

מבנים אלגבריים 1

21 במאי 2024



תוכן העניינים

שיעור 1 – 6.5.2024

5	הגדרה: חבורה
5	למה: קיום איבר נייטרלי יחיד
6	דוגמות
6	הגדרה: חבורה קומוטטיבית
6	דוגמות לחבורות קומוטטיביות
6	דוגמות לחבורות שאינן קומוטטיביות

תרגול 1 – 7.5.2024

7	דוגמות לחבורות
7	תכונות בסיסיות של חבורות
7	תתי-חבורות
7	קריטריון מקוצר לתת-חבורה
8	דוגמות
8	טענה: תת-חבורה לחבורה סופית
8	חבורת התמורות
8	הגדרה: סדר של חבורה
8	חזרה לתמורות
9	תתי-חבורות של חבורת התמורות
9	מחזורים

שיעור 2 – 8.5.2024

10	מבוא לאיזומורפיות
10	הגדרה: הומומורפיזם
10	למה: תנאי הכרחי להומומורפיזם
10	הגדרה: איזומורפיזם
10	למה: הופכי לאיזומורפיזם
11	מסקנה: תנאי הכרחי לאיזומורפיזם
11	הגדרה: איזומורפיות
11	למה: הרכבת הומומורפיזמים
11	מסקנה: הרכבת איזומורפיזמים
11	הגדרה: אוטומורפיזם
11	למה: חבורת האוטומורפיזמים
11	טענה, ערך (Z, Aut)
12	הגדרה: מכפלת חבורות
12	הגדרה: תת-חבורה
12	למה: חיתוך תת-חבורות

13 הגדרה: תת־חבורה נוצרת

14 שיעור 3 — 15.5.2024

14 תת־חבורות

14 הגדרה: תת־חבורה נוצרת

14 למה: תת־חבורה מינימלית

14 טענה: תת־חבורה נוצרת מפורשת

14 הגדרה: שלמות תת־חבורה יוצרת

14 חבורה ציקלית

15 טענה

15 טענה: תת־חבורות של Z

15 הגדרה: gcb

15 מסקנה: הלמה של Bézout

16 מחלקות (Cosets)

16 הגדרה: מחלקה ימנית ושמאלית

16 למה: שיוך למחלקה

16 מסקנה

16 טענה: כיסוי זר

16 טענה:

17 הגדרה: אוסף מחלקות

17 משפט לאגרנז'

17 דוגמות

18 שיעור 4 — 20.5.2024

18 חזרה

18 הגדרה: סדר של חבורה

18 למה: סדר

18 מסקנה מלאגרנז'

19 הבחנה

19 טענת בסיס למשפט השאריות הסיני

19 פעולות של חבורה על קבוצה

19 הגדרה: פעולה

19 דוגמות לפעולות כאלה

20 הגדרה: אינבולוציה

20 הגדרה: הפעולה הרגולרית

21 הגדרה: הצמדה

21 טענה: הצמדה היא הומומורפיזם

22 תרגול 3 — 21.5.2024

22	שאלות מתרגיל 1
22	שאלה 1
22	שאלה 4
23	מחלקות שקילות
23	הגדרה
23	תכונות של מחלקות
23	הגדרה: אינדקס
23	דוגמות
24	משפט לגרנו
24	הגדרה: סדר של איבר
24	משפט לגרנו
24	מסקנה
24	מסקנה:
24	מסקנה
25	משפט פרמה הקטן
25	שאלה 4 סעיף א'

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 D, E, F, G, H בהתאמה. 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:

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

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 $\circ : G \times G \rightarrow G$ ואיבר $e \in G$ כך שמתקיימות התכונות הבאות:

$$1. \text{ אסוציאטיביות (חוק הקיבוץ): } \forall x, y, z \in G : (x \circ y) \circ z = x \circ (y \circ z).$$

$$2. \text{ קיום איבר נייטרלי: לכל } x \in G \text{ מתקיים } x \circ e = e \circ x = x.$$

$$3. \text{ קיום איבר נגדי: לכל } x \in G \text{ קיים } y \in G \text{ כך שמתקיים } x \circ y = y \circ x = e.$$

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 $e_1 = e_2$.

$$\text{הוכחה. } e_1 = e_1 \circ e_2 = e_2$$

□

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 המתטיקאי אבל) אם $xy = yx$ לכל $x, y \in G$. חשוב להבין, למה שסימטריות התינה 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 $\{1, \dots, n\}$

• $\text{Sym}(X) = \{f : X \rightarrow X \mid f \text{ ועל}\}$

תמורות הן סימטריות 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

$GL(V) = \{f : V \rightarrow V \mid f \text{ ערכית}\}$

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 אותו גודל הן איזומורפיות אך לא שקולות.

תרגול 1 — 7.5.2024

דוגמות לחבורות

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

הערה לא קשורה: הסימון של כוכבית מסמן הסרת כלל האיברים הלא הפיכים מהקבוצה.
כל שלישיה $(\mathbb{Z}_p \setminus \{0\}, \cdot, 1)$ היא חבורה בתנאי ש- p הוא ראשוני.

