2 \leq G$ תתי חבורות. $1 \in H_1, H_2$ ולכן $1 \in H_1 \cap H_2$ ובפרט החיתוך לא ריק.

יהי $a \in H_1 \cap H_2$. תת חבורה ולכן $a^{-1} \in H_1$. כנ"ל לגבי H_2 . לכן $a^{-1} \in H_1 \cap H_2$. יהיו $a, b \in H_1 \cap H_2$. תת חבורה ולכן $ab \in H_1$. כנ"ל לגבי H_2 . לכן $ab \in H_1 \cap H_2$. תרגיל: תהי G חבורה סופית. כל H תת קבוצה לא ריקה סגורה לכפל של G היא תת חבורה.

הוכחה: צריך להראות את קיום ההופכי. יהי $a \in H$. בגלל ש- H סגורה לכפל, לכל n טבעי $a^n \in H$. בגלל ש- G סופית יש $n \neq m$ כך ש- $a^n = a^m$. בה"כ $n > m$. נכפיל בהופכי של a^m ונקבל $1 = a^{n-m}$. כמו כן, $a^{n-m-1} \in H$, ללכן לכל איבר ב- H יש הופכי ב- H . הגדרה: תהי G חבורה ויהי $a \in G$. אם כל איבר ב- G הוא חזקה (חיובית או שלילית) של a אז נאמר ש- G נוצרת ע"י a . אם קיים איבר כך ש- G נוצרת על ידו, אומרים ש- G ציקלית.

סימון: $G = \langle a \rangle = \{a^k : k \in \mathbb{Z}\}$

דוגמאות:

1. \mathbb{Z} נוצרת ע"י 1. שימו לב שהיוצר לא חייב להיות יחיד. למשל במקרה שלנו גם -1 הוא יוצר.

2. $n\mathbb{Z} = \langle k \rangle$

3. \mathbb{Z}_n נוצר ע"י 1.

4. \mathbb{Z}_6 למשל נוצר גם ע"י 1 וגם ע"י 5.

הגדרה: סדר של חבורה = מס' האיברים בחבורה (העוצמה שלה כקבוצה) ומסומן: $|G|$.

לדוגמא: $|\mathbb{Z}_n| = n, |\mathbb{Z}| = \infty$

דוגמא חשובה: פונקציית אוילר: $\varphi(n) = |U_n|$

עבור p ראשוני, אנחנו כבר יודעים ש $\varphi(p) = p - 1$.

ניתן להראות (בהרצאה) כי לכל ראשוני p ולכל k טבעי, $\varphi(p^k) = p^k - p^{k-1}$, כמו כן, אם $(a, b) = 1$ אזי $\varphi(ab) = \varphi(a)\varphi(b)$. מכאן מתקבלת ההכללה:

יהי $n = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ אזי $\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_n}\right)$

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

הגדרה: סדר של איבר: יהי $a \in G$, הסדר של a , מסומן $o(a)$ הוא: $\min\{n \in \mathbb{N} : a^n = 1\}$ אם לא קיים כזה, נאמר שהסדר הוא אינסוף.

דוגמאות:

1. $o(5) = 2, U_6$

2. נתבונן ב $(GL_2(\mathbb{R}), \cdot)$, $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. אזי $o(b) = 3$ כי $b^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$

$b^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

טענה: $|G| = n$ היא ציקלית אמ"ם קיים איבר מסדר n

לדוגמא, ב U_8 קל לבדוק ש $o(3) = o(5) = o(7) = 2$ ולכן החבורה אינה ציקלית.

תרגיל: תהי G חבורה אבלית. הוכיחו שאוסף האיברים מסדר סופי הוא תת חבורה.

פתרון: נסמן את האוסף הנ"ל ב A . נוכיח את התנאים הדרושים:

1. $A \neq \emptyset$ כי $e \in A$

2. סגירות לפעולה: יהיו $a, b \in A$. אז יש n, m טבעיים כך ש $a^n = b^m = e$. אז:

$(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = e^m e^n = e$

3. סגירות להופכי: יהי $a \in A$. יש n כך ש $a^n = e$, אז $a \cdot a^{n-1} = e$ לכן $a^{-1} = a^{n-1}$

וכבר ראינו שיש סגירות לפעולה.

תרגיל: תהי G חבורה והיו $a, b \in G$ מסדר סופי. האם גם ab בהכרח מסדר סופי?

פתרון: ראינו כבר שאם G אבלית, אז זה נכון. באופן כללי, לא. נמצא דוגמא נגדית: נקח

$(GL_2(\mathbb{R}), \cdot)$, ונתבונן ב: $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. ניתן לבדוק שמתקיים:

$a^4 = b^3 = I$. אולם $ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ אינו מסדר סופי כי $(ab)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

מספר תכונות של הסדר:

1. אם $g^n = 1$ אז $o(g) | n$

2. אם G חבורה ציקלית סופית מסדר n אז לכל $g \in G$ מתקיים $g^n = e$

3. בחבורה סופית הסדר של כל איבר הוא סופי (הוכחנו כבר משהו דומה)

4. $o(a^i) \leq o(a)$

5. $o(a) = o(a^{-1})$

נוכיח את 5:

מספיק להראות ש $o(a^{-1}) \leq o(a)$ (כי $(a^{-1})^{-1} = a$). ובכן, נניח $o(a) = n$, אז $a^n = 1$.
 $(a^{-1})^n = (a^n)^{-1} = 1^{-1} = 1$. לכן $o(a^{-1}) \leq n$.
מקרה שני, נניח שהסדר של a אינסופי. אז גם הסדר של a^{-1} אינסופי, כי אם הוא היה איזהו n , אז מהמקרה הראשון, היינו מקבלים ש $o(a) = n$, בסתירה.
תזכורת:

בהנתן שתי חברות A, B ניתן להגדיר את המכפלה הקרטזית שלהן כ: $A \times B = \{(a, b) : a \in A, b \in B\}$ והפעולה היא רכיב-רכיב. הראתם בשיעורי בית שזאת אכן חבורה.

תרגיל: זה טריוויאלי שאם $N \leq A$ ו $M \leq B$ אז $N \times M \leq A \times B$. תנו דוגמא לתת חבורה של $A \times B$ שאינה מכפלה קרטזית של תתי חבורות.
פתרון: נסתכל על $A = B = \mathbb{Z}_2$, ועל $\langle (1, 1) \rangle$ בתוך $\mathbb{Z}_2 \times \mathbb{Z}_2$. האיברים בחבורה הם בעצם: $(0, 0), (1, 1)$, וברור שזאת לא מכפלה.
תרגיל: האם $\mathbb{Z}_n \times \mathbb{Z}_n$ היא ציקלית?

פתרון: הסדר של החבורה הוא n^2 . ע"מ שהיא תהיה ציקלית יש למצוא איבר שהסדר שלו הוא n^2 . אולם לכל $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n$ מתקיים: $n(a, b) = (na, nb) = (0, 0)$ ולכן הסדר של כל איבר קטן או שווה ל n .