① 23.10.07
ג. מבנים

המתרגל: עמי אייזנמן amie@math.huji.ac.il
תרגילים - חייבים להגיש לפחות 70%.
המתרגלים לא שופטים אבל מאשרים כרגיל, חוץ מזה,
ההרצאות גם מתקיימות ולכן אין שום בעיה.

זה קורס שעיקרו תורת החבורות הוא לא כל כך קשה אבל יש
מלא של מושגים וצריך לזכור ולהבין את כולם. אז נתחיל.

<u>הגדרה</u>: חבורה $(G,\cdot)$ היא קבוצה G שעליה מוגדרת
פעולה דו-מקומית $\cdot : G\times G\to G$ כך שמתקיימות התכונות:

(א) אסוציאטיביות. לכל $a,b,c\in G$ $a\cdot(b\cdot c)=(a\cdot b)\cdot c$
(האינדוקציה לה נכון לכל מספר של איברים ולכל סידור של הסוגריים)

(ב) קיים איבר $e\in G$ (איבר יחידה) כך שמתקיים $a\cdot e=e\cdot a=a$
לכל $a\in G$

(ג) לכל $a\in G$ קיים איבר $b\in G$ המקיים $a\cdot b=b\cdot a=e$

<u>הערה</u>: במקום אקסיומות ב+ג אפשר לדרוש את הבאים:
(ב*) קיים איבר $e\in G$ כך ש- $e\cdot a=a$ ולכל $a\in G$
(ג*) לכל $a\in G$ קיים $b\in G$ כך ש- $ba=e$.
כלומר מספיק לדרוש איבר יחידה רק מצד אחד ונובע
מכך שהוא גם איבר יחידה מצד שני.

<u>הוכחה</u>:
ראשית, נראה שאם $a\cdot a=a$ עבור $a\in G$ אז
$a=e$. יש $b\in G$ כך ש- $ba=e$ לכן נכפיל
את שני האגפים ונקבל

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

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

$e\cdot a=e$

$a=e$

כעת ננסה להוכיח את הטענה:

יהי $a \in G$ ונניח ש- $ba = e$. נרצה להראות שגם $ab = e$. (שתמש במה שהוכחנו קודם:

$$(ab)(ab) = a((ba)b) = a(eb) = ab$$

$\Leftarrow$ $ab = e$ $\Leftarrow$ מתקיים ①

נותר להראות ש-e הוא איבר יחידה גם מימין ואכן,

$$ae = a(ba) = (ab)a = ea = a$$

$\Leftarrow$ מתקיים ② ☺

דוגמאות לחבורות

① **חבורות תמורות**

תהי X קבוצה נסמן ב- S_x את קבוצת כל התמורות על X כלומר $S_x = \{ f : f$ חח"ע ועל $: f: X \to X\}$

פעולת הכפל ב- S_x תהיה הרכבה של העתקות.

ברור ש- S_x אכן סגורה תחת הרכבה.

איבר היחידה הוא כמובן העתקת הזהות.

הרכבת העתקות היא פעולה אסוציאטיבית.

מכיוון שהתמורות הן חח"ע ועל לכל תמורה יש תמורה הפכית.

אם $X = \{1, \dots, n\}$ נסמן $S_x = S_n$

__הגדרה:__ חבורה G תיקרא אבלית אם לכל $a, b \in G$ מתקיים $ab = ba$

S_n היא לא חבורה אבלית. למשל נסתכל על שתי תמורות ב- S_3

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \text{ אז}$$

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \text{ואילו} \quad \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

<u>תרגיל</u>: S_n אינה אבלית עבור $n \geq 3$.

<u>פיתרון</u>: זה די ברור. פשוט ניקח את הדוגמה הקודמת ונרפד אותה.

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix} \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{pmatrix}$$

<u>הגדרה</u>: אם G חבורה סופית (נקרא) מספר האיברים בה סדר החבורה ונסמנו $|G|$

<u>דוגמה</u>: $|S_n| = n!$

<u>המשך דוגמאות</u>

② $(\mathbb{Z}, +)$ (השלמים עם פעולת החיבור)
איבר היחידה הוא 0 ולכל $a \in \mathbb{Z}$ $a+(-a)=0$

③ אם F שדה אז $(F, +)$ חבורה (ברור לפי אקסיומות השדה) ובנוסף אם נסמן $F^* = F \setminus \{0\}$ אז גם $(F^*, \cdot)$ חבורה (גם ברור מהאקסיומות)

④ אם V מרחב וקטורי מעל שדה F אז $(V, +)$ חבורה.

⑤ $(\mathbb{Z}_n, +)$ - השאריות מודולו n. הוכחנו בלינארית 1 שזה שדה מקיים את מה שצריך.
אנו לא נתבלבל עם שדות. מאחר שאנחנו מסתכלים רק על פעולת החיבור אין צורך ש-n יהיה ראשוני.
אם n פריק אז יש איברים פרט לאפס שאינם הפיכים. הרי אם $n = a \cdot b$ אז $\bar{0} = \bar{a} \cdot \bar{b}$.
אבל $\bar{a} \neq \bar{0}$ אם $\bar{a}$ היה הפיך אז היינו מקבלים $\bar{b} = \bar{a}^{-1} \cdot \bar{a} \cdot \bar{b} = \bar{0}$ אבל גם $\bar{b} \neq 0$
(הסבר סימון: לכל a מסמנים $\bar{a} = a \bmod n$)

נסמן ב- $\mathbb{Z}_n^*$ את G השאריות $\bar{a} \in \mathbb{Z}_n$ כך ש-
a זר ל- n

<u>תזכורת:</u> a ו- זרים אם אין להם מחלק משותף לא טריוויאלי. מסמנים ב- (a,b) את המחלק המשותף המקסימלי של a ו- b. כלומר $(a,b)=d$ כך ש-
$d|a$, $d|b$ וגם $d'|a$ וגם $d'|b$ אז $d'|d$

ברור ש- $(a,b)=1$ אמ"מ a ו- b זרים.

ממשפט מתורת המספרים נובע שאם $(a,n)=1$ אז יש $x,y \in \mathbb{Z}$ כך ש- $ax+ny=1$, לכן
$ax=1-ny \Rightarrow \bar{a}\cdot\bar{x} \equiv 1 \pmod{n}$ ולכן יש ל- $\bar{a}$ הופכי כפלי ב- $\mathbb{Z}_n^*$.

<u>דוגמה:</u> $\mathbb{Z}_8^* = \{1,3,5,7\}$

(1) $S^1=\{z\in\mathbb{C} : |z|=1\}$ עם פעולת הכפל של מרוכבים

ברור שיש סגירות לכפל כי כשכופלים מרוכבים הערך המוחלט הוא מכפלת הערכים המוחלטים ולכן כשכופלים מספרים ב- S^1 התוצאה היא ב- S^1.
מאותה סיבה גם יש הופכי. הערך המוחלט של מספר עם ערך מוחלט 1 הוא 1: לכל $z\in S^1$ יש z^{-1} כך ש- $z^{-1}z=1$ ולכן
$$|z^{-1}| = |z^{-1}||z| = |z^{-1}z| = |1| = 1$$

[ויש כתיב נוסף של מספרים מרוכבים:
$$e^{i\theta} = \cos\theta + i\sin\theta$$
ולכן
$$e^{i\theta_1}\cdot e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$$
]

(5) שורשי היחידה - n
$$\left\{ e^{i\frac{2\pi l}{n}} : 0\le l\le n-1 \right\}$$
$$\left\{ \cos\frac{2\pi l}{n} + i\sin\frac{2\pi l}{n} : 0\le l\le n-1 \right\}$$
עם פעולת הכפל.

ח) חבורות מטריצות / ט"ל יהי V מ"ו מעל F נסמן ב- $GL(V)$ את אוסף ההעתקות הלינאריות ההפיכות $\varphi: V \to V$.

נסמן $GL_n(F)$ את אוסף המטריצות $n\times n$ ההפיכות
אלה חבורות ביחס לפעולת ההרכבה או כפל מטריצות. איבר היחידה הוא העתקת הזהות או מטריצת הזהות.

<u>הגדרה</u>: תהי G חבורה. קבוצה $H \subseteq G$ תיקרא תת חבורה אם היא חבורה ביחס לפעולה של G.
במקרה זה נסמן $H \leq G$.

<u>דוגמה</u>: $SL_n(F) = \{A \in GL_n(F) : \det A = 1\}$ זאת תת חבורה של $GL_n(F)$.

- אסוציאטיביות ברורה כי זה נכון בכללי
- סגירות תחת כפל נובעת מהכפליות של הדטרמיננטה
- הופכי קיים מאותה סיבה - האיברים הפיכים כי הם ב- $GL_n(F)$ ואילו הדטרמיננטה של ההופכי היא 1 כי

$$1 = |A \cdot A^{-1}| = |A| \cdot |A^{-1}| = |A^{-1}|$$

אם ניקח $F = \mathbb{R}$ אז $O(n) = \{$המטריצות האורתוגונליות$\}$
גם פעולת הכפל של מטריצות היא חבורה, ומעשה $O(n) \leq GL_n(\mathbb{R})$.

אם $F = \mathbb{C}$ אז $U(n) = \{$המטריצות האוניטריות$\}$
גם פעולת כפל מטריצות היא תת חבורה של $GL_n(\mathbb{C})$.

סימון:

$$T_n(F) = \left\{ \begin{array}{l} \text{מטריצות משולשיות} \\ \text{עליונות הפיכות} \end{array} \right\}$$

$$U_n(F) = \left\{ \begin{array}{l} \text{מטריצות אוניפוטנטיות} \\ \text{(כלומר משולשיות עליונות} \\ \text{עם 1-ים באלכסון} \end{array} \right\}$$

Ⓐ ברור ש- U_n, $I_n \in T_n$

Ⓑ אם $A, B \in T_n$! $AB = C$ אז נראה ש- $C_{ij} = 0$ עבור $i > j$.

$$C_{i,j} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

אם $i > k$ אז $a_{ik} = 0$

אם $k > j$ אז $b_{kj} = 0$

⇐ $a_{ik} b_{kj} \neq 0$ רק כאשר $i \leq k$ וגם $j \geq k$

⇐ אם $i > j$ אז $c_{ij} = 0$

⇐ T_n סגורה לכפל מטריצות

הטיעון דומה מראים סגירות לכפל של U_n.

