מבנים אלגבריים 1

4 ביוני 2024

תוכן העניינים

1 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:

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

1.1 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).

1.2 למה: קיום איבר נייטרלי יחיד

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

הוכחה. $e_1 = e_1 \circ e_2 = e_2$ ☐

דהינו, קיים איבר נייטרלי יחיד.

1.3 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: $xy = x \cdot y$.

1.4 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 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 $\{1,\dots,n\}$
- $\mathrm{Sym}(X) = \{f : X \to X \mid f$ 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
  $GL(V) = \{f : V \to V \mid f$ 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.

2 תרגול 1 — 7.5.2024

2.1 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.

2.2 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 $x^n \cdot x^m = x^{n+m}$ ואף $(x^n)^m = x^{n\cdot m}$.

2.3 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 $H \le G$.
לדוגמה נראה $(2\mathbb{Z}, +, 0) \le (\mathbb{Z}, +, 0)$ חבורת הזוגיים בחיבור היא תת־חבורה של השלמים.
$(\mathrm{diag}_n(\mathbb{R}), \circ, I_n) \le (GL_n(\mathbb{R}), \circ, I_n)$ חבורת המטריצות האלכסוניות היא תת־חבורה של המטריצות.
$(GL_n(\mathbb{Q}), \circ, I_n) \le (GL_n(\mathbb{R}), \circ, I_n)$ מטריצות הפיכות מעל הרציונליים חלקיות למטריצות הפיכות מעל הממשיים.

קריטריון מקוצר לתת־חבורה

תהי G חבורה ותהי קבוצה $H \subseteq G$ אז $H \le G$ (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

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

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. □

2.4 חבורת התמורות

תהי X קבוצה, אז $\mathrm{Sym}(X)$ היא קבוצת הפונקציות החד־חד ערכיות ועל מ־X לעצמה.
$(\mathrm{Sym}(X), \circ, Id)$ היא חבורה, מורכבת מכלל התמורות, הרכבת פונקציות ופונקציית הזהות.
אם X היא קבוצה סופית אז $S_n = \mathrm{Sym}(X)$, 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:

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

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 $\sigma = (x_1\, x_2\, \ldots\, x_l)$.

בהינתן $\tau \in S_n$, מתקיים

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

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

3 שיעור 2 — 8.5.2024

3.1 מבוא לאיזומורפיות

המטרה שלנו היא להבין מתי שתי חבורות שונות הן שקולות, ולחקור את מושג האיזומורפיות.
נבחן את $\mathbb{Z}/2$ ואת $(\{\pm1\},\cdot)$ ובשתיהן יש רק שני איברים, אחד נייטרלי ואחד לא, ובשתיהן הפעולות מתנהגות אותו דבר בדיוק.

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

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

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

הגדרה: הומומורפיזם

עבור G ו־H חבורות:
הומומורפיזם מ־G ל־H היא פונקציה $\varphi : G \to H$ 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

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

הוכחה. נראה ששלושת התכונות מתקיימות:

1. נבחר $x \in G$ ונראה כי $e_H = \varphi(e_G) \iff \varphi(x) = \varphi(e_G x) = \varphi(e_G)\varphi(x)$.
2. נתון
3. $\varphi(e_G) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) = e_H \implies \varphi(x^{-1}) = \varphi^{-1}(x)e_H$

ומצאנו כי שלושת התנאים מתקיימים. □

הגדרה: איזומורפיזם

איזומורפיזם 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

ההומומורפיזם $\varphi : G \to H$ הוא איזומורפיזם אם ורק אם קיים הומומורפיזם $\psi : H \to G$ 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 $(\{\pm 1\}, \cdot) \cong \mathbb{Z}/2$ 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 $GL_2(\mathbb{F}_2) \ncong S_3$. 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

$\varphi : G \to H$ ו־$\psi : H \to K$ שני הומומורפיזמים, אז גם $\psi \circ \varphi : G \to K$ 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 $\varphi(1+3) = \varphi(4) = 5, \varphi(1) + \varphi(3) = 6$.
פונקציית הזהות היא אוטומורפיזם, והפונקציה $\varphi(n) = -n$ על־פי בדיקה ישירה של הגדרות.
נבחן את פונקציית הכפל בקבוע, $\varphi(n) = 2n$, נראה כי $\varphi(n+m) = 2(n+m) = 2n + 2m, \varphi(n) + \varphi(m) = 2n + 2m$. הומומורפיזם, אבל לא כל איבר שייך לקבוצה השנייה ולכן לא אוטומורפיזם.

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

טענה, ערך (Aut (Z

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

הוכחה. יהי $\varphi : \mathbb{Z} \xrightarrow{\sim} \mathbb{Z}$, ראשית נראה כי $\varphi(n) = n\varphi(1)$.
עבור $n = 0$ ברור, עבור $n > 1$ נראה כי $\varphi(n) = \varphi(1 + \cdots + 1) = \varphi(1) + \cdots + \varphi(1) = n\varphi(1)$.
עבור $n \le 1$ 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 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 $e = (e_G, e_H) \in G \times H$
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: 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:

- $\{0°, 90°, 180°, 270°\} \leq D_4$
- $\{\sigma \in S_n \mid \sigma(1) = 1\} \leq S_n$
  - 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: חיתוך תת־חבורות

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

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 $xy \in \bigcap_{\alpha \in S}$.

ומצאנו כי זוהי חבורה. $\square$

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.

4 שיעור 3 — 15.5.2024

4.1 תת־חבורות

הגדרה: תת־חבורה נוצרת

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

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

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 סגירות 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

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

וידוע כי $(xy)(x^{-1}y^{-1}) = xyx^{-1}y^{-1} = xx^{-1} = 1$

הגדרה: שלמות תת־חבורה יוצרת

אם $G = \langle S \rangle$ אומרים ש־$S - e$ יוצרת את G.
דוגמה: מתקיים $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. כקונספט כללי $d\mathbb{Z} = \langle d \rangle$.
מה לגבי $\mathbb{Z}/n$? מתקיים $\mathbb{Z}/n = \langle 1 \rangle$.

חבורה ציקלית

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

טענה

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

דוגמה:

$G = D_4$.
נגדיר את σ להיות סיבוב בתשעים מעלות, ואת τ להיות היפוך על ציר האיקס.
אז יש לנו את $\langle \sigma \rangle = \{e, \sigma, \sigma^2, \sigma^3\}$
וגם $\langle \tau \rangle = \{e, \tau\}$.

אנחנו יכולים להכפיל כל שני איברים משתי הקבוצות שסימנו עכשיו.

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

נראה כי לדוגמה $\tau\sigma = \sigma^3\tau, \sigma^4 = e, \tau^2 = e$.

ונראה כי $\tau\sigma\tau^{-1} = \sigma^3 = \sigma^{-1}$.

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.

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

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

נקבל כי $r = a - nd \in H$. מהמינימליות של d נובע כי $r = 0$ ולכן $a = nd \in d\mathbb{Z}$. □

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 $d = \gcd(a, b)$ (Greatest common divisor) מחלק משותף מקסימלי כך שמתקיים: $d \mid a, b$ וגם לשלכל $m \mid a, b$ מתקיים גם $m \mid d$.

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

נראה ש־$d = \gcd(a, b)$.

מצד אחד $a, b \in d\mathbb{Z}$ ולכן $d \mid a, b$.

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

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

מסקנה: הלמה של Bézout

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

4.2 מחלקות (Cosets)

הגדרה: מחלקה ימנית ושמאלית

תהי G חבורה ו־$H \leq G$ ו־$x \in G$. נגדיר את המחלקה המשלאתי 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.

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

$\square$

מסקנה

לכל $x, y \in G$ מתקיים
$xH = yH$ (אם ורק אם $x^{-1}y \in H$).
או $xH \cup yH = \emptyset$

הוכחה. אם $z \notin xH \cup yH$ אז מהלמה הקודמת $yH = ZH = xH$. $\square$

טענה: כיסוי זר

$H \leq G$ התת־קבוצות מהצורה xH עבור $x \in G$ מהוות כיסוי זר של G.

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

טענה:

לכל $x, y \in G$ יש התאמה חד־חד ועל ערכית של קבוצות $yH \xrightarrow{\sim} xH$.
בפרט אם H סופית אז לכל המחלקות אותו גודל, $|xH| = |yH|$.

הוכחה. נגדיר $\varphi : xH \to yH$ על־ידי $\varphi(z) = yx^{-1}z$.
ונגדיר פונקציה חדשה $\psi : yH \to xH$ על־ידי $\psi(z) = xy^{-1}z$.
אז מתקיים $\psi = \varphi^{-1}$ ובהתאם נובע כי φ איזומורפיזם. $\square$

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 $|G| = |H| \cdot |G/H|$.
הגודל של $|G/H| = |G|/|H|$. $\square$

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

דוגמות

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

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

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

5 שיעור 4 — 20.5.2024

5.1 חזרה

הגדרה: סדר של חבורה

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

למה: סדר

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

הוכחה. נוכיח שאם $o(x)$ סופי אז

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

ואם $o(x) = \infty$ אז

$$\langle x \rangle = \{1, x, x^2, \ldots,\} \cup \{x^{-1}, x^{-2}, \ldots\} \tag{2}$$

הוכחה ל־(1).

(1) תת־חבורה:

- $x^k \cdot x^m = x^{(m+k) \mod o(x)}$.
- $(x^n)^{-1} = x^{o(x)-n}$.

