מבנים אלגבריים 1 — סיכום

8 באוגוסט 2024

תוכן העניינים

1 שיעור 1 — 6.5.2024

1.1 מבוא לחבורות

הקורס עוסק בעיקרו בתורת החבורות, ממנה גם מתחילים.
חבורה (באנגלית Group) היא מבנה מתמטי.
ברעיון חבורה מייצגת סימטריה, אוסף השינויים שאפשר לעשות על אובייקט ללא שינוי שלו, קרי שהוא ישאר שקול לאובייקט במקור.
מה הן הסימטריות שיש לריבוע? אני יכול לסובב ולשקף אותו בלי לשנות את הצורה המתקבלת והיא תהיה שקולה. חשוב להגיד שהפעולות האלה שקולות שכן התוצאה הסופית זהה למקורית.
אפשר לסובב ספציפית אפס, תשעים מאה שמונים ומאתיים שבעים מעלות, נקרא לפעולות האלה A, B, C בהתאמה.
בנוסף אפשר לשקף סביב ציר האמצע, ציר האמצע מלמעלה, ועל האלכסונים, ניתן גם לאלה שמות, נקרא לפעולות אלה בהתאמה D, E, F, G, H.
אלה הפעולות הבסיסיות ואי אפשר לעשות פעולה שלא בקבוצה הזאת, אבל אפשר להרכיב את הפעולות האלה והתוצאה הסופית תהיה שקולה לפעולה מהקבוצה.
נגדיר את הפעולות:

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

נראה כי הרכבת פעולות שקולה לפעולה קיימת:

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

חשוב לשים לב שהפעולה הזאת לא חילופית: $X \circ Y \neq Y \circ X$.
היא כן קיבוצית: $X \circ (Y \circ Z) = (X \circ Y) \circ Z$.
תכונה נוספת היא קיום האיבר הנייטרלי, במקרה הזה A. איבר זה לא משפיע על הפעולה הסופית, והרכבה איתו מתבטלת ומשאירה רק את האיבר השני:

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

התכונה האחרונה היא קיום איבר נגדי:

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

הגדרה 1.1 (חבורה) חבורה היא קבוצה G עם $\circ : G \times G \to G$ ואיבר $e \in G$ כך שמתקיימות התכונות הבאות:

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

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

למה 1.2 (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.

1.2 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 1.3 (חבורה קומוטטיבית) חבורה G תיקרא קומוטטיבית או חילופית או אבלית (על שם המתמטיקאי אבל) אם $xy = yx$ לכל $x, y \in G$.
חשוב להבין, למה שסימטריות תהינה חילופיות.

דוגמה 1.1 (לחבורות קומוטטיביות) $(\mathbb{Z}, +, 0)$ חבורת החיבור מעל השלמים, היא חבורה קומוטטיבית.
באופן דומה גם $(\mathbb{Z}_n, +, 0)$.

דוגמה 1.2 (חבורות לא קומוטטיביות) נבחין במספר דוגמות לחבורות שאין בהן חילופיות.

- $(D_4, \circ, A)$ 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 חבורות ותתי־חבורות

דוגמה 2.1

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.

למה 2.1 (בסיסיות של חבורות)

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

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

הגדרה 2.2 (תת־חבורה) 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 $H \le G$.

דוגמה 2.2 $(2\mathbb{Z}, +, 0) \le (\mathbb{Z}, +, 0)$ 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.

טענה 2.3 (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*

דוגמה 2.3

$1 \in \mathbb{N}_0 \land -1 \notin \mathbb{N}_0$	$(\mathbb{N}_0, +, 0) \not\subseteq (\mathbb{Z}, +, 0)$
כלל התנאים מתקיימים	$\{0, 2, 4, 6, 8\} \subseteq (\mathbb{Z}_{10}, +_{10}, 0)$

טענה 2.4 (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. □

2.2 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 $X = [n] = \{1, \ldots, n\}$, וחבורת התמורות תהיה $(S_n, \circ, Id)$.

הגדרה 2.5 (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

דוגמה 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 2.6 מחזור פשוט $\sigma \in S_n$ יקרא l־**מחזור** אם קיימים $x_1, \ldots, x_l \in [n]$ כך שלכל $0 \le i < l$ מתקיים $\sigma(x_i) = x_{i+1}$ ו־$\sigma(x_l) = x_0$.

טענה 2.7 *כל תמורה היא הרכבה של מספר כלשהו של מחזורים, ההוכחה מסתמכת על היכולת לשרשר את ערכי המחזור משרשראות שאינן נוגעות אחת לשנייה.*

דוגמה 2.4 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 $\sigma(x_1) = \sigma(\tau^{-1}(\tau(x_1)))$ 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 $(\{\pm 1\}, \cdot)$ 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 3.1 (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 3.2 (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 3.3 (איזומורפיזם) איזומורפיזם G ל־H הוא הומומורפיזם חד־חד ערכי ועל ומסומן $\varphi : G \xrightarrow{\sim} H$.

למה 3.4 (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 3.5 (תנאי הכרחי לאיזומורפיזם) המומורפיזם $\varphi : G \to H$ הוא איזומורפיזם אם ורק אם קיים הומומורפיזם $\psi : H \to G$ כך שמתקיים $\varphi \circ \psi = \psi \circ \varphi = Id_G$.

הגדרה 3.6 (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 3.7 (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 3.8 (הרכבת איזומורפיזמים) הרכבה של איזומורפיזמים היא איזומורפיזם.

הגדרה 3.9 (אוטומורפיזם) אוטומורפיזם של G הוא איזומורפיזם $G \xrightarrow{\sim} G$. נסמן ב־$Aut(G)$ את קבוצת האוטומורפיזמים של G.

למה 3.10 (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 3.11 (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 $n \leq 1$ 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 3.12 (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 3.13 (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 3.14 (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. ☐

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

הגדרה 3.15 (תת־חבורה נוצרת) G חבורה ו־$S \subseteq G$, תת־קבוצה, התת־חבורה הנוצרת על־ידי S מוגדרת להיות:

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

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

4 שיעור 3 — 15.5.2024

4.1 תת־חבורות

הגדרה 4.1 (תת־חבורה נוצרת) תהי $S \subseteq G$ תת־קבוצה לחבורה, נגדיר

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

למה 4.2 (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 4.3 (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 4.4 (שלמות תת־חבורה יוצרת) אם $\langle S \rangle = G$ אומרים ש־$e - S$ יוצרת את G.

דוגמה 4.1 מתקיים $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. כקונספט כללי $\langle d \rangle = d\mathbb{Z}$.
מה לגבי $\mathbb{Z}/n$? מתקיים $\mathbb{Z}/n = \langle 1 \rangle$.

הגדרה 4.5 (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 4.6 *כל חבורה ציקלית G מקיימת $G \simeq \mathbb{Z}$ או $G \cong \mathbb{Z}/n$ הוכחה בתרגיל.*

דוגמה 4.2 $G = D_4$.
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 4.7 (תת־חבורות של 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 4.8 (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 $m\mid a,b$ 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 4.3 עבור $2\mathbb{Z}=\langle 2\rangle=\langle 6,10\rangle$

מסקנה 4.9 (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 4.10 (מחלקה ימנית ושמאלית) תהי G חבורה ו־$H\leq G$ ו־$x\in G$. נגדיר את המחלקה השמאלית של x על־ידי

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

ואת המחלקה הימנית של x בהתאם

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

תרגיל 4.1 הראו כי המחלקות הימניות והשמאליות הן איזומורפיות, והראו כי זה לא מתקיים עבור מונואידים.

למה 4.11 (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 4.12 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 $yH=ZH=xH$. □

טענה 4.13 (כיסוי זר) *התת־קבוצות מהצורה* xH *עבור* $x\in G$ *מהוות כיסוי זר של* G *עבור* $H\leq G$.

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

טענה 4.14 *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. □

הגדרה 4.15 (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 4.16 (משפט לאגרנז') *אם* G *חבורה סופית, אז לכל* $H\leq G$ *מתקיים* $|H|\Big||G|$.

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 4.17 $|G/H| = |G : H|$ **האינדקס** של H ב־G.

דוגמה 4.4 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 סדר

הגדרה 5.1 (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 5.2 (סדר)

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

הוכחה. נוכיח שאם $o(x)$ סופי אז

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

ואם $o(x) = \infty$ אז

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

הוכחה ל־(1).

(1) תת־חבורה:

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

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.

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

מסופיות קיימים $0 \leq k < m$ עבורם

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

ולכן ל־x יש סדר סופי, משובך היונים.

2 תרגיל. □

מסקנה 5.3 (משפט לגרנז' לחבורה סופית) G חבורה סופית, אז לכל $x \in G$ מתקיים

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

מסקנה 5.4 אם קיים $x \in G$ עבורו $o(x) = |G|$ אז G ציקלית.

טענה 5.5 (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 5.6 (פעולה) פעולה של חבורה G על קבוצה X זו פונקציה $\cdot : G\times X\to X$, $(g,x)\mapsto g\cdot x$ 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.

דוגמה 5.1 (לפעולות) מספר פעולות:

1. S_n פועלת על הקבוצה $X=\{1,2,\dots,n\}$ על־ידי
$$S_n\times\{1,\dots n\}\to\{1,\dots,n\}$$
כאשר $(\sigma,k)\mapsto\sigma(k)$.
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 ריגורוזי 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 5.7 (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 5.8 (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 5.9 (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 5.10 (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 $z = tz^2 = tz = e$. □

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

למה 6.2 (תכונות מחלקות שקילות) *תהי $H \leq G$ חבורה ותת־חבורה, אז הטענות הבאות מתקיימות:*

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

הגדרה 6.3 (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.

דוגמה 6.1 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 6.4 (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 6.5 (משפט לגרנז') *תהא G חבורה סופית ו־H תת־חבורה של G. אז*

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

ובפרט $|H|\Big||G|$.

מסקנה 6.6 תהא G סופית ו$g \in G$ אז $ord(g)\Big||G|$.

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

למה 6.7 $|H| = ord(g)$.

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 6.8 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 6.9 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 $1 < ord(g)$ אך מצד שני $|\langle g\rangle| = ord(g) \big| p$

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

סעיף ב' בתרגיל 2. ☐

משפט 6.10 (משפט פרמה הקטן) *יהיה p ראשוני, ו־$a \in \mathbb{Z}$, אם $\gcd(a,p) \equiv 1$ 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 $0 < r \le p-1$, וזה נכון כי הם זרים, דהינו $r \in \mathbb{Z}^{\times}_{/p}$.

נשים לב כי

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

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, $H = \{A \in M_n(\mathbb{F}) \mid$ 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 $\varphi(A) = A$. ☐

7 שיעור 5 — 22.5.2024

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

7.1 פעולות על קבוצות

סימון 7.1 בהינתן $X \circlearrowleft G$ 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 7.2 (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: $x\sim y, y\sim z \implies \exists g,h\in G, gx=y, hy=z \implies (hg)x=h(gx)=hy=z \implies x\sim z$

□

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 7.3 (מסלולים) בהינתן $X \circlearrowleft G$, 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 $G\backslash X$.

מסקנה 7.4 $X=\bigcup_{O\in G\backslash X} O$, דרך מזוצעת 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 7.5 (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 7.6 (טרנזיטיבית) פעולה $X \circlearrowleft G$ 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 7.7 $H\backslash G$ קבוצת המסלולים של $G \circlearrowleft H$ רגולרית משמאל שקולה ל־$H\backslash G$ קבוצת המחלקות הימניות של H ב־G.

באופן דומה G/H המסלולים של הפעולה $G \circlearrowleft H$ 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.

דוגמה 7.1 נבחין בכמה פעולות שונות והשובות:

1. $G \circlearrowleft G$ 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 $G \circlearrowleft H$, 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. $GL_2(\mathbb{R}) \circlearrowleft \mathbb{R}^2$ 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. $O_2(\mathbb{R}) \circlearrowright \mathbb{R}^2$, ידוע כי $O_2(\mathbb{R}) \le GL_2(\mathbb{R})$. הפעם כל וקטור צריך להגיע רק לוקטור 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. $S_n \circlearrowright \{1, \dots, n\}$ 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 7.8 (מקבע) תהינה $G \circlearrowright X$, 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 7.9 (מייצב) יהיו $G \circlearrowright X$, 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 7.10 (מייצב הוא תת־חבורה) *G_x תת־חבורה של G.*

הוכחה. נבדוק את הגדרת תת־החבורה:

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

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

הגדרה 7.11 (פעולה חופשית) $G \circlearrowright X$ 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.

הגדרה 7.12 נבחן את $G \circlearrowright G$ 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 7.13 (מרכז) ישנו המרכז של x ב־G והוא $C_G(x) = G_x = \{g \in G \mid gxg^{-1} = x\} \iff gx = xg$. באנגלית Centrilizer.
מרכז הוא סוג של מייצב במקרה שבו $X = G$.

משפט 7.14 (מסלול־מייצב) *$G \circlearrowright X$ ו־$x \in X$. $|O(x)| = [G : G_x]$. וזה נכון גם כשהחבורה לא סופית. $O(x) \xrightarrow{\sim} G/G_x$.*
בפרט אם G סופית אז $|O(x)| = \frac{|G|}{|G_x|}$ וונובע 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־$g'G_x = gG_x \overset{\text{סגירות להופכי}}{\Longrightarrow} (g')^{-1}g \in G_x \implies (g')^{-1}gx = x \implies g \cdot x = f(gG_x) = f(g'G_x) = g' \cdot x$. $\square$

דוגמה 7.2 תהינה חבורה G ותת־חבורתה $H \leq G$, יש פעולה "רגולרית" של G על G/H:

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

משפט 7.15 (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 $|O(x)| = 1, p \iff |O(x)| \Big| p$.

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 $X = \bigcup_{O \in \mathbb{Z}_{/p} \setminus X} O$, ובהתאם מהאיחוד הזר נקבל גם $|X| = \sum_{O \in \mathbb{Z}_{/p} \setminus X} |O|$.

אם $(e, \ldots, e)$ היה נקודת השבת היחידה אז $\sum_{O \in \mathbb{Z}_{/p} \setminus X} |O| \equiv 1 (\mod p)$, 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 $x^n = e$. $\square$

הערה ההוכחה מוויקיפדיה הרבה יותר ברורה.

8 שיעור 6 — 27.5.2024

8.1 מקבעים של פעולות

ניזכר בהגדרת המקבע, $X^g = \{x \in X \mid gx = x\}$, 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.

למה 8.1 (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

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

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 $x = O$, 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 $g \in G$, $x \in X$ 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. $\square$

דוגמה 8.1 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 8.2 (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 8.3 (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 $Z(G)\le G$. □

למה 8.4 (חיתוך מרכזים) *תהי G חבורה, נזכר 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 □

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

סימון 8.5 (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 8.6 (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

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

$\square$

9 תרגול 4 — 28.5.2024

9.1 צביעות

הגדרה 9.1 (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 9.2 (**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 $[m]^X \to [m]^X \times G :$. 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 9.3 (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 $v_0, \ldots, v_3$ 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 9.4 (**פעולת סימטריות על הקודקודים**) *הפעולה $\cdot : \mathrm{Sym}(\Delta^3) \times \{v_0, \ldots, v_3\} \to \{v_0, \ldots, v_3\}$ הנתונה על־ידי $T \cdot v_i = T(v_i)$ היא פעולה על הקבוצה $\{v_0, \ldots, v_3\}$.*

הוכחה. בתרגיל □

מסקנה 9.5 (איזומורפיות הסימטריות) הפונקציה $\varphi : \mathrm{Sym}(\Delta^3) \to S(\{v_0, \ldots, v_3\})$ 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 $S(\{v_0, \ldots, v_3\})$ ולכן היא מכילה קבוצה יוצרת, ומכאן נקבל $\varphi(\mathrm{Sym}(\Delta^3)) = S(\{v_0, \ldots, v_3\})$, מהטענות הקודמות נקבל גם חד־חד ערכיות. □

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

מסקנה 9.6 (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 9.7 (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 9.8 (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 9.9 (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 $|\mathrm{Sym}_+(\delta^3)| = 12$.
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. □

הגדרה 9.10 (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 10.1 (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 10.2 (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־$|C(h)|<|G|$ בלי להגביל את כלליות ההוכחה ונקבל כי $p\Big|\frac{|G|}{|C(h)}$ וקיבלנו כי הסכום מחולק על־ידי p. □

דוגמה 10.1 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

ניזכר בהגדרת ההומומורפיזם. תהינה G,H חבורות אז הומומורפיזם $\varphi:G\to H$ היא העתקה שמקיימת

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

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

הגדרה 10.3 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 10.4 (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 10.5 (תמונה) יהי $\varphi:G\to H$ המומורפיזם, **התמונה** של φ המסומנת $\operatorname{Im}(\varphi)$ מוגדרת על־ידי

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

בדומה לתמונה של פונקציות.

טענה 10.6 (גרעין ותמונה הם תת־חבורות) *אם $\varphi:G\to H$ הומורפיזם אז:*

1. *$\operatorname{Im}(\varphi)$ 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: $g \in \ker(\varphi) \implies \varphi(g) = e_H \implies \varphi(g^{-1}) = \varphi^{-1}(g) = e_H$

$\square$

טענה 10.7 (תנאי מספיק לאפימורפיזם ומונומורפיזם) *אם φ הומומורפיזם אז:*

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 טריויאלית 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 $\varphi(g_2 g_1^{-1}) = \varphi(g_2)\varphi(g_1^{-1}) = \varphi(g_2)\varphi^{-1}(g_1) = e_H$. $\square$

נראה עתה מספר דוגמות להומומורפיזמים:

דוגמה 10.2 (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 $\ker(|\cdot|) = SL_n(\mathbb{R})$.

דוגמה 10.3 (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.

דוגמה 10.4 (העתקות לינאריות) כל העתקה לינארית $T : \mathbb{R}^d \to \mathbb{R}^m$ היא לינארית ולכן הומומורפיזם.

דוגמה 10.5 (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.

דוגמה 10.6 (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.

דוגמה 10.7 (צמצום להומומורפיזם) אם $\varphi : G \to H$ הומומורפיזם, אז עבור $\mathrm{Im}(\varphi) \subseteq H' \subseteq H$ היא תת־חבורה ומתקיים

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

דוגמה 10.8 (שרשור הומומורפיזמים) אם $\varphi : G \to H$ וגם $\phi : H \to K$ שני הומומורפיזמים, אז גם $\phi \circ \varphi : G \to K$ הומומורפיזם.

נוכיח:

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

דוגמה 10.9 (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 $|A_3| = 3 = |\{e, (1\ 2\ 3), (3\ 2\ 1)\}|$.

דוגמה 10.10 (פעולה על חבורה) תהי קבוצה X ותהי פעולה $G \circlearrowright X$. הפעולה ניתנת להגדרה על־ידי ההעתקה $\varphi : G \to \mathrm{Sym}(X)$, 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

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

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.

דוגמה 10.11 (שיכון) יהי חבורה ותת־חבורה שלה $H \leq G$.

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

טענה 10.8 (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. $\square$

הגדרה 10.9 (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 10.10 (משפט האיזומורפיזם הראשון) *יהי $\varphi : G \to H$ הומומורפיזם, אז $G/\ker\varphi \xrightarrow{\sim} \operatorname{Im}(\varphi)$.*
דהינו התמונה של הומומורפיזם והמחלקות השמאליות של הגרעין הן איזומורפיות.

הוכחה. נסמן $N = \ker(\varphi)$ אז

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

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. $\square$

משפט 10.11 (משפט ההתאמה) *תהי G חבורה ו־$N \trianglelefteq G$ תת־חבורה נורמלית שלה.*
יש התאמה חד־חד ערכית ועל בין תת־חבורות של G/N לבין תת־חבורות של G המכילות את N.
דהינו קיימת פונקציה חד־חד ערכיתו על $\varphi : \{H \mid N \leq H \leq G\} \to \{K \mid K \leq G/N\}$.
ההתאמה נוצרת על־ידי $\pi : G \to G/N$ הומומורפיזם המתאים לפעולת חלוקה לאגפים.
התאמה זו שומרת על יחסי הכלה, נורמליות, אינדקסים.

11 שיעור 8 — 3.6.2024

11.1 הומומורפיזמים

טענה 11.1 (תנאי התמונה לאיזומורפיזם) *העתקה $f : G \to H$ היא חד־חד ערכית אם ורק אם $\mathrm{Im}(f) \xrightarrow{\sim} G$.*

דוגמה 11.1 (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 $\mathbb{C}^\times \hookrightarrow GL_2(\mathbb{R})$ על־ידי $a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

ניזכר כי מצאנו קשר בין פעולה לבין הומומורפיזם וננסחו כלמה.

למה 11.2 (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 11.3 *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. $\square$

דוגמה 11.2 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.

סימון 11.4 העתקה חד־חד ערכית מסומנת $\hookrightarrow$, העתקה על מסומנת $\twoheadrightarrow$.

