מבנים אלגבריים 1

8 במאי 2024

שיעור 1 — 6.5.2024

הקורס עוסק בעיקרו בתורת החבורות, ממנה גם מתחילים.

חבורה (באנגלית Group) היא מבנה מתמטי.

ברעיון חבורה מייצגת סימטריה, אוסף השינויים שאפשר לעשות על אובייקט ללא שינוי שלו, קרי שהוא ישאר שקול לאובייקט במקור.

מה הן הסימטריות שיש לריבוע? אני יכול לסובב ולשקף אותו בלי לשנות את הצורה המתקבלת והיא תהיה שקולה. חשוב להגיד שהפעולות האלה שקולות שכן התוצאה הסופית זהה למקורית.

אפשר לסובב ספציפית אפס, תשעים מאה שמונים ומאתיים שבעים מעלות, נקרא לפעולות האלה A, B, C בהתאמה.

בנוסף אפשר לשקף סביב ציר האמצע, ציר האמצע מלמעלה, ועל האלכסונים, ניתן גם לאלה שמות, נקרא לפעולות אלה בהתאמה D, E, F, G, H.

אלה הפעולות הבסיסיות ואי אפשר לעשות פעולה שלא בקבוצה הזאת, אבל אפשר להרכיב את הפעולות האלה והתוצאה הסופית תהיה שקולה לפעולה מהקבוצה.

נגדיר את הפעולות:

$$D_4 = \{A, B, C, D, E, F, G, H\}, \circ : D_4 \times D_4 \to D_4$$

נראה כי הרכבת פעולות שקולה לפעולה קיימת:

$$E \circ G = C, E \circ B = H, B \circ F = F$$

חשוב לשים לב שהפעולה הזאת לא חילופית: $X \circ Y \neq Y \circ X$.

היא כן קיבוצית: $X \circ (Y \circ Z) = (X \circ Y) \circ Z$.

תכונה נוספת היא קיום האיבר הנייטרלי, במקרה הזה A. איבר זה לא משפיע על הפעולה הסופית, והרכבה איתו מתבטלת ומשאירה רק את האיבר השני:

$$\forall X \in D_4 : A \circ X = X \circ A = X$$

התכונה האחרונה היא קיום איבר נגדי:

$$\forall X \in D_4 \exists Y \in D_4 : X \circ Y = Y \circ X = A$$

הגדרה: חבורה

חבורה היא קבוצה G עם $\circ : G \times G \to G$ ואיבר $e \in G$ כך שמתקיימות התכונות הבאות:

1. אסוציאטיביות (חוק הקיבוץ): $\forall x, y, z \in G : (x \circ y) \circ z = x \circ (y \circ z)$.
2. קיום איבר נייטרלי: לכל $x \in G$ מתקיים $x \circ e = e \circ x = x$.
3. קיום איבר נגדי: לכל $x \in G$ קיים $y \in G$ כך שמתקיים $x \circ y = y \circ x = e$.

חשוב לציין כי זו היא לא הגדרה מינימלית, ניתן לצמצם אותה, לדוגמה להגדיר שלכל איבר יש הופכי משמאל בלבד (יש להוכיח שקילות).

למה: קיום איבר נייטרלי יחיד

אם $e_1, e_2 \in G$ נייטרליים אז $e_1 = e_2$.

הוכחה. $e_1 = e_1 \circ e_2 = e_2$ **מש"ל**

דהינו, קיים איבר נייטרלי יחיד.

דוגמות

הקורס מבוסס על הספר "מבנים אלגבריים" מאת דורון פודר, אלכס לובוצקי ואהוד דה שליט, אך יש הבדלים, חשוב לשים לב אליהם. ניתן לקרוא שם דוגמות.

דוגמות כלליות לחבורות, עבור $(\mathbb{F}, +, \cdot, 0, 1)$ שדה:

1. חבורה החיבורית היא $(\mathbb{F}, +, 0)$
2. החבורה הכפלית היא $(\mathbb{F}, \cdot, 1)$

הסימון הכי נפוץ לפעולה של החבורה היא כפל או נקודה או לא בכלל: $xy = x \cdot y$.

הגדרה: חבורה קומוטטיבית

חבורה G תיקרא קומוטטיבית או חילופית או אבלית (על שם המתמטיקאי אבל) אם $xy = yx$ לכל $x, y \in G$.

חשוב להבין, למה שסימטריות תהינה חילופיות.

דוגמות לחבורות קומוטטיביות

$(\mathbb{Z}, +, 0)$ חבורת החיבור מעל השלמים, היא חבורה קומוטטיבית.

