

הרצאה 3  
תת-חבורות, תת-חוגים ותת-שדות

**הגדרה 1.** תהי  $(G, \cdot)$  חבורה כלשהי. תת-קבוצה  $H \neq \emptyset$  של  $G$  נקראת תת-חבורה של  $G$  (סימון  $H \leq G$ ) אם היא חבורה ביחס לפעולה של  $G$ .

מהגדרה זו נובע ש- $H \leq G \wedge F \leq H \Rightarrow F \leq G$ .

**טענה 1.** תת-קבוצה  $H \neq \emptyset$  תהיה תת-חבורה אם ורק אם היא מקיימת שלושה תנאים:

א.  $\forall a \in H \forall b \in H \quad ab \in H$

ב.  $e \in H$

ג.  $\forall a \in H \quad a^{-1} \in H$

**הוכחה.**

$H \leq G \Leftrightarrow$  א-ג.

א.  $H$  מקיימת 4 אקסיומות של חבורה, בפרט היא מקיימת את אקסיומת סגירות השקולה לתנאי א' של הטענה.

ב. בחבורה  $H$  יש איבר היחידה כלפי הכפל:  $e_H$ . לכן  $e_H \cdot e_H = e_H$ . בחבורה  $G$  יש איבר הפכי ל- $e_H$ . לכן

$$e_H \cdot e_H = e_H \Rightarrow (e_H)^{-1} \cdot (e_H \cdot e_H) = (e_H)^{-1} \cdot e_H = e \Rightarrow e_H = e \Rightarrow e \in H$$

ג. מפני ש- $H$  חבורה, לכל  $a \in H$  קיים  $b \in H$  כך ש- $a \cdot b = b \cdot a = e_H = e$ . נכפיל את השוויון  $a \cdot b = e$  משני הצדדים ב- $a^{-1}$ . אז נקבל  $b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot e$ . לכן

$$a^{-1} \in H$$

$H \leq G \Rightarrow$  א-ג.

תנאים א-ג הן אקסיומות G1, G3, G4 בהתאם. אקסיומה G2 נובעת מהחוק האסוציאטיבי שמתקיים בכל חבורה  $G$ . מ.ש.ל.

מהגדרה של תת-חבורה נובע שכל תת-חבורה  $H$  של חבורה  $G$  היא חבורה בפני עצמה ביחס לפעולה של  $G$ .

בכל חבורה  $G$  תמיד ישנן 2 תת-חבורות: היא עצמה ותת-חבורה טריביאלית:  $\{e\}$ , כלומר תמיד מתקיים ש- $G \leq G$  ו- $\{e\} \leq G$ .

**טענה 2.** תת-קבוצה  $H \neq \emptyset$  תהיה תת-חבורה אם ורק אם היא מקיימת:

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

**הוכחה.**

אם  $H$  תת-חבורה, אז היא מקיימת את התנאים א-ג של טענה 1 ולכן היא גם מקיימת את התנאי  $\forall a \in H \forall b \in H \quad ab^{-1} \in H$ .

נניח עכשיו ש- $H$  מקיימת  $\forall a \in H \forall b \in H \quad ab^{-1} \in H$  ונוכיח שהיא מקיימת את התנאים א-ג של טענה 1.

ניקח  $h \in H$  (זה אפשרי, כי  $H \neq \emptyset$ ) כלשהו. אז  $e = hh^{-1} \in H$  ותנאי ב' מתקיים.

ניקח  $h \in H$  כלשהו. אז  $h^{-1} = e \cdot h^{-1} \in H$  ותנאי ג' מתקיים.

ניקח  $a, b \in H$  שני איברים כלשהם. הוכחנו ש- $b^{-1} \in H$ . לכן

$$a \cdot b = a \cdot (b^{-1})^{-1} \in H \quad \text{מתקיים.} \quad \text{מ.ש.ל.}$$

**דוגמה 1.** נביט בחבורה  $\mathbb{Z}$  ביחס לחיבור. לכל מספר טבעי  $n$  הקבוצה  $n\mathbb{Z} := \{nx \mid x \in \mathbb{Z}\}$  היא תת-חבורה ביחס לחיבור, מפני שהיא מקיימת את התנאים של טענה 2.

**דוגמה 2.** נביט בחבורה  $\mathbb{Z}_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$  ביחס לחיבור. תת-הקבוצה  $H = \{0,3,6,9\}$  היא תת-חבורה ביחס לחיבור. תת-הקבוצה  $H = \{0,3,6,10\}$  לא תת-חבורה מפני ש- $3+6=9 \notin H$ .

**טענה 3.** אם  $H \leq G, F \leq G$ , אז  $H \cap F \leq G$ .  
**הוכחה.**

$H \cap F \neq \emptyset$  מפני ש- $e \in H \cap F$ . מהטענה 2 נובע שמספיק להוכיח ש-  
 $xy^{-1} \in H \cap F$  לכל  $x, y \in H \cap F$  ולכל  $x \in H \cap F, y \in H \cap F$  שייכים לחבורה  $H$  לכן  
 $xy^{-1} \in H$ . באופן דומה ניתן להוכיח ש- $xy^{-1} \in F$ . מכאן נובע ש- $xy^{-1} \in H \cap F$ .  
 מ.ש.ל.

