

שיעור 1: (אלגברה של גדולים)

בתוכנית: פעולות אלגבריות כפונקציות, סגירות לפעולה, תורת החבורות.

הרחבה:

הגדרה-פעולה בינארית על קבוצה (בניגוד לפונקציות נהוג לסמן בין האיברים), תכונות- חילופיות, אסוציאטיביות. דוגמאות- חיבור, כפל, מכפלה סקלרית, מכפלה וקטורית, הרכבת פונקציות, הרכבת תמורות, max. לא מוגדר: חילוק, שורש ועוד. סגירות לפעול- הגדרה קבוצה סגורה לפעולה.

הגדרת חבורה:

חבורה היא זוג סדור של קבוצה G שסגורה לפעולה בקבוצה $G \times G \rightarrow G$ כך ש:

- 1) הפעולה אסוציאטיבית.
- 2) קיים איבר יחידה (הגדרה על שני הצדדים).
- 3) לכל איבר קיים איבר הופכי (הגדרה לשני הצדדים).

הגדרה: ללא קיום של איבר הופכי המבנה נקרא מונואיד.

דוגמאות:

- Z עם חיבור
- N עם חיבור לא חבורה כן מונואיד
- R עם חיבור R עם כפל לא חבורה לא מונואיד.
- R ללא 0 עם כפל כן חבורה,
- חבורת התמורות,
- חבורת השאריות עם חיבור.
- תהא G חבורה ו- A קבוצה, נגדיר פעולה על G^A , $f * g(a) = f(a) * g(a)$, אז $\langle G^A, * \rangle$ חבורה.

הגדרה: חבורה נקראת אבלית אם $x * y = y * x$. (לעבור על הדוגמאות הקודמות)

טענה: איבר יחידה הוא יחיד (גם במונואיד)
הוכחה: אם e איבר הופכי נוסף אז $e = ee' = e'$

סימון $1_G, 0_G, e_G$.

טענה: איבר הופכי הוא יחיד

הוכחה: יהי b, b' איברים הופכיים ל- a אז $b = be = b(ab') = (ba)b' = eb' = b'$

סימון: $a^{-1}, -a$

הגדרה: לכל $a \in G$ ו- $n \in \mathbb{N}$ נגדיר רקורסיבית:

$$a^{n+1} = a * a^n \text{ ו- } a^0 = e_G$$

עבור מספר שלם שלילי נגדיר $a^{-n} = (a^{-1})^n$.

תרגיל: תהא G חבורה $a \in G$, אזי

$$a^{z_1+z_2} = a^{z_1} * a^{z_2}, \quad (a^{z_1})^{z_2} = a^{z_1 z_2}, \quad (ab)^{-1} = b^{-1} a^{-1}, \quad (a^i)^{-1} = (a^{-1})^i$$

טענה: למשוואה $xa = b$ קיים פתרון יחיד ב- G

הוכחה: קיים פתרון כי לדוגמא נגדיר $x = ba^{-1}$ ואז $xa = b$ והוכחה: $(ba^{-1})a = b(a^{-1}a) = be = b$ הפתרון יחיד כי אם $xa = b$ אז נכפיל את שני האגפים המשוואה **ימין** (הפעולה היא פונקציה ולכן יחס חד ערכי אז אם נכפיל משני האגפים את אותו האיבר נקבל תוצאה זהה) ב- a^{-1} ואז $(xa)a^{-1} = ba^{-1}$ ולכן $x = ba^{-1}$.

מסקנה: חוק הצמצום, אם $xa = ya$ אז $x = y$.

הגדרה-סדר של איבר (לא מוגדר לכל איבר), ה- n הקטן ביותר כך ש- $a^n = e$. מסומן $ord(a)$.

דוגמא: סדר של איבר בחבורת התמורות (חילוף, המעגל המלא) סדר של איבר בחבורת השאריות.