באופן דומה גם $(\mathbb{Z}_n, +, 0)$.

דוגמות לחבורות שאינן קומוטטיביות

- $(D_4, \circ, A)$ אשר מייצג את הריבוע עליו דובר בתחילת ההרצאה
- S_n תמורות על $1, \dots, n$ עם הרכבה.

  תמורה היא פעולה שמחליפה שני איברים כפונקציה, לדוגמה $s(1) = 2, s(2) = 1, s(n) = n$.

  S_n הוא מקרה פרטי של תמורות על קבוצה $\{1, \dots, n\}$
- $\mathrm{Sym}(X) = \{f : X \to X \mid f \text{ הופכית, חח"ע ועל}\}$

  תמורות הן סימטריה של קבוצה, כל תמורה היא העתקה חד־חד ערכית ועל שמשמרת את מבנה הקבוצה.
- $GL_n(\mathbb{F})$ מטריצות $n \times n$ הפיכות מעל שדה $\mathbb{F}$.
- אם V מרחב וקטורי מעל שדה $\mathbb{F}$ אז

  $GL(V) = \{f : V \to V \mid f \text{ לינארית וחד חד ערכית}\}$

נשים לב כי $GL_n(\mathbb{F}) \cong GL(\mathbb{F}^n)$, דהינו הם איזומורפיים. זה לא אומר שהם שווים, רק שיש להם בדיוק אותן תכונות.

גם בקבוצות שתי קבוצות עם אתו גודל הן איזומורפיות אך לא שקולות.

תרגול 1 — 7.5.2024

דוגמות לחבורות

לא חבורה בגלל 0	$(\mathbb{Z}, \cdot, 1)$
לא חבורה בגלל מטריצות רגולריות ומטריצת האפס לדוגמה	$(M_{n\times n}(\mathbb{R}), \circ, I_n)$
אכן חבורה	$(\mathbb{Z}_4, +_4, 0)$
אכן חבורה	$(\mathbb{Z}_3, +_3, 0)$
לא חבורה, $2 \cdot 2 = 0$	$(\mathbb{Z}_4^*, \cdot, 1)$
אכן חבורה, מבוסס על מספר ראשוני	$(\mathbb{Z}_3^*, \cdot, 1)$

הערה לא קשורה: הסימון של כוכבית מסמן הסרת כלל האיברים הלא הפיכים מהקבוצה.

כל שלישייה $(\mathbb{Z}_p \setminus \{0\}, \cdot_p, 1)$ היא חבורה בתנאי ש־p הוא ראשוני.

תכונות בסיסיות של חבורות

יחידות האיבר הנייטרלי	$e_1 = e_1 e_2 = e_2$
יחידות ההופכי	$x \in G, y, y_1 = x^{-1} : y = y \cdot e = yxy_1 = e \cdot y_1 = y_1$

תהי G חבורה, $g = x_1 \cdot \ldots \cdot x_n$ ביטוי לא תלוי בהצבת סוגריים, טענה זו אפשר להוכיח באינדוקציה.

לכל $n, m \in \mathbb{N}$ מתקיים גם $(x^n)^m = x^{n \cdot m}$ ואף $x^n \cdot x^m = x^{n+m}$.

תתי־חבורות

תהי חבורה $(G, \cdot_G, e_G)$, ותהי $H \subseteq G$ תת־קבוצה, אז $(H, \cdot_G, e_G)$ תיקרא תת־חבורה אם היא מהווה חבורה תקינה. נסמן $H \leq G$.

לדוגמה נראה $(2\mathbb{Z}, +, 0) \leq (\mathbb{Z}, +, 0)$ חבורת הזוגיים בחיבור היא תת־חבורה של השלמים.

$(\mathrm{diag}_n(\mathbb{R}), \circ, I_n) \leq (GL_n(\mathbb{R}), \circ, I_n)$ חבורת המטריצות האלכסוניות היא תת־חבורה של המטריצות.

$(GL_n(\mathbb{Q}), \circ, I_n) \leq (GL_n(\mathbb{R}), \circ, I_n)$ מטריצות הפיכות מעל הרציונליים חלקיות למטריצות הפיכות מעל הממשיים.

