

① 22.10.04
מבחן 1

מקור טוב! המורה חושש שיבינו הרבה למושגים אבל הוא מקווה שיהיה מסדר.
הוא נשאל ד"ר פסאי ואומר שהוא צריך להשלמה תורה אברה ויל
מצה שאין למושגים הציונים והמתונים וכו'. אז הוא נוצר להבהר
שם ג' שם א' להוציא את כי הוא רוצה אלא ואחד אק שיתן
עבור שחסר לא יבנה צין.

- אופייה אקוס: (כח) = (כח) - (כח) = כח
- אי אפשר לומר א' העצם - העצם, סתם ומתוך אי אפשר
לענות חיוב שדיקפו בהם עדיף והחסר. זו בעיה שפונקציה החלפני
מה ולקח סמל שנה אבננה שלו סתם אפשרי! לה נעשה הולכה
תורה השורה.
 - פיתרון משמאל פונקציה - בעיה תורה והתבונה הוניהו של איש
למה נוסה סתם לפיתרון משמאל אבננה והחלפה!

חבורות

הצורה תבונה היא אברה $(G, \cdot, e)$ ואשר:

- G קבוצה
- פעולה בינארית - סוגר על $a, b \in G$ אוצר ויחיד $a \cdot b$
- $e \in G$

ומתקיים:

- (1) קשירות: על $a, b \in G$ קיים ויחיד $a \cdot b \in G$
- (2) קיבור: על $a, b, c \in G$ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- (3) איבר יחידה: על $a \in G$ $e \cdot a = a \cdot e = a$
- (4) אבר הופכי: על $a \in G$ קיים $b \in G$ וק $a \cdot b = b \cdot a = e$

הצורה: עברות משמאל א' הסמן • $a \cdot b = ab$

אזכור: באר הוורכי ב של a הוא יחיד (והוא a^{-1}).

הערה: לפעמים מאתרים את ההורכי ב $\frac{1}{a}$ אבל זה לא סימון טוב

ב רק. והערה היא שאם נתונים $\frac{1}{a}$ אז אפשר לחשוב

בנוסף לכתוב $\frac{c}{a}$ ואז לא נכון אם זה $\frac{c}{a}$ או $\frac{1}{a} \cdot c$.

אזי החברה בלגה היא לא בהכרח קומוטטיבית!

הנחת: אם $a \cdot c_1 = e$ ו $a \cdot c_2 = e$ וקיים b רק של-

$ba = e$, נכפיל את שתי המשוואות ב b ונשתמש בקיבוציות:

$$b(ac_1) = (ba)c_1 = ec_1 = c_1$$

$$b(ac_2) = (ba)c_2 = ec_2 = c_2$$

$$\Leftrightarrow c_1 = c_2 \quad (\text{ש})$$

הסקנה מההנחה: השמנון רק במקל $ac_1 = ac_2$ ואם

המשוואה אפילו $ax = d$ (אם x - יחיד a, d (תקיים)

יש פתרון יחיד.

הנחה: יש פתרון והוא $x = a^{-1} \cdot d$ והוא יחיד לפי ההנחה

הקבוצה. (ש)

יש לפי זה אף גבולות שנקבעו אפריורי, אבל זה קרה לישותם

המשקל בזה את כל השיעור אמרנו (המשקל) המשקל שנקבע, וזהו אותו

המקום (או שיש יסוד אלו כמובן).

דוגמה לחבורה:

1) $(\mathbb{Z}, +, 0)$, ואן - הקבוצה היא השלמים

- הפעולה היא חיבור שלמים

- יסוד החבורה הוא המספר אפס

2) אם $(F, +, \cdot)$ שדה אז יש שתי חבורות שיהן, אחת

היא $(F, +, 0)$ והשנייה $(F \setminus \{0\}, \cdot, 1)$.

אזכור: אם יש קבוצה G וחבורה $(G, +, \cdot)$ שבה קומוטטיביות

אז $(G, +, 0)$ ו $(G \setminus \{0\}, \cdot, 1)$ חבורות ומקיים דיסטרביוטיביות

אם G שדה.

2

הצורה: תבור G נקרא תבורי (או קומוטטיבי, או אבלי) אם לכל $a, b \in G$ מתקיים $a \cdot b = b \cdot a$.

ציאור: נניח שיש לנו תבור מסדר 5 (כלומר יש בו 5 איברים). ונניח שאנחנו נותנים את טבלת הכפל שלו. מה המשמעות של זה שאמרו לנו $ax = d$ יש פיתרון יחיד? - זה אומר שהם שורה של טבלת הכפל זניבים לרעיון של האובייקט של התבורה והפירוקים אחת? כמה?

$\cdot$	a_1	a_2	a_3	a_4	a_5
a_1					
a_2					
a_3					
a_4					
a_5					

אנחנו שואלים את עצמנו - איפה זה הטל מופיע אצל כל אחד של d בשורה הפשוטה? ודי שמי יופיע שם זניב, זה הקיים שיש פיתרון $a_i x = d$. זאת יקרה שפיתרון קיים ויחיד. אז השורה הפשוטה היא תבור של איברי התבורה. למעשה כל שורה היא

תמונה של איברי היחידה. באופן פורמלי זה כל העמודות הן תמונה של איברי התבורה. אז כל העל של התבורה היא זניב קסם!!! (ואי ששיתק בזה זה ריבוע קסם יוצא שזה לא רק סבבן אלא).

קואזיאל:

1) תבור מסדר 1: $G = (\{e\}, \cdot, e)$ נאמר $ee = e$ זה

נקרא התבורה הטרייוויאלית. נשים לב שכל מרחב וקטורי (הוא תבור אלמנטרי) הוא תבור וקטורי ואז התבורה הטרייוויאלית היא למעשה הפירוק כמו מרחב העצם. זו אולי גרר השלנו אצורה. פורמלית את תבורה אינברטיות.

הצורה: יהיו G ו- H שתי תבניות (פונקציה $\varphi: G \rightarrow H$)
 וקראו הומומורפיזם אם לכל $a, b \in G$ מתקיים

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

$\swarrow$ (על G) $\swarrow$ (על H)

(כלומר, סגור תחת פעולת המכונה φ)

2. φ גורם אונימורפיזם אם φ הומומורפיזם חד-חד-ערכי.

3. φ גורם איזומורפיזם אם φ הומומורפיזם חד-חד-ערכי.

4. φ גורם איזומורפיזם אם φ הומומורפיזם חד-חד-ערכי והתמונה $\varphi(G)$ היא תבנית.

שק"מ: $\varphi: G \rightarrow H$ איזומורפיזם נאמר ש- $G \cong H$ איזומורפית.

המשק קומוטטור:

2. תמונה מסדר 2: אחד האיברים חייב להיות e ולכן נקרא a

את האפשרות האחרת?

$\cdot$	e	a
e	e	a
a	a	e

כלומר, תבנית קטנה היא תבנית! אם קיימת תבנית מסדר 2

אז זה חייב להיות e והכל נגזר מכאן. אז נניח שיש לנו

תבנית, אז נחזיק אותה (נניח) שיש לנו תבנית מסדר 2 ונניח

אין לנו ברירה וזהו! אבל ידוע שקיימת תבנית כזו - $\mathbb{Z}_2$

אז $G = (\mathbb{Z}_2, +, 0)$ היא תבנית איזומורפית ל- $(\mathbb{Z}_2, +, 0)$

המשק נמוקרה

המשק נמוקרה: כל תבנית איזומורפית ל- $\mathbb{Z}_2$ היא תבנית מסדר 2

3

הפועל (עניינים) אצמניסטרביה:

המורה: אורס אובזקי

אי-מייל: alexlub@math.huji.ac.il

שיתוף: אי שרונה שישל אי-מייל

1) Rotman, Introduction to Group Theory

2) Herstein, Topics in Algebra

המסך פועל:

3) תורגם מספר 3: נתתי מילא את עמוד הרפס:

·	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

aa=e
ba=e
אם
אז
אז
אז

תמיד אהיה
אחריה e

שלב, וצאנו שאת ק"א- תמונה מספר

3 אז היא יחידה. ואנחנו יוצאים שהיא

ק"א- כי $\mathbb{Z}_3$ תמונה מספר 3. ב-התמונה מספר

0 $\rightarrow$ e
1 $\rightarrow$ a
2 $\rightarrow$ b

3 הן איזומורפיה

אז, נשים לעתה שיתרנו ברא קואוטריבר כי זה הרפס שלר
ס'מטרי.

4) תמונה מספר 4:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

הצגה שלר שלר רחמים. הניסיון

השקנים. ציור המדוק א-מהם א-כ

תמונה.

נשים ש-שע' החלפה a-b

הוא ציור הטאור איזומורפיה לאפצור

הירוקה

זה קצת מבוזבז אז נכתוב שוב:

אופציה סטאר

•	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

אופציה ירוקה

•	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

נציגו פונקציה:

$$\begin{aligned} \varphi: e &\mapsto e \\ a &\mapsto b \\ b &\mapsto a \\ c &\mapsto c \end{aligned}$$

אפשר לראות שזה איזומורפיזם.

אין ודאות שהאופציה הראשונה לא איזומורפית. האופציה הירוקה? גבולות של איזומורפיזם הם ש- $\varphi(e) = e$. ה- φ האחרון של האופציה הראשונה הוא e ואילו באופציה הירוקה זה לא כך. לכן זה יכול להיות שכן איזומורפיזם.

תנאי: מספיק שיהיה קבוצה $a \cdot a = c$ (קבוצה אופציה איזומורפית) — האופציה הירוקה.

L

אם תחליטו אנתוני וקצרים שיש זה הוגר שמי תבחרו מספר 4. ואין אנתוני וקצרים שאין קיימור שגים בזה? אנתוני וקצרים שאין קיימור? 2 מספרים 4 איברים: $\mathbb{Z}_4$ (שפירא כמו היתכנות הירוקה) ושהם 4 איברים ואצין 2 (שפירא כמו היתכנות הראשונה) - ואנתוני וקצרים זה לא (האחרון).

המתחילים יסבירו אלינו אם זה פוזיטילר נאה.

④

למה: אם $a = e$ אז $ab = b$, $a, b \in G$
 הוכחה: אם $a = e$ אז $e \cdot b = b$ ישר מן יחידתיות e והוא
 פירוק. אם a מקיים את השוויון אז $a = e$

⑤

הוכחה: אם $\varphi: G \rightarrow H$ הומומורפיזם של תבניות אז $\varphi(e_G) = e_H$

$$\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G)$$

$\Leftarrow$ מזה נובע ש $\varphi(e_G) = e_H$ (אם $a = \varphi(e_G), b = \varphi(e_G)$)

⑥

אם G תבנית ואין בה פוטנציאל לתבנית קומוטטיבית. אז נכון שיש
 למצוא תבנית.

תבנית קומוטטיבית:

$$S_n = \text{Perm}(\{1, \dots, n\}) \quad \text{קבוצת כל הפונקציות ההדדיות (אם)}$$

א- $\{1, \dots, n\}$ ל- $\{1, \dots, n\}$

על $n > 2$ כי לא תבנית קומוטטיבית (כיום אפשר להוכיח
 וזאת הניסוחי גמור (הכלל). אז קשה לראות שיש תבנית (יהי צי
 ברור מלפני). וזה לא קשה לראות שיש לא קומוטטיבית.

⑦ F שדה. אז $M_n(F)$ תבנית - תבנית - תבנית F תבנית

תבנית תבנית (אם תבנית) אז תבנית תבנית תבנית

$$GL_n(F) = \{ A \in M_n(F) : \det A \neq 0 \}$$

general linear group

תת-חבורות

הגדרה: תת-חבורה H של חבורה G היא תת-קבוצה $H \subseteq G$ תת-חבורה (או חבורה) חלקית של G עם אותו חבורה (החבורה):

$$(1) \quad H \neq \emptyset$$

$$(2) \quad a, b \in H \implies ab \in H$$

$$(3) \quad a \in H \implies a^{-1} \in H$$

כלומר, H חבורה ביחס לאותה פעולה הפעולה של G . במקרה זה $H \leq G$ אומרים.

תשובה (ההבין) מהי הפעולה של חבורה $(\mathbb{R}, +, 0)$ חבורה היא $(\mathbb{R}, \cdot, 1)$ חבורה. ומתקיים $\mathbb{Z} \subseteq \mathbb{R}$ אבל זה לא חבורה משום שלפעולה של $\mathbb{Z}$ שונה!

$$e \in H \quad H \leq G \quad \text{אם } G \text{ חבורה}$$

הוכחה: טוב, זה ברור. $H \neq \emptyset$ קיים $a \in H$ ופי תכונה

$$(3) \quad a^{-1} \in H \quad \text{ואפי (2) יש סגירות חבורה. דבר } e = aa^{-1} \in H$$

(1)

הוכחה: תת-חבורה ונניח $H \leq G$ תת-קבוצה לא ריקה. אז:

$$a, b \in H \implies ab \in H \quad a^{-1}b \in H$$

הוכחה:

$$(2) \iff (3) \quad \text{ברור מתכונות}$$

$$(1) \iff (2) \quad \text{נתון ש- } H \text{ לא ריקה. יהיו } a, b \in H \quad \text{אזי ופי (הנתון)}$$

$$ab = (a^{-1})^{-1}b \in H \quad \text{אם } e \in H \quad \text{כמו כן } e \in H \quad \text{אזי}$$

$$e = a^{-1}a \in H \quad \text{אם } a \in H \quad \text{אזי}$$

$$H \leq G \iff a^{-1} = a^{-1}e \in H$$

(1)

צדקה: אם $\{H_i\}_{i \in I}$ אוסף תת-חבורות של G אז $H = \bigcap_{i \in I} H_i$ גם תת-חבורה.

בוכחה: נראה אז קיום התכונות הנדרשות.

$$(1) \quad H \neq \emptyset \Leftrightarrow e \in \bigcap H_i \Leftrightarrow e \in H_i \quad i \in I$$

$\hookrightarrow$ כי H_i תת-חבורה

$$(2) \quad i \in I \text{ אם } a, b \in H_i \Leftrightarrow a, b \in H$$

$$\Leftrightarrow ab \in H_i \quad i \in I \text{ כי אלה תת-חבורות}$$

$$\Leftrightarrow ab \in \bigcap H_i$$

$$(3) \quad i \in I \text{ אם } a \in H \text{ אז } a \in H_i \text{ אם } i \in I \text{ אם } a^{-1} \in H_i$$

$$\Leftrightarrow a^{-1} \in \bigcap H_i \quad i \in I \text{ אם}$$

☺

דוגמה: ניקח $G = \mathbb{Z}$ עם פעולת החבורה. אז $H_1 = 5\mathbb{Z}$

! - $H_2 = 7\mathbb{Z}$ הן תת-חבורות (קל לבדוק). ומכאן ש- $H = H_1 \cap H_2$

שביא למצוא $35\mathbb{Z}$ תשובה חלקית. אז כן.

אם $H_1 \cup H_2$ אינה תשובה חלקית. שכן $5, 7 \in H_1 \cup H_2$

אם $5+7=12 \notin H_1 \cup H_2$!

אזכרה: תהייה S תשובה. $S \subseteq G$ תת-קבוצה. אזי הקבוצה

$$\hat{S} = \bigcap_{\substack{H \leq G \\ S \subseteq H}} H$$

התשובה. כל תוצאה של התכונות אשר מתארה S .

$\Leftrightarrow S$ הנה תשובה המינימלית שמכילה את $\hat{S}$. (קרא לה

התשובה החלקית הנוצרת ע"י S .)

צדקה: גופי G תשובה. ואם $S \subseteq G$ תת-קבוצה. (סמן

$$\langle S \rangle = \{ x_1^{\epsilon_1} \dots x_n^{\epsilon_n} : n \in \mathbb{N} \cup \{0\}, \epsilon_i = \pm 1, x_i \in S \}$$

$$\langle S \rangle = \hat{S} \quad \text{אז}$$

6

הוכחה ראשונה, נראה ש- $\langle S \rangle$ חבורה חלקית. ואכן, $e \in \langle S \rangle$
 בתור מילה של אפס איברים. כעת, אם $x_1^{e_1} \dots x_n^{e_n}, y_1^{d_1} \dots y_m^{d_m} \in \langle S \rangle$
 אז $x_1^{e_1} \dots x_n^{e_n} y_1^{d_1} \dots y_m^{d_m} \in \langle S \rangle$ אבסורד, עפ"י מה שהוכחנו
 בתרגיל. $x_1^{-e_1} \dots x_n^{-e_n} = (x_1^{e_1} \dots x_n^{e_n})^{-1}$ ואכן גם ההפכי ב- $\langle S \rangle$.
 ומכאן ש- $\langle S \rangle \leq G$.

בהינתן ש- $S \subseteq \langle S \rangle$ לפי הגדרתה (ואכן $\hat{S} \leq \langle S \rangle$ משום
 ש- $\hat{S}$ היא חבורה תת-החבורה שמכילה את S . ואפשר

$\langle S \rangle$ היא תת-חבורה)

כעת, $\hat{S}$ היא חבורה חלקית שמכילה את S ואכן גם את
 $S^{-1} = \{s^{-1} : s \in S\}$. ואכן היא מכילה את אוסף ה- S המכפולים של

איברים מ- S ו- S^{-1} . מכאן אלק ואכן מכילה את $\langle S \rangle$. (11)

דוגמה: $S = \{x\} \subseteq G$. אם $\langle S \rangle = \{x, x^{-1}, x'x^{-1}, \dots\}$

ב- $\langle S \rangle$ יכולות להיות חברים, למשל במקרה שהחבורה
 סופית. החבורה $\langle S \rangle$ הנ"ל נקראת חבורה מנדלסון (או ציקלית).

השקוד שלר ורניו שלם G תבורה $S \subseteq G$ תר קבורה אג
 $\langle S \rangle =$ היתר תבורה S הנוצרת $= \bigcap_{S \subseteq H \leq G} H = \{g \in G : g = s_1^{\epsilon_1} \dots s_n^{\epsilon_n}, n \in \mathbb{N}, \epsilon_i = \pm 1\}$
 $\leftarrow$ רון אנתו וסכיות לקולור
 סאוק אפס וס איור היחידה e .

דוגמאות:

① $(\mathbb{Z}, +, 0)$ אם $S = \{3\}$ קר זראור ש- $\langle S \rangle = 3\mathbb{Z}$

אם $S = \{5, 7\}$ סא $\langle S \rangle = \mathbb{Z}$ למד $\{$ אנתו ירור
 עובר אר 1 נצחל עינאר ש $5, 7$:

$$1 = 5 - 2 - 2 = 5 - (7 - 5) - (7 - 5) = 3 \cdot 5 - 2 \cdot 7$$

רובן ססון - הכולל הסו אחרור ורורסכי.

כרת, אחר ש- $\langle S \rangle$ $e \in \langle S \rangle$ אר $\mathbb{Z} \in \langle S \rangle$ שיק $\langle S \rangle$.

סאפן ללי יש סעס שאחרת: אם $a, b \in \mathbb{Z}$ אפי קיים $x, y \in \mathbb{Z}$

ק ש- $ax + by = 1$ אנט $(a, b) = 1$ (סאור הס רורס).

$$\langle \{a, b\} \rangle = \mathbb{Z} \text{ אנט}$$

אג רניו ש- $\mathbb{Z}$ נוצר ע' איור אחר. אר ס תבורה נוצר ע' איור

אחר. ארס אר רר יש תבורה שנוצר ע' איור אחר אג הס

תורח ארס, שרר ס האיררס כה הס תנקל ש איור ס שרר.

ארס ס תבורה ארס נוצר ע' איור אחר - ארס $\mathbb{R}$ עס חסור...

② $G = \mathbb{Z}_n = \{0, 1, \dots, n-1\}$ אר $\mathbb{Z}_n = \langle \{1\} \rangle$.

תרסל: $1 \leq a < n$! $(a, n) = 1$ אנט $\langle \{a\} \rangle = \mathbb{Z}_n$.

היחידה: אם קיים $a \in G$ ק ש- $\langle a \rangle = \langle \{a\} \rangle = G$

נאר ש- G תבורה ארסלר (ציקלי)

סענפ: אם G תבורה ציקלי אפי:

Ⓐ אם G אינסופי אפי $G \cong \mathbb{Z}$

Ⓑ אם G ספור ארס n אר $G \cong \mathbb{Z}_n$

הוכחה: אפי' הנתון יש $a \in G$ רק של $\langle a \rangle = G$.
 בואו, a איבר ב- G והוא מזהה ב- a ו- a^{-1} ואם a איבר
 ב- G והוא מהצורה a^k כאשר $k \in \mathbb{Z}$.

(א) אם a באיברים a^k שונים זה מזה, והפרט G אינסופי,
 נגדיר הפונקציה $\varphi: \mathbb{Z} \rightarrow G$ $\varphi(k) = a^k$. זהו
 הומומורפיזם כי $\varphi(k+l) = a^{k+l} = a^k \cdot a^l = \varphi(k)\varphi(l)$. φ הוא חד-
 כי $\langle a \rangle = G$ | φ חתום כי הנתון שנוסח שונים זה מזה.
 $\varphi \Leftarrow$ איזומורפיזם.

(ב) נניח שיש $k \neq l$ שלמים רק של $a^k = a^l$. $a^{k-l} = e$
 בהכרח $0 < k-l$ (כי אחרת $e = (a^{k-l})^{-1} = a^{l-k}$)

פירוש הדבר יש $m > 0$ רק של $a^m = e$. יהי n החזקה
 הראשון רק של $a^n = e$. אזי נסמן של $G = \{e, a, a^2, \dots, a^{n-1}\}$
 ואז n איברים שונים. אם $k \geq n$ אזי נחלק את k ב- n
 $k = r \cdot n + s$ עבור $0 \leq s < n$ ואז

$a^k = a^{rn+s} = a^{rn} a^s = (a^n)^r a^s = e^r \cdot a^s = e a^s = a^s$
 באופן דומה, אם $k < 0$ אפשר להציג את a^k לתוך הקבוצה.
 נחלק נראה שהם כולם שונים. נניח $a^i = a^j$ כאשר $0 \leq i < n$ ו- $0 \leq j < n$
 אז $a^{i-j} = e$ הסתירה לאינדיקציה של n .

נגדיר $\varphi: \mathbb{Z}_n \rightarrow G$ $\varphi(k) = a^k$ $k \in \mathbb{Z}_n$.
 דיוברוק של φ חתום ושל φ איזומורפיזם כי
 $\varphi(k+r) = a^{k+r} = a^k \cdot a^r = \varphi(k)\varphi(r)$
 זה חתום מפניו n
 זה חתום ב- G מפני
 שיש שונים.

(II)

הצגה: G חבורה | $a \in G$. נגדיר את $[a]$ (הסדר של a):
 $o(a) = \min \{n : n > 0, a^n = e\}$
 אם אין n כזה נאמר שהסדר של a הוא אינסופי.

8

מסקנה מהדיון הקודם: אם G תכונה $a \in G$! -

$H = \langle a \rangle$ התכונה הנולדת a . אזי $|H| = o(a)$

אז קוצר הסדר של איבר זה הסדר של התכונה החלקית שלה יוצר.

טענה שנוכח את: אם G ספיר, אזי $|G| = o(a)$

מסקנה: G תכונה מסדר 5 היא איזומורפית ל- $\mathbb{Z}_5$, יותר מזה - G

תכונה מסדר p ראשוני איזומורפית ל- $\mathbb{Z}_p$.

הנחה למסקנה: יהי $a \in G, a \neq e$. אזי $p \mid o(a) < p$ דבר

$p = o(a)$. $\Leftarrow$ $p = |H| = |\langle a \rangle|$, כלומר $H = G$. כלומר

G ציקלית מסדר p . אמר ראיון שתכונה ציקלית מסדר p יש רק אחת.

9

מתחלקת של תכונה חלקית

הגדרה: נניח G - תכונה ו- H תכונה חלקית. (אחר שלעבור $a, b \in G$

$a \equiv b \pmod{H}$ אם $a^{-1}b \in H$.

פיתוח: נניח $G = \mathbb{Z}$ ו- H היא תכונה של a ו- b שקולים

מכיוון הנוצרים אם ההפרש שלהם זוגי, כלומר הנוצרים שקולים

כיום והאיזומורפיות שקולים חזים.

אנחנו רואים אם $H = 7\mathbb{Z}$ אזי $\pmod{H}$ הוא כמו $\pmod{7}$.

תכונה: תהא X קבוצה. יחס $\sim$ על X הוא מתקבוצה $R \subseteq X \times X$

ואחרים של $a \sim b$ אם $(a, b) \in R$.

יחס R על X (קרא יחס שקילות אם היא מקיים את 3 התכונות:

א) רפלקסיביות: לכל $a \in X$ $a \sim a$

ב) סימטריות: לכל $a, b \in X$ אם $a \sim b$ אז $b \sim a$

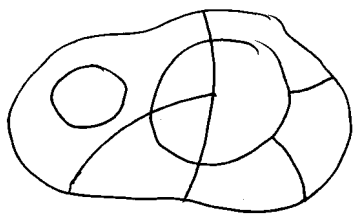
ג) טרנזיטיביות: לכל $a, b, c \in X$ אם $a \sim b$ ו- $b \sim c$ אז $a \sim c$.

פיתוח: נסתכל על $X = \mathbb{Z}$. היחס $\leq$ רפלקסיבי וטרנזיטיבי.

היחס $<$ רק טרנזיטיבי. היחס $\equiv \pmod{7}$ היא רפלקסיבי, סימטרי

וטרנזיטיבי - כלומר היא יחס שקילות

טענה: יחס שקילות $\sim$ ארוק אר X מאתקאר שקולות זכור
 לאיחודן נא X .
 (הוכחה במתמטיקה פיסקטור)



טענה: היחס שהזכרנו $\sim$ נא יחס שקולות.
הוכחה: צריך להראות אר קיים 3 התכונות:

- פאקסיביות: זר $a \in G$ $a \equiv a \pmod{H} \Leftarrow a^{-1}a = e \in H$
- סימטריה: נניח $a \equiv b \pmod{H} \Leftarrow a^{-1}b \in H$
- טרנזיטיוויות: נניח $a \equiv b \pmod{H}$! $b \equiv c \pmod{H}$
 $a^{-1}b \in H, b^{-1}c \in H$ $\Leftarrow$
 $a^{-1}c = a^{-1}b b^{-1}c \in H \Leftarrow a \equiv c \pmod{H}$

Ⓜ

שאלה: אי נא האגרים לשקולים $\sim$ - e ?

תשובה: e איננו H ונקר נא. שיהי אר $b \in H$ אר $b^{-1} \in H$
 ואר $e \equiv b \pmod{H}$ אר $e^{-1}b \in H$ נא, נא $b \in H$.

סיכום: אר G חבורה ! $H \leq G$ נאן זר $a \in G$
 a $[a] = \{b \in G : a \equiv b \pmod{H}\}$
 גרר סיכום נא ארקים $[e] = H$

טענה: אר $a \in G$ אר $[a] = aH = \{a \cdot h : h \in H\}$

הוכחה: נראה קרפ $[a] \supseteq aH$. ואר, אר $b = ah \in aH$

אז $a \equiv b \pmod{H} \Leftarrow a^{-1}b = a^{-1}ah = h \in H$

אז נא, אר $b \in [a]$ אר $h = a^{-1}b \in H$ אר $b = ah$
 $b \in aH \Leftarrow$

Ⓜ

הערה: האתקאר aH נא לא היכרה גר חבורה. זמל אר G
 אר חבורה קטנה אר aH אר $a \neq e$ נא ישינו!

9

הצגה: aH נקרא המחלקה השמאלית של H המכילה את a .
 Ha נקרא מחלקה ימנית של H המכילה את a , והיא מתקבלת
 מהצגה יחס שקילות $a \equiv b \pmod{H} \leftrightarrow ab^{-1} \in H$.

אברהם חמורה: בד"כ $aH \neq Ha$!

הצגה: מספר המחלקות השמאליות של H ב- G נקרא האינדקס של
 H ב- G ויסומן $[G:H]$

דוגמה: יוני זרינג של H אינסופי, אבל האינדקס שלה סופי. למשל
 $n \in \mathbb{Z} \quad [n\mathbb{Z}:\mathbb{Z}] = n$

טענה: אם $[a], [b]$ שתי מחלקות שמאליות של H , אזי קיימת
 פונקציה חד-חד ערכית $f: [a] \rightarrow [b]$ ובהפך $|[a]| = |[b]|$.

הוכחה: $c \in [a]$ נותן ארתיבה באופן יחיד כ- $c = ah$
 כי אם $ah = ah'$ אז $h = h'$.

נגדיר $f: [a] \rightarrow [b]$ כ- $f(ah) = bh$. זה מוגדר היטב
 כי ההצגה כ- ah היא יחידה.

הפונקציה f היא איזומורפיזם בין $[a]$ ל- $[b]$ והיא חד-חד ערכית
 כי אם $ah = ah'$ אז $bh = f(ah) = f(ah') = bh'$ וכן $h = h'$.

⑩ $ah = ah' \Leftrightarrow f(ah) = f(ah') \Leftrightarrow bh = bh' \Leftrightarrow |[a]| = |[b]|$.

מסקנה: אם G סופית אז $|G| = [G:H] \cdot |H|$
 (כי $|aH| = |eH| = |H|$).

משפט לגראנז': אם G סופית $H \leq G$ אז $|H| \mid |G|$

אחמורה מספר של a יחידה ארתיבה מתנה חלקית מספר $|G|$!

G חבורה $| H \leq G$ חבורה חלקית. נגדירנו יחס שקילות - $a, b \in G$
 $a \equiv b \pmod{H}$ אם $a^{-1}b \in H$.

ראינו שזה יחס שקילות. במחלקת aH של G נגדירנו $[a] = aH$.
 באינו גם שההתאמה $f: [a] \rightarrow [b]$ המוגדרת $f(ah) = bh$
 היא תה"ז וזה אכן $[a] = [b]$ אם $a, b \in H$. אפשר להמחיש זאת
 מסומן $[G:H]$ ונקרא האינדקס של H . מתקיים $[e] = H$
 (זו המחלקה היחידה שהיא גם תת-חבורה) אכן, אם G סופית
 אז $|G| = [G:H] \cdot |H|$ - שהיא יחס השקילות מחלק את G
 $[G:H]$ - מחלקת G לזרועות שוות גודל.

משפט לגראנז': תהי G חבורה סופית ותהי $H \leq G$ חבורה חלקית. אז
 $|H| \mid |G|$

הערה: אחרים בחרו לכתוב את G בתורה עם מחלקת שמאלית. האופיה
 איזה אפשר לכתוב בדיוק את אותה הדבר עבור מחלקת ימנית (אולי
 בתנאי). הם אופן חשוב לשים לב להבדל $aH \neq Ha$. יש
 תכונות מיוחדות שבהן זה דווקא מתקיים ובהן נדון בהמשך.

יהי $g \in G$ ונסמן H את החבורה החלקית של G הנוצרת על ידי g .
 זאת חבורה ציקלית. אם G סופית גם H סופית ואז
 $H \cong \mathbb{Z}_n$ כאשר $n = o(g)$ - הסדר של g שהוא גם גודל של H .
 פירוט הדבר של $g \in G$ אפשר למצוא תת-חבורה של G בגודל
 $(g) \leq G$ אם G סופית אז $|G| \mid o(g)$ $\Leftrightarrow g^{|G|} = e$
 (כי נניח $|G| = r \cdot o(g)$ אז $e = e^r = (g^{o(g)})^r = g^{r \cdot o(g)} = g^{|G|}$).

מסקנה: אם G חבורה מסדר ראשוני p אז $G \cong \mathbb{Z}_p$.

הוכחה: יהי $e \neq g \in G$ אז $|G| \mid o(g)$ - $o(g) \neq 1$ כי $g \neq e$.
 $\Leftrightarrow p = o(g)$ אכן $H = \langle g \rangle$ היא מסדר p אכן $H = G$.
 נומר G נוצרת על ידי g , נומר היא ציקלית מסדר p , אכן $G \cong \mathbb{Z}_p$.

משפט פתח (הקטן): אם p ראשוני, $a \in \mathbb{Z}$ אז $a^p \equiv a \pmod{p}$

הוכחה: אם $p \mid a$ אז זה ברור, שכן $a^p \equiv 0 \pmod{p}$ אם $p \mid a$.
 אחרת $(a, p) = 1$ (לפי (6) הוא זר). $\Rightarrow p \mid a^p - a$

נתבונן בתחבורה הכפולית $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \{1, 2, \dots, p-1\}$ עם פעולת הכפל

אופרטור $\cdot$ (זו התחבורה הכפולית של השדה $\mathbb{Z}_p$) וזו תחבורה מסדר

$p-1$. $\Leftarrow$ $b = 1, 2, \dots, p-1$ מתקיים $b^{p-1} \equiv 1 \pmod{p}$ אם b זר, אז

$a \in \mathbb{Z}$ כלשהו אם $(a, p) = 1$ אז יש $b \in \mathbb{Z}_p^*$ כך ש-

$a \equiv b \pmod{p}$. אז $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p}$. (כפי שראינו שיש 2 הצגות

ב- a ונקבל $a^p \equiv a \pmod{p}$)

(11)

הגדרה: יהי $n \in \mathbb{N}$ (נסמן $\mathbb{Z}_n^* = \{1 \leq a < n : (a, n) = 1\}$)

$$\varphi(n) = |\mathbb{Z}_n^*|$$

$\varphi(n)$ (קראו פונקציית אويلר) וזה מספר האיברים הקטנים מ- n ולזר לו.

לדוגמה, אם $p \neq q$ ראשוניים אז $\varphi(p) = p-1$ $\varphi(pq) = \varphi(p)\varphi(q)$

$$\varphi(6) = 2, \quad \varphi(15) = 8$$

לענף דלדל (הוכחה): אם $(m, n) = 1$ אז $\varphi(mn) = \varphi(m)\varphi(n)$

אם p ראשוני אז $\varphi(p^r) = (p-1)p^{r-1}$

בהינתן הטענה הראשונה אפשר להסיק את $\varphi(n)$ לכל $n \in \mathbb{N}$

טענה: $\mathbb{Z}_n^*$ היא תחבורה ביחס לכפל. - זו תחבורת האיברים ההפיכים

בהיחס $\cdot$ (חייב להראות שזה תת-קבוצה של האיברים ההפיכים).