Ⓒ בלינארית למדנו נוסחה למטריצה ההופכית:

$$(A^{-1})_{i,j} = \frac{(-1)^{i+j}}{\det A} \cdot A_{ji}$$

אפשר להשתמש בזה בשביל להראות את הדרוש,
אבל אנחנו נעשה משהו יותר אלגנטי.

נתבונן ב- $A \in U_n$ אז $A = I - N$ כאשר
N נילפוטנטית (כלומר $N^k = 0$ עבור k כלשהו)

$$(I-N)(I+N+N^2+\dots+N^r) =$$
$$= I - N + N - N^2 + \dots + N^r - N^{r+1} =$$
$$= I - N^{r+1} = I$$

עבור $k < r$ כלשהו

⇐ $A^{-1} = I + N + \dots + N^{k-1}$. לכן A^{-1} אוניפוטנטית.

עבור T_n מתקבל מ- U_n כי כל איבר ב- T_n הוא
מכפלת מטריצה אלכסונית (הפיכה) עם מטריצה ב- U_n.

יהי F שדה סופי עם q איברים (למשל $\mathbb{Z}_q$ עבור q ראשוני)

נחשב את $|GL_n(F)|$

נזכור שמטריצה הפיכה אמ"מ העמודות שלה הן בת"ל.

עבור $A\in GL_n(F)$ יש q^n-1 אפשרויות לבחור את העמודה הראשונה (כל ה-n-יות פרט ל-$\vec{0}$).

יש q^n-q אפשרויות לבחירת העמודה השנייה כי היא לא יכולה להיות כפולה של העמודה הראשונה.

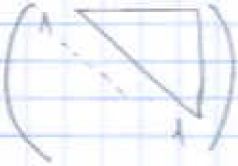
עבור העמודה השלישית יש q^n-q^2 אפשרויות וכו'.

$$\Leftarrow \quad |GL_n(F)| = \prod_{i=0}^{n-1}(q^n-q^i) =$$

$$= q\cdot q^2\cdot\ldots\cdot q^{n-1}(q^n-1)(q^{n-1}-1)\ldots(q-1) =$$

$$= q^{1+2+\ldots+(n-1)}\prod_{i=1}^{n}(q^i-1) = q^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}(q^i-1)$$

נחשב את $|U_n(F)|$. זה הרבה יותר פשוט מאחר שברור שמטריצות הפיכות יש חופש מוחלט בבחירת הקואורדינטות מעל האלכסון.



מאחר שיש $1+2+\ldots+(n-1)$ קואורדינטות יש $q^{\frac{n(n-1)}{2}}$ אפשרויות.

כלומר $|U_n(F)| = q^{\frac{n(n-1)}{2}}$

הערה מעניינת: $q^{\frac{n(n-1)}{2}}$ זו החזקה המקסימאלית של q שמחלקת את הסדר של $GL_n(F)$. ומצאנו גם תת חבורה שזה הסדר שלה.

הגודל של $|T_n(F)|$ גם לא מסובך.

$$|T_n(F)| = \underbrace{q^{\frac{n(n-1)}{2}}}_{\text{קואורדינטות מעל האלכסון}}\cdot\underbrace{(q-1)^n}_{\text{קואורדינטות של האלכסון}}$$

(5)

30.10.04

ת. מבנים

הערות (תרגול) 2

$$n\mathbb{Z} = \{nz : z\in\mathbb{Z}\}$$
$$\mathbb{Z}/m = \{\tfrac{a}{m} : a\in\mathbb{Z}\}$$
$$d\mathbb{Z}_n = \{d\cdot a : a\in\mathbb{Z}_n\}$$

העתקות צפידות ב-$\mathbb{R}^n$

הגדרה: העתקה $T:\mathbb{R}^n\to\mathbb{R}^n$ נקראת צפידה אם לכל $x,y\in\mathbb{R}^n$ $\|Tx-Ty\| = \|x-y\|$ כאשר $\|(x_1,\dots,x_n)\| = \sqrt{\sum x_i^2}$

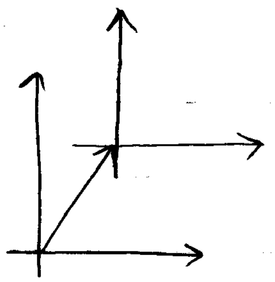
אלה פשוט העתקות ששומרות מרחקים.

דוגמאות:

(א) העתקות לינאריות אורתוגונליות

(ב) אם $\varepsilon\in\mathbb{R}^n$ נסמן $T_\varepsilon(v)=v+\varepsilon$

T_ε נקראת הזזה ב-ε. וזה ממש ברור שהיא משמרת מרחקים. (אבל לא לינארית)



משפט ללא הוכחה: כל העתקה צפידה היא הרכבה $T_\varepsilon\circ S$ כאשר T_ε הזזה ב-ε ו-S אורתוגונלית.

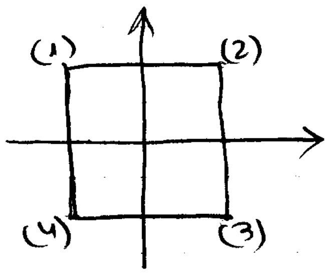
מסקנה: קבוצת ההעתקות הצפידות היא חבורה ביחס להרכבה.

הוכחה:

- סגירות - ברור
- אסוציאטיביות - ברור
- איבר יחידה - העתקת הזהות שהיא צפידה
- הופכי - אם $T_\varepsilon\circ S$ העתקה צפידה קל למצוא לה הופכי שהרי S אורתוגונלית ולכן הפיכה ו- $T_\varepsilon^{-1} = T_{-\varepsilon}$.

חבורת סימטריות (דיהדרליות)

נתבונן בכל ההעתקות הצפידות במישור המעבירות ריבוע לעצמו. יש 8 אפשרויות:



- זהות
- סיבוב ב- $90°, 180°, 270°$
- שיקוף ביחס לציר x, y
- שיקוף ביחס לאלכסון חיובי ושלילי

ההעתקות האלה נקראות **הסימטריות של הריבוע**.

הערה: כל סימטריה אפשר לתאר כתמורה של קודקודי הריבוע. אבל לא כל תמורה מייצגת סימטריה. למשל $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ אינה סימטריה.

קבוצת הפונקציות שנוצרות ע"י הרכבת 8 הסימטריות היא חבורה והיא נקראת החבורה הדיהדרלית D_8.
נשים לב שהגודל של החבורה הוא 8. כל הרכבה נותנת אחת מהסימטריות. למשל, אפשר לראות שהחבורה נוצרת ע"י סיבוב ב- $90°$ ושיקוף ביחס לציר ה- x.

$f(x,y) = (x,-y) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$ - שיקוף ציר x

$g(x,y) = (y,-x) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$ - סיבוב $90°$

$f \circ g(x,y) = f(y,-x) = (y,x) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$

וזה שיקוף סביב האלכסון החיובי.

טענה: D_8 הוא מהצורה $\{ f^i \circ g^j : i=0,1 \;\; j=0,1,2,3 \}$

באופן כללי, החבורה הדיהדרלית D_{2n} (חבורת הסימטריות של מצולע משוכלל עם n קודקודים) נוצרת ע"י איבר f מסדר 2 ואיבר g מסדר n.

נעיר רק ש- D_8 אינה אבלית כי $g \circ f(x,y) = g(x,-y) = (-y,-x)$

החבורה החופשית

תהי X קבוצה. נגדיר את החבורה החופשית של (היוצרים) של X. נגדיר X^{-1} קבוצה זרה ל- X עם התאמה חח"ע ועל בין $x\in X$ ו- $x^{-1}\in X^{-1}$.

נתבונן באוסף $X\cup X^{-1}\cup\{1\}$ (כרגע 1 הוא סתם סימן).

<u>הגדרה:</u> מילה של X היא סדרה $\omega=(a_1,a_2,\dots)$ כאשר $a_i\in X\cup X^{-1}\cup\{1\}$ ו- $a_n=1$ החל ממקום מסוים.

המילה $(1,1,1,\dots)$ נקראת המילה הריקה.

מאחר שהחל ממקום מסוים ב המילה היא 1-ים אפשר לרשום מילים כ- $\omega=x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_n^{\varepsilon_n}$ כאשר $\varepsilon_i=0,1,-1$ לכל $i<n$, ו- $\varepsilon_n=1,-1$ ו- $x_i\in X$ ומגדירים $x^0\equiv 1$.

<u>הגדרה:</u> ההופכי של $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_n^{\varepsilon_n}$ הוא $x_n^{-\varepsilon_n}\dots x_2^{-\varepsilon_2}x_1^{-\varepsilon_1}$

<u>הגדרה:</u> מילה $w=x_1^{\varepsilon_1}\dots x_n^{\varepsilon_n}$ תיקרא מצומצמת אם לכל $1\le i\le n$ $\varepsilon_i\in\{1,-1\}$ וגם $x_{i+1}^{\varepsilon_{i+1}}\ne x_i^{-\varepsilon_i}$ - כלומר אין שני איברים הפוכים עוקבים. גם 1 נקראת מילה מצומצמת.

נגדיר כפל של מילים מצומצמות: אם $w=x_1^{\varepsilon_1}\dots x_n^{\varepsilon_n}$ ו- $u=y_1^{\delta_1}\dots y_m^{\delta_m}$ מילים מצומצמות אז wu היא המילה המצומצמת המתקבלת מ- $x_1^{\varepsilon_1}\dots x_n^{\varepsilon_n}y_1^{\delta_1}\dots y_m^{\delta_m}$ אחרי צמצום (למשל $x_1x_2^{-1}x_3\cdot x_3^{-1}y_1y_2=x_1x_2^{-1}y_1y_2$)

<u>טענה:</u> אוסף המילים המצומצמות עם פעולת הכפל מתקבל מבנה של חבורה.

החלק הבעייתי של ההוכחה הוא דווקא אסוציאטיביות וכל השאר ברור.

החבורה הזאת נקראת <u>החבורה החופשית של X</u>.

נשים לב שאם F החבורה החופשית של X, G חבורה, ו- $f:X\to G$ פונקציה אז ישנו הומומורפיזם $\varphi:F\to G$ כך ש- $\varphi|_X=f$. (זה די ברור כי כל מילה, בעזרת תכונות ההומומורפיזם יודעים לאן היא הולכת).

<u>דוגמה:</u> $\mathbb{Z}_5$ נוצרת ע"י 1. נגדיר
$f:\{1\}\to\mathbb{Z}_7$ ע"י $f(1_5)=1_7$

אז אין הומומורפיזם $\varphi:\mathbb{Z}_5\to\mathbb{Z}_7$ המרחיב את f:
$$0_7=\varphi(0)=\varphi(1+1+1+1+1)=5\varphi(1)=5_7$$
וזו סתירה.