כל ההאיברים שונים כי אם $x^k = x^m$ ל־$0 \leq k < k \leq o(x)$ אז

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

ונקבל $1 \leq m - k < o(x)$ בסתירה למינימליות של $o(x)$.

הוכחה ל־(2):

אם $H = \langle x \rangle$.

סופיות נתונה בקבוצה.

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

מסופיות קיימים $0 \leq k < m$ עבורם

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

ולכן ל־x יש סדר סופי, משובך היונים.

2 תרגיל. $\square$

מסקנה מלאגרנז'

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

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

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

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

ולכן $a|n,b|n$, a,b זרים ולכן $ab|n$.
מכיוון ש־$|\mathbb{Z}/a\times\mathbb{Z}/b|=|\mathbb{Z}/a|\cdot|\mathbb{Z}/b|=ab$
נובע ש־$\mathbb{Z}/a\times\mathbb{Z}/b$ ציקלית מגודל ab ולכן איזומורפית ל־$\mathbb{Z}/ab$. □

5.2 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 $\cdot : G\times X\to X$, $g\cdot x$ ↤ $(g,x)\mapsto g\cdot x$ כך שמתקיים:

1. $1\cdot x=x$ לכל $x\in X$.
2. $h\cdot(g\cdot x)=(hg)\cdot x$ לכל $x\in X,g,h\in G$.

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

דוגמות לפעולות כאלה

1. S_n פועלת על הקבוצה $X=\{1,2,\dots,n\}$ על־ידי
$$S_n\times\{1,\dots n\}\to\{1,\dots,n\}$$
על־ידי $(\sigma,k)\mapsto\sigma(k)$.
2. $D_n\le S_n$ 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. $GL_n(\mathbb{R})\circlearrowright\mathbb{R}^n$ על־ידי
$$GL_n(\mathbb{R})\times\mathbb{R}^n\to\mathbb{R}^n,\qquad (A,v)\mapsto Av$$
קבלת וקטור ומטריצה וכפל הווקטור במטריצה.
$O_n(\mathbb{R})\le GL_n(\mathbb{R})\circlearrowright\mathbb{R}^n$ פעולה אורתוגונלית על וקטורים, שקול למעשה ל־S^{n-1}.
$SO_2(\mathbb{R})=O_2(\mathbb{R})\cap SL_n(\mathbb{R})$. אף היא פעולה על $\mathbb{R}$.
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 ריגורזי ושיטתי. נשים לב לדוגמה ש־$D_4\circlearrowright\{D_1,D_2\}$, 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 $\tau : X \to X$ שמקיימת $\tau \circ \tau = Id_X$, זאת שכן

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

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

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

$$\tau(\begin{bmatrix} x \\ y \end{bmatrix}) = \begin{bmatrix} -x \\ y \end{bmatrix}, \qquad \tau(\begin{bmatrix} x \\ y \end{bmatrix}) = \begin{bmatrix} x \\ -y \end{bmatrix}, \qquad \tau(\begin{bmatrix} x \\ y \end{bmatrix}) = \begin{bmatrix} x \\ y \end{bmatrix}$$

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 $G \circlearrowright G$.

האם פעולה ימנית גם עומדת בהגדרת הפעולה?
נבדוק את $G \times G \to G$ המוגדרת על־ידי $(g, x) \mapsto xg$:
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 $(g, x) \mapsto xg^{-1}$
פעולה זאת היא אכן פעולה מוגדרת והיא נקראת **הפעולה הרגולרית הימנית**.

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

הגדרה: הצמדה

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

היא פעולת ההצמדה, נחקור אותה בתרגיל. באנגלית Conjugacy. באופן דומה הפעולה היא $conjugate$.

בהינתן פעולה של $G \circlearrowright X$ נגדיר פונקציה $f : G \to Sym(X) \subseteq End(X)$ על־ידי

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

זאת שכן $G \times X \to X$ שקול ל־$G \to \{X \to X\}$.

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 $f(g) \in Sym(X)$?
כי $f(g^{-1}) \cdot f(g) = f(g^{-1}g) = f(1) = Id$. גם $f(g) \cdot f(g^{-1}) = f(gg^{-1}) = f(1) = Id$.

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

6 תרגול 3 — 21.5.2024

6.1 שאלות מתרגיל 1

שאלה 1

$$End(X) = \{f : X \to X\}$$

והיה 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 $\operatorname{Im} M$ 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 $z = tz^2 = tz = e$. $\square$

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

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

$\square$

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

נבחן את $End(\mathbb{N})$ ונבחר את $f(x) = x + 1$ ו־ $g(x) = \begin{cases} 1, & x = 1 \\ n-1, & n > 1 \end{cases}$

שאלה 4

סעיף ב', צריך להראות שזה איזומורפי

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

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 למצור פונקציה

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

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

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

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

6.2 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. $gH = H \iff g \in H$
2. אם H סופית אז לכל $g \in G$ מתקיים $|gH| = |H|$.
3. $\forall g \in G : gH = Hg \iff gHg^{-1} \subseteq H$.
4. ישנה התאמה בין הקבוצות gH 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.

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

וזה מן הסתם מקיים $D_3 = \langle r, f \rangle$.
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:

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

עתה נדבר על סדר.

6.3 משפט לגרנז'

הגדרה: סדר של איבר

תהא G חבורה סופית ו־, לכן $g \in G$ נגדיר את הסדר של g, או $|g| = ord(g)$ 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 $|G| \Big| |H|$.

מסקנה

תהא G סופית ו־$g \in G$ אז $|G|\Big|ord(g)$.

הוכחה. על־ידי התבוננות ב־$H = \langle g \rangle$. ☐

למה: $|H| = ord(g)$.

הוכחה. נגדיר $\varphi : \mathbb{Z}/ord(g) \to H$ על־ידי $\varphi(b) = g^n$.
נראה כי φ חד־חד ערכית ועל.
יהיו $n, m \in \mathbb{Z}/ord(g)$ 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 $ord(g)$.
מה החבורה הנוצרת על־ידי $\langle g \rangle = \{g^n \mid n \in \mathbb{N}\}$.
יהא $n \in \mathbb{Z}$ נחלק את n עם שארית בסדר של g, $n = m \cdot ord(g) + r$ ו־$r \in \mathbb{Z}/ord(g)$. לכן $g^n = g^{m \cdot ord(g)+r} = g^r$.
הראינו כי $|H| = ord(g)$ ולכן הסדר של $|G|\Big|ord(g)$. ☐

מסקנה:

תהיה G חבורה סופית.

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

הוכחה. לפי המסקנה הקודמת

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

☐

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 $ord(g) > 1$ אך מצד שני $|\langle g \rangle| = ord(g)\big|p$
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 $\gcd(a, p) = 1$ אז $a^{p-1} \equiv 1(\mod p)$

הוכחה. נתבונן בחבורה הכפלית של $\mathbb{Z}/p$, מסומנת $\mathbb{Z}^{\times}_{/p}$ שהוא השדה בלי 0
הגודל של $\mathbb{Z}^{\times}_{/p}$ הוא $p - 1$ ולכן לכל x בחבורה הזאת $x^{p-1} =_{\mathbb{Z}/p} 1$.
כעת נחלק את a ב־p עם שארית, ונקבל $a = np + r$ כאשר $0 < r \leq p - 1$, וזה נכון כי הם זרים, דהינו $r \in \mathbb{Z}^{\times}_{/p}$.
נשים לב כי

$$a^{p-1} = (mp + r)^{p-1} \implies a^{p-1} = (mp + r)^{p-1} \mod p = \sum_{i=0}^{n-1} \binom{p-1}{i} (mp)^{p-1} \cdot r = r^{p-1} \mod p$$

לכן $a^{p-1} = r^{p-1} = 1$. ☐

6.4 שאלה 4 סעיף א'

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

פתרון. אוסף מטריצות הפרמוטציה, $H = \{A \in M_n(\mathbb{F}) \mid \text{בכל שורה או עמודה יש איבר בודד שאיננו אפס והוא אחת}\}$.
המטריצות האלה הן כידוע מטריצות שפשוט מחליפות אגפים בווקטורים ולמעשה זה פשוט תמורה על הווקטורים מסדר n.
$S_n = S([n])$ ולכן נגדיר $\varphi : H \to S_n$ על־ידי התמורה שפועלת על A $\varphi(A) = A$. $\square$

7 שיעור 5 — 22.5.2024

צריך ללכת לשעות קבלה, ליאור כועס עלינו שאנחנו לא הולכים אליהן. תברר מה השעת קבלה שלו ולך פעם אחת.

נניח שיש לי G חבורה סופית. מלגרז' נובע ש־$|H|\Big||G|$ $\implies$ $H \leq G$. משפט קושי אומר שאם $p\Big||G|$ ו־p ראשוני אז קיימת חבורה $H \leq G$ כך ש־$|H| = p$. למעשה קיים $x \in G$ עם $o(x) = p$.

7.1 פעולות על קבוצות

בהינתן $G \circlearrowright X$ נסמן עבור $x, y \in X$ את $x \sim y$ כיחס שמתקיים אם $\exists g \in G : g \cdot x = y$.

במילים פשוטות, שני איברים בקבוצה הם דומים אם קיים איבר בחבורה שמוביל מאחד מהם לשני. רעיונית מדובר בסימטריה, ולכן הגיוני לשאול אם שני מצבים הם סימטריים ללא קשר למה הפעולה שמשרה את הסימטריה.