תוצאה: $a \in \mathbb{Z}_n^*$ אגב קיים $b \in \mathbb{Z}_n^*$ כך ש- $ab \equiv 1 \pmod{n}$.

מסקנה: מכלל שני איברים הפיכים היא הפיכה.

משפט אويلר: $a, n \in \mathbb{Z}$ כאשר $(a, n) = 1$ אז $a^{\varphi(n)} \equiv 1 \pmod{n}$

הוכחה: אחרת ל $(a, n) = 1$ קיים $b \in \mathbb{Z}_n^*$ כך ש- $a \equiv b \pmod{n}$.

$$a^{\varphi(n)} \equiv 1 \pmod{n} \Leftarrow b^{\varphi(n)} \equiv 1 \pmod{n}$$

(11)

התאמים רביעי והקרום השיעורים של יום רביעי
"מסכום שיעורים: 1-9 ער 11
הסידור הלה "משקל עור יש לביתה

חבורת התמורות

תבא X קבוצה. נסמן $\{f: X \rightarrow X : f \text{ תח'ע ושל}\}$
לא אנוס התמורות של X . זו חבורה ביחס לפעולת ההרכבה:

- איבר היחידה הוא הזהות הלה
- הרכבה של G פונקציה מקימה אסוציאטיביות
- $f: X \rightarrow X$ תח'ע ושל יש $f^{-1}: X \rightarrow X$ רק ש-
 $f^{-1} \circ f = id = f \circ f^{-1}$
- הרכבה של פונקציות תח'ע ושל היא תח'ע ושל.

אם X סופית נניח שהיא $X = \{1, 2, \dots, n\}$ מתקרה לה
 $Per(X) = Sym(n) = S_n = \Sigma_n$ (נסמן)
והיא נקראת החבורה הסימטרית על n אלמנטים.

משפט קוילי: כל חבורה G קיימת קבוצה X רק ש- G
איזומורפית לחבורה חלקית של $Per(X)$.

מה שממשט גרע אומר היא לא שתונת החבורה לה פשוט אלא
שתמורה (התמורות היא מאקז אדא מסומכת ...)

הורחג: ניקח $X = G$. $a \in G$ יציר $la: G \rightarrow G$
שהיו הפונקציה הומוגרפה זו $la(x) = ax$

la היא תח'ע ושל, שמוי אם $la(x_1) = la(x_2)$ אז $ax_1 = ax_2$ מתק
חבורה G אפשר לצמצם אק $x_1 = x_2$. אדא שני אמי יש לנו $y \in X = G$
אז המקור שלו תח'ע la היא $a^{-1}y$ שמוי $la(a^{-1}y) = aa^{-1}y = y$

יציג $\varphi: G \rightarrow \text{Per}(X)$ ע"י $\varphi(a) = \ell_a$.

צריך להראות ל- φ הומומורפיזם ושל- φ תח"ע ושה יראה
 ש $\varphi: G \rightarrow \text{Per}(X)$ הומומורפיזם שלשה בדיוק מה שלולמספט אומר.

$\varphi(ab) = \varphi(a)\varphi(b)$? צריך לבדוק אם $\ell_{ab} = \ell_a \circ \ell_b$
 אם $x \in G$ מתקיים $\ell_{ab}(x) = (ab)x = a(bx) = \ell_a(bx) = \ell_a(\ell_b(x)) = (\ell_a \circ \ell_b)(x)$
 $\Leftarrow$ זה הומומורפיזם.

- φ תח"ע כי אם $\varphi(a) = \varphi(b)$ אז $\ell_a = \ell_b$
 $a = \ell_a(e) = \ell_b(e) = b$

Ⓜ

מסקנה מהחלטה: אם G תבורה סופית מספר n אז $G \cong S_n$
 נוגת לשיעור בתבורה חלקית של S_n .

S_n (התבורה)

אם $X = \{1, 2, \dots, n\}$ אז $\pi \in S_n$ גקנולס לסמן

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$$

נופשט גלגל שאומר מה הערך של $\pi(a)$ ל $a \in X$.

אנא פשוט להרכיב פרמוטציות בתח"ע גלגל. זכור $n=5$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$$

$$\Rightarrow \pi \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \cancel{3} & \cancel{1} & \cancel{4} & \cancel{5} & \cancel{2} \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} \begin{matrix} \sigma \\ \pi \end{matrix}$$

$$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \cancel{5} & \cancel{3} & \cancel{2} & \cancel{4} & \cancel{1} \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix} \begin{matrix} \pi \\ \sigma \end{matrix}$$

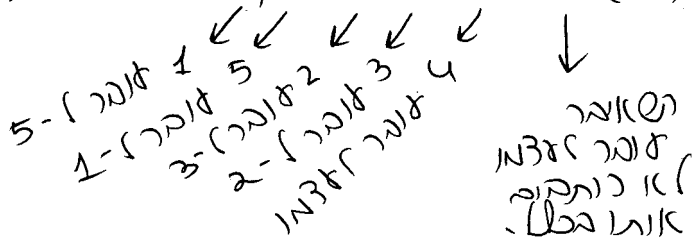
האן אנחנו חאים להכבה והאזא קלמולמול

(12)

צורת ההתניה הנ"ל קצת מאשמת בשיטה הנ"ל אי אפשר
 מיד להבין מה סדר של תמונה. להראות את אולי (ל- n)
 זקוק לה אישם וקשה לעקוב אחרי התהליך...

שיטה יותר נוחה היא הציקלוסים. (סמור בעל-דממה)

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix} \Rightarrow \pi = (1,5)(2,3)(4) = (1,5)(2,3)$$



$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix} \Rightarrow \sigma = (1,3,4,5,2)$$

$$\pi \circ \sigma = (1,2,5,3,4)$$

$$\sigma \circ \pi = (1,2,4,5,3)$$

מהתניה הנ"ל ברור שהסדר של σ הוא 5 וזה גם $\pi \circ \sigma$
 , $\pi \circ \sigma$ ואילו π מסדר 2.

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

ואם קשה להבין זה
 (הסדר של φ)

$$\varphi = (1,3,5)(2,4) \quad \text{(נניח)}$$

אם ברור שהסדר של
 φ הוא 6 כי זה
 מספר המהפכים המינימלי
 שמחזיר את הציקלוסים
 למקומם המקורי.

הגדרה: תמונה $\varphi \in S_n$ נקראת מחזור / ציקלוס

מסדר r אם קיימים $i_1, \dots, i_r \in \{1, \dots, n\}$ (זכור $r \leq n$)

$$\text{כך ש-} \begin{cases} \varphi(i_1) = i_2 \\ \varphi(i_2) = i_3 \\ \vdots \\ \varphi(i_r) = i_1 \end{cases} \quad \text{ו} \quad \varphi(j) = j \quad \text{אם } j \notin \{i_1, \dots, i_r\}$$

סקמוצה $\{i_1, \dots, i_r\}$ נקרא החלק של φ

הסימונים של הדימואורקאצם σ הוא ציקלוס. אבל π אינה
 ציקלוס. π היא מרכבה של שני ציקלוסים.

נשים $\mathbb{S}_n$ מחפשה של ציקלוסים לנים היא קומפוטטיבית -
 שהיית ציקלוס נותן רק באמצעות אלגוריתם האנטי של אף
 ציקלוס אחר.

אם הציקלוסים σ ו- τ הן מחפשה $\sigma \tau$ הן קומפוטטיביות.

$$(1\ 3)(3\ 5) = (1\ 3\ 5)$$

$$(3\ 5)(1\ 3) = (1\ 5\ 3)$$

הערה: אם σ ציקלוס מסדר r אז $\sigma(r) = r$ (בדוק!).

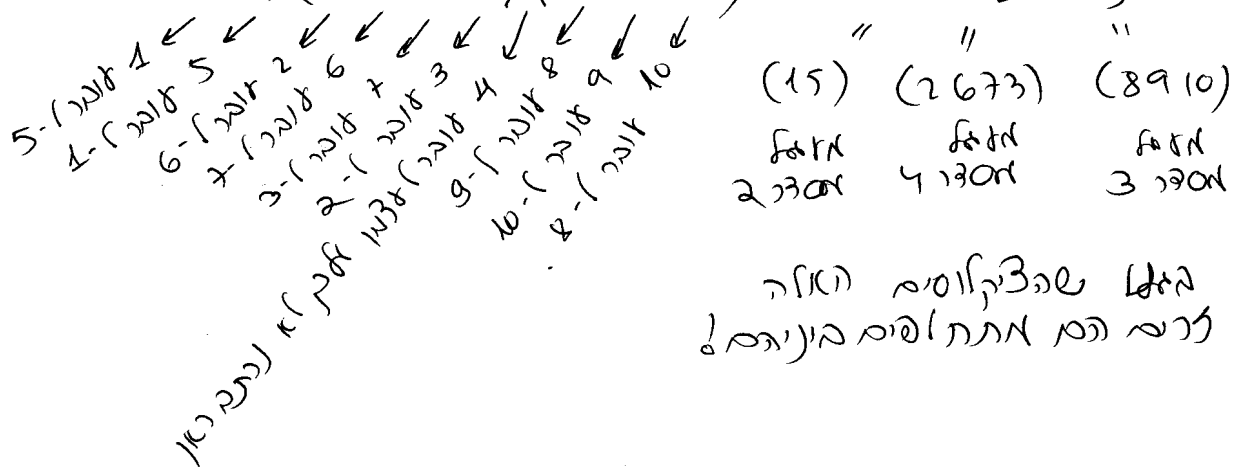
טענה: S_n תמורה ה- n היא מחפשה של ציקלוסים לנים
 (ז"א לכל n תלכסם לנים זה לזה)

הוכחה בעזרת צימוד: $n =$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 6 & 2 & 4 & 1 & 7 & 3 & 9 & 10 & 8 \end{pmatrix}$$

(כתוב את π כמחפשה של מחפשים:

$$\pi = (1\ 5)(2\ 6\ 7\ 3)(8\ 9\ 10) = \varphi_1 \cdot \varphi_2 \cdot \varphi_3$$



הכלל שהציקלוסים (ואלה
 לנים הם מתחלפים ביניהם!)

הערה: ציקלוסים לנים מתחלפים זה לזה.

מסקנה: אם $\pi = \varphi_1 \circ \dots \circ \varphi_r$ כאשר $\{\varphi_i\}_{i=1}^r$ הם מחזוריים לנים
 אז $\sigma(\pi) = \text{lcm}\{\sigma(\varphi_i)\} =$ המכנה המשותף האינמינלי
 של הסדרים של $\varphi_1, \dots, \varphi_r$.

$$\text{least common multiplier} = \text{lcm} \quad *$$

אלהרה המורה: המסקנה לא (כונה) מחפשה של מחפשים σ לנים

(13)

למטה: נניח $\pi = (a_1, a_2, \dots, a_r)$ מעתה מסדר r ראשוני
 $a_i \in \{1, 2, \dots, n\}$. אכן π נותן זרימה במחלקה של
 מעתה מסדר 2 .

הוכחה: $(a_1, a_2, \dots, a_r) = (a_1, a_r)(a_1, a_{r-1}) \dots (a_1, a_2)$
 אם $a_j \in \{a_1, \dots, a_r\}$ $j \neq r$ של a_1 הופכים משאירים את האותיות אחרים.
 נסתכל על a_1 . צד שמאל מעביר אותו ל- a_2 . צד ימין מעביר
 אותו ל- a_2 ואם a_2 לא מופיע בשאר הציקלוסים שמשמאל
 ל- (a_1, a_2) אכן נשארו אלו של a_1 עבר ל- a_2 .
 a_2 עבר הוצע שמאל ל- a_3 . הוצע ימין a_2 עבר ל- a_1 .
 ואם עבר ל- a_3 . ואם הציקלוסים שמאל ל- $(a_1, a_3)(a_1, a_2)$ a_3
 נוצרים יותר ה- a_3 וסוף a_2 עבר ל- a_3 .
 ככה אפשר לראות שכל $r \geq 1$.

(11)

מה שהיה אמרת היא של תמונה מעתה מסדר r (יותר
 עתה מסדר במחלקה של $r-1$ תמונות מעתה מסדר 2 .
 אכן r תמונה היא מחלקה של מעתה מסדר 2 .

מסקנה: כל תמונה ה- S_n היא מחלקה של חילופים (טרנספוזיציות)
 מעתה מסדר 2 .

מסקנה: (11) וחילופים יוצרים את התמונה S_n .

הערה: $(i, j)^{-1} = (i, j)$

$(a_1, \dots, a_r)^{-1} = (a_r, \dots, a_1)$ פתיחה שמאלה היא
 ההופכי לפתיחה ימנית.

למטה: $n-1$ החילופים $(1, 2), (2, 3), \dots, (n-1, n)$
 יוצרים את S_n .

הוכחה: מספיק להוכיח של i : i - j החילוף (i, j)
 הוא מחלקה של החילופים הלא.

אָבן, נניח ב'ה"ב $j < i$. א"כ

$$(i, j) = (i, i+1) \dots (j-2, j-1)(j-1, j) \dots (i+1, i+2)(i, i+1)$$

אפש זעקלע אומי דע זעראו שלע נעמט אונז.

בשנייה הקדשה צבחנו $S_n = \text{Per}(\{1, 2, \dots, n\})$

ראינו של אחר $\pi \in S_n$ ניתן לכתבה במחשה של מחלוקים לרים :

$$\pi = (a_1, a_2, \dots, a_r)(b_1, b_2, \dots, b_{r_2}) \dots$$

ראינו גם של אחר ניתן לכתבה במחשה של מחלוקים (ראו דוגמא לרים) :

$$(a_1, a_2, \dots, a_r) = (a_1, a_r)(a_1, a_{r-1}) \dots (a_1, a_2)$$

לדוגמה לריוכה של אחר נכון - פשוט לב a_i (נכון, אם שני הרצפים מחבורים אותו אחר a_j).

לדוגמה, אחר $r-1$ הוא מחשה של r מחלוקים. אחר לכתבה מחשה בולט הדבר, היחידה לבחן אותו מחלוקים, אבל הוא אחר.

מסקנה: ב תמונה S_n ניתנת לכתבה במחשה של לב ביותר n מחלוקים.

הוכחה: ב תמונה π ניתנת לכתבה במחשה של מחלוקים האחרים $i_1, \dots, i_l$

כך ש- $\sum_{i=1}^l i_i \leq n$ וב אחר האחר i_i ניתן לכתבה במחשה של i_i-1

מחלוקים לבחן π ניתנת לכתבה במחשה של $\sum_{i=1}^l (i_i-1) < n$ מחלוקים. (11)

ב מחלוק (a, b) ניתן לכתבה במחשה של מחלוקים אחר $(i, i+1)$ עבור

$i=1, \dots, n-1$. (נראה בהכרח ש- $a < b$ אחר

$$(a, b) = (a, a+1)(a+1, a+2) \dots (b-2, b-1)(b-1, b) \dots (a+1, a+2)(a, a+1)$$

למה? נסתכל לאן a עבור הרצף ימין : $a \leftarrow a+1 \leftarrow \dots \leftarrow a+2 \leftarrow \dots \leftarrow b-1 \leftarrow b$

ואם נסתכל נוספים בו יותר בצורה פורמלית ב עבור a .

דבר אחר לבחן של אחר ששונה a ו- $a+1$ עבור אחר $a+1$, אחר $a+1$

עבור a ו- $a+1$ נוספים בו עד המחלוק $(a, a+1)$ שמחלוק אותו חלוק $a+1$.

מסקנה: ב תמונה π ניתנת לכתבה במחשה של לב ביותר n^2 מחלוקים אחר

$(i, i+1)$

הוכחה: ב מחלוק (a, b) הוא מחשה של לב ביותר n מחלוקים אחר

$(i, i+1)$ ואם אחר ש לב ביותר n מחלוקים יוצא לב ביותר n^2 . (11)

מסקנה: הקבוצה $\{(1, 2), (2, 3), \dots, (n-1, n)\}$ יוצרת את S_n .

דוגמה S_n נוצרת על ידי איברים. למשל, $S_n = \langle \tau, \sigma \rangle$ כאשר

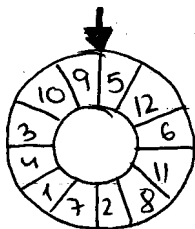
$$\tau = (12) \quad \sigma = (123 \dots n-1 \ n)$$

הוכחה: מספיק להוכיח של תחילת מוצג $(i \ i+1)$ ניתן להכתוב כמחזור
 ב- τ ו- σ והוכחה. נטען ש- $(i \ i+1) = \sigma^{-i+1} \tau \sigma^{-(i-1)}$

מה שקורה כאן הוא שמצבים את המצב הנוכחי קדימה אחת יחידה ואז
 מתחילים תהליך. השמות $i+1$ ו- $i-1$ צצים למטה הם מזהים 2-
 ואז 2 עובר ל-1 ואז צצים $i+1$ ו- $i-1$ צצים ימנה והוא מזהים
 למקום i . באופן דומה i עובר ל- $i+1$. אם יש לנו $a < i$ אז אחרי
 הפעולה $\sigma^{-(i-1)}$ הוא לא מזהים לא למקום הראשון ולא לשני ולכן לא מושפע מ- τ
 ואז σ^{i-1} מתחיל אותו למקום. רק אם $a < i+1$ (11)

נשים לב ש- $\sigma^{-(i-1)} = \tau \sigma^{-(i-1)}$ ולכן $(i \ i+1)$ הוא מילה באורך $n+1$ ב- τ
 ו- τ ולכן סה"כ אורך ב- S_n ניתן להכתוב כמילה באורך $O(n^3)$ על ידי τ ו- σ .
 למעשה, $O(n^2)$ מספיק! למעשה $(ab) = (a \ a+1) \dots (a+2 \ a+3) \dots (a+1 \ a+2)$
 $\dots \underbrace{\sigma^{a+1} \tau \sigma^{-(a+1)}}_{\text{יש צמצומים}} \underbrace{\sigma^a \tau \sigma^{-a}}_{\text{יש צמצומים}} \dots \sigma^{a-1} \tau \sigma^{-(a-1)}$

אם אנו נותנים את זה על הסף אפשר לראות שבעצם התחילת (ab) הוא מילה
 באורך $O(n)$ ו- σ ו- τ ומכאן יוצא $O(n^2)$ תחלופים.



מיון בועות: יש מכונה שיכולה להסתובב ולהחליף את

שני האיברים שנמצאים בקוטר הצפוני. המטרה היא

לסדר את המספרים לפי הסדר. בדוגמה שאנחנו (המכונה

קופס תסתובב עד ש-2 ו-7 יבוצע בקוטר ותחילת בניהם. ואז 1 ו-2 יהיו אחד

אחד השני. אז המכונה תחילת בין 3 ל-10 ואז בין 3 ל-9 וכן הלאה עד ש-3 ו-10

י-4 יתחלפו ו-1,2,3 יהיו לפי הסדר. כנור שלכה אפשר לסדר.

בעצם מה שמכונה עושה זה לחלף את התמונה הראשונה בעזרת τ ו- σ

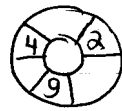
הנחנו אז שהאיבריתם עובד ב- $O(n^2)$. אנחנו נוכיח שאם אפשר להשיג

תסם טוב יותר. צריך להראות שקיימת תמונה (התחלית) שאי אפשר לסדר אותה

בפחות n - $O(n^2)$ צצים. באופן לא אפתי מפורסם התמונה יהפוכה.

$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ n & n-1 & \dots & 1 \end{pmatrix}$ שיטת $\{1, 2, \dots, n\}$ תיקרא רצה ביחס לתמונה π אם היא לא מסודרת.

15



בכיוון השעון. ב- π שלנו ב השליש נהוג ויש

$$\frac{n^3}{6} \sim \binom{n}{3}. \text{ סיבוב } \sigma \text{ ותזקזקתו } \tau \text{ אף שלישית ואילו תחילת } \tau$$

מתקן לא הייתה ח שלישית. לכן, כדי לסדר את π שלנו צריך להפעיל את

$$\tau \text{ לפחות } \frac{n^2}{6} \approx \frac{n^3}{6} \text{ פעמים, וסימנו, שהי הכאני ל- } \tau \text{ חייבת}$$

להגיע לפחות $O(n^2)$ פעמים...

הצעה: תמונה $\pi \in S_n$ נקראת זוגית אם היא נותנת צורתה של מספר זוגי של

חלופים ואתה תיקר איזוגית. אם π זוגית נסמן $sg(\pi) = 1$ ואם π איזוגית

נסמן $sg(\pi) = -1$. (שגור השאלה הגם סימן של תמונה מוגדר היטב?)

סעיף: יהא f הפולינום ב- n משתנים $x_1, \dots, x_n$. $f = \prod_{1 \leq i < j \leq n} (x_i - x_j)$. תבס S_n

תמונה. נסמן $f^\varphi = \prod_{1 \leq i < j \leq n} (x_{\varphi(i)} - x_{\varphi(j)})$. אז $f^\varphi = sg(\varphi) \cdot f$.

הוכחה: ראשית, נסמן שחילוף אחד מתחיל את הסיון. נניח שהיה לנו $x_1, \dots, x_i, \dots, x_j, \dots, x_n$

והחלפנו את זה ל- $x_1, \dots, x_j, \dots, x_i, \dots, x_n$. איך החילוף הזה משפיע על $\prod_{i < j} (x_{\varphi(i)} - x_{\varphi(j)})$?

אם $i < a$ אז $x_a - x_i, x_a - x_{\varphi(i)}$ בשני אופנים סימן כי עדיין $a < \varphi(i)$. אם

$j < a$ אז $x_j - x_a, x_{\varphi(j)} - x_a$ בשני אופנים סימן כי עדיין $a < \varphi(j)$. אם

$i < a < j$ אז יש שני אופנים משופעים: $x_i - x_a$ משנה סימן, $x_a - x_j$

משנה סימן. ב סאר הזוגי, ל- i ו- j לא מופיעים בהם ולא מושפעים. אז אנו

יש שנייה בסימן אחר ל- $j < a < i$. השנייה היא רחוק מתהלים. אז גורם $x_i - x_j$

הוא הופך שמתחיל סימן ולכן.

כעת, נניח φ מפלה של מספר זוגי של חלופים. הפעול φ על f פירושה הפעול

מספר זוגי של חלופים על f . ב חילוף משנה את הסימן אך בסה"כ φ אינה משנה

את הסימן של f . ואילו אם φ מפלה של מספר איזוגי של חלופים אז הסימן

של f מתחלף. כעת, אלה $\pm 1 = f/\varphi$ (נשים לב שמאחר ש φ תמונה אותם

האזורים שמופיעים בחנופה מופיעים גם בחנופה אך הם מתבטלים זה לנשאר זה

16

רק הסימן.

מסקנה: אם φ נותנת צורתה של מספר זוגי של חלופים אזי ב צורה של מספר

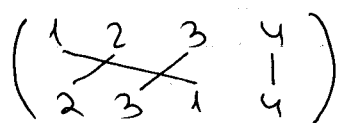
של חלופים היא מפלה של מספר זוגי של חלופים ונאפשר דומה זהו φ איזוגית.

הוכחה: נאמר f/φ קבועה ואינה תלויה בחלופים. לכן חלופים. $\Leftarrow$ חייבת

להיות החלופה לא יכל להיות ל- φ את הזוג והם איזוגית.

17

אין יוצאים מה הסמן של תמונה? יש כמה דרכים. אפשר לכתוב תמונה ברתים
 (הכל) ואז לתאר איך בשורה השנייה הצמנו בשורה התחתונה. מספר
 ההצמדות בין הקווים המתחברים אומר אי-סמן התמונה.



בפנימה משמאל יש שתי הצמדות
 ולכן התמונה זוגית.

אם צינן יותר נורמליזציה היא הסתגור ברתים המעופים. מעל האורך זוגי היא
 תמונה איזומורפית ומעל האורך איזומורפית היא תמונה זוגית. לכן תמונה היא זוגית
 אולם בהתבוננות במבנה מעופים יש מספר זוגי של מעופים האורך זוגי.
 במקרה שלנו התמונה היא (123) ובה אפשר מעופים האורך זוגי
 ולכן היא זוגית.

נתם הצמדות ב- S_n . אם G תבונה סגורה אז $a, b \in G$ (קראים צמדות) אם
 קיים $g \in G$ כך ש- $gag^{-1} = b$. בתורו ראנו שזה חסם שקילות.

סעיף תהיה π ! π' ב- S_n . נרשום אותן במסלול של מעופים לנים
 באותם יוצאים: $\pi = (a_1^1 \dots a_{r_1}^1) \dots (a_1^{l'} \dots a_{r_{l'}}^{l'})$; $\pi' = (b_1^1 \dots b_{r_1}^1) \dots (b_1^{l'} \dots b_{r_{l'}}^{l'})$. אז
 π ו- π' צמודות אם $l = l'$ ו- $r_i = s_i$ $1 \leq i \leq l$.

דוגמה: $\pi = (347)(52)(61)$ (צמודה) - $\pi' = (624)(71)(35)$ - $\pi'' = (713)(25)(46)$ - π''

הורחבו: הצמדה ב- g שקולה להפצלה g על התכנים:

$$g(a_1^1 \dots a_{r_1}^1)(a_1^2 \dots a_{r_2}^2) \dots (a_1^{l'} \dots a_{r_{l'}}^{l'})g^{-1} = (g(a_1^1) \dots g(a_{r_1}^1)) \dots (g(a_1^{l'} \dots g(a_{r_{l'}}^{l'}))$$

16) 12.11.04
זכור

אוטומופיזמים ואוטומופיזמים פנימיים

הגדרה: תבא G חבורה. הומומורפיזם $\phi: G \rightarrow G$ שהדומנה והקודם (ערכים) (תחום) אוטומופיזם.

טענה: אוטומופיזמים של G מהווה חבורה (ביחס לרכיב) $\text{Aut}(G)$ (החבורה) לשמאל $\text{Per}(G)$ (גרעין) של G .
הוכחה: איננו בוחנים את החבורה.

קל יותר: הוכחה של שני הומומורפיזמים הם הומומורפיזם ותנאי מלחמה
הוכחה של פונקציות הפיכות הם פונקציה הפיכה.

הלכנו: כל אוטומופיזם קיימת פונקציה הפיכה. צריך רק לבדוק

שהיא גם הומומורפיזם. נניח $\alpha: G \rightarrow G$ אוטומופיזם. אז

$$\alpha^{-1}: G \rightarrow G \text{ מוגדרת ע"י } \alpha^{-1}(x) = y \text{ אם } \alpha(y) = x$$

אנחנו רוצים להראות - $\alpha^{-1}(x_1 x_2) = \alpha^{-1}(x_1) \alpha^{-1}(x_2)$ נסמן $\alpha^{-1}(x_1) = y_1$

$$! \alpha^{-1}(x_2) = y_2 \text{ אז } \alpha(y_1) = x_1 \text{ ! } \alpha(y_2) = x_2 \text{ , כלומר ,}$$

$$\alpha^{-1}(x_1 x_2) = y_1 y_2 \iff \alpha(y_1 y_2) = \alpha(y_1) \alpha(y_2) = x_1 x_2$$

$$\alpha^{-1}(x_1 x_2) = \alpha^{-1}(x_1) \alpha^{-1}(x_2) \text{ וזה מה שרצנו.}$$

☺

הגדרה: תבא G חבורה והא $g \in G$ (צדד) אוטומופיזם

$$\iota_g: G \rightarrow G \text{ " } \iota_g(x) = g x g^{-1} \text{ (קרא אוטומופיזם פנימי).}$$

טענה: ι_g אוטומופיזם של G

הוכחה: ι_g הומומורפיזם לבדוק את הק"מ:

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

נראה ש- ι_g תהיה: $\iota_g(x) = \iota_g(y)$ אז $g x g^{-1} = g y g^{-1}$

נכפול מימין ב- g^{-1} ונקבל $x = y$.

$$\iota_g(g^{-1} x g) = g g^{-1} x g g^{-1} = x \quad x \in G \text{ כל } x$$

☺

טענה: יהי $i: G \rightarrow \text{Aut}(G)$ ההצבה $i(g) = i_g$ היא הומומורפיזם.

הוכחה: צריך להוכיח ש-
 $i(g_1 g_2) = i(g_1) i(g_2)$
 ה- Aut של G היא חבורה.

אם צריך להראות ש- $i(g_1 g_2) = i(g_1) \circ i(g_2)$ יהי $x \in G$ אז מתקיים
 $i_{g_1 g_2}(x) = (g_1 g_2) x (g_1 g_2)^{-1} = (g_1 g_2) x (g_2^{-1} g_1^{-1}) =$
 $= g_1 (g_2 x g_2^{-1}) g_1^{-1} = g_1 i_{g_2}(x) g_1^{-1} = i_{g_1} \circ i_{g_2}(x)$

Ⓜ

המשפט קי"ו הראנו שאם G אפשר לסמן ה- $\text{Per}(G)$ זרשן.
 ראנו עוד הומומורפיזם של G לתוך $\text{Per}(G)$, אפילו לתוך $\text{Aut}(G)$.
 אז לא נראה שיש להשתמש ב- i ? - כי רצינו לומר שזהו הומומורפיזם
 והיה חז"ל! וזה חשוב, כי זה אומר ש- G איננה חבורה אבל G
 $i_g = \text{id}$, שיהי $x = g g^{-1} x = x = g x g^{-1}$! אז ה- G חבורה
 קלסטרית איבר אחד - הצבת ה- i - וזהו זה שרצינו ...

תוצאה: $\text{Ker } i = Z(G)$ כאשר $Z(G)$ היא המרכז של G ,
 כלומר אוסף איברי G המתחברים עם כל איברי G .

מסקנה: אוסף האוטומורפיזמים הפנימיים של חבורה G מהווה חבורה
 חלקית של $\text{Aut}(G)$.

הוכחה: אוסף האוטומורפיזמים הפנימיים היא תת-חבורה של i .
 וידוע ש- $\text{Im } i = \text{Aut}(G)$ היא חבורה חלקית, לכן i הומומורפיזם. Ⓜ

Ⓜ' (הצגה של S_n)

$$g = (1644)(58)$$

$$x = (157)(26)(38) \quad \text{נסתב על}$$

$$: g \times g^{-1} \quad \text{נתם את ההצגה}$$

(14)

$$g \times g^{-1} = (1674)(58)(157)(26)(38)(1476)(58) =$$

$$= (1)(27)(35)(468) = (468)(27)(35) =$$

$$= (684)(27)(35) = (g(1) g(5) g(7))(g(2) g(6))(g(3) g(8))$$

זו תופעה מעניינת מאוד! הצמדה כ- g פוקדת את המסנה הצקדי של x ומחזירה את התבנית ה- g .

טענה: נניח שנתונה $x = (a_1^1 \dots a_{r_1}^1) \dots (a_1^l \dots a_{r_l}^l)$ תמונה של $g \in S_n$ מרצה של l ציקלוסים לריס מאונכים $r_1, \dots, r_l$ אזי $g \times g^{-1}$ יהיה כדל:

$$g \times g^{-1} = (g(a_1^1) \dots g(a_{r_1}^1)) \dots (g(a_1^l) \dots g(a_{r_l}^l))$$

סקירה: לתמונות צמודות יש אותו מסנה צקדי

סקירה: שתי תמונות עם אותו מסנה צקדי הן צמודות.

הוכחה: נניח שנתונה $x = (a_1^1 \dots a_{r_1}^1) \dots (a_1^l \dots a_{r_l}^l)$

$y = (b_1^1 \dots b_{r_1}^1) \dots (b_1^l \dots b_{r_l}^l)$

יחד זהויה שתיק, מה- r_i הם 1 דבר (נניח של $\{1, \dots, n\}$

מופיעים גם ב- x וגם ב- y . את התמונה g המוצגת ע"

$$g = \begin{pmatrix} a_1^1 \dots a_{r_1}^1 \dots a_1^l \dots a_{r_l}^l \\ b_1^1 \dots b_{r_1}^1 \dots b_1^l \dots b_{r_l}^l \end{pmatrix}$$

(15) מצמידה בין x ל- y , סומך $g \times g^{-1} = y$.

*הק (שם ל- g שהצטרנו בהלחה היא לא היחידה שמצמידה

בצמידה שלנו יש כמה אפשרויות, תיק מהן:

$$\begin{pmatrix} 157 & 26 & 38 & 4 \\ 684 & 27 & 35 & 1 \end{pmatrix} \quad \begin{pmatrix} 157 & 26 & 38 & 4 \\ 468 & 35 & 27 & 1 \end{pmatrix}$$

Partition Function מחלקות

פונקציה $\mathcal{P}: \mathbb{N} \rightarrow \mathbb{N}$ נאשר $\mathcal{P}(n)$ היא מספר האפשרויות לחלק את n מסומ של מספרים טבעיים חיוביים מספר יחיד.

$$\sigma(1) = 1$$

, למד

$$\sigma(2) = 3$$

$$2 = 2 \quad 2 = 1+1$$

$$\sigma(3) = 6$$

$$3 = 3 \quad 3 = 2+1 \quad 3 = 1+1+1$$

$$\sigma(4) = 10$$

$$4 = 4 \quad 4 = 3+1 \quad 4 = 2+2 \quad 4 = 2+1+1$$

$$4 = 1+1+1+1$$

$$\sigma(7) = 15$$

$$7 = 7 = 6+1 = 5+2 = 5+1+1 = 4+3 =$$

$$= 4+2+1 = 4+1+1+1 = 3+3+1 =$$

$$= 3+2+2 = 3+2+1+1 = 3+1+1+1+1 =$$

$$= 2+2+2+1 = 2+2+1+1+1 =$$

$$= 2+1+1+1+1+1 = 1+1+1+1+1+1+1$$

אקסנה: מספר מחלקות ה- S_n היא $\sigma(n) = Pr(n)$ שהיא מסתברת של מה שמעניין אותנו זה מספר ה- $Pr(n)$...

חבורות חלקיות (נוחיות) ותכונות מנה

הגדרה: חבורה חלקית H של חבורה G נקראת נוחית אם לכל $g \in G$ מתקיים $gHg^{-1} = H$. במקרה זה נסמן $H \triangleleft G$.

הערה: בחבורה אבליה G כל חבורה חלקית היא נוחית.