אז העניין פה הוא שלא תמיד אפשר להרחיב. אפשר לעשות את זה רק על החבורה החופשית והסיבה לזה הוא שאין עליה שום אילוצים. ב- $\mathbb{Z}_5$ אנחנו יודעים ש- $5\cdot 1_5=0_5$ וזה מה שדפק אותנו.

<u>דוגמה:</u> החבורה החופשית על איבר אחד היא איזומורפית ל- $\mathbb{Z}$.

<u>דוגמאות להומומורפיזמים</u>

(א) $\varphi:\mathbb{Z}\to\mathbb{Z}$ - עבור $n\in\mathbb{Z}$ נתון אפשר להגדיר $\varphi(a)=na$,
אז $\operatorname{Im}\varphi=n\mathbb{Z}$

(ב) $\varphi:\mathbb{Z}\to\mathbb{Z}_n$ המוגדרת ע"י $a\mapsto a(\mathrm{mod}\,n)$
מתקיים $a+b\mapsto(a+b)(\mathrm{mod}\,n)=$
$=[(a\bmod n)+(b\bmod n)](\mathrm{mod}\,n)$

(ג) $\log_a:(\mathbb{R}^+,\cdot)\to(\mathbb{R},+)$
ידועה הזהות $\log_a(xy)=\log_a x+\log_a y$
ולכן זה הומומורפיזם.
זהו איזומורפיזם כי יש לו הופכי $a^x:(\mathbb{R},+)\to(\mathbb{R}^+,\cdot)$

(ד) $\mu_n=\{e^{i\frac{2\pi k}{n}}:0\le k\le n-1\}$ - שורשי היחידה ה- n,
אז $\mu_n\cong\mathbb{Z}_n$ ע"י ההעתקה $e^{i\frac{2\pi k}{n}}\mapsto k(\mathrm{mod}\,n)$
ומתקיים $e^{i\cdot\frac{2\pi k}{n}}\cdot e^{i\frac{2\pi l}{n}}=e^{i\frac{2\pi(k+l)}{n}}$
$\Leftarrow$ זה הומומורפיזם. ומכאן, זה גם איזומורפיזם.

(7)

ה) בתרגיל הוכחנו שההצמדה $x \mapsto \gamma x \gamma^{-1}$ עבור $\gamma \in G$ נתון הוא איזומורפיזם מ-G ל-G

הגדרה: איזומורפיזם $\varphi : G \to G$ נקרא אוטומורפיזם.

ו) יהי $y \in \mathbb{R}$. נגדיר $f_y : \mathbb{R} \to S^1$ ע"י $f_y(x) = e^{iyx}$
זה הומומורפיזם אבל הוא לא חח"ע כי הוא מחזורי.

ז) תהי $H \le G$ תת חבורה. אז השיכון $\varphi : H \hookrightarrow G$, $h \mapsto h$
הוא הומומורפיזם חח"ע.
למשל, אפשר לשכן את S_n ב-S_{n+1} כך:

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

למעשה ניתן לשכן אותה ב-S_{n+k} לכל k. אז אפשר לחשוב על S_n כתת חבורה של חבורת תמורות גדולה יותר.

ח) $\det : GL_n(F) \to (F^*, \cdot)$ מתכונות של הדטרמיננטה נובע שזה הומומורפיזם. הגרעין שלו הוא G המטריצות עם דטרמיננטה 1. כלומר $\ker\det = SL_n(F)$.

המבנה של S_3

$$S_3 = \left\{ id, \underbrace{\begin{pmatrix} 1&2&3 \\ 2&1&3 \end{pmatrix}, \begin{pmatrix} 1&2&3 \\ 3&2&1 \end{pmatrix}, \begin{pmatrix} 1&2&3 \\ 1&3&2 \end{pmatrix}}, \underbrace{\begin{pmatrix} 1&2&3 \\ 2&3&1 \end{pmatrix}, \begin{pmatrix} 1&2&3 \\ 3&1&2 \end{pmatrix}} \right\}$$

איברים מסדר 2, כלומר $\sigma^2 = id$; איברים מסדר 3, כלומר $\sigma^3 = id$

למה, S_3 זו בדיוק החבורה הדיהדרלית D_6.

טענה: יהיו $\sigma, \tau \in S_3$, σ מסדר 2 ו-τ מסדר 3.
אז $\{\sigma, \tau\}$ יוצרת את S_3, כלומר $\langle \sigma, \tau \rangle = S_3$.
הוכחה: נראה שע"י המכפלות שלהם אפשר לקבל 6 איברים שונים ואז זו הרי חייבת להיות G החבורה.

יש לנו כבר את $\underline{\tau}, \underline{\sigma}, \underline{id}$.
נשים לב ש- $\underline{\tau^2} \neq id$ כי הוא מסדר 3. היא
גם לא τ כי אז $\tau = id$. $\tau \neq \sigma$ כי
$(\tau^2)^2 = \tau$ אבל σ מסדר שני.
$\underline{\sigma\tau} \neq id$ כי $\tau^{-1} = \tau^2$ והרי $\tau^2 \neq \sigma$.
$\sigma\tau \neq \tau\sigma$ כי אחרת $\sigma = id$ או $\tau = id$)
$\sigma\tau \neq \tau^2$ כי אחרת $\sigma = \tau$.
האיבר האחרון הוא $\underline{\sigma\tau^2}$.
$\sigma\tau^2 \neq id$ מאותה סיבה ש $\sigma\tau \neq id$
$\sigma\tau^2 \neq \sigma$, אחרת $\tau^2 = id$
$\sigma\tau^2 \neq \tau$, אחרת $\sigma\tau = id$
$\sigma\tau^2 \neq \sigma\tau$, אחרת $\tau = id$
$\sigma\tau^2 \neq \tau^2$, אחרת $\sigma = id$.

(:

יחס שקילות

יחס שקילות $\sim$ על קבוצה X הוא יחס רפלקסיבי, סימטרי וטרנזיטיבי.
עבור $x \in X$ נגדיר את מחלקת השקילות של x ע"י
$[x] = \{y \in X : x \sim y\}$
מתקיים ש- X איחוד זר של מחלקות השקילות של $\sim$.

נגדיר יחס שקילות על $\mathbb{Z}$: $a \sim_n b$ אמ"מ $a \equiv b \pmod{n}$
אמ"מ $n \mid b-a$.
לא קשה לראות שהוא יחס שקילות:
- ברור ש- $n \mid a-a$
- אם $n \mid b-a$ אז $n \mid a-b$ (היפוך הסימן)
- אם $n \mid b-a$; $n \mid c-b$ אז $n \mid (b-a)+(c-b)$
כלומר $n \mid c-a$

מחלקות השקילות הן מהצורה
$[a] = \{b \in \mathbb{Z} : cn = b-a\} = \{a + cn : c \in \mathbb{Z}\}$

(8) 6.11.07
ת. מבנים

הערה לתרגיל: G תמורה ניתנת לפירוק למכפלה של מחזורים זרים. לא קשה לראות שהפירוק הזה הוא יחיד עד כדי הסדר של המחזורים.

יחסי שקילות ומחלקות שקילות

דוגמאות

א) יחס שקילות על $\mathbb{Z}$ (יחס הקונגרואנציה מודולו n)
$a \sim b$ אמ"מ $n \mid b-a$. מסמנים $a \equiv_n b$.
מחלקות השקילות הן מחלקות השארית $\mathbb{Z}_n$:
$[a] = \{a+kn : k \in \mathbb{Z}\}$

ב) תהי G חבורה. נגדיר יחס שקילות באופן הבא:
$x, y \in G$ אז $x \sim y$ אמ"מ קיים $g \in G$ כך ש- $gxg^{-1} = y$. נראה שזה אכן יחס שקילות:
רפלקסיביות: $exe^{-1} = x$
סימטריות: $gxg^{-1} = y \Leftarrow x = g^{-1}yg$
טרנזיטיביות: $x = gyg^{-1}$, $y = hzh^{-1}$
$\Leftarrow hgxg^{-1}h^{-1} = (hg)x(hg)^{-1} = z$
מחלקות השקילות של היחס הזה נקראות מחלקות צמידות. למשל, אם G חבורה אבלית אז
$[x] = \{gxg^{-1} : g \in G\} = \{xgg^{-1}\} = \{x\}$

ג) תהי $H \leq G$ חבורה חלקית. בשיעור הגדרנו יחס שקילות על G: אומרים $a \sim b$ אמ"מ $b^{-1}a \in H$
מחלקות השקילות של היחס הזה נקראות מחלקות שמאליות של H ב- G.
$[a] = aH = \{ah : h \in H\}$

אפשר גם להגדיר את היחס $a \sim b$ אמ"מ $ab^{-1} \in H$
ומקבלים מחלקות ימניות של H ב- G
$[a] = Ha = \{ha : h \in H\}$
למשל $n\mathbb{Z} \leq \mathbb{Z}$. יחס השקילות במקרה שלנו הוא
$a \sim b$ אמ"מ $-b+a = a-b \in n\mathbb{Z}$
כלומר אמ"מ $n \mid a-b$ שזה יחס הקונגרואנציה מודולו n.
בגלל שזו חבורה אבלית מחלקות השקילות השמאליות שוות למחלקות השקילות הימניות.

בשיעור ראינו שגודל המחלקות השמאליות / הימניות שווה (ראינו העתקה חח"ע של H ו- aH)

למשל, בתרגיל ראינו שהמחלקות השמאליות ב- $G = GL_n(\mathbb{Z}_p)$ ביחס ל- $H = SL_n(\mathbb{Z}_p)$ הן המטריצות עם דטרמיננטה $1,2,3,\dots,p-1$ והן שוות גודל.

לעומת זאת, במקרה של מחלקות צמידות גודל המחלקות בד"כ אינו זהה. תמיד $[e] = \{e\}$ אבל למשל ב- S_n יש מחלקות צמידות עם כמה איברים.