קריטריון מקוצר לתת־חבורה

תהי G חבורה ותהי קבוצה $H \subseteq G$ אז $H \leq G$ (תת־חבורה של G) אם ורק אם:

1. $e_G \in H$, איבר היחידה נמצא ב־H
2. $\forall x \in H : x^{-1} \in H$, לכל איבר גם האיבר ההופכי לו נמצא בקבוצה
3. $\forall x, y \in H : x \cdot y \in H$, הקבוצה סגורה לכפל האיברים בה

דוגמות

$1 \in \mathbb{N}_0 \wedge -1 \notin \mathbb{N}_0$	$(\mathbb{N}_0, +, 0) \nsubseteq (\mathbb{Z}, +, 0)$
כלל התנאים מתקיימים	$\{0,2,4,6,8\} \subseteq (\mathbb{Z}_{10}, +_{10}, 0)$

טענה: תת־חבורה לחבורה סופית

אם חבורה היא סופית, אז תנאי 2 איננו הכרחי לתתי־חבורות.

הוכחה. תהי G חבורה סופית ותהי $H \subseteq G$ אשר מקיימת את סעיפים 1 ו־3 בקריטריון.
יהי $x \in H$, נבחין כי $\{x^n \mid n \in \mathbb{N}\} \subseteq H$ בעקבות סעיף 3 של הקריטריון.
לכן קיימים שני מספרים $n, m \in \mathbb{N}$ כך ש־$m < n$ אשר מקיימים $x^n = x^m$.
כמובן מתקיים $x^n \cdot x^{-m} = e$ ומהסגירות לכפל נובע כי $x^{n-m} \in H$ ומצאנו כי התנאי השני מתקיים. **מש"ל**

חבורת התמורות

תהי X קבוצה, אז $\text{Sym}(X)$ היא קבוצת הפונקציות החד־חד ערכיות ועל מ־X לעצמה.
$(\text{Sym}(X), \circ, Id)$ היא חבורה, מורכבת מכלל התמורות, הרכבת פונקציות ופונקציית הזהות.
אם X היא קבוצה סופית אז $S_n = \text{Sym}(X)$, ובדרך כלל נגדיר $X = [n] = \{1, \ldots, n\}$, וחבורת התמורות תהיה $(S_n, \circ, Id)$.

הגדרה: סדר של חבורה

סדר של חבורה הוא מספר האיברים בחבורה.
אילו G אז נגיד שסדר החבורה הוא אינסוף.
נסמן את הסדר $|G|$.
אילו G חבורה ו־$x \in G$, הסדר של x הוא $n \in \mathbb{N}$ המינימלי כך שמתקיים $x^n = e$, נסמנו $|x|$ או $\sigma(x)$.

חזרה לתמורות

נשים לב שמתקיים $|S_n| = n!$.
$\sigma \in \S_n$, נכתוב את התמורה כך:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

לדוגמה $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.
אילו $\sigma \in S_n$ ו־$i \in [n]$ נקיים $\sigma(i) = i$ אז i נקרא **נקודת שבט** של σ.
בדוגמה שנתנו, $\sigma(3) = 3$ ולכן זוהי נקודת שבט של σ.

תתי־חבורות של חבורת התמורות

גודמה ראשונה:

$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \subseteq S_3$$

היא תת־חבורה של S_3 שכן כללי הקריטריון מתקיימים מבדיקה.

גם $\{\sigma \in S_n \mid \sigma(1) = 1\}$ היא תת־חבורה, שכן $\sigma(\tau(1)) = \tau(\sigma(1)) = 1$.

לעומת זאת $\{\sigma \in S_n \mid \sigma(1) \in \{1, 2, 3\}\}$ איננה חבורה. נראה כי אם σ, τ המקיימות $\tau(1) = 2, \tau(2) = 1, \sigma(2) = 4, \sigma(4) = 2$ וכל השאר נקודות שבט, $\sigma(\tau(1)) = 4$ שלא נמצא בקבוצה על־פי הגדרתה.

מחזורים

מחזור הוא רצף של איברים שהתמורה מחזירה כרצף, זאת אומרת שהתמורה עבור האיבר הראשון במחזור תחזיר את השני, השני את השלישי וכן הלאה.

הגדרה: מחזור פשוט $\sigma \in S_n$ יקרא l**־מחזור** אם קיימים $x_1, \dots, x_l \in [n]$ כך שלכל $0 \le i < l$ מתקיים $\sigma(x_i) = x_{i+1}$ ו־$\sigma(x_l) = x_0$.

טענה: כל תמורה היא הרכבה של מספר כלשהו של מחזורים, ההוכחה מסתמכת על היכולת לשרשר את ערכי המחזור משרשראות שאינן נוגעות אחת לשנייה.

לדוגמה, נבחין כי אם

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 7 & 5 & 1 & 4 & 3 \end{pmatrix}$$

אז נוכל להרכיב $\sigma = (1\,6\,4\,5)(2)(3\,7)$.

נשים לב למקרה מיוחד, יהי $\sigma \in S_n$ כך ש־σ הוא l־מחזור, ונגדיר $\sigma = (x_1\,x_2\,\dots\,x_l)$.