טענה 11.5 (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 11.6 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 $(1\ 3)(1\ 2)(3\ 1) = (1)(2\ 3)$. $\square$

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 11.7 (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 11.8 (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 11.9 (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 11.10 *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 $x \in N \iff xN = \pi(x) = N$. $\square$

דוגמה 11.3 נבחין בחבורות המנה הבאות:

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 $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = ((a+b) + n\mathbb{Z}) \equiv (a + b \mod n) + n\mathbb{Z}$.
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

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

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. $\square$

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

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

13 שיעור 9 — 5.6.2024

13.1 משפטי האיזומורפיזם

בשיעור הקודם דיברנו על זה שאם יש לנו הומומורפיזם $f : G \to H$ אז $\ker(f) \trianglelefteq G$. מצד שני אם $N \trianglelefteq G$ אז קיים $\pi : G \to G/N$ העתקה מהחבורה למחלקות השמאליות של N על־ידי כפל תת־חבורות וזוהי חבורה. מה שאמרנו זה ששתי הטענות הן כמעט הופכיות אחת לשנייה. מצאנו כי $\ker(\pi) = N$. נבחין כי $N \subseteq G, N \in G/N$. בזמן שאי־אפשר לשחזר את הפונקציה המקורית, אנחנו כן יכולים להסיק על התמונה שלה על־פי הגרעין.

משפט 13.1 (משפט האיזומורפיזם הראשון) *תהינה G, H חבורות, ו־$f : G \to H$ הומומורפיזם אז נובע* $G/\ker(f) \xrightarrow{\sim} \operatorname{Im}(f)$.
אף קיים איזומורפיזם יחיד α כך ש־$\alpha \circ \pi = f$.

הוכחה. בנינו פונקציה חד־חד ערכית ועל $\alpha : G/\ker(f) \to \operatorname{Im}(f)$ על־ידי $\alpha(x\ker(f)) = f(x)$.
נראה ש־α הומומורפיזם.

$$\alpha(x\ker(f))\alpha(y\ker(f)) = f(x)f(y) = f(xy) = \alpha((xy)\ker(f))$$

נותר להוכיח את היחידות של α.
לכל $y \in G/\ker(f)$ קיים $x \in G$ כך ש־$y = x\ker(f)$ ולכן

$$\alpha(y) = \alpha(x\ker(f)) = \alpha(\pi(x)) = f(x)$$

וקיבלנו כי $f = \alpha \circ \pi$ וזהו אכן איזומורפיזם יחיד. □

מתברר שכל הומומורפיזם בעולם הם הרכבה של חלוקה למחלקות גרעין, הליכה לתמונה ואז הפעלת אוטומורפיזם כלשהו.

דוגמה 13.1 יהי $\mathbb{Z}_{/n} \xrightarrow{\bmod n} \mathbb{Z}$ וראינו כי $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ ונקבל $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}_{/n}$ ממשפט האיזומורפיזם הראשון.

דוגמה 13.2 יהי $\mathbb{R}^\times \xrightarrow{\det} GL_n(\mathbb{R})$ הומומורפיזם שהוא על. הגרעין הוא הדטרמיננטות עם גודל 1, דהינו $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$. לכן גם $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^\times$.

דוגמה 13.3 $GL_n(\mathbb{R})$, ונראה את המרכז $Z(GL_n(\mathbb{R})) = \{aI_n \mid a \in \mathbb{R}^\times\}$, המטריצות הסקלריות.
נחלק עתה את חבורה במרכזה ונקבל

$$GL_n(\mathbb{R})/Z(GL_n(\mathbb{R})) := PGL_n(\mathbb{R})$$

דוגמה 13.4 אם יש שתי חבורות G, H, נבחן את $G \xleftarrow{\pi_G} G \times H \xrightarrow{\pi_H} H$, כאשר $\pi_G(gh) = g$ ו־$\pi_H(gh) = h$.
$\ker(\pi_G) = \{(e, h) \mid h \in H\} = \{e\} \times H$ ובאופן דומה $\ker(\pi_H) = G \times \{e\}$.
ממשפט האיזומורפיזם הראשון אנו מקבלים כי $(G \times H)/(G \times \{e\}) \cong H$, גם אינטואיטיבית זה מאוד הגיוני שכן אנו מקבצים לפי איברי G.

הערה אם G סופית ו־$N \trianglelefteq G$ אז $|G| = |N| \cdot |G/N|$ כנביעה ממשפט לגרנז'.

בהינתן שתי חבורות G, H, אז נוכלי לבנות חבורה E כך ש־$G \trianglelefteq E$ כך ש־$E/G \xrightarrow{\sim} H$. כך לדוגמה אם נבחן את $H = G = \mathbb{Z}_{/2}$ אז נוכל להגדיר $E = \mathbb{Z}_{/2} \times \mathbb{Z}_{/2}$ או גם $E = \mathbb{Z}_{/4}$, ולכן נקבל $\mathbb{Z}_{/2} \xrightarrow{\sim} \mathbb{Z}_{/2} \times \mathbb{Z}_{/2}$ אשר מקיימת את הטענה.

בהינתן חבורות G, H, K והומומורפיזמים $K \xrightarrow{\alpha} G, K \xrightarrow{\beta} H$ אז נוכל לבנות גם $K \xrightarrow{(\alpha,\beta)} G \times H$ על־ידי $(\alpha, \beta)(x) = (\alpha(x), \beta(x))$.
הגרעין מקיים במקרה זה $\ker(\alpha, \beta) = \ker(\alpha) \cap \ker(\beta)$.

בהינתן $\mathbb{Z}_{/a} \xleftarrow{\pi_a} \mathbb{Z} \xrightarrow{\pi_b} \mathbb{Z}_{/b}$ נוכל להגדיר $\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_{/a} \times \mathbb{Z}_{/b}$ ונקבל $\ker(\pi) = a\mathbb{Z} \cap b\mathbb{Z} = lcm(a, b)\mathbb{Z}$.

מסקנה 13.2 $\mathbb{Z}_{/lcm(a,b)} \cong \operatorname{Im}(\pi) \leq \mathbb{Z}_{/a} \times \mathbb{Z}_{/b}$ ואם $\gcd(a, b) = 1$ אז $lcm(a, b) = ab$ ונקבל את משפט השאריות הסיני:

$$\mathbb{Z}_{/ab} \xrightarrow{\sim} \mathbb{Z}_{/a} \times \mathbb{Z}_{/b}$$

נבחן עתה על $G, G/N$ בלבד, ומה המבנה שלה. נגדיר כי $G \xrightarrow{\pi} G/N$. אם $K \leq G$ אז בהתאם $\pi(K) \leq G/N$ כנביעה ישירה מהעובדה ש־π הומומורפיזם.

אם $L \leq G/N$ אז $\pi^{-1}(L) \geq N$, שכן כל איבר בחבורת המנה מתרגם למספר איברים (למעשה מחלקות שקילות שלמות) בחבורה המקורית, וכל תת־חבורה מכילה איבר נייטרלי שמתרגם לחבורה N עצמה במקור. נסמן את התמונה על־ידי $\overline{\pi}(K) = \{\pi(x) \mid x \in K\}$ מטעמי נוחות.

משפט 13.3 *תהי G חבורה ו־$N \trianglelefteq G$ תת־חבורה נורמלית שלה, אז*

$$\{K \leq G \mid N \leq K\} \xrightarrow{\overline{\pi}} \{L \leq G/N\} \qquad \{L \leq G/N\} \xrightarrow{\pi^{-1}} \{K \leq G \mid N \leq K\}$$

הוכחה. **כיוון ראשון:** יהי $L \leq G/N$ ונקבל מהגדרת π כי

$$\overline{\pi}(\pi^{-1}(L)) \subseteq L$$

מצד שני נטען כי $L \subseteq \overline{\pi}(\pi^{-1}(L))$ שכן $y = \pi(x) \implies y \in L$ לאיזשהו $x \in \pi^{-1}(L)$. לכן $y = \pi(x) \in \overline{\pi}(\pi^{-1}(L))$.

כיוון שני: תהי $N \leq K \leq G$ ונחשב

$$K \overset{\text{לפי הגדרה}}{\subseteq} \pi^{-1}(\overline{\pi}(K)) \overset{(1)}{\subseteq} K$$

ונסביר את (1):

$$\overline{\pi}(K) = \{\pi(x) \mid x \in K\} = \{xN \mid x \in K\}$$

ולכן

$$\pi^{-1}(\overline{\pi}(K)) = \bigcup_{x \in K} \pi^{-1}(xN) = \bigcup_{x \in K} xN \subseteq K$$

$\square$

הערה שתי הפונקציות $\overline{\pi}, \pi^{-1}$ משמרות הכלה.

סימון 13.4 אם $N \subseteq K \leq G$ אז נסמן $\overline{\pi}(K) = K/N$.

משפט 13.5 (משפט האיזומורפיזם השלישי) *תהי $N \trianglelefteq G$ אז לכל $N \trianglelefteq K \leq G$ מתקיים*

$$K \trianglelefteq G \iff K/N \trianglelefteq G/N$$

ובמקרה זה

$$G/K \cong (G/N)/(K/N)$$

הוכחה. נניח $K/N \trianglelefteq G/N$ ונסתכל על ההומומורפיזם

$$G \overset{\pi}{\twoheadrightarrow} G/N \overset{\varphi}{\twoheadrightarrow} (G/N)/(K/N)$$

אז

$$\ker(\varphi \circ \pi) = \pi^{-1}(\ker(\varphi)) = \pi^{-1}(K/N) = K$$

ממשפט האיזומורפיזם הראשון נקבל $G/K \xrightarrow{\sim} (G/N)/(K/N)$.
שכן קיבלנו כי $G/\ker(\varphi \circ \pi) \xrightarrow{\sim} \operatorname{Im}(\varphi \circ \pi)$.

כיוון שני: נניח כי $N \trianglelefteq K \trianglelefteq G$ ונסתכל על הפונקציה

$$\alpha : G/N \to G/K, \qquad xN \mapsto (xN)K = x(NK) = xK$$

ונראה ש־α הומומורפיזם.

פונקציה זו היא בבירור הומומורפיזם שכן מדובר על כפל חבורות. נבחין כי

$$\ker(\alpha) = \{xN \mid xK = K\} = \{xN \mid x \in K\} = K/N$$

ונוכל להסיק ממשפט האיזומורפיזם הראשון כי

$$(G/N)/(K/N) \xrightarrow{\sim} G/K$$

$\square$

דוגמה 13.5 נגדיר את ההומומורפיזם $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. אנו יודעים כי $n\mathbb{Z} \leq d\mathbb{Z} \leq \mathbb{Z}$ לכל $d \mid n$, ולכן נוכל להשתמש במשפט האיזומורפיזם השלישי ונקבל

$$(\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}_{/d}$$

ולמעשה הצלחנו לפשט משמעותית את חבורת המנה הזו.

14 שיעור 10 — 10.5.2024

14.1 מכפלות

הגדרה 14.1 (מכפלה ישרה) יהיו X,Y חבורות, נגדיר על $X\times Y$ מבנה של חבורה על־ידי

$$(x_1,y_1)\cdot(x_2,y_2)=(x_1x_2,y_1y_2)$$

דוגמה 14.1 $\mathbb{Z}_{/n}\cong\mathbb{Z}_{/m}$ אם ורק אם $\gcd(m,n)=1$.

דוגמה 14.2 אם A חבורה אבלית ו־K,H תת־חבורות של A כך ש־$HK=A$ ו־$H\cap K=\{e\}$ אז $A\cong H\times K$ כפי שמצאנו בהרצאות הקודמות.

משפט 14.2 *תהי G חבורה ו־$X,Y\leq G$ אז $\varphi(x,y)=xy$ הוא איזומורפיזם אם ורק אם מתקיימים התנאים הבאים:*

1. $G=XY$
2. $X\cap Y=\{e\}$
3. $X,Y\trianglelefteq G$

הוכחה. נראה כי 1 שקול להיות φ על:
אם φ על, אז $\mathrm{Im}(\varphi)=X\cdot Y=G$.
אם $XY=G$ אז נקבל $\mathrm{Im}(\varphi)=XY=G$.

נניח כי φ חד־חד ערכית. נניח ש־$g\in X\cap Y$ אז $g=e \implies \varphi(g,e)=ge=eg=\varphi(e,g)$.
מצד שני נניח כי $X\cap Y=\{e\}$, ונניח כי $x_1y_1=x_2y_2$ ונקבל $x_2^{-1}x_1=y_2y_1^{-1}$ ונקבל כי $x_1=x_2 \implies x_2^{-1}x_1=e$ ונקבל באופן דומה כי גם $y_1=y_2$.

נניח ש־φ היא איזומורפיזם. אנחנו רוצים להראות כי $\forall g\in G, gXg^{-1}=X, gYg^{-1}=Y$. בפרט φ היא הומומורפיזם, לכן $\varphi(x_1,y_1)\cdot\varphi(x_2,y_2)=\varphi(x_1y_1,x_2y_2)$ ולכן נקבל $x_1y_1x_2y_2=x_1x_2y_1y_2$, נובע כי $y_1x_2=x_2y_1$ ובהתאם $\forall x\in X,y\in Y: xy=yx$.
יהיה $g\in G$ וידוע כי ההעתקה על ולכן קיימים x,y כך ש־$g=xy$ ולכן אנחנו יודעים ש־$gXg^{-1}=xyXy^{-1}x^{-1}$ ומההילופיות נקבל $xXyy^{-1}x^{-1}=xXx^{-1}=X$, נעשה תהליך דומה ל־$Y$.

נניח ששלושת התנאים מתקיימים, וצריך להראות כי $\forall x\in X,y\in Y: xy=yx \iff y_1x_2=x_2y_1 \iff x_1y_1x_2y_2x_1y_1x_2y_2$.
אנחנו צריכים להראות כי $x^{-1}(y_{-1}xy)=e \iff xy=yx$ ולכן $x^{-1}\in X, y^{-1}xy\in Y$ ולכן $x^{-1}y^{-1}xy\in X,Y$ ולכן נובע $x^{-1}y^{-1}xy=e$. □

טענה 14.3 *D_4 היא לא איזומורפית למכפלה ישרה של תת־חבורות ממש שלה.*

הוכחה. נניח בשלילה ש־$X,Y\leq D_4$ כך ש־$\varphi: X\times Y\to D_4$ המוגדרת על־ידי $\varphi(x,y)=xy$ היא איזומורפיזם.
ראינו כי תת־החבורה הנורמלית היחידה מגודל 2 של D_4 היא $\langle\sigma^2\rangle$ ולכן נניח כי $Y=\langle\sigma^2\rangle$.
בנוסף ב־X חייב להיות איבר מסדר ארבע, דהינו σ,σ^3 האיברים היחידים מסדר 4 ולכן $\sigma\in X$ ונקבל כי $X\cap Y\neq\{e\}$.
חייב להיות איבר מסדר ארבע ב־X, נוכיח שלא. נניח שלא ונקבל כי $(xy)^2\mapsto x^2y^2=e$, וקיבלנו כי לא יתכן שהסדר של x הוא שתיים בלבד.
קיבלנו גם כי $\tau\notin X,Y$ ולכן בהכרח φ לא על D_4. □

ברצוננו להגדיר מבנה של חבורה על מכפלה $X\cdot Y$ כאשר $X,Y\leq D_4$ כך ש־φ כן תהיה איזומורפיזם. נתבונן ב־$X=\langle\sigma\rangle, Y=\langle\tau\rangle$. נראה כי $XY=D_4$ וגם כי $X\cap Y=\{e\}$, לכן $\varphi: X\times Y\to D_4$ שהגדרנו על־ידי $\varphi(x,y)=xy$ היא חד־חד ערכית ועל.
ננסה להגדיר פעולה חדשה על תת־חבורות שתניב מבנה חבורה. נגדיר על $X\times Y$ מבנה של חבורה על־ידי

$$(x_1,y_1)\cdot(x_2,y_2)=(x_1(y_1x_2y_1^{-1}),y_1y_2)\in X\times Y$$

טענה 14.4 *המבנה שהגדרנו הוא אכן חבורה.*

הוכחה. אסוציאטיביות:

$$\begin{aligned}((x_1,y_1)\cdot(x_2,y_2))\cdot(x_3,y_3) &= (x_1y_1x_2y_1^{-1},y_1y_2)(x_3,y_3)\\ &= (x_1y_1x_2y_1^{-1}y_1y_2x^3y_2^{-1}y_1^{-1},y_1y_2y_3)\\ &= (x_1y_1x_2y_2x^3y_2^{-1}y_1^{-1},y_1y_2y_3)\\ &= (x_1,y_1)\cdot((x_2,y_2)\cdot(x_3,y_3))\end{aligned}$$

קיום איבר יחידה:

$$(x,y)\cdot(e,e)=(eyey^{-1},y)=(x,y)$$

ובאופן דומה גם

$$(e,e)\cdot(x,y)=(eexe^{-1},y)=(x,y)$$

קיום הופכי: נחפש ל־(x_1,y_1) איבר הופכי:

$$y_1y_2=e\implies y_2=y_1^{-1},\qquad x_1y_1x_2y_1^{-1}=e\implies x_2=y_1^{-1}x_1^{-1}y_1$$

מצאנו איבר כזה ולכן זוהי אכן חבורה. $\square$

$\varphi:X\times Y\to D_4$ המוגדרת על־ידי $\varphi(x,y)=xy$ היא איזומורפיזם לפי מה שמצאנו, φ חד־חד ערכית ונבדוק הומומורפיזם.

$$\varphi((x_1,y_1)\cdot(x_2,y_2))=\varphi(x_1y_1x_2y_1^{-1},y_1y_2)=x_1y_1x_2y_2=\varphi(x_1,y_1)\cdot\varphi(x_2,y_2)\qquad \varphi(x_1,y_1)\varphi(x_2,y_2)=x_1y_1x_2y_2,$$

הגדרה 14.5 (מכפלה פנימית חצי ישרה) תהי G חבורה ויהיו $H,K\le G$ כך ש־$H\trianglelefteq G$.
נגדיר את הפעולה הבינארית על $H\times K$ על־ידי

$$(h_1,k_1)\cdot(h_2,k_2)=(h_1k_1h_2k_1^{-1},k_1k_2)$$

פעולה זו נקראת המכפלה הפנימית החצי ישרה, ונסמן את החבורה שנוצרת על־ידה על־ידי $H\rtimes K$.

הערה סדר המכפלה חשוב, ולא בהכרח $H\rtimes K$ איזומורפי ל־$K\rtimes H$.

משפט 14.6 *תהי G חבורה ו־$H,K\le G$ כך ש־$H\trianglelefteq G$, $H\cdot K=G$ ו־$H\cap K=\{e\}$,*
אז $\varphi:H\rtimes K\to G$ המתקבלת על־ידי $\varphi(h,k)=h\cdot k$ היא איזומורפיזם.

הוכחה. נבדוק ונקבל

$$\varphi((h_1,k_1)\cdot(h_2,k_2))=\varphi(h_1k_1h_2k_1^{-1},k_1k_2)=h_1k_1h_2k_2=\varphi(h_1,k_1)\cdot\varphi(h_2,k_2)\qquad \varphi(h_1,k_1)\cdot\varphi(h_2,k_2)=h_1k_1h_2k_2,$$

וקיבלנו מההחד־חד ערכיות ועל כי זהו איזומורפיזם. $\square$

מסקנה 14.7 תהי D_n החבורה הדהידרלית מסדר n ונגדיר $\sigma=(1\ 2\ \dots\ n)$ ונגדיר $\tau(k)=n-k+1$ אז

$$D_n\overset{\varphi}{\cong}\langle\sigma\rangle\rtimes\langle\tau\rangle$$

דהינו, D_n איזומורפית לחבורה של זוגות סדורים של שתי תת־החבורות יחד עם פעולת הכפל הפנימי החצי ישר.

הגדרה 14.8 (מכפלה חצי ישרה חיצונית) יהיו H,K חבורות כלשהן. נניח כי $\theta:K\to Aut(H)$ וכי θ היא הומומורפיזם.
נגדיר על $H\times K$ פעולה בינארית על־ידי

$$(h_1,k_1)\cdot(h_2,k_2)=(h_1\cdot\theta(k_1)(h_2),k_1k_2)$$

פעולה זו על המכפלה $H\times K$ משרה מבנה של חבורה ונסמן חבורה זו על־ידי $H\rtimes_\theta K$, נקרא לה **המכפלה החצי ישרה החיצונית** כאשר K פועלת על H ביחס ל־θ.

משפט 14.9 *תהי G חבורה, אז G איזומורפית למכפלה חצי ישרה חיצונית רק אם קיימים H,K חבורות כך שקיימים הומומורפיזמים $\pi:G\to$ $K,s:K\to G$ כך ש־$\pi\circ s=id_H$.*

הוכחה. נניח כי $G=H\rtimes_\theta K$ אז נצטרך למצוא $\pi:G\to K,s:K\to G$ אז נגדיר

$$\pi(h,k)=k,s(k)=(e,k)$$

ונקבל מבדיקה ישירה כי אלו הם הומומורפיזמים, ואף $\pi(s(k)) = k$.