שענה: נניח G חבורה, $H \leq G$ חבורה חלקית. אזי התנאים הבאים שקולים:

$$H \triangleleft G \quad (א)$$

$$gH = Hg \quad g \in G \quad (ב) \quad \text{כל } g \in G \text{ (כלומר לכל } g \text{ שכן } H \text{ חלקית)}$$

$$gHg^{-1} = H \quad (ג) \quad \text{כל } g \in G \text{ (כלומר לכל } g \text{ שכן } H \text{ חלקית)}$$

הוכחה:

$$(א) \Rightarrow (ב) \quad gHg^{-1} = H \quad \text{(נפיל אינ' ב-} g \text{ ונקח)}$$

$$(ב) \Rightarrow (א) \quad gHg^{-1} = H \quad \text{(נפיל אינ' ב-} g^{-1} \text{ ונקח)}$$

$$(ב) \Rightarrow (ג) \quad \text{ברור}$$

$$(ג) \Rightarrow (א) \quad \text{אם } gHg^{-1} = H \text{ אזי } H \text{ חלקית. } \triangleleft$$

(18)

g רק e - $gH = Hg$. אפוא זה אומר $e = ge \in Hg$.

$\Leftarrow$ $Hg = [g] = Hg$, לכן $g \in g^{-1}H$ באותה מחלקה לקוחה

של מחלקות ימניות של H . $\Leftarrow gH = Hg$. (19)

בידור: תהי G חבורה ותהי $N \triangleleft G$ חבורה חזקה נורמלית. (20)

חבורת מנה G/N מכונה חבורה אברהיחבורה הם המחלקות

השלמאיות של N ב- G (לשכחן הימניות). הפעל מחדש רק:

$$(g_1 N) \cdot (g_2 N) = (g_1 g_2) N$$

טענה: הפעל ב- G/N מחדש הישם.

נזכיר את הטענה של G אכן קוראים לזה לפרק תוצאות

אברהיחבורה של G/N היא $N = eN$, לכן

$$(g_1 N)(eN) = (g_1 e)N = g_1 N$$

$$(eN)(g_1 N) = (eg_1)N = g_1 N$$

זכור $gN \in G/N$ האברהיחבורה הפעל היא $(gN)^{-1} = g^{-1}N$

$$(gN)(g^{-1}N) = (gg^{-1})N = eN$$

יש אברהיחבורה הפעל האברהיחבורה ב- G :

$$\begin{aligned} [(g_1 N)(g_2 N)](g_3 N) &= ((g_1 g_2)N)(g_3 N) = ((g_1 g_2)g_3)N = \\ &= (g_1(g_2 g_3))N = (g_1 N)((g_2 g_3)N) = \\ &= (g_1 N)[(g_2 N)(g_3 N)] \end{aligned}$$

טענה: הפעל מחדש הישם.

הוכחה: ליה e - $g_1 N = x_1 N$; $g_2 N = x_2 N$ זכור אברהיחבורה

e - $g_1 g_2 N = x_1 x_2 N$, או לחלופין $(g_1 g_2)(x_1 x_2)^{-1} \in N$

$$(g_1 g_2)(x_1 x_2)^{-1} = g_1 g_2 x_2^{-1} x_1^{-1}$$

ותהי e - $g_2 N = x_2 N \Leftarrow g_2 x_2^{-1} \in N \Leftarrow g_2 x_2^{-1} = n' \in N$

$$g_1 g_2 x_2^{-1} x_1^{-1} = g_1 n' x_1^{-1} = (g_1 n' g_1^{-1})(g_1 x_1^{-1})$$

$g_1 n' g_1^{-1} \in N$ כי N נורמלית וכן $g_1 x_1^{-1} \in N$ כי $g_1 N = x_1 N$

$$g_1 g_2 x_2^{-1} x_1^{-1} = g_1 n' x_1^{-1} \in N \Leftarrow$$

(21)

$$\text{קריאה: } G = \mathbb{Z} \quad ! \quad N = m\mathbb{Z} \quad \text{אז} \quad G/N = \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$$

לכדי להחזיקו של $\mathbb{Z}_m$ הן בדיוק רפי הנסכיות של איברים הם
 שקולים אחד ישרהם אחר שאלויה בחוקה - m .

תבונות נורמליות

G תבורה. $N \leq G$ תיקרא נורמלית ותסומן $N \triangleleft G$ או $N \trianglelefteq G$ אם לכל $g \in G$ $gNg^{-1} = N$ (אובייקט לקח $g^{-1}Ng = N$).

טענה: $N \leq G$ תבורה חלקית. אזי התנאים הבאים שקולים:

- (1) $N \triangleleft G$
- (2) לכל $g \in N$ $g^{-1}Ng \subseteq N$
- (3) לכל $g \in G$ אם $n \in N$ אז $g^{-1}ng \in N$

הוכחה:

$$(1) \Leftrightarrow (2) \Leftrightarrow (3)$$

(1) $\Leftrightarrow$ (3) ברור ש- (3) אומר שלכל $g \in G$ $g^{-1}Ng \subseteq N$. מה שצריך להוכיח הוא שיש שוויון, כלומר שלכל $n \in N$ קיים $m \in N$ כך ש- $g^{-1}ng = m$. ואכן, נבחר $n_0 = g^{-1}ng$. $n_0 \in N$ ע"פ (3) כי $n_0 = (g^{-1})^{-1}n(g^{-1}) \in N$ ואז $g^{-1}ng = g^{-1}(gng^{-1})g = n$ 

אנדרה: "תן מצד שני H תבורה חלקית ו- $g \in G$ כך ש- $g^{-1}Hg \neq H$ אבל אם H נורמלית לכל $g \in G$ שיתן שקורה לכל $g \in G$."

דוגמאות:

(1) F שדה, $G = GL_n(F)$, $N = SL_n(F)$. אז $N \triangleleft G$ כי

$$g \in G, n \in N \Rightarrow g^{-1}ng \in N$$

$$\det(gng^{-1}) = \det(g)\det(n)\det(g^{-1}) = \det(g) \cdot 1 \cdot \det(g)^{-1} = 1$$

(2) $G = S_n$, $N = A_n$ (תבורה התיאורית-הזוגית על $\{1, \dots, n\}$)

$g \in S_n$ זוגי או אי-זוגי. אם n זוגי אז $g^{-1} \in S_n$ זוגי. אם n אי-זוגי אז $g^{-1} \in S_n$ אי-זוגי. נניח ש- n אי-זוגי. אז g אי-זוגי. אז gng^{-1} אי-זוגי. אז $gng^{-1} \in A_n$ כי $l+m+l = 2(l+m)$ אי-זוגי. אז $N \triangleleft G$.

צריך שקורה לומר לאי-היות $\text{sgn}: S_n \rightarrow \{\pm 1\}$ (היא הומומורפיזם). $A_n = \text{Ker}(\text{sgn})$

③ G חבורה $\varphi: G \rightarrow M$ הומומורפיזם. $N = \text{Ker } \varphi$

אז $N \triangleleft G$. אם $n \in N$, $g \in G$ אז

$$\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g)^{-1} = \varphi(g)e_n\varphi(g)^{-1} = e_n$$

$$. N \triangleleft G \iff gng^{-1} \in \text{Ker } \varphi \iff$$

לענין: אם חבורה חזקה $N \triangleleft G$ קיימת חבורה M ואפימורפיזם

$$\varphi: G \rightarrow M \text{ כן, } N = \text{Ker } \varphi$$

הוכחה: תבא $M = G/N$, נומר איברי M הם המעלקות

השטחיות של N ב- G . ראוי שאולי המעלקות מהווה חבורה ביחס

$$\text{לחיבור הרגל } (g_1N)(g_2N) = (g_1g_2)N$$

נצייר הצתקה $\varphi: G \rightarrow G/N$ זו $\varphi(g) = gN$. (ראו)

ל- φ הומומורפיזם (ברור ל- φ) : אם $g_1, g_2 \in G$

$$\varphi(g_1g_2) = (g_1g_2)N = (g_1N)(g_2N) = \varphi(g_1)\varphi(g_2)$$

כזה, נסמן ל- $N = \text{Ker } \varphi$. $e_{G/N} = eN = N$. כזה

$$\text{Ker } \varphi = \{g \in G : gN = N\} = \{g \in G : g \in N\} = N$$

Ⓜ

משפט ההומומורפיזם (הראשון): תהיה G ו- M חבורות, $\varphi: G \rightarrow M$

$$\bar{G} = \text{Im } \varphi \quad (\bar{G} \text{ אפימורפיזם של } G)$$

$$\bar{G} \cong G / \text{Ker } \varphi$$

דוגמה: $G = GL_n(F)$ $\det: GL_n(F) \rightarrow F^*$ לה הומומורפיזם

$N = GL_n(F)$ - $F^* = F \setminus \{0\}$ שום חבורה ביחס לכפולת הכפל.

הזרעין היא $SL_n(F)$. התמונה היא F^* כי אם $a \in F^*$

$$\text{אז } \det \begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = a$$

$$\text{ל- } GL_n(F) / SL_n(F) \cong F^*.$$

הוכחת המשפט: יש לנו אפימורפיזם $\varphi: G \rightarrow \bar{G}$. נצייר הצתקה

$$\bar{\varphi}: G/N \rightarrow \bar{G} \quad (\text{כאשר } N = \text{Ker } \varphi)$$

תבוא $g \in G$ נצייר $\bar{\varphi}(gN) = \varphi(g)$. (כפוף ל- $\bar{\varphi}$ מוגדר

היטב. זכים להראות שאין תלות בהחירה הנבחרת.

נניח ש- $gN = g'N$ אז $g' = gn$ לכל $n \in N$.
 אז $\varphi(g'N) = \varphi(gN)$. אבל φ הומומורפיזם אז $\varphi(gn) = \varphi(g)\varphi(n)$
 והרי $n \in \text{Ker } \varphi \Leftrightarrow \varphi(g') = \varphi(g) \Leftrightarrow \bar{\varphi}(g'N) = \bar{\varphi}(gN)$ אז $\bar{\varphi}$ אוניברסל היטב.
 (והרוביק, ש- $\bar{\varphi}$ איזומומורפיזם:

$$\begin{aligned}\bar{\varphi}(g_1 N g_2 N) &= \bar{\varphi}(g_1 g_2 N) = \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) = \\ &= \bar{\varphi}(g_1 N) \bar{\varphi}(g_2 N)\end{aligned}$$

$\bar{\varphi}$ הומומורפיזם.

$\bar{\varphi}$ על כי אם $h \in \bar{G}$ יהיו שקיים $g \in G$ כך ש- $\varphi(g) = h$ (כי φ על G)
 אז $\bar{\varphi}(gN) = \varphi(g) = h$.

בתכנה נניח ש- $\varphi: G \rightarrow H$ הומומורפיזם אז φ תהיה אנוני
 $\text{Ker } \varphi = \{e_G\}$. אז כדי להוכיח ש- $\bar{\varphi}$ תהיה צריך להראות ש-
 $\bar{\varphi}(gN) = e_{\bar{G}}$ אז $gN = N$. ואכן, אם $\bar{\varphi}(gN) = e_{\bar{G}}$
 $\varphi(g) = e_H \Leftrightarrow g \in \text{Ker } \varphi = N \Leftrightarrow gN = N$.

(11)

דוגמה (תרגיל): אם G תבורה, $N \triangleleft G$, $H \leq G$ אז HN תבורה
 חלקי של G , המכילה את N ואת H ובורה ש- $N \triangleleft HN$.
אלהה תמונה: בצד HN אינה תבורה. אבל אם אחת-למק (נוחשים)
 אז לוקח תבורה.

משפט ההומומורפיזם (השני): תהי G תבורה (להיניח $N \triangleleft G$, $H \leq G$).
 אז $HN/N \cong H/H \cap N$ (כל $H \cap N \triangleleft H$ (התבורה איזומומורפיה)).

דוגמה: G תבורה, $N \triangleleft G$, $H \leq G$ אז $H \cap N \triangleleft H$.
הוכחה: צריך להוכיח ש- $h \in H$, $n \in H \cap N$ אז $h^{-1}nh \in H \cap N$
 ואכן $h^{-1}nh \in H$ כי $h^{-1}, n, h \in H$. ומצד שני, $h^{-1}nh \in N$ כי
 N נורמלית. $\bar{h}^{-1}\bar{n}\bar{h} \in HN/N \Leftrightarrow h^{-1}nh \in H \cap N$.

(12)

הוכחת המשפט: נגדיר הומומורפיזם $\varphi: H \rightarrow HN/N$ ע"י $\varphi(h) = hN$.
 לה הומומורפיזם כי $\varphi = \varphi|_H$ כאשר $\varphi: HN \rightarrow HN/N$ $hn \mapsto hnN$ ו- φ צמצום
 של הומומורפיזם אחר לה בולבאי הומומורפיזם.

φ הוא גזס פא כי אם $gN \in H^N/N$ אזי g ניתן לפרטיקה
 כ- $g = h_1 n_1$ אז $gN = h_1 n_1 N = h_1 N$ $\varphi(h_1) = h_1 N = gN$
 (בעצם, אחרת האן שלם אפר של H^N/N שהוא מתקפה של N
 יש צג מתק h).

$$\text{Ker } \varphi = \{h \in H : \varphi(h) = e_{H^N/N}\} = \bigcup \text{Ker } \varphi \quad \text{מהו}$$

$$= \{h \in H : hN = N\} = \{h \in H : h \in N\} = H \cap N$$

(אחר H זרעין של נומורפזם אפר היסו נכחליר אפר אר
 היינו חיבור לפרכיה אר זה קוצם).

כזה, אפי משט פדומומורפזם הראשון $H/H \cap N \cong H^N/N$ (11)

משט פדומומורפזם (השלישי): תהי G חבורה ונניח K, N

חבורה חלקייה נוחליוג ב- G יק ש- $N \subseteq K \subseteq G$ אז

$$K/N \triangleleft G/N$$

$$(G/N)/(K/N) \cong G/K \quad \text{וכ}$$

הוכחה בשילור והם

21) 19.11.07
מכנים

נניח G - קבוצה, M - חבורה, $\varphi: G \rightarrow M$ הומומורפיזם (נסמך)

$N = \text{Ker } \varphi$ אם $g \in G$! $h \in N$ אז

$\varphi(gN) = \varphi(g)$ כי $\varphi(gN) = \varphi(g) \varphi(h) = \varphi(g)$

הזדהות $\bar{\varphi}: G/N \rightarrow M$ המוגדרת "ז" $\bar{\varphi}(gN) = \varphi(g)$ התאמת

ל $\bar{\varphi}$ שמה $\text{Im}(\varphi)$ $\bar{\varphi}$ הומומורפיזם מחבורת המנה G/N ל M :

$$\bar{\varphi}(g_1 N \cdot g_2 N) = \bar{\varphi}(g_1 g_2 N) = \varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) = \bar{\varphi}(g_1 N) \cdot \bar{\varphi}(g_2 N)$$

וכן $\text{Ker } \bar{\varphi}$

$$\text{Ker } \bar{\varphi} = \{gN : \bar{\varphi}(gN) = e_M\} = \{gN : \varphi(g) = e_M\} = \{N\} = \{e_G\}$$

תורת השלש: הומומורפיזם φ היא חתך אנני $\text{Ker } \varphi = \{e\}$

מכאן נראה ש- $\bar{\varphi}$ חתך וסוגו זה הזדהות (נסמך)

משפט ההומומורפיזם הרגולרי: אם $\varphi: G \rightarrow M$ הומומורפיזם אז φ

משנה איזומורפיזם $\bar{\varphi}: G/N \rightarrow \text{Im}(\varphi)$ ה"ה, "ז" $\bar{\varphi}(gN) = \varphi(g)$

אז $N = \text{Ker } \varphi$

דוגמאות:

$$\varphi(x) = x \pmod{n} \quad \varphi: \mathbb{Z} \rightarrow \mathbb{Z}_n \quad (1)$$

$$\text{Ker } \varphi = n\mathbb{Z}$$

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

$$f(x) = e^{2\pi i x} \quad f: \mathbb{R} \rightarrow S^1 = \{z \in \mathbb{C} : |z| = 1\} \quad (2)$$

$$e^{2\pi i x} = \cos 2\pi x + i \sin 2\pi x \quad \text{מספר מרוכב (הכיוון)}$$

$$f(x+y) = e^{2\pi i(x+y)} = e^{2\pi i x + 2\pi i y} = e^{2\pi i x} \cdot e^{2\pi i y} = f(x) f(y)$$

זו הזדהות של $\mathbb{R}$ אל S^1 $f|_{[0,1]}$ היא רצף

$$\text{Ker } f = \mathbb{Z} \quad \text{הזדהות של } f \text{ היא}$$

$$\Rightarrow \mathbb{R}/\mathbb{Z} \cong S^1$$

$\mathbb{R}/\mathbb{Z}$ הנקרא מה שמעניין אותו הוא השטח $\mathbb{R}$ מודול 1 (כחור)

החוק השלש. אראוה יש שם משתתף קצת מופתע (פלאי איזומורפיזם)

פונקציות אלה הן S^1 הוא למשל חיבור צווי!

③ $\text{sign}: S_n \rightarrow \{\pm 1\}$ תכונה (כפול)
 והתמונה $\text{Ker Sign} = A_n$ והצלחה
 $\Rightarrow S_n/A_n \cong \{\pm 1\}$

④ $\text{det}: GL_n(F) \rightarrow F^*$ של F
 $\text{Ker det} = SL_n(F)$ וכן
 $\Rightarrow GL_n(F)/SL_n(F) \cong F^*$

למה: נניח $\varphi: G \rightarrow M$ הומומורפיזם. אם $N = \text{Ker } \varphi$
 תהא H ת"ח בשהי של G . וכן $HN = NH$ וזו ת"ח של G .
הוכחה: אם $n \in N$, $h \in H$ וכן
 $hn = \underbrace{hn h^{-1}}_{n' \in N} \cdot h = n' h$

$HN \subseteq NH \quad \Leftarrow$
 מצד שני,
 $NH \subseteq HN \quad \Leftarrow$
 $HN = NH \quad \Leftarrow$

נותר לבדוק שזו תכונה חלוקה. (נראה ש- HN חבורה חלוקה).
 זרים זהבאל שאם $h_1, h_2 \in H$, $n_1, n_2 \in N$ וכן $h_1 n_1, h_2 n_2 \in HN$
 $h_1 n_1 h_2 n_2 = \underbrace{h_1 h_2}_{H \ni h} \underbrace{h_2^{-1} n_1 h_2}_{n \in N} n_2 = hn \in HN$
 אז יש סגורות חלוקה. (נותר להראות סגורות כיתום לחלופי).
 $(hn)^{-1} = n^{-1} h^{-1} \in NH = HN$

אם ישנם סגורות לחלופי. $\Leftarrow$ זו תכונה חלוקה
 (11)

נשים לב ש- HN זו חבורה חלוקה הנחלקת את H ואי N . כחור
 ש- $N \triangleleft HN$ אם ניתן לבדוק ש- HN/N

משפט ההומומורפיזם השני: תהא G חבורה; $H \leq G$, $N \triangleleft G$
 אזי HN חבורה חלוקה של G הנחלקת את N ומתקיים
 $HN/N \cong H/H \cap N$

הוכחה: נתבונן בהטויה הנחה G/N ובהצגה הסבירה
 $\pi: G \rightarrow G/N$ המוגדרת ע"י $\pi(g) = gN$

(22) נשים $\heartsuit$ של HN/N זו תמונה חזקה של G/N כי HN/N זה אוסף החזקות של N הנחלקות ב- HN (נשים HN עצם xN מחלקה של N החתוכה את HN באיבר y ואזי G החזקה xN נמצאת ב- HN להיו $y = xh_1$ ו $y = h_2n_2$ כך
 $(yN = xN = h_1N \subseteq HN$ אז $\pi(HN) = HN/N \subseteq G/N$ (אם π של $\pi(HN) = \pi(H)$ למי אם $hn \in HN$ אז
 $\pi(hn) = \pi(h) \cdot \pi(n) = (hN) \cdot (eN) = hN = \pi(h)$
 סיכום בעיניים: אם נצמצם את π ונראה אותו בהומומורפיזם H/N -
 G/N אזי תמונתו היא HN/N .
 מהו $\ker(\pi|_H)$?

$$\ker(\pi|_H) = \{h \in H : \pi(h) = e_{G/N}\} = \{h \in H : hN = N\} = \{h \in H : h \in N\} = H \cap N.$$

נשתדף משפט ההומומורפיזם הנגשן עבור $\pi|_H$ מתקבל

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

משפט ההתאמה: תהי G תצורה, $N \triangleleft G$. תהי $\pi: G \rightarrow G/N$
 ההסטה הסטנדרטית ק"מ-ה התאמה $\bar{\pi}$ חז"ז ו $\bar{\pi}$ בין הת"ח
 של G/N לבין הת"ח של G הנחלקות את N . התאמה
 זו ניתנת ע"י: אם $N \leq L \leq G$ אז $\bar{\pi}(L) = \pi(L)$
 אם $M \leq G/N$ אז $\bar{\pi}^{-1}(M) = \{g \in G : \pi(g) \in M\} = \pi^{-1}(M)$

במילים אחרות, ההומומורפיזם הסטנדרטי $\pi: G \rightarrow G/N$ משלח
 התאמה תה"ז ו $\bar{\pi}$ בין הקבוצות $\{L : N \leq L \leq G\}$ לבין
 $\{M : M \leq G/N\}$ הניתנת ע"י $L \mapsto \pi(L)$! $M \mapsto \pi^{-1}(M)$
הערה: עבור שאם L תצורה חזקה של G הנחלקת את N אז
 $\pi(L)$ תצורה חזקה של G/N . כמו כן, $\pi^{-1}(M)$ אם היא
 תצורה חזקה.

למה: אם $\psi: G \rightarrow S$ הומומורפיזם ψ ת"ח של S אז
 $\psi^{-1}(T)$ ת"ח של G הנחלקת את $\ker \psi$.

הוכחת תהא: נניח $g_1, g_2 \in \varphi^{-1}(T)$ ו- $g_1 g_2^{-1} \in \varphi^{-1}(T)$ - ל
 $\varphi(g_1 g_2^{-1}) = \varphi(g_1) \varphi(g_2)^{-1} \in T$ ואכן
 $S \subseteq \varphi^{-1}(T) \iff g_1 g_2^{-1} \in \varphi^{-1}(T) \iff$
 $\text{Ker } \varphi$ כחבורה נורמלית. $\odot$

(חשוב להוכיח את המשפט).

(ראה שבתאמה זו היא חתך ושל).

של: תהא M חתך של G/N . נסמן $L = \pi^{-1}(M)$ ונראה

ל- $\pi(L) = M$. זה ברור כי $\pi(\pi^{-1}(M)) \subseteq M$

אם $m \in M$ יש $g \in G$ כך ש- $\pi(g) = m$

כי π על. g זה נמצא ב- $\pi^{-1}(M)$ ע"פ ההגדרה.

$\pi(\pi^{-1}(M)) = M$ $\iff \pi(L) = M$ $\iff$

חתך: אם L_1, L_2 חבורות תת-קבוצות של G הנחלקות

אם N רק ל- $\pi(L_1) = \pi(L_2)$ אם נראה ל- $L_1 = L_2$.

(נראה ל- $L_1 \subseteq L_2$ (ובאופן סימטרי אם $L_2 \subseteq L_1$).

יהי $g \in L_1$. אזי קיים $h \in L_2$ כך ש- $\pi(g) = \pi(h)$.

בואו $gN = hN$. $\iff g \in hN$ $\iff g \in hN$, בואו קיים n

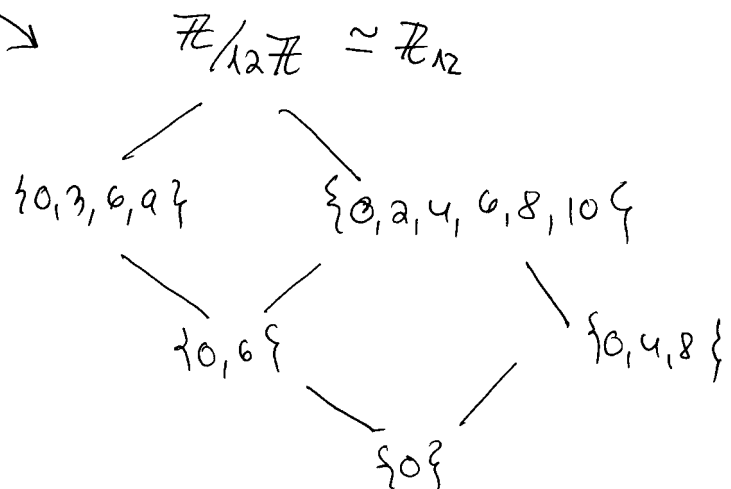
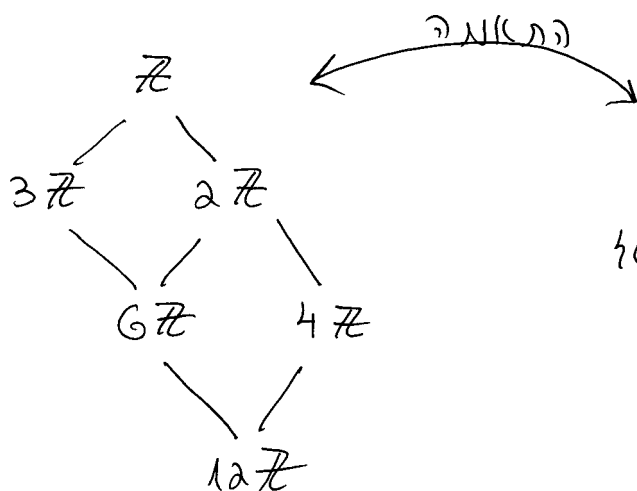
$h \in N$ - $h = g n$. אם $N \subseteq L_2$ אז $g \in L_2$ $\iff$

$L_1 \subseteq L_2$ $\iff g \in L_2$ $\iff$

$\odot$

דוגמה: מהן החבורות של $\mathbb{Z}$? ב החבורות מהצורה

$\mathbb{Z}$. מהן החבורות של $\mathbb{Z}_n$? ב החבורות
 $\mathbb{Z}$ רק ל- $n|12$.



23

משפט ההומומורפיזם השלישי: אם G חבורה, N, K חבורות
 תת-חבורות נורמליות של G , $N \subseteq K$ אז $K/N \trianglelefteq G/N$
 וכן $(G/N)/(K/N) \cong G/K$

הוכחה: נבדוק תכונות $K/N \trianglelefteq G/N$: יהיו $gN \in G/N$
 ! $kN \in K/N$. צריך להראות ש- $(gN)(kN)(gN)^{-1} \in K/N$
 $(gN)(kN)(gN)^{-1} = (gN)(kN)(g^{-1}N) = \underbrace{gkg^{-1}}_{k' \in K} N = k'N \in K/N$

נגדיר תמונה ההומומורפיזם $\psi: G/N \rightarrow G/K$ $\psi(gN) = gK$

ψ מוגדרת היטב כי אם $g_1N = g_2N$ אז $g_1 = g_2n$ עבור

$n \in N \subseteq K$. $\psi(g_1N) = \psi(g_2N)$, $g_1K = g_2nK = g_2K$

ψ היא פונקציה אם $gK \in G/K$ אז $gK = \psi(gN)$

עכשיו, $\ker \psi = \{gN \in G/N : \psi(gN) = e_{G/K}\} =$

$= \{gN \in G/N : \psi(gN) = e_K\} = \{gN : gK = e_K\} =$

$= \{gN : g \in K\} = K/N$

לפי תוצאות קודמות ψ איזומורפיזם בין G/N ל- G/K שבהם

K/N הוא איבר השני של ההומומורפיזם ההוא

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

24

$$\left(\mathbb{Z}/12\mathbb{Z} \right) / \left(6\mathbb{Z}/12\mathbb{Z} \right) \cong \mathbb{Z}/6\mathbb{Z}$$

דוגמה: $G = \mathbb{Z}$

$\downarrow$

$K = 6\mathbb{Z}$

$\downarrow$

$N = 12\mathbb{Z}$

Zassenhaus (1932)

נניח ש- G תבורה ! $A \triangleleft A^*$ $B \triangleleft B^*$ 4 תבורה חלקית

ש- G אז ! $A(A^* \cap B) \triangleleft A(A^* \cap B^*)$

$B(B^* \cap A) \triangleleft B(B^* \cap A^*)$

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \cong \frac{B(B^* \cap A^*)}{B(B^* \cap A)}$$

וקיים איזומורפיזם

למה:

1) אם $B \triangleleft B^*$! A 3 תבורה חלקית של G אז

$$A \cap B \triangleleft A \cap B^*$$

2) אם N, K תבורה חלקית (נוכחיות) של G אז KN (נוכחיות)

הוכחה:

1) תבא $g \in A \cap B^*$ ו- $n \in A \cap B$ זיק-פדראו-ש-

$gng^{-1} \in A \cap B$ אבל $n \in B$! $g \in B^*$! $B \triangleleft B^*$

אז $gng^{-1} \in B$ מצד שני אם $g \in A$ ואם $n \in A$ אז

$$gng^{-1} \in A \cap B$$

נניח ש- $g \in G$! $kn \in KN$ אז למחרת ש-

$$g^{-1}knng = \underbrace{g^{-1}kg}_{\in K} \underbrace{gng^{-1}}_{\in N} \in KN$$

אז, בתורו ראינו ש- KN תבורה.

⊙

הוכחת זאסנאוס

לפי למה 1 $A \cap B^* \triangleleft A^* \cap B^*$ והאכן צומה $A^* \cap B \triangleleft A^* \cap B^*$

2) לפי למה 2 $(A^* \cap B)(A \cap B^*) \triangleleft A^* \cap B^*$ (נסמן D כך)

אז $(A^* \cap B)(A \cap B^*) \triangleleft B(B^* \cap A^*)$ (נסתר) $B(B^* \cap A^*) \triangleleft B^*$

! $B \triangleleft B^*$ אז $B(B^* \cap A^*)$ תת-תבורה של B^* ובפרט

תת-תבורה של G . נניח ש- $x \in B(B^* \cap A^*)$ מהצורה $x = bc$

כאשר $c \in B^* \cap A^*$ ו- $b \in B$ (חזיר)

$$f(x) = f(bc) = c \in D \quad f: B(B^* \cap A^*) \rightarrow \frac{A^* \cap B^*}{D}$$

$\phi \neq (3)$

$$\text{Ker } f = B(B^* \cap A) \quad (4)$$

אם צריך להוכיח את טענת הנזכר נקבע
נוסחה ומשפט הפורמורפליזם הראשון

$B(B^* \cap A)$ - ע

$$\frac{B(B^* \cap A^*)}{B(B^* \cap A)} \cong \frac{A^* \cap B^*}{(A^* \cap B)(B^* \cap A)}$$

במסלול הנסימטריה בין A - B אתמים זמ

$$\frac{A(A^* \cap B^*)}{A(A^* \cap B)} \approx \frac{B^* \cap A^*}{(B^* \cap A)(A^* \cap B)}$$

$$\frac{B(B^* \cap A^*)}{B(B^* \cap A)} \cong \frac{A(A^* \cap B^*)}{A(A^* \cap B)} \quad - \text{e joni}$$

ראוי רק אהלכיר שמתפלל שמי גת חבורי היס חבורה

$$(A^* \cap B)(B^* \cap A) = (B^* \cap A)(A^* \cap B) \quad \text{רשמי נחלק (החלוקה)}$$

ה'אבות' סענות ה'על:

(1) $\neq$ מומצאת היטב: (יית) $x = bc = b'c'$ כאשר $b, b' \in B$

3K. $C, C' \in B^* \cap A^* - !$

$$B^* \cap A^* \ni c'c^{-1} = b'^{-1}b \in B$$

$$C'C^{-1} \in B \cap (B^* \cap A^*) = B \cap A^* \subseteq D$$

$C'D = CD$ (כי לאור ההיזרה של השקוף אובדו D) $\Leftarrow$

! $x = ey \in B(B^* \cap A^*)$ $\exists x \ y \in A^* \cap B^*$ $\text{OK} : \text{f (3)}$

$$f(x) = y \cdot D$$

$$c, c_1 \in B^* \cap A^*, \quad b, b_1 \in B \quad \text{then } y = b_1 c_1 \quad \text{and } x = bc \quad \text{--- (2)}$$

$$f(x) \cdot f(y) = (C \cdot D)(C_1 \cdot D) = (CC_1) D$$

$$f(xy) = f(bc \underbrace{b_1 c^{-1}}_e c_1) = f(bc c_1) = f(bcc_1)$$

$$CEB^*NA^*CB^* \vdash B \triangleleft B^*, \quad \overbrace{B}^{EB} \quad \overbrace{EB^*NA^*}$$

$C' \in B^* A^*$; $b' \in B$ נחזור $b' C'$ נבחר xy כעת נתבונן

המרחב f - הוא מרחב הוויכוח CC_1D -

25

(4) נתון את הגרעין φ :

$$\text{Ker } \varphi = \{x \in B(B^* \cap A^*) : \varphi(x) = e_{A^* \cap B^*}\}$$

$$= \{x = bc : b \in B \wedge c \in B^* \cap A^* \wedge cD = D\} =$$

$$= \{x = bc : c \in D\} = BD = \underline{B(A^* \cap B)(B^* \cap A)} =$$

$$A^* \cap B \subseteq B \text{ כי } = B$$

$$= B(B^* \cap A)$$

כלומר סימני את האות c החדר והאות b (האות a כולה).

11

(11) צורות נורמליות

(1) תהא G חבורה סדורה של חבורות חלקיות $G = G_0 \geq G_1 \geq \dots \geq G_\ell = \{e\}$

תיקרא סדרה נורמלית אם לכל $0 \leq i \leq \ell-1$ $G_{i+1} \triangleleft G_i$

$$G = G_0 \geq G_1 \geq \dots \geq G_\ell = \{e\}$$

$$G = H_0 \geq H_1 \geq \dots \geq H_m = \{e\}$$

סדרה נורמלית G נאמר שהשנייה צידון של הראשונה

$$\{G_0, G_1, \dots, G_\ell\} \subseteq \{H_0, H_1, \dots, H_m\}$$

אם

ואז אל אחת של

הסדרה אינה צידון

של השנייה

$$\mathbb{Z}_{10}$$

$$\downarrow$$

$$\{0, 2, 4, 6, 8\}$$

$$\downarrow$$

$$\{0\}$$

$$\mathbb{Z}_{10}$$

$$\downarrow$$

$$\{0, 5\}$$

$$\downarrow$$

$$\{0\}$$

דוגמה:

האמינים לעדון את הסדרה האלה? טכניקת התשובה היא תמיד

כן כי אפשר לבדוק את $\mathbb{Z}_{10}$ סדרה, אבל זה טריוויאלי.