תכונות בסיסיות של חבורות

$$e_1 = e_1 e_2 = e_2 \quad \text{יחידות האיבר הנייטרלי}$$

$$x \in G, y, y_1 = x^{-1} : y = y \cdot e = y x y_1 = e \cdot y_1 = y_1 \quad \text{יחידות ההופכי}$$

תהי G חבורה, $g = x_1 \cdot \dots \cdot x_n$ ביטוי לא תלוי בהצבת סוגריים, טענה זו אפשר להוכיח באינדוקציה.
לכל $n, m \in \mathbb{N}$ מתקיים גם $x^n \cdot x^m = x^{n+m}$ ואף $(x^n)^m = x^{n \cdot m}$.

תתי-חבורות

תהי חבורה (G, \cdot, e_G) , ותהי $H \subseteq G$ תת-קבוצה, אז (H, \cdot, e_G) תיקרא תת-חבורה אם היא מהווה חבורה תקינה. נסמן $H \leq G$.
לדוגמה נראה $(\mathbb{Z}, +, 0) \leq (2\mathbb{Z}, +, 0)$ חבורת הזוגיים בחיבור היא תת-חבורה של השלמים.
 $(\text{diag}_n(\mathbb{R}), \circ, I_n) \leq (GL_n(\mathbb{R}), \circ, I_n)$ 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:

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

$$(\mathbb{N}_0, +, 0) \not\subseteq (\mathbb{Z}, +, 0)$$

$$1 \in \mathbb{N}_0 \wedge -1 \notin \mathbb{N}_0$$

$$\{0, 2, 4, 6, 8\} \subseteq (\mathbb{Z}_{10}, +_{10}, 0)$$

כלל התנאים מתקיימים

טענה: תת-חבורה לחבורה סופית

אם חבורה היא סופית, אז תנאי 2 איננו הכרחי לתת-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.

□

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 $X = [n] = \{1, \dots, n\}$, 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:

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

$$\cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ לדוגמה}$$

אילו $\sigma \in S_n$ ו- $i \in [n]$ נקיים $\sigma(i) = i$ או 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 $\sigma(1) = 2, \sigma(2) = 4, \tau(2) = 1, \tau(1) = 2$ וכל השאר נקודות שבת, $\sigma(\tau(1)) = 4$ 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 $0 \leq i < l$ מתקיים $\sigma(x_i) = x_{i+1}$ ו- $\sigma(x_l) = x_1$.

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 $(1\ 6\ 4\ 5)(2)(3\ 7)$.

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

מבוא לאיזומורפיות

המטרה שלנו היא להבין מתי שתי חבורות שונות הן שקולות, ולחקור את מושג האיזומורפיות. נבחן את $\mathbb{Z}/2$ ואת $(\{\pm 1\}, \cdot)$ ובשתיים יש רק שני איברים, אחד נייטרלי ואחד לא, ובשתיים הפעולות מתנהגות אותו דבר בדיוק.

$$1 \leftrightarrow -1, 1 \leftrightarrow 0$$

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

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

הגדרה: הומומורפיזם

עבור H ו- G חבורות:

הומומורפיזם מ- G ל- H היא פונקציה $\varphi : G \rightarrow H$ שמקיימת:

$$1. \varphi(e_G) = e_H$$

$$2. \varphi(xy) = \varphi(x)\varphi(y)$$

$$3. \varphi(x^{-1}) = \varphi(x)^{-1}$$

למה: תנאי הכרחי להומומורפיזם

$\varphi : G \rightarrow H$ היא הומומורפיזם אם ורק אם לכל $x, y \in G$ מתקיים $\varphi(xy) = \varphi(x)\varphi(y)$.

הוכחה. נראה ששלושת התכונות מתקיימות:

$$1. \text{ נבחר } x \in G \text{ ונראה כי } e_H = \varphi(e_G) \iff \varphi(x) = \varphi(e_G x) = \varphi(e_G)\varphi(x)$$

2. נתון

$$3. \varphi(e_G) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) = e_H \implies \varphi(x^{-1}) = \varphi(x)^{-1}e_H$$

ומצאנו כי שלושת התנאים מתקיימים. □

הגדרה: איזומורפיזם

איזומורפיזם מ- G ל- H הוא הומומורפיזם חד-חד ערכי ועל ומסומן $\varphi : G \xrightarrow{\sim} H$.

למה: הופכי לאיזומורפיזם

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

הוכחה. נראה כי לכל $x, y \in H$

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

ומצאנו כי התנאי ההכרחי להומומורפיזם מתקיים. □

מסקנה: תנאי הכרחי לאיזומורפיזם

הומומורפיזם $\varphi : G \rightarrow H$ הוא איזומורפיזם אם ורק אם קיים הומומורפיזם $\psi : H \rightarrow G$ כך שמתקיים $\varphi \circ \psi = \psi \circ \varphi = Id_G$.

הגדרה: איזומורפיות

נגדיר שתי חבורות כאיזומורפיות אם ורק אם קיים איזומורפיזם ביניהן.

נשים לב שמספר האיזומורפיזמים בין החבורות, גם אם הוא אינסופי, הוא חסר משמעות, ובמקום אנו מסתכל על עצם האיזומורפיות.

דוגמה לחבורות איזומורפיות הן $(\mathbb{Z}/2, \cdot) \cong (\{\pm 1\}, \cdot)$ כפי שראינו בהתחלה.