אם $G = S_3$, $H = \langle(123)\rangle$ המחלקות השמאליות של H הן:
$idH = H \qquad (12)H = \{(12),(13),(23)\}$
המחלקות הימניות של H הן $Hid = idH, (12)H = (21)H$
לעומת זאת, תהי $K = \langle(12)\rangle$. המחלקות השמאליות הן:
$K, \ (123)K = \{(123),(13)\},$
$(23)K = \{(23),(132)\}$
המחלקות הימניות הן:
$K, \ K(123) = \{(123),(23)\}, \ K(13) = \{(13),(132)\}$

לסיכום, מספר המחלקות השמאליות שווה למספר המחלקות הימניות, אבל לא תמיד מקבלים את אותן קבוצות.

<u>תרגיל</u>: מספר מחלקות שמאליות שווה למספר הימניות.
<u>הוכחה</u>: ההתאמה $aH \mapsto Ha^{-1}$ היא חח"ע ועל בין המחלקות השמאליות לימניות.

<u>למה לא הגדרנו $aH \mapsto Ha$?</u>

<u>תשובה</u>: כי העתקה של מחלקות שקילות מוגדרת היטב רק כאשר היא לא תלויה בבחירת נציג.
במקרה שלנו צריך להראות שאם $b \in aH$ אז $Ha = Hb$, כלומר אם $a^{-1}b \in H$ אז $ab^{-1} \in H$ אבל זה לא בהכרח נכון.
לעומת זאת עבור $aH \mapsto Ha^{-1}$ ההעתקה מוגדרת היטב. אם $b \in aH$ אז $a^{-1}b \in H$ ולכן $b^{-1}a \in H \Rightarrow Ha^{-1} = Hb^{-1}$.

העשרה בתורת מספרים אלמנטרית

<u>המשפט היסודי של האריתמטיקה</u>: כל מספר טבעי n אפשר לכתוב כמכפלת מספרים ראשוניים והפירוק יחיד עד כדי שינוי סדר. $n = p_1^{e_1} \cdots p_k^{e_k}$
כאשר $\{p_i\}$ ראשוניים, $\{e_i\} \in \mathbb{N}$

<u>הגדרה</u>: יהיו $a,b \in \mathbb{Z}$. $d=(a,b)$ הוא מחלק משותף מקסימלי אם $d|a$, $d|b$ וכל d' המקיים $d'|a$; $d'|b$ מתקיים $d'|d$.

טענה: לכל $a,b\in\mathbb{Z}$ קיים (a,b)

הוכחה: נניח $a=p_1^{e_1}\cdots p_k^{e_k}$

$b=p_1^{f_1}\cdots p_k^{f_k}$

כאשר $e_i,f_i\in\mathbb{N}\cup\{0\}$. אז קל לראות ש-

$$(a,b)=p_1^{\min(e_1,f_1)}\cdots p_k^{\min(e_k,f_k)}$$

☺

הערה: אם $a,b\in\mathbb{Z}$ אז הכפולה המשותפת המינימלית של a,b $m=[a,b]$ היא מספר המקיים $a|m$ ו- $b|m$ ולכל m' כך ש- $a|m'$ ו- $b|m'$ מתקיים $m|m'$.

תרגיל: לכל $a,b\in\mathbb{Z}$ קיים $[a,b]$ ומתקיים

$$[a,b](a,b)=ab$$

טענה: יהיו $a,b\in\mathbb{Z}$ ונסמן $d=(a,b)$. אזי קיימים $x,y\in\mathbb{Z}$ כך ש- $ax+by=d$.

הוכחה: נגדיר $R=\{ax+by : x,y\in\mathbb{Z}\}$

יהי $0<d'$ מינימלי ב- R. נטען ש- $d'=(a,b)$

נראה שלכל $z\in R$ $d'|z$. נחלק עם שארית:

$z=qd'+r$ $\quad 0\le r<d'$

אם $0<r$ אז $r=z-qd'\in R$ אבל $r<d'$

בסתירה להנחת המינימליות של d'. $\Leftarrow$ $r=0$

$\Leftarrow$ $z=qd'$ או $d'|z$. $\Leftarrow$ d' מחלק משותף.

בנוסף, אם $d''|a$, $d''|b$ אז $d''|ax+by$

לכל $x,y\in\mathbb{Z}$ $\Leftarrow$ $d''|d'$.

לכן d' מחלק משותף מקסימלי. בפרט, אם $(a,b)=1$ קיימים $x,y\in\mathbb{Z}$ כך ש- $ax+by=1$ - מאידך, אם עבור a,b יש x,y כנ"ל אז $(a,b)=1$. אחרת, אם $(a,b)=d>1$ נקבל $d|ax+by=1$ וזו סתירה

☺

לכן, אם $0\le a<n$ אז קיים $b\in\mathbb{Z}$ כך ש-
$ab\equiv 1 \pmod n$ אמ"מ $(a,n)=1$
ובמקרה זה גם $(b,n)=1$.

<u>הערה</u> - יש חבורה יחידה מסדר 1
- חבורה יחידה מסדר 2,3
- 2 חבורות מסדר 4
- חבורה יחידה מסדר p לכל p ראשוני.

- בשביל להראות שיש שתי חבורות מסדר 4 עבדנו קשה. אבל אפשר להוכיח את זה בצורה פשוטה. אם G חבורה מסדר 4 אז סדרי האיברים השונים מהיחידה ב-G יכולים להיות 2 או 4. אם יש איבר מסדר 4 אז G ציקלית. אחרת כל האיברים מסדר 2 ואז אין ברירה ללוח הכפל אלא להיראות כך:

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

- אם p ראשוני אז סדר איבר שאינו היחידה הוא p ולכן איבר יוצר את החבורה, בפרט החבורה ציקלית.

- נטען שעד כדי איזומורפיזם יש שתי חבורות מסדר 6: $\mathbb{Z}_6$ (חבורה אבלית) ! - S_3 (לא אבלית). נניח G חבורה מסדר 6. סדרי האיברים השונים מ-e יכולים להיות 2,3,6. אם יש איבר מסדר 6 אז קיבלנו את החבורה הציקלית מסדר 6.

אם כל האיברים מסדר 2 אז G אבלית (לפי תרגיל)
יהיו $a,b\in G$ ונניח $ab=c$. אז $cb=bc=a$
וגם $ac=ca=b$. $\Leftarrow$ $H=\{e,a,b,c\}$ תת חבורה
של G. אבל $|H|=4$! $4\nmid 6$ סתירה (משפט
לגרנז').

$\Leftarrow$ יש איבר מסדר 3 ב-G. (נסמנו ב-a. נסמן
$b=a^2$. גם זה איבר מסדר 3.
נראה שאלה האיברים היחידים מסדר 3. נניח
$c\notin\langle a\rangle$ גם מסדר 3 ונסמן $d=c^2$. אז יש
4 איברים מסדר 3 ועוד איבר f מסדר 2.
נחשב את bc. $bc\neq e,b,c,b^2,c^2$, באופן דומה
גם $bc^2\neq e,b,c,b^2,c^2$. $\Leftarrow$ $bc=f$ וגם
$bc^2=f$ וזו סתירה (כי $bc^2\neq bc$).
$\Leftarrow$ ב-G יש 3 איברים מסדר 2 ושני איברים מסדר 3.
נניח שהחבורה היא $G=\{e,\underbrace{a,b}_{\text{סדר }3},\underbrace{c,d,f}_{\text{סדר }2}\}$

נראה שמכפלת שני איברים מסדר 2 היא איבר
מסדר 3: בשלילה, אם $cd=f$ אז
$(cd)(cd)=e$ $\Leftarrow$ $dc=e\cdot cd$ וכנ"ל
$fc=d=cf$ ו- $fd=df=c$. $\Leftarrow$
$\{e,c,d,f\}$ תת חבורה מסדר 4 וזו סתירה.

המשך שבוע הבא.

(11) 13.11.07
ת. מבנים

<u>הגדרה</u>: תהי G חבורה. המרכז (Center) של G הוא הקבוצה

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

זו קבוצת האיברים שמתחלפים עם כל האיברים האחרים.
קל לראות ש- $Z(G)$ תת חבורה של G.

<u>הגדרה</u>: תהי G חבורה ויהי $x\in G$. המרכז (centralizer) של x ב- G הוא הקבוצה:

$$C_G(x)=\{g\in G : gx=xg\}$$

קל לראות שזו תת חבורה של G.

<u>טענה</u>: חבורה מסדר 6 איזומורפית ל- $\mathbb{Z}_6$ או ל- S_3.
<u>המשך הוכחה</u>: הראנו שאם יש איבר מסדר 6 אז $G\cong\mathbb{Z}_6$. אחרת, יש 3 איברים מסדר 2 ושני איברים מסדר 3. הראנו שמכפלת שני איברים מסדר 2 היא איבר מסדר 3.

נסמן את האיברים מסדר 3 ע"י $a, a^2=b$
נסמן את האיברים מסדר 2 ע"י c, d, f
נניח בה"כ $cd=a$. dc מסדר 3 ולכן
$dc=cd$ (אחרת $(cd)(dc)=id$) ⇐ $dc=b$
$cf\neq cd$, אבל cf מסדר 3 ⇐ $cf=b$
$fd\neq cd$ ⇐ $fd=b$.
$fc\neq dc$ ⇐ $fc=a$
$df\neq dc$ ⇐ $df=a$

$cd=a$ ⇐ $ca=d$; $ad=c$
$dc=b$ ⇐ $bc=d$; $db=c$
$cf=b$ ⇐ $bf=c$; $cb=f$
$fc=a$ ⇐ $ac=f$; $fa=c$.

וכן הלאה...

לוח הכפל המתקבל:

·	id	a	b	c	d	f
id	id	a	b	c	d	f
a	a	b	id	f	c	d
b	b	id	a	d	f	c
c	c	d	f	id	a	b
d	d	f	c	b	id	a
f	f	c	d	a	b	id

אם נשים את הסימונים המתאימים נקבל את הטבלה של S_3. הטבלה הזו נקבעה באופן יחיד עד כדי הבחירה השרירותית של ההתחלה. כל בחירה אחרת היתה מביאה תוצאה איזומורפית.

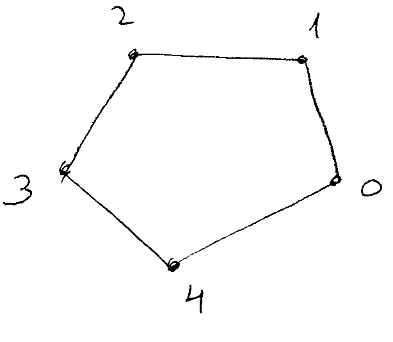
גרף קיילי

<u>הגדרה:</u> גרף הוא זוג (V,E) כאשר V קבוצה של איברים שנקראים קודקודים (vertices) ו- E קבוצה של זוגות של איברים מ- V (ללא חשיבות לסדר). איברי E נקראים צלעות (edges). נאמר ש- $v_1, v_2 \in V$ מחוברים בצלע אם $\{v_1, v_2\} \in E$.