המקרה הזה אי אפשר לעדון אותו מאופן לא טריוויאלי.

(3) שתי סדרה נורמלית $\{G_i\}_{i=0}^l$ ו- $\{H_j\}_{j=0}^m$ תיקראנה שקולות

אם $m=l$ וקיימת התאמה חד-חד ערכית בין החבורה הסדורה

$$\{G_i/G_{i+1}\}_{i=0}^{l-1} \quad ! \quad \{H_j/H_{j+1}\}_{j=0}^{m-1}$$

איזומורפיות. (כלל הכפוליות אם יש נאמה)

משפט העציון של Schrier (1928)

תבא G חבורה $\{G_i\}_{i=0}^l$ $\{H_j\}_{j=0}^m$ סדרות נורמליות

ה- G אז יש עתה עציונים שקולים

הוכחה: נגדיר $G_{ij} = G_{i+1} (G_i \cap H_j)$ עבור $0 \leq i \leq l-1$

!- $0 \leq j \leq m-1$ אם נסמן $H_{j+1} = B^*$, $G_{i+1} = A$, $G_i = A^*$, $H_j = B$

אז לפי אלמנט Zassenhaus במהרה $0 \leq j \leq m$

$$G_{ij} = G_{i+1} (G_i \cap H_j) = A(A^* \cap B) \triangleleft A(A^* \cap B^*) = G_{i+1} (G_i \cap H_{j+1}) = G_{i,j+1}$$

באופן דומה $G_{i,j+1} \triangleleft G_{i,j}$ אם $j=0$ אז $G_{i,0} = G_i$!

$G_{i,m-1} \triangleleft G_{i,m}$ אז נצבן את $\{G_i\}$ באופן הבא:

$$G = G_{0,0} \geq G_{0,1} \geq \dots \geq G_{0,m-1} \geq G_{1,0} \geq G_{1,1} \geq \dots \geq G_{1,m-1} \geq G_{2,0} \geq \dots$$

באופן דומה נצבן את הסדרה $\{H_j\}$ $H_{j+1} = H_j (H_j \cap G_i)$ ו' $H_{j+1} \leq H_j$

מתקיים $H_{0,j} = H_j$! $H_{i+1,j} \leq H_{i,j} \leq H_j$ והעציון הוא

$$H = H_{0,0} \geq H_{1,0} \geq \dots \geq H_{l-1,0} \geq H_{0,1} \geq H_{1,1} \geq H_{2,1} \geq \dots$$

נשים לב להתהוות שלביצטנו הסדרות החדשות (המחזוריות)

ה- l של A נוסף ל- l של B הסדרה בסוף קיבלנו

שני עציונים של הסדרה. לפיהם $m+1 = m+1$

$$G_{ij}/G_{i,j+1} \cong H_{ij}/H_{i+1,j}$$

באופן של אברהם ל-

$$\frac{G_{i+1}(G_i \cap H_j)}{G_{i+1}(G_i \cap H_{j+1})} \cong \frac{H_{j+1}(H_j \cap G_i)}{H_{j+1}(H_j \cap G_{i+1})}$$

אם לזה קצת נוסף אלמנט Zassenhaus אנו רואים

$$A = G_{i+1}, A^* = G_i$$

$$B = H_{j+1}, B^* = H_j$$



הגדרה:

(1) סדרה נורמלית היא $G = G_0 \geq G_1 \geq \dots \geq G_n = \{e\}$ כן ש- $G_{i+1} \triangleleft G_i$ $i = 0, 1, \dots, n-1$

(2) נניח שיש שתי סדרות

$$G = G_0 \geq G_1 \geq \dots \geq G_n = \{e\}$$

אזי $\{H_i\}_{i=0}^n$ היא ציפון של $\{G_i\}_{i=0}^n$ אם האוסף $\{G_i\}_{i=0}^n$ הוא תת אוסף של $\{H_i\}_{i=0}^n$

(3) תבורה G נקראת פשוטה אם התבורות החלקיות הנורמליות היחידות שלה הן $\{e\}$ ו- G

(4) סדרה נורמלית $G = G_0 \geq G_1 \geq \dots \geq G_n = \{e\}$ נקראת סדרת דירכל אם לכל $i = 0, \dots, n-1$ G_i/G_{i+1} היא תבורה פשוטה.

הערה: דפ אשפט ההתאמה הראשון של גאלואה מתאר את

בין התבורות החלקיות של תבורה A והחבורה החלקית

נורמלית N לבין התבורות החלקיות של A/N (התאמה בי

מצורה תבורות חלקיות נורמליות ב- A לתבורות חלקיות נורמליות

של A/N) G_i/G_{i+1} פשוטה אמ"כ G_i/G_{i+1} תבורה חלקית

אמש נורמלית מקסימלית ב- G_i (מפ"שים אלה מלשפט על $A = G_i$ $i = 0, \dots, n-1$)

תלכורות: תבורה חלקית נורמלית $A \triangleleft B$ נקראת מקסימלית

נורמלית אם לכל C אמצע $A \triangleleft C \triangleleft B$ $C = A$ או $C = B$

אז או $C = B$ או $C = A$

משפט העצום של לרנר (1928)

כל שתי סדרות נורמליות בתבורה G יש תצפיות שקולים

תלכורת: סדרות נורמליות $G = G_0 \geq G_1 \geq \dots \geq G_n = \{e\}$

$$G = H_0 \geq H_1 \geq \dots \geq H_l = \{e\}$$

הי קראנה לקוחה אם $l = n$ וקיימת תאורה $\alpha: \{0, 1, \dots, n\} \rightarrow \{0, 1, \dots, l\}$

27

$n = p^2 q^3$

$\mathbb{Z}_n$	$\mathbb{Z}_n$
$\mathbb{Z}_n/p\mathbb{Z}_n \cong \mathbb{Z}_p$	$\mathbb{Z}_n/q\mathbb{Z}_n \cong \mathbb{Z}_q$
$p\mathbb{Z}_n = \langle p \rangle$	$q\mathbb{Z}_n$
$p^2\mathbb{Z}_n/p^2\mathbb{Z}_n \cong \mathbb{Z}_p$	$q^2\mathbb{Z}_n/pq\mathbb{Z}_n \cong \mathbb{Z}_p$
$p^2\mathbb{Z}_n = \langle p^2 \rangle$	$pq\mathbb{Z}_n$
$p^2\mathbb{Z}_n/p^2q\mathbb{Z}_n \cong \mathbb{Z}_q$	$pq\mathbb{Z}_n/pq^2\mathbb{Z}_n \cong \mathbb{Z}_q$
$p^2q\mathbb{Z}_n = \langle p^2q \rangle$	$pq^2\mathbb{Z}_n$
$p^2q\mathbb{Z}_n/p^2q^2\mathbb{Z}_n \cong \mathbb{Z}_q$	$pq^2\mathbb{Z}_n/p^2q^2\mathbb{Z}_n \cong \mathbb{Z}_p$
$p^2q^2\mathbb{Z}_n = \langle p^2q^2 \rangle$	$p^2q^2\mathbb{Z}_n$
$p^2q^2\mathbb{Z}_n/p^2q^3\mathbb{Z}_n \cong \mathbb{Z}_q$	$p^2q^2\mathbb{Z}_n/p^2q^3\mathbb{Z}_n \cong \mathbb{Z}_q$
$p^2q^3\mathbb{Z}_n = \langle p^2q^3 \rangle = \{e\}$	$p^2q^3\mathbb{Z}_n$

ביאור: סדרה הרבה (קראת) אם סדרה ג' אבן-הולד.

והתבוננות והמפגשים במנוח בסדרת הרבם (קראי) אמרי הרבם

על G או ארמי גורדן - קורבן על G.

נשים ♥ שיכולות להיות לך חבורה שיש להן את אורח
החיים (עצבני אינטואיטיב) את החבורה אין אינטואיטיב
בן העניין וזה פי דוגמה מאזקלות ואטומים יש מאקלות שיש
להן את החיים מאזקלות, כלומר את אטומים ארכיטקטורה,
אתה הן לא את המאזקלות.

אז כמו שיש את הטבלה המתמורה לאותיות אלה האטומים
הקיימים בטבע יש ענין מיוחד אחר היתכנות הפשוטה
הסופריו. כחצי יל - 60000 טמונים שאונים או נולד ויל
פתטיקס יצאו של הלכה לשאר הנן אך היתכנות.

כריז אנחנו ירצו להמכור $\mathbb{Z}$ עבור $\mathbb{Q}$ ראשוני
 הן פשוטות

משפט: התמונה האיטרנטיבית A_n (= תמונת התמונה
 הנצחה של קבוצה n חברים) הן פשוטות עבור
 $n \geq 5$.

צגנו התמונה A_n נוצרת $\mathbb{Q}$ אוסף הציקלסים מסדר 3 ($n \geq 3$)
 הרכבה הולכת ל- A_n נוצרת $\mathbb{Q}$ ציקלסים מסדר 2 (= חילופים)
 התמונה הנצחה (A_n איננה) הן אומן תמונות שבתמונה
 כמכילה של מספר לא של חילופים. נובע מראש A_n
 נוצרת $\mathbb{Q}$ בתמונה מהצורה $(xy)(zw)$
 דבר מספק להראות של תמונה מהצורה $(xy)(zw)$ היא
 אחתה של שלשה.

יש לתת כמה אופציות: (יהי w, z, y, x חברים שלשה)

$$(xy)(xy) = e$$

$$(xy)(yw) = (xyw)$$

$$(xy)(zw) = (xy)(yz)(yz)(zw) =$$

$$= (xyw)(yzw)$$

②

צגנו עליה: A_5 פשוטה (הוכחה בעתיד)

צגנו עליה: עבור $n \geq 5$ A_n היא פשוטה. צמודה לזו.
 (יחס של השלשה S_n צמודים. התחילתה שאפשר
 להציגם A_n).

הוכחה: צריך להראות ל- (xyz) צמוד ל- (abc) ב- A_n .
 ירצו לקיים $g \in S_n$ יק ל- $(abc) = g^{-1}(xyz)g$
 אם $g \in A_n$ סימן. אם לא, ניקח u, v שניהם לא
 ושניהם x, y, z (יש נגדה כי $n \geq 5$).

28

35

$$((uv)g)^{-1}(xyz)((uv)g) = g^{-1}(uv)^{-1}(xyz)(uv)g =$$

$$= g^{-1}(uv)^{-1}(uv)(xyz)g = (abc)$$

כי x, y, z, uv, g הם שייכים

$(uv)g \in A_n$, שהיה בפנינו תאורה

אויסואמר בתחילת. אז $(xyz) : (abc)$

צמודים ע"י $(uv)g$ שהם כוונת

מסקנה ביניים: אנתוני חזרים פרימאל $K \triangleleft A_n$ ($n \geq 5$)

פסל $K \neq A_n$ אז $K = A_n$. מהדיון עד כה נובע שמספיק

שנוכח ל- K מרחבה ציקלוס אחד באורך 3, כי אז מתוך

הנוכחיות ינבע שכל מרחבה אר 6 הציקלוסים מאורך 3,

אם השלשות הללו יוצרות אר A_n ורק $K = A_n$.

תבא נזהר פסל $K \triangleleft A_n$, יהי $e \neq k \in K$

נניח $k = (a'_1 \dots a'_n) \dots (a''_1 \dots a''_m)$ נסתב בשלשה $t = (a_2^1 a_1^1 x)$

ואשר $x \neq a_3^1$ אם קיים כזה. נסתב כ- $t k t^{-1} k^{-1}$

K נורמלית ורק $t k t^{-1} \in K \iff t k t^{-1} k^{-1} \in K$ (אם)

$$t k t^{-1} k^{-1} = (a_2^1 a_1^1 x) k (a_2^1 a_1^1 x) k^{-1} =$$

$$= (a_2^1 a_1^1 x) (k(a_2^1) k(a_1^1) k(x)) =$$

$$= (a_2^1 a_1^1 x) (a_2^1 a_1^1 y) \in \text{Alt}(a_1^1, a_2^1, a_3^1, x, y) \cong A_5$$

a_2^1 או $k(x)$

בואו, בחלק A_n מצאנו חלק של A_5 שיש לו חיתוך עם

כיווילי עם K . לפי טענת העזר A_5 פשוטה. אם

$$K \cap A_5 = A_5 \iff \text{פסל} \neq K \cap A_5 \triangleleft A_5$$

בואו $K \cap A_5$ מרחבה אר 6 התמורות הכוללות על $\{a_1^1, a_2^1, a_3^1, x, y\}$

ובפרט מרחבה שלשה ואיילנו.

תבניות פתירות

הגדרה: תבנית G נקראת פתירה (Solvable) אם יש

סדרה נורמלית $\{e\} = G_n \leq G_{n-1} \leq \dots \leq G_1 \leq G_0 = G$ כך של-
 G_i/G_{i+1} אבליזם לכל $0 \leq i < n$.

סימון: $G' = G^{(1)} = [G, G] = \langle \{g^{-1}h^{-1}gh : g, h \in G\} \rangle$

התבנית הנורמלית "הקומטורנטורית".

הערה: $[G, G]$ אבליזם! $[G, G]$ היא התבנית התחתונה

הנורמלית הקטנה ביותר של G כך של- $[G, G]$ אבליזם.

סימון: G תבנית. נגדיר באינדוקציה:

$$\begin{cases} G^{(0)} = G \\ G^{(i+1)} = [G^{(i)}, G^{(i)}] \end{cases}$$

טענה: תבנית G היא פתירה אם ורק אם $n \in \mathbb{N}$ כך של-
 $G^{(n)} = \{e\}$ (תראה קל)

טענה: תבנית סופית G היא פתירה אם ורק אם G היא אברהם פרימיטיבי.
שהוא הוא תבנית ציקלית מסדר ראשוני.

דוגמה: תבנית אבליזם פשוטה היא ציקלית מסדר ראשוני.

פעולה של תבנית על קבוצה

הגדרה: תבנית G תבנית אברהם X קבוצה. (אמר ש- G

פועלת על X אם קיימת פונקציה $\alpha : G \times X \rightarrow X$

המקיימת:

- $\alpha(e, x) = x$
- $\alpha(g_1 g_2, x) = \alpha(g_1, \alpha(g_2, x))$

טענה: α כנ"ל מגדירה הומומורפיזם $\varphi : G \rightarrow \text{Per}(X)$

הניתן על ידי $\varphi(g)(x) = \alpha(g, x)$ וזהו הפק, $\varphi(g)(*) = \alpha(g, x)$

כך הומומורפיזם $\varphi: G \rightarrow \text{Per}(X)$ מתאר פירוט של G על X באופן הבא: $\alpha(g, x) = \varphi(g)(x)$ (**)

הוכחה: הפונקציה α נגזרת מ- φ ו- (α) זניק אבסורד ל- φ הומומורפיזם $\text{Per}(X)$

זהו (α) $\varphi(g)$ זוהי עתקה מ- X ל- X מזהה היא זהה ואלו מספיק להראות ש- $\varphi(g)$ עתקה הפיכה. נטען שהעתקה $\varphi(g^{-1})$ היא הפיכה.

$$\begin{aligned} \varphi(g^{-1})(\varphi(g)(x)) &\stackrel{(*)}{=} \alpha(g^{-1}, \alpha(g, x)) \stackrel{(*)}{=} \alpha(g^{-1}g, x) = \alpha(e, x) = x \\ &= \alpha(g^{-1}g, x) = \alpha(e, x) = x \end{aligned}$$

$$\varphi(g) \circ \varphi(g^{-1}) = \text{id} \quad \text{באופן דומה} \quad \varphi(g^{-1}) \circ \varphi(g) = \text{id} \quad \Leftarrow$$

$$\varphi(g) \in \text{Per}(X) \quad \Leftarrow \text{הפיכה} \quad \varphi(g) \quad \Leftarrow$$

וגם להוכיח ש- φ הומומורפיזם

$$\begin{aligned} \varphi(g_1 g_2)(x) &= \alpha(g_1 g_2, x) = \alpha(g_1, \alpha(g_2, x)) = \\ &= \alpha(g_1, \varphi(g_2)(x)) = \varphi(g_1)(\varphi(g_2)(x)) = \\ &= (\varphi(g_1) \circ \varphi(g_2))(x) \end{aligned}$$

$$\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2) \quad \Leftarrow$$

כעת, בהנחת הומומורפיזם $\varphi: G \rightarrow \text{Per}(X)$ נגזרת

זניק אבסורד α מ- φ מקיימת את התכונות $(**)$ הפורטול:

$$\alpha(e, x) = \varphi(e)(x) \stackrel{(*)}{=} \text{id}(x) = x$$

$$\begin{aligned} \alpha(g_1 g_2, x) &= \varphi(g_1 g_2)(x) = \varphi(g_1) \circ \varphi(g_2)(x) = \\ &= \varphi(g_1)(\varphi(g_2)(x)) = \varphi(g_1)(\alpha(g_2, x)) = \\ &= \alpha(g_1, \alpha(g_2, x)) \end{aligned}$$



סיכום: הוצגו דוגמאות הפירוט של G על X בהוכחה.

(א) פשוט $g \cdot x$ או $x \cdot g$.

(א) תבא G תבורה ! H תבורה תתקנה נוסח X א
קבוצה המתקנה השמאלית H ב- G (דעו
אם מסתבר שאם G/H אף כפינו - אז תבורה
אנחנו).

G פוזל X באופן הבא: אם $x \in X$ אז מתקנה yH
, $g \in G$ אז $g \cdot x = g \cdot yH = gyH$
כאשר, נראה שזה מוגדר היטב: נניח $yH = y'H$
אז $gyH = gy'H$ שכן $gy = y'g'g''y'' = y'y' \in H$
כזה נראה שזו אכן פתרון:

$$(i) e \cdot yH = eyH = yH$$

$$(ii) g_1 g_2 \cdot yH = (g_1 g_2) yH = g_1 (g_2 yH) =$$

$$= g_1 \cdot g_2 yH = g_1 \cdot (g_2 \cdot yH)$$

מסקנה: G תבורה של H , H תבורה של G
מאידך n אינדיקס תבורה תתקנה N ונראה
כן $N \leq H$! $[G:N] = n!$

הנחתה יש פתרון של G $X =$ המתקנה השמאלית
ל H ב- G $|X| = n$ מה מתקנה $G \rightarrow \text{Per}(X)$ ו
הוא/אנחנו $N = \text{Ker } \varphi$ מתקנה

$[G:N] = n!$ $G/\text{Ker } \varphi \cong \text{Im } \varphi \leq S_n$
כמו כן, $k \in N$ פתרון של eH היא eH
 $kH = keH = k(eH) = eH = H$

$$(ב) N \leq H \iff k \in H \iff$$

מסקנה: אם G פשוטה אינסופית אז אין לה
תת תבורה מאידך S_n

הנחתה: אם הייתה G תת תבורה מאידך n אז
הייתה G תת תבורה ונראה שזו
אם יוכלו שפירא

המקרה הפרטי של $H = \{e\}$ מחזיר אותנו לפעולה G
 על עצמה. ע"י כך נשמע שיש לה השתמש בה. במילים
 קצרות: כדי לתת שייך של G בתוך $\text{Per}(G)$

(ב) נגדיר ההצמדה של G ו- $X = G$ ניקח
 (באופן G פונקציה) אם $g \in G$ ו- $x \in X$
 (הצורה) $g \cdot x = g x g^{-1}$. האם זה פונקציה?
 $e \cdot x = e x e^{-1} = x$

$$\begin{aligned} g_1 g_2 \cdot x &= (g_1 g_2) x (g_1 g_2)^{-1} = \\ &= (g_1 g_2) x (g_2^{-1} g_1^{-1}) = g_1 (g_2 x g_2^{-1}) g_1^{-1} = \\ &= g_1 \cdot (g_2 \cdot x) g_1^{-1} = (g_1 g_2) \cdot x \end{aligned}$$

הצמדה וס'מנים:

אם G חבורה הפונקציה של קבוצה X אזי $x \in X$
 מסמן $[x] = \{g \cdot x : g \in G\}$ = המסלול של x ב- G .

למה אם $x, y \in X$ ו- G פונקציה על X אז
 $[x] = [y]$ או $[x] \cap [y] = \emptyset$.

במילים אחרות, המסלולים של פונקציה G על X
 מחזיקים יחס שקילות על X המוגדר ע"י $x \sim y$
 אם קיים $g \in G$ כך ש- $g \cdot x = y$.

הוכחה: לראות האם מספיק לעינינו ש- $z \in [x] \cap [y]$
 אז $[x] \subseteq [y]$ (כי אז האופן שבו x נגזר $[y]$).

ואם קיימים $g_1, g_2 \in G$ כך ש- $g_1 \cdot x = z = g_2 \cdot y$
 דבר $g_1^{-1} g_2 \cdot y = x$ יהיה זה א"כ $u \in [x]$

אז $u = g_3 \cdot x$ ואז $u = g_3 (g_1^{-1} g_2 \cdot y)$ באופן

$$[x] \subseteq [y] \iff u \in [y] \iff u = g_3 g_1^{-1} g_2 \cdot y$$

(ג)

סיומ: אם $x \in X$ מסמן $G_x = \{g \in G : g \cdot x = x\}$

החבורה של x ב- G (החבורה של ההצמדה של x).

31

טענה:

- (א) G_x חבורה חלקית של G
 (ב) יש הרמאה חתום ושל מן איברי המסלול $[x]$ למחלקת
 השמאליות של G_x ה- G . בפרט, אם $[x]$ סופי
 אזי $|[x]| = |G_x|$
 ההתאמה נקראת $g \cdot x \mapsto gG_x$

הלוחות

- (א) תרגיל
 (ב) ההתאמה מורכבת היטב כי אם $gG_x = g'G_x$ אז
 $g = g't$ עבור $t \in G_x$ ואז
 $g \cdot x = (g't) \cdot x = g' \cdot (t \cdot x) = g' \cdot x$

צריך להראות שלכל חתום $[x]$ נקרא $y \in [x]$ אזי קיים $g \in G$ כך
 $y = g \cdot x$ ואם $y = g' \cdot x$ אז $g'G_x = gG_x$ אם כי
 אם מתקדם.

מל"י נניח שההתאמה בעברה את g_1G_x ואת
 g_2G_x לאותו איבר, כלומר $g_1 \cdot x = g_2 \cdot x$. אז
 $g_1^{-1}g_2 \cdot x = x \iff g_1^{-1}g_2 \in G_x$

$$g_1G_x = g_2G_x \iff g_1^{-1}g_2 \in G_x$$

32

מסקנה: אם G חבורה סופית הפועלת על קבוצה X ,
 אזי לכל $x \in X$ $|[x]| \mid |G|$

מסקנה: אם G חבורה סופית $|G| = n$ ומחלקת C צמידות
 ה- G אזי $|C| \mid n$

הנחה: כי מחלקת צמידות של מסלול של החבורה G
 הפועלת על עצמה היא עצמה.

33

מסקנה: נניח G חבורה סופית מסדר n ואשלי p

כאשר n (חבורה כזו נקראת חבורת פאסור - p)

לא מתחלקת במידת שלמה. מספר חלקי p (כי

זה חייב לחלק את n) (p^n) .

נניח שמתחלקת בדמיון p^n C p ואשר

$|C| = p^n$. חייב להיות $\sum_{i=1}^n |C_i| = p^n$.

$|C_i| = 1$ אם $C_i \in C$ הוא המרכז.

כל מקרה אחר, $|C_i| = p$ אז מספר $|C_i|$

אשר 1 או p איננו שלמות p .

$C_i = \{e\}$ אם $|C_i| = 1$ $\Leftrightarrow$ חייב להיות מספר!

$\Leftrightarrow$ יש בהכרח $p-1$ מתחלק במידת p^n $p^n = 1$

$\Leftrightarrow Z(G) \neq \{e\}$ G .

$Z(G)$ זו חבורה אברהם נורמליזציה $G/Z(G)$ אם

חבורת p חלקי יש p מרכז C כיווילי (אז)

אם $G = Z(G)$ אז $Z(G/Z(G))$ C

כיווילי. לפי משפט הפתאמה של חבורה נורמליזציה $Z_2(G)$

של G שמתחלק $Z(G) = Z_1(G)$ p .

$$Z_2(G)/Z_1(G) = Z(G/Z_1(G))$$

אזכר כי p סדרה של חבורות חלקיות נורמליות

$G = Z_1(G) \leq Z_2(G) \leq \dots \leq Z_k(G) = G$

והמנה $Z_k(G)/Z_{k-1}(G)$ אברהם G חבורה

פתיחה. כלומר חבורת p היא פתיחה.

3.12.07
אמנים

הפעם הקדמנו דברנו על פעולה של חבורה G על קבוצה X .
 $\varphi: G \rightarrow \text{Per}(X)$ חבורת הפרמוטציות
 $g \cdot x = \varphi(g)(x)$ ואשר $g \in G, x \in X$.

החסמים של $x \in X$ תחת G הם

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

החבורה $G_x = \{g \in G : g \cdot x = x\}$ היא החבורה

ראשונית של x בתאמת החזק. ואל בין איברי החסמים $O(x)$

סמתיקל. השמאליות של G_x היא G . ההתאמה הזו

$$g \mapsto g \cdot x \text{ היא חזקה}$$

ראשונית של x היא חזקת G_x אם $g \in G_x$ אז

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

$$|O(x)| = [G : G_x] = |G| / |G_x| \leq |G|$$

החבורה G_x היא חבורה של G אם $x \in G$

$$g \cdot x = x \iff g \in G_x \iff g \in \{x\} \iff x = 1$$

צורת אלה

(1) G פוזמל על G חזקת G חבורה משמאל:

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

אם $x \in G$ אז $G_x = \{g \in G : g \cdot x = x\} = \{g \in G : gx = x\}$

חזקת G חבורה משמאל - זאת פשוט

תכונה חסיונות של חבורה. (ניקח $g \cdot x = x$)

החבורה של x היא $G_x = \{e\}$ אם x חזקת G

השמאליות הן בדיוקם איברי G ונחלקן יש התאמה חזקת

$$O(x) = G$$

(2) G פוזמל על $X = G$ חזקת G חבורה משמאל

אם $x \in G$ אז החבורה של x היא $G_x = \{g \in G : gx = x\}$

החבורה של x היא $G_x = \{g \in G : gx = x\}$

$$|O(x)| = [G : G_x] = |G| / |G_x|$$

נשים $\hookrightarrow$ $|x^G| = 1$ א"ח $x \in Z(G)$

משקלה של G סופית אז $|G| = |Z(G)| + \sum_{i=1}^t [G : C_G(x_i)]$ $x_1, \dots, x_t$ נציג מחלקה צמידות δ מכילים.

משקלה: אם G חבורה - $\forall p$, $Z(G)$ חבורה מסדר p^n

אשר p ראשוני $1 \leq n \in \mathbb{N}$, אז $Z(G) \neq 1$

הוכחה: נסתב δ - (א) אז $p^n = 1 + \sum_{i=1}^t p^{k_i}$

ראשי $[G : C_G(x_i)] = k_i$ (לפי $1 < [G : C_G(x_i)]$)

$\Leftarrow$ הנספחים היחידים שלחלקיה של p^n וגם δ ו 1

(כי אם $x \in Z(G)$ $x \neq 1$ היא מהצורה p^{k_i} $\delta - k_i \geq 1$.)

אז p/p^n וגם $p \mid \sum_{i=1}^t p^{k_i}$

$\Leftarrow p \mid Z(G)$ נחלק $|Z(G)| \neq 0$ כי $e \in Z(G)$

ולכן $|Z(G)| \geq p$

☺

משפט קליי: תהא G חבורה סופית, p ראשוני, $p \mid |G|$

אז יש ב- G איבר מסדר p .

הוכחה: נסמ

$$X = \{ (g_1, g_2, \dots, g_p) : g_i \in G, \prod_{i=1}^p g_i = e \} \subseteq G^p$$

החבורה $C_p = \mathbb{Z}/p\mathbb{Z}$ פועלת על G^p י"ר

$$i. (g_1, \dots, g_p) \mapsto (g_i, g_{i+1}, \dots, g_{i+p-1})$$

זה פשוט סיבוב שמאלה ב- i צעדים

קל לבדוק שזו אכן פעולה פועלת על שומה של הקבוצה X .

שהי אם $\prod_{i=1}^p g_i = e$ אז $g_1 \dots g_p = e$ כי

זהויה שלם $e = g_1 g_2 \dots g_p = g_1 g_2 \dots g_p$ מספיק לפרט את זה $i=1$

כי אם זה נשמר נאיבית של צעד אחד אז באינדוקציה זה

(חן δ סיבוב ואכן אם $e = g_1 g_2 \dots g_p = g_1 g_2 \dots g_p$ אז $e = g_1 g_2 \dots g_p$)

לכן $e = g_1 g_2 \dots g_p = g_1 g_2 \dots g_p$ וזה בדיוק מה שרצינו.

$\Leftarrow$ מוגדרת פעולה על X $\cdot p = \pi/p \pi$ $\cdot p = \pi/p \pi$

מהו $|X|$? $|X| = |G| = p^n$ יי אפשר לבחור את $2-p, \dots, p$ שיוכלו $|X|$ ו- p נקרא למספרים על יום. אז יש p זוגות חופשי.

מראו ל- $|X| = p$. אלה התכונות הפונקציה על X היא מספר p זוגות מספרים בפעולה $\cdot p$ על X הסדר שלו מתק, את p . זמן או שהוא מספר p או מספר L , בואו המספרים של X מספר p אי ש- X נקראת לזה.

יש לפחות נקודה שבה אחת והיא $(e, e, \dots, e)$. מראו שיש עוד נקודות שבה, כי $|X| = \text{מספר זוגות} + \text{מספר זוגות} = p + \dots$

$\Leftarrow$ מספר נקודות השבה מתחיל ב- p . $\Leftarrow$ יש לפחות p נקודות שבה. בואו יש עוד נקודות שבה הן p $(e, e, \dots, e)$. ונקודות שבה היא וקראו $X \in (h, h, \dots, h)$ יק ש- $p = e$ והנה מצאנו איבר $h \neq e$ מספר p .

שבה p | h מספר ומספר e $h \neq e$ אז $p = o(h)$. (ii)

הערה: תהא G חבורה מסדר $m \cdot p^n$ כאשר p ראשוני; m זוגי. חבורה חסיד p של G מספר p^n נקרא חבורת p -סילבס של G (Sylow).

משפט סילבס: G חבורה סופית מסדר $m \cdot p^n$ כאשר p ראשוני, אזי

- (א) קיימת חבורת p -סילבס
- (ב) חבורת p -סילבס G מובנית באיזו חבורת p -סילבס
- (ג) כל החבורות p -סילבס G צמודות זו לזו. (בפרט הן כולן איזומורפיות)

(ד) אם $p \nmid m$ מספר חבורת p -סילבס G איז $1 \pmod{p}$

הערה: אם G חבורת $N \leq G$ יק ש- N G/N פתורה אז G פתורה.

שימושים של משפט סימא:

- ① תהא G חבורה מסדר 48. אזי G פתירה.
 הנוחה: $48 = 2^4 \cdot 3$. לכן לפי משפט סימא יש ב- G חבורה חזקה P מסדר 16 ואינדקס שלה 3.
 $\Leftarrow P$ מרכזית בחבורה חזקה-נורמלית G^N לאינדקס לכל היותר 6 = $3!$ (משפט של סרד) לכן N היא חבורה-2 ולכן פתירה (נייט חבורה- p היא פתירה). N/G חבורה מסדר לכל היותר 6 ולכן פתירה (אנחנו מכירים את G כחבורה מסדר לכל היותר 5 ואנחנו יוצאים להן פתרונות ובהן תרגילי יש לפרוט שחבורה A מסדר 6 היא פתירה ולמעשה $K \cong \mathbb{Z}/6\mathbb{Z}$ וכן היא אבליה ופתירה או ל-
 $K \cong S_3$ (היא פתירה).
 ט)

הוכחת משפט סימא

- Ⓐ נסמן ב- X את קבוצת החתך קבוצה של G מסדר p^r . אז $|X| = \binom{p^m}{p^r}$ (תרגיל)
למה: $\binom{p^m}{p^r} p^r$ ראשי מלא p . (תרגיל)
 G פוזזת על X באופן חופשי: אם $B \in X$ אז $B \cdot G = G$ וזוהי
 $B \cdot G = G \cdot B$ - מופת G באיבר B .
 (זאת לא מתחקה שמאליה של אחת לאשר ש- B זה חבורה!)
 קדם לראות שיש את פזוזתה.
 מאחר ש- X ואלו p יש לפחות קבוצה אחת B_0 מסדר p^r
 שזוהי המסלול שלה בפזוזת G אינו מתחלק ב- p .
 נסמן $\{B_0 = B_0 \cdot g : g \in G\} = \{B_0 \cdot g : g \in G\} = B_0 \cdot G$. זו חבורה חזקה של G ואינדקס p . (היא האינדקס שלה שזה לא חלק מהמסלול של B_0).
 מאחר $H = G \cdot B_0$ מתחלק אז $p^m / |H|$ - p^r חלקי p .
 $\Leftarrow |H| \geq p^r$ ובפרט $|H| \geq p^r$.

(34)

דרג'ו (נכיה ל - $|H| \leq p^r$ להכך (נכיה ל - H היא חבורה
 p -סעא, שהכ' המ"צב גאד חבורה חזקה ואנחנו
 מראים ל - $|G| = p^r$.

יהי $B_0 \in B$ ונחפיר פונקציה $f: H \rightarrow B_0$ ע"י

$$f(h) = hb_0 \quad h \text{ במ"צב גאד } hb_0 \in B_0$$

ננסה ל - f חת"ע וזה יראה ל - $|H| \leq |B_0| = p^r$ אלא שזה ברור.

כי אם $f(h_1) = f(h_2)$ אז $h_1 b_0 = h_2 b_0 \Leftrightarrow h_1 = h_2$.

וסיימנו עם הוכחה משפט סילוב (א).

35) 5.12.07
מסנים

הגדרה: תבא G תבורה מסדר $m = p^r \cdot n$ כאשר p ראשוני ו- $m \nmid p$.
תבורה חזיקה P מסדר p^r של G תיקרא תבורה p -סילטא.