חשוב לשים לב שגם אם יש כמות איברים זהה בין החבורות, הן לא בהכרח תהינה איזומורפיות, לדוגמה $GL_2(\mathbb{F}_2)$, חבורת המטריצות ההפיכות מעל שדה עם שני איברים. יש בשורה העליונה 3 אפשרויות, ובשורה השנייה 2 ולכן יש 6 איברים בחבורה הזו. גם ב- S_3 יש בדיוק שישה איברים, אבל $GL_2(\mathbb{F}_2) \not\cong S_3$. 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: הרכבת הומומורפיזמים

$\varphi : G \rightarrow H$ ו- $\psi : H \rightarrow K$ שני הומומורפיזמים, אז גם $\psi \circ \varphi : G \rightarrow K$ הוא הומומורפיזם.

הוכחה. $\forall x, y \in G : (\psi \circ \varphi)(xy) = \psi(\varphi(xy)) = \psi(\varphi(x)\varphi(y)) = \psi(\varphi(x))\psi(\varphi(y)) = (\psi \circ \varphi)(x)(\psi \circ \varphi)(y)$. □

מסקנה: הרכבת איזומורפיזמים

הרכבה של איזומורפיזמים היא איזומורפיזם.

הגדרה: אוטומורפיזם

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

למה: חבורת האוטומורפיזמים

$Aut(G)$ היא חבורה ביחס להרכבה.

הוכחה. הרכבה היא אסוציאטיבית, העתקת הזהות מוכלת בקבוצה ונייטרלי להרכבה, והוכחנו שלכל אוטומורפיזם φ יש הופכי $\varphi^{-1} \in Aut(G)$. □

מהי $Aut(\mathbb{Z})$? לדוגמה $\varphi(n) = n + 1$. פונקציה זו איננה אוטומורפיזם שכן $\varphi(1) + \varphi(3) = 6$, $\varphi(1 + 3) = \varphi(4) = 5$.

פונקציית הזהות היא אוטומורפיזם, והפונקציה $\varphi(n) = -n$ על-פי בדיקה ישירה של הגדרות.

נבחן את פונקציית הכפל בקבוע, $\varphi(n) = 2n$, נראה כי $\varphi(n) + \varphi(m) = 2n + 2m$, $\varphi(n + m) = 2(n + m) = 2n + 2m$. הומומורפיזם, אבל לא כל איבר שייך לקבוצה השנייה ולכן לא אוטומורפיזם.

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

(טענה, ערך $Aut(\mathbb{Z})$)

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

הוכחה. יהי $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$, ראשית נראה כי $\varphi(n) = n\varphi(1)$.

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

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

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

□

הגדרה: מכפלת חבורות

אם G ו- H הן חבורות, המכפלה הישרה ל G ו- H היא החבורה שמקיימת $G \times H = \{(x, y) \mid x \in G, y \in H\}$. עם הפעולה

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2)$$

נראה בהמשך שמתקיים $\mathbb{Z}/6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. אבל $\mathbb{Z}/4 \not\cong \mathbb{Z}/2 \times \mathbb{Z}/2$.

הגדרה: תת-חבורה

G חבורה, ותהי תת-קבוצה $H \subseteq G$ נקראת תת-חבורה אם

$$1. e \in H$$

$$2. x, y \in H \implies xy \in H$$

$$3. x \in H \implies x^{-1} \in H$$

נשים לב כי 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:

$$\bullet \{0^\circ, 90^\circ, 180^\circ, 270^\circ\} \leq D_4$$

$$\bullet \{\sigma \in S_n \mid \sigma(1) = 1\} \leq S_n$$

$$\text{- תהי } G \text{ חבורה סופית אז } S_n \cong \text{Sym}(G) \leq \text{Aut}(G)$$

$$\bullet GL_n(\mathbb{F}) \leq SL_n(\mathbb{F}) \text{ מטריצות עם דטרמיננטה 1 הן חלקיות למטריצות הפיכות.}$$

$$\bullet GL_n(\mathbb{F}) \leq B_n(\mathbb{F}) \text{ מטריצות משולשיות עליונות עם אלכסון 1 הן חלקיות אף הן להפיכות.}$$

$$\bullet GL_n(\mathbb{F}) \leq O_n(\mathbb{F}) \text{ חבורת המטריצות האורתוגונליות חלקיות לחבורת המטריצות ההפיכות. } O_n(\mathbb{F}) = \{A \in GL_n(\mathbb{F}) \mid I_n =$$

$$AA^t = A^t A$$

למה: חיתוך תת-חבורות

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

הערה קטנה: משפחה היא קבוצה של קבוצות ככה שאפשר לזהות כל אחת לפי מספר, אפשר להשתמש בלמה גם בקבוצות כרגיל.

$$\bullet \text{ הוכחה. } e \in H_\alpha \text{ לכל } \alpha \in S \text{ ולכן } e \in \bigcap_{\alpha \in S} H_\alpha.$$

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

□

ומצאנו כי זוהי חבורה.

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

הגדרה: תת־חבורה נוצרת

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

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

ונשים לב כי על־פי הלמה האחרונה מתקבל כי זוהי אכן תת־חבורה.

שיעור 3 — 15.5.2024

תת־חבורות

הגדרה: תת־חבורה נוצרת

תהי $S \subseteq G$ תת־קבוצה לחבורה, נגדיר

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

למה: תת־חבורה מינימלית

$S \subseteq G$ התת־חבורה המינימלית $\langle S \rangle$ היא התת־חבורה המינימלית של G המכילה את S .

קצת קשה לעבור על זה, איזה אפיון נוסף יש לדבר הזה?