כעת נניח כי קיימת $\pi : G \to K$ ו־$s : K \to G$ כך ש־π, s הומומורפיזמים ואף כי $\pi \circ s = id_K$.

נגדיר $H = \ker \pi$ ונגדיר $s(K)hs^{-1}(k) = \theta(k)(h)$ ולכן נובע θ היא הומומורפיזם ל־$Aut(H)$ וגם s הומומורפיזם.

$$\varphi(h, k) = h \cdot s(k)$$

נוכיח כי φ חד־חד ערכית אם היא הומומורפיזם.

נניח ש־$\varphi(h, k) = e$ אז נקבל $h \cdot s(k) = e$ וגם $s(k) = h^{-1} \in H$ אבל אם $s(k) \in H = \ker(\pi)$ נקבל $k = \pi(s(k)) = e$. קיבלנו כי $k = e_K$ ולכן גם $h = e_G$.

על: אנו מחפשים ל־$g \in G$ איברים כך ש־$h \cdot s(k) = g$. נגדיר $k = \pi(g)$ וידוע לנו כי $\pi(g \cdot s^{-1}(k)) = \pi(g)\pi(s^{-1}(k)) = k\pi^{-1}(s(k)) =$ kk^{-1}. □

הערה יתר על־כן, $G \cong H \rtimes_\theta K$ כאשר $H = \ker \pi$.

דוגמה 14.3 נגדיר $\pi : S_n \to \mathbb{Z}_{/2}$ על־ידי $\sigma \mapsto sign(\sigma)$ ונגדיר $s : \mathbb{Z}_{/2} \to S_n$ על־ידי $s(n) = \tau^n$.

אז $\pi \circ s = id_K$ ולכן S_n תהיה מכפלה חצי ישרה חיצונית, ונקבל

$$S_n \cong \ker(sign) \rtimes \mathbb{Z}_{/2}$$

דוגמה 14.4 נתבונן ב־$FL_n(\mathbb{F})$ ו־$\pi : GL_n(\mathbb{F}) \to \mathbb{F}^\times$, $\tau(A) = \det(A)$, ולכן

$$\det(s(x)) = x, s(x) = \begin{pmatrix} x & 0 & \dots \\ 0 & 1 & 0 \\ \vdots & 0 & 1 \end{pmatrix} s(xy) = s(x)s(y)$$

15 שיעור 11 — 17.5.2024

15.1 משפטי האיזומורפיזם

הערה (תזכורת) דיברנו בשיעור הקודם על משפטי האיזומורפיזם. משפט האיזומורפיזם הראשון קובע כי הומומורפיזם $\varphi : G \to H$ גורס כי $G/\ker(f) \xrightarrow{\sim} \mathrm{Im}(f)$.

משפט האיזומורפיזם השלישי טוען כי אם $N \triangleleft K \triangleleft G$ אז מתקיים

$$(G/N)/(K/N) \cong G/K$$

אבל למעשה משפט זה מדבר בצורה כוללנית על היכולת שלנו לבחור תת־חבורות שמוכלות בגרעין ותת־חבורות המכילות את הגרעין, והמשפט קושר קשר בין תת־חבורות אלה. טענה זו נובעת ממשפט ההתאמה.

עתה נעסוק במשפט השני, אם יש לנו $N \triangleleft G \geq H$ אנו לא יכולים לדבר על H/N שכן הן לא קשורות בהכרה אחת לשנייה בשום דרך. אפשר להקטין את N ולדבר על $H/(N \cap H)$ וזה מן הסתם מוגדר, אבל אפשר לנסות להגדיל במקום את H עצמה, דהינו לבחון את HN ולבדוק אותה במקום, ונוכל לבחון כך את NH/N.

משפט 15.1 (משפט האיזומורפיזם השני) *אם $N \triangleleft G \geq H$ חבורה ותת־חבורות שלה, אז*

$$(HN)/N \cong H/(N \cap H)$$

בפרט $N \cap H \triangleleft H$ ו־$N \triangleleft HN \leq G$.

הוכחה. ברור ש־$N \cap H$ תת־חבורה של H. עבור נורמליות לכל $h \in H$ ו־$x \in N \cap H$ צריך להראות כי $hxh^{-1} \in N \cap H$. נראה כי $hxh^{-1} \in N$ כי $N \triangleleft G$ וגם $hhxx^{-1} \in H$ כי $x \in H$ ו־$H \leq G$.

נראה ש־$HN \leq G$. לכל $g_i \in HN$ נוכל להגדיר $h_i x_i = g_i$ עבור $h_i \in H, x_i \in N$, עבור $i = 1, 2$. מתקיים

$$g_1 \cdot g_2 = (h_1 x_1)(h_2 x_2) = (h_1 h_2)(h_2^{-1} x_1 h_2 x_2)$$

ונבחין כי $h_2^{-1} x_1 h_2 x_2 \in N$.

סגירות להופכי דומה בהוכחתה ומושארת כתרגיל.

נתבונן בהומומורפיזם $H \hookrightarrow G \xrightarrow{\pi} G/N$ ונקרא להרכבה זו f. נראה כי $\ker(f) = \ker(\pi) \cap H = N \cap H$. נבחן את התמונה גם ונקבל $\mathrm{Im}(f) = \{hN \mid h \in H\} \subseteq G/N$. נותר להראות ש־$\mathrm{Im}(f) = HN/N$. ההכלה $\mathrm{Im}(f) \subseteq HN/N$ ברורה. בכיוון השני לכל $hx = g \in HN$ עם $h \in H, x \in N$ מתקיים

$$gN = hxN = h(xN) = hN$$

ולכן שייך ל־$\mathrm{Im}(f)$.

לכן ממשפט האיזומורפיזם הראשון נקבל $H/\ker(f) \cong \mathrm{Im}(f)$ ולכן $H/(H \cap N) \cong HN/N$. □

הערה (תזכורת) ממשפט האיזומורפיזם השלישי מצאנו כי

$$3\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_{/2}$$

ואנו יודעים כי $6\mathbb{Z} \triangleleft \mathbb{Z}$ ולכן $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_{/6}$, ונקבל

$$3\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_{/2}$$

שכן $3\mathbb{Z} \xrightarrow{\cdot 3} \mathbb{Z}$. עוד נראה כי $6\mathbb{Z} \xrightarrow{\cdot 3} 2\mathbb{Z}$ והחבורות אלה איזומורפיות בהתאמה (מקור למקור).

דוגמה 15.1 ניקח את $\mathbb{Z}$ ואת $a\mathbb{Z}$ ו־$b\mathbb{Z}$ ונבחין כי $a\mathbb{Z} \cap b\mathbb{Z} = lcm(a,b)\mathbb{Z}$. נבחן גם את $a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b)\mathbb{Z}$ (הלמה של בוזו). משפט האיזומורפיזם השלישי גורר כי $\mathbb{Z}/\frac{lcm(a,b)}{b}\mathbb{Z} \cong b\mathbb{Z}/lcm(a,b)\mathbb{Z} \cong \gcd(a,b)\mathbb{Z}/a\mathbb{Z} \cong \mathbb{Z}/\frac{a}{\gcd(a,b)}\mathbb{Z}$.

לכן נקבל ממשפט האיזומורפיזם השני

$$\frac{a}{\gcd(a,b)} = \frac{lcm(a,b)}{b}$$

15.2 חבורת הסימטריות של קוביה

כשהגדרנו את D_4 לא הראינו למה היא שקולה לסימטריות של ריבוע, ולכן נוכל להגדיר ריבוע במרחב $C_2=\{(x,y)\in\mathbb{R}^2 \mid -1\leq xy\leq 1\}$ ואת ההזזות על־ידי העתקות אורתוגונליות $G_2=\{v\in C_2, g\in O(2)\mid gv\in C_2\}$. נבחין כי $G_2\leq O(2)$.

טענה 15.2 $G_2\cong D_4$.

הוכחה. לכל $g\in G_2$ מתקיים $gv\in\{v_1,v_2,v_3,v_4\}:=V$ הקודקודים של הריבוע במרחב. ידוע כי $V\subseteq C_2$ קבוצת וקטורים עם אורך מקסימלי ($\sqrt{2}$) ו־g משמרת אורכים.

בפרט G_2 פועלת על V, כלומר מקבלים הומומורפיזם $G_2\xrightarrow{\varphi}\mathrm{Sym}(V)\cong S_4$. $\square$

למה 15.3 φ *חד־חד ערכית.*

הוכחה. אם $\varphi(g)=Id$ אז בפרט $g(v_1)=v_1$ ו־$g(v_2)=v_2$. מכיוון ש־$\{v_1,v_2\}$ בסיס של $\mathbb{R}^2$ נובע ש־$g=Id$. $\square$

נבחין כי שיקוף בתשעים מעלות מעל המרחב שהגדרנו הוא

$$A=\begin{pmatrix}0&-1\\1&0\end{pmatrix}, B=\begin{pmatrix}-1&0\\0&1\end{pmatrix}\in G_2$$

ולכן $\sigma=(1\ 2\ 3\ 4)=\varphi(A)$ ו־$\tau=(1\ 2)(3\ 4)=\varphi(B)$.

מסקנה 15.4 $\mathrm{Im}(\varphi)\supseteq\langle\sigma,\tau\rangle=D_4$

נותר להראות $|G_2|\leq 8$.

כל $g\in G_2$ היא העתקה לינארית הפיכה ולכן לוקחת זוג וקטורים בלתי תלויים לינאית ב־V לזוג וקטורים בת"ל ב־V, לכן אם $g(v_1)=v_i$ אז נובע כי $g(v_2)\neq v_i,-v_i$ ולכן יש ארבע אפשרויות ל־v_i ולכל בחירה שלו יש שתי אפשרויות ל־$g(v_2)$, ונקבל כי יש שמונה אפשרויות שונות.

נעבור לבחון את $\mathbb{R}^3$, בניסיון לבסס פורמלית את הסימטריות של קוביה, נגדיר

$$C_3=\{(x,y,z)\in\mathbb{R}^3\mid -1\leq x,y,z\leq 1\}$$

ונגדיר גם

$$G_3:=\{g\in O(3)\mid \forall v\in C_3, gv\in C_3\}$$

משפט 15.5 $G_3\cong S_4\times\mathbb{Z}_{/2}$.

נגדיר $C_3\supseteq\{(1,1,1),(-1,1,1),(1,-1,1),(-1,-1,1),(1,1,-1),(-1,1,-1),(1,-1,-1),(-1,-1,-1)\}=V$ ונקבל כי $\|(x,y,z)\|=\sqrt{x^2+y^2+z^2}$ ונקבל מקסימום אורך אם ורק אם $x,y,z=\pm 1$, דהינו אם ורק אם $(x,y,z)\in V$.

מקבלים הומומורפיזם $G_3\xrightarrow{\varphi}S_8$ והוא חד־חד ערכי כי V פורשת את המישור.

מסקנה 15.6 G_3 חבורה סופית.

16 תרגול 6 — 18.6.2024

16.1 מענה על שאלות מתרגיל 4

טענה 16.1 *בחבורה S_n כל מחלקת צמידות מכילה תמורות מאותה חלוקה למחזורים, מבחינת גודל.*

הוכחה. בתרגיל. $\square$

נתחיל בשאלה 2, יש להראות כי הפעולה של החבורה $\mathrm{Sym}_+(\Delta^3)$ על הטטרההדרון משרה פעולה על צלעות הטטרההדרון.

ראינו כי $S_4 \cong \mathrm{Sym}(\Delta^3) \trianglelefteq \mathrm{Sym}_+(\Delta^3) \cong A_4$, כאשר $A_n = \ker(sign)$. נקבל כי גם $A_4 \trianglelefteq S_4$ (ידוע כבר). אם $g \in \mathrm{Sym}_+(\Delta^3)$ אז $g.\,(v_i, v_j) = (g.\,v_i, g.\,v_j)$. נבדוק את איבר היחידה ונראה כי $e.\,(v_i, v_j) = (e.\,v_i, e.\,v_j) = (v_i, v_j)$. נראה גם $h.\,(g.\,(v_i, v_j)) = h.\,(g.\,v_i, g.\,v_j) = (h \circ g.\,v_i, h \circ g.\,v_j)$. מצאנו כי זו פעולה המוגדרת היטב.

נעבור לסעיף ב', נאמר כי $X = [m]^E$ כאשר $m \in \mathbb{N}$ צביעה ב־m צבעים והתבקשנו לראות כי הפעולה מהסעיף הקודם משרה פעולה של $\mathrm{Sym}_+(\Delta^3)$ על X. נובע מטענה 2 בתרגול 4.

בסעיף ג' עלינו למצוא את מספר המסלולים שהפעולה משרה על הצביעות.

נשתמש בלמה של ברנסייד, הגורסת כי מספר המסלולים הוא ממוצע המייצבים, דהינו

$$|X/\,\mathrm{Sym}_+(\Delta^3)| = \frac{1}{|\,\mathrm{Sym}_+(\Delta^3)|} \sum_{g \in \mathrm{Sym}_+(\Delta^3)} |Fix(g)|$$

יהי $g \in \mathrm{Sym}_+(\Delta^3)$, נבחן את A_4 כדי לענות על השאלה. דהינו, ב־S_4 ישנן תמורות מהמבנה

$$\begin{aligned}
1\,1\,1\,1 &\implies \{e\} \\
1\,1\,2 &\implies \{(i\ j) \mid i, j \in [4]\} \\
1\,3 &\implies \{(i\ j\ k)\} \\
2\,2 &\implies \{(i\ j)(k\ l)\} \\
4 &\implies \{(i\ j\ k\ l)\}
\end{aligned}$$

כל שורה מגדירה מחלקת צמידות ב־S_4. נבחין כי $A_4 = \{e, (i\ j\ k), (i\ j)(k\ l)\}$. עבור מחזורים מגודל 3 נבחין כי הם מסובבים את הצלעות של בסיס בטטרההדרון ובהתאם $Fix(g) = m^2$. עבור שני מחזורים מגודל 2 נקבל כי $Fix(g) = m^4$ משיקולים גאומטריים.

נקבל אם כן כי

$$|X/\,\mathrm{Sym}_+(\Delta^3)| = \frac{1}{12}(m^6 + m^4 \cdot 3 + m^2 \cdot 8)$$

נעבור לשאלה 5, שהייתה על הקוונטרניונים.

$$Q = \{\pm 1, \pm i, \pm j, \pm k\}$$

המוגדרת על־ידי $ijk = -1, i^2 = j^2 = k^2 = -1$.

בסעיף ב' התבקשנו להראות כי $Q \ncong D_4$. נמנה ונראה כי $D_4 = \{\sigma, \sigma^2, \sigma^3, e, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$. נבחן את הסדרים.

i, j, k הם מסדר 4, וכך גם $-i, -j, -k$, לעומת זאת רק σ, σ^3 הם מסדר 4.

עתה נוכיח ונניח בשלילה שקיים $\varphi : Q \to D_4$, נבחין כי $\varphi(i) \ne \varphi(j) \ne \varphi(k)$ אך בגלל הסדר של איברים אלה נקבל כי הסדר של $\varphi(i)$ מסדר 4, אבל יש שני איברים בלבד שונים כאלה.

בהמשך השאלה עלינו למצוא את $Z(Q)$ ומצאנו כי הוא $Z(Q) = \{1, -1\}$, שכן אלו הם האיברים המתחלפים היחידים. לדוגמה i לא מתחלף עם j, נראה כי $-jij = -jk = -i$ ולכן $ij \ne ji$.

נמצא את מחלקות הצמידות, הן $\{1\}, \{-1\}, \{i, -i\}, \{j, -j\}, \{k, -k\}$.

16.2 חבורת התמורות

טענה 16.2 *תהי $\sigma \in S_n$ המוגדרת על־ידי הרכבה של מחזורים $\sigma = \tau_1 \circ \cdots \circ \tau_k$, כאשר ישנם m מחזורים מגודל זוגי, אז*

$$sgn(\sigma) = (-1)^m$$

הוכחה. נבחין כי $sgn : S_n \to \{1, -1\}$ היא הומומורפיזם, דהינו

$$sgn(\sigma) = sgn(\tau_1) \cdots sgn(\tau_k)$$

אנו יודעים כי $sgn((i\ j)) = -1$ כנביעה מההגדרה מבוססת דטרמיננטות, ונבחין כי $(i\ j\ k) = (i\ j)(j\ k)$ מבדיקה ישירה.
לכן נקבל כי $sgn((i\ j\ k)) = sgn((i\ j)) \cdot sgn((j\ k)) = (-1)(-1) = 1$.
נקבל גם $(i\ j\ k\ l) = (k\ j)(k\ i)(k\ l)$ ועבור מחזור מאורך m ניתן לרשום אותו על־ידי הרכבה של $m-1$ חילופים.
נקבל בהתאם כי מחזור מאורך זוגי יהיה בעל סימן שלילי, וכי מחזור מגודל אי־זוגי יהיה מסימן חיובי. $\square$

טענה 16.3 *אם G חבורה ו־$N \trianglelefteq G$ אז N היא איחוד של מחלקות צמידות של G.*

הוכחה. נובע מההגדרה של מחלקות צמידות ושל תת־חבורה נורמלית ישירות. ידוע כי $\forall g \in G, h \in N : ghg^{-1} \in N$. $\square$

דוגמה 16.1 נמצא את תתי־החבורות הנורמליות של הלא טריוויאליות של S_5, A_5, A_4.
החבורה הנורמלית היחידה של S_5 היא A_5.

הוכחה. עבור $sgn : S_n \to \{1, -1\}$, נבחין כי $\ker(sgn) = A_n$ ולכן $A_n \trianglelefteq S_n$.
נבחן את מחלקות הצמידות של S_5:

$$\begin{aligned}
&1\,1\,1\,1\,1 \implies Id \implies 1 \\
&1\,1\,1\,2 \implies (i\ j) \implies \binom{5}{2} = 10 \\
&1\,2\,2 \implies (i\ j)(k\ l) \implies \frac{1}{2}\binom{5}{2}\binom{3}{2} = 15 \\
&1\,1\,3 \implies (i\ j\ k) \implies 2\binom{5}{3} = 20 \\
&1\,4 \implies (i\ j\ k\ l) \implies 3!\binom{5}{4} = 30 \\
&2\,3 \implies (i\ j)(k\ l\ m) \implies 2\binom{5}{2} \\
&5 \implies (i\ j\ k\ l\ m) \implies 4! = 24
\end{aligned}$$

נחפש לפי משפט לגרנז' מחלקות שכמות איבריהן מחלקות את S_5, דהינו שמחלקות את 120, ונראה שאין אף קומבינציה שאיננה A_5 שמחלקת את 120. $\square$

הגדרה 16.4 (חבורה פשוטה) חבורה נקראת פשוטה אם אין לה תת־חבורות נורמליות לא טריוויאליות.

נקבל כי ל־A_5 אין תת־חבורה נורמלית לא טריוויאלית, דהינו היא פשוטה. עוד נבחין כי $N \trianglelefteq S_5 \not\Rightarrow N \trianglelefteq A_5$.
מחלקות הצמידות של A_5 הן מגודל $1, 15, 12, 20, 12$ בלבד.
מכאן נוכל להסיק כי הטענה נכונה.

17 שיעור 12 — 19.5.2024

17.1 קוביות

בשיעור הקודם התחלנו לבחון את הקודקדים של קוביה והסיבוב שלה על־פי $G_3 \leq (3)$, איברים אלה משמרים את מבנה הקבוצה של הקודקדים, היא C_3.

ראינו גם שהקודקדים הם הרחוקים ביותר ממרכז הקוביה, ומשום שהעתקות אורתוגונליות משמרות מרחק, הן גם מזיזות קודקודים לקודקודים בלבד.

משפט 17.1 $G_3 \cong S_4 \times \mathbb{Z}_{/2}$

משפט זה יוכח בשלבים במהלך ההרצאה.

נראה כי הקודקודים הם

$$V = \{(1,1,1), (-1,1,1), (1,-1,1), (-1,-1,1), (-1,-1,-1), (1,-1,-1), (-1,1,-1), (1,1,-1)\}$$

וידוע כי $\|(x,y,z)\| = \sqrt{x^2+y^2+z^2}$.

למה 17.2 *לכל* $g \in G_3$ *ו־*$v \in V$ *מתקיים* $gv \in V$.

ההוכחה זהה למקרה של G_2 ולא נחזור עליה.

מקבלים $\varphi : G_3 \to S_8$.

למה 17.3 φ *חד־חד ערכית ובפרט* $|G_3| < \infty$.