טענה: אם G חבורה סופית אז לכל איבר a קיים סדר קטן או שווה ל- $|G|$. (לא נכון לאינסופית לדוגמא Z) הוכחה: מספיק להוכיח כי קיים m ואז קיים גם הקטן ביותר. נניח כי ב- G יש n איברים, ונתבונן ב-

$$a, a^2, a^3, \dots, a^{n+1}$$

לפי עקרון שובך היונים (הסבר מהיר) יש $i < j$ כך ש- $a^i = a^j$. נכפיל את שני האגפים ב- a^{-i} ואז $a^i a^{-i} = a^{j-i} a^{-i}$ או $a^0 = a^{j-i-i} = a^{j-2i}$ ומתקיים $a^m = a^{i-i} = a^0 = e$.

הגדרה:

תהא $\langle G, * \rangle$ חבורה. $H \subseteq G$ נקראת תת חבורה (ומסמנים $H \leq G$) אם $\langle H, * \rangle_{H \times H}$ היא חבורה.

משפט:

תהא $\langle G, * \rangle$ חבורה ו- $H \leq G$. אזי $H \leq G$ אמ"ם:

1. $e_G \in H$
2. H סגורה לפעולה $*$.
3. $\forall h \in H. h^{-1} \in H$.

הוכחה:

נניח כי $\langle H, * \rangle_{H \times H}$ תת חבורה, אז לפי הגדרה $HxH \rightarrow H$ $\langle H, * \rangle_{H \times H}$ סגורה לפעולה.

קיים איבר e_H ניטרלי לחיבור ביחס לאיבר H , נוכיח כי $e_H = e_G$. מתקיימות המשוואות:

$$e_H * e_H = e_H = e_H * e_G$$

לפי חוק הצמצום נובע כי $e_H = e_G$. מיחידות האיבר ההופכי (כבר הוכחנו כי איבר היחידה הוא אותו איבר יחידה)

נובע כי $\forall h \in H. h^{-1} \in H$.

בכיוון השני, נניח כי $H \subseteq G$ מקיים (1)-(3), אז $|_{H \times H}^*$ אכן פעולה בינארית אסוציאטיבית על H , e_G נייטרלי ל- $*$ ב- G אז בטח ב- H , ודאגנו כי לכל איבר יש איבר הופכי. לכן H חבורה.

דוגמאות:

1. Z בתוך Q . עם חיבור.
2. Q בתוך R עם כפל.
3. באופן כללי אם G חבורה אז $\{e_G\} \leq G$ נקראת החבורה הטריבויאלית.
4. על R^2 עם חיבור חיות והציר הממשי.
5. חבורת התמורות על 5 איברים וכל האיברים שמשאירים את 1 במקום.

הגדרה: תהא $H \leq G$ נגדיר יחס שקילות ב- G באופן הבא: $g_1 \sim_H g_2 \Leftrightarrow g_1 \cdot g_2^{-1} \in H$

הוכחה כי זה יחס שקילות:

רפלקסיבי כי איבר היחידה.

$$\text{סימטרי: } g_2 g_1^{-1} = (g_1 g_2^{-1})^{-1} \in H$$

טרנזיטיבי: ברור.

דוגמא: חבורת השאריות, מה קורה כאשר עושים R מודולו Q עם חיבור?

הערה: מהי $[g]_{\sim_H} = \{gh \mid h \in H\}$ ולכן מסמנים $[g]_{\sim_H} = g \cdot H$ (נקרא co-set או קוסט שמאלי)

טענה: לכל שתי מחלקות שקילות $g_1 H, g_2 H$ הן שוות עוצמה:

$$f: g_1 H \rightarrow g_2 H, \quad f(x) = g_2 g_1^{-1} x$$

מסקנה חשובה 1: (אפילו תרגיל שראינו פעם בבדידה) $|G| = |H| \cdot |G/\sim_H|$

הגדרה: האינדקס של תת חבורה H בחבורה G מגודר כ- $[G:H] = |G/\sim_H|$

מסקנה חשובה 2: אם G חבורה סופית ו- $H \leq G$ אז $|H|$ מחלקת את $|G|$ ומתקיים $[G:H] = \frac{|G|}{|H|}$.

דוגמא: ב- $Z \times Z$ נתבונן ב- $\langle (1,0) \rangle$ אז $Z/\sim_H = "Z"$

חבורה Z_6 עם חיבור. נתבונן ב- $\langle 2 \rangle \leq Z_6$ הסדר של 2 הוא 3 שאכן מחלק את 6.