טענה: תת־חבורה נוצרת מפורשת

$S \subseteq G$ אז

$$\langle S \rangle = \overline{S} \equiv \{x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n} \mid x_i \in S, \epsilon_i = \pm 1\}$$

הוכחה:

כיוון ראשון: נניח שעבור תת־חבורה H המכילה של S סגורות H לכפל והופכי גוררת שהקבוצה \overline{S} הנתונה מוכלת ב- H .

מצד שני נראה שזוהי כבר תת־חבורה.

• $1 \in \overline{S}$ מכפלה ריקה.

• $x, y \in \overline{S}$ אז נסמן

$$x = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n}, y = y_1^{\epsilon_1} y_2^{\epsilon_2} \cdots y_n^{\epsilon_n}, xy = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n} y_1^{\epsilon_1} y_2^{\epsilon_2} \cdots y_n^{\epsilon_n}$$

• $x \in \overline{S}$ אז

$$x^{-1} = x_1^{-\epsilon_1} x_2^{-\epsilon_2} \cdots x_n^{-\epsilon_n},$$

$$(xy)(x^{-1}y^{-1}) = xyx^{-1}y^{-1} = xx^{-1} = 1 \text{ וידוע כי } 1 \in \overline{S}$$

הגדרה: שלמות תת־חבורה יוצרת

אם $\langle S \rangle = G$ אומרים ש- S יוצרת את G .

דוגמה: מתקיים $\langle 1 \rangle = \mathbb{Z}$. $\langle -1 \rangle = d\mathbb{Z}$ כקונספט כללי $\langle d \rangle$.

מה לגבי \mathbb{Z}/n ? מתקיים $\langle 1 \rangle = \mathbb{Z}/n$?

חבורה ציקלית

חבורה G נקראת ציקלית אם היא נוצרת על־ידי איבר אחד, דהיינו קיים $x \in G$ כך ש- $\langle x \rangle = G$.

טענה

כל חבורה ציקלית G מקיימת $G \cong \mathbb{Z}$ או $G \cong \mathbb{Z}/n$ הוכחה בתרגיל.

דוגמה:

$$G = D_4$$

נגדיר את σ להיות סיבוב בתשעים מעלות, ואת τ להיות היפוך על ציר האיקס.

$$\langle \sigma \rangle = \{e, \sigma, \sigma^2, \sigma^3\}$$

$$\langle \tau \rangle = \{e, \tau\}$$

אנחנו יכולים להכפיל כל שני איברים משתי הקבוצות שסימנו עכשיו.

$$D_4 = \langle \sigma, \tau \rangle = \{e, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$$

$$\tau\sigma = \sigma^3\tau, \sigma^4 = e, \tau^2 = e$$

$$\tau\sigma\tau^{-1} = \sigma^3 = \sigma^{-1}$$

טענה: תת-חבורות של \mathbb{Z}

לכל $H \leq \mathbb{Z}$ קיים $d \geq 0$ יחיד כך ש- $H = d\mathbb{Z}$.

הוכחה. אם $H \neq \{0\}$ אז קיים $0 < d \in H$ וניקח את d להיות המינימלי שמקיים את אי-השוויון.

$$\langle d \rangle = d\mathbb{Z} \subseteq H$$

מצד שני, עבור $a \in H$ וידוע $a > 0$ אז נכתוב $a = nd + r$ כאשר $0 \leq r < d$ שארית.

$$r = a - nd \in H$$

יחידות של זה: תרגיל נגלה בהמשך שתת-חבורה של חבורה ציקלית היא בעצמה ציקלית.

הגדרה: gcb

עבור שני מספרים $a, b \in \mathbb{Z}$ שלא שניהם 0 נגדיר $\gcd(a, b) = d$ (Greatest common divisor) מחלק משותף מקסימלי כך שמתקיים: $d \mid a, b$

וגם לשלכל a, b מתקיים גם $m \mid d$.

$$\langle a, b \rangle = d\mathbb{Z} \text{ הוכחה. לאיזשהו } d \geq 0 \text{ יחיד.}$$

$$d = \gcd(a, b)$$

$$d \mid a, b \text{ ולכן } a, b \in d\mathbb{Z}$$

$$m \mid a, b \text{ אם שני אם } a, b \text{ אז } n \mid a, b \subseteq m\mathbb{Z} = \{a, b\} \text{ ולכן } d \in d\mathbb{Z} \text{ והוא מחלק מקסימלי.}$$

$$2\mathbb{Z} = \langle 2 \rangle = \langle 6, 10 \rangle \text{ עבור}$$

מסקנה: הלמה של Bézout

לכל $a, b \in \mathbb{Z}$ קיימים $n, m \in \mathbb{Z}$ עבורם $\gcd(a, b) = na + mb$.

מחלקות (Cosets)

הגדרה: מחלקה ימנית ושמאלית

תהי G חבורה ו- $H \leq G$ ו- $x \in G$. נגדיר את המחלקה המשאלית של x על-ידי

$$xH = \{xh \mid h \in H\}$$

ואת המחלקה הימנית של x בהתאם

$$Hx = \{hx \mid h \in H\}$$

תרגיל: להוכיח שהמחלקה הימנית והשמאלית הן איזומורפיות. וזה לא נכון במונואיד.

למה: שיוך למחלקה

$$y \in xH \iff yH = xH$$

הוכחה.

$$y \in xH \iff y = xh \iff x^{-1}y \in H \iff y^{-1}x \in H \iff x \in yH, y \in xH \iff xH = yH$$

□

מסקנה

לכל $x, y \in G$ מתקיים

$$xH = yH \text{ (אם ורק אם } x^{-1}y \in H \text{)}$$

$$\text{או } xH \cup yH = \emptyset$$

□

הוכחה. אם $xH \cup yH \neq \emptyset$ אז מהלמה הקודמת $yH = xH$.