משפט סילטא: תבא G תבורה מסדר $m = p^r \cdot n$ כאשר p ראשוני ו- $m \nmid p$.

(א) יש G -תבורה p -סילטא P מסדר p^r

(ב) אם Q תבורה חזיקה של G שהיא תבורה- p , אזי Q מוכלת בתבורה p -סילטא של G .

(ג) שתי תבורות p -סילטא של G צמודות זו לזו (אם P_1, P_2

תבורות p -סילטא אזי קיים $g \in G$ כך ש- $P_2 = g P_1 g^{-1}$

(ד) אם $P_1, \dots, P_\ell$ הן תבורות p -סילטא של G אזי $\ell \equiv 1 \pmod{p}$! $m \mid \ell$.

כה משפט שממש קשה להגדיר בתליבות.

נסתבא על אמצע של S_3 . $|S_3| = 6 = 2 \cdot 3$. אכן תבורות 2-סילטא

של S_3 הן אלה תבורות מסדר 2 - לכן יש 3 כאלה - כי יש 3

איברים מסדר 2. אכן, $3 \equiv 1 \pmod{2}$, ! $3 \mid 6$.

מבדשני, אם יש תבורה מסדר 6 (שהיא אף צמודה לזו תבורה 3-

סילטא יש לה, יש לפחות תבורה אחת, ואזל פיותר 2 לברי

מסדר התבורות אמור להיות 2. לא יכונן לפיכך שיש 2 כי

צריך להתיקיים $\ell \equiv 1 \pmod{3}$ (והכי $2 \not\equiv 1 \pmod{3}$). $\Leftarrow$ בתבורה

מסדר 6 יש רק תבורה 3-סילטא אחת!

הכנה להוכחה: דוגמה נוספת לפעולה של תבורה G על קבוצה X .

תבא X קבוצה התבורות החזיקות של G . נגדיר פעולה של G

על X כך: אם $H \in X$ תבורה חזיקה של G ו- $g \in G$

$$g \cdot H = g H g^{-1}$$

הצמדה היא אוטומורפיזם של G ואכן $g H g^{-1}$ היא תבורה

חזיקה, אז כה מוגדר היטב. קל לראות שזו אכן פעולה.

מהו המייצג של H בפעולה זו?

$$G_H = \{g \in G : g \cdot H = H\} = \{g \in G : gHg^{-1} = H\} = N_G(H)$$

← זה הנוכח (מכאן) של H .

תכונות הנוכחיות:

(i) $N_G(H)$ תכונה תתקבוצה של G

(ii) $H \leq N_G(H)$

(iii) $N_G(H)$ היא התכונה התתקבוצה המקסימלית

של G היותם לתכונה זו, טומר $N_G(H)$ היא התכונה התתקבוצה המקסימלית של H נוחלת בה.

(iv) מספר התכונות התתקבוצה של G הצמודות ל- H שנה ל- $[G:N_G(H)]$

כי קבוצת G התכונות התתקבוצה של G הצמודות ל- H היא בפיק המסלול של H תחת פעולה G וראינו שמספר איברי המסלול שונה לאינדקס המייצג.

(v) מספר התכונות התתקבוצה הצמודות ל- H מתק א $[G:H] = \frac{|G|}{|H|}$

כי מספר זה הוא $[G:N_G(H)] = \frac{|G|}{|N_G(H)|}$ וראינו

$$[G:H] = \frac{|G|}{|H|} = \frac{|G|}{|N_G(H)|} \cdot \frac{|N_G(H)|}{|H|} = [G:N_G(H)] \cdot [N_G(H):H]$$

הוכחה משפט סילוא (3, 2, 1):

תהא P תכונה ק-סילוא של G . (ק"מ כגא מסלול (א)).

תהינה $\mathcal{Y} = \{P_1, \dots, P_k\}$ התכונות התתקבוצה של G הצמודות ל- P , זא המסלול של P בפעולה G ה"ה הצמדה של תכונות תתקבוצה.

לפי הדיון קודם $m|k$ (לפי v). בפרט k לר- p , טומר

$k \nmid p$. תהא Q תכונה p -תתקבוצה של G כלפי. Q פועל של

$\mathcal{Y}$ ה"ה הצמדה. המסלולים של Q בפעולה של $\mathcal{Y}$ הם מספר תתקבוצה P

כי אורך מסלול של תכונה מתק א-סדר התכונה. זמן הם מספרים

$p^s, \dots, p^2, p, 1$ אם $|Q| = p^s$. (נסמן שיש לפחות מסלול אחד באורך

1 - טומר נקודה שבה. אבל זה בכו כי $|Y| = k$, $k|p$.

המסלולים לרם. אם רחם מתתקבוצה p -אזים סטום k מתתקבוצה p וזו

סתרה. זמן קיים $i \in \{1, \dots, k\}$ כך של- P_i נקודה שבה של Q .

36

לומר $Q \leq N_G(P_i)$, $Q \in \mathcal{Q}$, $P_i \cdot q = P_i$

לומר $q \in N_G(P_i)$, $P_i \cdot q^{-1} = P_i$

נסמן $D = N_G(P_i)$, $\bar{P} = P_i$, אז $\bar{P} \triangleleft D$! $Q \leq D$

אז $|D| = p^r \cdot m$, כאשר $m \mid m$ שריר $p^r = |P|$ ומכאן D

! $D \leq G$ (נסתב בחבורה $Q \cdot \bar{P}$ זו חבורה חלקית ואפי

משפט. הפתאמותהם השני, $Q/\bar{P} \cong Q/\bar{P} \cap Q$

$Q/\bar{P} \cap Q$ היא מסדר חלקית Q (כי זו חבורה מנה של Q) ואז

$$|Q/\bar{P}| = [Q/\bar{P} : \bar{P}] = |Q/\bar{P}| \Leftrightarrow |Q/\bar{P}| \leq p^r$$

אם הוא חלקית Q , לפרט $p^r = |P|$. אז אין G חבורה חלקית

מסדר חלקית Q אפוא r . $|Q/\bar{P}| = p^r \Leftrightarrow Q/\bar{P} = \bar{P}$

$Q \leq \bar{P}$ וזה מוכיח את סעיף (ב). אז למעשה הוכחנו

תוצאת יותר. היכאנו של חבורה חלקית שהיא חבורה Q מ- G מוכיח

באותה מציאות P .

אזכור, אם Q חבורה היא Q -סילוא, ז"א מסדר p^r , אזי היא מוכיח

באותה מציאות P , אז הם מאפיל זהה ואז Q שווה לאחד מציאות

P ובלאג הוכחנו את סעיף (ג). (הפרט אנתנו אומרים של החבורה

Q -סילוא הן איזומורפיה זו לזו)

עכשיו אנתנו יידעם לביסיונים הקודמים אם $P_1, \dots, P_r$ הן G וחבורה

Q -סילוא אז $k = l$. $m \mid k$ ואז $m \mid l$.

נתבונן בפרט P על צמודים Y .

המסלולים של P ב- Y הם או מאפיל 1 (לומר נקודה לבד) או מתחלקים

ב- P . יש נקודה לבד - P חבורה באיבר של Y הוא נקודה לבד.

נאמן שאין נקודה לבד (נוסבר). לפני אחת אם P מייצגת את P_i

אז ראוי ש- $P \leq N_G(P_i)$ וזה $P \leq P_i$ ואז $P = P_i$, כי הן

מאות מסדר. $P \triangleleft P$ מקבוצה במקום רק את חבורה Q של המסלולים

בפרט P על Y הם מספרים המתחלקים ב- p . $l \equiv 1 \pmod{p}$

שהרי Y איחוד של מסלולים זרים.



מסקנה: חבורה Q -סילוא היא יחידה אמ"ה היא (נורמלית)

טענה: תכונה מסדר 35 היא אבליה (זמנה היא ציקלית)

הוכחה: $35 = 7 \cdot 5$. גשש סיום אבליהנו שיש ב- G תכונה חלקית

A מסדר 7 - תכונה 7-סלוא. מספר תכונה 7 סלואל מתק את

5; $l \equiv 1 \pmod{7}$. $l = 1 \Leftrightarrow A \triangleleft G$, שהי

כצמח סלוא נותר סלוא ויש רק אחת כזוא

יש ב- G גם תכונה 5-סלוא B . מספר תכונה 5-סלוא

t מקיים $t \mid 4$, $t \equiv 1 \pmod{5}$. $t = 1 \Leftrightarrow B \triangleleft G$.

A מסדר 7 ורק ציקלית $A = \langle a \rangle$. גם B ציקלית

כיהא מספר 5 $B = \langle b \rangle$.

נסחג ל- $ab = ba$. נסתב $\&$ הקומוטא $[a, b] = a^{-1}b^{-1}ab$

$$a^{-1}b^{-1}ab \in A \cap B \begin{cases} a^{-1}b^{-1}ab \in B \Leftrightarrow B \triangleleft G \\ a^{-1}b^{-1}ab \in A \Leftrightarrow A \triangleleft G \end{cases}$$

נסחג ל- $A \cap B = \{e\}$. הרי $|A \cap B| \mid 5$ וגם $|A \cap B| \mid 7$

$$\Leftrightarrow |A \cap B| = 1 \Leftrightarrow a^{-1}b^{-1}ab = e \Leftrightarrow ab = ba$$

אם $G = \langle a, b \rangle$ שהי $H = \langle a, b \rangle \leq G$ תכונה חלקית

שמחלה גם א A וגם א B . הסדר $|H|$ מתחלק גם

ב- 5 וגם ב- 7. $35 \mid |H| \Leftrightarrow |H| = 35$. אפוא גם $|H| = 35$.

$H = G$. אף בתכונה להיווצרה ליה מתחלפים היא עצמה אבליה.

יתר על כן, ציקלית, ורק $G \cong \mathbb{Z}_{35}$. מספיק להוכיח שיש איבר

מסדר 35. נסתב $g = ab$. (ראה ל- g^{35} , אף זה ברור

כי היא בחלק תכונה מסדר 35 ורק $35 \mid o(g)$. לכן $o(g) = 5$

או $o(g) = 7$, או $o(g) = 35$. א

אם $o(g) = 1$ אז $ab = e \Leftrightarrow a = b^{-1} \Leftrightarrow a, b \in A \cap B$ (הרי

$A \cap B = e$ וכו' סתירה. אם $o(g) = 5$ אז $e = a^5$ (אם

$o(a) = 4$ ורק לו סתירה. אם $o(g) = 7$ אז $e = a^4 b^7 = b^2$ (אם

$o(b) = 5$ ורק לו סתירה. $o(g) = 35$! $\odot$

(37)

G על פונקציה- p תחומה נח $r_p(G)$.

① סכיוןא י

(2) תבורה אסתר ראשוןי אכן $\mathbb{Z}_2 \cong$ אכן פתירה

ਅਧਿਕਾਰ $\mathbb{Z}_3$ (3)

2. תורת ה- SK - $|G| = 2^2$ 4 תחנות G נ"ח (4)

יבוא Q , $N \triangleleft G$, N פתירה , G/N פתירה. G פתירה או

פתירה. מראן אפשר לראות האינפוקציה של תבור - ק ויא

פתירה (כ) $Z(G) \neq 1$ $G/Z(G) \cong \{$ פתירה ע"פ (ח) (האינדוקציה).

4 תבונה מספר 4 פיא פתירה.

 $\mathbb{Z}_5$ ⑤

⑥ י"ז 3 - סוף ספר 3 ואינך 2 א"כ זה נורמלי. א"כ

6 אב 6 תורה.

 $\mathbb{Z}_7$ (7)

⑧ תחנות - 2

(9) תבונה - 3

(10) $10 = 2.5$ אפק י' ב- G תמורת 5 - סוף (ורחמים) . עתה

אנשים פה תהי'ק אצפוקטאב. אמור לט הקצמור פתיחה יוצא

G_N - פתירה G פתירה.

$$\mathbb{Z}_{11} \quad (11)$$

12 - אם G מסדר 12 אז יש לה חבורה חלקית 12 $12 = 2^3 \cdot 3$

מספר 4 (2- סרט) אם H מכילה חבורה חלקית $N \triangleleft G$

$G \neq N \neq \{e\}$ $\rho \delta$. (H ל וקטור) $3! = 6 \geq \dim N$

N פתירה | G/N פתירה ו G פתירה

 $\mathbb{Z}_{13}$ (13)

14) $14 = 7 \cdot 2$ SK דתבורה 4-סילוא היא מאיפס 2 אס נאנאלי

(15) $15 = 3 \cdot 5$ ה- 5-10 לא היא מאינדיקט 3 לכן מראה תבונה חלקי

נרמאלה $N \triangleleft G$ מאנצקס אלס רינער G . ריכמו ב.ו. G פתירה.

(16) תמורה 2-

(14) $\mathbb{Z}_4$

(18) $18 = 3^2 \cdot 2$ אם תמורה 3-סילא נורמליזאציה

(19) $\mathbb{Z}_{19}$

(20) $20 = 2^2 \cdot 5$ אם $r_5 \equiv 1 \pmod{5}$; $r_5 \mid 4$

$r_5 = 1 \Leftarrow \Leftarrow$ תמורה 5-סילא היא נורמליזאציה

(21) $21 = 3 \cdot 7$ אם 7-סילא הם אינדיקס 3 $r_7 \equiv 1 \pmod{7}$

$r_7 \mid 3 \Leftarrow \Leftarrow r_7 = 1 \Leftarrow$ תמורה 7-סילא היא נורמליזאציה

(22) $22 = 2 \cdot 11$ תמורה 11-סילא היא נורמליזאציה

(23) $\mathbb{Z}_{23}$

(24) $24 = 2^3 \cdot 3$ תמורה 2-סילא יש אינדיקס 3 אם

היא אחתה תמורה חלקי נורמליזאציה $6 \geq 0$

(25) תמורה 5-

(26) $26 = 13 \cdot 2$ תמורה 13-סילא נורמליזאציה

(27) תמורה 3-

(28) $28 = 7 \cdot 2^2$, $r_7 \equiv 1 \pmod{7}$, $r_7 \mid 4 \Leftarrow \Leftarrow r_7 = 1$

$\Leftarrow$ תמורה 7-סילא היא נורמליזאציה

(29) $\mathbb{Z}_{29}$

(30) $30 = 5 \cdot 3 \cdot 2$, $r_5 \equiv 1 \pmod{5}$, $r_5 \mid 6$, $r_5 = 1 \Leftarrow$

או $r_5 = 6$ אם $r_5 = 1$ אם סיימי כי אם תמורה

5-סילא היא נורמליזאציה אם $r_5 = 6$ אם יש 6 תמורה 5-סילא

שהסדר שלהן 5. $\Leftarrow$ זיקרון מספר 5 שפוא נאשני, אם 6

האיברים מספר 5. ה-6 יש 24 איברים מספר 5 כי

כל תמורה 5-סילא יש אר 6 וכן תמורה אחרתתק רק ה-6

כי אחתה קן היו שונה. האמו אפן , $r_3 \equiv 1 \pmod{3}$; $3 \mid 6$

$\Leftarrow \Leftarrow r_3 = 1$ או $r_3 = 10$ אם $r_3 = 1$ אם סיימי אם

$r_3 = 10$ אם יש 20 איברים מספר 3 ונה לא יתר זיקרון

באור לא יתכן שיהיה 5-סילא היא לא נורמליזאציה ה-3-סילא

היא לא נורמליזאציה $\Leftarrow$ 6 פתירה

(38)

$$\mathbb{Z}_{31} \quad (31)$$

$$2 \text{ - תבונה} \quad (32)$$

$$33 = 11 \cdot 3 \quad (33) \quad \text{ה-11 - סילון חייבת להיות (נרמלית)}$$

$$34 = 14 \cdot 2 \quad (34) \quad \text{ה-14 סילון מסביר 2 ולכן (נרמלית)}$$

$$35 = 7 \cdot 5 \quad (35) \quad \text{ה-7 - סילון (נרמלית) כי } r_7 \equiv 1 \pmod{7} \quad ; \quad r_4 | 5$$

$$\Leftarrow r_7 = 1 \quad \text{והוא (נרמלית)}$$

$$\text{האופן ללי אם } |G| = p \cdot q \text{ זמנה } q > p \text{ , } p \text{ - ראשוני אז}$$

$$\text{ה- } p \text{ - סילון (נרמלית) למה } r_p \equiv 1 \pmod{p} \text{ אם } r_p | q$$

$$\Leftarrow r_p = 1 \quad \Leftarrow \text{התבונה } p \text{ - סילון (נרמלית)}$$

$$36 = 2^2 \cdot 3^2 \quad (36) \quad \text{תבונה 3 - סילון מכילה תבונה חלקית מאינסופים } 24 = 4! \geq$$

$$\text{והוא (נרמלית)}$$

$$\mathbb{Z}_{37} \quad (37)$$

$$38 = 19 \cdot 2 \quad (38) \quad \text{ראשוני } 19 > 2$$

$$39 = 13 \cdot 3 \quad (39) \quad \text{ראשוני } 13 > 3$$

$$40 = 5 \cdot 2^3 \quad (40) \quad r_5 \equiv 1 \pmod{5} \quad ; \quad r_5 | 8 \quad \Leftarrow r_5 = 1$$

$$\mathbb{Z}_{41} \quad (41)$$

$$42 = 4 \cdot 6 \quad (42) \quad \text{ראשוני } 7 > 6$$

$$\mathbb{Z}_{43} \quad (43)$$

$$44 = 11 \cdot 4 \quad (44) \quad \text{ראשוני } 11 > 4$$

$$45 = 3^2 \cdot 5 \quad (45) \quad r_5 \equiv 1 \pmod{5} \quad ; \quad r_5 | 9 \quad \Leftarrow r_5 = 1$$

$$46 = 23 \cdot 2 \quad (46) \quad \text{ראשוני } 23 > 2$$

$$\mathbb{Z}_{47} \quad (47)$$

$$48 = 2^4 \cdot 3 \quad (48) \quad \text{תבונה 2 - סילון מאינסופים 3 ולכן יש לה תר תבונה}$$

$$\text{(נרמלית מאינסופים } 3! = 6 \geq)$$

$$7 \text{ - תבונה} \quad (49)$$

$$50 = 5^2 \cdot 2 \quad (50) \quad \text{ה-5 - סילון מאינסופים 2 ולכן (נרמלית)}$$

$$51 = 17 \cdot 3 \quad (51) \quad \text{ראשוני } 17 > 3$$

$$52 = 13 \cdot 4 \quad (52) \quad \text{ראשוני } 13 > 4$$

$$\mathbb{Z}_{53} \quad (53)$$

$$(54) \quad 54 = 3^3 \cdot 2 \quad \text{ה-3 סילוא מספר 2 ולק נורמלי}$$

$$(55) \quad 55 = 11 \cdot 5 \quad 11 > 5 \quad \text{ראשני}$$

$$(56) \quad 56 = 2^3 \cdot 7 \quad r_7 \equiv 1 \pmod{7} \quad ; \quad r_7 \mid 8 \quad \Leftrightarrow \quad r_7 = 1 \quad \text{או} \quad r_7 = 8$$

אם $r_7 = 1$ סילוא. אם $r_7 = 8$ אז יש $8 \cdot 6 = 48$ איברים מספר 7 ועוד איבר אחד מספר 1. ה-2 סילוא יש 8 איברים. מתקבל 1 אינונטי והשגה 8. $\Leftrightarrow$ יש רק 2-סילוא אחד ולק הוא נורמלי. לשני אם $r_2 > 1$ אז צריך ליהיה ה-G לפחות 8 איברים מספר חלקי 2 עם טריונטיים. אבל זה קטני אפסי על $r_7 = 8$. $\Leftrightarrow$ או 7-סילוא נורמלי או 2-סילוא נורמלי.

$$(57) \quad 57 = 19 \cdot 3 \quad 19 > 3 \quad \text{ראשני}$$

$$(58) \quad 58 = 29 \cdot 2 \quad 29 > 2 \quad \text{ראשני}$$

$$(59) \quad \mathbb{Z}_{59}$$

(11)

חבורות אבליאן

תבא A תבורה אבליאן. בעצב נסמן את הפעולה על A ה- + ואת איבר היחידה ה- 0.

דוגמאות

(1) א תבורה ציקלית היא אבליאן (ספירה או אינסופית)

(2) סכום ישר של תבורות ציקליות הוא אבליאן (כיהם קלאודינארה לה אבליאן)

* תבנית $G_1, \dots, G_n$ תבורות. הסכום הישר

$$G = \bigoplus_{i=1}^n G_i \quad \text{הוא תבורה ה-חבורה}$$

קלאודינארה קלאודינארה, סומר

$$\vec{g} \cdot \vec{h} = (g_1 \cdot h_1, g_2 \cdot h_2, \dots, g_n \cdot h_n)$$

G תבורה. ניתן לומר את G בתבורה חלקית של

$$G \curvearrowright G' \quad r' = (e, \dots, e, g, e, \dots, e) \quad \text{על ידי } g \in G$$

אקטואלי

(39)

③ סכום ישר של תהורה אטלית הוא אטלית (ובפרט סכום ישר של ציקליות הוא אטלית)

אנחנו נראה שתהורה אטלית סופית הוא סכום ישר של ציקליות.

④ $\mathbb{Q}_+$ תהורה והאפס הם הצינוריים ביותם לחיבור. $\mathbb{Q}_+$ לא ציקלית. התהורה הנורמה "אספר צינור" $\frac{a}{b}$ ב אטלית האמה שלהם אחת. א-ב ואז לא יחד זהות שמתקבל $\mathbb{Q}_+$.
תוצאה: ב תהורה חזקה נורמה סופית של $\mathbb{Q}_+$ היא ציקלית.
 $\mathbb{Q}^+ \not\leq \mathbb{Q}_+$ היא לא נורמה סופית. זמש $\{\frac{1}{n} : n \in \mathbb{N}\}$ יורה א- $\mathbb{Q}_+$.

⑤ $\mathbb{Q}_x$ תהורה והאפס הם הצינוריים ביותם לפרט (זא אפס) היא בוזאא לא ציקלית אלא היא לא נורמה סופית.

$$\mathbb{Q}_x = \langle p \text{ ראשונה} \mid p > -1 \rangle$$

$$\mathbb{Q}_x^{zo} = \bigoplus_{p \text{ ראשונה}} \langle p \rangle$$

40 12.12.04
מקני"פ

A חבורה אבלית עם פעולה $+$ ואיבר יחידה 0

אם $n \in \mathbb{N}$! $a \in A$ אז $na = \underbrace{a+a+\dots+a}_n$ n פעמים

$$(-n)a = \underbrace{(-a)+\dots+(-a)}_n$$

מתקיימים 6 התוקים הבאים:

$$(m+n)a = ma + na$$

$$m \cdot 0_A = 0_A$$

$$n(a+b) = na + nb$$

$$0_{\mathbb{Z}} \cdot a = 0_A$$

זה קצת מלכיד מרחב וקטורי מעל שדה $\mathbb{Z}$ הוא
התפקיד השדה, אבל $\mathbb{Z}$ הוא לא שדה כי הוא לא סגור
לכפל הפוך.

הגדרה: A חבורה אבלית ! $X = \{\alpha_1, \dots, \alpha_n\} \subseteq A$ תת קבוצה סופית.

נאמר ש- X בסיס של A אם $a \in A$ ניתן לכתוב

באופן יחיד כ- $a = a_1\alpha_1 + \dots + a_n\alpha_n$ ואז $a_1, \dots, a_n \in \mathbb{Z}$

$$a = a_1\alpha_1 + \dots + a_n\alpha_n$$

אם היינו נשללים הכפלי אז היה

וכן מזהב- X . אז X יוצרת את A . החיבור בסיס (הם

שמוא פורש באופן יחיד, ולא דורש פורש.

למשל, לחבורה סופית אין בסיס. אם G סופית ! $g \in G$

אז $0 \cdot g = 0$ אבל גם $0 = (g) \cdot g$ אז הפעולה היא

לא יחידה.

דוגמה: $A = \mathbb{Z}^n$ וניקח $X = \{e_1, \dots, e_n\}$ כאשר

$e_i = (0, \dots, 0, 1, 0, \dots, 0)$ X בסיס של A כי לכל $\alpha = (a_1, \dots, a_n) \in A$

$$\alpha = a_1e_1 + \dots + a_ne_n$$

מקום i

הכתובה היא גם יחידה. הרי X בסיס של $\mathbb{Q}^n$ ושלם וכתובה

היא יחידה. (כי $\mathbb{Q}^n$ מרחב וקטורי מעל השדה $\mathbb{Q}$) אז בוגדא

אם בתת קבוצה $\mathbb{Z}^n \subseteq \mathbb{Q}^n$ וכתובה היא יחידה.

הפיתוח: בחזרה וקטנו V עם בסיס α אם $n \cdot \alpha$
 בסיס β של $F[x]$. $n \in F \setminus \{0\}$. את n בתמונה זה לא חשוב.
 למשל $\{2e_1, \dots, 2e_n\}$ הוא לא בסיס $-\mathbb{Z}^n$. למשל, הוא בסיס
 של $-\mathbb{Z}^n$ שהוא תת-תמונה.

הערה: בסיס A חסומה הוא לא יחיד. למשל, תרגיל: אם
 $X = \{\alpha_1, \dots, \alpha_n\}$ בסיס A אז $Y = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ גם
 $\alpha_1 = \alpha_1 + \sum_{i=2}^n c_i \alpha_i$ (צריך להכיל) .
 שלה $\sum c_i \alpha_i$ ושהצורה יחידה).

המשפט: אם A חסומה אז $X = \{\alpha_1, \dots, \alpha_n\}$ גם קבוצה
 נאמרת A חסומה תופשה X אם כל תמונה D
 של העתקה קבוצתית $\varphi: X \rightarrow D$ קיימת תמונה יחידה $\tilde{\varphi}: A \rightarrow D$
 שהיא הומומורפיזם. $\tilde{\varphi}(\alpha_i) = \varphi(\alpha_i)$ $1 \leq i \leq n$.

משפט: תהא A חסומה אז $X = \{\alpha_1, \dots, \alpha_n\}$ גם קבוצה של
 A . אזי התנאים הבאים שקולים:

- ① X בסיס של A
- ② A תופשה של X
- ③ קיים איזומורפיזם $\tilde{\varphi}: \mathbb{Z}^n \rightarrow A$ רק של $\tilde{\varphi}(e_i) = \alpha_i$
 $1 \leq i \leq n$ ואשר $\{e_i\}$ הבסיס הסטנדרטי של $\mathbb{Z}^n$.

הוכחה:

(1 $\Leftrightarrow$ 2) תהא D חסומה $\varphi: X \rightarrow D$ העתקה קבוצתית.
 צריך להוכיח שקיים הומומורפיזם יחיד $\tilde{\varphi}: A \rightarrow D$ יחיד רק של $\tilde{\varphi}|_X = \varphi$
 יהי $\alpha \in A$. X בסיס . $\alpha = \sum_{i=1}^n m_i \alpha_i$ קיימת הצורה יחידה
 נציב $\tilde{\varphi}(\alpha) = \sum_{i=1}^n m_i \varphi(\alpha_i)$, אם אנתנו חזים של $\tilde{\varphi}$ יהיה הומומורפיזם
 אין לנו בחירה אלא להגדיר אותו ככה, ולכן הומומורפיזם הוא בחירה אחת
 להא היא הומומורפיזם. למתכנת φ של X . אם חזים שלה יהיה
 הומומורפיזם אז תים אלו $\tilde{\varphi}(\sum_{i=1}^n m_i \alpha_i) = \sum_{i=1}^n m_i \tilde{\varphi}(\alpha_i)$ ואם $\tilde{\varphi}|_X = \varphi$ אז
 מתקבל $\tilde{\varphi}(\sum_{i=1}^n m_i \alpha_i) = \sum_{i=1}^n m_i \varphi(\alpha_i)$. נתר אבדוק של $\tilde{\varphi}$ הומומורפיזם (תרגיל)
 כן יש שימוש בחיפוי $\rightarrow$

(41)

(2) נניח A -על $X = \{\alpha_1, \dots, \alpha_n\}$ תופעה

$\psi: X \rightarrow \mathbb{Z}^n$ "ע" $\psi(\alpha_i) = e_i$ מאתר A -על X תופעה

קיים הומומורפיזם $\tilde{\psi}: A \rightarrow \mathbb{Z}^n$ רק $\tilde{\psi}(\alpha_i) = e_i$.

מצד שני, ראינו $e_1, \dots, e_n$ בסיס של $\mathbb{Z}^n$. מאתר A שבר

הוכחנו $(1) \Leftarrow (2)$ קיים הומומורפיזם $\tilde{\psi}: \mathbb{Z}^n \rightarrow A$ המקיים

$\tilde{\psi}(e_i) = \alpha_i$. יש $\tilde{\psi}: A \rightarrow \mathbb{Z}^n$! $\tilde{\psi}: \mathbb{Z}^n \rightarrow A$ המקיים

$\tilde{\psi} \circ \tilde{\psi}(e_i) = \tilde{\psi}(\alpha_i) = e_i$. מאתר A $\{e_1, \dots, e_n\}$ יוצרת את $\mathbb{Z}^n$

נבנה $\tilde{\psi} \circ \tilde{\psi} = \text{id}_{\mathbb{Z}^n}$ (זה אומר $\tilde{\psi}$ חתך $\tilde{\psi}$).

באופן דומה $\tilde{\psi} \circ \tilde{\psi}(\alpha_i) = \tilde{\psi}(e_i) = \alpha_i$. ראינו כי $\tilde{\psi} \circ \tilde{\psi} = \text{id}_A$.

עתה ראינו $X = \{\alpha_1, \dots, \alpha_n\}$ יוצרת את A .

למה: אם A תופעה $X = \{\alpha_1, \dots, \alpha_n\}$ אזי X יוצרת את A .

הוכחה: תבא $B = \langle \alpha_1, \dots, \alpha_n \rangle$ התכונה החלקית של A הנוצרת

"ע" $\alpha_1, \dots, \alpha_n$. צריך להוכיח $B = A$ או במילים

אחרות, $A/B = \{0\}$. נניח שלא. נניח $A/B = D$ היא

אל התכונה הסכימטית. נציין שני הומומורפיזמים $\tilde{\psi}_1, \tilde{\psi}_2: A \rightarrow D$

כאשר $\tilde{\psi}_1: A \rightarrow A/B$ הומומורפיזם המנה $\tilde{\psi}_2: A \rightarrow A/B$ הומומורפיזם

האפס. אז $\tilde{\psi}_1(\alpha_i) = \alpha_i B = B$, $\tilde{\psi}_2(\alpha_i) = 0_{A/B}$.

$\tilde{\psi}_2(\alpha_i) = 0_{A/B}$. $\tilde{\psi}_1|_X = \tilde{\psi}_2|_X \Leftarrow$. ראינו התכונה של תכונה

תופעה יש המשכה יחידה ונסיק $\tilde{\psi}_1 = \tilde{\psi}_2$. מכאן, יש לה

אותה תמונה, כלומר $A/B = \{0_{A/B}\}$ וכן סתירה.

(3) $(1) \Leftarrow (3)$ ברור כי $e_1, \dots, e_n$ בסיס של $\mathbb{Z}^n$

(42)

משפט: תבא A תכונה אדמית עם בסיס $X = \{\alpha_1, \dots, \alpha_n\}$ תבא B

תכונה חלקית של A . אזי קיים A -על $\bar{\psi}: A \rightarrow B$ $\bar{\psi} = \{\bar{\alpha}_1, \dots, \bar{\alpha}_n\}$

רק $B = \langle m_1 \bar{\alpha}_1, \dots, m_k \bar{\alpha}_k \rangle$ עבור $k \leq n$ $m_i \in \mathbb{Z}$!

ומתקיים $m_1 | m_2 | m_3 | \dots | m_k$

הוכחה: גאומטרית על n .

אם $n=1$, A תופעה על $\{\alpha\}$ אזי $A \cong \mathbb{Z}$ וכל יוצרים של

התכונות הבסיסיות של $\mathbb{Z}$ הן מהצורה $B = \langle m, 1 \rangle$.

עיה שמשפט נכון - ו-ח ונכוח א-ח.

בהינתן הסט B של $\mathbb{Z}$ וחסומה חלקית $B \leq A$ (נסמן ב- $f(\alpha, B)$)
אם השלש וחיבור m הקטן ביותר רק שלמים $0 \neq b \in B$ שמחזיקותו α
והסטים α מופיע m באחד המקדמים. תמיד קיים כזה אם $B \neq \{0\}$. למה
ניקח איזה $B \in \mathbb{Z}$ ונכתוב אותו לפי α . אז יש או מקדמים שלמים. אם
הם כלם שלילים אז נסתכל ב- $-B$. אז נקבל המקדמים החיוביים לא רק
אם קיים זה מניחים.

אנו נתונה B . יהי m המספר הקטן ביותר מבין $f(\alpha, B)$ ואשר α ח
כל הסטים A . נניח ש- m זה מתקבל עם הסטים $\{\alpha'_1, \dots, \alpha'_n\}$
ונניח $B \ni \beta = m\alpha'_1 + a_2\alpha'_2 + \dots + a_n\alpha'_n$ (בה"כ m המקדם של α'_1 כי
הסדר של הסטים לא חשוב וזה אומרו בחסומה אלוטרי).

למה: $m | a_i$ לכל $1 \leq i \leq n$

הוכחה: נחבר $a_i = q_i m + r_i$ כאשר $0 \leq r_i < m$. (ראה ל- $r_i = 0$).
(נחיל את הסטים α בסטים $\alpha = \{\bar{\alpha}_1, \alpha'_2, \dots, \alpha'_n\}$ ואשר $\bar{\alpha}_1 = \alpha'_1 + \sum_{i=2}^n q_i \alpha'_i$)
אז נרשיו $\beta = m\bar{\alpha}_1 + \sum_{i=2}^n r_i \alpha'_i$. לפי ההצדק שבה בחנו את m נובע
ש- $r_i = 0$, אחרת r_i מקדם קטן יותר של איבר של B ביותם אלוה
בסטים. $m | a_i \iff$

אז נאן ש- $\bar{\alpha}_1 = m\beta$. נעזר תהאן $A' = \langle \alpha'_2, \dots, \alpha'_n \rangle$. אזי $\alpha'_2, \dots, \alpha'_n$

בסטים של A' (כי ההצדקה יחידה). נסמן $B' = B \cap A'$. כוחסומה חלקית

של A' ונניח, אופציונלי שיהא את הנחת האינדוקציה.