טענה: יחס שקילות בפעולה על קבוצות

$\sim$ הוא יחס שקילות.

הוכחה. נבחין כי הגדרת יחס השקילות מתקיימת:

- רפלקסיבי $e \cdot x = x$.
- סימטרי: $x \sim y \implies \exists g \in G g \cdot x = y \implies g^{-1}y = x \implies y \sim x$.
- טרנזיטיבי: $x \sim y, y \sim z \implies \exists g, h \in G, gx = y, hy = z \implies (hg)x = h(gx) = hy = z \implies x \sim z$

$\square$

משמעות הדבר היא שסימטריות הן שקולות. שוב, מדובר ברעיון מאוד הגיוני שכן אם בוחנים את הכול בעיניים של סימטריה. כלל המצבים שסימטריים בזוגות גם סימטריים בכללי.

הגדרה: מסלולים

בהינתן $G \circlearrowright X$, המסלולים של G הם מחלקות השקילות של $\sim$ והמסלול של $x \in X$ הוא

$$O(x) = \{y \in X \mid y \sim x\} = \{y \in x \mid \exists g \in G : g \cdot x = y\}$$

סימון: קבוצת המסלולים מסומנת $G\backslash X$.

אבחנה: $X = \bigcup_{O \in G\backslash X} O$, דרך מזעזעת להגיד שהקבוצה המקורית מורכבת מהחלוקה למסלולים שלה.

מהותית אנו מדברים פה על החלוקה של X לפי השקילות, בכל קבוצה יהיו רק איברים ששקולים אחד לשני.

הגדרה: נקודת שבת

$x \in X$ נקודת שבת של G אם $|O(x)| = 1$.

כלומר $\forall g \in G : g \cdot x = x$.

הרעיון הוא שהפעולה על איבר מסוים תמיד מחזירה אותו עצמו, ללא קשר לאיזו סימטריה מהחבורה אנחנו בוחרים.

הגדרה: טרנזיטיבית

פעולה $G \circlearrowright X$ נקראת טרנזיטיבית אם $|G\backslash X| = 1$.

הפעולה היא טרנזיטיבית אם יש רק קבוצת מסלולים (שהיא חלוקת שקילות) אחת, דהינו שכל איבר בקבוצה סימטרי לכל איבר אחר.

מסקנה

$H\backslash G$ קבוצת המסלולים של $G \circlearrowright H$ רגולרית משמאל שקולה ל־$H\backslash G$ קבוצת המחלקות הימניות של H ב־G.
באופן דומה G/H המסלולים של הפעולה $G \circlearrowright H$ הרגולרית מימין.
יש פה התכנסות מאוד אלגנטית גם של הרעיון של מחלקות ימניות ושל השקילויות מבחינת רגולרית משמאל, זו הרי מהותית מגדירה הכפלה של האיברים משמאל, ולכן גם המסלולים מעל התת־חבורה הם המחלקות האלה.

דוגמות

1. $G \circlearrowright G$ פעולה רגולרית שמאלית. $\forall x, y \in G, x \sim y \iff g \in G : gx = y$ ותמיד קיים g כזה והוא אף יחיד, $g = yx^{-1}$. לכן יש מסלול אחד והפעולה טרנזיטיבית.
2. יהי $H \le G$, ונבחן את $G \circlearrowright H$, רגולרית משמאל, הפעם $x \sim y \iff \exists h \in H : hx = y \iff yx^{-1} \in H \iff Hx = Hy$ מחלקות ימניות.

מצאנו הפעם כי יש מסלול בין איברים רק אם הם באותה מחלקה ימנית (על אף שמדובר על רגולרית שמאלית). נראה את המסקנה האחרונה.

3. $\mathbb{R}^2 \circlearrowright GL_2(\mathbb{R})$ מטריצות הפיכות פועלות על המרחב $\mathbb{R}^2$.
מסלולים: $\{\{0\}, \mathbb{R}^2 \setminus \{0\}\}$.

ביתר פירוט, מטריצות הפיכות משמרות את האי־איפוס, אבל כן נוכל להגיע מכל וקטור לכל וקטור אחר עם המטריצה הנכונה. לעומת זאת וקטור אפס ישאר אפס מכל מטריצה שתוכפל בו, ולכן הוא לא סימטרי לאף וקטור אחר בפעולה.

4. $\mathbb{R}^2 \circlearrowright O_2(\mathbb{R})$, ידוע כי $O_2(\mathbb{R}) \le GL_2(\mathbb{R})$. הפעם כל וקטור צריך להגיע רק לווקטור מאותו גודל.
מסלולים: $\{\{0\}, \{\{v \in \mathbb{R}^2 \mid |v| = a\} \mid a > 0\}\}$.

לכל וקטור שנבחר, כל מטריצה בחבורה משמרת את הנורמה שלו, אבל לא את הכיוון, ובהתאם נוכל להסיק שכל שני וקטורים עם אותה נורמה שקולים ונמצאים באותה קבוצה.

5. $\{1, \ldots, n\} \circlearrowright S_n$ הפעולה הזו היא טרנזיטיבית.

זה די טריוויאלי בגדול, נוכל לסדר מחדש את רשימת המספרים בכל דרך על־ידי איזושהי תמורה, ובהתאם כל הסדרים דומים אחד לשני ויש ביניהם מסלול.

6. כל הדגלים שמחולקים לשלושה פסים בשלושה צבעים, וכל האופציות לבחור את של שלושת הצבעים. יש מן הסתם שמונה דגלים כאלה. אפשר להגדיר פעולה $\mathbb{Z}/2$ של סיבוב ב־$180°$ ואז אפשר לראות אילו דגלים מתקשרים לאילו דגלים אחרים. יש שישה מסלולים.

הגדרה: מקבע

תהינה $X \circlearrowright G$, עבור $g \in G$, ונגדיר את **המקבע** להיות $Fix(g) = \{x \in X \mid gx = x\}$.
עוד סימון הוא X^g, אבל לא מומלץ להשתמש בו, הוא יחסית מבלבל.
עבור איבר בחבורה, המקבע הוא כל האיברים בקבוצה שהפעולה לא משנה, הם לא בהכרח נקודות שבת כי אנחנו מדברים פה בהקשר של סימטריה ספציפית.

הגדרה: מייצב

יהיו $X \circlearrowright G$, אז נגדיר את המייצב של $x \in X$ להיות $Stab(x) = \{g \in G \mid gx = x\}$, באנגלית Stabilizer.
סימון נוסף הוא G_x.
במילים זוהי קבוצת איברי החבורה שלא משנים את x, או לחילופין שולחים אותו לעצמו.
האינטואציה היא שיש איברים שסימטריות מסוימות פשוט לא משפיעות עליהם, ובהתאם המייצב הוא קבוצת הסימטריות הכאלה שנייטרליות לאיבר שבחרנו.

למה: מייצב הוא תת־חבורה

G_x תת־חבורה של G.

הוכחה. נבדוק את הגדרת תת־החבורה:

1. איבר נייטרלי: $e \cdot x = x \implies e \in G_x$.
2. סגירות לכפל: $\forall g,h \in G, g\cdot x, h\cdot x = x \implies (gh)\cdot x = g\cdot(h\cdot x) = g\cdot x = x \implies gh \in G_x$.
3. קיום הופכי: $g \in G \implies g\cdot x = x \implies x = g^{-1}\cdot x \implies g^{-1} \in G_x$.

מצאנו כי כלל התכונות מתקיימות ולכן G_x, המייצב של x, הוא תת־חבורה של G. □

הגדרה: פעולה חופשית

$X \circlearrowleft G$ נקראת חופשית אם $G_x = \{e\}$ לכל $x \in X$. במילים אחרות, הפעולה לעולם לא שולחת איבר לעצמו.
היא נקראת נאמנה אם $\bigcap_{x\in X} G_x = \{e\}$, החיתוך הזה בכללי גם נקרא גרעין.
נאמנה זה שם קצת מוזר אבל הוא בגדול מבטיח שאין איבר בחבורה שכל איברי הקבוצה נייטרליים אליו, חוץ מהאיבר הנייטרלי עצמו.
עניין הגרעין הוא די דומה למה שקורה בלינארית גם, איבר שהפעולה איתו לא משפיעה על אף איבר בקבוצה.

דוגמה

נבחן את $G \circlearrowleft G$ על־ידי הצמדה.

$$O(x) = \{gxg^{-1} \mid g \in G\}$$

המסלול של x הוא קבוצת האיברים שמקיימים $gxg^{-1} = y$, באופן מאוד דומה למטריצות דומות. נקרא למסלול הזה מחלקת צמידות.

הגדרה: מרכז

ישנו המרכז של x ב־G והוא $gx = xg \iff C_G(x) = G_x = \{g \in G \mid gxg^{-1} = x\}$. באנגלית Centrilizer.
מרכז הוא סוג של מייצב במקרה שבו $X = G$.

משפט: מסלול־מייצב

$X \circlearrowleft G$ ו־$x \in X$. $|O(x)| = [G : G_x]$. וזה נכון גם כשהחבורה לא סופית. $G/G_x \xrightarrow{\sim} O(x)$.
בפרט אם G סופית אז $|O(x)| = \frac{|G|}{|G_x|}$ ונובע שהגודל של כל מסלול מחלק את גודל החבורה.
במילים הטענה היא שהמסלול של x, שהוא מספר האיברים שאפשר להגיע אליהם ממנו, שווה לאינדקס של המייצב, דהינו מספר מחלקות השקילות השונות שאפשר ליצור בעזרת מחלקות שמאליות עם התת־חבורה שלא מושפעת מ־x.