טענה: כיסוי זר

$$G \leq H \text{ התת-קבוצות מהצורה } xH \text{ עבור } x \in G \text{ מהוות כיסוי זר של } G.$$

□

הוכחה. נשאר לשים לב $x \in xH$ ולכן כיסוי ומהמסקנה זר.

טענה:

$$\text{לכל } x, y \in G \text{ יש התאמה חד-חד ועל ערכית של קבוצות } xH \xrightarrow{\sim} yH$$

$$\text{בפרט אם } H \text{ סופית אז לכל המחלקות אותו גודל, } |xH| = |yH|.$$

$$\text{הוכחה. נגדיר } \varphi : xH \rightarrow yH \text{ על-ידי } \varphi(z) = yx^{-1}z.$$

$$\text{ונגדיר פונקציה חדשה } \psi : yH \rightarrow xH \text{ על-ידי } \psi(z) = xy^{-1}z.$$

$$\text{אז מתקיים } \psi = \varphi^{-1} \text{ ובהתאם נובע כי } \varphi \text{ איזומורפיזם.}$$

□

הגדרה: אוסף מחלקות

$H \leq G$ אז נסמן

$$G/H = \{xH \mid x \in G\}, H \backslash G = \{Hx \mid x \in G\}$$

אוסף המחלקות השמאליות והימניות בהתאמה.

משפט לאגרנז'

אם G חבורה סופית, אז לכל $H \leq G$ מתקיים $|H| \mid |G|$.

הוכחה. ל- G יש כיסוי זר על-ידי מחלקות שמאליות של H ולכן הגודל של $|G/H|$ הוא $|G| = |H| \cdot |G/H|$.

הגודל של $|G/H| = |G|/|H|$.

סימון $|G/H| = |G : H|$ האינדקס של H ב- G .

דוגמות

המחלקות של $3\mathbb{Z} \leq \mathbb{Z}$:

$$3\mathbb{Z} + 0 = 3\mathbb{Z}, 3\mathbb{Z} + 1, 3\mathbb{Z} + 2$$

הקבוצה $\mathbb{Z}/3\mathbb{Z}$ היא השאריות האפשריות בחלוקה לשלוש.

□

שיעור 4 – 20.5.2024

חזרה

הגדרה: סדר של חבורה

G חבורה ו- $x \in G$ מסומן $o(x)$ הוא המספר הקטן ביותר כך ש- $x^n = e$ או $n \in \mathbb{N}$, $1 \leq n$ או ∞ אם לא קיים n כזה.

למה: סדר

$$o(x) = |\langle x \rangle|$$

הוכחה. נוכיח שאם $o(x)$ סופי אז

$$\langle x \rangle = \{1, x, x^2, \dots, x^{o(x)-1}\} \quad (1)$$

ואם $o(x) = \infty$ אז

$$\langle x \rangle = \{1, x, x^2, \dots\} \cup \{x^{-1}, x^{-2}, \dots\} \quad (2)$$

הוכחה ל-(1).

(1) תת-חבורה:

$$x^k \cdot x^m = x^{(m+k) \bmod o(x)}.$$

$$(x^n)^{-1} = x^{o(x)-n}.$$

כל ההאיברים שונים כי אם $x^k = x^m$ ל- $o(x) < k < m \leq o(x)$ אז

$$1 = x^0 = x^{m-k}$$

ונקבל $o(x) < m - k < o(x)$ בסתירה למינימליות של $o(x)$.

הוכחה ל-(2):

אם $H = \langle x \rangle$

סופיות נתונה בקבוצה.

$$\{1, x, x^2, \dots\} \subseteq H$$

מסופיות קיימים $0 \leq k < m$ עבורם

$$x^k = x^m \implies x^{m-k} = 1$$

ולכן ל- x יש סדר סופי, משובך היוגים.

2 תרגיל.

מסקנה מלאגרנו

G חבורה סופית, אז לכל $x \in G$ מתקיים

$$o(x) \mid |G|$$

הבחנה

אם קיים $x \in G$ עבורו $o(x) = |G|$ אז G ציקלית.

טענת בסיס למשפט השאריות הסיני

לכל $a, b \geq 1$ זרים אז $\gcd(a, b) = 1$, מתקיים

$$\mathbb{Z}/a \times \mathbb{Z}/b \cong \mathbb{Z}/ab$$

הוכחה. נראה שהסדר של $x = (1, 1) \in \mathbb{Z}/a \times \mathbb{Z}/b$ הוא ab ונסיק מההבחנה.

$$x^{ab} = (ab, ab) = (0, 0) = 1$$

ראשית, $x^n = 1$ אם $x^n = (0, 0) \in \mathbb{Z}/a \times \mathbb{Z}/b$ כלומר $(n, n) = (0, 0)$

$$0 = n \in \mathbb{Z}/a, \quad 0 = n \in \mathbb{Z}/b$$

ולכן $a|n, b|n$ וזרים a, b ולכן $ab|n$.

$$|\mathbb{Z}/a \times \mathbb{Z}/b| = |\mathbb{Z}/a| \cdot |\mathbb{Z}/b| = ab$$

מכיוון ש- ab הוא סדר של x ו- ab הוא סדר של $\mathbb{Z}/a \times \mathbb{Z}/b$ נובע ש- $\mathbb{Z}/a \times \mathbb{Z}/b \cong \mathbb{Z}/ab$ ולכן איזומורפית ל- \mathbb{Z}/ab .