במקום לבחון פאות נבחן את מרכזי הפאות, מטעמי נוחות ופשטות. יש שש פאות ובהתאם שישה וקטורים המייצגים את הפאות. נגדיר

$$F = \{(1,0,0), (0,1,0), (0,0,1), (-1,0,0), (0,-1,0), (0,0,-1)\}$$

למה 17.4 G_3 *משמרת את* F.

הוכחה. נראה שלכל $g \in G_3$ מתקיים $ge_1 \in F$.

$v_1 = (1,1,1), v_2 = (1,-1,-1)$ אז נקבל $e_1 = \frac{v_1+v_2}{2}$ ולכן נקבל גם $ge_1 = \frac{gv_1+gv_2}{2}$.

ניזכר שמתקיים $\langle (x,y,z), (x',y',z') \rangle = xx'+yy'+zz'$ ולכן עבור וקטורים ב־V נקבל את כמות האגפים בהם הם זהים פחות כמות האגפים בהם הם שונים.

לכן $\langle gv_1, gv_2 \rangle = \langle v_1, v_2 \rangle = -1$ ולכן $ve_1 = \frac{gv_1+gv_2}{2} \in F$. □

מקבלים המומורפיזם $\varphi : G_3 \to S_6$.

למה 17.5 *הפעולה שקיבלנו* $G_3 \circlearrowright F$ *היא טרנזיטיבית.*

הוכחה. בתרגיל. □

ניזכר במשפט מסלול־מייצב

$$G \circlearrowright X, |Q_x| = \frac{|G|}{|G_x|}$$

אנו יודעים את גודל המסלול, ואנו רוצים למצוא את $|G|$, אז נמצא את גודל המייצב.

למה 17.6 $(G_3)_{e_1} = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix} \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_2 \right\}$

הוכחה. נגדיר את המטריצה החיצונית A ואת הפנימית B. נראה כי

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x \\ ay+bz \\ cy+dz \end{pmatrix}$$

אז $\left(A\begin{pmatrix}x\\y\\z\end{pmatrix}\in C_3\right) \implies \begin{pmatrix}x\\y\\z\end{pmatrix}$) $\iff A\in G_3$. מכיוון ש־ $A\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}x\\B\begin{pmatrix}y\\z\end{pmatrix}\end{pmatrix}$ זה שקול לכך ש־$B\in G_2$. ☐

מסקנה 17.7 $|G_3|=48$

הוכחה. ממשפט מסלול־מייצב לפעולה $F \circlearrowleft G_3$ ו־$e_1\in F$ מקבלים

$$|O(e_1)|=\frac{|G_3|}{(G_3)_{e_1}}$$

מטרנזיטיביות $O(e_1)=F$ ולכן $|O(e_1)|=6$ וגם $(G_3)_{e_1}\cong G_2\cong D_4$ ולכן $|(G_3)_{e_1}|=8$ ונקבל

$$|G_3|=|O(e_1)|\cdot|(G_3)_{e_1}|=6\cdot 8$$

☐

נגדיר את קבוצת האלכסונים הראשיים $D=\{x_1,x_2,x_3,x_4\}$, כאשר לדוגמה $x_1=\{(1,1,1),(-1,-1,-1)\}$, דהינו $x=\{v,-1\}$.
נגדיר גם עבור $g\in G_3$ את $gx=\{gv,g(-v)\}$.

טענה 17.8 *זוהי פעולה של* G_3 *על* D.

מקבלים הומומורפיזם $f:G_3\to S_4$.

למה 17.9 $\ker(f)=\{Id\}$.

הוכחה. ברור ש־$-Id,Id\in\ker(f)$. נניח ש־$g\in\ker(f)$. נבחר $v_1\in V$. מספיק להראות שאם $gv_1=v_1$ אז $gv=v$ לכל $v\in V$. בלי הגבלת הכלליות $v_1=(1,1,1)$ ולכן עבור $v=(x,y,z)$ נקבל

$$\langle v,v_1\rangle=x+y+z\neq -x-y-z=\langle -v,v_1\rangle$$

מכיוון שצריך להתקיים $\langle v,v_1\rangle=\langle gv,gv_1\rangle=\langle gv,v_1\rangle$ וגם $gv=\pm v$ כי $g\in\ker(f)$ נובע ש־$gv=v$ כי $\langle v,v_1\rangle\neq 0$ ולכן

$$\langle v,-v_1\rangle=-\langle v,v_1\rangle\neq\langle v,v_1\rangle$$

☐

מסקנה 17.10 f על.

הוכחה. ממשפט האיזומורפיזם הראשון נקבל

$$G_3/\{\pm Id\}\cong \mathrm{Im}(f)$$

ולכן בפרט גם $48/2=|G_3|/|\{\pm Id\}=|\mathrm{Im}(f)|=|S_4|$. ☐

נסתכל על $G\xrightarrow{\det}\{\pm1\}\cong\mathbb{Z}_{/2}$, נסמן $SG_3=\ker(\det)\triangleleft G_3$. נתבונן בהומומורפיזם $\psi:G_3\to S_4\times\{\pm1\}$ המוגדר על־ידי $g\mapsto(f(g),\det(g))$.

טענה 17.11 ψ *היא איזומורפיזם.*

הוכחה. מתקיים כי $|G_3|=48=24\cdot 2=|S_4\times\{\pm1\}|$ ולכן מספיק להראות כי ψ היא חד־חד ערכית.
נחשב:

$$\ker(\psi)=\ker(f)\cap\ker(\det)=\{\pm Id\}\cap SG_3=\{Id\}$$

ולכן ψ חד־חד ערכית. ☐

בנינו העתקה ל־S_4 על־ידי האלכסונים ואז בנינו העתקה לדטרמיננטה, ואז הוכחנו שהם הפיכים. אפשר להוכיח את הגודל של קוביה n־ממדית על־ידי שימוש במשפט מסלול מייצב והגודל של הקוביה מממד אחד יותר נמוך באינדוקציה בשיטה שבה עבדנו גם עכשיו עם הפאות.
$G_3\le O(3)$ אבל לא מצאנו מהם האיברים שנמצאים בחבורה זו. אז מהם האיברים הללו?

1. שיקופים:

$$\begin{pmatrix} \pm1 & & \\ & \pm1 & \\ & & \pm1 \end{pmatrix} \cong \left(\mathbb{Z}_{/2}\right)^3$$

יש 8 כאלה.

2. מטריצות הפרמוטציה: לדוגמה

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cong S_3$$

כאלה יש 6.

G_3 וגם G_n הן מטריצות פרמוטציה מוכללות.

נבחין כי S_3 פועל על הצירים, או על זוגות של פאות.

18 שיעור 13 — 24.6.2024

18.1 חבורות סופיות

הפעם נניח שחבורה היא סופית וננתח את המבנה שלה לעומק.
ראינו כי אם חבורה היא מגודל ראשוני אז אין לה תת־חבורות, וכי היא ציקלית, וראינו גם כי אפשר לבנות חבורות מתת־חבורות ראשוניות.

$$|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots$$

הגדרה 18.1 (חבורת p) חבורת p היא חבורה G מגודל p^n לאיזשהו $n \in \mathbb{N}$.

טענה 18.2 *אם G חבורת p אז $Z(G) \neq \{e\}$.*

שימושי לנו ליכולת לפרק חבורות מסוג זה על־ידי שימוש במרכז.

מסקנה 18.3 חבורת p לא אבלית איננה פשוטה.

מסקנה 18.4 אם $|G| = p^n$ אז קיימת $H \leq G$ כך ש־$|H| = p^k$ לכל $0 \leq k \leq n$.

הוכחה. $Z(G)$ תת־חבורת p לא טריוויאלית, דהינו $p \mid |Z(G)|$ ולכן ש תת־חבורה $H \leq Z(G)$ כך ש־$|H| = p$. מכיוון ש־H מרכזית היא נורמלית ב־G. מתקיים $|G/H| = p^{n-1}$. לכן באינדוקציה לכל $0 \leq k \leq n-1$ יש תת־חבורה $\overline{K} \leq G/H$ כך ש־$|\overline{K}| = p^k$. ממשפט ההתאמה $\overline{K}$ מתאימה לאיזושהי $K \leq G$ עם $\overline{K} = K/H$ ונקבל

$$[G : K] = [G/H : \overline{K}] = p^{n-k-1}$$

לכן $|K| = p^{k+1}$. $\square$

עתה נעסוק בשאלה איך ניתן למצוא שרשרת של תת־חבורות נורמליות עבור חבורה סופית כלשהי. השאלה המעניינת היא באיזה סדר מספר תת־החבורות גדל ביחס לגודל החבורה הסופית.

נעבור עתה לעיסוק בחבורה $|G| = n = p^r \cdot m$ כאשר $\gcd(m, p) = 1$.

הגדרה 18.5 (חבורות סילו) תת־חבורה $P \leq G$ מגודל p^r נקראת p־סילו (p-Sylow).

משפט 18.6 (משפט סילו הראשון) *לכל חבורה סופית G וראשוני p יש ל־G תת־חבורה p־סילו.*

הערה $p \nmid |G|$ אם ורק אם $\{e\} \leq G$ היא p־סילו.

דוגמה 18.1 אם G חבורת p אז $P = G \leq G$ היא p־סילו יחידה של G.

דוגמה 18.2 נניח $G = \mathbb{Z}_{/n}$ אז יש p־סילו יחידה $P = m\mathbb{Z}/n\mathbb{Z}$ מגודל $\frac{n}{m} = p^r$. ממשפט השאריות הסיני נקבל גם

$$\mathbb{Z}_{/n} \cong \mathbb{Z}_{/m} \times \mathbb{Z}_{/p^r}$$

במקרה זה $P \cong \{e\} \times \mathbb{Z}_{/p^r}$.

דוגמה 18.3 $G = S_p$, $|S_p| = p! = p \cdot (p-1)!$. ונגדיר $m = (p-1)!$. נוכל לבחור $P = \langle (1\ 2\ \dots\ p) \rangle \leq S_p$ נוכל גם להשתמש במשפט קיילי ולקבל

$$\mathbb{Z}_{/p} \hookrightarrow \mathrm{Sym}(\mathbb{Z}_{/p}) \cong S_p$$

דוגמה 18.4 $G = GL_n(\mathbb{F}_p)$, נבחן את המטריצות המשולשיות העליות, כאשר האלכסון הוא 1, ונוכל לבחור במשלוש עצמו מה שאנחנו רוצים, נגדיר חבורה זו להיות $U_n(\mathbb{F}_p)$.

$$|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1})$$

משיקולי אלגברה לינארית. נראה גם

$$|U_n(\mathbb{F}_p)| = p^0 p^1 \cdots p^{n-1} = p^{\binom{n}{2}}$$

לכן נקבל

$$|GL_n(\mathbb{F}_p)/U_n(\mathbb{F}_p)| = (p^n - 1)(p^{n-1} - 1) \cdots (p - 1)$$

וזה זר ל־p.

למה 18.7 $\gcd(p,m)=1$ אז

$$\binom{p^r m}{p^r} \equiv m(\mod p)$$

הוכחה. נבחן את הפולינום $(x+y)^p=\sum_{k=0}^{p}\binom{n}{k}x^k y^{n-k}$.
עבור $0<k<p$ מתקיים ש־$p\mid\binom{p}{k}$ שכן

$$\binom{p}{k}=\frac{p!}{k!(p-k)!}$$

ולכן $(x+y)^p\equiv x^p+y^p(\mod p)$ ולכן באינדוקציה

$$(x+y)^{p^r}\equiv x^{p^r}+y^{p^r}(\mod p)$$

לכן $(x+y)^{p^r m}\equiv (x^{p^r}+y^{p^r})^m(\mod p)$. לכן בפרט יש שוויון של המקדמים של $x^{p^r}\cdot y^{p^r(m-1)}$, כלומר

$$\binom{p^r m}{p^r}=\binom{m}{1}(\mod p)$$

□

משפט 18.8 (משפט סילו הראשון) *לכל חבורה G מהגודל $p^r m$ יש תת־חבורה p־סילו.*

הוכחה. נבחן את $X=\{S\subseteq G\mid |S|=p^r\}$. לא כל האיברים פה הם תת־חבורות וננסה להוכיח שאחד מהם הוא כן.
נסתכל על הפעולה הרגולרית של G על X המוגדרת על־ידי

$$g\cdot S=gS=\{gs\mid s\in S\}$$

ראית נשים לב כי $|X|=\binom{p^r m}{p^r}$ לפי הגדרת הבינום. ואנו יודעים כי ביטוי זה שקול ל־$m(\mod p)$ ולכן בפרט

$$p\nmid |X|$$

לכן קיים מסלול $O(S)$ כך ש־$p\nmid|O(S)|$.
ממשפט מסלול־מייצב נקבל $|O(S)|=|G|/|G_S|$ ולכן $|G_S|\geq p^r$.
נקבל ש־G_S פועלת (רגולרית) על S. לכל $x\in G_S$ ו־$s\in S$ מתקבל כי $xs\in S$.
בפרט אם $xs=ys$ אז $x=y$ לכל $x,y\in G_S$.

□

למה 18.9 *עבור $s\in S$ הפונקציה $G_s\to S$ על־ידי $x\mapsto s_0$ היא חד־חד ערכית.*

הוכחה. $x,y\in G_S$ אם $xs_0=ys_0$ אז על־ידי כפל מימין ב־s_0^{-1} נקבל $x=y$.

□

מסקנה 18.10

$$|G_S|\leq|S|=p^r$$

ולכן

$$|G_S|=p^r$$

משפט 18.11 (משפט סילו השני) *כל תת־החבורות p־סילו של G הן צמודות זו לזו.*

ישנו ינסוח מורחב למשפט, נראה גם אותו

משפט 18.12 (משפט סילו השני המורחב) *תהי G חבורה מסדר סופי ותהיה P חבורת p־סילו של G, אז לכל $K\leq G$ קיים $a\in G$ כך ש־$K\cap aPa^{-1}$ היא חבורת p־סילו של K. בפרט, כל חבורות p־סילו צמודות זו לזו.*

טענה 18.13 *$P\leq G$ תת־חבורה p־סילו ו־$Q\leq G$ תת־חבורה p כלשהי אז קיים $g\in G$ כך ש־$gQg^{-1}\leq P$.*

הטענה הזו גוררת את משפט סילו השני משיקלוי גודל.

למה 18.14 (למת הספירה היסודית) *אם G חבורת p פועלת על X סופית אז*

$$|Fix_G(X)|\equiv|X|(\mod p)$$

נקראת גם "הלמה היסודית".

הוכחה. לכל $x \in X$ נקבל

$$|O(x)| = |G|/|G_x| \in \{1, pm\}$$

ולכן בפרט

$$|X| = \sum |O(x)| \equiv |Fix_G(x)| \pmod p$$

$\square$

19 שיעור 14 — 26.6.2024

19.1 חבורות p־סילו

נתחיל בתזכורת לשיעור הקודם.

הגדרה 19.1 G חבורה כך ש־$|G| = p^r m$ כאשר $p \nmid m$. תת־חבורה $P \leq G$ נקראת p**־סילו** אם $|P| = p^n$ (או באופן שקול אם $[G : P]$ זר ל־p).

משפט 19.2 (משפט סילו הראשון) *לכל G סופית וראשוני p יש ל־G תת־חבורה p־סילו.*

טענה 19.3 *לכל $P \leq G$ תת־חבורה p־סילו ו־$Q \leq G$ תת־חבורה p. קיים $g \in G$ כך ש־$gQg^{-1} \leq P$.*

הוכחה.

$$Q \circlearrowright X = G/P$$

על־ידי כפל משמאל. אז $q(gP) = qgP$. Q חבורת p ו־$|X| = m$ ובפרט שונה מאפס מודולו p.
לכן מהלמה היסודית מקבלים כי ישנה נקודת שבת:

$$|Fix_Q(G/P) = |G/P| = m \neq 0(\mod p)$$

לכל $q \in Q$ מתקיים $qgP = gP$, כלומר $g^{-1}qg \in P$ ולכן $g^{-1}Qg \subseteq P$. □

משפט 19.4 (משפט סילו השני) *לכל G סופית וראשוני p כל ה־p־סילו צמודים זה לזה.*

הוכחה. P, Q הן p־סילו, קיים $g \in G$ כך ש־$g^{-1}Qg \subseteq P$.
מכיוון ש־$|g^{-1}Qg| = |P| = p^n$ נובע ש־$g^{-1}Qg = P$. □

מסקנה 19.5 $P \leq G$ תת־חבורה p־סילו. P נורמלית ב־G אם ורק אם p־סילו יחידה.

כאשר $G = p^r m$ נסמן ב־$Syl_p(G)$ את קבוצת תת־חבורות p־סילו של G וב־$n_p = |Syl_p(G)|$ מספר חבורות אלה.

הגדרה 19.6 (מנרמל) תהי חבורה G ו־$H \leq G$, אז נגדיר את המנרמל של H ונסמנו $N_G(H) = N(H)$ על־ידי

$$N(H) = \{x \in G \mid x^{-1}Hx = H\}$$

דהינו, חבורת האיברים שמצמידים את H לעצמה, וקבוצת האיברים כך שהמחלקה הימנית והשמאלית של H שוות.

תזכורת:

הגדרה 19.7 (מרכז) המרכז של $H \leq G$ הוא

$$C_G(H) = \{x \in G \mid \forall h \in H\ x^{-1}hx = h\}$$

אוסף האיברים שמצמידים כל איבר ב־H לעצמו.
נבחין כי $C_G(H) \leq N_G(H)$.
נקרא מרכז כי הוא כמו המרכז עבור איברים מסויימים.

משפט 19.8 (משפט סילו השלישי) *1. $n_p \mid m$*

2. $n_p \equiv 1(\mod p)$

הוכחה. **1.** $G \circlearrowright Syl_p(G)$ על־ידי הצמדה. ממשפט סילו השני נובע כי הפעולה היא טרנזיטיבית.
לכן ממשפט מסלול־מייצב אם נבחר $P \in Syl_p(G)$ אז $n_p = |Syl_p(G)| = |G|/|G_P|$.
מכיוון שלכל $x \in P$ מתקיים $x^{-1}Px = P$ מקבלים ש־$P \leq G_P$ ולכן

$$|G|/|G_P| \Big| |G|/|P| = m$$

הערה: $G_P = N_G(P)$, המנרמל של P, זה מה שמשאיר במקום את P. תת־החבורה הגדולה ביותר של G בה P היא תת־חבורה נורמלית.

.2 $P \circlearrowright Syl_p(G)$ על־ידי הצמדה. לפעולה זו יש נקודת שבת P. נראה ש־P נקודת השבת היחידה.
נניח ש־Q גם היא נקודת שבת ולכן

$$P \leq N(Q) \trianglerighteq Q$$

P ו־Q גם תת־חבורות p־סילו של $N(Q)$ ומכיוון ש־Q היא p־סילו נורמלית ב־$N(Q)$ אז נובע שהיא היחידה, כלומר $P = Q$.
המסקנה היא ש־$Fix_P(Syl_p(G)) = \{P\}$. מהלמה היסודית מקבלים כי

$$|Syl_p(G)| = |Fix_P(Syl_p(G))| \equiv 1(\mod p)$$

□

תזכורת לתנאים של משפט סילו השלישי הם: $|G| = p^r m$ כאשר $p \nmid m$, n_p הוא מספר ה־p־סילו של G, אז התנאים הם $n_p \mid m$ וכי $n_p \equiv 1(\mod p)$.

דוגמה 19.1 $|G| = 40 = 5^8 \cdot 8$ אז נגדיר $m = 8, p = 5$ ומסילו III מקבלים כי $n_5 \mid 8$ וגם כי $n_5 \equiv 1(\mod 5)$.
מבין המספרים 8 4 2 1 רק 1 מקיים את שני התנאים ולכן $n_5 = 1$ ולכן יש תת־חבורה 5־סילו יחידה $P \triangleleft G$ נורמלית ($P \cong \mathbb{Z}_{/5}$).

טענה 19.9 *תהי G אבלית, אז G פשוטה אם ורק אם $G \cong \mathbb{Z}_{/p}$.*

הוכחה. $\mathbb{Z}_{/p}$ פשוטה כי אין לה תת־חבורות נורמליות חוץ מ־$\{0\}, \mathbb{Z}_{/p}$.
מצד שני, אם G פשוטה אז ניקח $e \neq x \in G$ ונסתכל על $N\langle x\rangle = G$ ולכן G ציקלית, כלומר $G \cong \mathbb{Z}_{/p}$ או $G \cong \mathbb{Z}$.
ל־$\mathbb{Z}$ יש תת־חבורה לא טריוויאלית $n\mathbb{Z}$ לכל $n \neq 0, 1$, ולכן $G \ncong \mathbb{Z}$ ול־$\mathbb{Z}_{/n}$ יש תת־חבורה לכל $d \mid n$ שאיננה טריוויאלית $d \neq 1, n$ ולכן בהכרח $n = p$. □

טענה 19.10 *חבורת p סופית P היא פשוטה אם ורק אם $|P| = p$.*

הוכחה. אם $P \neq \{e\}$ אז $Z(P) \neq \{e\}$ ולכן מפשטות $Z(P) = P$. כלומר P אבלית והטענה נובעת מהטענה הקודמת. □

בתרגיל ראינו כי A_5 פשוטה לא אבלית. מתקיים $|A_5| = 60$.