חוגים

חוג זו שלשה $\langle R, +, * \rangle$ באשר $+$, הן פעולות בינאריות על R אשר מקיימות:

1. $\langle R, + \rangle$ היא חבורה חילופית.
2. $*$ היא פעולה בינארית אסוציאטיבית על R .
3. חוק הפילוג: לכל $a, b, c \in R$. $a * (b + c) = a * b + a * c$

חוג עם יחידה- אם קיים איבר יחידה בכלל.
 חוג חילופי- אם הכפל חילופי.

סימונים:

- 0. איבר ניטרלי בחיבור 0_R .
- 1. איבר ניטרלי בכפל 1_R .
- $n + 1_R = n_R + 1_R$.
- איבר הופכי לחיבור מסומן ב- a .
- איבר הופכי בכפל מסומן a^{-1} .

דוגמא: Z, R, Z_n (גם עבור n לא ראשוני)

דוגמא חשובה: חוג הפולינומים מעל חוג R

הגדרת פולינום: סדרה $p: N \rightarrow R$ נקראת פולינום פורמלי במשתנה X , אם קיים N כך שלכל $n \geq N, p(n) = 0_R$.

מסמנים $p(k) = p_k$ ו- $p = p_0 X^0 + p_1 X^1 + p_2 X^2 \dots + p_{N_p} X^{N_p}$ כאשר $N_p = \min(N | \forall n \geq N, p_n = 0)$ (נקרא המעלה של p).

חיבור פולינומים: $(p + q)(n) = p(n) + q(n)$ מתאים לחיבור סוגריים:

$$(p_0 X^0 + p_1 X^1 + p_2 X^2 \dots + p_{N_p} X^{N_p}) + (q_0 X^0 + p_1 X^1 + p_2 X^2 \dots + p_{N_q} X^{N_q})$$

כפל פולינומים: מתאים לכפל סוגריים (קונבולוציה)

$$(p_0 X^0 + p_1 X^1 + p_2 X^2 \dots + p_{N_p} X^{N_p}) \cdot (q_0 X^0 + p_1 X^1 + p_2 X^2 \dots + p_{N_q} X^{N_q})$$

$$(p + q)(n) = \sum_{k=0}^n p_k q_{n-k}$$

איבר ניטרלי לחיבור- סדרת האפסים, האיבר הניטרלי לכפל $p = 1$.
 נרחיב בהמשך על חוג הפולינומים אבל יש לבדוק עצמאית כי מדובר בחוג חילופי עם יחידה מסומן $R[X]$.

טענות:

1. $0_G, 1_G - a$ יחידים (כבר ראינו את ההוכחה עבור מונואידים).
2. $\forall x \in G, 0_G x = 0_G$.
3. אם $0_G = 1_G$ אז $G = \{0_G\}$ (נקרא החוג הטריוויאלי).
4. $(-1_G)x = -x$.
5. נוסחת הבינום, אם $x \cdot y = y \cdot x$ אז $(x + y)^n = \sum_{k=0}^n \binom{n}{k}_R x^k y^{n-k}$.

הוכחה: 5 זה פשוט נובע מחוק הפילוג וההוכחה כמו שראינו בבדידה.

עבור 2, $0_G x = (0_G + 0_G)x = 0_G x + 0_G x$, נחסיר משני האגפים את $0_G x$ ונקבל: $0_G x = 0_G$.

עבור 3, $x = 1_G x = 0_G x = 0_G$, ולכן $G = \{0_G\}$.

עבור 4, $x + (-1_G)x = 1_G x + (-1_G)x = (1_G + (-1_G))x = 0_G x = x$.

יש הרבה מה לומר על חוג אבל נעצור כאן.

תחום שלמות ושדה

הגדרה: יהי R חוג. איבר $a \in R$ נקרא מחלק 0, אם $a \neq 0_R$ וקיים $b \neq 0_R$ כך ש- $a \cdot b = 0_R$.

הגדרה: חוג חילופי עם יחידה נקרא תחום שלמות אם אין מחלקי 0.