□

פעולות של חבורה על קבוצה

נתעסק בחבורות לא אבליות ואיך הן מופיעות כסימטריות פעמים רבות. הסיבה שאנחנו מתעסקים בחבורות היא לראות את הפעולות שלהן על דברים.

הגדרה: פעולה

פעולה של חבורה G על קבוצה X זו פונקציה $\cdot : G \times X \rightarrow X$ כך שמתקיים:

$$1 \cdot x = x \quad \forall x \in X$$

$$h \cdot (g \cdot x) = (hg) \cdot x \quad \forall x \in X, g, h \in G$$

סימון: $G \curvearrowright X$. באנגלית Group action.

דוגמות לפעולות כאלה

1. S_n פועלת על הקבוצה $X = \{1, 2, \dots, n\}$ על-ידי

$$S_n \times \{1, \dots, n\} \rightarrow \{1, \dots, n\}$$

$$(\sigma, k) \mapsto \sigma(k)$$

2. $D_n \leq S_n$ כפי שהגדרנו בתרגיל.

D_n פועלת על $\{1, 2, \dots, n\}$ באותו אופן כמו S_n , והיא אינטואיטיבית שקולה לביצוע פעולה סימטרית נתונה על מצב מסוים של הריבוע.

3. $\mathbb{R}^n \curvearrowright GL_n(\mathbb{R})$ על-ידי

$$GL_n(\mathbb{R}) \times \mathbb{R}^n \rightarrow \mathbb{R}^n, \quad (A, v) \mapsto Av$$

קבלת וקטור ומטריצה וכפל הווקטור במטריצה.

$$\mathbb{R}^n \supset O_n(\mathbb{R}) \leq GL_n(\mathbb{R})$$

$$SO_2(\mathbb{R}) = O_2(\mathbb{R}) \cap SL_2(\mathbb{R})$$

הערה: הסימון $O(n) = O_n(\mathbb{R})$ הוא קבוצת האורתוגונליים על \mathbb{R} , באופן דומה $SO_n(\mathbb{R})$ קבוצת האורתוגונליים עם דטרמיננטה 1.

4. דוגמה 0: המקרה הטריוויאלי, כל חבורה G ולכל קבוצה X יש את הפעולה הטריוויאלית של G על X והיא

$$g \cdot x = x, \forall g \in G, x \in X$$

הרציונל מאחורי ההגדרה הזאת הוא שאנחנו יכולים לפרק את החבורות מתוך פעולות שאנחנו כבר מכירים ולחקור את התכונות של הפעולות האלה באופן ריגורוזי ושיטתי. נשים לב לדוגמה ש- $\{D_1, D_2\} \cup D_4$, אנחנו יכולים לחקור את המקרה היחסית טריוויאלי הזה של סימטריה גאומטרית על-ידי הגדרת הפעולה המתאימה.

הגדרה: אינבולוציה

נבחן את הפעולה של $\mathbb{Z}/2$ על X . האיבר הנייטרלי לא עושה כלום ולכן קל להגדיר אותו, יש להגדיר פעולה רק עבור איבר לא נייטרלי.

זה אותו דבר בגדול כמו פונקציה $\tau : X \rightarrow X$ שמקיימת $\tau \circ \tau = Id_X$, זאת שכן

$$\mathbb{Z}/2 \times X \rightarrow X, \quad g \cdot x \mapsto \begin{cases} x, & g = 0 \\ \tau(x), & g = 1 \end{cases}$$

לפונקציה כזאת קוראים אינבולוציה, פעולה שריבועה הוא Id , באנגלית Involution, וכבר ראינו פונקציות רבות כאלה.

כדוגמה יש לנו לפחות שלוש פעולות של $\mathbb{Z}/2$ על \mathbb{R}^2 כאלה

$$\tau\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} -x \\ y \end{bmatrix}, \quad \tau\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} x \\ -y \end{bmatrix}, \quad \tau\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} x \\ y \end{bmatrix}$$

הגדרה: הפעולה הרגולרית

G חבורה, הפעולה הרגולרית (השמאלית) של G על G שנתונה על-ידי

$$g \cdot x = gx$$

פעולה המוגדרת על-ידי הכפל של החבורה. זוהי כמובן פעולה והסימון הוא $G \curvearrowright G$.

האם פעולה ימנית גם עומדת בהגדרת הפעולה?

נבדוק את $G \times G \rightarrow G$ המוגדרת על-ידי $hg, x \mapsto (g, x)$:

נבדוק אסוציאטיביות

$$h \cdot (g \cdot x) = h \cdot (xg) = (xg)h, \quad (hg) \cdot x = x(hg), \quad (xg)h \neq x(hg)$$

ומצאנו כי הביטויים לא שווים ואין שמירה על אסוציאטיביות כחלק מהגדרת הפעולה, ולכן כמובן זוהי לא פעולה.

נשתמש במקום זאת בהופכית ונגדיר $hg, x \mapsto xg^{-1}$

פעולה זאת היא אכן פעולה מוגדרת והיא נקראת הפעולה הרגולרית הימנית.

יש עוד פעולה מעניינת של חבורה על עצמה, על-ידי הצמדה

הגדרה: הצמדה

$$G \times G \rightarrow G, \quad (g, x) \mapsto xgx^{-1}$$

היא פעולת ההצמדה, נחקור אותה בתרגיל. באנגלית Conjugacy.