<u>הגדרה:</u> תהי G חבורה ו- X קבוצת יוצרים ב- G. גרף קיילי $\Gamma(G,X)$ נתון באופן הבא: הקודקודים V הם איברי החבורה G. $g,h \in V$ מחוברים אמ"מ $gx = h$ או $gx^{-1} = h$ לאיזה $x \in X$.

<u>דוגמאות:</u>

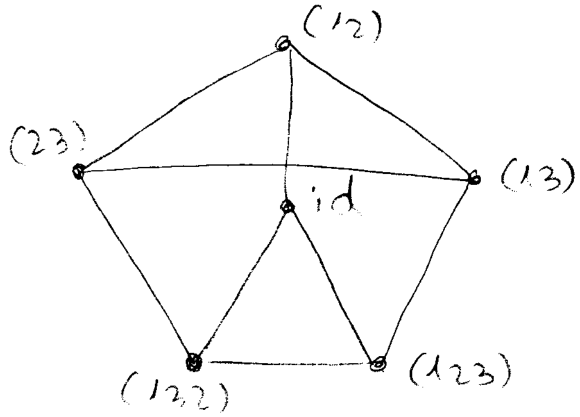
① $\Gamma(\mathbb{Z}_5, \{1\})$



(12)

ב) אם $G=X$ מקבלים גרף מלא - כל איבר מחובר לכל איבר (כולל עצמו).

ג) $\Gamma(S_3, X)$ כאשר $X=\{(12),(123)\}$



הערה: גרף קיילי תלוי ביוצרים!

הגדרה: מסילה בגרף היא סדרה $(v_0, v_1, \ldots, v_n)$ כאשר $v_i \in V$; v_i, v_{i+1} מחוברים בצלע. אורך המסילה הוא n.

הגדרה: גרף ייקרא קשיר אם כל שני קודקודים שלו מחוברים במסילה.
בגרף קשיר עבור שני קודקודים a,b נגדיר את המרחק ביניהם להיות האורך המינימלי של מסילה מ-a ל-b.

נשים לב שגרף קיילי תמיד קשיר כי לכל איבר $g \in G$ יש מסילה מתחילה ל-g. שהרי אם $g = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ אז המסילה נתונה ע"י $(id, x_1^{\varepsilon_1}, x_1^{\varepsilon_1} x_2^{\varepsilon_2}, \ldots, g)$

יהיו $g,h \in G$. מסילה מ-g ל-h נתונה ע"י w רק ש- $gw=h$. $w = x_1^{\varepsilon} \ldots x_n^{\varepsilon}$.

הגדרה: בהינתן חבורה G וקבוצת יוצרים X נסמן עבור $g \in G$ את $l(g)$ להיות המספר המינימלי של יוצרים

כך שאפשר לכתוב את g כמכפלתם. במקרה שלנו עבור $h = g\omega$, $d(g,h)=\ell(\omega)$ (יש התאמה בין מסילות מ-g ל-h לבין מילים של ω ע"י היוצרים).

<u>הגדרה:</u> הקוטר של גרף הוא $\sup_{u,v\in V} d(u,v)$

הקוטר של גרף קיילי הוא האורך המקסימלי של איבר ב-G. (נשים ♡ שזה יכול להיות אינסופי!)

<u>הגדרה:</u> G חבורה. תת חבורה $H\leq G$ תיקרא נורמלית אם $gHg^{-1}=H$ לכל $g\in G$ (ולמעשה מספיק $gHg^{-1}\subseteq H$).
במקרה זה נסמן $H\lhd G$
באופן שקול $H\lhd G$ אמ"מ כל מחלקה שמאלית היא גם מחלקה ימנית.

<u>דוגמאות</u>

ⓐ $A_n \lhd S_n$ (A_n הן התמורות הזוגיות) שהרי אם $\sigma\in A_n$; $\tau\in S_n$ אז

$$sgn(\tau\sigma\tau^{-1}) = sgn(\tau)sgn(\sigma)sgn(\tau) = sgn(\sigma)$$

ⓑ $SL_n(F)\lhd GL_n(F)$ כי אם $A\in SL_n(F)$; $B\in GL_n(F)$ אז

$$det(BAB^{-1}) = det(A) = 1$$

$\Leftarrow BAB^{-1}\in SL_n(F)$

ⓒ יהיו G, H חבורות, $\varphi: G\to H$ הומומורפיזם, אז $Ker\varphi\lhd G$: נניח $k\in Ker\varphi$; $g\in G$. אז

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

אנחנו עוד נראה שזאת הדוגמא הכללית ביותר.
למשל, בדוגמא א' $sgn: S_n\to\{\pm1\}$ הוא הומומורפיזם ו-$A_n = Ker\, sgn$.

דוגמה ב) $\det : GL_n(F) \to F^*$ הוא הומומורפיזם.

3) S_3 - תת החבורה הנוצרת ע"י (123) היא נורמלית. למעשה זו A_3 - ה התמורות מסדר

ג) . ראינו שהמחלקות השמאליות והימניות שוות.
מצד שני, תת החבורה $\langle (12) \rangle$ אינה נורמלית כי המחלקות השמאליות והימניות שלה לא שוות.

נניח $H \lhd G$ ו- $x \in H$. אז $H \supseteq x^G = \{gxg^{-1} : g \in G\}$

<u>מסקנה:</u> $H \lhd G$ אמ"מ H הוא איחוד של מחלקות צמידות.

ראינו שמחלקות הצמידות ב- S_n נקבעות לפי מבנה המחזורים של התמורות.

<u>שאלה:</u> אם $H \lhd S_4$ מה יכול להיות $|H|$?

<u>פיתרון:</u> $|S_4| = 24 \Rightarrow$ סדר של כל תת חבורה יכול להיות אחד מהבאים $1, 2, 3, 4, 6, 8, 12, 24$

מהם גדלי מחלקות הצמידות ב- S_4?

id	$\leftrightarrow$	1
(ab)	$\leftrightarrow$	6
(abc)	$\leftrightarrow$	8
$(abcd)$	$\leftrightarrow$	6
$(ab)(cd)$	$\leftrightarrow$	3

סה"כ 24

תת חבורה נורמלית היא איחוד מחלקות צמידות $\Rightarrow$ הסדר שלה צריך להיות סכום של הגדלים האלה.

$\Rightarrow$ האפשרויות הבאות נפסלות: $2, 3, 6, 8, 12$

כלומר האפשרויות היחידות הן 4 ו- 12

<u>חבורות מנה:</u> מהינתן $H \triangleleft G$ מגדירים מבנה של חבורה של המחלקות של H:

(א) נקבוצות $(aH)\cdot(bH)=(ab)H$
כי $Hb=bH$ כי H נורמלית

(ב) במחלקות שקילות $[a][b]=[ab]$
הכפל מוגדר היטב, כלומר לא תלוי בנציגים, כי H נורמלית.

<u>דוגמאות:</u>

(א) $A_3 \triangleleft S_3$. $|S_3/A_3|=2 \Leftarrow S_3/A_3 \cong \mathbb{Z}_2$.
למשל $(12)A_3\,A_3=(12)A_3$
$(12)A_3\,(12)A_3=A_3$

(ב) אם G אבלית אז כל $H \leq G$ היא נורמלית,
שהרי $gHg^{-1}=gg^{-1}H=H$
ניקח למשל את $\mathbb{Z}_n$. נניח $H \leq \mathbb{Z}_n$ נוצרת ע"י d כאשר $d|n$. אז $|H|=\frac{n}{d}$.
קל לראות שחבורת המנה $\mathbb{Z}_n/H$ היא ציקלית (אם a יוצר את $\mathbb{Z}_n$ אז aH יוצר את $\mathbb{Z}_n/H$). $\Leftarrow \mathbb{Z}_n/H \cong \mathbb{Z}_d$.

(14) 20.11.07
ת' מבנים

הערות לתרגיל ובכלל

* $N \lhd G$ אמ"מ לכל $g \in G$ $gNg^{-1}=N$
אמ"מ לכל $g \in G$ $gNg^{-1} \subseteq N$

הכיוון הלא טריוויאלי ראו הבו ש- $gNg^{-1} \subseteq N$ לכל g
צ"ל ש- $gNg^{-1}=N$. אבל מאחר שזה נכון לכל g
זה נכון בפרט ל- g^{-1} ולכן $g^{-1}Ng \subseteq N$ וע"י
העברת אגפים מתקבל $N \subseteq gNg^{-1}$ וסיימנו.

* שאלה 7: $H=\left\{\begin{pmatrix}1&n\\0&1\end{pmatrix} : n\in\mathbb{Z}\right\}$; $A_m=\begin{pmatrix}m&0\\0&1\end{pmatrix}$
כאן מראים שייתכן שעבור איבר מסויים $gHg^{-1} \subsetneq H$
אבל מרגע ש- H נורמלית לא ייתכן שזה נכון לכל האיברים.

* <u>הגדרה:</u> חבורה G תיקרא פשוטה אם היא לא מכילה אף תת חבורה נורמלית לא טריוויאלית.

* תהי G חבורה ; $K \le H \le G$ תתי חבורות.
אזי מתקיים $[G:K]=[G:H]\cdot[H:K]$
<u>הוכחה:</u> אם G סופית זה ברור כי לכל תת חבורה $F \le G$ $[G:F]\cdot|F|=|G|$
נוכיח למקרה ש- G אינסופית אבל האינדקסים סופיים.
נסמן ב- $g_1H,\dots,g_\ell H$ את המחלקות השמאליות של H ב- G.
נסמן ב- $h_1K,\dots,h_mK$ את המחלקות השמאליות של K ב- H.
אז נקבל שהאיחוד הזר של המחלקות הבאות נותן את G
$g_1h_1K,\dots,g_1h_mK,\ g_2h_1K,\dots,g_2h_mK,\dots,g_\ell h_1K,\dots,g_\ell h_mK$

לכן $\{g_i h_j K\}_{i=1,j=1}^{l,m}$ הן בדיוק כל המחלקות של K ב-H. (☺)

* הומומורפיזם $\varphi: G \to H$ הוא חח"ע אמ"מ $Ker\varphi = \{e\}$

חבורות מנה

עבור $N \trianglelefteq G$ ניתן להגדיר את חבורת המנה G/N שאיבריה הם המחלקות של N ב-G והכפל נתון ע"י
$$aN \cdot bN = abN$$
או באופן שקול לאמר ע"י הכפל נציגים מהמחלקות.