טענה 19.11 *A_5 החבורה הלא אבלית הפשוטה הקטנה ביותר.*

טענה 19.12 *אם $m < p$ אז $n_p = 1$.*

הוכחה. אם $n_p \neq 1$ אז $n_p \geq p + 1$ ולכן $n_p > m$ בסתירה לכך ש־$n_p \mid m$. □

לדוגמה $3 \cdot 11 = 33$ ונבחן את הפירוק של 3 הוא 3 1 ו־11 גדול משניהם ומבטל את היכולת שיהיו יותר מתת־חבורה p־סילו אחת, בהתאם היא נורמלית.
נשארים לטפל במספרים $12, 24, 30, 36, 48, 56$.
נניח ש־$H \lneq G$ חבורה ותת־חבורתה. נבחן את $G \circlearrowright G/H$ רגולרית, ונקבל הומומורפיזם $f : G \to \mathrm{Sym}(G/H)$. אנו יודעים כי $\ker(f) \trianglelefteq G$ תת־חבורה נורמלית. מאיזו I נקבל $G/\ker(f) \cong \mathrm{Im}(f)$ ובהתאם $|G|/|(|G|/|H|)! \geq |\mathrm{Im}(f)| = |G|/|\ker(f)|$. מכיוון ש־$G \circlearrowright G/H$ טרנזיטיבית מתקיים $\ker(f) \neq G$.

מסקנה 19.13 אם $|G| < |G/H|!$ אז G לא פשוטה.

טענה 19.14 *$|G| = p^n m, |P| = p^n$, אם $m! < p^n m$ אז G איננה פשוטה, לכן גם $(m-1)! < p^n$.*

הוכחה. $H = P$ ו־$|G|/|H| = m$. □

נראה כי $12 = 2^2 \cdot 3$ אבל $2^2 = 4 < (3-1)!$. גם $36 = 3^2 2^2$ ו־$(4-1)! = 6 < 9 = 3^2$.
נבדוק עתה את $56 = 7 \cdot 2^3$.

טענה 19.15 *אין חבורה פשוטה מגודל 56.*

הוכחה. $n_7 \mid 8$ וגם $n_7 \equiv 1 (\mod 7)$ ולכן $n_7 = 1, 8$. אם $n_7 = 1$ סיימנו ולכן נניח כי $n_7 = 8$, נגדיר $P_1, \dots, P_8$ להיות החבורות 7־סילו השונות של G. $|P_i| = 7$ ולכן $P_i \cong \mathbb{Z}_{/7}$ לכל $i = 1, \dots, 8$, וגם $P_i \cap P_j = \{e\}$ לכל $i \neq j$ ולכן יש ב־G בדיוק $8 \cdot 6$ איברים מסדר 7. משאיר $56 - 48 = 8$ איברים שאינם מסדר 7. ל־G יש חבורת 2־סילו Q מגודל 8 ולכן $Q = \{x \in G \mid 7 \neq \text{order of } x\}$ ולכן נורמלית. $\square$

20 שיעור 15 — 1.7.2024

20.1 פירוק חבורות סופיות

בשיעור הקודם ראינו כי $N \lhd G \xrightarrow{\pi} G/N$ ובחנו את ההתנהגות והקשר בין החבורות האלה.

הגדרה 20.1 (סדרה תת־נורמלית) עבור חבורה G סדרה תת־נורמלית של G היא סדרה של תת־חבורות

$$\{e\} \trianglelefteq G_r \trianglelefteq G_{r-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G$$

הערה סדרה נקראת נורמלית אם בנוסף כל $G_i \trianglelefteq G$.

הערה סדרה נקראת לא מגמגמת אם $G_i \lhd G_{i+1}$.

הערה סדרה תת־נורמלית א' נקראת עידון של סדרה תת־נורמלית ב' אם סדרה ב' מתקבלת מסדרה א' על־ידי השמטת איברים.

הגדרה 20.2 חבורה G נקראת פתירה (Solvable) אם קיימת ל־G סדרה תת־נורמלית (G_i) כך ש־G_i/G_{i+1} אבלית לכל $1 \le i \le r$.

חבורה אבלית גורר שהחבורה פתירה.

דוגמה 20.1 $\overbrace{A_4 \lhd S_4}^{\mathbb{Z}_{/2}} \lhd V \lhd \{0\}$, כאשר $V = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \dots\} \simeq \mathbb{Z}_{/2} \times \mathbb{Z}_{/2}$.
לכן S_4 פתירה. לעומת זאת S_n לא פתירה עבור $n \ge 5$.

הגדרה 20.3 (סדרת הרכב) סדרת הרכב (Composition series) של G זו סדרה תת־נורמלית $(G_i)_{i=0}^r$ כך ש־G_i/G_{i+1} פשוטה לכל i.

הערה יש חבורות שאין להן סדרת הרכב, למשל $\mathbb{Z}$.

אנחנו נטען שהבעיה היא רק עם חבורות אינסופיות.

טענה 20.4 *תהי G חבורה סופית.*
כל סדרה תת־נורמלית לא מגמגמת (G_i) של G ניתן לעדן לסדרת הרכב.

הוכחה. תהי $\{e\} = G_r \lhd G_{r-1} \lhd \cdots \lhd G_1 \lhd G_1 = G$.
אם יש מנה לא פשוטה G_i/G_{i+1} יש $\{e\} \ne \overline{N} \lhd G_i/G_{i+1}$ ממשפט ההתאמה יש $\overline{N} = N/G_{i+1}$,$G_{i+1} \lhd N \lhd G_i$.
מתקיים $|G_i/N|, |N/G_{i+1}| < |G_i/G_{i+1}|$.
נניח באינדוקציה שכל סדרה תת־נורמלית (H_i) של G, אם $\max_i |H_i/H_{i+1}| < n$ יש עידון שהוא סדרת הרכב ונקבל שאם $\max |G_i/G_{i+1}| = n$ אז ל־(G_i) יש עידון שהוא סדרת הרכב.
הסבר: באינדוקציה על הגודל של המנה G_i/G_{i+1} המקסימלית ומספרן יש עידון שהוא סדרת הרכב. □

אפשר להסתכל על חבורת הרכב כעל הרחבה לקונספט של חבורות פשוטות. במקום שתהיה סדרה של 1, תהיה סדרה כזו באורך כלשהו. נעבור לשאול את השאלה האם סדרת הרכב היא יחידה. התשובה היא שלא, נראה דוגמה.

דוגמה 20.2 נבחן את

$$0 \overbrace{\lhd}^{\mathbb{Z}_{/2}} 3\mathbb{Z}_{/6} \overbrace{\lhd}^{\mathbb{Z}_{/3}} \mathbb{Z}_{/6}$$

ואת

$$0 \overbrace{\lhd}^{\mathbb{Z}_{/3}} 2\mathbb{Z}_{/6} \overbrace{\lhd}^{\mathbb{Z}_{/2}} \mathbb{Z}_{/6}$$

ואלה כמובן סדרות הרכב **שונות**.

בדוגמה מקודם $S_4 \overset{\mathbb{Z}_{/2}}{\rhd} A_4 \overset{\mathbb{Z}_{/3}}{\rhd} 0$ הסדר הוא סדר זה בלבד.

משפט 20.5 (משפט ז'ורדן־הולדר) *תהי G חבורה עם סדרת הרכב* $\{e\} = G_r \lhd \cdots \lhd G_0 = G$.
כל סדרת הרכב אחרת $\{e\} = H_s \lhd \cdots \lhd H_0 = G$ *מקיימת* $r = s$ *וגם*

$$H_i/H_{i+1} \simeq G_{\sigma(i)}/G_{\sigma(i)+1}$$

לאיזושהי תמורה σ על $0, \dots, r-1$.

למה 20.6 *תהי G חבורה עם סדרת הרכב* $\{e\} = G_r \triangleleft \cdots \triangleleft G_0 = G$.
לכל תת־חבורה $N \triangleleft G$ הסדרה $N = G_0 \cap N \triangleleft \cdots \triangleleft G_r \cap N = e$ נהיית סדרת הרכב אחרי שמוחקים כפילויות.

הוכחת המשפט. נוכיח את הטענה באינדוקציה על r שמייצג את אורך סדרת ההרכב הקצרה ביותר של G.
תהינה שתי הסדרות $G = G_0 \triangleleft \cdots \triangleleft G_r = \{e\}$, $G = H_0 \triangleleft \cdots \triangleleft H_s = \{e\}$.
נסתכל $G \triangleleft GH_1 \triangleleft H_1$, מנה זו פשוטה ולכן $G_1H_1 = H_1$ או $G_1H_1 = H$.
במקרה הראשון אז $H_1 \subseteq G_1$ ולכן $G \triangleleft H_1 \triangleleft G_1$ והמנה פשוטה, ולכן $G_1 = H_1$.
באינדוקציה $r - 1 = s - 1$ והמנות העוקבות $G_i/G_{i+1} \simeq H_{\sigma(i)}/H_{\sigma(i)+1}$ ל־$\sigma \in \mathrm{Sym}(\{1, \ldots, r-1\})$ וסיימנו.
אם המקרה השני נכון אז נגדיר $K = G_i \cap H_i$ ונקבל $G = G_1H_1$ ו־$G_1 = H_1$ שווה ל־$K = G_1 \cap H_1$, ונקבל ממשפט האיזומורפיזם השני

$$G/G_1 = G_1H_1/G_1 \simeq H_1/(G_1 \cap H_1) = H_1/K$$

ומצד שני

$$G/H_1 = G_1H_1/G_1 \simeq G_1/(G_1\ capH_1) = G_1/K$$

וקיבלנו

$$K \triangleleft G_1 \triangleleft G, \qquad K \triangleleft H_1 \triangleleft G$$

כאשר המנות מתחלפות באלכסון (המנה הראשונה שקולה למנה השנייה בשרשרת השנייה והפוך).
ל־K מהלמה נקבל שיש סדרת הרכב $K = K_2 \triangleleft K_3 \triangleleft \cdots \triangleleft K_l$.
לכן נוכל לבנות ולקבל

$$\{e\} = K_l \triangleleft \ldots K_2 \triangleleft G_1 \triangleleft G \qquad \{e\} = K_l \triangleleft \ldots K_2 \triangleleft H_1 \triangleleft G$$

וקיבלנו ארבע סדרות (יחד עם הסדרות המקוריות). מאינדוקציה על G_1 אנחנו מקבלים כי $r = l$ וכי המנות העוקבות של G_i שקולות למנות בסדרה הראשונה הנוספת עד כדי שינוי סדר והמשפט מתקיים.
מאינדוקציה על H_i והסדרה השנייה שיצרנו נקבל $s = l$ והמשפט מתקיים.
אבל גם לשתי הסדרות שהגדרנו זה עתה יש אותן מנות עוקבות עד כדי שינוי סדר כפי שכבר ראינו, ולכן משפט ז'ורדן־הולדר מתקיים גם לשתי הסדרות השונות המקוריות. $\square$

סדרת הרכב מאורך 1 היא חבורה פשוטה.

הוכחת הלמה. צריך להראות

$$(G_i \cap N)/(G_{i+1} \cap N)$$

פשוטה או טריוויאלית. נרצה להפעיל את איזו 2 אבל זה לא המקרה וצריך לעבוד יותר קשה.

$$(G_i \cap N)/(G_{i+1} \cap N) = (G_i \cap N)/(G_{i+1} \cap N \cap G_i) \overset{\text{איזו } 2}{\simeq} ((G_i \cap N) \cdot G_{i+1})/G_{i+1}$$

אבל

$$(G_i \cap N) \cdot G_{i+1} \subseteq (G_i \cap N) \cdot G_i = G_i$$

ולכן

$$((G_i \cap N) \cdot G_{i+1})/G_{i+1} \triangleleft G_i/G_{i+1}$$

וזו כמובן פשוטה ולכן כל תת־חבורה היא או G_i/G_{i+1} ולכן פשוטה או טריוויאלית.
צריך לבדוק שאכן $(G_i \cap N)G_{i+1} \triangleleft G_i$ תת־חבורה נורמלית (תרגיל). $\square$

21 שיעור 16 — 3.7.2024

21.1 סדרות נורמליות — המשך

חפש ביוטיוב finite simple group of order 2.

הגדרה 21.1 (גורמי הרכב) עבור G עם סדרת הרכב, ונגדיר כי היא סופית, אז **גורמי ההרכב** של G הם הקבוצה של G_i/G_{i+1} קבוצה עם כפילויות לכל סדרת הרכב $(G_i)_{i=1}^r$.

ישנן חבורות אינסופיות ויש חבורות סופיות ויש מקרים שבהם אלו נוצרות יחדיו, לדוגמה במקרה של $GL_n(\mathbb{F})$, נוכל לבחור $\mathbb{F}_p$ וליצור חבורות סופיות.

טענה 21.2 *עבור G חבורה סופית מתקיים ש־G פתירה אם ורק אם גורמי ההרכב שלה כולם ציקליים מסדר ראשוני ($\simeq \mathbb{Z}_{/p}$).*

הוכחה. אם גורמי הרכב מהצורה $\mathbb{Z}_{/p}$ אז הם בפרט אבליים ולכן G פתירה.

לכיוון ההפוך אם היא פתירה אז ניקח סדרה תת־נורמלית עם מנות עוקבות G_i/G_{i+1} אבליות, ונעדן אותה לסדרת הרכב. כל גורם ברכב מקיים $G_i \lhd \cdots \lhd H \lhd K \lhd \cdots \lhd G_{i+1}$ ולכן כל גורם הרכב הוא אבלי כי הוא מנה של תת־חבורה של חבורה אבלית G_i/G_{i+1}. מכיוון שפשוטה סופית ואבלית היא ציקלית מגודל ראשוני קיבלנו את הטענה. $\square$

מחוץ לקונטקסט של הקורס כי זאת הוכחה עצומה אבל לידע כללי המשפט הזה קיים

משפט 21.3 (משפט Feit-Thompson) *כל חבורה סופית מגודל אי־זוגי היא פתירה.*

טענה 21.4 *G חבורה פתירה אז*

1. *כל $H \le G$ פתירה אף היא.*
2. *לכל $N \lhd G$ חבורת המנה G/N פתירה.*
3. *לכל תת־חבורה נורמלית N וגם G/N פתירות אז גם G פתירה.*

למה 21.5 *עבור חבורה G עם סדרה תת־נורמלית $\{e\} = G_r \lhd \cdots \lhd G_0 = G$ ותת־חבורה $H \le G$ נגדיר*

$$\{e\} = H_r \lhd \cdots \lhd H_0 = H$$

על־ידי $H_i = G_i \cap H$. אז מתקיים

$$H_i/H_{i+1} \simeq G_i/G_{i+1}$$

בפרט זה גורר את סעיף 1 של הטענה הקודמת שכן אם G_i/G_{i+1} אבלית אז H_i/H_{i+1} אבלית.

הוכחה. ראשית נשים לב כי $H_{i+1} = H \cap G_{i+1} \lhd H \cap G_i = H_i$.

נחשב ונקבל

$$H_i/H_{i+1} \simeq (H_i)/(H \cap G_{i+1}) = H_i/((H \cap G_i) \cap G_{i+1}) = H_i/(H_i \cap G_{i+1})$$

לכן נקבל כי

$$H_i/(H_i \cap G_{i+1}) \overset{\text{Iso II}}{\simeq} H_iG_{i+1}/G_{i+1} \le G_i/G_{i+1}$$

$\square$

למה 21.6

$$\{e\} = G_r \lhd \cdots \lhd G_0 = G$$

ו־$N \lhd G$ עם $K = G/N$ נגדיר

$$K_i = G_iN/N$$

מתקיים כי K_i/K_{i+1} איזומורפית למנה של G_i/G_{i+1} ובפרט אם G פתירה אז G/N פתירה.

הוכחה.

$$K_i/K_{i+1} = (G_iN/N)/(G_{i+1}N/N) \overset{\text{Iso III}}{\simeq} (G_iN)/(G_{i+1}N) \simeq \frac{G_i(G_{i+1}N)}{G_{i+1}N} \overset{\text{Iso II}}{\simeq} G_i/(G_i \cap G_{i+1}N)$$

מכיוון ש־$G_{i+1} \leq G_i \cap G_{i+1}N$ נובע ש־$G_i/(G_i \cap G_{i+1}N)$ איזומורפית למנה של G_i/G_{i+1}.

הסבר: $G_{i+1} \triangleleft G_i \cap G_{i+1}N \triangleleft G_i$ והפעלת משפט האיזומורפיזם השלישי על המנה של הדברים האלה. ☐

למה 21.7 *$N \triangleleft G$ עם מנה $K = G/N$ ו־$\{e\} = N_r \triangleleft \cdots \triangleleft N_0 = N$.*

$\{e\} = G_r/N \triangleleft \cdots \triangleleft G_0/N = G/N$.

אז $\{e\} = N_r \triangleleft \cdots \triangleleft N_0 = G_s \triangleleft \cdots \triangleleft G_0 = G$ עם מנות עוקבות איזומורפיות N_i/N_{i+1} ו־$G_i/G_{i+1} \simeq (G_i/N)/(G_{i+1}/N)$.

בפרט אם N ו־G/N פתירות אז G פתירה.

הוכחה. ממשפט האיזומורפיזם השלישי נקבל ישר $G_i/G_{i+1} \simeq (G_i/N)/(G_{i+1}/N)$. ☐

איך אפשר לפרק חבורה סופית G כלשהי בלי להכיר אותה לפני זה? בשלב הראשון אנו מחפשים תת־חבורה נורמלית $N \triangleleft G$ כך ש־G/N אבלית. לכאורה אנו יכולים לבחור את החבורה הלא נכונה ואז להיתקע בתהליך, אבל למעשה על־ידי עידון לסדרת הרכב ומשפט ז'ורדן־הורדר מהשיעור הקודם נקבל כי נוכל להמשיך את מלאכת הפירוק. אבל יש דבר אפילו יותר יעיל, בכל שלב אפשר לעשות את המנה הכי גדולה שאפשר, למצוא את החלוקה הכי יעילה בכל שלב. ככה כל צעד יהיה הכי גדול ויכיל כמה שיותר עבודה. נבחן את

$$\pi : G \twoheadrightarrow G/N$$

צריך שיתקיים $\pi(x)\pi(y) = \pi(y)\pi(x)$ ונבחין כי נקבל מהם $\pi(xy) = \pi(yx)$ וזה קורה אם ורק אם $\pi(xyx^{-1}y^{-1}) = e$, דהינו אם $\pi(x)\pi(y)(\pi(x))^{-1}(\pi(y))^{-1} = e$, טם $xyx^{-1}y^{-1} \in \ker(\pi) = N$.

מסקנה 21.8 G/N אבלית אם ורק אם לכל $x, y \in G$ מתקיים $xyx^{-1}y^{-1} \in N$

הגדרה 21.9 (קומוטטור) הביטוי $[x, y] = xyx^{-1}y^{-1}$ נקרא הקומוטטור של x ו־y.

נקבל כי $[x, y]yx = xy$.

הגדרה 21.10 (חבורה נגזרת) עבור חבורה G **החבורה הנגזרת** של G המסומנת על־ידי $G' = \langle\{[x, y] \mid x, y \in G\}\rangle$.

טענה 21.11 *G' תת־חבורה נורמלית של G.*

הוכחה. מספיק להראות שלכל $z \in G$ ולכל יוצר מהצורה $[x, y]$ ב־G מתקיים $z[x, y]z^{-1} \in G'$.

זה נובע מ־$z[x, y]z^{-1} = zxyx^{-1}y^{-1}z^{-1} = zxz^{-1}zyz^{-1}zx^{-1}z^{-1}zy^{-1}z^{-1} = [zxz^{-1}, zyz^{-1}]$ ☐

בהוכחה השתמשנו באוטומורפיזם ולכן נוכל לטעון טענה יותר משמעותית על כל אוטומורפיזם. במקרה הזה זה סוג של אפשרי, נקרא חבורה אופיינית (Characteristic).

הגדרה 21.12 (אבליזציה) האבליזציה של G מוגדרת להיות

$$G^{ab} := G/G'$$

הערה אם $N \triangleleft G$ כך ש־G/N אבלית אז $N \triangleleft G'$ ו־G/N איזומורפית למנה של G^{ab}.

הגדרה 21.13 G חבורה. לכל $n \geq 0$ נסמן $G^{(0)} = G$ ו־$G^{(n+1)} = (G^{(n)})'$.

הסדרה הנגזרת $G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots$.