טענה 1: $B' = \langle \beta \rangle \oplus B'$, שומרי B איבר של B נותן, ארתיבה באופן

יחיד סכומ של $\beta + r$ ושר $r \in \mathbb{Z}$! $\beta' \in B'$.

לפי הנחת האינדוקציה יש ל- A' בסיס. $\{\bar{\alpha}_2, \dots, \bar{\alpha}_k\}$ רק ל- $B' = \langle m_2 \bar{\alpha}_2, \dots, m_k \bar{\alpha}_k \rangle$

! - $m_2 | m_3 | \dots | m_k$. אחד עם סענה 1 נקבל ל- $B = \langle m\bar{\alpha}_1, m_2 \bar{\alpha}_2, \dots, m_k \bar{\alpha}_k \rangle$

טענה 2: $m | m_2$.

(נותר להוכיח את הטענה ...)

תחבורה אבליאן

הגדרה: תחבורה אבליאן A היא תופשי של X קבוצה $X = \{\alpha_1, \dots, \alpha_n\}$
 אולם הנתונה קבוצתית $X \rightarrow B$ ויש ψ מה B תחבורה אבליאן,
 קיימת המשכה יחידה והומומורפיזם $\tilde{\psi}: A \rightarrow B$

כיון שיש קורה אחר X מסים של A , ז"ל β אחר α של A
 נותן לרתיבה באופן יחיד כ- $\alpha = \sum_{i=1}^n a_i \alpha_i$ כאשר $a_i \in \mathbb{Z}$
 וכן ראינו שכל אחד של A איזומומורפיזם ל- $\mathbb{Z}^n$.
 בפרט נאמר ל- A תופשי של המסומ $\alpha_1, \dots, \alpha_n$

משפט: אם A תחבורה תופשי של מסים $\{\alpha_1, \dots, \alpha_n\}$ ב- B ,
 תחבורה חלקית של A , אזי קיים מסים $\{\bar{\alpha}_1, \dots, \bar{\alpha}_n\}$ ל-
 A ומספרים שלמים חיוביים $m_1, m_2, \dots, m_k \in \mathbb{Z}$ כך ל- $k \leq n$!
 $B = \langle m_1 \bar{\alpha}_1, \dots, m_k \bar{\alpha}_k \rangle$

הוכחה: נוכיח באינדוקציה על n . אם $n=0$ אז הכל ברור.
 אחרת, נניח $0 < n$. אם $\beta = \alpha$ אז נקח $k=0$ וסיימנו.
 אחרת, נניח $\beta \neq \alpha$. נניח $m = m_1$ (המספר השלם החיובי
 הקטן ביותר כך שלקיים מסים $\{\alpha'_1, \dots, \alpha'_n\}$ של A וקיים
 $\beta \in B$ כך ל- $\beta = m\alpha'_1 + a_2\alpha'_2 + \dots + a_n\alpha'_n$. אנחנו צוברים על β
 המסומים הגדולים ל- A ולכן אתה מהם צוברים על β הוקטורים
 ב- B שלמים מסופים ובתחתית אותם לפי המסומים המותרים ל-
 הוקטורים המצוינים מלמעלה האלה. נניח שהמסומים שממנו התקבל
 המסומ m הם $\{\alpha'_1, \dots, \alpha'_n\}$ ו- $\beta = m\alpha'_1 + \sum_{i=2}^n a_i \alpha'_i$.
 בשורה הקודמת הראינו ל- $a_2, a_3, \dots, a_n$ - $m \mid a_i$ - $a_i = q_i m$ - $(\alpha_i = q_i m - \alpha_i)$
 עבור $2 \leq i \leq n$ ונרשמו במסומים:

$$\{\bar{\alpha}_1 = \alpha'_1 + \sum_{i=2}^n q_i \alpha'_i, \alpha'_2, \dots, \alpha'_n\}$$

וכך אק מסים עם אלה קבוצתית. (נשים לב שהמסומים החדש הנה
 $\beta = m\alpha'_1 + \sum_{i=2}^n a_i \alpha'_i = m\alpha'_1 + \sum_{i=2}^n q_i m \alpha'_i =$
 $= m(\alpha'_1 + \sum_{i=2}^n q_i \alpha'_i) = m\bar{\alpha}_1$

נסמן $A' = \langle \alpha'_1, \dots, \alpha'_n \rangle$ קי ארואל של תמונה חופשית
 של המסומים $\{\alpha'_1, \dots, \alpha'_n\}$, שדרי תהיך ממסומים וואן זמ מסומים
 סתת תמונה שנוצרת של ידו. זו תמונה חופשית של $n-1$ יוצרים.
 נסמן $B' = B \cap A'$

למטה: $B = \langle m\bar{\alpha}_1 \rangle \oplus B'$, נומר $\langle \beta \rangle \cap B' = \{0\}$ וכל אבר
 של B נותן אריתמטיה כ- $\beta + \beta'$ כאשר
 $\beta' \in B'$, $\beta \in \langle \beta \rangle$

הוכחה: נניח $0 \neq \gamma \in \langle \beta \rangle \cap B'$ אז $\gamma \in \langle \beta \rangle$
 אז $\gamma \in B'$. $\gamma = r\beta = rm\bar{\alpha}_1$ עבור $r \in \mathbb{Z}$ כלל
 אז $\gamma \in B' \subseteq A'$ $\nLeftarrow \gamma = \sum_{i=1}^n a_i \alpha'_i$ עבור $a_i \in \mathbb{Z}$
 אז נכונה של $\{\alpha'_1, \alpha'_2, \dots, \alpha'_n\}$ מסומים אלק תמימות
 של יחידה. אז מצאנו שמי רתבאר שונוה וזו סתירה.
 (אם $r=0$ אז $\gamma=0$)

נוצר אריתמטיה של $\delta \in B$ נותן אריתמטיה כ- $\delta = \beta + \beta'$
 כאשר $\beta' \in B'$, $\beta \in \langle \beta \rangle$. נכתוב
 $\delta = a\bar{\alpha}_1 + \delta'$

כאשר $\delta' \in A'$. נסמן $a = qm + r$, $m \mid a$, $0 \leq r < m$
 כאשר $0 \leq r < m$ אז

$$\begin{aligned} B \ni \delta - \underbrace{qm\bar{\alpha}_1}_{\in B} &= (a\bar{\alpha}_1 + \delta') - qm\bar{\alpha}_1 = \\ &= (a - qm)\bar{\alpha}_1 + \delta' = r\bar{\alpha}_1 + \delta' \end{aligned}$$

זוהי של $\alpha'_1, \dots, \alpha'_n$

קבלנו איבר כ- B שיש לו הצגה לפי מסומים אם
 מקדמים $r < m$ וזו סתירה למניחיות של m , אלא אם

$$r=0 \quad \nLeftarrow m \mid a \quad \nLeftarrow a = mq \quad \text{אז}$$

$$\delta = mq\bar{\alpha}_1 + \delta' = q(m\bar{\alpha}_1) + \delta' = q\beta + \delta'$$

כאשר $\delta' \in A'$. אז $\delta' = \delta - q\beta \in B$, $\delta' \in A' \cap B = B'$ $\nLeftarrow$

וסיימנו את הוכחה הזו.

43) B' הוא חבורת חלקי ℓ A' של $n-1$ גורמים $\overline{d_2}, \dots, \overline{d_n}$ A' ק"מ מסוים $B' = \langle m_2 \overline{d_2}, \dots, m_k \overline{d_k} \rangle$ $m_2 | m_3 | \dots | m_k$ תוס"ם $k \leq n \iff k-1 \leq n-1$

$B = \langle m\bar{\alpha}_1, m_2\bar{\alpha}_2, \dots, m_k\bar{\alpha}_k \rangle$; A על סוס $\{\bar{\alpha}_1, \dots, \bar{\alpha}_n\}$ -
 $\beta \in B$ אז $B' = B$ - ושלום -
 נגד אחרון - $m = m_1 | m_2$

רצוי להוכיח זאת (נתון) $m_2 = qm + r$ עבור $0 \leq r < m$
 ונראה ש- $r=0$. (אם לא) $\bar{\alpha}_1 = \bar{\alpha}_1 + q\bar{\alpha}_2$ (אם לא) $\bar{\alpha}_1 = \bar{\alpha}_1 + q\bar{\alpha}_2$
 $\{\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n\}$ חסמים של A . (אם לא) $\bar{\alpha}_1 = \bar{\alpha}_1 + q\bar{\alpha}_2$

$$\begin{aligned} B \quad \Rightarrow m \bar{a}_1 + m_2 \bar{a}_2 &= m \bar{a}_1 + m g \bar{a}_2 + r \bar{a}_2 = \\ &= m (\bar{a}_1 + g \bar{a}_2) + r \bar{a}_2 = \\ &= m \bar{a}_1 + r \bar{a}_2 \end{aligned}$$

אם $r \neq 0$ וישם קיבלנו סתירה (מניחים) ל m כי $m \geq 3$ ואם $r = 0$ $\Rightarrow r < m$ מקבל $r = 0$ וסיום.

(2) אסתר ניה: $\frac{\text{ת"ה של}}{\text{חמורה}}$ אפ"ה חופש'ה של n יוצרים ויא חופש'ה של $k \leq n$ יוצרים.

הוכחה: אם $B \leq A$ ו- k קיים בסיסם של A $X = \{\bar{\alpha}_1, \dots, \bar{\alpha}_n\}$ רק ל- $B = \langle m, \bar{\alpha}_1, \dots, m_k \bar{\alpha}_k \rangle$. נאמן ל- $Y = \{m, \bar{\alpha}_1, \dots, m_k \bar{\alpha}_k\}$ סיסם של B . אבל זה ברור כי B אינה B המו ציורו פונקציה של איברי Y $\varphi = \sum_{i=1}^k a_i (m_i \bar{\alpha}_i)$ $B \ni \varphi$ כי הם יוצרים a_i - (קבוצים באופן יחיד כי $a_i m_i$ קבוצים באופן יחיד כי X סיסם.

הצורה: אם M חבורה אבלית נוצרת ספית, נניח נוצרת
 $\mathcal{A}$ " ח אבליים אזי M ^{אויסלויפ} מתבוננת מנה של n חבורות החופשיות
 $\mathcal{A}$ ח " נוצרים. כי אם A חופשית על $\mathcal{A}$, $\dots$, וואל M -
 נוצרת " $\mathcal{A} \subseteq M, \dots, \mathcal{A}$ אזי אם ההצטרפה הקבוצתית $\mathcal{A} \mapsto \mathcal{A}$

ניתן להרחיב למונחורפוס $\tilde{\varphi}: A \rightarrow M$ ותואר $\tilde{\varphi}$ כי $\{a_1, \dots, a_n\}$ יוצר את M . $M \cong A/B$ שם $B = \text{Ker } \tilde{\varphi}$.

^{אספקת} משקלה: אם M תורה אספקת נוצר סופי, ונניח $d(M) = n$ אזי קיימים שלמים $m_1, m_2, \dots, m_k$ כאלו $k \leq n$ כך ש-
 $M \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/m_k\mathbb{Z} \oplus \mathbb{Z}^{n-k}$.
 נוצר סופי הוא סכום של תורה ציקליות.

הוכחה מסתמך על $M \cong A/B$. $\tilde{\varphi}$ היא המלכה המרכיב ישר A הסוס $\{\bar{a}_1, \dots, \bar{a}_n\}$ רק ל- $B = \{m_1\bar{a}_1, \dots, m_k\bar{a}_k\}$.

כאשר $k \leq n$ $m_1, m_2, \dots, m_k$.
 $A/B \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/m_k\mathbb{Z} \oplus \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{\substack{\text{n-k פרטים} \\ \text{וסה איסומורפ} \\ \text{ל } \mathbb{Z}^{n-k}}}$
 (הסבר בתרגיל)
 (11)

משקלה: תורה סופי אספקת M היא סכום ישר של תורה ציקליות. יגדל k היא איסומורפיה ל- $\mathbb{Z}/m_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/m_k\mathbb{Z}$ ואשר $m_1 | m_2 | \dots | m_k$.

סלנה: ל תורה אספקת ספר M היא איסומורפיה לסכום ישר של תורה ק-סולא שלה.

משקלה: אם M תורה ק אספקת סופי, טואר M אספר r אספר $r \in \mathbb{N}$ בלען, אלץ קיימים $r_1, \dots, r_k$ כך ש-
 $M \cong \mathbb{Z}/r_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/r_k\mathbb{Z}$! $\sum_{i=1}^k r_i = r$, $r_1 \leq \dots \leq r_k$.
הוכחה: משקנה מייצר משקנה 3.

סלנה: הפירוק המשקנה 4 הוא יחיד. (הוכחה בתרגיל)

משקנה: אספר התורה האספקת אספר r שונה ל- $\sigma(r)$ (פונקציה החלוקה).

(iii)

הלכה: מספר החבורה האנליטית מסדר r שווה למספר
האנליטיות איתן r כסכום $r_1 + \dots + r_k = r$ ואלו
 $r_1 \geq 1, \dots, r_k \geq 1$ ומספר זה שווה ל- $\sigma(r)$ (זו בדיוק
ההיגדרה של $\sigma(r)$).

(iv)

נשים  שהמספר שלהן תלוי רק ב- r , לא ב- p .
אם מספר החבורה האנליטית מסדר $2^3 = 8$ שווה למספר
החבורה האנליטית מסדר $3^2 = 9$.

(v) מסתבר: יחס $n \in \mathbb{N}$ ונניח $n = p_1^{d_1} \dots p_e^{d_e}$ הפירוק של n
למכפלה ראשונית נגיד $p_i \neq p_j$ אזי $i \neq j$. אז
מספר החבורה האנליטית מסדר n הוא $\sigma(d_1) \cdot \dots \cdot \sigma(d_e)$.
לכנס תלוי רק בהצגה ולא בראשוניים.
הלכה: מסתבר מהעצמה של חבורה אנליטית היא מכפלה
ה- p -סימולטאניה + מסתבר s .

יום רביעי אין שיעור

Rings

חוג' P



הגדרה: חוג הוא קבוצה R עם איבר נייטר 0 (האפס) ושני פעולות בינאריות $+$ ו- $\cdot$ (כפל) המקיימות:

$$(R, 0, +) \text{ תבורה קומוטטיבית} \quad (א)$$

$$\forall r, s, t \in R \quad r(s \cdot t) = (r \cdot s) \cdot t \quad (ב)$$

$$\forall r, s, t \in R \quad r \cdot (s + t) = r \cdot s + r \cdot t \quad (ג)$$

$$\forall r, s, t \in R \quad (r + s) \cdot t = r \cdot t + s \cdot t$$

הערות:

(א) אם פורשים גם 1 - $r \cdot s = s \cdot r$ R נקרא חוג קומוטטיבי

(ב) אם פורשים קיום איבר $1 \neq 0$ המקיים $1 \cdot r = r \cdot 1 = r$ כל

$r \in R$ נקרא חוג עם יחידה.

(ג) חוג קומוטטיבי עם יחידה יקרא R יש r^{-1} יקרא r -

$$r r^{-1} = 1$$

(ד) $r \in R$ נקרא הפיך אם קיים $s \in R$ כך ש- $rs = sr = 1$ (חברים r ו- s)

יש ספרים שמראש מגדירים שכל חוג יש יחידה. זה לא אגבני כן

כי בהינתן חוג כללי יחידה יש דרך קאנונית להחזיק אותו

אם יחידה.

רוב החוגים שנלמדו בהם יהיו חוגים עם יחידה.

פולינומים

(א) שדה הם חוגים

(א) $\mathbb{Z}$ השלמים עם החיבור והכפל הרגילים. זה חוג קומוטטיבי עם יחידה.

(ב) F שדה. x משתנה. $F[x]$ היא חוג הפולינומים במשתנה x

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

כאשר $a_i \in F$. a_0 נקרא המקדם התופש. $a_n \neq 0$ היא

המקדם העליון. n היא מעלה (או צורת) הפולינום.

חיבור פולינומי

$$\sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i) x^i$$

כפל פולינומים

$$(\sum a_i x^i)(\sum b_j x^j) = \sum_k (\sum_{i+j=k} a_i b_j) x^k = \sum_{i,j} a_i b_j x^{i+j}$$

נתון ההגדרה ה"נ" $F[X]$ תוך קומפטיבי עם חיבור וקל

$$0 \text{ היא הפולינום } f(x)=0 \quad 1 \text{ היא } f(x)=1$$

באופן דומה ניתן להגדיר פולינומים עם כמה משתנים.

$$f(x,y) = \sum a_{ij} x^i y^j \quad f \in F[X,Y] \text{ מהצורה}$$

והחיבור והכפל נעשים לפי חוקי האגדה הרגילים.

אם S מחוג פולינומים ביותר ממשתנה אחד הם הרבה הרבה

הרבה יותר מסובכים מחוגי פולינומים במשתנה אחד.

(3) F שדה, $M_n(F)$ מנסל המטריצות $n \times n$ מעל שדה F

אם ϕ חיבור וזמנים של מטריצות. ידוע ש-

$$A(B+C) = AB + AC$$

$$(A+B)C = AC + BC$$

$$A(BC) = (AB)C$$

$$AB \neq BA \quad n \geq 2 \text{ כל } n$$

כל $n \times n$ עבור $2 \leq n$ $M_n(F)$ תוך עם קומפטיבי עם 0

$$1 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

(4) V או n מעל שדה F - $R = \text{End}(V)$ היסטורמורפיזמים

ההיסטוריות $T: V \rightarrow V$ או ϕ והרכבה של היסטורמורפיזמים

$$(T_1 + T_2)(v) = T_1(v) + T_2(v)$$

$$(T_1 \cdot T_2)(v) = T_1(T_2(v))$$

אם ϕ האפס היא $0(v) = 0$ ואיבר היחידה היא

$$1(v) = v$$

$$(T_1 + T_2)S = T_1S + T_2S$$

מתקיים

כה נובע ישירות מההגדרה הישירה:

$$((T_1 + T_2)S)(v) = (T_1 + T_2)(S(v)) = T_1(S(v)) + T_2(S(v))$$

(46)

$$S(T_1 + T_2) = ST_1 + ST_2 \quad \text{אחריות זה}$$

זה נובע ישירות מהגדרתו של S :

$$\begin{aligned} (S(T_1 + T_2))(v) &= S((T_1 + T_2)(v)) = S(T_1(v) + T_2(v)) = \\ &= S(T_1(v)) + S(T_2(v)) = (ST_1 + ST_2)(v) \end{aligned}$$

אז זה מתקין: החוק הקריטיבי הישן נכון בלי שום קשר

עליונות. זה עובד לכל הפונקציות $V \rightarrow V$. ואילו החוק

הקריטיבי הישן עובד עדיין...

ההתקנה

(5) תהא Γ חבורה אבלית ויהי F שדה. נסמן $F[\Gamma]$.

אם אנחנו הביטויים הסופיים $\sum_{g \in \Gamma} a_g g$ כאשר $a_g \in F$

ציתים זיכרונות של איברי Γ הם מקדמים n - F .

הכפל והחיבור מוגדרים באופן הבא:

$$(\sum a_g g) (\sum b_h h) = \sum_{g,h} a_g b_h gh$$

שדה חבורה (להשלכה)

$$(\sum a_g g) + (\sum b_g g) = \sum (a_g + b_g) g$$

שני איברים ב- $F[\Gamma]$ הם שווים אם המקדמים שלהם שווים.

עם ההגדרה הזו טובה.

קל לראות ש- $F[\Gamma]$ הוא אסוציאטיב של חבורה:

$$\begin{aligned} ((\sum a_g g) (\sum b_h h)) (\sum c_k k) &= (\sum a_g b_h gh) (\sum c_k k) = \\ &= \sum (a_g b_h) c_k (gh) k = \sum a_g (b_h c_k) g (hk) = \\ &= (\sum a_g g) (\sum b_h h) (\sum c_k k) \end{aligned}$$

יש טון שימוש באסוציאטיביות בין החבורה וקו הבלדה.

החוק הקריטיבי אמנם התקנה קלאסית.

איפה הדבר הזה נשאר? רשמיים הם אינסופיים? הבעיה היא

כלים: מסופו של דבר ב- $F[\Gamma]$ צריך להיות נתיב

הצורה $\sum_{g \in \Gamma} a_g g$. אז רשמיים אפי' ההצורה אחי הכפל צריך

עכשיו ארס האברים הלדים. אבל זה מן הנמנע שאחרי הכפל

איזה איבר g יופיע אינסוף פעמים בסכום. אז צריך לקדם את

המקדמים שלו. אבל בלדה בלי בלדה אנחנו בלל לא יוצאים אף

לחבר מספר אינסופי של איברים...

$$(g^3=e) \quad \Gamma = C_3 = \{e, g, g^2\} \quad ; \quad F = \mathbb{R} \quad , \text{מרחב} \\ F[\Gamma] = \{ae + bg + cg^2 : a, b, c \in \mathbb{R}\} \quad \text{מרחב}$$

$$(e+g+g^2)(g-e) = g+g^2+e - e-g-g^2 = 0$$

$$(אם) \quad g-e \neq 0 \quad ! \quad e+g+g^2 \neq 0 \quad \text{אם יש לנו מרחב, אפשר!}$$

$$(6) \quad [0,1] \text{ אולי הפונקציות הממשיות הנצפות } \mathbb{C}[0,1]$$

$$(f+g)(x) = f(x) + g(x)$$

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

$$0(x) = 0$$

$$1(x) = 1$$

זה תהי קואמוטטיבית עם יחידה. זה נותן מאנאלזה כי סכום ופח
של רציפות הוא פונקציה רציפה.

האיברים ההפיכים ב- $\mathbb{C}[0,1]$ הם אלה שאינם נאולים

$$f(x)g(x) = 1$$

אז אלה הפונקציות שלא נאולות אף מקומם 0! כי אז

$$g(x) = \frac{1}{f(x)}$$

ובו פונקציה רציפה אם $f(x) \neq 0$. הכול הרציפה נותן $f(x) < 0$
או $f(x) > 0$ לכל $x \in [0,1]$.

טענה: אולי האיברים ההפיכים בחוג $\mathbb{R}$ מהווים חבורה כפול
המסומנת $\mathbb{R}^*$.

$$\mathbb{Z}^* = \{ \pm 1 \}$$

$$\mathbb{Z}_4^* = \{ 1, 3 \}$$

$$\mathbb{R}[x] = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$$

הוכחה: צריך להראות שלחוקי החבורה נוחה:

$$r_1 s_1 = s_1 r_1 = 1 \quad \text{נניח ש-}$$

$$r_2 s_2 = s_2 r_2 = 1$$

$$(r_1 r_2)(s_2 s_1) = r_1 (r_2 s_2) s_1 = r_1 s_1 = 1 \quad \text{אם}$$

אם (מחשבה) הפיכה

- אסוציאטיבית (נותן מהאסוציאטיביות ב- $\mathbb{R}$).

47

(י)

- סטורות (הופכי) נובע מהגדרת R^* .

הגדרה: גל תחיל של תחיל R הינו תחיל קבוצה S המהווה תחיל חבורה
 ביחס לחיבור ו (היא סגורה תחת כפל). (סמן $S \subseteq R$
 (אם R יש יחידה (קרוס e - $1 \in S$).

דוגמאות:

$$M_n(\mathbb{R}) \subseteq M_n(\mathbb{C}) \quad (1)$$

$$F[\Delta] \subseteq \Gamma(\Gamma) \quad \Delta \subseteq \Gamma \text{ תחיל חבורה} \quad (2)$$

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \quad (3)$$

$$\mathbb{R}[X] \subseteq \mathbb{R}[X, Y] \quad (4)$$

הומומורפיזמים

הגדרה: הומומורפיזם $\varphi: R \rightarrow S$ בין תחילים הינו העתקה

המתאימה לכל איבר $r \in R$ איבר $\varphi(r) \in S$ כך ש-

(א) φ הינו הומומורפיזם של חבורה קומוטטיבית ביחס $+$ - $\varphi(r+s) = \varphi(r) + \varphi(s)$

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad ! \quad \varphi(0_R) = 0_S$$

$$\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s) \quad (ב)$$

$$\varphi(1_R) = 1_S \quad \text{אם יש } 1 \text{ } (ג)$$

אנומורפיזם = הומומורפיזם ההפוך

איזומורפיזם = הומומורפיזם של

אנדרומורפיזם = הומומורפיזם $R \rightarrow R$

איסומורפיזם = הומומורפיזם ההפוך (ואם φ ההעתקה ההפוכה)

י"א (איסומורפיזם)

אויסומורפיזם = איסומורפיזם $R \rightarrow R$

$$\varphi|_R = id \quad ! \quad \mathbb{R}[X, Y] \xrightarrow{\varphi} \mathbb{R}[X, Y]$$

נויה $\varphi(x) = f$! $\varphi(y) = g$ φ בהכרח תחיל אומקיים

$$\varphi(\sum a_{ij} x^i y^j) = \sum a_{ij} f^i g^j$$

סעיף: אם $f, g \in R[X, Y]$ הנוסחה לעיל מחזירה הומומורפיזם.

הוכחה: ראשית, זה מוגדר הוכח כי f פולנום יש צדק גת ויתרה איתנה גתו כ- $\sum a_j X^j Y^j$.

שנית, דנים למפיק תימוריות ונראה אם זה סבור. (תניא!) (ii)

שאלה: אתי φ נגד איזומורפיזם φ סבור מהו התנאי על f, g נגד φ תהיה? וכן?

זו תהיה בעיה. תחת הנחה מסוימת נותן לפתור את זה. למשל אם $f = ax + by$ $g = cx + dy$ אז φ איזומורפיזם אמנם $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ הפירה.

למקרה ש- f, g אינם ליניאריים יש איזו השערה. אולי שם צבר לא מוחל על צדן...

הערה: יהי φ הומומורפיזם.

$$\text{Im } \varphi = \text{התמונה של } \varphi$$

$$\text{Ker } \varphi = \{r \in R : \varphi(r) = 0\} = \text{הגרעין של } \varphi$$

סעיף: $\text{Im } \varphi$ הוא $\varphi: R \rightarrow S$ הומומורפיזם (הוא גת-חוק של S (כי הוא גת חבורה - זה יבדוק בה) $\varphi(r_1)\varphi(r_2) = \varphi(r_1 r_2)$; סבור יש סבור אולי)

סעיף: $\text{Ker } \varphi$ הוא $\varphi: R \rightarrow S$ הומומורפיזם (הוא גת-חבורה חבורה של החוק R (הוא חבורה) $a \in \text{Ker } \varphi$ $r \in R$ $sr = r \in R$ $\varphi(ar) = \varphi(a)\varphi(r) = 0$

אם $a \in \text{Ker } \varphi$ $r \in R$ $ar \in \text{Ker } \varphi$, $ra \in \text{Ker } \varphi$.

הערה: אידיאל בחוק R הוא קבוצה I של R גת חבורה חבורה- $a \in I$ $r \in R$ $ra \in I$, $ar \in I$.

סעיף: אם הומומורפיזם φ $\text{Ker } \varphi$ הוא אידיאל של R .

תרג R הוא $(R, +, \cdot, 0)$ טור R קבוצה ו-
 מוגדרת לפי פעולות בינאריות $+, \cdot : R \times R \rightarrow R$ כך ש-
 $(R, +, 0)$ תהווה קומוטטיב, $\cdot$ פעולה אסוציאטיבית
 ומתקיימת דיסטריביוטיוו ממש: $r, s, t \in R$ δ

$$r(s+t) = rs+rt$$

$$(r+s)t = rt+st$$

בהינתן R ו- S תהיה $\varphi : R \rightarrow S$ תהיה
הומומורפיזם של תהיה אם היא שמרנית על התיכור אם δ
 הרפ: $a, b \in R$ δ

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$

$$\varphi(ab) = \varphi(a) \varphi(b)$$

אם $\varphi : R \rightarrow S$ הומומורפיזם (סמן)
 $K = \ker \varphi = \{a \in R : \varphi(a) = 0\} \subseteq R$
 $L = \text{Im } \varphi = \{b \in S : \exists a \in R \varphi(a) = b\} \subseteq S$
 כאנו ש- $\text{Im } \varphi$ תהיה תהיה S ו- $\ker \varphi$ תהיה
 תהיה תהיה של R אכן, יתכן מלה, $\ker \varphi$ הוא אידיאל!

נשים לב שאם R תהיה δ יחידה: $1 \in \ker \varphi$ אז $\varphi \equiv 0$
 לכן $\varphi(a) = \varphi(a \cdot 1) = \varphi(a) \cdot \varphi(1) = \varphi(a) \cdot 0 = 0$

נסתב δ $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in \mathbb{Z}\}$ קדם לראות שזה אכן
 תהיה (ללא הופכי). בתוך זה יש דבר מוזר. נסתב למה
 δ $3 = (1+\sqrt{2})(1-\sqrt{2})$ אנתוני רצאים ש-3
 הוא ראשוני - שומר או אפשר לפרק אולי. אכן ה- $\mathbb{Z}[\sqrt{2}]$
 פוקא ק נימא אפיון!

אפשר להגדיר עתים δ אידיאלים ואז אידיאל ראשוני, ושל
 דווקא אפשר להבין את של אידיאל (הוא מרפס) של אידיאלים
 ראשוניים.

אבוי! לא הגדתי מהו אידיאל.

אם R חוג $I \subseteq R$! - תת קבוצה I (נקראת אידיאל)

דו צדדי גם מתקיימים התנאים הבאים:

(1) I תת חבורה תחתונה של R

(2) אם $r \in R$ ואם $a \in I$ אז $ra, ar \in I$

(האידיאל ימני מתקיים רק $ar \in I$ והאידיאל שמאלי מתקיים

רק $ra \in I$). אידיאל דו צדדי מסומן $I \triangleleft R$.

זרעון של הומומורפיזם הוא אידיאל, שפר+

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0$$

$$\varphi(ar) = \varphi(a)\varphi(r) = 0 \cdot \varphi(r) = 0$$

$$ar, ra \in \text{Ker } \varphi \Leftarrow$$

(לכיוו שחבורה היא נורמלית אמ"ה היא זרעון של אידיאל הומומורפיזם. תכל' נראה שלא כל החבורות קליר בתחומים עם אידיאלים.

יהא R חוג $I \subseteq R$ אידיאל. אזי I חבורה חלקית (נורמלית

של החבורה החבורית של R (נורמלית כי היא אבלי)

אם מוגדר R/I בחבורה מנה. (עם מתקל $a+I$)

נאמר על R/I גם אמנה של (פ) ונרשום אותו מוג:

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

זכר, ארשק שלה מוגדר היטב ושלם מתקיים אסוציאטיביות ופוטנציאליות.

ראשית, הפש (זה מוגדר היטב. נניח ש- $a+I = a'+I$ (*)

! - $b+I = b'+I$ (**). צריך להראות ש- $ab+I = a'b'+I$.

אם $a = a' + j$ עבור $j \in I$! - (**).

נבדד ש- $b = b' + l$ עבור $l \in I$. אם

$$ab = (a'+j)(b'+l) = a'b' + \underbrace{a'l + j'b' + jl}_{\in I} = a'b' + k$$

$$\in I \text{ (רפי גבורה האידיאל)}$$

$$ab+I = a'b'+I \Leftarrow \text{אם ההפך}$$

(49)

כזה (הוא) שלמקסימום התכונות הפורמליות (הרוב):

$$\begin{aligned} \star (a+I)((b+I)(c+I)) &= (a+I)((b+c)+I) = \\ &= (a+(b+c)) + I \stackrel{\text{קסר } R-2}{=} ((a+b)+c) + I = \\ &= ((a+b)+I)(c+I) = ((a+I)(b+I))(c+I) \end{aligned}$$

$$\begin{aligned} \star (a+I)((b+I)+(c+I)) &= (a+I)((b+c)+I) = \\ &= (a(b+c)) + I \stackrel{\text{קסר } R-2}{=} (ab+ac) + I = \\ &= (ab+I) + (ac+I) = (a+I)(b+I) + (a+I)(c+I) \end{aligned}$$

$$\begin{aligned} \star ((a+I)+(b+I))(c+I) &= ((a+b)+I)(c+I) = \\ &= (a+b)c + I \stackrel{\text{קסר } R-2}{=} (ac+bc) + I = \\ &= (ac+I) + (bc+I) = (a+I)(c+I) + (b+I)(c+I) \end{aligned}$$

יפסי ספי, $\pi: R \rightarrow R/I$, אז R/I הוא פירעון (פי) של R .

ההשלכה הספיקה $\pi: R \rightarrow R/I$ המוגדרת "ע" $a \mapsto a+I$

היא הומומורפיזם של חוגים, שפרט:

$$\pi(ab) = ab+I = (a+I)(b+I) = \pi(a)\pi(b)$$

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

וד כמובן של אבריו של I הוא, כלומר, I אידיאל

הוא גרעין של הומומורפיזם.

אסימטרית תת-קבוצה של חוג היא אידיאל אמר היא גרעין

של הומומורפיזם.

משפט ההומומורפיזם יהיו R, S חוגים, $\varphi: R \rightarrow S$

הומומורפיזם (סמ) $I = \ker \varphi$ אז

$$\operatorname{Im} \varphi \cong R/I \quad ! \quad S \text{ תת חוג של } S$$

הנחה: אנו יבנה יוצרים של φ משהו איזומורפיזם של חבורה

$$\tilde{\varphi}: R/I \rightarrow \operatorname{Im} \varphi \quad \text{המשקל "ע" } \tilde{\varphi}(a+I) = \varphi(a)$$

דבר זה שיש להנחה הוא של $\tilde{\varphi}$ איזומורפיזם של חוגים ואכן:

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

(5)

משפט ההתאמה: R חוג $! - R/I$ אידיאל. יש התאמה
 חד-חד-חד ϕ בין תת-חוגים של R/I לתת-חוגים של R החתומים
 אחר I . וכן יש התאמה חד-חד ϕ בין אידיאלים (בהתאמה:
 אידיאלים ימניים / אידיאלים שמאליים) של R/I לבין
 אידיאלים (בהתאמה: אידיאלים ימניים / אידיאלים שמאליים)
 של R החתומים אחר I .