בהינתן $\tau \in S_n$, מתקיים

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1)\,\tau(x_2)\,\dots\,\tau(x_n))$$

זאת שכן לדוגמה $\sigma(\tau^{-1}(\tau(x_1))) = \sigma(x_1)$ ובהתאם $(\tau \circ \sigma \circ \tau^{-1})(x_1) = \tau(x_1)$.

שיעור 2 — 8.5.2024

אנחנו מקבלים את האחריות על תהליך הלמידה בקורס מבחינת שיעורי בית, דהינו מטלות. בבקשה תפתור לבד כמה שאפשר ואשכרה תחשוב על כל שאלה, כדי ללמוד ממנה.

מה זה אומר ששתי חבורות הן אותו דבר? מושג האיזומורפיזם. נבחן את $\mathbb{Z}/2$ ואת $(\{\pm 1\}, \cdot)$ ובשתיהן יש רק שני איברים, אחד נייטרלי ואחד לא, ובשתיהן הפעולות מתנהגות אותו דבר בדיוק.

$$1 <-> 10 <-> -1$$

עוד דוגמה היא $(\mathbb{R}, +)$ ו־$(\mathbb{R}^{>0}, \cdot)$.

$$(\mathbb{R}, +) \xrightarrow{\exp} (\mathbb{R}^{>0}, \cdot), \exp(x+y) = \exp(a)\exp(b)$$

הגדרה:

עבור G ו־H חבורות:

הומומורפיזם מ־G ל־H היא פונקציה $\phi : G \to H$ שמקיימת:

1. $\phi(e_G) = \phi(e_H)$
2. $\phi(xy) = \phi(x)\phi(y)$
3. $\phi(x^{-1}) = \phi(x)^{-1}$

למה: $\phi : G \to H$ היא הומומורפיזם אם לכל $x, y \in G$ מתקיים $\phi(x^{-1}) = \phi(x)^{-1}$. תוכיח בעצמך

הגדרה: איזומורפיזם G ל־H הוא הומורפיזם חד־חד ערכי ועל ומסומן $\phi : G \xrightarrow{\sim} H$.

למה: עבור $\phi : G \xrightarrow{\sim} H$ גם ההופכי הומומורפיזם (ולכן גם איזומורפיזם).

הוכחה: $x, y \in H$.

$$\phi^{-1}(xy) = \phi^{-1}(\phi(\phi^{-1}(x))\phi(\phi^{-1}(y))) = \phi^{-1}(x)\phi^{-1}(y)$$

מסקנה: המומורפיזם $\phi : G \to H$ הוא איזומורפיזם אם ורק אם קיים הומומורפיזם $\psi : H \to G$ כך שמתקיים $\phi \circ \psi = \psi \circ \phi = Id_G$

אומרים על שתי חבורות שהן איזומורפיות אם יש ביניהן איזומורפיזם. יכולים להיות אינסוף איזומורפיזמים, מה שחשוב זאת התכונה עצמה.

לדוגמה $GL_2(\mathbb{F}_2)$. יש בשורה העליונה 3 אפשרויות, ובשורה השנייה 2 ולכן יש 6 איברים בחבורה הזו.

גם ב־S_3 יש בדיוק שישה איברים, ולכן $GL_2(\mathbb{F}_2) \not\cong S_3$. גם החבורה החיבורית $\mathbb{Z}/6$ היא חבורה עם שישה איברים. החבורה הראשונה לא קומוטטיבית והשנייה כן, כי כפל מטריצות לא ניתן לשינוי סדר.

למה: $\phi : G \to H$ ו־$\psi : H \to K$ שני הומומורפיזמים, אז גם $\psi \circ \phi : G \to K$ הוא הומומורפיזם. תוכיח לבד.

מסקנה: הרכבה של איזומורפיזמים היא איזומורפיזם.

הגדרה: אוטומורפיזם של G הוא איזומורפיזם $G \xrightarrow{\sim} G$. נסמן ב־$Aut(G)$ את קבוצת האוטומורפיזמים של G.

למה: $Aut(G)$ היא חבורה ביחס להרכבה. הוכחה: הרכבה היא אסוציאטיבית, העתקת הזהות מוכלת בקבוצה ונייטרלי להרכבה, והוכחנו שלכל אוטומורפיזם יש הופכי $\phi^{-1} \in Aut(G)$.

דוגמה: מהי $Aut(\mathbb{Z})$? לדוגמה $\phi(n) = n + 1$. זה לא טוב כי $\phi(1+3) = \phi(4) = 5, \phi(1) + \phi(3) = 6$.