דוגמא: נתבונן ב- Z_4 , $[2]_4 \cdot [2]_4 = [0]_4$, ולכן יש מחלקי 0. אז לא תחום שלמות וכן חוג.

תכונה חשובה בתחום שלמות(חוק הצמצום): $a * b = a * c$ אז $b = c$ (איך לתקן את הניסוח השגוי הזה?)

נדרוש כי a לא 0

הוכחה שגויה: $a^{-1} \dots$

הוכחה נכונה $a * (b + (-c)) = 0_G$ ולכן $a = 0$ או $b + (-c) = 0_G$ ולכן $b = c$.

מבנה שנדבר עליו הרבה בקורס הוא שדה.

הגדרה(שדה):

חוג חילופי עם יחידה $\langle G, +, * \rangle$ נקרא שדה אם:

1. $\langle G \setminus \{0_G\}, * \rangle$ חבורה.

2. $0_G \neq 1_G$.

דוגמאות:

R,Q,Z_2,Z_3,Z_5

טענה: יהי F שדה, אזי F תחום שלמות.

הוכחה: ההוכחה השגויה ממקודם.

מסקנה: Z_n לא שדה ובאופן כללי אם n פריק אז Z_n לא שדה.

הוכחה: יש מחלקי 0 ולכן זה לא שדה.

משפט: אם $F \neq \{0_G\}$ תחום שלמות סופי אז F שדה.

הוכחה: צריך להוכיח קיום של איבר הופכי, וההעתקת ההכפלה חז"ע ולכן עלול להיות הופכי.

מאפיין ו"השלמים" של שדה

הגדרה: יהי F שדה, נגדיר באופן רקורסיבי כמו קודם
 $(-n)_F = -n_F$ ו- $(n+1)_F = n_F + 1_F = 1_F + 1_F + \dots + 1_F$.

זה מגדיר פונקציה $n_F \in Z$. פונקציה זו משמרת חיבור וכפל

תרגיל: $l_F + k_F = (l+k)_F$, $l_F * k_F = (l * k)_F$

הגדרה: המציון (המאפיין) של שדה F , מסומן $char(F)$ הינו המספר הקטן ביותר $p > 0$ כך ש- $p_F = 0_F$ אם קיים כזה, ואם לא קיים כזה, אז $char(F) = 0$.

דוגמה 1.17: $char \mathbb{Q} = char \mathbb{R} = char \mathbb{C} = 0$; אם p ראשוני, אז $char \mathbb{Z}_p = p > 0$.

טענה: יהי F שדה עם $char(F) > 0$ אז $char(F)$ ראשוני.
הוכחה: אחרת, $p = n \cdot m$, ולפי התרגיל $p_F = n_F \cdot m_F = 0_F$ אבל אין מחלקי 0, סתירה.
אז אחד מביניהם שווה 0 בסתירה לכך ש- p_F הקטן ביותר.

תרגיל: הוכיחו הפריכו:

א. אם $a = 0_F$ אז $a = -a$

ב. אם $char(F) \neq 2$ אז $a = -a$ אם $a = 0_F$

הגדרה: תת שדה $F' \subseteq F$ אם הוא שדה ביחס לפעולות $+|_{F' \times F'}$ ו- $*|_{F' \times F'}$.

דוגמא: Q תת שדה של R .

משפט: $F' \subseteq F$ שדה אמ"ם:

1. F' סגורה לפעולות $+, *$.

2. $0_F, 1_F \in F'$.

3. $\forall a \in F' \setminus \{0_F\}, -a, a^{-1} \in F'$.

למה: (ללא הוכחה) יהי F שדה עם $char(F) > 0$ אז

1. $F_0 = \{k_F \mid k \in Z\}$ מהווה תת שדה סופי של $char(F)$.

2. $F_0 \simeq Z_p$.

למה: (ללא הוכחה) אם $char(F) = 0$ אז יש שיכון של Q ב- F .

דיון על איזומורפיזמים וסוגי הומומורפיזם/ הפימורפיזם/ מונומורפיזם/ איזומורפיזם (קבוצות, גרפים, סדרים,
חבורות, חוגים, שדות)