הוכחה. נגדיר $f : G/G_x \to O(x)$ ונראה שהיא חד־חד ערכית ועל.
נבחר $f(gG_x) = g\cdot x$. זה לא בהכרח מוגדר היטב ולכן נבדוק למה זה כן.
אם יש איבר $g' \in gG_x$ אז $g' = g\cdot h$ כך ש־$h \in G_x$. מתקיים ש־$g\cdot x \overset{h\in G_x}{=} ghx = g'\cdot x$.
על: לפי הגדרה.
חד־חד ערכי: נניח ש־$gG_x = g'G_x \overset{\text{סגירות להופכי}}{\implies} (g')^{-1}g \in G_x \implies (g')^{-1}gx = x = g'\cdot x = f(g'G_x) = f(gG_x) = g\cdot x$. □

דוגמה

תהינה חבורה G ותת־חבורתה $H \leq G$, יש פעולה "רגולרית" של G על G/H:

$$g\cdot(xH) = (g\cdot x)H$$

משפט קושי

יהיו G חבורה סופית ו־p ראשוני כך ש־$p \,\Big|\, |G|$. אז קיים $x \in G$ כך ש־$ord(x) = p$.

הוכחה. נגדיר פעולה של החבורה $\mathbb{Z}_{/p}$ על הקבוצה $X = \{(g_1, \ldots, g_p) \in G^p \mid g_1 g_2 \cdots g_p = e\}$.
הפעולה פועלת על־ידי שיפט ציקלי: $u \in \{0, 1, \ldots, p-1\}$ אז $k \cdot (g_1, \ldots, g_p) = (g_{k+1}, g_{k+2}, \ldots, g_{p \mod p}, g_1, \ldots, g_k)$.
אז $k(g_{k+1}, \ldots, g_p) = e$ וגם $(g_{k+1}, \ldots, g_p)(g_1, \ldots, g_k) = e$.
נבחין כי כלל המסלולים בפעולה הם אחד משני סוגים:

- מסלולים בגודל p. אם לא כל האיברים זהים, מעגל שלם יקח ככמות האיברים והיא מוגדרת להיות p.
- מסלולים בגודל 1. אם כל האיברים זהים אז שיפט יחזיר את האיבר עצמו.

ממשפט מסלול־מייצב p $|O(x)| = 1, \iff |O(x)|\Big|p$.
עתה נבחין כי אם ישנו מסלול בגודל p אז הוא כמובן ממלא את טענת ההוכחה ולכן נניח שאין כזה.
נראה כי מסלול בגודל 1 הוא מסלול שמקיים $(g_1, \ldots, g_p) = (g_2, \ldots, g_p, g_1)$ כלומר $x = (g, \ldots, g)$, $g^p = e$.
נשים לב כי נוכל לחלק את הקבוצה המקורית ומתקיים $\bigcup_{O \in \mathbb{Z}_{/p} \setminus X} O = X$, ובהתאם מהאיחוד הזר נקבל גם $|X| = \sum_{O \in \mathbb{Z}_{/p} \setminus X} |O|$.
אם $(e, \ldots, e)$ היה נקודת השבת היחידה אז $\sum_{O \in \mathbb{Z}_{/p} \setminus X} |O| = 1 (\mod p)$, שכן כל מסלול כולל p חילופים ונקודת השבת היחידה הייתה תורמת 1 בלבד.
לכן מצד אחד $p\Big||G|^{p-1}$ ומצד שני $|G|^{p-1} \cong 1 (\mod p)$ ולכן קיים $x \neq e$ עם $x^n = e$. $\square$

ההוכחה מוויקיפדיה הרבה יותר ברורה.

8 שיעור 6 — 27.5.2024

8.1 מקבעים של פעולות

תזכורת: מקבע

מקבע $X^g=\{x\in X\mid gx=x\}$, דהינו האיברים ב־X שלא משתנים על־ידי הסימטריה g.

לדוגמה עבור החבורה D_4 ו־$X=\{1,2,3,4\}$ אוסף קודקודי ריבוע נבחן את g סיבוב על האלכסון: $g=(1\ 3)$ ואת $h=(1\ 2)(3\ 4)$ שיקוף על האמצע. אז כמובן המקבע של g ב־X הוא $X^g=\{1,3\}$ אוסף הקודקודים שלא מושפעים מהסימטריה g. באופן דומה $X^h=\emptyset$, דהינו הסמיטריה h תמיד משנה את כל הקודקודים ובהתאם המקבע הוא ריק.

8.2 למה: הלמה של ברנסייד

תהיה חבורה סופית G ופעולה $X \circlearrowleft G$ כאשר X סופית גם היא. יהי $g\in G$ ונסמן $Fix(g)=X^g=\{x\in X\mid gx=x\}\subseteq X$.

אז מספר המסלולים (מסומן גם X/G) הוא

$$|X/G|=\frac{1}{|G|}\sum_{g\in G}|Fix(g)|$$

דהינו ממוצע כמות האיברים שנשארים במקום היא ככמות המסלולים השונים.

הוכחה. תהי חבורה סופית G. עבור X סופית ופעולה $X \circlearrowleft G$ נגדיר

$$E(X)=\frac{1}{|G|}\sum_{g\in G}|X^g|$$

נוכיח כי $E(x)=|X/G|$.

נשים לב שאם X,Y קבוצות זרות עם פעולה של G, אז נובע מהזרות ומהגדרת המסלולים של הקבוצות כי

$$(X\sqcup Y)/G=X/G\sqcup Y/G\implies|(X\sqcup Y)/G|=|X/G|+|Y/G|$$

עוד נראה כי $\forall g\in G:(X\sqcup Y)^g=X^g\sqcup Y^g$ ולכן גם $|(X\sqcup Y)^g|=|X^g|+|Y^g|$, ונוכל להסיק ש־$|E(X\sqcup Y)|=E(X)+E(Y)$.

נסיק כי אילו הלמה נכונה עבור X,Y זרים, אז היא מתקיימת גם עבור איחודם $X\sqcup Y$.

תהי X קבוצה כלשהי, נוכל לכתוב גם

$$X=\bigsqcup_{O\in G\backslash X}O$$

במילים ש־X היא איחוד זר של קבוצות המסלולים השונות שמוגדרות על־ידי הפעולה $X \circlearrowleft G$.

על־כן מהטענה שהוכחנו זה עתה מספיק להוכיח את הטענה כאשר ל־X יש מסלול יחיד $O=x$, ובמקרה הכללי נוכל לאחד איחוד זר של מסלולים.

נניח מעתה כל $X\neq\emptyset$ עם מסלול יחיד (פעולה טרנזיטיבית). במקרה הזה צריך להוכיח

$$\frac{1}{|G|}\sum_{g\in G}|X^g|=E(X)=1$$

נגדיר עבור $x\in X,g\in G$ את $s(g,x)$ על־ידי

$$s(g,x)=\begin{cases}1, & gx=x\\ 0, & gx\neq x\end{cases}$$

דהינו s מחזירה 1 אם g מקבעת את x. ואנו יודעים כי $X^g=\{g\in G\mid gx=x\}=\{g\in G\mid s(g,x)=1\}$. לכן נוכל להסיק שמתקיים

$$|X^g|=\sum_{x\in G}s(g,x)$$

ועתה נציב ונקבל כי

$$\sum_{g\in G}|X^g|=\sum_{g\in G}\sum_{x\in X}s(g,x)=\sum_{x\in X}\sum_{g\in G}s(g,x)\overset{(1)}{=}\sum_{x\in X}|G_x|\overset{(2)}{=}|X|\cdot|G_x|=|G|$$

(1) נובע ישירות מההגדרה של מייצב $G_x=\{g\in G\mid gx=x\}$.

(2) ממשפט מסלול־מייצב נקבל כי $|G|=|G_x|\cdot|O(x)|$ אבל ידוע שהפעולה טרנזיטיבית ולכן $\forall x\in X: O(x)=X$, לכן $|G|=|X|\cdot|G_x|$.
קיבלנו כי $|E(X)|=1$ ולכן נוכל להסיק כי הטענה מתקיימת תמיד. $\square$

דוגמות

בתזכורת הראינו כי עבור D_4 ו־$X=\{1,2,3,4\}$ מתקיים $|X^g|=2, |X^h|=0$. נחשב את כלל המקבעים ונקבל על־פי הלמה:
$$\frac{1}{8}(4+2+2+0+0+0+0+0)=1=|D_4\backslash X|$$
דהינו D_4 טרנזיטיבית לפי הלמה, שכן יש לה רק מסלול אחד.

דוגמה נוספת היא בחירת G סופית ופעולה שלה על עצמה עם הצמדה.
לכן $g(h)=ghg^{-1}$ ונשים לב כי המקבע הוא $C(g)=G^g=\{h\in G\mid ghg^{-1}=h\}$.
כמות מחלקות הצמידות — היא מספר המסלולים על־פי הצמדה — ניתנת לחישוב על־ידי
$$\frac{1}{|G|}\sum_{g\in G}|C(g)|$$

הגדרה: מרכז חבורה

נגדיר את **המרכז** של חבורה G, המסומן $Z(G)$, להיות קבוצת האיברים שנייטרליים לסדר ההכפלה בהם:
$$Z(G)=\{h\in G\mid \forall g\in G: gh=hg\}$$
לחילופין הגדרה שקולה היא קבוצת האיברים שצמודים לעצמם בלבד.
נגדיר גם C_x מחלקת הצמידות של x, דהינו
$$C_x=\{g\in G\mid gxg^{-1}=x\}$$

טענה: מרכז הוא תת־חבורה

תהי G חבורה, אז $Z(G)\subseteq G$ היא תת־חבורה.