בהינתן פעולה של $G \curvearrowright X$ נגדיר פונצקיה $f : G \rightarrow \text{Sym}(X) \subseteq \text{End}(X)$ על-ידי

$$f(g)(x) = g \cdot x$$

זאת שכן $G \times X \rightarrow X$ שקול ל- $\{X \rightarrow X\}$.

טענה: הצמדה היא הומומורפיזם

f היא הומומורפיזם של חבורות.

הוכחה.

$$f(hg)(x) = (hg) \cdot x = h \cdot (g \cdot x) = f(h)(g \cdot x) = f(h)(f(g)(x)) = (f(h) \cdot f(g))(x)$$

□

למה $f(g) \in \text{Sym}(X)$?

$$f(g) \cdot f(g^{-1}) = f(gg^{-1}) = f(1) = Id \quad \text{גם} \quad f(g^{-1}) \cdot f(g) = f(g^{-1}g) = f(1) = Id$$

בשיעור הבא נגדיר המון דברים על פעולות על קבוצות, אז צריך להבין את זה ואת הדוגמות באופן מאוד כבד ושלם.

תרגול 3 — 21.5.2024

שאלות מתרגיל 1

שאלה 1

$$\text{End}(X) = \{f : X \rightarrow X\}$$

היה צריך להוכיח שזה מונואיד. וזה חבורה רק כשהקבוצה היא הקבוצה הריקה או יחידון או משהו כזה. הסעיף השני הוא שיהא M מונואיד כך שלכל $x \in M$ קיים הופכי משמאל ומראים ש- M חבורה.

פתרון. יש לי $x \in M$ וצריך להראות שקיים $y \in \text{Im } M$ כך ש- $xy = yx = e$.

נתון קיום של $y \in M$ כך ש- $yx = e$ ואנחנו רוצים להראות שגם $xy \in M$.

$$xy = e \implies (xy)^2 = e = x(yx)y = xy = e$$

ולכן $\exists t \in M : tz = e$ ונקבל $z = tz^2 = tz = e$.

עכשיו נגיד שיש לנו מונואיד M כך ש- $x \in M$ ול- x יש הופכי מימין והופכי משמאל וצריך להראות שהם שווים.

פתרון. קיימים $y, z, xz = yx = e$.

לכן

$$z = ez = (yx)z = y(xz) = y$$

הסעיף האחרון הוא לתת דוגמה לאיבר במונואיד עם הופכי משמאל ולא מימין.

$$g(x) = \begin{cases} 1, & x = 1 \\ n-1, & n > 1 \end{cases} \quad f(x) = x+1$$

נבחר את $\text{End}(\mathbb{N})$ ונבחר את $f(x) = x+1$

שאלה 4

סעיף ב', צריך להראות שזה איזומורפי

$$\varphi : (\mathbb{R}^\times, \cdot) \rightarrow \mathbb{Z}/2 \times \mathbb{R}^+$$

ונאחנו משתמשים בבינאריות של $\mathbb{Z}/2$, ואנחנו יודעים שלוגריתם משמר פעולות.

$$\varphi(x) = \begin{cases} (1, \ln |x|), & x < 0 \\ (0, \ln |x|), & x > 0 \end{cases}$$

ועכשיו לסעיף ג':

צריך למצוא פונקציה

$$\varphi : GL_2(\mathbb{Z}/2) \xrightarrow{\sim} S(\{v_1, v_2, v_3\}), \quad v_1 = (1, 0), v_2 = (0, 1), v_3 = (1, 1)$$

$$\varphi(T) = \begin{pmatrix} v_1 & v_2 & v_3 \\ T(v_1) & T(v_2) & T(v_3) \end{pmatrix}$$

$$\varphi(T)\varphi(S) = \begin{pmatrix} v_1 & v_2 & v_3 \\ T(v_1) & T(v_2) & T(v_3) \end{pmatrix} \begin{pmatrix} v_1 & v_2 & v_3 \\ S(v_1) & S(v_2) & S(v_3) \end{pmatrix} = \begin{pmatrix} v_1 & v_2 & v_3 \\ T(S(v_1)) & T(S(v_2)) & T(S(v_3)) \end{pmatrix}$$

וזה מן הסתם עובד די טוב. אז בקיצור זה איזומורפיזם. ועכשיו נתחיל באשכרה תרגול.

מחלקות שקילות

הגדרה

תהא G חבורה, ו- $H \leq G$. מחלקות השקילות השמאליות של H הן קבוצות מהצורה $gH, g \in G$.

תכונות של מחלקות

$$1. \quad gH = H \iff g \in H$$

$$2. \quad \text{אם } H \text{ סופית אז לכל } g \in G \text{ מתקיים } |gH| = |H|.$$

$$3. \quad \forall g \in G : gH = Hg \iff gHg^{-1} \subseteq H$$

$$4. \quad \text{ישנה התאמה בין הקבוצות } gH \text{ ל-} Hg.$$

הגדרה: אינדקס

תהי $H \leq G$ חבורה ותת-חבורתה.

נגדיר $[G : H]$ להיות מספר המחלקות השמאליות של H . אם מספר זה אינסופי אז נגדיר את האינדקס $[G : H] = \infty$. מספר זה נקרא אינדקס של H ב- G .