הוכחה: ראוי, שיש התאמה חד-חד ϕ בין החבורה החתומה
 האצטביוג של $(R, +)$ החתומה אחר I לבין החבורה החתומה
 האצטביוג של R/I הניתנת ϕ : אם L חבורה חתומה
 של $(R, +)$ החתומה אחר I נבאים את $\bar{L} = \{l+I : l \in L\}$
 הפופק, אם M חבורה חתומה של $(R/I, +)$ אז
 אנחנו זה $\tilde{M} = \{a \in R : a+I \in M\}$. ומקיים

$$\tilde{\bar{L}} = L \quad \text{חבורה חתומה חתומה אחר } I$$

$$\bar{\tilde{M}} = M \quad \text{חבורה חתומה חתומה אחר } M \text{ של } (R/I, +)$$

דיווחנו את המשפט שלו צריך:

(א) אם L חתומה חתומה אחר $\bar{L}$ חתומה
 ואם M חתומה אחר $\tilde{M}$ חתומה

(ב) אם L אידיאל (ימני/שמאלי) אזי $\bar{L}$ אידיאל (ימני/שמאלי)
 אם M אידיאל (ימני/שמאלי) אזי $\tilde{M}$ אידיאל (ימני/שמאלי).

(וכי כן אחר (כ) (א' נשלח באופן דומה).

יהא L אידיאל נ- R החתומה אחר I . צב $\bar{L} = \{l+I : l \in L\}$

אידיאל נ- R/I . ואכן, נניח $a+I$ איבר של R/I .

$$(a+I)(l+I) = \underbrace{al}_{\in L} + I \in \bar{L}$$

ובאופן דומה $(l+I)(a+I) \in \bar{L}$. לכן $\bar{L}$ אידיאל.

נניח עתה M אידיאל נ- R/I . וצריך להוכיח ש- $\tilde{M}$ אידיאל.

נניח $a \in R$, $m \in \tilde{M}$. צריך להראות ש- $am, ma \in \tilde{M}$.

אם $\tilde{M} = \{r \in R : r+I \in M\}$. אם $m \in \tilde{M}$ אז $m+I \in M$ וכן

להראות ש- $am, ma \in \tilde{M}$ צריך להראות $am+I, ma+I \in M$

50

$$(am + I) = (a + I)(m + I) \in M$$

ואם

כי M איז רינג

$$(ma + I) = (m + I)(a + I) \in M$$

11

משפט ההומומורפיזם השלישי: אם I, K אידיאלים ב- R כזה ש- $K \subseteq I$ אז

$$(R/K)/(I/K) \cong R/I$$

הוכחה: ידוע של איזומורפיזם של חבורות אבליאניות המוגדרת

$$\psi: (r+K) + I/K \mapsto r+I$$

זוהי, אכן, איזומורפיזם של חבורות אבליאניות, כי הוא שלול

הומומורפיזם של תוצאות. ואכן:

$$\begin{aligned} \psi(((r_1+K) + I/K)((r_2+K) + I/K)) &= \\ = \psi((r_1+K)(r_2+K) + I/K) &= \psi(r_1 r_2 + I) = \\ = r_1 r_2 + I &= (r_1 + I)(r_2 + I) = \\ = \psi((r_1+K) + I/K) \psi((r_2+K) + I/K) \end{aligned}$$

12

משפט ההומומורפיזם השלישי: אם R רינג, I אידיאל ב- R

! H - תת חבור של R אזי $H \cap I$ אידיאל ב- H !

$$H/H \cap I \cong H + I/I$$

הוכחה: $H \cap I$ אידיאל ב- H כי אם $h \in H \cap I$

$\rightarrow h \in H$ ו- $h \in I$ אז $h \in H \cap I$!

אם $h \in H$ אז $h + H \cap I$ אידיאל ב- $H/H \cap I$!

אז $H/H \cap I \cong H + I/I$ (לפי משפט ההומומורפיזם השלישי).

הערה: האיזומורפיזם (למעשה) $\psi: h + H \cap I \mapsto h + I$

$$\psi((h_1 + H \cap I)(h_2 + H \cap I)) = \psi(h_1 h_2 + H \cap I) = h_1 h_2 + I =$$

$$= (h_1 + I)(h_2 + I) = \psi(h_1 + H \cap I) \psi(h_2 + H \cap I)$$

13

51) 31.12.04
מספרים ממשיים

הצורה: תחום שלמות (Integral Domain) הוא חוג קומוטטי R
כזה שחוקי אפס, כלומר אם $a, b \in R$ וכן $ab = 0$ אז
 $a = 0$ או $b = 0$.

דיווח

1 - עזרה

2 - ב תת חוג של R הוא תחום שלמות

משפט: ב תחום שלמות ניתן לשיכון כלשהו

משפחה (2) היא הדוגמה הבאה של

רעיון ההוכחה: נושאים משני מסלול דומה לרעיון של הרציונלים
השלמים. מסתמים על $R \times R$ ומגדירים יחס שקילות $(a, b) \sim (c, d)$
אם $ad = bc$...

שאלון

אנחנו: תחום שלמות R סופי הוא שדה.

הוכחה: נניח $a \in R$, $a \neq 0$. אז ההפחה $a \cdot$ היא תחומה על R .

אם $a(b_1 - b_2) = 0$ אז $ab_1 = ab_2$ כי אם $a(b_1 - b_2) = 0$

אז $a \neq 0$ ואין מחלקי אפס $\Leftrightarrow 0 = b_1 - b_2 \Leftrightarrow b_1 = b_2$.

אם $a \neq 0$ סופי ולכן יש הפחחה $a \cdot$ על R , שזו תמונה.

עבור $c \in R$ יש $c = ac$ זהו c על c , אבל $c \in R$ קיים

$d_b \in R$ וכן $ad_b = b$ עבור d_b .

$$bc = (ad_b)c = acd_b = ad_b = b$$

$\Leftrightarrow c$ איבר יחידה (אוכל).

עבור $c \in R$, $c \neq 0$ וקיים הפחחה $c \cdot$ על R שזו תמונה.

יש $c = cb$ וכן $c = cb$ וכן $c = cb$.

$\Leftrightarrow R$ שדה, שבהי הדברים היחידים מסתמים לתחום שלמות

ובו שיהיה שדה גם איבר יחידה וסגור תחת כפל.

☺

52

הגדרה: R הוא (אברהם קומוטטיבי) $a \in R$ אז

$$Ra = \{ ra : r \in R \}$$

הוא אידיאל שמאל. הנקרא האידיאל הימני הנורמלי a .

$aR = \{ ar : r \in R \}$ האידיאל הימני הנורמלי a .

אם R קומוטטיבי אז $Ra = aR$ (הוא נקרא האידיאל הנורמלי a).

הגדרה: תחום ראשי (Principal Ideal Domain) זה תחום קומוטטיבי שבו כל אידיאל הוא ראשי.

דוגמה: $\mathbb{Z}$ הוא תחום ראשי כי כל אידיאל בו הוא מנוון.

$a \in \mathbb{Z}$ אידיאל הוא בהכרח מנוון. חלקי, אבל התכונות

החלקי היתרון הן $a \in \mathbb{Z}$ - a הם אידיאלים ראשיים.

$\Leftarrow$ כל אידיאל הוא ראשי $\mathbb{Z}$ - תחום ראשי.

דוגמה: יש תחום ראשי $R = \mathbb{Z}[x]$ -

יהי I האידיאל הנורמלי $2, x - 1$ (סגור בהחבורה

$$\mathbb{Z}[x] \xrightarrow[\substack{x \rightarrow 0 \\ a \mapsto a \pmod{2}}]{\varphi} \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$$

$\mathbb{Z}[x] \rightarrow \mathbb{Z}/2\mathbb{Z}$ $\varphi_2 \circ \varphi_1$ הרכבה של שני הומומורפיזמים φ_1, φ_2 (הומומורפיזמים

$I = \ker(\varphi_2 \circ \varphi_1)$ האידיאל המנייאל של $\mathbb{Z}[x]$ ואל x .

I נורמלי $2, x - 1$ אם x אינו נורמלי 2 אינו ראשי $\mathbb{Z}[x]$ אינו

ראשי. כי אם היה $f(x) \in \mathbb{Z}[x]$ יק $I = R f(x)$

אז יש $g(x) \in R$ יק $2 = g(x)f(x)$ $f(x) \in \mathbb{Z}$ $g(x) \in \mathbb{Z}$

סקר. נניח $f(x) = c \in \mathbb{Z}$ $2 = c \cdot h(x)$ $\Leftarrow$

$$R f(x) = R \neq I \Leftarrow c = \pm 1 \Leftarrow h(x) = \frac{x}{c}$$

צדקה: תחום אוקלידי R הוא תחום ראשי.

הוכחה: יהי $I \triangleleft R$ אם $I \neq 0$ אז $I = R \cdot 0$

אם $0 \neq a \in I$ אז $I \neq 0$ ונניח $I \neq 0$ ונניח

$d(a)$ מנייאל. (הוא אברהם יחיד אם קיים כזה).

לר (ה):

X התנאים הנכונים שקולים:

(i) $C \in R$ הפס

(ii) C יחיד על $\perp$

(iii) $R_C = R$ (במובן האידיאל שנוצר על ידי C הוא R)

I התנאים הנכונים שקולים עבור $a, b \in R$:

(i) a, b יחידים

(ii) $R_a = R_b$ (במובן "צורה אחת אגל אידיאל")

הוכחה:

$(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$ אם a, b יחידים אז $C = 1$ והפס רק

$R_a = R_{eb} = R_b$ וכן $a = eb = e$

(ii) $\Rightarrow$ $e \neq 1$ אז $R_e \neq R$ וכן $R_e \neq R_{de} = R_1 = R$

$(i) \Leftrightarrow (ii)$ אם $R_a = R_b$ אז קיימים $c_1, c_2 \in R$ כך $a = bc_1$

$$\begin{cases} ac_1 = b \\ bc_2 = a \end{cases}$$

$\Rightarrow a = bc_2 = ac_1c_2 \Rightarrow a(1 - c_1c_2) = 0$

$\Rightarrow 1 - c_1c_2 = 0 \Rightarrow 1 = c_1c_2$

$c_1 \leq 1$ הפס! $ac_1 = b$ (זהו יחידים)

X נראה ל- (ה) כי יש $\heartsuit$ שיעדים על $\perp$ הם בדיוק והפס רק

$(i) \Leftrightarrow (ii)$ אם כן $R_C = R_1 = R$ וכן $C = 1$ הפס

יחידים (ע"פ (ה)) אז $C = 1$ הפס.

(ii)

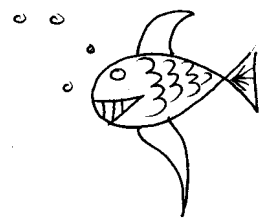
לר (ה):

(i) $d(1) \leq d(a) = d(a)$ $a \in R$ $d(1) \leq d(a)$ (ii)

(ii) $d(c) = d(1)$ עבור $C \in R$ הפס

(iii) $d(a) = d(b)$ אז a, b יחידים!!!

היום R תח קומוטטיו



תח אוקלידי - R תח קומוטטיו עם וחידה עם פוקציה

$$d: R \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\} \text{ הנקראת:}$$

$$d(a) \leq d(ab) \quad 0 \neq a, b \in R \quad \text{כאן (i)}$$

$$q, r \in R \quad a \neq 0 \quad \text{אם } a, b \in R \quad \text{כאן (ii)}$$

$$d(r) < d(a) \quad \text{או} \quad r = 0 \quad \text{!} \quad b = qa + r$$

(כאן חוקה עם לאור)

דוגמאות

(i) (אמנים) שבה F (היא תח אוקלידי עם

$$a \in F \setminus \{0\} \text{ כאן } d(a) = 0 \quad \text{החלטה "ע" } d: F \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\}$$

(1) $F[X]$ פולינומים עם d פוקציה (הדרגה

(2) $\mathbb{Z}$ עם d פוקציה (הערך המוחלט

החלטה: $a, b \in R$ נאמר ש-a מחלק את b ונסמן

$$b = ac \quad \text{אם קיים } c \in R \quad \text{כאן } b = ac$$

דוגמאות: בשדה האמנים השונים אמנם מחלקים זה את זה

החלטה: איבר $u \in R$ נקרא הפך אם הוא מחלק את 1

$$(1 = u \cdot u^{-1} \quad \text{כאן } u^{-1} \text{ הפך של } u)$$

החלטה: אם $a \mid b$! - $a \mid a$ נאמר ש-a יבועים

$$(1 = u \cdot u^{-1} \text{ הפך של } u) \quad \text{אם } a \mid b \text{ ו- } b \mid a \text{ אז } a = bu$$

$$b = bdc \quad \text{אם } a = bd \quad \text{אז } b \mid a$$

$$a = bu \quad \text{אם } d, c \text{ הפכים, אז } dc = 1 \quad \Leftarrow$$

$$(a \mid b \text{ !} \quad b = au^{-1} \text{ !} \quad b \mid a \text{ אז})$$

לדוגמה

$$d(a) = d(u) \quad \text{אם } a \in R \text{ הפך}$$

$$d(ac) = d(a) \quad \text{!} \quad a, c \in R \quad \text{אם } c \text{ הפך}$$

תזכורת: ראוי הפסד הקצתם של אידיאל I ב- R .
 חוק אלקוידו הוא ראשי, ויתר על $I \neq R$ אז
 $I = Ra$ ראשי a אינו בלתי- I (נראה)
 מינימלי. (נסתב באידיאל Ra , אז $Ra \subseteq I$ ניקח
 $b \in I$. נחלק את b ב- a שאנו: $b = qa + r$.
 אם $r = 0$ אז $b \in Ra$ אחרת $r = b - qa \in I$ (אז
 $d(r) < d(a)$ וסו סתירה מינימליות של a . $I = Ra \Leftarrow$
הנחת הנחה:

① a הפיק, אזי קיים a' כך $a'a = 1$. אז
 $d(1) \leq d(1 \cdot a) = d(a)$, מצד שני, $d(1) = d(a'a) \geq d(a)$
 $d(a) = d(1) \Leftarrow$

כזה, אם $d(a) = d(1)$ צריך להראות a הפיק.
 בנפלא $1 \cdot R = R$ אז 1 יוצר את האידיאל R .
 אכן כי האיברים המינימליים ורק הם יוצרים את R . $d(a) = d(1)$.
 אז, הנחה של a מינימלית. $a \Leftarrow Ra = R \Leftarrow$
 יוצר של 1 אז הפיק.

② (נסתב באידיאל $I = Ra$ ובאידיאל $J = Rac = Rca$ נראה
 ע- $J \subseteq I$. מצד שני, $a, ac \in I$ מאותו נורמה אז
 ac יוצר את I אז $I = Rac$ אז קיים $d \in R$
 כך $a = acd$ - $a = acd \Leftarrow cd = 1 \Leftarrow c$ הפיק. (י)

הצדקה: יהי R תחום שלמות. איבר $p \in R$ "קרא ראשוני"
 אם הוא מקיים את התנאי הבא: אם $a, b \in R$ אז $p \mid ab$
 אז $p \mid a$ או $p \mid b$.

הצדקה: יהי R תחום שלמות. איבר $q \in R$ "קרא אי-פריק"
 אם מקיים: אם $q = ab$ אז a הפיק או b הפיק.

דוגמה: אי פריק וראשוני אינם שקולים!!! (נסתב $R = \mathbb{Z}[\sqrt{-5}]$
 בראיית מה צורה $a + b\sqrt{-5}$ עבור $a, b \in \mathbb{Z}$.

(55)

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \quad \text{ב-} R \text{ מתקיים}$$

תכאן: $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ כולם אי-פריקים אבל לא ראשוניים.

למשל נסתכל על 2: היות לא הפיך, כי אין פיתוחן -

$$2a + 2b\sqrt{-5} = 1 \quad \text{הטור לא ראשוני כי } 2 \nmid 1 + \sqrt{-5}$$

$$2 \nmid 1 - \sqrt{-5} \quad \text{אם } 2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5}) \quad \text{אבל } 2 \nmid 2 \quad \text{לכן}$$

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) \quad \text{אם } 2 \text{ אי-פריק, כי אם}$$

$$2 = ac + ad\sqrt{-5} + bc\sqrt{-5} - bd5$$

$$= (ac - 5bd) + (ad + bc)\sqrt{-5}$$

$$ad = -bc \Leftrightarrow ad + bc = 0 \quad \text{וכי}$$

$$ac = 2 + 5bd \Leftrightarrow ac - 5bd = 2$$

בהכרח $a, c \neq 0$ כי $2 = -5bd$ (לא יתכן אחרת).

$$\Rightarrow \frac{ac = 2 + 5bd}{a^2c = 2a - 5b^2c} \quad \text{אם } d = 0 \text{ אז } b = 0 \text{ ואז } a \text{ ו-} c \text{ הפיכים כי}$$

אם $d = 0$ אז $b = 0$ ואז a ו- c הפיכים כי

$$2 = ac \quad \text{אז } a \text{ ו-} c \text{ הפיכים כי } b = 0$$

אם $d \neq 0$, $b \neq 0$... אז, זה אמור לצאת בסוף.

משפט: בחוג אנליטי איבר הווא ראשוני אם ואי-פריק.

דוגמה: R תחם שלמות. איבר ראשוני הוא אי-פריק.

הוכחה: יהי p ראשוני ונניח ש- $p = ab$. כפי ש- $p \mid ab$

אז $p \mid a$ או $p \mid b$. בהי"כ $p \mid a$, נומר $a = pc$

$$p = ab = pcb \quad \Leftrightarrow \quad p(1 - cb) = 0 \quad \Leftrightarrow \quad p \neq 0 \quad \text{ואין}$$

$$1 - cb = 0 \quad \Leftrightarrow \quad cb = 1 \quad \text{נומר } b$$

(11)

הפיך.

משפט: R חוג אנליטי. אזי a איבר ראשוני אם ואי-פריק.

אם $a = p_1 \dots p_m$ ו- $a = q_1 \dots q_n$ אז

ראש $\{p_i\}$ ו- $\{q_j\}$ ראשוניים אזי $m = n$ ואז a שווה

זי חזר על q_i כל $1 \leq i \leq m$.

הוכחה: באינדוקציה על $d(a)$ נוכיח את קיום הפריק.
 אם $d(a) = d(1) = 1$ אז a הפריק
 והטענה נכונה.

נניח שהוכחנו לכל האיברים $d(c) < d(a)$ אוזרים אלוהים
 פ- a . אם a ראשוני אז סיימו. אחרת a פריק,
 כלומר נותן אחרת את $a = bc$ כאשר b ו- c
 לא 1 הפריים. $d(b), d(c) < d(a)$ ולכן $d(b), d(c) < d(a)$
 לפי הנניח אלה ראשוניים. כי b או c לא ראשוניים
 לא ראשוניים $a = bc$ אחרת לא ראשוניים.
 נחזיר הוכחה את הוכחה. באינדוקציה על $d(a)$.

נניח ל- $a = p_1 \dots p_m = q_1 \dots q_n$ עבור q_i, p_i ראשוניים
 אם $d(a)$ אינו אחד אז סיימו. אחרת a לא הפריק
 ופריק. p_1 ראשוני: $(q_1 \dots q_n) \mid p_1 \Leftrightarrow q_i \mid p_1$ או
 $q_1 \dots q_n \mid p_1$. נחשיב יחס $q_i \mid p_1$ לא. אז $q_i = p_1$
 אכן ראשוני ולכן אי-פריק ולכן נהפך q הפריק!
 $p_1 \dots q_n = p_1 \dots p_m = (p_1 q) q_2 \dots q_n$ אז $j = 1$ ו-
 $\Rightarrow p_1 (p_2 \dots p_m - q q_2 \dots q_n) = 0$

אין אחרת אפשר לכתוב $p_2 \dots p_m = (q q_2) q_3 \dots q_n$
 נשים לב ל- $q q_2$ הם ראשוניים (תלוי: ראשוני הפריק = ראשוני)
 יתכן כי, $d(p_2 \dots p_m) < d(p_1 \dots p_m)$ כי $d(p_1) > d(1)$.
 ולכן אפשר להשתמש בהנחת האינדוקציה ונקבל $l-1 = m-1$ ולכן
 $l = m$ וכל השוויון סדר $p_2, \dots, p_m$ יצאים ל- $q, q_2, q_3, \dots, q_n$
 אז $q q_2, q_3, \dots, q_n$ חברים ולכן $p_2, p_3, \dots, p_m$ חברים וסיימו. (11)

המשפט: $a, b \in R$ יהא R חוג אינטיגרי. $d \in R$
 נקרא d של a ו- b יסוד $d = \gcd(a, b)$ אם מקיים: $d \mid a$
 $d \mid b$ ואם $c \mid a$ ו- $c \mid b$ אז $c \mid d$.
 נשפט: לכל $a, b \in R$ אי-אפס יהא $\gcd(a, b)$ והוא יחיד
 (עד חבורה).

59

בלחמה יהא I האידיאל המניאלי המורכב מ- a, b .
 $I = R_d$ (כאן d הוא האי.מ.ר).
 עבור $d = \gcd(a, b)$ נכון.

ראשית, $a, b \in I$ וכן קיימים c_1, c_2 כך
 $a = c_1 d$ ו- $b = c_2 d$ $\Leftarrow d|a$ ו- $d|b$.
 שנית, נניח $c|a$ ו- $c|b$ אז $a, b \in Rc$
 ולכן $I \subseteq Rc$ וכן $d \in I \subseteq Rc$ ולכן $d = fc$ עבור $f \in R$.
 מכאן $c|d$.

נניח d_1, d_2 שניהם מניאליים ב- a, b וכן
 $d_1|d_2$ ו- $d_2|d_1$, כלומר הם חסרים.

60

הצורה: יהי R תחום שלמות.

א $p \in R$ ראשוני אם $p \nmid ab \Rightarrow p \nmid a$ או $p \nmid b$
 ב $p \in R$ אי-פריק אם $p \nmid ab \Rightarrow p \nmid a$ או $p \nmid b$
 א b הפיך.

דוגמאות:

$R = \mathbb{Z}[\sqrt{-5}]$. 2 הוא אי-פריק אבל אינו ראשוני:

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

בנוסף $2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5})$ אבל 2 אינו מחלק את 3 או 1.
 מהאחרים.

טענה: בתוך אוקליד R $p \in R$ ראשוני אם ורק אם אי-פריק.
 הוכחה:

($\Leftarrow$) אם $p = ab$ אז מהשוויון $p \nmid a$ או $p \nmid b$.

בהיפוך $p \nmid a$ וכן $a = pc$ $\Rightarrow p \mid c$ $\Rightarrow p = pc$

$\Rightarrow p(1-c) = 0$ $\Rightarrow p(1-c) = 0$ $\Rightarrow 1-c = 0$ $\Rightarrow c = 1$

$\Rightarrow cb = 1$ $\Rightarrow$ b הפיך. (שימו לב שאין להשתמש בן

הפך ל- R תחום שלמות.)

($\Rightarrow$) (סביר ל- $d = \gcd(a, b)$ אז $d \mid a$, $d \mid b$ אז

$c \mid a$; $c \mid b$ מחלקים $c \mid d$. הוכחנו

שבתוך ראשי תיבות מחלק משותף מקסימלי (יהי I

האידיאל שנוצר "א" a ; b : $I = Ra + Rb$. I ראשוני,

בנוסף $d \mid a$, $d \mid b$ $\Rightarrow Ra + Rb \subset Rd$ $\Rightarrow I \subset Rd$

$a, b \in I$. נשים לב d -הוא מחלק $d = r_0 a + s_0 b$

אם $c \mid a$; $c \mid b$ אז $c \mid d$

הצורה: $a, b \in R$ יוקראו זרים אם $\gcd(a, b) = 1$ (נלכו בן

ל- $\gcd$ (קראו מאוחר יותר על זה בהמשך)

טענה: אם $c \mid ab$! $\gcd(c, a) = 1$ אז $c \mid b$.

הוכחה: אם $\gcd(c, a) = 1$ אז קיימים $r_0, s_0 \in R$ כך $r_0 c + s_0 a = 1$.

נתון $a, b \in \mathbb{Z}$, $ab = cm$, $c \mid ab$, $c \mid a$, $c \mid b$.

$$b = b \cdot 1 = b \cdot c + (-c) \cdot a$$

$$b = b \cdot c + (-c) \cdot a \quad ; \quad c \mid b \iff c \mid (-c) \cdot a \quad ; \quad c \mid b$$

כעת נניח a ונניח b . נניח $c \mid a$, $c \mid b$.

$$c \mid a \implies a = c \cdot k \quad ; \quad c \mid b \implies b = c \cdot l$$

$$ab = c^2 \cdot kl = cm \implies c \mid m$$

$$p = dc \quad ; \quad d = \gcd(p, a) \quad ; \quad d \mid p \quad ; \quad d \mid a$$

$$p = dc \quad ; \quad d = \gcd(p, a) \quad ; \quad d \mid p \quad ; \quad d \mid a$$

$$p = dc \quad ; \quad d = \gcd(p, a) \quad ; \quad d \mid p \quad ; \quad d \mid a$$

⊙

האלגוריתם של אוקלידס

$$a, b \in \mathbb{Z}$$

יהי R חוג אוקלידי .

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

$$b = q_0 a + r_1$$

$$d(r_1) < d(a)$$

$$a = q_1 r_1 + r_2$$

$$d(r_2) < d(r_1)$$

$$r_1 = q_2 r_2 + r_3$$

$$d(r_3) < d(r_2)$$

$$r_2 = q_3 r_3 + r_4$$

$$d(r_4) < d(r_3)$$

$$r_{m-2} = q_{m-1} r_{m-1} + r_m$$

$$d(r_m) < d(r_{m-1})$$

$$r_{m-1} = q_m r_m + 0$$

התהליך מתחיל ב d , d הוא המחלק המשותף הגדול ביותר של a ו b .

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

הוכחה: נניח $a = r_m \cdot a'$, $b = r_m \cdot b'$.

$$r_m \mid a \quad ; \quad r_m \mid b \quad ; \quad r_m \mid r_{m-1} \quad ; \quad r_m \mid r_{m-2} \quad ; \quad \dots \quad ; \quad r_m \mid r_1$$

$$r_m \mid a \quad ; \quad r_m \mid b \quad ; \quad r_m \mid r_{m-1} \quad ; \quad r_m \mid r_{m-2} \quad ; \quad \dots \quad ; \quad r_m \mid r_1$$

$$r_m \mid a \quad ; \quad r_m \mid b \quad ; \quad r_m \mid r_{m-1} \quad ; \quad r_m \mid r_{m-2} \quad ; \quad \dots \quad ; \quad r_m \mid r_1$$

$$r_m \mid a \quad ; \quad r_m \mid b \quad ; \quad r_m \mid r_{m-1} \quad ; \quad r_m \mid r_{m-2} \quad ; \quad \dots \quad ; \quad r_m \mid r_1$$

$$r_m \mid a \quad ; \quad r_m \mid b \quad ; \quad r_m \mid r_{m-1} \quad ; \quad r_m \mid r_{m-2} \quad ; \quad \dots \quad ; \quad r_m \mid r_1$$

$$r_m \mid a \quad ; \quad r_m \mid b \quad ; \quad r_m \mid r_{m-1} \quad ; \quad r_m \mid r_{m-2} \quad ; \quad \dots \quad ; \quad r_m \mid r_1$$

⊙

(58)

$$\gcd(759, 323) = ?$$

מחלק

$$759 = 2 \cdot 323 + 113$$

$$323 = 2 \cdot 113 + 97$$

$$113 = 1 \cdot 97 + 16$$

$$97 = 6 \cdot 16 + 1$$

$$16 = 16 \cdot 1$$

$$\Rightarrow \gcd(759, 323) = 1$$

שני איברים מסוגים מסוימים (איברים) אחד
התחילי והאחר ה'אחר'.

$$89 = 55 + 34$$

$$55 = 34 + 21$$

$$34 = 21 + 13$$

$$21 = 13 + 8$$

$$13 = 8 + 5$$

$$8 = 5 + 3$$

$$5 = 3 + 2$$

$$3 = 2 + 1$$

$$2 = 1 + 1$$

$$1 = 1$$

$$\left. \begin{array}{l} 90 = 55 + 35 \\ 55 = 35 + 20 \\ 35 = 20 + 15 \\ 20 = 15 + 5 \\ 15 = 3 \cdot 5 \end{array} \right\} \text{ה'אחר'}$$

ה'אחר' הוא R יוקרא חוק פשוט אם $I = R$ או $I = \{0\}$.

דוגמה F שדה. אם $M_n(F)$ חוק פשוט.
נשים לב שיש פה אידיאלים 'מחזיקים' - $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix} \right)$, $\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix} \right)$.
אם אין אידיאל זר צדדיים טריוויאליים.

טענה: אם R חוק קומוטטיב אם וחידה שהוא פשוט אז R שדה.

הנחת: זוג סתמי של $a \in R, a' \in R$ כ"כ $a \neq 0$ ו- $a' \in R$ כך ש-
 $a' \cdot a = a \cdot a' = 1$

נסתכל על האידיאל Ra . זה אידיאל זוגי ב- R וישנו מאפיין
 כי $a = 1 \cdot a \in Ra$. לכן $Ra = R$ זהו המסקנה.

הפניס ק"מ $r \in R$ כך ש- $ra = 1$. לכן a הפניס ק"מ. (11)

הערה: אם R חוג קומוטטי עם יחידה 1 ו- $M \triangleleft R$ אידיאל

מקסימלי (3) אז $M \neq R$ אם $I \triangleleft R$! $M \subseteq I \subseteq R$

אם $I = R$ או $I = M$ (אז R/M הוא שדה).

הוכחה: לפי משפט ההתאמה יש התאמה חד-חד ערכית בין האידיאלים

של R/M לאידיאלים של R שחוסים את M . (למעשה M).

של R/M יש רק אחד אידיאל ה-0 וזה החוג, כלומר זהו

שדה ולכן R/M שדה. (12)

הערה: למעשה ההסקנה היא אחרת: כלומר R/M שדה אם ורק אם M מקסימלי.

הצדקה: נניח ש- R הוא קומוטטי עם יחידה. אידיאל $I \triangleleft R$

וקרא אידיאל ראשוני אם מתקיים התנאי הבא:

$$ab \in I \Leftrightarrow a \in I \text{ או } b \in I$$

דוגמה: $R = \mathbb{Z}$, $I = 5\mathbb{Z}$. אם $ab \in 5\mathbb{Z}$ אז

$$ab \in 5\mathbb{Z} \Leftrightarrow 5 \mid ab \Leftrightarrow 5 \mid a \text{ או } 5 \mid b \Leftrightarrow a \in 5\mathbb{Z} \text{ או } b \in 5\mathbb{Z}$$

אם יש קשר בין אידיאל ראשוני לאידיאל ראשוני!

הערה: R חוג קומוטטי עם יחידה. אידיאל $I \triangleleft R$ הוא ראשוני

אם ורק אם R/I תחום סגור.

הוכחה: R/I קומוטטי עם יחידה.

נניח I ראשוני ויהיו $x, y \in R/I$ כך ש- $xy = 0_{R/I}$ כלומר

$$xy = (a+I)(b+I) = ab + I = I! \quad y = b+I, \quad x = a+I$$

$$\Leftrightarrow ab \in I \text{ או } a \in I \text{ או } b \in I$$

⑤9 $\text{ann } \mathbb{R}/I$ $\text{pr } x = a + I = I \iff a \in I$ $\text{min } \mathbb{Q}$

$ab \in I$ - כל מוצא מוצא $\mathbb{R}/I$ אז, יש 3 נק
 פס $I = ab + I = (a+I)(b+I) \in \mathbb{R}/I$ שכן
 $a+I = I$ וכן $b+I = I$ וכן $a+I = I$

(ii) $\vdash \neg \exists x (x \neq x)$

תשובה: כיצד נקראת התורה? והיא נקראת תורה.

ה'תשנ"ה: אם I 'סרופ' SK R/I זה. אתה זה

(4) $(\alpha, \beta) \in \mathcal{R} \iff \alpha \in \beta$

הצטלה לא שון ערפס. אה קורה ג. $\neq$? איהם האוצרים

האם $n \in \mathbb{Z}$ יכול להיות ראשוני? $\mathbb{Z}$ הוא שדה?

የቺድ ስኬት ስለሚቀርብ ምሳሌ ማሳሰቢያ

חבור קראשני. ליקי הם. לם ב. זה ציור א אלו דם...

שאלה: R הוא חץ, $I \triangleleft R$. I היא התכנסות המכונים לקוים:

Exoplan I (c)

ନିମ୍ନ R/I ②

→ IN Q. 20th R/I (C)

51200 I (a)

הולדה:

(c) $\Leftrightarrow$ (b) - רמז ה'כתנו

(c) $\Leftrightarrow (3) -$ רמז הלוחות

2) $\Rightarrow$ (c) - 2172

(2) $\leq$ (1) $\Rightarrow$ אכן I אידיאל (ואשנוי) חזק פהלחה (דא)

מקטעים. מנהל, גליל, סומך ק"מ $\mathbb{I} \neq \mathbb{J} \neq \mathbb{R}$ ביחידה.

10) a. $\mathbb{Q} \subset \mathbb{C}$. $J = \mathbb{R}d$; $I = \mathbb{R}a$; 10 , 10 10

אי פריק, או מאלן לל, וצב איזאס (אשוי) ווא 12-פריק.

$$(C_1 + I)(C_2 + I) = a + I \quad \text{with } C_1, C_2 \in R_a \quad a = C_1 C_2 \quad \text{with}$$
$$C_1 \mid a \text{ پر } a \mid C_2 \Leftarrow C_1 \in I \text{ و } C_2 \in I \text{ و } C_1 \in I \Leftarrow$$

מכפלה חצי-ישירה

משפחה ישירה - A, N תבורות ! $G = N \times A$
 כל יוצרים נקרא משפחה ישירה חיצונית.
 אם יוצרים מתחילים מתבורות $A, N \triangleleft G$ ואם $G = NA$
 ! $\{e\} = A \cap N$ אז $G \cong N \times A$ כל (נקרא משפחה
 ישירה פנימית).

כשמוכחים את כל מראים ל- $[N, A] = \{e\}$ כל מאוד פשוט:
 אם $n \in N$! $a \in A$ אז

$$[a, n] = \frac{\overbrace{a^{-1} n^{-1} a}^{\in A} \underbrace{n}_{\in N}}{\underbrace{\phantom{a^{-1} n^{-1} a}}_N} \in N \cap A = \{e\}$$

! $an = na \quad \Leftarrow$

משפחה חצי-ישירה: G תבורה, $A, N \leq G$ תבורות חלקיות
 ! $N \triangleleft G$ רק ל- $AN = G$! $A \cap N = \{e\}$

ל זה כמעט כמו משפחה ישירה אבל שאת התבורות לא נורמלית.
 כן אי אפשר לומר שהן מתחלפות כי הקומוטטור לא ב- A .
 אלא רק ב- N .