דוגמאות

① $G = \mathbb{Z}_n$; $H \leq \mathbb{Z}_n$ תת חבורה. ראינו כבר ש-H ציקלית ומאחר ש-G אבלית אז H נורמלית. אם $|H| = d$ אז G/H חבורה מסדר $\frac{n}{d}$ והיא ציקלית (תרגיל) לכן $G/H \cong \mathbb{Z}_{\frac{n}{d}}$ במקרה זה G/H איזומורפית לתת חבורה של G (התחבורה הנוצרת ע"י $d \in \mathbb{Z}_n$).

② אבל זה לא תמיד המקרה. למשל $G = \mathbb{Z}$; $H = n\mathbb{Z}$. אז $G/H \cong \mathbb{Z}_n$ אבל ברור שאין ל-$\mathbb{Z}$ תת חבורה איזומורפית ל-$\mathbb{Z}_n$.

③ $G = S_4$ $\quad V = \{id, (12)(34), (13)(24), (14)(23)\}$

G/V :
$$idV = V$$
$$(12)V = \{(12), (34), (1324), (1423)\}$$
$$(13)V = \{(13), (1234), (24), (1432)\}$$
$$(23)V = \{(23), (1342), (1243), (14)\}$$
$$(123)V = \{(123), (134), (243), (142)\}$$
$$(132)V = \{(132), (234), (124), (143)\}$$

אפשר להגדיר איזומורפיזם באופן מפורש ע"י

$$V \mapsto id$$
$$(12)V \mapsto (12)$$
$$(13)V \mapsto (13)$$
$$\vdots$$

האיזומורפיזם לא תלוי בבחירה המיוחדת בנציגים $\{id, (12), (13), \dots\}$. אפשר באותה להגדיר

$$(23)V \mapsto (12)$$
$$(24)V \mapsto (13)$$
$$\vdots$$

(4) $G=\mathbb{R}$; $N=\mathbb{Z}$. אז מספרים נמצאים באותה מחלקה אמ"מ ההפרש ביניהם שלם. אז בקטע $[0,1)$ ניתן למצוא נציג לכל אחד מהמחלקות.

מצד שני אפשר לחשוב על $[0,1]$ כאשר 0 ו-1 מזוהות אחת עם השנייה. אינטואיטיבית זה יוצא מעגל.

נתבונן בהעתקה $\varphi: \mathbb{R} \to S^1$ הנתונה ע"י $x \mapsto e^{2\pi i x}$

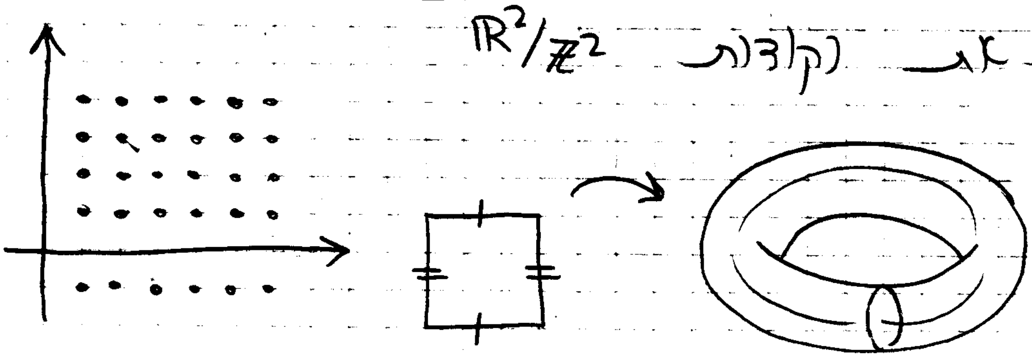
קל לראות שזה הומומורפיזם.

$$\operatorname{Ker}\varphi = \{x \in \mathbb{R} \,;\, \varphi(x) = 1\} =$$
$$= \{x \in \mathbb{R} \,;\, e^{2\pi i x} = 1\} = \mathbb{Z}$$

וכעת ממשפט ההומומורפיזם הראשון $\mathbb{R}/\mathbb{Z} \cong S^1$.

(5) $G=\mathbb{R}^2$ $H=\mathbb{Z}^2$ אלה חבורות חיבוריות.

ניתן לזהות את נקודות $\mathbb{R}^2/\mathbb{Z}^2$ עם הטורוס:



הגדרה: G חבורה ו- $a,b\in G$. נגדיר את **הקומוטטור** של a ו- b להיות $[a,b]=a^{-1}b^{-1}ab$

נשים ♡ ש- $[a,b]=1$ אמ"מ $ab=ba$.

הגדרה: תת חבורת הקומוטטור היא תת החבורה הנוצרת ע"י כל הקומוטטורים

$$G'=\langle [a,b] : a,b\in G \}$$

הערה: יתכן שהאוסף $\{[a,b]\}$ לא שווה ל- G (דוגמה ב- Rotman).

למה: $G' \triangleleft G$

הוכחה: נניח ש- $g\in G$ ו- $[a,b]\in G'$. אז

$$ga^{-1}b^{-1}abg^{-1}=ga^{-1}g^{-1}gb^{-1}g^{-1}gag^{-1}gbg^{-1}=$$
$$=[gag^{-1},gbg^{-1}]\in G'$$

הצמדה לוקחת יוצרים לתת החבורה לכן את את תת החבורה הנוצרת ע"י [..] וכו. ☺

⇐ מוגדרת חבורת המנה G/G'.

טענה: G/G' אבלית.

הוכחה: צריך להראות שלכל $a,b\in G$

$$(aG')^{-1}(bG')^{-1}(aG')(bG')=[aG',bG']=e_{G/G'}=G'$$

אבל

$$(aG')^{-1}(bG')^{-1}(aG')(bG')=(a^{-1}G')(b^{-1}G')(aG')(bG')=$$
$$=a^{-1}b^{-1}abG'=[a,b]G'=G'$$

↓ כי $[a,b]\in G'$.

☺

הגדרה: יהיו H, K חבורות. המכפלה הקרטזית $H\times K$ היא אוסף הזוגות (h,k) כאשר $h\in H$ $k\in K$ עם כפל קואורדינטה קואורדינטה.

דוגמה: $\mathbb{Z}_2\times\mathbb{Z}_2$ חבורה מסדר 4 והיא איזומורפית ל- $\mathbb{Z}_8^*$ או ל- V מקודם.

טענה: יהיו $m,n\in\mathbb{N}$ רק ש- $(m,n)=1$. אזי

$$\mathbb{Z}_n\times\mathbb{Z}_m \cong \mathbb{Z}_{nm}$$

הוכחה: נגדיר $\varphi:\mathbb{Z}_{nm}\longrightarrow\mathbb{Z}_n\times\mathbb{Z}_m$ ע"י

$$x \bmod nm \longmapsto (x \bmod n,\ x \bmod m)$$

ההעתקה מוגדרת היטב: אם $x'\equiv x \pmod{mn}$ צריך להראות ש- $x'\equiv x \pmod{n}$ וגם $x'\equiv x \pmod{m}$ כלומר $n \mid x-x'$ וגם $m\mid x-x'$ אבל זה ברור כי $nm \mid x-x'$.

ההגדרה חח"ע: נניח ש- $x\mapsto(0,0)$. אז $n\mid x$ וגם $m\mid x$ אז $bm=x=an$.

$\Leftarrow$ $[n,m]=lcm(n,m)\mid x$. אבל

$(n,m)[n,m]=nm \Leftarrow n\cdot m=[n,m] \Leftarrow nm\mid x$

$\Leftarrow$ $x\equiv 0 \pmod{mm}$. ברור ש- $0\mapsto(0,0)$

$\Leftarrow$ $\mathrm{Ker}\,\varphi=\{0\}$. לא קשה לראות ש- φ הומומורפיזם ולכן φ חח"ע.

מאחר שגודל החבורות זהה φ היא גם על ולכן איזומורפיזם!

אפשר להגדיר מכפלה קרטזית של כמה חבורות $G_1\times\dots\times G_n$ וקל לראות גם ש-

$$(G_1\times G_2)\times G_3 \cong G_1\times(G_2\times G_3)\cong G_1\times G_2\times G_3$$

טענה: יהיו $n_1, \dots, n_k$ מספרים זרים בזוגות.
אז $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k} \cong \mathbb{Z}_{n_1 \cdots n_k}$

אם $(n,m) \neq 1$ אז $\mathbb{Z}_n \times \mathbb{Z}_m \ncong \mathbb{Z}_{nm}$

דוגמה: אם p ראשוני אז $\mathbb{Z}_p \times \mathbb{Z}_p \ncong \mathbb{Z}_{p^2}$
למה? כל האיברים ב- $\mathbb{Z}_p \times \mathbb{Z}_p$ הם מסדר p ואילו
ב- $\mathbb{Z}_{p^2}$ יש איבר מסדר p^2!

נשים ♡ שיש הומומורפיזם חח"ע $H \longrightarrow H \times K$
$h \longmapsto (h,1)$

$K \longrightarrow H \times K$
$k \longmapsto (1,k)$

אז $H \cong H \times \{1\}$; $K \cong \{1\} \times K$
⇐ ניתן לזהות את H ו- K עם תת חבורות
של $H \times K$. למעשה, אלה תת חבורות נורמליות.
החבורות האלה יוצרות את $H \times K$ והחיתוך שלהן
טריוויאלי.

משפט: תהי G חבורה. H,K תת חבורות נורמליות
כך ש- $HK = G$; $H \cap K = \{e\}$ אזי $G \cong H \times K$.

הוכחה:

(א) כל איבר ב- G יש הצגה יחידה $g = hk$ כאשר $h \in H$
ו- $k \in K$: אם $hk = h_1 k_1$ אז $H \ni h_1^{-1} h = k_1 k^{-1} \in K$
⇐ $k_1 k^{-1}, h_1^{-1} h = e$ ⇐ $h = h_1$; $k = k_1$.
(הגדרה מתקבלת) $\varphi: G \longrightarrow H \times K$ חח"ע $hk \longmapsto (h,k)$

(ב) לכל $h \in H$, $k \in K$: $hk = kh$: נתבונן ב- $h^{-1}k^{-1}hk$

$h^{-1}kh \in K$ ⇐ $h^{-1}k^{-1}hk \in K$
$k^{-1}hk \in H$ ⇐ $h^{-1}k^{-1}hk \in H$
⇐ $[h,k] = e$

(ג) φ הומומורפיזם כי $hkh_1k_1 = hh_1kk_1$ ולכן
$\varphi(hk \cdot h_1k_1) = (hk, h_1k_1) = (h,k)\cdot(h_1,k_1) = \varphi(hk)\varphi(h_1k_1)$

(ד) קל לראות ש- φ חח"ע ועל.