הוכחה. נראה כי תכונות החבורה חלות על $Z(G)$:

1. איבר נייטרלי: $\forall g\in G: eg=ge \implies e\in Z(G)$
2. סגירות לכפל: $\forall a,b\in G: \forall g\in G, abg=agb=gab \implies ab\in Z(G)$.
3. סגירות להופכי: $n\in Z(G): ng=gn \implies \forall g\in Gn^{-1}g=gh^{-1}$

לכן $Z(G)$ חבורה וחלקית ל־G ולכן נובע $Z(G)\leq G$. $\square$

למה: חיתוך מרכזים

תהי G חבורה, ניזכר כי המרכז של $x\in G$ מוגדר על־ידי
$$C_G(x)=C(x)=\{g\in G\mid gxg^{-1}=g\}$$
ומתקיים
$$Z(G)=\bigcap_{x\in G}C(x)$$

הוכחה. נובע ישירות מההגדרות $\square$

לכן נשים לב שחיתוך המרכזים הוא המרכז של החבורה, והיא תת־חבורה אבלית.

סימון: מחלקות צמידות

תהי חבורה G, אז נסמן את אוסף מחלקות הצמידות שלה:

$$cong(G) := \{X \subseteq G \mid \forall x, y \in X \exists g \in G : x = gyg^{-1}\}$$

נשים לב שמרכז עבור צמידות מסומן באופן מיוחד, וגם כאן זהו סימון מיוחד עבור $G \backslash G$ עם פעולת ההצמדה.
כל איבר ב־$cong(G)$ הוא קבוצה שכלל האיברים בה צמודים זה לזה. נשתמש בהגדרת המרכז ונכתוב גם

$$cong(G) = \{X \subseteq G \mid \forall x, y \in X : y \in C(x)\}$$

ונסמן $[g] \in cong(G)$ איבר כלשהו מייצג מכל מחלקת צמידות.
נסמן גם C_h מחלקת הצמידות של h ומתקיים

$$C_h = \{g \in G \mid \exists k \in G : khk^{-1} = g\}$$

טענה: נוסחת המחלקות

תהי חבורה סופית G, אז מתקיים

$$|G| = |Z(G)| + \sum_{[h] \in cong(G), h \notin Z(G)} \frac{|G|}{|G_h|}$$

הוכחה. תחילה נבחין כי נוכל לפרק את G:

$$G = \bigsqcup_{[h] \in cong(G)} C_h$$

ונבחין כי לכל $h \in G$ מתקיים

$$h \in Z(G) \iff |C_h| = 1 \iff \forall g \in G : ghg^{-1} = h$$

אז נוכל לראות כי

$$G = Z(G) \sqcup \bigsqcup_{[h] \in cong(G), h \notin Z(G)} C_h$$

ומכאן נסיק

$$|G| = |Z(G)| + \sum_{[h] \in cong(G), h \notin Z(G)} |C_h| \overset{\text{מסלול־מייצב}}{=} |Z(G)| + \sum_{[h] \in cong(G), h \notin Z(G)} \frac{|G|}{|G_h|(= |C_G(h))|}$$

□

9 תרגול 4 — 28.5.2024

9.1 צביעות

הגדרה: צביעה

תהי קבוצה X ותהי צביעה עם m צבעים, אז אז **צביעה** של X עם m היא פונקציה $f : x \to [m]$.
הרעיון פה הוא שאנחנו יכולים לקחת את הקבוצה ולסווג לכל איבר בה צבע (מספר) ומן הסתם יש לנו $[m]^{|X|}$ צביעות רעיוניות כאלה.

טענה: צביעה מעל פעולה

תהי קבוצה X ו־$G \circlearrowright X$ חבורה ופעולה המסומנת על־ידי ., ויהי $[m]^X$ אוסף הצביעות ב־m של X.
אז הפונקציה $. : G \times [m]^X \to [m]^X$ המוגדרת על־ידי

$$\forall g \in G, f \in [m]^X, \forall x \in X : g.\, f(x) = f(g^{-1}.\, x)$$

היא פעולה של G על $[m]^X$.

הוכחה. אנו צריכים לבדוק ששתי התכונות של פעולה של החבורה על הקבוצה מתקיימות.

- נייטרליות האיבר הנייטרלי: $\forall f \in [m]^X, x \in X : e.\, f(x) = f(e^{-1}x) = f(x)$.
- סגירות לכפל: $\forall f \in [m]^X, x \in X : g.\, (h.\, f)(x) = (h.\, f)(g^{-1}.\, x) = f(h^{-1}g^{-1}.\, x) = (gh).\, f(x)$

ומצאנו כי התנאים לפעולה מתקיימים ומתקיים $G \circlearrowright [m]^X$. □

מה שבעצם עשינו פה הוא להרחיב פעולה של G על X להשרות פעולה מעל אוסף הצביעות השונות שלו, ועשינו את זה על־ידי שימוש בכפל בהופכי.
מאוד חשוב לשים לב שאנחנו מקבלים את הצביעה כפונקציה של אוסף האיברים ב־X לאוסף הצבעים, אבל זה עדיין איבר בקבוצת הצביעות.

הגדרה: שימור צביעה

נגדיר שצביעה $f \in [m]^X$ נשמרת על־ידי $g \in G$ אם $f \in Fix(g)$, דהינו ש־$g \cdot f = f$.

9.2 טטרההדרון

נבחן עתה את הטטרההדרון (ארבעון) שמרכזו הוא $0 \in \mathbb{R}^3$ ושקודקודיו מסומנים על־ידי $v_0, \dots, v_3$ ונגדיר אותו מעתה להיות Δ^3. ונגדיר את חבורת הסימטריה $\mathrm{Sym}(\Delta^3)$ להיות אוסף האיזומטריות הלינאריות שמשמרות את הטטרההדרון:

$$\mathrm{Sym}(\Delta^3) = \left\{T \in GL_3(\mathbb{R}) \middle| |\det T| = 1, T\Delta^3 = \Delta^3\right\}$$

ונגדיר גם את חבורת הסימטריות האיזומטריות שנוצרות על־ידי פעולות נוקשות:

$$\mathrm{Sym}_+(\Delta^3) = \left\{T \in \mathrm{Sym}(\Delta^3) \middle| \det T = 1\right\}$$

נשים לב כי כל $T \in \mathrm{Sym}(\Delta^3)$ היא למעשה תמורה בין קודקודי הטטרההדרון. יותר מזה גם נשים לב כי אם שתי העתקות סימטריות משנות את הקודקודים באופן זהה אז הן מתנהגות באופן זהה.
נגדיר אם כן את התורה σ_T כתמורה שמזיזה את הקודקודים על־פי $T \in \mathrm{Sym}(\Delta^3)$.

טענה: פעולת סימטריות על הקודקודים

הפעולה $\cdot : \mathrm{Sym}(\Delta^3) \times \{v_0, \dots, v_3\} \to \{v_0, \dots, v_3\}$ הנתונה על־ידי $T \cdot v_i = T(v_i)$ היא פעולה על הקבוצה $\{v_0, \dots, v_3\}$.

הוכחה. בתרגיל □

מסקנה: איזומורפיות הסימטריות

הפונקציה $\varphi : \mathrm{Sym}(\Delta^3) \to S(\{v_0, \dots, v_3\})$ המוגדרת על־ידי $\varphi(T) = \sigma^T$ היא איזומורפיזם.

הוכחה. מספיק להוכיח ש־φ היא הומומורפיזם ושכל מחזור מהצורה (v_i, v_j) הוא בתמונת φ. העובדה שהיא הומומורפיזם נובעת מיידית מהיותה פעולה על הקבוצה. יהיו $i \neq j$ המתארים קודקודים, אז ישנו מישור העובר בין שני הקודקודים האחרים ודרך $\frac{v_i+v_j}{2}$. השיקוף סביב מרחב זה שולח את v_i ל־v_j והפוך, בלי להשפיע על שאר הקודקודים. לכן $(v_i, v_j) \in \varphi(\mathrm{Sym}(\Delta^3))$. נראה כי $\varphi(\mathrm{Sym}(\Delta^3))$ היא תת־חבורה של $S(\{v_0, \dots, v_3\})$ ולכן היא מכילה קבוצה יוצרת, ומכאן נקבל $\varphi(\mathrm{Sym}(\Delta^3)) = S(\{v_0, \dots, v_3\})$, מהטענות הקודמות נקבל גם חד־חד ערכיות. □

מעתה נתייחס באופן שקול ל־$T \in \mathrm{Sym}(\Delta^3)$ ו־σ_T.

מסקנה: טרנזיטיביות הפעולה

הפעולה של $\mathrm{Sym}(\Delta^3)$ על הקודקודים היא טרנזיטיבית.