באופן דומה ניתן להוכיח שחיתוך של מספר כלשהו של תת-חבורות גם היא תת-חבורה.

**בעיה 2.** הוכח שאיחוד  $H \cup F$  של שתי תת-חבורות יהיה תת-חבורה אם ורק אם  $H \subseteq F \vee F \subseteq H$ .

**הגדרה 2.** תת-קבוצה  $S \neq \emptyset$  של חוג  $R$  נקראת **תת-חוג** אם היא מקיימת את התנאים הבאים:

- א.  $S$  תת-חבורה של חבורה  $(R, +)$ .
- ב.  $S$  סגורה ביחס לכפל.
- ג.  $1 \in S$ .

**טענה 4.** כל תת-חוג  $S$  של חוג  $R$  הוא חוג בפני עצמו (ביחס לפעולות של  $R$ ).  
**הוכחה.**

מפני ש- $S$  תת-חבורה של החבורה  $(R, +)$ , היא מקיימת את האקסיומות A1-A5 של חוג.

מתנאים ב' ו ג' של ההגדרה 2 נובע ש- $S$  מקיימת את האקסיומות M1, M3. האקסיומה M2 (החוק האסוציאטיבי לכפל) והחוקים הדיסטריבוטיביים נובעים מהחוקים המתאימים שמתקיימים ב- $R$ .  
 מ.ש.ל.

לא כל תת-קבוצה של חוג  $R$  שהיא חוג ביחס לפעולות  $R$  תהיה תת-חוג במובן של ההגדרה 2 (ראה את הדוגמה 3).

**דוגמה 3.** נביט בחוג  $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$  תת-הקבוצה  $H = \{0,2,4\}$  היא לא תת-חוג לפי ההגדרה 2 מפני ש-1 לא שייך ל- $H$ . אבל  $H$  מקיימת את כל האקסיומות של חוג ביחס לפעולות ב- $\mathbb{Z}_6$ . למשל, איבר-היחידה של  $H$  ביחס לכפל שווה ל-4.

**דוגמה 4.** נביט בתת-הקבוצה  $S = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$  של חוג המטריצות

$M_2(\mathbb{R})$ . בדיקה ישירה מראה שהקבוצה  $S$  מקיימת את כל התנאים של ההגדרה

2, ולכן היא תת-חוג של  $M_2(\mathbf{R})$ .

**הגדרה 3.** תת-קבוצה  $S \neq \emptyset$  של שדה  $R$  נקראת תת-שדה אם היא מקיימת את התנאים הבאים:

א.  $S$  תת-חוג של  $R$ .

ב.  $\forall s \in S \setminus \{0\} \quad s^{-1} \in S$ .

**דוגמה 5.** המספרים הרציונאליים  $\mathbf{Q}$  מהווים תת-שדה של השדה  $\mathbf{R}$ .

**טענה 5.** תת-קבוצה  $S \neq \emptyset$  של שדה  $R$  תהיה תת-שדה אם ורק אם היא מקיימת את התנאים הבאים:

א.  $S$  תת-חבורה של החבורה  $(R, +)$ .

ב.  $S \setminus \{0\}$  תת-חבורה של  $(R^*, \cdot)$ .

**הוכחה.**

אם  $S$  תת-שדה, אז  $S$  תת-חוג ולכן תת-חבורה של החבורה  $(R, +)$ . מהגדרת תת-שדה נובע ש- $S \setminus \{0\}$  סגורה כלפי כפל,  $1 \in S \setminus \{0\}$  ו- $s^{-1} \in S \setminus \{0\}$  לכל  $s \in S \setminus \{0\}$ . לכן  $S \setminus \{0\}$  תת-חבורה של  $(R^*, \cdot)$  (ראה טענה 1). להפך, אם  $S$  מקיימת א-ב, אז  $S$  סגורה כלפי הכפל ו- $1 \in S$ . לכן  $S$  תת-חוג של  $R$ . בנוסף לזה, מסעיף ב' נובע ש- $s^{-1} \in S \setminus \{0\}$  לכל  $s \in S \setminus \{0\}$ . לכן  $S$  תת-שדה. מ.ש.ל.

**בעיה 1.** הוכח שלחוג  $\mathbf{Z}_n$  יש תת-חוג אחד בלבד – הוא עצמו.

**בעיה 2.** הוכח שקבוצות כל המספרים הממשיים מהצורה  $a + b\sqrt{2}$ ,  $a, b \in \mathbf{Q}$  היא תת-שדה של  $\mathbf{R}$ .

**בעיה 3.** יהי  $F$  שדה כלשהו. נבחר איבר  $a \in F$  ונגדיר את קבוצת המטריצות

$$S_a = \left\{ \begin{pmatrix} x & y \\ ay & x \end{pmatrix} \mid x, y \in F \right\} \subseteq M_2(F)$$

א. הוכח ש- $S_a$  תת-חוג של  $M_2(F)$ .

ב. הוכח שאם בשדה  $F$  לא קיים שורש ריבועי ל- $a$  (כלומר,  $a \neq b^2$  לכל  $b \in F$ ) אז  $S_a$  שדה.

**בעיה 4.** הוכח שהקבוצה  $S = \left\{ \frac{a}{2^b} \mid a, b \in \mathbf{Z} \right\}$  היא תת-חוג של  $\mathbf{Q}$ . הוכח ש- $S$  לא

תת-שדה.