(17) 27.11.07
ת' מבנים

<u>הערה</u>: משפט השאריות הסיני:
יהיו $n_1, \dots, n_k$ זרים בזוגות ויהיו $a_1, \dots, a_k$
שלמים כלשהם. אזי יש מספר שלם x רק ש-

$$x \equiv a_1 (\mathrm{mod}\ n_1)$$
$$\vdots$$
$$x \equiv a_k (\mathrm{mod}\ n_k)$$

למה? ראינו שאם $n_k, \dots, n_1$ זרים בזוגות אז
יש איזומורפיזם $\mathbb{Z}_{n_1 \cdot \dots \cdot n_k} \to \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}$
הנתון ע"י $(x \bmod \prod n_i) \longmapsto (x \bmod n_1, \dots, x \bmod n_k)$
אז במשפט השאריות הסיני אנחנו למעשה מחפשים
את המקור של $(a_1, \dots, a_k)$ תחת האיזומורפיזם
הזה. ומאחר שהוא על, אכן יש מקור!
נשים ♡ גם שכל הפתרונות שקולים מודולו $\prod n_i$
(הפתרון הוא אם יחיד מודולו $\prod n_i$)

תת חבורות אפייניות

<u>הגדרה</u>: תהי G חבורה, $H \leq G$ תת חבורה.
H תיקרא אפיינית (נסמן $H \,\mathrm{char}\, G$) אם
לכל $\varphi \in \mathrm{Aut}(G)$ $\varphi(H) \subseteq H$.

<u>תכונות</u>:
(א) אם H אפיינית אז $H \trianglelefteq G$ כי אם γ_g ההצמדה
ב-g אז γ_g אוטומורפיזם ולכן $\gamma_g(H) \subseteq H$
לכל $g \in G$.
(ב) אם $K \leq H \leq G$ ומתקיים $K \,\mathrm{char}\, H$, $H \,\mathrm{char}\, G$
אז $K \,\mathrm{char}\, G$: אם $\varphi \in \mathrm{Aut}(G)$ אז
$\varphi(H) \subseteq H$ לפי ההנחה. לכן ניתן להגדיר את
$\varphi|_H : H \to H$ וזה אוטומורפיזם ובו' ומר

$\varphi|_H \in Aut(H)$. $\Rightarrow$ $\varphi|_H(K) \subseteq K$.

$\Rightarrow$ $\varphi(K) \subseteq K$.

נשים לב שזה בניגוד למה שקורה בתת חבורות נורמליות. אם $H \lhd G$ ו- $K \lhd H$ אז לא בהכרח $K \lhd G$. למשל:

$$\{id,(12)(34)\} \lhd V \lhd S_4$$

אבל $\{id,(12)(34)\} \ntriangleleft S_4$!

(6) דוגמה לתת חבורה נורמלית שאינה אופיינית:

$G=\mathbb{Z}_2\times\mathbb{Z}_2$, $H=\{(0,0),(0,1)\}$

$H \lhd G$ כי זו תת חבורה מאינדקס 2.

מאידך נגדיר אוטומורפיזם של $\mathbb{Z}_2\times\mathbb{Z}_2$ ע"י

$$\left.\begin{aligned} \varphi(0,0)&=(0,0)\\ \varphi(0,1)&=(1,0)\\ \varphi(1,0)&=(0,1)\\ \varphi(1,1)&=(1,1) \end{aligned}\right\}$$

קל לראות שזה אכן אוטומורפיזם

אבל $\varphi(H) \not\subseteq H$.

דוגמה: $H \lhd G$ ו- $|G|=p^n m$ כאשר $(p,m)=1$ ו- $|H|=p^n$. אז H char G .

הוכחה: יהי $\varphi \in Aut(G)$. נתבונן ב- $H\varphi(H)$ - זו תת חבורה שהגודל שלה הוא

$$|H\varphi(H)| = \frac{|H||\varphi(H)|}{|H\cap\varphi(H)|} = \frac{|H|^2}{|H\cap\varphi(H)|} = \frac{p^{2n}}{|H\cap\varphi(H)|}$$

אם $|H\cap\varphi(H)|<p^n$ נקבל שתת החבורה $H\varphi(H)$ היא מסדר p^k עבור $n<k$ בסתירה לכך ש $|G|=p^n\cdot m$ ו- $p\nmid m$

לכן $|H\cap\varphi(H)|=p^n \Rightarrow H=\varphi(H)$

(10)

תרגיל: אם $H \triangleleft G$ ומתקיים $(|H|, [G:H]) = 1$ אזי $H \text{ char } G$.

הגדרה: תהי G חבורה. G תיקרא פתירה אם יש סדרה נורמלית $G \triangleright G_1 \triangleright G_2, \dots, \triangleright G_n = \{1\}$ כך שהמנות G_i/G_{i+1} הן אבליות.

טענה:

(א) אם G פתירה ו-$H \le G$ אז H פתירה.

(ב) אם G פתירה ; $H \triangleleft G$ אז G/H פתירה.

(ג) אם G חבורה, $H \triangleleft G$ פתירה ; G/H פתירה אז G פתירה.

הגדרה: חבורות הקומוטטור הגבוהות:

נגדיר באינדוקציה
$$\begin{cases} G^{(0)} = G \\ G^{(i+1)} = (G^{(i)})' \end{cases}$$

מקבלים סדרה יורדת... $G \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \dots \triangleright G^{(i)} \triangleright \dots$

בפרט, אם יש n שעבורו $G^{(n)} = \{1\}$ נקבל סדרה נורמלית.

הערה: $G^{(i)} \text{ char } G$ ובפרט $G^{(i)} \triangleleft G$

הוכחה: $G' \text{ char } G$ כי אם $\varphi \in Aut(G)$ אז

$$\varphi([a,b]) = \varphi(a^{-1}b^{-1}ab) = \varphi(a)^{-1}\varphi(b)^{-1}\varphi(a)\varphi(b) = [\varphi(a), \varphi(b)]$$

(11)

ועכשיו באינדוקציה $G^{(i)} \text{ char } G$

למה: אם $G \triangleright G_1 \triangleright \dots \triangleright G_n = \{1\}$ סדרה פתירה (כלומר סדרה נורמלית כך ש- G_i/G_{i+1} אבליות) אז $G_i \ge G^{(i)}$ לכל i.

הוכחה: באינדוקציה: עבור $i=0$: $G_0 = G^{(0)} = G$

נניח ש- $G_i \ge G^{(i)}$ ונראה ש- $G_{i+1} \ge G^{(i+1)}$

$G^{(i+1)} = (G^{(i)})' \le G_{i+1}$

כי $G_i \ge G^{(i)}$ ולכן $G_i' \ge G^{(i+1)}$ אבל

$G_i' \le G_{i+1}$ כי G_i/G_{i+1} אבלית ומתרגיל ראינו

שאם G/H אבלית אז $G' \subseteq H$. $\Leftarrow$ $G^{(i+1)} \le G_{i+1}$

☺

<u>משפט:</u> G חבורה פתירה אמ"מ הסדרה הנגזרת יורדת ל- $\{1\}$, כלומר יש $n \in \mathbb{N}$ כך ש- $G^{(n)} = \{1\}$

<u>הוכחה:</u> אם הסדרה הנגזרת יורדת ל- $\{1\}$ אז זו סדרה נורמלית עם מנות אבליות, כלומר היא פתירה.

אם G פתירה אז יש סדרה פתירה $G \rhd G_1 \rhd \dots \rhd G_n = \{1\}$ ומתקיים $G^{(n)} \le G_n$. $\Leftarrow$ $G^{(n)} = \{1\}$. ☺

(א) אם G פתירה; $H \le G$ אז H פתירה.

<u>הוכחה:</u> קל: מתקיים $H^{(i)} \le G^{(i)}$.

לכן אם $G^{(n)} = \{1\}$ גם $H^{(n)} = \{1\}$. ☺

(ב) אם G פתירה; $H \lhd G$ אז G/H פתירה

<u>הוכחה:</u> תהי $\nu : G \to G/H$ ההעתקה הטבעית.

אז נתבונן ב- $\nu(G) \rhd \nu(G') \rhd \dots \rhd \nu(G^{(n)})$ ($G^{(n)} = \{1\}$). אז קל לראות ש- $\nu(G^{(i)}) = (\nu(G))^{(i)}$ ושיש $m \in \mathbb{N}$ כך שעבורו

$(\nu(G))^{(m)} = \nu(G^{(m)}) = \{1\}$ ☺

(ג) אם $H \lhd G$ פתירה; G/H פתירה אז G פתירה

<u>הוכחה:</u> $(G/H) \rhd (G/H)^{(1)} \rhd \dots \rhd (G/H)^{(n)} = \{1\}$

$H \rhd H^{(1)} \rhd \dots \rhd H^{(m)} = \{1\}$

כמו בטענה $(G/H)^{(i)} = \nu(G^{(i)})$ לכן $G^{(n)} \le H$

(כי $\nu(G^{(n)}) = \{1\}$ בחבורת המנה.)

מכיוון ש- $H^{(m)}=\{1\}$ נובע ש- $(G^{(n)})^{(m)}=\{1\}$

אבל $G^{(n+m)} \le (G^{(n)})^{(m)}$ (תרגיל באינדוקציה על m)

$\Rightarrow G^{(n+m)}=\{1\} \Rightarrow G$ פתירה ☺

<u>טענה:</u> A_5 חבורה פשוטה.

<u>הוכחה:</u> $|A_5|=60$. מהם איברי A_5?

id - 1

מחזורים באורך 3 - 20

מחזורים באורך 5 - 24

מכפלות של שני חילופים זרים - 15

(א) כל ה-3-מחזורים צמודים ב-A_5 כי לכל מחזור σ באורך 3 יש חילוף המתחלף איתו (זר) לכן $C_{A_5}(\sigma) \neq C_{S_5}(\sigma)$. לכן $[S_5:A_5]=2$ ראשוני (מתרגיל נכונות שאם $H \triangleleft G$, $[G:H]$ ראשוני ואם ל- $x \in H$ מתקיים $C_H(x) \neq C_G(x)$ אז $|x^G|=|x^H|$)

$\Rightarrow$ מחלקת הצמידות של σ ב-A_5 שווה למחלקת הצמידות ב-S_5.