הוכחה. נסיק מכך שכל $(v_i, v_j) \in \mathrm{Sym}(\Delta^3)$ שהמסלול של הגעה מכל קודקוד לכל קודקוד הוא יחיד, ולכן ככלל יש מסלול יחיד בפעולה. □

נבחן עתה את הפעולה של $\mathrm{Sym}(\Delta^3)$ על $[m]^X$ כאשר $X = \{v_0, \dots, v_3\}$ כפי שהגדרנו בחלק הקודם.

טענה: מקבעי הסימטריות

יהי $T \in \mathrm{Sym}(\Delta^3)$, אז נוכיח כי $|Fix(T)|$ תלוי בסוג המחזור של T בלבד.

הוכחה. נכתוב את כלל סוגי המחזורים ב־$\mathrm{Sym}(\Delta^3)$ על־פי אורכם:

$1\ 1\ 1\ 1$

$2\ 1\ 1$

$2\ 2$

$3\ 1$

4

מספר התמורות מכל סוג ב־S_4 הן $1, 6, 3, 8, 6$ בהתאמה. עתה נחשב את הצביעות המשתמרות על כל מקרה.
עבור $1\ 1\ 1\ 1$ ישנה רק תמורת הזהות, ובהתאם היא משמרת את הצבע של כל קודקוד, ולכן $|Fix(e)| = m^4$.
עתה נבחן מחזור בגודל 2, דהינו $\sigma = (i, j)$. התמורה הזו תשמר את הצביעה של קודקודים אם ורק אם v_i, v_j הם מאותו הצבע. לכן לשני הקודקודים v_i, v_j יכולות להיות m צביעות שונות כך שהתמורה תשמר את הצביעה, כאשר שאר הקודקודים בלתי תלויים, ולכן במקרה זה ישנן m^3 צביעות משתמרות.
באופן דומה יש m^2 צביעות משתמרות עבור שרשור שני מחזורים מגודל 2.
כאשר בוחנים מחזורים בגודל 3 אז יכולה להיות רק צביעה אחת לשלושת הקודקודים כך שהצביעה תשתמר, ולקודקוד הנותר הצבע חופשי, ונקבל m^2.
עבור תמורות שהן מחזור בודד מגודל 4 אז על כלל הקודקודים להיות באותו צבע, ונקבל כמובן את מספר הצבעים עצמו m. □

נשתמש בלמה של ברנסייד כדי לחשב את מספר המסלולים של סימטריות על קודקודים על צביעות שונות של הקודקודים.

$$|\mathrm{Sym}(\Delta^3) \backslash [m]^X| = \frac{1}{|\mathrm{Sym}(\Delta^3)|} \sum_{T \in \mathrm{Sym}(\Delta^3)} |Fix(T)| = \frac{1m^4 + 6m^3 + 11m^2 + 6m}{24}$$

מסקנה: מסלולים מעל צביעה

בעוד הפעולה של הסימטריות על X היא טרנזיטיבית, הפעולה מעל הצביעות היא עצמה לא כזו בהכרח, דהינו הטרנזיטיביות של פעולה לא מעידה על טרנזיטיביות הצביעה מעליה.

טענה: כמות הצביעות בסימטריות חיוביות

נבחן את הפעולה של $\mathrm{Sym}_+(\Delta^3)$ על הצביעות של הקודקודים ונחשב את כמות המסלולים השונים בה.

פתרון. נובע *ממשפט לגרנז'*. סיבובים ללא היפוך יכולים להיות מורכבים רק מסיבוב סביב אחת הפאות, ולכן רק ממחזורים מהצורה $(i\ j\ k)$. יש כמובן 8 סיבובים אפשריים כאלה (סביב כל פאה יש שניים). לכן יש בחבורה $\mathrm{Sym}_+(\delta^3)$ לפחות 9 איברים יחד עם הנייטרלי, וממשפט לגרנז' נובע כי $\mathrm{Sym}_+(\delta^3)\Big|24$ ולכן $\mathrm{Sym}_+(\delta^3) \in \{12, 24\}$.
אבל אנו יודעים כי $|\mathrm{Sym}(\delta^3)| < |\mathrm{Sym}_+(\delta^3)|$ שכן ישנן העתקות שהופכות את הצורה, ולכן נקבל $12 = |\mathrm{Sym}_+(\delta^3)|$.
נחפש אם כן את שלוש התמורות החסרות. נשים לב כי תמורות מהצורה $(i\ j)(l\ l)$ מוכלות גם הן ב־$\mathrm{Sym}_+(\delta^3)$ שכן הן הופכות את סימן הדטרמיננטה פעמיים. לכן נוכל לבחור את התמורה בין שלושה זוגות כפולים של קודקודים ונקבל את שלוש התמורות החסרות. $\square$

מסקנה: מספר המסלולים בסימטריות סיבוביות

נשתמש בלמה של ברנסייד ונקבל כי מספר המסלולים של $\mathrm{Sym}_+(\delta^3)$ על $[m]^X$ היא

$$|\mathrm{Sym}_+(\Delta^3)\backslash[m]^X| = \frac{1}{|\mathrm{Sym}_+(\Delta^3)|}\sum_{T\in\mathrm{Sym}_+(\Delta^3)}|Fix(T)| = \frac{1m^4+11m^2}{12}$$

הערה: צביעה של פאות

נשים לב כי ישנן ארבע פאות ולכן נוכל לקשר כל פאה לקודקוד ונקבל כי מספר הצביעות של פאות שקול למספר הצביעות של הקודקודים.

10 שיעור 7 — 29.5.2024

10.1 חבורות p

תזכורת: מרכז של חבורה

המרכז של חבורה $Z(G)$ הוא תת־חבורה נורמלית של איברים שמתחלפים עם כלל האיברים בחבורה המקורית.

$$Z(G) = \{g \in G \mid \forall h \in, gh = hg\}$$

הגדרה: חבורת p

תהי חבורה סופית G, אז נקרא ל־G חבורת p אם קיים p ראשוני ו־$n \in \mathbb{N}$ כך שמתקיים $|G| = p^n$.

טענה: מרכז של חבורת p

אם G חבורת p ו־$|G| \neq 1$ (G לא טריוויאלית) אז $|Z(G)| > 1$.

הוכחה. למעשה נוכיח ש־$p \Big| |Z(G)|$ ולכן $|Z(G)| \geq p$.
נשתמש בנוסחת המחלקות

$$|G| = |Z(G)| + \sum_{[h] \in cong(G), n \notin Z(G)} \frac{|G|}{|C_G(h)|}$$

ידוע כבר כי $|G|$ מתחלק ב־p ומספיק לבדוק את הסכום ולקבל את החלוקה.
כמובן ש־$|G|$ מחולק על־ידי p, ולכן גם חלוקתו בגודל מרכז מחולק ב־p או ב־1.
אם $|G| = |C(h)|$ אז $C(h) = G$ ולכן $h \in Z(G)$. ולכן נניח ש־$|G| < |C(h)|$ בלי להגביל את כלליות ההוכחה ונקבל כי $p \Big| \frac{|G|}{|C(h)}$ וקיבלנו כי הסכום מחולק על־ידי p. $\square$

דוגמה

עבור S_3, נקבל $|S_3| = 6$, והמרכז כולל רק את האיבר הטריוויאלי ולכן $|Z(S_n) = 1|$, מחלקות הצמידות בתמורות הן תמורות שקולות מחזור ולכן ישנן שלוש מחלקות צמידות, מתוכן שתיים לא במרכז. אז נקבל

$$6 = 1 + \frac{6}{3} + \frac{6}{2}$$

10.2 הומומורפיזמים

תזכורת: הומומורפיזם

תהינה G, H חבורות אז הומומורפיזם $\varphi : G \to H$ היא העתקה שמקיימת

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$$

ומכאן נובע גם $\varphi(e_G) = e_H$ וגם $\varphi(g^{-1}) = \varphi^{-1}(g)$.

הגדרות נוספות

אם φ חד־חד ערכית אז נאמר שהיא **מונומורפיזם**.
אם היא על היא תיקרא **אפימורפיזם**.
אם היא חד־חד ערכית ועל אז היא תיקרא **איזומורפיזם**.

הגדרה: גרעין

יהי φ הומומורפיזם $\varphi : G \to H$. **הגרעין** של φ ושמסומן $\ker(\varphi)$ מוגדר להיות

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = e_H\}$$

כלל האיברים שההעתקה שולחת לאיבר הנייטרלי.

הגדרה: תמונה

יהי $\varphi : G \to H$ המומורפיזם, **התמונה** של φ המסומנת $\mathrm{Im}(\varphi)$ מוגדרת על־ידי

$$\mathrm{Im}(\varphi) = \{h \in H \mid \exists y \in G : \varphi(y) = h\}$$

בדומה לתמונה של פונקציות.

טענה: גרעין ותמונה הם תת־חבורות

1. $\mathrm{Im}(\varphi)$ תת־חבורה של H.
2. $\ker(\varphi)$ תת־חבורה של G.