טענה 21.14 *G פתירה אם ורק אם קיים $n \geq 0$ כך ש־$G^{(n)} = \{e\}$.*

הוכחה. אם $G^{(n)} = \{e\}$ לאיזושהו n אז G פתירה כי מצאנו סדרה תת־נורמלית עם מנות עוקבות אבליות.

נניח כי G פתירה עם $\{e\} = G_r \triangleleft \cdots \triangleleft G_0 = G$ כך שכל המנות אבליות.

נוכיח באינדוקציה ש־$G^{(i)} \leq G_i$.

עבור $i = 0$ לפי הגדרה, ונוכיח עבור $i + 1$,

$$G^{(i+1)} = (G^{(i)})' \leq (G_i)'$$

מכיוון ש־G_i/G_{i+1} אבלית אז $G'_i \leq G_{i+1}$. ☐

הנושא של חבורות נילפוטנטיותת שהוא מה שיושב בין חבורות אבליות לפתירות הוא נושא שננסה לעשות בשיעור אחד ובמקסימום נוותר ופשוט נמשיך לתורת החוגים במקום כדי להספיק.

22 שיעור 17 — 8.7.2024

22.1 סדרות וחבורות פתירות

דיברנו על זה שאם $\{e\} = G_r \triangleleft \cdots \triangleleft G_0 = G$ סופית ו־G_i/G_{i+1} אבלית לכל i.
אין אופציה לטעות, תמיד אפשר להמשיך, ונוכל להראות שהיא פתירה מכל זווית.
נוכל לקחת את הסדרה שמצטמצמת הכי מהר, היא סדרת הנגזרות

$$\{e\} = G^{(r)} \triangleleft \cdots \triangleleft G^{(0)} = G$$

המוגדרת על־ידי יוצרים מורכבים מקומוטטורים.

נטען כי אם אנחנו מנסים לבנות את הסדרה הזאת בכיוון ההפוך, מהאיבר הנייטרלי עד ל־G, אז אנחנו יכולים להיתקע, נראה דוגמה

דוגמה 22.1

$$\{e\} \triangleleft A_3 \triangleleft S_3$$

אבל אם היינו מתחילים מהאיבר הנייטרלי היינו יכולים לבחור

$$\{e\} \triangleleft \langle (1\ 2) \rangle \le S_3$$

אבל אנו יודעים כי אין חבורה נורמלית שתאפשר לנו להתקדם.

בתרגיל של השבוע אנו מראים כי כל אחת מהחבורות בסדרה הנגזרת היא נורמלית בחבורה כולה. ולכן סדרת הנגזרות היא לא סתם תת־נורמלית, היא נורמלית, תנאי חזק הרבה יותר.
לכן אם תמיד נבחר סדרות נורמליות נוכל להסיק שלא ניתקע בתהליך בניית הסדרה, משני הכיוונים.
תמיד אפשר למצוא סדרה נורמלית עם איבר G.

דוגמה 22.2 אם $Z(G) \ne \{e\}$ אז נוכל לבחור $\{e\} \triangleleft Z(G) \triangleleft G$.
נסמן $Z(G) = Z_1$ ונבדוק את $Z(G/Z_1) \simeq Z_2/Z_1$ ונקבל חבורה נורמלית גדולה יותר ונוכל לבנות ככה סדרה

$$\{e\} \triangleleft Z_1 \triangleleft Z_2 \triangleleft \cdots \triangleleft G$$

לחבורות כאלה יש שם, הן חבורות נילפוטנטיות, חבורות שבהן אפשר לבנות סדרה נורמלית משני הכיוונים.

הגדרה 22.1 (חבורה נילפוטנטית) חבורה G נקראת r־**נילפוטנטית** כאשר $G/Z(G)$ היא $r-1$־נילפוטנטית, כאשר תנאי העצירה הוא 0־נילפוטנטית ולכן היא טריוויאלית.
חבורה נקראת נילפוטנטית אם היא r־נילפוטנטית לאיזשהו $r \in \mathbb{N}$.

הערה חבורה 0־נילפוטנטית היא טריוויאלית, חבורה 1־נילפוטנטית היא אבלית.

דוגמה 22.3 כל חבורת p היא נילפוטנטית.

דוגמה 22.4 S_3 היא פתירה אך לא נילפוטנטית.

נגדיר למה שלא קשורה לחומר ותעזור לנו

למה 22.2 *אם $N_1 \triangleleft G_1, N_2 \triangleleft G_2$ אז $N_1 \times N_2 \triangleleft G_1 \times G_2$ ומתקיים*

$$(G_1 \times G_2)/(N_1 \times N_2) \simeq (G_1/N_1) \times (G_2/N_2)$$

הוכחה. נבנה הומומורפיזם $\pi : G_1 \times G_2 \to (G_1/N_1) \times (G_2/N_2)$.
נשתמש בהטלות הקנוניות $\pi_1 : G_1 \to G_1/N_1, \pi_2 : G_2 \to G_2$ ונגדיר

$$\pi(x_1, x_2) = (\pi_1(x_1), \pi_2(x_2))$$

קל לראות שזה הומומורפיזם (תרגיל).
נחשב את הגרעין:

$$(\pi_1(x_1), \pi_2(x_2)) = \pi(x_1, x_2) = (e_1, e_2) \iff x_1 \in \ker(\pi_1) = N_1, x_2 \in \ker(\pi_2) = N_2$$

מצד שני מכיוון ש־π_1 ו־π_2 על אז גם π על ולכן ממשפט האיזומורפיזם הראשון נקבל

$$(G_1 \times G_2)/(N_1 \times N_2) = (G_1 \times G_2)/\ker(\pi) \simeq \mathrm{Im}(\pi) = (G_1/N_1) \times (G_2/N_2)$$

$\square$

דוגמה 22.5 $\mathbb{R}/\mathbb{Z} \simeq S^1 \subseteq \{z \in \mathbb{C}^\times \mid |z| = 1\}$
באופן דומה $\mathbb{R} \times \mathbb{R}/\mathbb{Z} \times \mathbb{Z} \simeq S^1 \times S^1$.

טענה 22.3 *1. תת־חבורה של חבורה r־נילפוטנטית היא בעצמה r־נילפוטנטית.*

2. מנה של חבורה r־נילפוטנטית היא בעצמה גם r־נילפוטנטית.

3. מכפלה ישרה של חבורות r־נילפוטנטיות היא r־נילפוטנטית.

הוכחה. הטענה הראשונה והשנייה בתרגיל.

נוכיח את הטענה השלישית.

ראשית

$$Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$$

ונוכיח באינדוקציה על r.

עבור $r = 0$ זה ברור שכן שתי החבורות טריוויאליות.

ל־$r \geq 1$ נראה

$$(G_1 \times G_2)/(Z(G_1 \times G_2)) \simeq (G_1 \times G_2)/(Z(G_1) \times Z(G_2)) \overset{\text{הלמה}}{\simeq} (G_1/Z(G_1)) \times (G_2/Z(G_1))$$

ונקבל כי הביטוי האחרון הוא $(r-1)$־נילפוטנטי כחלוקה במרכזים כפי שהגדרנו נילפוטנטיות, ומהנחת האינדוקציה $(r-1)$ נילפוטנטית. $\square$

דוגמה 22.6 לכל $\mathbb{F}$ שדה ו־$U_n(\mathbb{F}) \leq GL_n(\mathbb{F})$ אז U_n נילפוטנטית, אבל נבחין כי יתכן כי $\mathbb{F} = \mathbb{R}$ ובכלל לא בהכרח היא סופית, דהינו נילפוטנטיות היא לא סגורה לסופיות.

משפט 22.4 *עבור G חבורה סופית, התנאים הבאים שקולים*

1. G נילפוטנטית.

2. G איזומורפית למכפלה ישרה של חבורות p.

3. לכל ראשוני p החבורה ה־p־סילו של G היא יחידה (שקול לנורמליות).

מספר הערות עבור ההוכחה:

הערה אם $p_1, \ldots, p_n$ ראשוניים שונים ו־$P_1, \ldots, P_n$ כך ש־P_i חבורת p_i אז ה־p_i־סילו של $G = P_1 \times \cdots \times P_n$ היא P_i.

הערה אם $N \lhd G$ ו־$H \leq G$ אז $HN \leq G$.

אם $N \lhd G, H \lhd G$ אז $HN \lhd G$ כנביעה מ:

$$g(hn)g^{-1} = (ghg^{-1})(gng^{-1}) \in HN$$

הערה אם $H \leq G = \langle g_1, \ldots, g_e \rangle$ אז

$$H \lhd G \iff \forall i \in [r]\, H = g_i H g_i^{-1}$$

הוכחה. הגרירה של 2 ל־3 הייתה בתרגיל, ו־2 גורר את 1 מהטענה האחרונה, ולכן נוכיח את הגרירה מ־1 ל־2 בלבד.

$(1) \implies (2)$ ברור.

נוכיח $(3) \implies (1)$ באינדוקציה על $|G|$. ראשית $\{e\} \neq Z(G) \lhd G$ אז נבחר ראשוני כך ש־$p \mid |Z(G)|$. ממשפט קושי קיים $z \in Z(G)$ מסדר p, כלומר תת־החבורה $W = \langle z \rangle \leq Z(G)$ מגודל p. מכיוון ש־$W \leq Z(G)$ אז מתקיים $W \lhd G$, ולכן נסתכל על $\overline{G} = G/W$ שהיא מגודל $|\overline{G}| = \frac{|G|}{|W|} = \frac{|G|}{p}$ ובפרט קטן מ־$|G|$. בתור מנה של G החבורה $\overline{G}$ נילפוטנטית ולכן מהנחת האינדוקציה יש ל־$\overline{G}$ חבורת q־סילו יחידה ונורמלית לכל ראשוני q.

ראשית נראה של־G יש חבורת p־סילו נורמלית (המקרה $p = q$). נבחר $\overline{P} \lhd \overline{G}$ ה־p־סילו של $\overline{G}$. ממשפט ההתאמה נקבל עבור $\overline{P} = P/W$

$W \triangleleft P \triangleleft G$. נשים לב כי P תת־חבורה נורמלית כלשהי, ועלינו להוכיח שהיא חבורת p־סילו, נעשה זאת על־ידי שיקולי גודלי החבורות. נשים לב ש־P היא p־סילו של G

$$|P| = |\overline{P}| \cdot p \qquad |G| = |\overline{G}| \cdot p$$

עבור ראשוני $q \neq p$ ניקח q־סילו $\overline{Q} \triangleleft \overline{G}$ כאשר $\frac{\tilde{Q}}{W} \simeq \overline{Q} \triangleleft \overline{G}$ $W \triangleleft \tilde{Q} \triangleleft G$ (ממשפט ההתאמה) ומתקיים

$$|\tilde{Q}| = |Q| \cdot p = q^m \cdot p$$

כאשר החבורות q־סילו של G כולן מגודל q^m.

לכל q־סילו $Q \leq G$

$$W \triangleleft Q \cdot W \leq G$$

ממשפט ההתאמה $\overline{QW} = \frac{QW}{W}$ תת־חבורה מגודל q^m של $\overline{G}$.

ולכן q־סילו של $\overline{G}$, מהנחת האינדוקציה ל־$\overline{G}$ נקבל q־סילו יחידה ולכן ממשפט ההתאמה $Q \leq WQ = \tilde{Q}$.

הסבר: Q ו־W מתחלפות ו־$Q \cap W = \{e\}$ ולכן $WQ \simeq W \times Q$ ובפרט $|WQ| = |W| \cdot |Q| = p \cdot q^m$ ו־$WQ \to W \times Q$.

בפרט כל q־סילו של G מוכלת ב־$\tilde{Q}$. נותר להראות של־$\tilde{Q}$ עצמה יש q־סילו יחידה (נורמלית).

- כל $g \in Q$ מקיים $gQg^{-1} = Q$
- כל איבר $w \in W$ מקיים $wQw^{-1} = Q$ שכן $W \leq Z(G)$

ולכן $Q \triangleleft \tilde{Q}$ (ולכן גם יחידה). $\square$

דוגמה 22.7 אם $n = p_1^{d_1} \cdots p_n^{d_n}$ אז נקבל

$$\mathbb{Z}_{/n} \simeq \mathbb{Z}_{/p_1^{d_1}} \times \cdots \times \mathbb{Z}_{/p_n^{d_n}}$$

וקיבלנו את משפט השאריות הסיני.

23 שיעור 18 — 10.7.2024

23.1 תורת החוגים

הערה $(\mathbb{F},+,\cdot,0,1)$ היא שדה אם

- $(\mathbb{F},+,0)$ היא חבורה אבלית
- $(\mathbb{F}^\times,\cdot,1)$ היא חבורה אבלית
- יש פילוג
- $0\neq 1$

הגדרה 23.1 (חוג) $(R,+,\cdot,0,1)$ היא חוג כאשר

1. $(R,+,\cdot)$ חבורה אבלית
2. $(R,\cdot,1)$ מקיימת
   א. קיבוץ: $\forall x,y,z\in R:(xy)z=x(yz)$.
   ב. קיום נייטרלי: $1\cdot x=x\cdot 1$ לכל $x\in R$
3. פילוג: $\forall x,y,z\in R:(x+y)\cdot z=x\cdot z+y\cdot z, z\cdot(x+y)=z\cdot x+z\cdot y$.

הגדרה 23.2 חוג R נקרא

1. חוג קומוטטיבי אם $x\cdot y=y\cdot x$ לכל $x,y\in R$
2. חוג חילוק אם $\forall x\in R\setminus\{0\}$ קיים $y\in R$ כך ש־$1=x\cdot y=y\cdot x$.

חוג האפס $R=\{0\}$ הוא חוג. בתרגיל נראה שתכונות של חוגים מתקיימות ומזכירות את התכונות של חבורות. לדוגמה $0\cdot x=x\cdot 0=0$, או ש־$(-1)\cdot x=-x$. אם ב־R יש לפחות שני איברים אז $1\neq 0$.

הגדרה 23.3 (תת־חוג) עבור חוג R תת־חוג זו תת־קבוצה $S\subseteq R$ כך שמתקיים

1. S תת־חבורה ביחס לחיבור
2. S היא תת־מונואיד ביחס לכפל, כלומר
   א. סגורה לכפל
   ב. $1\in S$

הערה תת־חוג הוא בפרט חוג עם אותן הפעולות ו־0 ו־1.

דוגמה 23.1 כל שדה $\mathbb{F}$ הוא חוג, למשל $\mathbb{R},\mathbb{C},\mathbb{Q},\mathbb{F}_p$ או למשל $\mathbb{R}(f)$ הפולינומים.
גם $\mathbb{Z}$ הוא חוג, וגם $\mathbb{Z}_{/n}$ עם הפעולות הרגילות.
גם $M_n(\mathbb{F})$ מטריצות $n\times n$ מעל שדה $\mathbb{F}$ עם חיבור וכפל מטריצות הוא חוג.
כמובן גם חוג האפס.
יותר מזה, $M_n(R)$ מטריצות מעל חוג הוא גם חוג.
גם $\mathbb{F}[x]$ פולינומים מעל שדה הם חוג, מוגדרים על־ידי $\mathbb{F}[x]=\{a_0+a_1x+\cdots+a_nx^n\mid n\in\mathbb{N},a_i\in\mathbb{F}\forall i\}$, עם המוסכמה שלכל $m\geq n$

$$a_0+a_1x+\cdots+a_nx^n=a_0+\cdots+a_nx^n+0x^{n+1}+\cdots+0x^m$$

ולכן זה חוג יחד עם חיבור לפי מקדם ועם כפל פולינומים מהצורה

$$(a_0+\cdots+a_nx^n)\cdot(b_0+\cdots+b_mx^n)=a_0b_0+(a_0b_1+a_1b_0)x+\cdots+(a_nb_m)x^{n+m}$$

כלומר המקדם של x^k במכפלה נתון על־ידי $\sum_{0\leq i\leq n,0\leq j\leq m,i+j=k}a_ib_j$.
גם $R[x]$ הוא חוג מעל כל חוג R, אם הוא חוג קומוטטיבי, למשל $(\mathbb{F}[x])[y]:=\mathbb{F}[x,y]$.

דוגמה 23.2 חוג טורי החזקות $\mathbb{F}[[m]]=\{\sum_{i=0}^\infty a_ix^i\mid a_i\in\mathbb{F}\}$. באותו האופן כמו $\mathbb{F}[x]$. למשל $\mathbb{R}[[x]]$ המוגדר על־ידי $\sum_{n=0}^\infty n!x^n$

הערה $\mathbb{F}[x]$ הוא תת־חוג של $\mathbb{F}[[x]]$.

הערה $\mathbb{F}_2[x]$ הוא חוג אינסופי.

דוגמה 23.3 אם R חוג ו־X קבוצה אז $R^X := \{f : X \to R \mid f \text{ פונקציה}\}$ עם חיבור וכפל בטווח.

$$(f+g)(x) = f(x) + g(x), \qquad (f \cdot g)(x) = f(x) \cdot g(x)$$

דוגמה 23.4 ניקח את $C([0,1];\mathbb{R}) \subseteq \mathbb{R}^{[0,1]}$ הפונקציות הרציפות היא חוג.

דוגמה 23.5 לכל $D \in \mathbb{Z}$ שלילי נוכל להגדיר $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$ כתת־חוג של המרוכבים $\mathbb{C}$.
בפרט $\mathbb{Z}[i] \subseteq \mathbb{C}$ נקרא חוג השלמים של גאוס.

נבחן עתה חוגי חילוק,

$$\mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}$$

חוג הקוורטרניונים, המוגדר על־ידי

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

כאשר $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j$, נבחין כי זהו לא חוג קומוטטיבי. מתברר שזהו חוג החילוק היחיד שהוא חוג חילוק כחזקה סופית של שדה הממשיים.

נשים לב שבקורס זה וכנראה בעולם בכללי חוג הוא בהגדרה וחוג ללא יחידה נקרא פשוט חוג ללא יחידה ולא ממש נעסוק בו.
עוד נבחין שבזמן שהומומורפיזם משמר פעולות, יתכן מצב שבו הוא לא משמר יחידה, לדוגמה

$$\mathbb{R} \hookrightarrow M_2(\mathbb{R}), \qquad a \mapsto \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

ולכן נגדיר

הגדרה 23.4 פונקציה $f : R \to S$ היא הומומורפיזם של חוגים אם

$$\forall x, y \in R, \quad f(x+y) = f(x) + f(y), \qquad f(xy) = f(x) \cdot f(y), \qquad f(1) = 1$$

כל החוגים שלנו הם עם יחידה והומומורפיזמים מעתה מכבדים את היחידה.

הגדרה 23.5 (איזומורפיזם) הומומורפיזם של חוגים נקרא איזומורפיזם אם הוא חד־חד ערכי ועל.

למה 23.6 *אם $f : R \to S$ איזומורפיזם אז $f^{-1} : S \to R$ היא הומומורפיזם (ולכן איזומורפיזם).*

הגדרה 23.7 (שיכון) הומומורפיזם נקרא מונומורפיזם או שיכון אם הוא חד־חד ערכי.

דוגמה 23.6 $f : \mathbb{Z} \to \mathbb{Z}_{/n}$ המוגדרת על־ידי $f(n) = a \mod n$ היא המומורפיזם של חבורות ונראה כי גם של חוגים.

דוגמה 23.7 נראה כי $f : M_d(\mathbb{Z}) \to M_d(\mathbb{Z}_{/n})$ שמפעילה $\mod n$ לכל קורדינטה היא גם הומומורפיזם.

דוגמה 23.8 לכל $a \in \mathbb{F}$ הפונקציה $ev_a : \mathbb{F}[x] \to \mathbb{F}$ המוגדרת על־ידי $ev_a(p(x)) = p(a)$.
כאשר $p(x) = c_0 + c_1x + \cdots + c_nx^n \in \mathbb{F}[x]$, ו־$p(a) = c_0 + \cdots + c_na^n \in \mathbb{F}$.
זהו הומומורפיזם שכן אנחנו בוחרים a קבוע ומשתמשים בחיבור מקדמים וכפל מקדמים יחד עם הקבוע הזה.

דוגמה 23.9 $\det : M_n(\mathbb{F}) \to \mathbb{F}$ היא לא הומומורפיזם של חוגים שכן

$$\det(A+B) \neq \det(A) + \det(B)$$

הגדרה 23.8 בהינתן הומומורפיזם של חוגים $f : R \to S$ נגדיר את התמונה והגרעין

$$\operatorname{Im}(f) := \{f(x) \mid x \in R\}, \qquad \ker(f) := \{x \in R \mid f(x) = 0\}$$

הערה האם $\operatorname{Im}(f) \subseteq S$ תת־חוג? התשובה היא שכן.
האם $\ker(f) \subseteq R$ הוא תת־חוג? הגרעין הוא לא תת־חוג

24 שיעור 19 — 15.7.2024

24.1 תורת החוגים — הומומורפיזמים

הומומורפיזם של חוגים $f:R\to S$ פונקציה שמקיימת $\forall x,y\in R: f(x+y)=f(x)+f(y), f(xy)=f(x)\cdot f(y)$ ואנו דורשים בנוסף מטעמי נוחות וקונבנציה ש־$f(1)=1$.