במקרה זה נומר ל- G משפחה חצי ישירה של N !- A
 אם $a \in A$! $n \in N$ $a^{-1} n^{-1} a n$ נמצא ב- N ואין
 צורך ב- A .

אם מתקיים שלב $a \in A$ ואם $n \in N$ $an a^{-1} \in N$, נומר
 a פועל על N כאוטומורפיזם. דהיינו, a משה אוטומורפיזם
 פנימי של G (זו הצמד) !- N , כל תבורה (נורמלית,
 אינווריאנטית תחת אוטומורפיזם זה).

תצפית 8 יהיה עתקה $A \rightarrow \text{Aut}(N)$ נאשר $\varphi_a(n) = ana^{-1}$
 היא הומומורפיזם $A \rightarrow \text{Aut}(N)$ $a \mapsto \varphi_a$

הולחה: בחר ל- φ_a אוטומורפיזם של N . לכן רבדוק
 שהעתקה $a \mapsto \varphi_a$ היא הומומורפיזם. לא, אם $a, b \in A$

צריך להראות ל - $\varphi_{ab} = \varphi_a \circ \varphi_b$ ואכן, לכל n מתקיים

$$\begin{aligned}\varphi_{ab}(n) &= (ab)n(ab)^{-1} = (ab)n(b^{-1}a^{-1}) = \\ &= a(bnb^{-1})a^{-1} = a\varphi_b(n)a^{-1} = \varphi_a(\varphi_b(n)) = \\ &= (\varphi_a \circ \varphi_b)(n)\end{aligned}$$

(11)

נסמן לשם יופעים A - N ! ואם ההומומורפיזם הלה
אכן ניתן לשלול את G המבנה של החבורה.

הצעה: תהי N - A ! חבורה G של N יוצרת
הומומורפיזם $\Phi: A \rightarrow \text{Aut}(N)$ (זכור $a \in A$)

$$\text{(נסמן)} \quad \Phi(a) = \varphi_a \quad \text{אוטומורפיזם של } (A)$$

נבנה חבורה G באופן הבא: בקבוצה $G = N \times A$
פעולה החבורה מוגדרת ע"י

$$(n_1, a_1) \cdot (n_2, a_2) = (n_1 \varphi_{a_1}(n_2), a_1 a_2)$$

העסקה אוטומורפיה: יש לנו חבורה G מסדר $24 = 3 \cdot 4$.

יש לה חבורה 4 -סיוט נורמלית. יש לה חבורה 3 -סיוט
וראיה יש אחת או 4 . אם יש רק אחת אז היא נורמלית.

ואז ה- 4 סיוט נורמלית $\mathbb{Z}_4$ או 3 -סיוט נורמלית $\mathbb{Z}_3$

אז G היא המרחבה הישירה שלהן (היא ציקלית מסדר 12 או

אם לא קרה אם יש 4 חבורה 3 -סיוט?

יש חבורה 4 סיוט נורמלית P וחבורה 3 סיוט לא

צוקא נורמלית Q . מתקיים $P \cap Q = \{e\}$! המרחבה שלהן היא

הם משים של P נורמלית. יש הומומורפיזם $\Phi: Q \rightarrow \text{Aut}(P)$

אנחנו רוצים להשתמש בהומומורפיזם הלה קבוצה A מבנה
החבורה.

המשק והצעה: לחבורה G נקרא המרחבה (החצי ישירה של A

$$G = N \rtimes A \quad N - \text{ע"י } \Phi \text{ ותסומן}$$

$\Phi \leftarrow$ אופרטורים משמאלים (שבהם אנו Φ)

6)

ע"כ:

- א) G תכונה
- ב) $\bar{N} = \{ \bar{n} = (n, e_A) : n \in N \}$ זו תכונה חלקה (נחמדי) ל G איזומורפי N -f
- ג) $\bar{A} = \{ \bar{a} = (e_N, a) : a \in A \}$ תכונה חלקה ל G איזומורפי A -f
- 3) $\bar{a} \bar{n} \bar{a}^{-1} = \overline{\varphi_a(n)}$

הערה: אם $\Phi: A \rightarrow \text{Aut}(N)$ ההומומורפיזם האדיטיבי, אז אם $N \times_{\Phi} A = N \times A$ אז $\varphi_a = \text{id}$ $a \in A$
 אם צמד תצט...
 הוכחה:

- א) ציב, הוכיח שתקיימו תכונה ותכונה
- הסתיוור תכונה כי A ו- N תכונות זכך $n, \varphi_a(n_2) \in N$
- ! - $a_1, a_2 \in A$
- איבר היחידה הוא (e_N, e_A)
- $(e_N, e_A)(n, a) = (e_N \cdot \varphi_{e_A}(n), e_A \cdot a) =$
 $= (e_N \cdot \text{id}(n), a) = (e_N \cdot n, a) = (n, a)$
 ובאופן אופן מהצד השני
- אסוציאטיביות

$$\begin{aligned} (n_1, a_1) ((n_2, a_2)(n_3, a_3)) &\stackrel{?}{=} ((n_1, a_1)(n_2, a_2))(n_3, a_3) \\ (n_1, a_1) (n_2 \varphi_{a_2}(n_3), a_2 a_3) &\stackrel{?}{=} (n_1 \varphi_{a_1}(n_2), a_1 a_2) (n_3, a_3) \\ (n_1 \varphi_{a_1}(n_2 \varphi_{a_2}(n_3)), a_1 a_2 a_3) &\stackrel{?}{=} (n_1 \varphi_{a_1}(n_2) \varphi_{a_1 a_2}(n_3), a_1 a_2 a_3) \\ (n_1 \varphi_{a_1}(n_2) \varphi_{a_1}(\varphi_{a_2}(n_3)), a_1 a_2 a_3) &\stackrel{?}{=} (n_1 \varphi_{a_1}(n_2) \varphi_{a_1}(\varphi_{a_2}(n_3)), a_1 a_2 a_3) \checkmark \end{aligned}$$

$\downarrow \varphi_{a_1}$ הומומורפיזם $\downarrow \Phi$ הומומורפיזם

- איבר הפכי: בהנחה $(n, a) \in G$ יק'ן

$$(n, a)^{-1} = (\varphi_{a^{-1}}(n^{-1}), a^{-1})$$

$$\begin{aligned} (\varphi_{a^{-1}}(n^{-1}), a^{-1})(n, a) &= (\varphi_{a^{-1}}(n^{-1}) \cdot \varphi_{a^{-1}}(n), a^{-1} a) = \text{אז} \\ &= (\varphi_{a^{-1}}(n^{-1} n), e_A) = (\varphi_{a^{-1}}(e_N), e_A) = \\ &= (e_N, e_A) \end{aligned}$$

ובצורה דומה מהצד השני

② נתון $\psi: N \rightarrow G$ " $\psi(n) = \bar{n} = (n, e_A)$ זה איזומורפיזם

$$\psi(n_1 n_2) = \overline{n_1 n_2} = (n_1 n_2, e_A) = (n_1, e_A)(n_2, e_A) = \psi(n_1) \psi(n_2)$$

← נראה

$\bar{N} \trianglelefteq$ תתבורה חזקה

(ואם שיהא נורמלית)

$$\begin{aligned} (n_1, a)(n, e_A)(n_1, a)^{-1} &= (n_1, a)(n, e_A)(\psi_{a^{-1}}(n_1^{-1}), a^{-1}) = \\ &= (*, a e_A a^{-1}) = (*, e_A) \in \bar{N} \end{aligned}$$

③ $\bar{A}$ תתבורה חזקה

$$\begin{aligned} (e_N, a_1)(e_N, a_2) &= (e_N \psi_{a_1}(e_N), a_1 a_2) = \\ &= (e_N e_N, a_1 a_2) = (e_N, a_1 a_2) \in \bar{A} \end{aligned}$$

$$(e, a)^{-1} = (\psi_{a^{-1}}(e^{-1}), a^{-1}) = (\psi_{a^{-1}}(e), a^{-1}) = (e, a^{-1}) \in \bar{A}$$

וכן $\bar{A}$ תתבורה חזקה והיא איזומורפית ל- A " $a \mapsto \bar{a} = (e_N, a)$ זהה

$$a_1 a_2 \mapsto \bar{a}_1 \bar{a}_2 = (e_N, a_1 a_2) = (e_N, a_1)(e_N, a_2) = \bar{a}_1 \bar{a}_2$$

$$\bar{N} \cap \bar{A} = \{e_G\} = \{(e_N, e_A)\} \quad \text{③ (שייכים למקרה)}$$

$$(n, a) = (n, e_A)(e_N, a) \Rightarrow G = \bar{N} \cdot \bar{A}$$

$$\text{כל } \bar{n} = (n, e_A) \quad \bar{a} = (e_N, a) \quad \text{ללא}$$

$$\begin{aligned} \bar{a} n \bar{a}^{-1} &= (e_N, a)(n, e_A)(e_N, a)^{-1} = (e_N, a)(n, e_A)(e_N, a^{-1}) = \\ &= (e_N, a)(n \psi_{e_A}(e_N), a^{-1}) = (e_N, a)(n, a^{-1}) = \\ &= (e_N \psi_a(n), e_A) = (\psi_a(n), e_A) = \overline{\psi_a(n)} \end{aligned}$$

☺

נחשון (להלן) $\bar{n}$ ו- $\bar{a}$ הם n ו- a בהתאמה
ניתן לראות איברים מהבורה n ו- a (הם) אלוהם

$$n_1 a_1 n_2 a_2 = n_1 a_1 n_2 a_1^{-1} a_1 a_2 = \underbrace{n_1 \psi_{a_1}(n_2)}_{N''} \underbrace{a_1 a_2}_{A''}$$

נסתב על התבורה הדידוקטור $D_{2m} = C_m \rtimes C_2$
 $C_m \ni n \mapsto -n$ " C_m פועל על $C_2 = \langle a \rangle$
 $a^2 = \text{id}$

62

משפט: תהא G תבורה. נניח $N, A \leq G$ תבורות חתוכות.
 רק ל- $N \triangleleft G$, $NA = G$, $N \cap A = \{e\}$. $N \cap A = \{e\}$ פ"ק G
 $a \in A$ מתקיים אוטומופיזם על N ו' $\varphi_a(n) = ana^{-1}$ ו' φ_a ו' $\varphi_a(n) = ana^{-1}$ ו' φ_a
 מקבלים $\Phi: A \rightarrow \text{Aut}(N)$ $a \mapsto \varphi_a$ כזו.
 $G \cong N \rtimes_{\Phi} A$ ו' $\Psi: N \rtimes_{\Phi} A \rightarrow G$ $\Psi(n, a) = na$ ו' Ψ איזומופיזם.
 ונניח ש- Ψ איזומופיזם.

דמיון Ψ $NA = G$ הלאה תראה.

דוגמה: תהא G תבורה מסדר 24. (סמן ב- N את התבורה 4-סיומית
 כזו $N \triangleleft G$. (סמן ב- A איזו תבורה 3-סיומית.
 מספר ה- 3-סיומית הוא 4 או 1 - נמקד לה $A \triangleleft G$ -!
 $G = N \times A = C_4 \times C_3 \cong C_{12}$

או 7 ומתקנה לה $G \cong C_4 \rtimes_{\Phi} C_3$, נאשר $\Phi: C_3 \rightarrow \text{Aut}(C_4)$
 הומומורפיזם. אז מהן האפשרויות?

$$C_3 = \{1, a, a^2\} \quad a^3 = 1, \quad a^2 = a^{-1}$$

$$C_4 = \{0, 1, \dots, 6\} \quad (i+j) \bmod 4$$

אם $\varphi \in \text{Aut}(C_4)$ הוא נקבע לחלוטין ע"י $\varphi(1)$. $\varphi(1)$ יתכן
 להיות 1 או 3 (כי כולם יוצרים את C_4)
 למשל $\text{Aut}(C_4) \cong \mathbb{F}_4^*$, כי הרי אם $i \mapsto \varphi(i)$ $j \mapsto \varphi(j)$

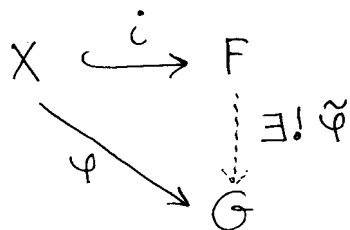
אז $j \mapsto \varphi(j) = \varphi(i)^j$. אז לא תבורה אבלור מסדר 6 ו' φ
 ציקלית. ערשנו נתפס את Φ הומומורפיזמים N - C_3 ו' Φ
 תבורה ציקלית מסדר 6. יש את הסיוויאלים אבלור מסדר
 6 או מופלג ישנה אז נניח שישנו ע"א סיוויאלים. אז a
 צריך לעבור לאיבר מסדר 3. יש שני איברים כאלה - 2 ו' 4.

אז יש שני הומומורפיזמים אלגבריים שונים, אבל הם לא נוסדו
 בסיוול התבורה שיוצאון הן איזומופיזם. נניח $\Phi_1, \Phi_2: A \rightarrow \text{Aut}(N)$

"יתכן ש- $\Phi_1 \neq \Phi_2$ אבל $N \rtimes_{\Phi_1} A \cong N \rtimes_{\Phi_2} A$ דמיון לה
 קורה אם $\Phi_2 = \Phi_1 \circ \alpha$ ו' $\alpha \in \text{Aut}(A)$ (ההנחה רלוונטית) ו' α
 מציוק את שלקורה במקרה שלנו, עבור α שמעביר את a ל- a^{-1} .

תבונה חופשית

הגדרה: תהא X קבוצה שלשה. תמונה F תיקרא חופשית על X אם יש פונקציה $i: X \rightarrow F$ תהא רק שלם תמונה G עם התקנה קבוצתית $\varphi: X \rightarrow G$ קיים הומומורפיזם וחי $\tilde{\varphi}: F \rightarrow G$ המקיים $\tilde{\varphi} \circ i = \varphi$.



זה ראוי משו מאוזן צומח לעמי תבונה חופשית - יש בהגדרה היה כתב "עם תמונה G חופשית ..."

זה נקרא הגדרה קטגורית. מתחילים על אסל עצמים ואומפומים ביניהם. ואז אומפיקט. תפשי הוא משותף עם האומפומים. אנחנו חאים איפה הוא יושב ביחס לעתירים.

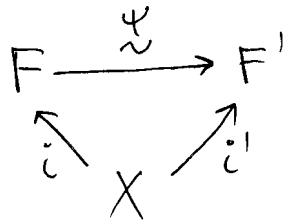
במהלך ראשון העל לא נהיה שקיימת תמונה כלל.

צומח תהא X קבוצה שלשה. נתבונן באוסל S המולים המצומחם X - להופכיהם (ההופכיים הם קבוצה X^{-1} שלה X ויש איזומורפיזם של קבוצות $X^{-1} \times X \rightarrow X \times X^{-1}$). מזה מצומחם פיוסו של חופש במזה לא $x^{-1}x$ ולא xx^{-1} על $x \in X$. אם המולה הריקה היא מצומחם (הצור של בין מולים מצומחם $\emptyset$ שרשר וראתו מכך צמצום. הסענה בים שלם תמונה. עמשה באופן מפתיע לה בעלם עמ טריוויאל עתירות את זה. הם פי פשוט אהם יש מזה עמ האסוציאטיב'ה. יש S מיני דרכים עתירות את זה. הם אופן זה מצומחן אהל עמ קשה עתירות עמ שלם עומה.

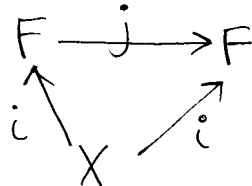
זו תמונה חופשית כי אם יש לנו $\varphi: X \rightarrow G$ אז נגדיר

$$\tilde{\varphi}(x_1 x_2^{-1} x_3 x_2 x_3) = \varphi(x_1) \varphi(x_2)^{-1} \varphi(x_3) \varphi(x_2) \varphi(x_3)$$

לענין: אם F - תמונה חופשית על X (זו העתקה)
 $\psi: F \rightarrow F'$ איזומופיזם ($i': X \rightarrow F'$, $i: X \rightarrow F$)
 כך ש- $i' = \psi \circ i$



הנחה: אומנפשיה על F יש $\tilde{i}: F \rightarrow F'$ כך ש- $\psi \circ i = \tilde{i}$
 באופן דומה יש $\tilde{i}: F' \rightarrow F$ כך ש- $\psi \circ i' = \tilde{i}$
 נתון הומומורפיזם $\psi \circ \psi: F \rightarrow F$ אז $x \in X$
 $(\psi \circ \psi)(i(x)) = \psi(i'(x)) = i(x)$
 לכן $\psi \circ \psi$ "פגור" את "העל" ההמשכה".



$j = \psi \circ \psi$ אז $j = id|_F$ היחידה
 באופן סימטרי $\psi \circ \psi = id|_F$ $\Leftarrow \psi = \psi^{-1}$!
 זה האיזומורפיזם שחישלנו.

(11)

אסתר: אם F תמונה חופשית על X אז X יוצרת את F
 שפירט ב התמונה החופשית על X איזומורפית וברורה
 שראינו F נוצרת על ידי X .

לענין: אם G תמונה , $A \subseteq G$ תת קבוצה . תהא X קבוצה
 אם התאמה תת' ופ' $j: X \rightarrow A$ אז G תופשת על A
 אלא $(i) \exists$ אלה מצומצמים. X על $w(x_1, x_2, \dots) \neq e$ מתקיים
 $w(j(x_1), j(x_2), \dots) \neq e_G$ וגם
 (ii) A יוצרת את G

הסבר: הענינה בעצם אומר שאפשר לבדוק אם תמונה היא חופשית
 מהפנימי - לא צריך להתעסק עם הדיאלים ואשלם...

64

באותה תהא F_X החבורה התופשה על X (היא
אוסף החזים המצומצמים על X). קיים הומומורפיזם $\tilde{j}: F_X \rightarrow G$
עם (i) $\tilde{j}$ חד-חד-חד (ii) $\text{Ker } \tilde{j} = \{e\}$ (iii) $\tilde{j}$ על
 $\tilde{j}$ איזומורפיזם שלוקח את X ל- A על
תמונה תופשה על X שיהא G היא גם תופשה על A .

65

המשפט (חמש) אכן מצטרפו הוכחה של קיום התנאים לא גמור
פשוטה כל כך...

דוגמה: $G = \langle A \rangle$; $A = \left\{ \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\}$
• תהיה: להוכיח ש- G תופשה על A ש- A
גמור (ii) דבר יש לנו מההצורה. צריך להוכיח ש- A
גמור (i).

דוגמה: $H = \langle B \rangle$; $B = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}$
• תהיה: להוכיח ש- H תופשה על B !

משפט (1): תמונה חלקית של תמונה תופשה היא תופשה
(אם היא בעצם צריכה יותר יוצרים מאשר התמונה המקורית)
(2) אם F תמונה תופשה על d יוצרים H - תמונה חלקית
אוינקס n אז H תמונה תופשה על $1+n(d-1)$ יוצרים.
(3) אם $F = F_d$ החבורה התופשה על d יוצרים $H = F' = [F, F]$
אז H תופשה על מספר מן אניה של יוצרים.

אנחנו יוצרים ש- H_n נוצרה ע"י איברים. אם ממשט קנה
א תמונה (יותר) לשיכון ב- H_n עבור H מספק הדגם. אם
לא א התמונה נוצרה ע"י שני איברים...

דוגמה לתמונה תופשה - אמר שניה תופשה - $\mathbb{Z} \times \mathbb{Z}$
 $\mathbb{Z}^2 = \langle e_1, e_2 \rangle$ תופשה אמר. אם או אפשר להמשיך
הומומורפיזם לזרוע תמונה לא אמר אמר נזרק $(1,2) \in S_2$

e_1, e_2 איז א פארגעבן פאר אונזערע $e_2 \mapsto (1, 2, \dots, 6) \in S_6$!
אונזערע פארשטייט דאס דאס איז א פארגעבן פאר אונזערע!

מסקנה מהמבחן: אם H תמונה חלקית אז H תמונה חופשית

$$H \cong \mathbb{Z} \quad \text{и} \quad H = \{e\} \quad \text{и} \quad K$$

תורת: אם $\varphi = H$ סימני. אחרת, H ~~היא~~ קטורה
 בלתי $\vdash$ X . אם φ היא X יש יותר משני איברים (היא לא
 אפילו כי $x_1 \neq x_2$ $\vdash$ X אינה אחת. אבל חתום
 תופש φ אינה אחת היא ציקלים $\neq$.

הערה על תאריך חתום:

$$F_2 = F_{\{a,b\}} = \{ \omega(a,b) : a,b \in \bigcup_{n \in \mathbb{N}} \mathbb{N} \}$$

$$H = \langle a^2, b^2, ab \rangle$$

$[F_2 : H] = 2$, "אין H יש 2 אינדקסים" כי H איז נורמל

המחיר של הרכב הוא 100,000 ש"ח.

$$H \cong \{a^2, b^2, ab, a^{-2}, b^{-2}, b^{-1}a^{-1}, ba^{-1}, b^{-1}a, \dots\}$$

$$\{ab^{-1}, a^{-1}b, ba, a^{-1}b^{-1}\} = \begin{matrix} \text{הקלחתן זהותם} \\ a, b, a^{-1}, b^{-1} \end{matrix} \in \mathbb{Z}_2$$

6. אולי מאריך זמן נצטרך - H.

$\Rightarrow$ אולם באופן זה נמצא ב- H.
 אולם (המילים באופן זה) אנו מוצאים (ונומליה) $\mathbb{Z}$ איננו

2 ב- F₂ מנפלה על אחים S אחיו יהא נאיס נחלים פצע

[illegible]

אני יודעת שמי איתנו ואנחנו נשאלים אם אנחנו זכאים

אם נצמים עם מילה בלתי (אפילו איטליה) כל אמתו מוסיפים

אז אורק תחילה פתח"ם ו' צא שו"י ואז את רב הוצאות זה עדיין

היא. כלומר יש גם חבורה נורמלית.

נתחיל ב- $G = F/N$. ה- G הוא G -מודול. אז $\exists g \in F$ כזה

מתקיים $g^2 \in N$ $\Leftrightarrow G/N \trianglelefteq$ (כ"ס חבורה G לבד

אם $y \in G$ אז $y^2 \in F$ כי $y^2 = (xyx^{-1})^2$.

$\bar{b} = bN$; $\bar{a} = aN$ - ה"ח 2 כ"ס'ים

(65)

$\Leftarrow ab \in N$ $\Rightarrow$ $a, b \in N$ $\Leftarrow \bar{a} = \bar{b}^{-1} \Leftarrow \bar{a}\bar{b} = e$
 $\Leftarrow \bar{a} = \bar{b}^{-1} \Leftarrow \bar{a}\bar{b} = e$
 $[F:N] \leq 2 \Leftarrow |G| \leq 2$ $\Rightarrow$ $[F:N] = 2$ $\Rightarrow$ $|G| = 2$

$$H = F \quad \text{IK} \quad H = N \quad \trianglelefteq \quad \underbrace{N \subseteq H \subseteq F}_{\trianglelefteq^2} \quad \text{IK} \quad \text{IK} \quad \text{IK}$$

$$H = N \quad \trianglelefteq \quad H \subseteq N \quad \trianglelefteq^2 \quad H = \langle a^2, b^2, ab \rangle \quad \text{f.w.K}$$

נותר אדמונה ש-H תופש שיה ϕ והסוס η לה.

צרכים, מרחוקים, לא $w \neq \varepsilon$ מרחק מרחק מרחק 3 אור, x_1, x_2, x_3 $j: (a^2)(b^2)(ab)$

$w(a^2, b^2, ab) = w(j(x_1), j(x_2), j(x_3))$

אזה תרחיל

16.1.08
אבני

כפסגה הקבוצה הסתגלה X ואתה שחבורה
 F עם העתקה חזרה $i: X \rightarrow F$ נקראת חפשיה על X
 אם על חבורה G ולא העתקה קבוצתה $\varphi: X \rightarrow G$ יש
 הומומורפיזם יחיד $\tilde{\varphi}: F \rightarrow G$ רק ש- $\tilde{\varphi} \circ i = \varphi$.
 באופן זה העתקה קבוצתה $\varphi: X \rightarrow G$ ניתנת להמשכה
 להומומורפיזם יחיד (כאשר חושבים על X כחבורה של F).

ראינו את הטענה שאם $A \subseteq F$ אזי F חופשיה על A
 אמרנו מתקיימים התנאים הבאים:
 $F = \langle A \rangle$ (i)

(ii) לכל מילה מוצמנת $w(x_1, \dots, x_n) \neq e$ ($n \leq |A|$)
 $a_1, \dots, a_n \in A$ שונים $w(a_1, \dots, a_n) \neq e$.

הצגות של חבורות

יוצרים ויחסים

$C_3 = \langle x \mid x^3 = e \rangle$ כאן ברור ליצרי אחי החבורה אתוק ההצגה.
 ערשיו (סתם) של משווא קצת יותר מסובק:

$$G = \langle x, y \mid x^2 = y^3 = x^{-1}y^{-1}xy = e \rangle$$

מה אנחנו יכולים להסיק מההצגה?

- G אינפניטית כי היא נוצרת ע"י שני יוצרים שלמתחלפים
- היא זוג היותר מסובק כי למשל $\{x^i y^j \mid 0 \leq i \leq 1, 0 \leq j \leq 2\}$
- אפשר להגיד ישירות ש- $o(x) = 2$; $o(y) = 3$ כי
 $x = e$ או $y^2 = e$...

הצגה: תבא X קבוצה ותבא F_X החבורה החופשיה על X .
 תבא R חבורה של F_X (סמן ב- N את החבורה
 התת-קבוצה הנורמלית המיוחסת של F_X המכונה R .

(בומר N היא תיבת $\mathcal{C}$ החבורות החלקיות הנורמליות של F_X
המחלק את R . נבדל: N היא החבורה החלקית של F_X
הנוצרת ע"י $\mathcal{C}$ צמודי R).

מסקנה: נאמר ש- $\langle X | R \rangle$ זו הצגה של $G = F_X / N$
ע"י יוצרים X ויחסים R . N (קטור הסגור הנורמלי) של R .

נחזור לדוגמאות שלנו.

$$C_3 = \langle X | X^3 \rangle$$

החבורה החופשית הנוצרת ע"י איבר אחד X היא $\mathbb{Z}$.
והשיו אנחנו מחלקים אותה בחבורה הנורמלית שנוצרת ע"י X^3
שהיא $\mathbb{Z}/3\mathbb{Z}$ וקיסטנו את $\mathbb{Z}_3$.

$$\langle X, Y | X^{-1}Y^{-1}XY \rangle$$

ההתאונות שני יוצרים אנחנו מסתמים על החבורה הנורמלית
המניחלית שנוצרת ע"י הקומוטטורים. אז לא החבורה החופשית
באמצעות שני יוצרים וזה $\mathbb{Z} \times \mathbb{Z}$.

$$\langle X, Y | X^2, Y^3, X^{-1}Y^{-1}XY \rangle$$

הסגור הנורמלי פה יתבצע הסגור הנורמלי בצוגלמה
הקצומה. אז לא תהיה חבורה אנה של $\mathbb{Z} \times \mathbb{Z}$.
אלה הקואורדינטה הראשונה מחלקים ב-2 ואם השנייה ב-3
ואתקבל $\mathbb{Z}_2 \times \mathbb{Z}_3$.

סגנון: X קבוצת יוצרים $\{ \}$ $R \subseteq F_X$; $N = \langle\langle R \rangle\rangle$ הסגור
בנורמלית של R . אז $G = \langle X | R \rangle$ מקימה את התכונה
הבאה:

(*) אם H תכונה כלשהי $\{ \}$ $\varphi: X \rightarrow H$ העתקה קבוצתית
המקיימת: $\{ \varphi(x_1), \varphi(x_2), \dots \} \in E_H$ לכל $w \in R$ אזי קיים הומומורפיזם
יתיר $\varphi': G \rightarrow H$ הממשק את φ .

64

מה קורה כאן? התחלנו מתבונה של X וזקתנו את

F_X התבונה החופשית הנוצרת על X ומתבונה בתרנו

בתבונה R בהיותה F_X תבונה חופשית אם $\varphi: X \rightarrow H$

קיים הומומורפיזם $\tilde{\varphi}: F_X \rightarrow H$ שממשיק את φ . זה נכון

תמיד מכיוון שההומומורפיזם φ

כזה נתון לנו על ידי $\tilde{\varphi}(\omega) = \omega(\varphi(x_1), \varphi(x_2), \dots) = e_H$

$$\left(\begin{aligned} \tilde{\varphi}(x_1 x_2 x_3^{-1} x_1) &= \tilde{\varphi}(x_1) \tilde{\varphi}(x_2) \tilde{\varphi}(x_3)^{-1} \tilde{\varphi}(x_1) = \\ &= \varphi(x_1) \varphi(x_2) \varphi(x_3)^{-1} \varphi(x_1) = \\ &= \omega(\varphi(x_1), \varphi(x_2), \varphi(x_3)) \end{aligned} \right)$$

אם $R \subseteq \text{Ker } \tilde{\varphi}$ ו $\omega \in R$ אז $\omega \in \text{Ker } \tilde{\varphi}$ $\Leftarrow$

$\Leftarrow$ N התבונה הנורמלית המינימלית שמכילה את R

$N \subseteq \text{Ker } \tilde{\varphi}$. מה זה אומר? יש לנו מצב כזה:

$$\tilde{\varphi}: F_X \rightarrow H$$

המשפטים ההומומורפיזם זה משרה לנו

$$\tilde{\varphi}: F_X / \text{Ker } \tilde{\varphi} \xrightarrow{\text{תחג}} H$$

ועכשיו אפשר להגדיר

$$\begin{aligned} \varphi': F_X / N &\longrightarrow F_X / \text{Ker } \tilde{\varphi} \longrightarrow H \\ aN &\longmapsto a \text{Ker } \tilde{\varphi} \end{aligned}$$

למעשה התכונה (*) קובעת את G .

לעבור בין הצגות $\langle x_1, \dots, x_n \rangle$ ו $\langle y_1, \dots, y_n \rangle$ תכונה נוספת

שהכרנו עד כה יתרה והיא בעיה מאד קשה.

למעשה, הבעיה הנכונה אינה ביעה: בהינתן תבונה מוצגת

$\langle x_1, \dots, x_n \rangle$ ו $\langle y_1, \dots, y_n \rangle$, האם התבונה סריוואלית?

נסתכל על התבונה הסריוואלית. אם n אפשר להציג

$$\langle x_1, \dots, x_n \mid y_1, \dots, y_n \rangle$$

אז יש לה הצגות אחרות $\langle x_1, \dots, x_n \mid w_1, \dots, w_n \rangle$

יש אמש צדק שיטתית לעשות את זה.
 מתחילים מהצגה הטרינומאלית $\langle x_1, \dots, x_n \mid x_1, \dots, x_n \rangle$
 יש פעולות שגורמות לעבור על היתוסים מלבד לפנות את
 התבונה :

- התלפת סדר היתוסים
- הצמדת אחד היתוסים ע"י אלה איבר בתבונה
- מנפח אחד היתוסים ביחס אחד או בהופכי לו
- התלפת אחד היתוסים בהופכי שלו

שאלה פתוחה: בהינתן הצגה של התבונה הטרינומאלית
 בעלת מיוצרים n יחסים. האם ניתן להגיע מהצגה
 הטרינומאלית להצגה הנמונה בעזרת הצדדים שהצגנו?
 ההשערה היא שהתשובה היא לא (נכון)

תצור דוגמה $G = \langle x, y \mid x y x^{-1} y^{-1}, x^2, y^3 \rangle$

(ראה שקיים הומומורפיזם $\varphi: G \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$:

$$\varphi: x \mapsto (1, 0)$$

$$y \mapsto (0, 1)$$

$$\Rightarrow \begin{cases} x y x^{-1} y^{-1} \mapsto (0, 0) \\ x^2 \mapsto (0, 0) \\ y^3 \mapsto (0, 0) \end{cases}$$

זכשו לפי הטענה קיים הומומורפיזם φ' הנ"ל והוא על.

דוג דוגמה: $G = \langle x, y \mid x^n, y^2, y x y^{-1} x \rangle \cong D_{2n}$

שקפים
 סמבונים

ה- G יש אל היותר חז אברים והוא
 מועתקת על D_{2n} אכן לפי הטענה יש
 איזומורפיזם

בחר של תבונה נותנת להצגה - היוצרים יכולים להיות
 ס הקבוצה והיתוסים היתוסים שיש.

68

אם התבונה נוצרה סופית אז ההצגה שלה קבוצה
היוצרים סופית אמנם זה לא אמנם צבר ליגה מספר
היחסים.

נשים אם שמספר התבונה שניתן להציג ההצגה סופית
הוא כמובן לא. אמנם הוכחו שמספר התבונה הוא $\aleph_1$.
 $\Leftarrow$ יש תבונות שאין להן הצגה סופית.

הצגה של S_n (Miller 1897):

$$S_n = \langle x_1, x_2, \dots, x_{n-1} \mid \forall i \quad x_i^2, (x_i x_{i+1})^3, x_i x_j x_i^{-1} x_j^{-1} \mid i-j \geq 2 \rangle$$

אפשר להראות שהיחסים האלה הם בדיוק מה שצריך.

יש פה $O(n)$ יוצרים, $O(n^2)$ יחסים.

האם אפשר לדעת יותר אם אלה? ההשערה של אבנון

אין היא שאפשר לדעת אם זה $\log n$ יחסים.

אם $n \log n \approx \log |S_n|$.

נסה אחרת:

$$S_n = \langle \tau = (12), \sigma = (1, \dots, n) \mid \tau^2, \sigma^n, (\tau \sigma \tau \sigma^{-1})^3, [\tau, \sigma^{i-2} \tau \sigma^{-(i-2)}] \rangle$$

פה יש רק $O(n)$ יחסים וזה חומר בהשערה של אן.

משפט: יש S_n הצגה τ 2 יוצרים g יחסים n .

הערה: ב הצגה של S_n k יוצרים צריכה לפחות $k+1$ יחסים.