הוכחה. נתחיל בטענה הראשונה, על־פי הגדרת תת־חבורה:

1. איבר נייטרלי: $e_h = \varphi(e_G) \implies e_H \in \mathrm{Im}(\varphi)$
2. סגירות לכפל: $h_1, h_2 \in \mathrm{Im}(\varphi) \implies \exists g_1, g_2 : \varphi(g_1) = h_1, \varphi(g_2) = h_2$
3. סגירות להופכי: $h \in \mathrm{Im}(G) \implies \exists g \in \varphi(G) = h \implies \varphi(g) = h^{-1} \implies h^{-1} \in \mathrm{Im}(\varphi)$

ונוכיח את הטענה השנייה באופן דומה:

1. איבר נייטרלי: $e_G \in \ker(\varphi)$ נובע מ־$\varphi(e_G) = e_H$
2. סגירות לכפל: $g_1, g_2 \in \ker(\varphi) \implies \varphi(g_1) = e_H, \varphi(g_2) = e_H \implies \varphi(g_1 g_2) = e_H e_H \implies g_1 g_2 \in \ker(\varphi)$.
3. סגירות להופכי: $g \in \ker(\varphi) \implies \varphi(g) = e_H \implies \varphi(g^{-1}) = \varphi^{-1}(g) = e_H$

□

טענה: תנאי מספיק לאפימורפיזם ומונומורפיזם

1. $\mathrm{Im}(\varphi) = H$ אם φ על (אפימורפיזם).
2. $\ker(\varphi) = \{e\}$ אם ורק אם φ חד־חד ערכית (מונומורפיזם).

הוכחה. טענה 1 היא טריוויאלית ונובעת מההגדרה, נוכיח את הטענה השנייה.

אם φ חד־חד ערכית אז הטענה ברורה.

נניח כעת כי $\ker(\varphi)$ הוא טריוויאלי ונוכיח כי φ חד־חד ערכית.

נניח בשלילה כי $\exists g_1, g_2 \in G : g_1 \neq g_2, \varphi(g_1) = \varphi(g_2)$.

נסתכל על $g_2 g_1^{-1} \neq e_G$ אבל $\varphi(g_2 g_1^{-1}) = \varphi(g_2)\varphi(g_1^{-1}) = \varphi(g_2)\varphi^{-1}(g_1) = e_H$. □

דוגמות

דטרמיננטה נשים לב כי הדטרמיננטה המוגדרת על־ידי $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ היא הומומורפיזם, שכן $|AB| = |A| \cdot |B|$.

נראה גם כי $\mathrm{Im}(|\cdot|) = \mathbb{R}^\times$ וגם $\ker(|\cdot|) = SL_n(\mathbb{R})$.

מטריצה שקולה למרוכבים יהי הומומורפיזם $\varphi : C^\times \to GL_2(\mathbb{R})$ המוגדר על־ידי

$$a+bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

נוכיח כי זהו הומומורפיזם:

$$\varphi(a+ib)\varphi(c+id) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -ad+bc & ac-bd \end{pmatrix} = \varphi(ac-bd+i(ad+bc)) = \varphi((a+ib)(c+id))$$

זוהי למעשה העתקה איזומורפית למרוכבים המשמרת כפל מרוכבים.

העתקות לינאריות כל העתקה לינארית $T : \mathbb{R}^d \to \mathbb{R}^m$ היא לינארית ולכן הומומורפיזם.

בלוקי ז'ורדן ההעתקה $\varphi : \mathbb{R} \to GL_2(\mathbb{R})$ המוגדרת על־ידי

$$a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

היא הומומורפיזם, נוכיח:

$$\varphi(a)\varphi(b) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix} = \varphi(a+b)$$

נשים לב כי העתקה זו מגדירה עבור כל מספר את בלוק הז'ורדן המתאים אליו, דהינו בלוק ז'ורדן משמר את תכונתו בכפל.

מטריצה בתמורה נגדיר את ההעתקה $\varphi : S_n \to GL_n(\mathbb{R})$ על־ידי

$$\tau \mapsto P_\tau, \qquad (P_\tau)_{ij} = \delta_{i\ \tau(j)}$$

כאשר δ_{ij} מוגדרת על־ידי

$$(\delta_{ij}) = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

זוהי למעשה פונקציה המקשרת תמורה למטריצה הפיכה, על־ידי שינוי סדר השורות להיות על־פי התמורה. נוכיח כי זהו הומומורפיזם:

$$\varphi(\tau)\varphi(\sigma) = P_\tau P_\sigma = \sum_{k=1}^{n} (P_\tau)_{ik}(P_\sigma)_{kj} = \delta_{i\ \tau(\sigma(j))}$$

ולכן $P_\tau P_\sigma = P_{\tau\circ\sigma}$ וקיבלנו כי ההעתקה היא הומומורפיזם.

נוכל לראות כי זהו גם איזומורפיזם, דהינו יש יצוג יחיד לכל תמורה כמטריצה בצורה הנתונה, והפוך.

צמצום להומומורפיזם אם $\varphi : G \to H$ הומומורפיזם, אז עבור $\operatorname{Im}(\varphi) \subseteq H' \subseteq H$ היא תת־חבורה ומתקיים

$$\varphi' : G \to H', \qquad \varphi'(g) = \varphi(g)$$

שרשור הומומורפיזמים אם $\varphi : G \to H$ וגם $\phi : H \to K$ שני הומומורפיזמים, אז גם $\phi \circ \varphi : G \to K$ הומומורפיזם.

נוכיח:

$$\phi\circ\varphi(g_1g_2) = \phi(\varphi(g_1g_2)) = \phi(\varphi(g_1)\varphi(g_2)) = (\phi\circ\varphi)(g_1)(\phi\circ\varphi)(g_2)$$

סימן של תמורה נבחן את שרשור ההומומורפיזמים:

$$S_n \xrightarrow{P} GL_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^\times$$

תמונת השרשור היא $\{-1, 1\}$ בלבד, נשתמש בהומומורפיזם זה כדי להגדיר סימן לתמורות.

לתמורות עם סימן חיובי נקרא תמורות זוגיות ולשליליות נקרא אי־זוגיות.

נגדיר את ההעתקה:

$$sign : S_n \to \{1, -1\} \cong \mathbb{R}_{/2}$$

ואף נגדיר את תת־חבורת התמורות החיוביות

$$A_n := \ker(sign)$$

אוסף התמורות הזוגיות.

כך לדוגמה $|A_3| = 3 = |\{e, (1\ 2\ 3), (3\ 2\ 1)\}|$.

פעולה על חבורה תהי קבוצה X ותהי פעולה $G \circlearrowright X$. הפעולה ניתנת להגדרה על־ידי ההעתקה $\varphi : G \to \text{Sym}(X)$, שכן $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$. לכן פעולות על קבוצות שקולות להומומורפיזמים מחבורות לסימטריות של X. נוכיח:

הוכחה. נגדיר

$$\varphi(g) \in \text{Sym}(X), \qquad \varphi(g) = fx$$

נבחן את $\varphi(g_1 g_2)$ על־ידי הצבה:

$$\varphi(g_1 g_2)(x) = (g_1 g_2)(x) = g_2(g_1(x)) = \varphi(g)(g_2(x)) = \varphi(g_1)(\varphi(g_2)(x)) = (\varphi(g_1) \circ \varphi(g_2))(x)$$

□

זאת למעשה טענה חזקה במיוחד, שכן היא קושרת כל פעולה על חבורה להומומורפיזם בין חבורה לסימטריות של קבוצה ומאפשרת לנו להסיק עוד מסקנות על הפעולה.

העתקת שיכון יהי חבורה ותת־חבורה שלה $H \leq G$.
אז אפשר לבנות את העתקת השיכון ונקבל $\varphi(h \in H) = h \in G$ ונקבל $\text{Im}(\varphi) = H$, דהינו כל תת־חבורה יכולה להוות תמונה להומומורפיזם כלשהו.

טענה: צמוד לגרעין

יהי $\varphi : G \to H$ הומומורפיזם.
לכל $g \in G$ מתקיים

$$g \ker(\varphi) g^{-1} = \ker(\varphi)$$

הוכחה. יהי $h \in \ker(\varphi)$ ו־$g \in G$ אז

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g) e_H \varphi^{-1}(g) = e_H$$

וקיבלנו כי השוויון מתקיים. □

הגדרה: תת־חבורה נורמלית

$N \leq G$ תת־חבורה של חבורה G נקראת **נורמלית** אם לכל $g \in G$ מתקיים $gNg^{-1} = N$.

נסמן $N \trianglelefteq G$.

נבחין כי מההגדרה נובע כי כל איבר ב־N הוא חילופי לשאר איברי G.

נשים לב כי מצאנו שלכל $\varphi : G \to H$ הומומורפיזם נובע מיידית ש־$\ker(\varphi) \trianglelefteq G$.

משפט: משפט האיזומורפיזם הראשון

יהי $\varphi : G \to H$ הומומורפיזם, אז $G/\ker\varphi \xrightarrow{\sim} \text{Im}(\varphi)$.

דהינו התמונה של הומומורפיזם והמחלקות השמאליות של הגרעין הן איזומורפיות.

הוכחה. נסמן $N = \ker(\varphi)$ אז

$$gN \mapsto \varphi(g)\varphi(N) = \varphi(g) \in \text{Im}(g)$$

נוכל לבחור נציג לכל מחלקה שכן:

$$\forall g_1, g_2 \in G : g_1N = g_2N \iff g_1g_2^{-1} \in N \iff \varphi(gg_2^{-1}) = e_h \iff \varphi(g_1) = \varphi(g_2)$$

ומצאנו כי זהו הומומורפיזם. קל לראות כי הוא אף הפיך, ולכן גם איזומורפיזם. $\square$

11 שיעור 8 — 3.6.2024

11.1 הומומורפיזמים

טענה: תנאי התמונה לאיזומורפיזם

העתקה $f : G \to H$ היא חד־חד ערכית אם ורק אם $G \xrightarrow{\sim} \mathrm{Im}(f)$.