דוגמות

נתבונן ב- D_3 . חבורת הסימטריות על משולש שווה צלעות. יש לנו שלושה צירי סימטריה, ויש לנו שלושה סיבובים לעשות.

$$D_3 = \{r, r^2, f, fr, fr^2\}$$

$$\text{וזה מן הסתם מקיים } D_3 = \langle r, f \rangle$$

$$\text{נגדיר } H_1 = \{e, f_2\}, H_2 = \{e, r, r^2\}$$

נראה כי מחלקות שקילות הן:

$$rH_1 = \{r, rf\}, r^2H_1 = \{r^2, r^2f\}, H_1 = H_1$$

ומהצד השני:

$$H_1r = \{r, fr\}, H_1r^2 = \{r^2, fr^2\}$$

ועבור H_2 :

$$fH_2 = \{f, fr, fr^2\}, \text{etc}$$

עתה נדבר על סדר.

משפט לגרנז'

הגדרה: סדר של איבר

תהא G חבורה סופית ו-, $g \in G$ נגדיר את הסדר של g , או $|g| = \text{ord}(g)$ הוא המינימום של המספרים הטבעיים כך ש- $g^n = e$.

משפט לגרנז'

תהא G חבורה סופית ו- H תת-חבורה של G . אז

$$[G : H] = \frac{|G|}{|H|}$$

ובפרט $|H| \mid |G|$.

מסקנה

תהא G סופית ו- $g \in G$ אז $|g| \mid |G|$.

הוכחה. עליידי התבוננות ב- $H = \langle g \rangle$.

למה: $|H| = \text{ord}(g)$.

הוכחה. נגדיר $\varphi : \mathbb{Z}/\text{ord}(g) \rightarrow H$ עליידי $\varphi(b) = g^b$.

נראה כי φ חד-חד ערכית ועל.

יהיו $n, m \in \mathbb{Z}/\text{ord}(g)$ ונניח כי $\varphi(n) = \varphi(m)$, אזי $g^n = g^m$ ולכן $g^{n-m} = e$ ולכן $n - m = 0$, שאם לא כן יש סתירה למינימליות של $\text{ord}(g)$.

מה החבורה הנוצרת עליידי $\langle g \rangle = \{g^n \mid n \in \mathbb{N}\}$.

יהא $n \in \mathbb{Z}$ נחלק את n עם שארית בסדר של g , $n = m \cdot \text{ord}(g) + r$ ו- $r \in \mathbb{Z}/\text{ord}(g)$ לכן $g^n = g^{m \cdot \text{ord}(g) + r} = g^r$.

הראינו כי $|H| = \text{ord}(g)$ ולכן הסדר של $|G| \mid |G|$.

מסקנה:

תהיה G חבורה סופית.

$$\forall g \in G, g^{|G|} = e$$

הוכחה. לפי המסקנה הקודמת

$$g^{|G|} = g^{k \cdot \text{ord}(g)} = g^{\text{ord}(g)} = e$$

□

מסקנה

יהיה p ראשוני, ו- G חבורה מסדר p . אז

1. G ציקלית.

2. G איזומורפית ל- \mathbb{Z}/p .

3. כל החבורות מגודל p איזומורפיות.

הוכחה. G היא לא חבורה טריוויאלית בגלל p ולכן נוכל להגדיר $g \in G \setminus \{e\}$.

נשים לב כי $1 < \text{ord}(g) \leq p$ אך מצד שני $|\langle g \rangle| = \text{ord}(g)$

לכן $\langle g \rangle = G, |\langle g \rangle| = p$

סעיף ב' בתרגיל 2.

□

משפט פרמה הקטן

יהיה p ראשוני, ו- $a \in \mathbb{Z}$, אם $\text{gcd}(a, p) = 1$ אז $a^{p-1} \equiv 1 \pmod{p}$

הוכחה. נתבונן בחבורה הכפלית של \mathbb{Z}/p , מסומנת \mathbb{Z}/p^\times שהוא השדה בלי 0

הגודל של \mathbb{Z}/p^\times הוא $p-1$ ולכן לכל x בחבורה הזאת $x^{p-1} = 1$

כעת נחלק את a ב- p עם שארית, ונקבל $a = np + r$ כאשר $0 < r \leq p-1$, וזה נכון כי הם זרים, דהינו $r \in \mathbb{Z}/p^\times$.

נשים לב כי

$$a^{p-1} = (np + r)^{p-1} \implies a^{p-1} = (np + r)^{p-1} \pmod{p} = \sum_{i=0}^{p-1} \binom{p-1}{i} (np)^i r^{p-1-i} \pmod{p} = r^{p-1} \pmod{p}$$

לכן $a^{p-1} \equiv r^{p-1} \equiv 1 \pmod{p}$

□

שאלה 4 סעיף א'

היה צריך למצוא תת-חבורה של $GL_n(\mathbb{F})$ שאיזומורפית ל- S_n .

פתרון. אוסף מטריצות הפרמוטציה, $\{ \text{בכל שורה או עמודה יש איבר בודד שאיננו אפס והוא אחת} \}$ $H = \{ A \in M_n(\mathbb{F}) \mid$

המטריצות האלה הן כידוע מטריצות שפשוט מחליפות אנפים בווקטורים ולמעשה זה פשוט תמורה על הווקטורים מסדר n .

$S_n = S([n])$ ולכן נגדיר $\varphi : H \rightarrow S_n$ על-ידי התמורה שפועלת על A $\varphi(A) = A$.

□