הגדרנו ש־$\mathrm{Im}(f)=\{f(x)\mid x\in R\}$ ו־$\ker(f)=\{x\in R\mid f(x)=0\}\subseteq R$. אמרנו ש־$\mathrm{Im}(f)$ הוא תמיד תת־חוג של S וגם שהגרעין הוא **לא** תת־חוג של R, בדרך־כלל.

נבחין מההגדרה של חוג שחיבור וכפל משתמרים בגרעין, ונקבל את הלמה הבאה.

למה 24.1 *$\ker(f)$ הוא תת־חוג של R אם ורק אם $f(1)=0$, דהינו אם $S=0$.*

הגדרה 24.2 (אידאל) R חוג, אידאל (Ideal) של R זו תת־קבוצה $I\subseteq R$ כך שמתקיימות התכונות הבאות:

1. I הוא תת־חבורה חיבורית של R
2. לכל $x\in I$ ו־$r\in R$ מתקיים $rx\in I, xr\in I$.

דהינו שהקבוצה שואבת לתוכה תחת פעולת הכפל.

סימון 24.3 נסמן אידאל כמו תת־חבורה נורמלית, על־ידי $I\triangleleft R$, וזה גם בגדול המושג המקביל.

למה 24.4 *עבור הומומורפיזם של חוגים $f:R\to S$ מתקיים ש־$\ker(f)$ הוא אידאל של R, דהינו $\ker(f)\triangleleft R$.*

הוכחה. אנו כבר יודעים כי זוהי חבורה חיבורית ואם $x\in\ker(f)$ ו־$r\in R$ אז $f(rx)=f(r)f(x)=f(r)\cdot 0=0$ ובדומה נקבל גם $f(xr)=0$. $\square$

עתה נבנה חוג מנה

הגדרה 24.5 (חוג מנה) R חוג ו־$I\triangleleft R$. נגדיר על R/I מבנה של חוג כך שיתקיים

1. כחבורה חיבורית זו חבורת המנה

$$(a+I)+(b+I)=(a+b)+I$$

2. נשים לב

$$(a+I)(b+I)=ab+aI+Ib+I^2\subseteq ab+I$$

אבל ממש לא בהכרח שווה, בגלל I^2 שאיננו בהכרח I עצמו.
נגדיר $(a+I)\cdot(b+I):=ab+I$.

טענה 24.6 *R/I חוג עם הפעולות שהוגדרו, וההטלה $\pi:R\to R/I$ המוגדרת על־ידי $\pi(r)=r-I$ הומומורפיזם של חוגים.*

הוכחה חלקית. $(R/I,+)$ אכן חבורה חיבורית אבלית.
נבדוק נייטרלי לכפל $1+I$ שכן מתקיים

$$(1+I)(a+I)=1a+I=a+I$$

וכמובן זה נכון גם בכיוון ההפוך של המכפלה.
נבדוק אחד מחוקי הפילוג והשאר הם תרגיל.
פילוג משמאל:

$$\begin{aligned}(a+I)((b+I)+(c+I)) &= (a+I)((b+c)+I)=a(b+c)+I\\ =ab+ac+I &= ((ab)+I)+((ac)+I)=(a+I)(b+I)+(a+I)(c+I)\end{aligned}$$

לכל $x,y\in R$ נקבל

$$\pi(xy)=xy+I=(x+I)(y+I)=\pi(x)\cdot\pi(y),\qquad \pi(1)=1+I,\qquad \pi(x+y)=\pi(x)+\pi(y)$$

$\square$

דוגמה 24.1 ננסה לחשב את $GL_n(\mathbb{R})/SL_n(\mathbb{R})$, ממשפט האיזומורפיזם הראשון נקבל ש־$\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$ אז $\ker(f) \simeq SL_n(\mathbb{R})$, השאל איך בונים הומומורפיזם כזה, אז נקבל $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^\times$.

נעבור לדבר על אידאלים באופן כללי.

למה 24.7 *R חוג ו־$I \lhd R$, עבור $\alpha \in S$ משפחה של אידאלים, אז גם $\bigcap_{\alpha \in S} \alpha$ גם אידאל.*

הוכחה בתרגיל.

הגדרה 24.8 R חוג ו־$X \subseteq R$ תת־קבוצה, האידאל שנוצר על־ידי X ב־R מוגדר להיות

$$(X) := \bigcap_{X \subseteq I \lhd R} I \lhd R$$

דוגמה 24.2 אם $r \in R$ אז

$$(r) = \bigcap_{r \in I \lhd R} I = \left\{ \sum_{i=1}^{n} a_i r b_i \mid n \in \mathbb{N}, a_i b_i \in \mathbb{R} \right\}$$

זהו האידאל הנוצר על־ידי איבר בודד.

הערה אם R קומומוטטיבי אז

$$(r) = \{ar \mid a \in R\} = rR$$

טענה 24.9 *האידאלים של $\mathbb{Z}$ הם בדיוק התת־קבוצות $n\mathbb{Z}$.*

הוכחה. אלה התת־חבורות החיבוריות של $\mathbb{Z}$ והן כולן אידאלים. $\square$

טענה 24.10 *אם $\mathbb{F}$ שדה אז האידאלים היחידים בו הם $\mathbb{F}$ ו־$\{0\}$.*

הוכחה. אם $0 \neq x \in I \lhd \mathbb{F}$ אז לכל $y \in \mathbb{F}$ נקבל $I = \mathbb{F} \implies y = (yx)^{-1}x \in I$. $\square$

משפט 24.11 (משפט האיזומורפיזם הראשון לחוגים) *עבור הומומורפיזם חוגים $f : R \to S$ מתקיים*

$$R/\ker(f) \simeq \operatorname{Im}(S)$$

ובראי העתקות הטלה, נקבל $x + \ker(f) \mapsto f(x)$.

הוכחה. בנינו כבר העתקה $\varphi : R/\ker(f) \xrightarrow{\sim} \operatorname{Im}(S)$. כחבורה חיבורית ונותר רק לבדוק שהיא משמרת כפל ויחידה.

$$\varphi((x+I)(y+I)) = f(xy+I) = f(xy) + I, \qquad \varphi(x+I)\varphi(y+I) = f(x)f(y)$$

ומצאנו כי הם שווים, נבדוק יחידה

$$\varphi(1+I) = \varphi(1) = 1$$

ולמעשה מצאנו כי כלל התכונות משתמרות. $\square$

אנחנו צריכים להסתכל על חוגים כעל חבורות אבליות עם ההרחבה של פעולה כפלית והתנהגות יותר ספציפית, ככה למשפטי האיזומורפיזם יש יותר משמעות והיגיון בהקשר של חבורות.

דוגמה 24.3 פעולת ההצבה בפולינום עבור $a \in \mathbb{F}$ היא $ev_a : \mathbb{F}[x] \to \mathbb{F}$ המוגדרת על־ידי $P(x) \mapsto P(a)$.
באופן דומה, $\varphi : \mathbb{R}[x] \to \mathbb{C}$ על־ידי $f(x) \mapsto f(i)$, הוא הומומורפיזם תקין ושנוכל לקבל ממנו ערכים מרוכבים. נטען כי

$$\operatorname{Im}(\varphi) = \mathbb{C}$$

שכן

$$\varphi(a+bx) = a+bi, \varphi(-1) = -1, \varphi(x^2) = -1, \varphi(x^2+1) = 0$$

ולכן $\mathbb{R}[x]/\ker(\varphi) \simeq \mathbb{C}$.

למה 24.12 $\ker(\varphi) = (x^2+1)$

הוכחה. ראינו ש־$x^2+1 \in \ker(\varphi)$ ולכן $(x^2+1) \subseteq \ker(\varphi)$.
אם $f(i)=0$ אז $(x-i) \mid f(x)$ ב־$\mathbb{C}[x]$ אבל ל־f מקדמים ממשיים ולכן $0=\overline{0}=\overline{f(i)}=f(-i)$ ולכן $x+1 \mid f(x)$. לכן $(x-i)(x+i) \mid f(x)$, דהינו $x^2+1 \mid f(x)$.
אזהרה: ההנחה השתמשה בתכונות של $\mathbb{C}[x]$. $\square$

מסקנה 24.13 $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$

25 שיעור 20 — 17.7.2024

25.1 חוגים — הומומורפיזמים המשך

נזכיר את משפט האיזומורפיזם הראשון לחוגים עליו דיברנו בשיעור הקודם

משפט 25.1 (משפט האיזומורפיזם הראשון לחוגים) *עבור הומומורפיזם של חוגים $f : R \to S$ מתקיים*

$$R/\ker(f) \xrightarrow{\sim} \operatorname{Im}(f), \qquad x + \ker(f) \mapsto f(x)$$

ישנם כמובן משפטי איזומורפיזם מקבילים לשני והשלישי.

משפט 25.2 (משפט האיזומורפיזם השני לחוגים) *R חוג ו־$I \triangleleft R$ אידאל ו־$S \subseteq R$ תת־חוג, אז מתקיים:*

1. *$I \cap S \triangleleft S$ אידאל*
2. *$I + S \subseteq R$ תת־חוג*
3. *$S/(I \cap S) \simeq (I + S)/I$*

משפט 25.3 (משפט האיזומורפיזם השלישי לחוגים) *R חוג ו־$I, J \triangleleft R$ כך ש־$I \subseteq J$ אז*

1. *$R/J \triangleright R/I$*
2. *$(R/I)/(J/I) \simeq R/J$*

דוגמה 25.1 (דוגמה למשפט האיזומורפיזם השני) $R = \mathbb{C}[x]$ ו־$R \triangleright I = (x) = \{a_1 x + \cdots + a_n x^n \mid a_1, \ldots, a_n \in \mathbb{C}\}$, יחד עם $R \supseteq S = \mathbb{R}[x]$. נוכל להסתכל על $S \cap I$, כל הפולינומים הממשיים שמתחלקים ב־x, ונוכל לבחון את $I + S$ שהיא קבוצת הפולינומים עם מקדם חופשי ממשי. נקבל מהמשפט כי $S/(S \cap I) \simeq (I + S)/I$. נבחין כי נקבל שמתקיים

$$R/I = \mathbb{C}[x]/(x) \simeq \mathbb{C}$$

שכן לקחנו את כל הפולינומים המרוכבים וכל מה שמתחלק מאיקס הכרזנו עליו כאפס, ונשאר למעשה רק המקדם החופשי עצמו בלבד. לכן גם בשוויון שקיבלנו קודם נקבל פעמיים את המספרים המרוכבים.

משפט 25.4 (משפט ההתאמה לחוגים) *אם R חוג ו־$I \triangleleft R$ אז יש התאמה חד־חד ערכית ועל*

$$\{\overline{J} \triangleleft R/I\} \simeq \{I \subseteq J \triangleleft R\}$$

ו־$\overline{J} \mapsto \pi^{-1}(\overline{J})$ כאשר $\pi : R \to R/I$.

ניזכר במשפט השאריות הסיני שראינו כבר, מתברר כי הוא מתקיים גם עבור חוגים

משפט 25.5 (משפט השאריות הסיני לחוגים) *אם n, m מספרים זרים אז*

$$\mathbb{Z}_{/nm} \simeq \mathbb{Z}_{/n} \times \mathbb{Z}_{/m}$$

כאיזומורפיזמים של חוגים.

הגדרה 25.6 (קבוצת ההפיכים כפלית) R חוג אז $R^\times \subseteq R$ היא קבוצת האיברים ההפיכים כפלית.

נבחין כי אם $\mathbb{F}$ שדה אז נקבל $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$.

טענה 25.7 *$R^\times$ חבורה ביחס לכפל.*

מסקנה 25.8 נסיק ממשפט השאריות הסיני כי לכל $n, m \in \mathbb{N}$ זרים מתקיים

$$(\mathbb{Z}_{/nm})^\times \simeq (\mathbb{Z}_{/n})^\times \times (\mathbb{Z}_{/m})^\times$$

הוכחה. $\mathbb{Z}_{/nm} \xrightarrow{\sim} \mathbb{Z}_{/n} \times \mathbb{Z}_{/m}$ ולכן נסיק כי גם $(\mathbb{Z}_{/nm})^\times \xrightarrow{\sim} (\mathbb{Z}_{/n} \times \mathbb{Z}_{/m})^\times$. והביטוי האחרון הוא כמובן שקול לפירוק הכפלי שלהם. $\square$

דוגמה 25.2 נבחן את $(\mathbb{Z}_{/8})^\times = \{1, 3, 5, 7\}$. נבדוק את הסדרים של המספרים, נראה כי $1^2 = 1$, כי $3^2 \cong 1$ וכך גם $5^2 \cong 7^2 \cong 1$, דהינו כל האיברים הם מסדר 2.

דוגמה 25.3 נקבל גם עבור $n = p_1^{d_1} \cdots p_r^{d_r}$ כי
$$(\mathbb{Z}_{/n})^\times \simeq (\mathbb{Z}_{/p_1^{d_1}})^\times \times \cdots \times (\mathbb{Z}_{/p_r^{d_r}})^\times$$
ואנו יודעים כי
$$|(\mathbb{Z}_{/p^d})^\times| = p^d - p^{d-1} = p^{d-1}(p-1)$$
ולכן נקבל כי $\varphi(n) := |(\mathbb{Z}_{/n})^\times| = \prod_{i=1}^r p_i^{d_i-1}(p_i-1)$ וזו נקראת פונקציית פי של אוילר.

הגדרה 25.9 R חוג ו־$I, J \lhd R$ אז נגדיר
$$I + J = \{a+b \mid a \in I, b \in J\}, \qquad I \cdot J = \{\sum_{i=1}^n a_i b_i \mid a_i \in I, b_i \in J\}$$

טענה 25.10 *גם $I + J, I \cdot J$ הם אידאלים.*

משפט 25.11 (משפט השאריות הסיני לחוגים) *יהי R חוג קומוטטיבי ו־$I, J \lhd R$ כך ש־$I + J = R$ אז*
$$R/(I \cdot J) \simeq (R/I) \times (R/J)$$

הוכחה.
$$\pi_I : R \to R/I, \qquad \pi_J : R \to R/J$$
ונגדיר
$$\pi : R \to R/I \times R/J$$
על־ידי
$$\pi(x) = (\pi_I(x), \pi_J(x))$$
צריך להראות ש־π על ו־$\ker(\pi) = I \cdot J$ נקבע על־ידי איזו הראשון:
$$R/(I \cdot J) \simeq R/I \times R/J$$
מתקיים
$$\ker(\pi) = \ker(\pi_I) \cap \ker(\pi_J) = I \cap J$$
הערת צד: $I \cdot J \subseteq I \cap J$ ולפעמים $I \cdot J \neq I \cap J$, למשל $(2\mathbb{Z})(2\mathbb{Z}) = 4\mathbb{Z}$ אבל $2\mathbb{Z} \cap 2\mathbb{Z} = 2\mathbb{Z}$.

מתקיים $I \cdot J \subseteq I \cap J$, ונראה שגם ההכפלה ההפוכה מתקיימת. נבחר איברים $a \in I, b \in J$ כך ש־$a + b = 1$, לכל $r \in I \cap J$ מתקיים $r = r \cdot 1 = \overbrace{r \cdot a}^{\in I \cdot J} + \overbrace{r \cdot b}^{I \cdot J} \in I \cdot J$. הוכחנו כי הגרעין הוא המכפלה, וההוכחה ש־π על תהיה בתרגיל. ☐

25.2 חוגים קומוטטיביים

ההבדל ביניהם לשדה הוא שלא קיים בהכרח הופכי לכל איבר שונה מאפס. אם R הוא חוג קומוטטיבי ו־$a \in R$ אז נוכל לבחון את הפונקציה $f_a : R \to R$ המקיימת $f_a(x) = ax$.

למה 25.12 *a הפיך אם ורק אם f_a פונקציה הפיכה, דהינו חד־חד ערכית ועל.*

הוכחה. אם a הפיך אז $f_{a^{-1}}$ היא הופכית של f_a:
$$f_{a^{-1}}(f_a(x)) = a^{-1}ax = x, \qquad f_a(f_{a^{-1}}(x)) = aa^{-1}x = x$$
מצד שני, אם f_a חד־חד ערכית ועל. קיים איבר $b \in R$ עבורו $f_a(b) = 1 = ab = ba$ ולכן b הופכי של a. ☐

למה 25.13 *$f_a : R \to R$ לא חד־חד ערכית אם ורק אם קיים $0 \neq b \in R$ עבורו $ab = 0$.*

הוכחה. אם קיים b כזה אז $f_a(b) = 0 = f_a(0)$.

מצד שני אם קיימים $b \neq c$ שונים ב־R כך ש־$ac = f_a(b) = f_a(c) = ac$ אז $f_a(b-c) = ab - ac = 0$. ☐

הגדרה 25.14 (מחלק אפס) R חוג קומוטטיבי, $0 \neq a \in R$ נקרא **מחלק אפס** (zero divisor) אם קיים $0 \neq b \in R$ כך ש־$a \cdot b = 0$.
R חוג קומוטטיבי נקרא **תחום שלמות** (Integral domain) אם אין בו מחלק אפס.

דוגמה 25.4 נראה כי הבאים הם תחומי שלמות. שדה, תת־חוג של שדה, למשל $\mathbb{Z}$. וגם $\mathbb{F}[x]$ ל־$\mathbb{F}$ שדה.

דוגמה 25.5 (דוגמות נגדיות) $\mathbb{Z}_{/4}$ שכן $2 \cdot 2 = 0$.

הגדרה 25.15 (איבר נילפוטנטי ואידמפוטנטי) R חוג קומוטטיבי, $x \in R$ נקרא

1. **נילפוטנטי** אם קיים $n \in \mathbb{N}$ כך ש־$x^n = 0$.
2. **אידמפוטנטי** אם $x^2 = x$, דהינו $x(1-x) = 0$, במקרה זה נוכל להגדיר $y = 1 - x$ ולקבל $y^2 = y$ ו־$x + y = 1$, וזהו נקרא האידמפוטנט המשלים.

26 שיעור 21 — 22.7.2024

26.1 חוגים קומוטטיביים

תרגיל 26.1 אילו $n \in \mathbb{N}$ ניתן לכתוב בצורה $n = a^2 + b^2$ כאשר $a, b \in \mathbb{N}$.

על שאלה זו נענה בהרצאה הבאה.

ניזכר כי ההבדל היחיד בין שדות לחוגים קומוטטיביים הוא עניין ההפיכות, בשדה כל האיברים ששונים מאפס הם הפיכים. לכן זו גם התופעה המעניינת בהפרש הזה בין שני התחומים. דיברנו גם על תחומי השלמות, המוכלים בחוגים, והמכילים שדות. בתחום שלמו נקבל $ab = 0 \implies a = 0 \lor b = 0$, דהינו ניתן לצמצם. נקבל גם $ab = ac \land a \neq 0 \implies b = 0$. דיברנו גם על איבר נילפוטנטי ועל איבר אידמפוטנטי. נראה עתה דוגמות לאיברים אידמפוטנטיים.

דוגמה 26.1 נבחן את מכפלת החוגים $R \times S$, ונבחר $x = (1, 0)$, הוא למעשה לא אפס ולא אחד, ונקבל $(1 - x) = (0, 1)$.

דוגמה 26.2 נבחן את $\mathbb{Z}_{/6}$ ונבחין כי $3^2 \cong 9 \cong 3 (\mod 6)$.

נגדיר איזומורפיזם $\mathbb{Z}_{/6} \xrightarrow{\sim} \mathbb{Z}_{/3} \times \mathbb{Z}_{/2}$ ונראה כי אם $(1, 0) \mapsto 3$ אז נקבל $(0, 1) \mapsto 4$ ולמעשה נוכל להסיק בכללי את הטענה הבאה.

טענה 26.1 *R חוג קומוטטיבי ו־$x \in R$ אידמפוטנטי אז קיים $\varphi : R \to R_1 \times R_2$ איזומורפיזם כך ש־$\varphi(x) = (1, 0)$.*

הוכחה. נבחן את $R \xrightarrow{\pi_2} R_2 = R/(x)$. נגדיר $R \xrightarrow{\pi_1} R_1 = R/(1 - x)$.
כמובן נגדיר $\varphi = (\pi_1, \pi_2)$, דהינו $\varphi : R \to R_1 \times R_2$. מתקיים

$$(x) + (1 - x) = R, \qquad x + 1 - x = 1$$

ולכן נוכל להסיק ממשפט השאריות הסיני כי φ איזומורפיזם. זאת מכיוון ש־$R/((x) \cdot (1 - x)) \simeq R_1 \times R_2$.
נותר לשים לב ש־$(0) = (x - x^2) = (x) \cdot (1 - x)$. □

כך לדוגמה בתהליכי פירוק לראשוניים משתמשים ברעיון הזה כדי לחשב מספרים אידמפוטנטיים מעל חבורת $\mathbb{Z}_{/n}$ לכל מספר טבעי.