עוד דוגמות להומומורפיזמים

$D_n \hookrightarrow S_n$ על־פי הגדרה.
גם $P \cdot S_n \hookrightarrow GL_n(\mathbb{F})$ מטריצות הפרמוטציה היא שיכון ואף אחד מאוד חשוב.
ראינו כי $P : S_n \hookrightarrow GL_n(\mathbb{F}) \xrightarrow{\det} \mathbb{R}^\times$ שמייצג סימן עבור תמורות.
ראינו גם את $GL_2(\mathbb{R}) \hookleftarrow \mathbb{C}^\times$ על־ידי $a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

תזכורת: הומומורפיזם ופעולה

הומומורפיזם $G \xrightarrow{f} \mathrm{Sym}(X)$ היא זהה לפעולה $G \circlearrowright X$ כך שמתקיים

$$\forall g \in G, \pi_g \in \mathrm{Sym}(X) : \pi_g(x) = g \cdot x, \pi_g \circ \pi_h = \pi_{gh}$$

ונסיק $f(g) = \pi_g$ הומומורפיזם.
עוד נבחין כי $\ker(f) = \{g \in G \mid \pi_g = Id_X\}$ ונסיק כי $gx = x \forall x \in X \iff g \in \ker(G)$ ולכן $\ker(f) = \bigcap_{x \in X} G_x$.

משפט קיילי

לכל חבורה G קיימת קבוצה X ושיכון $G \hookrightarrow \mathrm{Sym}(X)$.
אם $|G| = n$ אז יש שיכון $G \hookrightarrow S_n$.

הוכחה. G פועלת רגולרית (משמאל) על G. כלומר $\forall x \in G : G_x = \{e\}$ שכן $g = e \iff gx = x$.
בפרט אם $f : G \to \mathrm{Sym}(G)$ ההומומורפיזם המתאים אז $\ker(f) = \cap_{x \in G} G_x = \{e\}$ וקיבלנו כי f חד־חד ערכית. $\square$

דוגמות

נקבל כי $D_n \hookrightarrow S_{2n}$, עוד נקבל מהמשפט שאפשר ליצור את השיכון $S_n \hookrightarrow S_{n!}$. זה לא הכי עוזר לנו אבל זה כן אפשרי, אנו רואים כי המשפט מבטיח שיכון אבל הוא עלול להיות די חסר תועלת ומהיכרות עם החבורה נוכל לבנות שיכון מוצלח יותר.

הערה על סימון

העתקה חד־חד ערכית מסומנת $\hookrightarrow$, העתקה על מסומנת $\twoheadrightarrow$.

טענה: תנאי לתת־חבורה נורמלית

התנאים הבאים הם שקולים ואם אחד מהם מתקיים אז N תת־חבורה נורמלית.

1. $\forall g \in G : gNg^{-1} \subseteq N$.
2. $\forall g \in G : ggNg^{-1} = N$.
3. $\forall g \in G : gN = Ng$.

ההוכחה בתרגיל.

מסקנה

לא קיים הומומורפיזם $f : S_3 \to H$ כך שמתקיים $\ker(f) = \{Id, (1\ 2)\}$.

הוכחה. נבחין כי $\{Id, (1\ 2)\}$ היא לא תת־חבורה נורמלית של S_3 כי $(1\ 3)(1\ 2)(3\ 1) = (1)(2\ 3) = (1\ 3)(2\ 3)$. $\square$

דהינו לא כל תת־חבורה יכולה לשמש כגרעין, נשאל את עצמנו האם כל תת־חבורה נורמלית היא גרעין של הומומורפיזם כלשהו, על שאלה זו נענה עתה.

טענה: תמונת תת־חבורה נורמלית

כאשר $f : G \to H$ הומומורפיזם ו־$N = \ker(f)$ אז $f^{-1}(f(x)) = xN$, התמונה ההפוכה של תמונת x היא המחלקה xN.
יתרה מכך הפונקציה $G/N \to \mathrm{Im}(f)$ המוגדרת על־ידי $h \mapsto f^{-1}(h)$ היא חד־חד ערכית ועל.

הוכחה. תחילה נבחין כי מתקיים

$$f(x)^{-1}f(y) = x^{-1}y \in N \iff xN = yN$$

נראה כי ההעתקה היא על:

$$f^{-1}(f(x)) = xN$$

נראה כי ההעתקה היא גם חד־חד ערכית, עבור $f(x), f(y) \in \mathrm{Im}(f)$ מתקיים

$$f^{-1}(f(x)) = f^{-1}(f(y)) = yN \iff x^{-1}y \in N \iff f(x^{-1}y) = e$$

$\square$

11.2 חבורת המנה

תהינה $N \triangleleft G$ ונגדיר G/N מבנה של חבורה.

טענה: מכפלת מחלקות

N נורמלית אם ורק אם $\forall x, y \in G : (xN) \cdot (yN) = (xy)N$.

הוכחה. $(xN)(yN) = x(Ny)N \overset{\text{נורמליות}}{=} x(yN)N = (xy)(NN) = (xy)N$ $\square$

טענה: חבורת כפל מחלקות

G/N עם הכפל של מחלקות היא חבורה עם האיבר הנייטרלי eN.

הוכחה. נבדוק את התנאים לחבורה:

1. איבר נייטרלי: $\forall x \in N : (eN)(xN) = xN = (xN)(eN)$.
2. אסוציאטיביות: $((xN)(yN))(zN) = ((xy)z)N = (xyz)N = (xN)(yN)(zN)$.
3. סגירות להופכי: $(xN)(x^{-1}N) = (xx^{-1})N = eN$.

$\square$

טענה

תהי הפונקציה $\pi : G \to G/N$ המוגדרת על־ידי $x \mapsto xN$.
הפונקציה π היא הומומורפיזם כך שגם $\ker(\pi) = N$.

הוכחה. $\pi(x)\cdot\pi(y)=(xN)(yN)=(xy)N=\pi(xy)$.

עוד נבחין כי $x\in N \iff xN=\pi(x)=N$. □

דוגמות

1. עבור החבורה $\mathbb{Z}$. זוהי חבורה אבלית ולכן כל תת־חבורה שלה היא נורמלית ומתקיים $n\mathbb{Z}\triangleleft\mathbb{Z}$.
   בהתאם $\mathbb{Z}/n\cong\mathbb{Z}/n\mathbb{Z}=\{n\mathbb{Z},1+n\mathbb{Z},\dots,(n-1)+n\mathbb{Z}\}$.
   ונראה גם $(a+n\mathbb{Z})+(b+n\mathbb{Z})=((a+b)+n\mathbb{Z})=(a+b \mod n)+n\mathbb{Z}$.
2. ראינו בתרגול כי $GL_n(\mathbb{F})/SL_n(\mathbb{F})\cong\mathbb{F}^\times, A\cdot SL_n(\mathbb{F})\mapsto\det(A)$.
   ואנחנו רואים כי $\det:GL_n(\mathbb{F})\twoheadrightarrow\mathbb{F}^\times$ וגם כי $SL_n(\mathbb{F})=\ker(\det)$.

12 תרגול 5 — 4.6.2024

12.1 תת־חבורות נורמליות

דוגמה 12.1 תהי $H \subseteq GL_n(\mathbb{F})$ חבורת הייזנברג, המוגדרת על־ידי

$$H = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \middle| a, b, c \in \mathbb{F} \right\}$$

נבחין כי זו אכן חבורה שכן מטריצות מולשיות סגורות לפעולת הכפל ומכילות הופכי.

נגדיר גם

$$H = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| c \in \mathbb{F} \right\}$$

נבחין כי $Z \trianglelefteq H$ ואף מתקיים $H/Z \cong \mathbb{F}^2$.

למה 12.1 *תזכורת: אם $|G| = p$ אז G היא ציקלית.*

למה 12.2 *אם $|G| = p^2$ כאשר p ראשוני, אז G אבלית.*

הוכחה. ידוע כי $Z(G)$ לא טריוואלית, ולפי משפט לגרנז' מתקיים $|Z(G)| \,\Big|\, |G|$ אז נקבל כי $|Z(G)| \in \{p, p^2\}$.
נקבל כי $G/Z(G)$ היא מגודל 1 או מגודל p. לכן נקבל כי החלוקה הזו היא ציקלית ואז נובע כי היא אבלית. □

נבחין כי לא בהכרח כל G ציקלית היא מגודל p^2, לדוגמה $(\mathbb{Z}_{/p})^2$ היא לא ציקלית כלל שכן לא כל האיברים הם מסדר p ועל־כן אי־אפשר ליצור את החבורה מאיבר בודד. נשים לב לכן גם ש־$\mathbb{Z}_{/p^2} \ncong (\mathbb{Z}/p)^2$.

טענה 12.3 *יהי p ראשוני ו־G חבורה. אם $|G| = p^2$ אז G איזומורפית לאחת החבורות*

$$\mathbb{Z}_{/p^2}, \mathbb{Z}_{/p} \times \mathbb{Z}_{/p}$$

אם $|G| = p^3$ בהתאם היא איזומורפית לאחת החבורות

$$\mathbb{Z}_{/p^3}, \mathbb{Z}_{/p^2} \times \mathbb{Z}_{/p}, \mathbb{Z}_{/p} \times \mathbb{Z}_{/p} \times \mathbb{Z}_{/p}$$