פונקציית הזהות היא אוטומורפיזם, והפונקציה $\phi(n) = -n$.

נבחן את פונקציית הכפל בקבוע, $\phi(n) = 2n$, נראה כי $\phi(n+m) = 2(n+m) = 2n + 2m, \phi(n) + \phi(m) = 2n + 2m$. הומומורפיזם,

אבל לא כל איבר שייך לקבוצה השנייה ולכן לא אוטומורפיזם.

$$Aut(\mathbb{Z}) = \{Id, -Id\} \cong \mathbb{Z}/2$$

תרגיל: אם G חבורה מגודל 2 אז $G \cong \mathbb{Z}/2$.

טענה: $Aut(\mathbb{Z}) = \{Id, -Id\}$.

הוכחה: יהי $\phi : \mathbb{Z} \xrightarrow{\sim} \mathbb{Z}$, ראשית נראה כי $\phi(n) = n\phi(1)$.

עבור $n = 0$ ברור, עבור $n > 1$ נראה כי $\phi(n) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) = n\phi(1)$.

עבור $n \leq 1$ נשתמש ב־$\phi(-1) = -1$ ובהתאם $\phi(-n) = (-n)\phi(1)$. תתקן אחר כך את הסימנים.

לכן $\phi(1) = \pm 1 \implies \phi = \pm Id$.

מה הוא הגודל של $Aut(\mathbb{Z}/n)$?

הגדרה: אם G ו־H הן חבורות, המכפלה הישרה ל G ו־H או $G \times H$ היא החבורה שמקיימת $G \times H = \{(x, y) \mid x \in G, y \in H\}$. עם הפעולה $(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2, y_1y_2)$ והנייטרלי $e = (e_G, e_H) \in G \times H$

תרגיל: $G \times H$ היא חבורה, הוכיח. לדוגמה $(x, y)^{-1} = (x^{-1}, y^{-1})$.

נראה בהמשך שמתקיים $\mathbb{Z}/6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. אבל $\mathbb{Z}/4 \ncong \mathbb{Z}/2 \times \mathbb{Z}/2$.

הגדרה: G חבורה, ותהי תת־קבוצה $H \subseteq G$ נקראת תת־חבורה אם

1. $e \in H$
2. $x, y \in H \implies xy \in H$
3. $x \in H \implies x^{-1} \in H$

למה: תת־קבוצה $H \subseteq G$ היא תת־חבורה אם ורק אם H חבורה ביחס לאותה פעולה של G.

מסמנים $H \leq G$ תת־חבורה.

דוגמות:

- $\{0°, 90°, 180°, 270°\} \leq D_4$
- $\{\sigma \in S_n \mid \sigma(1) = 1\} \leq S_n$
  - תהי G חבורה סופית אז $Aut(G) \leq Sym(G) \cong S_n$
- $SL_n(\mathbb{F}) \leq GL_n(\mathbb{F})$ מטריצות עם דטרמיננטה 1 הן חלקיות למטריצות הפיכות.
- $B_n(\mathbb{F}) \leq GL_n(\mathbb{F})$ מטריצות משולשיות עליונות עם אלכסון 1 הן חלקיות אף הן להפיכות.
- $O_n(\mathbb{F}) \leq GL_n(\mathbb{F})$ חבורת המטריצות האורתוגונליות חלקיות לחבורת המטריצות ההפיכות. $O_n(\mathbb{F}) = \{A \in GL_n(\mathbb{F}) \mid I_n = AA^t = A^tA$.

למה: לכל קבוצה S ומשפחה $\{H_\alpha \leq G \mid \alpha \in S\}$. של תת־חבורה של G אז $\bigcap_{\alpha \in S} H_\alpha \leq G$ תת־חבורה.

תשלים הסבר על מה זה משפחה ולמה זה פה.

הוכחה:

- $e \in H_\alpha$ לכל $\alpha \in S$ ולכן $e \in \bigcap_{\alpha \in S}$.

- $x,y \in \bigcap_{\alpha\in S}$ אם ורק אם לכל α מתקיים $x,y \in H_\alpha$ ולכן $xy \in H_\alpha$ ובהתאם $xy \in \bigcap_{\alpha\in S}$.

למשל $SO_n = SL_n(\mathbb{R}) \cap O_n \leq GL_n(\mathbb{R})$

הגדרה: G חבורה ו־$S \subseteq G$, תת־קבוצה, התת־חבורה הנוצרת על־ידי S מוגדרת להיות:

$$\langle S\rangle = \bigcap_{S\subseteq H\leq G} H$$