דוגמה 26.3 ראינו כי $\mathbb{F}[x]/(x^2 + 1) \simeq \mathbb{C}$, ומצד שני דנו בשאלה מה מייצג $\mathbb{R}[x]/(x^2 - 1)$, שזוהי הוספה למעשה של איבר קיים לחוג הפולינומים, וזו שאלה הרבה פחות טריוויאלית. נבחין כי $(x - 1)$ נמצא במנה הזאת שכן הוא לא מתחלק במנה, וכך גם $(x + 1)$, אבל מכפלתם היא אפס תחת החוג, דהינו $(x - 1)(x + 1) = 0$ במנה זו, ובכללי נקבל כי $\mathbb{R}[x]/(x^2 - 1) \simeq \mathbb{R} \times \mathbb{R}$.
זאת שכן ממשפט השאריות הסיני נקבל $\mathbb{R}[x] = (\{x-1\}) + (\{x+1\})$, דהינו $\mathbb{R}[x]/(x^2-1) \simeq (\mathbb{R}[x]/(x-1)) \times (\mathbb{R}[x]/(x+1)) \simeq \mathbb{R} \times \mathbb{R}$ שכן זוהי מכפלה של פולינומים שמתאפסים באחת ופולינומים שמתאפסים ב־-1. רעיונית המנה הזאת היא המקרה שבו הפולינום אכן מתאפס, ולכן הוא מתאפס או באחת או במינוס אחת ולכן יש לנו למעשה מכפלה של המקרים בהם האיבר הראשון אפס ומקרים בהם האיבר השני אפס. כהסבר מוסף נראה ש־$(\{x^2 - 1\}) = (\{x - 1\}) \cap (\{x + 1\})$.

מה יקרה אם ננסה להוסיף שורש למספר שכבר יש לו שורש יחיד, לדוגמה $\mathbb{R}[\epsilon] := \mathbb{R}[x]/(x^2)$ כאשר $\epsilon = x + x^2\mathbb{R}[x]$ והוא מקיים ש־$\epsilon^2 = 0$. נקבל ש־$\mathbb{R}[\epsilon] = \{a + h\epsilon \mid a, h \in \mathbb{R}\}$. הדבר הזה הוא מעין גרסה אלגברית של מספר אינפיניטסמלי, בעצם זה שאנו אומרים שהריבוע שלו הוא אפס אנו אומרים שהוא "קטן". נראה כי $f(x) + x^2\mathbb{R}[x] = g(x) + x^2\mathbb{R}[x]$, דהינו אם $f(x) - g(x) \in x^2\mathbb{R}[x]$, אז אם $f(x) = a + bx + x^2h(x)$ אז $f(x) + x^2\mathbb{R}[x] = a + bx + x^2\mathbb{R}[x]$. החוג הזה נקרא Dual numbers.

תרגיל 26.2 יהי $f(x) \in \mathbb{R}[x]$, וננסה להציב איבר מהסוג הזה, נכתוב $f(a + h\epsilon) = f(a) + hf'(a)\epsilon$, ויש להבין למה זה נכון ומה המשמעות של זה.

הגדרה 26.2 (ניל־רדיקל) R חוג קומוטטיבי, נגדיר $N(R) = \{x \in R \mid \exists n \in \mathbb{N}, x^n = 0\}$ והיא נקראת הקבוצה **הניל־רדיקל** של R.

טענה 26.3 *$N(R)$ היא אידאל של R.*

הוכחה. נבדוק סגירות לכפל, $x \in N(R)$ ויהי $y \in R$ אז קיים $n \in \mathbb{N}$ כך ש־$x^n = 0$ ולכן $(xy)^n = x^n y^n = 0y^n = 0$ ולכן גם $xy \in N(R)$.
נבדוק סגירות לחיבור, $x, y \in N(R)$ אז קיימים $n, m \in \mathbb{N}$ כך ש־$x^n = y^m = 0$. לכן $(x + y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}$ ולכל k נקבל או $k \geq n$ או ש־$n + m - k \geq m$ ולכן $x^k y^{n+m-k} = 0$ ונקבל $x + y \in N(R)$. □

הגדרה 26.4 (חוג מצומצם) R חוג קומוטטיבי נקרא **מצומצם** (Reduced) אם $N(R) = \{0\}$.

בתרגיל נראה ש־$R/N(R)$ הוא מצומצם.

הגדרה 26.5 נניח ש־R חוג קומוטטיבי ו־$I \triangleleft R$ אז

1. I נקרא **מקסימלי** אם ורק אם לכל $I \subseteq J \triangleleft R$ מתקיים $J = R$ או $J = I$.
2. I נקרא **ראשוני** אם לכל $x, y \in R$ אם $x \cdot y \in I$ אז $x \in I$ או $y \in I$.

טענה 26.6 *R חוג קומוטטיבי ו־$I \triangleleft R$ כך ש־$I \neq R$ אז*

1. *R/I שדה אם ורק אם I מקסימלי*
2. *R/I תחום שלמות אם ורק אם I ראשוני*

הוכחה. **1.** $R/I \neq \{0\}$ שכן I אידאל ממש ולכן R/I שדה אם ורק אם אין בו אידאלים שהם לא האידאל הטריוויאלי, וזה בתרגיל. לכן ממשפט ההתאמה זה אם ורק אם אין אידאלים $I \subseteq J \triangleleft R$

2. R/I תחום שלמות אם ורק אם לכל $y, x \in R$ מתקיים $(x+I)(y+I) = I \implies x + I = I \vee y + I = I$. כלומר, אם ורק אם $xy \in I \implies x \in I \vee y \in I$. □

אם $R = \mathbb{Z}$ אז יש סוגיה קצת מרגיזה ש־$6 = 2 \cdot 3 = (-2)(-3)$ ויש קצת תסבוכת עם הסימנים, אנו יכולים לבחור לייצג את המספרים על־ידי חיוביים ומינוס יחיד ככה שנקבל יצוג יחיד וקאנוני.

הגדרה 26.7 (חברים) R תחום שלמות. $x, y \in R$ נקראים **חברים** אם קיים $u \in R^\times$ כך ש־$y = xu$ ומסמנים $x \sim y$, וזהו יחס שקילות.

דוגמה 26.4 ב־$\mathbb{Z}$ נקבל $n \sim -n$ בלבד, ב־$\mathbb{R}[x]$ מתקיים $x^2 - 3 \sim 2x^2 - 6$. ב־$\mathbb{Z}[i]$ מתקיים $x - i \sim ix + 1$.

הגדרה 26.8 (מחלק) נאמר ש־x מחלק את y אם קיים $z \in R$ עבורו $y = xz$ ונסמן $x \mid y$.

הגדרה 26.9 (פירוק) **פירוק** של x זו הצגה $x = yz$ ונאמר שהפירוק **אמיתי** אם y ו־z לא הפיכים.

הגדרה 26.10 (אי־פריק וראשוני) x נקרא **אי־פריק** אם הוא לא הפיך ואין לו פירוק אמיתי. x נקרא **ראשוני** אם הוא לא הפיך ולכל $0 \neq y, z \in R$ מתקיים $x \mid yz \implies x \mid y \vee x \mid z$.

הטענה שלנו היא שאת כל המונחים האלה אפשר לטעון במונחים של אידאלים.

טענה 26.11 *$x, y, z \in R$ איברים בחוג.*

1. $x \in R^\times \iff (x) = R$
2. $x \mid y \iff (x) \supseteq (y)$
3. $x \sim y \iff (x) = (y)$
4. *x אי־פריק (ולא הפיך לפי דרישה) אם ורק אם לכל $y \in R$ אם $(x) \subseteq (y) \triangleleft R$ אז $(y) = R \vee (x) = (y)$*
5. *x ראשוני אם ורק אם (x) ראשוני*

הוכחה. **1.** $x \in R^\times \iff x \mid 1 \iff R = (1) \subseteq (x) \subseteq R \iff (x) = R$

2. $x \mid y$ אם ורק אם קיים $z \in R$ כך ש־$y = xz$ אם ורק אם $y \in (x)$ אם ורק אם $(y) \subseteq (x)$

3. $x \sim y \overset{\text{בתרגיל}}{\iff} x \mid y \wedge y \mid x \iff (y) \subseteq (x) \wedge (x) \subseteq (y) \iff (x) = (y)$ □

27 שיעור 22 — 24.7.2024

27.1 חוגים — המשך

למה 27.1 *R תחום שלמות, ו־$0 \neq x \in R$.*
$x = yz$, מתקיים ש־y הפיך אם ורק אם $x \sim z$.

הוכחה. אם y הפיך אז $x \sim z$ לפי הגדרה. מצד שני, אם $x \sim z$ אז קיים $u \in R^\times$ כך ש־$z = xu$, ולכן נקבל $x = yz = yux$, מכיוון ש־$x \neq 0$ אז נקבל $yu = 1$ ובפרט y הפיך. $\square$

טענה 27.2 *R תחום שלמות, ויהיו $a, b \in R$, אז*

1. *$a \in R^\times$ הפיך אם ורק אם $R = (a)$*
2. *$a \mid b \iff (b) \subseteq (a)$*
3. *$a \sim b \iff (a) = (b)$*
4. *a אי־פריק אם ורק אם לכל $(a) \subseteq (b) \subseteq R$ מתקיים $(a) = (b)$ או $R = (b)$*
5. *a ראשוני אם ורק אם (a) ראשוני, דהינו אם הוא מחלק מכפלה הוא מחלק את אחד המוכפלים אם ורק אם האידאל ראשוני, דהינו שכשמחלקים בו מקבלים תחום שלמות*

הוכחה (המשך). **4.** a אי־פריק אם ורק אם אין לו פירוק אמיתי, אם ורק אם לכל $b \mid a$ מתקיים b הפיך או ש־$a \sim b$, לפי 1 ו־3 סיימנו.

5. a ראשוני אם ורק אם לכל $b, c \in R$ אם $a \mid bc$ אז $a \mid b$ או $a \mid c$. נסמן לכל $x \in R$ ב־$\overline{x}$ את תמונתו תחת ההטלה $R \to R/(a)$ ונקבל ש־a ראשוני אם ורק אם לכל זוג איברים $b, c \in R/(a)$ מתקיים $\overline{b}\overline{c} = 0$ אז $\overline{b} = 0$ או $\overline{c} = 0$, כלומר אם ורק אם $R/(a)$ תחום שלמות. $\square$

איזה סוג שאלות מעניין אותנו בהקשר למושגים האלה? בעולם של מספרים ראשוניים רגילים, אנחנו רגילים שהתכונה של ראשוניות שקולה לתכונה של אי־פריקות, אבל שתי התכונות האלה לא שקולות, רק עומדות ביחס גרירה.

טענה 27.3 *אם R חוג שלמות, כל $x \in R$ שהוא ראשוני הוא אי־פריק.*

הוכחה. אם נניח ש־$x = yz$, אז בפרט $x \mid yz$, ולכן בלי הגבלת הכלליות מהראשוניות $x \mid y$ ולכן $y = xw$. נקבל

$$x = yz = xwz$$

ולכן $wz = 1$, כלומר $z \in R^\times$ ועל־כן הפירוק $x = yz$ הוא לא אמיתי. $\square$

דוגמה 27.1 נבחן את $M = \{n \in \mathbb{N} \mid n \cong 1 (\mod 3)\} = \{1, 4, 7, 10, 13, \dots\}$ עם פעולת הכפל.
נראה ש־$10 \mid 4 \cdot 25$ אבל 10 לא מחלק לא את 4 ולא את 25, ולכן הוא לא ראשוני, אבל 10 כן אי־פריק, שכן הוא לא ניתן לכתיבה על־ידי מכפלת איברים לא הפיכים. נראה גם שאפשר לכתוב את $100 = 10 \cdot 10$, מכפלה של שני גורמים אי־פריקים, אבל גם $100 = 4 \cdot 25$, ובקבוצה זו (שהיא לא הטבעיים) פירוק זה הוא שונה.

הגדרה 27.4 (פירוק) R תחום שלמות, ו־$x \in R$.

1. **פירוק** של x לאי־פריקים זו משוואה מהצורה $x = y_1 y_2 \cdots y_n$ כאשר $y_1, \dots, y_n$ אי־פריקים
2. שני פירוקים לאי־פריקים $x = y_1 \cdots y_n = z_1 \cdots z_n$ הם **שקולים** אם $n = m$ ואחרי שינוי סדר $z_i \sim y_i$ לכל $1 \leq i \leq n$
3. נגדיר של־x יש פריקות **חד־ערכית** אם יש לו פירוק לאי־פריקים וכל שניים כאלה שקולים
4. R נקרא **תחום פריקות חד־ערכית** (UFD — unique factorization domain) אם לכל $0 \neq x \in R$ ולא הפיך יש פריקות חד־ערכית

טענה 27.5 *R תחום שלמות שבו לכל איבר לא הפיך ושונה מאפס יש פירוק לאי־פריקים, אז R תחום פריקות חד־ערכית אם ורק אם כל אי־פריק שונה מאפס הוא ראשוני.*

הוכחה. נניח ש־R הוא UFD, ו־$x \in R$ אי־פריק. בהינתן $x \mid yz$, קיים $w \in R$ עבורו $xw = yz$. נפרק את y, z, w לגורמים אי־פריקים ונקבל $y = y_1 \cdots y_m, w = w_1 \cdots w_n, z = z_1 \cdots z_k$. מפריקות חד־ערכית נקבל $x \sim y_i \iff x \mid y$ או $x \sim z_i \iff x \mid z$ לאיזשהו i.

בכיוון ההפוך, נניח שכל אי־פריק שונה מאפס הוא ראשוני ויש פירוק לאי־פריקים. יהיו $x = x_1 \cdots x_n, y = y_1 \cdots y_m$ כך שכל האיברים אי־פריקים. צריך להראות שהפירוקים שונים. $y \mid x_1$ ולכן בלי הגבלת הכלליות $x_1 \mid y_1$, כלומר $y_1 = x_1 \cdot w$ ומכיוון ש־y_1 אי־פריק w הפיך, דהינו $x = (wx_1)y_2 \cdots y_m$ ונוכל לצמצם ולקבל $x = y \implies$ $x_2 \cdots x_n = (wy_2) \cdots y_m$ כאשר wy_2 אי־פריק. באינדוקציה על n שני הפירוקים הללו הם שקולים ולכן גם המקוריים. □

הגדרה 27.6 R נקרא **תחום ראשי** (PID — Principal Ideal Domain) אם הוא תחום שלמות שבו כל אידאל הוא ראשי (נוצר על־ידי איבר אחד).

דוגמה 27.2 דוגמות לתחומים ראשיים:

1. $\mathbb{Z}$
2. שדה $\mathbb{F}$
3. $\mathbb{F}[x]$

לעומת זאת דוגמות נגדיות, $\mathbb{F}[x, y]$, האידאל (x, y) לא ראשי.

בכללי ההתנהגות הזאת של תחום ראשי זה משהו שקורה רק כשהמימד הוא 1, וסוג של מבדל אותם.

משפט 27.7 *כל PID הוא UFD*

הוכחה. לכל $x \in R$ לא הפיך ושונה מאפס נראה שקיים פירוק לאי־פריקים.

נניח בשלילה ש־x פריק ולכן $x = x_1y_1$ פירוק אמיתי. אם ל־x_1 ול־y_1 היה פירוק לאי־פריקים גם ל־x היה ולכן בלי הגבלת הכלליות ל־x_1 אין פירוק כזה ובפרט $x_1 = x_2y_2$ פירוק אמיתי. נקבל כי $\cdots \mid x_2 \mid x_1 \mid x$ ולכן $\ldots \subsetneq (x_2) \subsetneq (x_1) \subsetneq (x)$.

נסתכל על האידאל $R \rhd I = \bigcup_{n=1}^{\infty} (x_n)$ אך מכיוון ש־R הוא PID נקבל $I = (y)$, ולכן ישנו $n \in \mathbb{N}$ עבורו $y \in (x_n)$, וזו סתירה כי אז $I = (x_n) = (x_{n+1})$.

כעת נראה שכל אי־פריק הוא ראשוני. x אי־פריק גורר ש־(x) מקסימלי מבין הראשיין ולכן מ־PID נובע (x) מקסימלי ולכן (x) ראשוני. לכן $R/(x)$ שדה ולכן בפרט גם תחום שלמות ולכן נובע כי x ראשוני. □

מסקנה 27.8 $\mathbb{Z}$ ו־$\mathbb{F}[x]$ הם UFD.

משפט 27.9 (משפט שלא נוכיח) *R הוא UFD אז $R[x]$ הוא UFD.*

בפרט $\mathbb{F}[x, y] = (\mathbb{F}[x])[y]$ הוא UFD.

נחזור לענות על השאלה מה תוכן הקבוצה $S = \{a^2 + b^2 \mid a, b \in \mathbb{N}\}$.

משפט 27.10 *$n \in S$ אם ורק אם בפירוק שלו לראשוניים כל ראשוני שהוא 3 מודולו 4 מופיע בחזקה זוגית.*

כשאנחנו ניגשים למשוואה כזו, $a^2 + b^2 = n$, שהיא משוואה של שלמים, נרצה לבחון אותה מעל מודולו כדי לנסות להבין מה הולך איתה. במקרה זה נבדוק את $a^2 + b^2 \cong n(\mod 4)$, נקבל שאם $n \cong 3(\mod 4)$ אז $n \notin S$. נשתמש גם בטענה הבאה

טענה 27.11 *אם $n, m \in S$ אז $nm \in S$.*

הוכחה. נניח ש־$n = a^2 + b^2, m = c^2 + d^2$. ניקח את $(ac - bd)^2 + (ad + bc)^2 = a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 = (a^2 + b^2)(c^2 + d^2) = n \cdot m$. □

הדבר הזה מזכיר מאוד כפל של מרוכבים, וזה לא במקרה, נראה שמתקיים

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

הרעיון הוא שאפשר להזתכל על החוג $\mathbb{Z}[i]$, ונגדיר את $N : \mathbb{Z}[i] \to \mathbb{N}$ המוגדרת על־ידי

$$N(a + bi) = a^2 + b^2 = (a + bi)(a - bi) = \|a + bi\|^2$$

ומתקיים $N(xy) = N(x)N(y)$, ולכן $S = \operatorname{Im}(N)$. אז נשאל את עצמנו מהם האיברים ההפיכים ב־$\mathbb{Z}[i]$, ונקבל $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$. אם $a + bi$ הפיך אז $N(a + bi) = 1 = a^2 + b^2$.

טענה 27.12 *עבור p אי־זוגי וראשוני, $p \in S$ אם ורק אם $p \cong 1(\mod 4)$.*

למה 27.13 *p ראשוני אי־זוגי הוא פריק ב־$\mathbb{Z}[i]$ אם ורק אם $p \cong 1 \pmod 4$.*

כל מיני עובדות שלא נוכיח אבל משתמש בהן:

1. $\mathbb{Z}[i]$ הוא תחום ראשי ולכן UFD
2. $\mathbb{F}_p^\times$ היא ציקלית (מסדר $p-1$).

הוכחה. p אי־פריק ב־$\mathbb{Z}[i]$ אם ורק אם הוא ראשוני אם ורק אם (p) ראשוני אם ורק אם $\mathbb{Z}[i]/(p)$ תחום שלמות.

$$\mathbb{Z}[i] \simeq \mathbb{Z}[x]/(x^2+1)$$

ולכן $\mathbb{Z}[i]/(p) \simeq (\mathbb{Z}[x]/(x^2+1))/(p) \simeq \mathbb{Z}[x]/(x^2+1,p)$, וכך נקבל גם

$$\mathbb{Z}[i]/(p) \simeq (\mathbb{Z}[x]/(p))/(x^2+1) \simeq \mathbb{F}_p[x]/(x^2+1)$$

לכן p פריק ב־$\mathbb{Z}[i]$ אם ורק אם x^2+1 פריק ב־$\mathbb{F}_p[x]$ אם ורק אם קיים $a \in \mathbb{F}_p$ שמקיים $a^2 = -1$. נקבל $\mathbb{F}_p^\times \simeq \mathbb{Z}_{/p-1}$ אם ורק אם יש ל־$\mathbb{Z}_{/p-1}$ תת־חבורה מגודל 4, כלומר אם ורק אם $4 \mid p-1$. זה אומר שכאשר $p \cong 1 \pmod 4$ אז $p = zw \in \mathbb{Z}[i]$ פירוק אמיתי.

$$p^2 = N(p) = N(z)N(w)$$

ולכן $N(z) = N(w) = p$. אם $z = a+bi$ ונקבל $a^2+b^2 = p$. $\square$