(ב) כל המכפלות של חילופים זרים נמצאות באותה מחלקת צמידות ב-A_5:
לכל מכפלה של חילופים זרים יש חילוף המתחלף איתה (למשל $(12)(34)\cdot(34)=(34)\cdot(12)(34)$)
לכן ב' נובע מאותו טיעון כמו א'.

(ג) יש שתי מחלקות צמידות של 5-מחזורים, שתיהן מגודל 12. ראינו מתרגיל שאם $\sigma \in S_n$ n-מחזור אז $C_{S_n}(\sigma)=\langle\sigma\rangle$

בפרט, אם σ 5-מחזור אז $|C_{S_5}(\sigma)|=5$

אבל בתרגיל ראינו ש- $|G|=|x^G||C_G(x)|$

ובמקרה שלנו $|C_{A_5}(\sigma)||\sigma^{A_5}| = |A_5| = 60$

$\underbrace{|C_{A_5}(\sigma)|}_{5}$

$\Leftarrow \quad |\sigma^{A_5}| = 12$.

לכן גודלי מחלקות הצמידות הם $1, 12, 12, 15, 20$

תת חבורה נורמלית לא טריוויאלית היא איחוד
של מחלקות צמידות. לכן הסדר שלה הוא
סכום של 1 ועוד מספרים מהרשימה. כמו כן,
הסדר שלה מחלק את 60.
בדיקה מעלה שאין סכום כזה המחלק את
60 (פרט לסכום הכולל).

(20) 4.12.07

ת' אבנים.

<u>הגדרה:</u> תהי G חבורה מסדר $p^n m$ כאשר p ראשוני ו-$(p,m)=1$. אז תת חבורת p-סילו היא תת חבורה מסדר p^n.

<u>משפט:</u> תהי G חבורה מסדר $p^n m$ כאשר p ראשוני ו-$(p,m)=1$. אז קיימת ל-G תת חבורת p-סילו.

<u>למה:</u> $p \nmid \binom{p^n m}{p^n}$ כאשר p ראשוני ו-$(p,m)=1$.

<u>הוכחה:</u>

$$\binom{p^n m}{p^n} = \frac{(p^n m)!}{(p^n)!} = \frac{p^n m\,(p^n m-1)\cdots(p^n m-i)\cdots(p^n m-(p^n-1))}{p^n\,(p^n-1)\cdots(p^n-i)\cdots(p^n-(p^n-1))}$$

נראה שאם $p^k | (p^n m-i)$ אז $p^k | (p^n-i)$. לכן כל גורם p בפירוק של המונה לגורמים ראשוניים מצטמצם ע"י גורם במכנה.

ראשית, אם $p^k | p^n m-i$ אז $0 \le k \le n$ (תרגול).

אם $p^k | p^n m-i$ אז $p^k | i$ $\Leftarrow$ $p^k | p^n-1$. (11)

<u>החבורה הדיהדרלית</u> - נתון מצולע משוכלל Δ עם n צלעות. נתבונן בחבורה G של כל ההעתקות הצפופות (איזומטריות) רק ש- $g(\Delta)=\Delta$ לכל $g \in G$. בה"כ (נניח שמרכז הכובד) נמצא על הראשית ויש קודקוד על ציר ה-x. $\Leftarrow$ $G \le O(2)$.

<u>טענה:</u> חבורת הסימטריות של Δ היא חבורה מסדר $2n$ הנוצרת ע"י שני איברים S,T המקיימים $T^2=1$, $S^n=1$ ו- $TST=S^{-1}$.

<u>הוכחה:</u> G פועלת על הצלעות של Δ. מכיוון שאורכי הצלעות שווים הפעולה טרנזיטיבית (כלומר יש רק מסלול אחד). גודל המסלול הוא מספר הצלעות n. גודל המייצב של צלע הוא 2 (זהות או שיקוף). לכן $|G|=2n$.

יהי S סיבוב בזווית $\frac{2\pi}{n}$ (נגד השעון) ויהי T שיקוף ביחס לציר ה-x. $\Leftarrow$ בוודאי $S^n=1$ ו- $T^2=1$. קל לראות ש- $TST=S^{-1}$ (לרשום כמטריצות).

$G=\langle S,T\rangle$ כי $n=|\langle S\rangle|$ ו- $T\notin\langle S\rangle$. לכן יש
יותר מ-n איברים ב-G שהיא חבורה מסדר 2n. ☺

סימון: נסמן את חבורת הסימטריות של מצולע עם n צלעות ב-D_{2n} (או D_n) והיא נקראת החבורה הדיהדרלית.

מסקנה: $D_{2n}=\{T^iS^j : i=0,1,\ j=0,1,\dots,n-1\}$

הוכחה: כל איבר ב-D_{2n} ניתן להציג כ-
$S^{i_1}TS^{i_2}\cdots TS^{i_k}$ או $TS^{i_1}TS^{i_2}T\cdots TS^{i_k}$ וכו'
אבל מהיחס $TST=S^{-1}$ מתקבל שאפשר להציג כל איבר כ- T^iS^j כאשר $i=0,1$ ו- $j=0,\dots,n-1$
וברור שאלה בדיוק 2n איברי החבורה. ☺

משפט (ללא הוכחה): תהי G חבורה סופית ו- $a,b\in G$ איברים מסדר 2. אז $\langle a,b\rangle\cong D_{2n}$ ל-n כלשהו.

דוגמה: בתרגול הקודם ראינו ש- $H=\langle(13),(1234)\rangle\le S_4$ היא חבורה מסדר 8. $|S_4|=24=2^3\cdot 3$ לכן H חבורת 2-סילו של S_4.
$H\cong D_8$ (חבורת הסימטריות של הריבוע). האיבר שמחליף את 1 ו-3 הוא שיקוף בציר ה-x והאיבר שמתאים ל-(1234) הוא רבע סיבוב נגד השעון.

חבורות נילפוטנטיות

הגדרה: תהי G חבורה ו- $H,K\le G$ תת חבורות. נסמן
$[H,K]=\langle\{[h,k] : h\in H,\ k\in K\}\rangle$

הגדרה: סדרה מרכזית יורדת. נגדיר באינדוקציה:
$\gamma_1(G)=G$
$\gamma_{i+1}(G)=[\gamma_i(G),G]$

לא קשה לראות ש- $\gamma_i(G)$ char G, שהרי אם $\varphi \in Aut(G)$

אז $\varphi([g_1,g_2]) = [\varphi(g_1), \varphi(g_2)]$

בפרט $\gamma_i(G) \trianglelefteq G$ ומאוד קל לראות ש- $\gamma_{i+1}(G) \le \gamma_i(G)$.

הסדרה המרכזית היורדת היא הסדרה

$$G = \gamma_1(G) \ge \gamma_2(G) \ge \dots$$

<u>הגדרה</u>: הסדרה המרכזית העולה. נגדיר באינדוקציה:

(zeta) $\zeta^{(0)}(G) = 1$

בהינתן $\zeta^{(i)}(G)$ נתבונן במנה $G/\zeta^{(i)}(G)$. ישנה

יהי $Z(G/\zeta^{(i)}(G))$ המרכז של חבורת המנה. משפט ההתאמה

יש תת חבורה של G שנסמנה $\zeta^{(i+1)}(G)$ כך ש- $\zeta^{(i)}(G) \le \zeta^{(i+1)}(G)$

ו- $\zeta^{i+1}(G)/\zeta^{i}(G) \cong Z(G/\zeta^{i}(G))$. בפרט $\zeta^1(G) = Z(G)$.

הסדרה המרכזית העולה היא

$$\{1\} = \zeta^{(0)}(G) \le \zeta^{(1)}(G) \le \dots$$

<u>משפט</u>: אם G חבורה אז קיים $c \in \mathbb{N}$ רק ש- $\zeta^{(c)}(G) = G$ אמ"מ $\gamma_{c+1}(G) = \{1\}$

<u>הוכחה</u>: נראה שאם קיים c כנ"ל אז מתקיים

$$\forall i \quad \gamma_{i+1}(G) \le \zeta^{c-i}(G)$$

בפרט $\gamma_{c+1}(G) \le \zeta^{(0)}(G) = \{1\}$ או $G = \gamma_1(G) \le \zeta^{(c)}(G)$

(לשם הקיצור נכתוב מעכשיו ζ^i ו- ! γ_{i+1})

נניח תחילה ש- $G = \zeta^c$. נוכיח את הטענה באינדוקציה

על i. אם $i=0$ אז $G = \gamma_1 \le \zeta^c = G$

נניח $\gamma_{i+1} \le \zeta^{c-i}$ אז

$$\gamma_{i+2} = [\gamma_{i+1}, G] \le [\zeta^{c-i}, G]$$

<u>למה</u>: אם $K \trianglelefteq G$, $K \le H \le G$ אז

$$H/K \le Z(G/K) \iff [H,G] \le K$$

<u>הוכחה</u>: אם $h \in H$, $g \in G$ אז

$$[h,g]K = K \iff gKhK = hKgK \iff [h,g] \in K$$

לכן $[H,K] \le K \iff gkhk = hkgk$ לכל $h \in H$, $g \in G$.
כלומר $H/K \le Z(G/K)$.

נחזור להוכחת המשפט. ניקח $K = \xi^{c-i-1}$, $H = \xi^{c-i}$ אז
מההגדרה $H/K = Z(G/K) \Leftarrow [\xi^{c-i}, G] \le \xi^{c-i-1}$ לכן

$$\gamma_{i+2} \le [\xi^{c-i}, G] \le \xi^{c-i-1}$$

אגף שני, נניח ש- $\gamma_{c+1}(G) = \{1\}$. נוכיח את הטענה באינדוקציה. נראה ש- $\gamma_{c+1-j} \le \xi^j$ לכל j

עבור $j=0$: $\{1\} = \gamma_{c+1} = \xi^0 = \{1\}$

נניח ש- $\gamma_{c-(j-1)} = \gamma_{c-j+1} \le \xi^j$ אז

$$[\gamma_{c-j}, G] = \gamma_{c+1-j} \underset{\text{ה"א}}{\le} \xi^j$$

לכן לפי הלמה נקבל ש-

$$\gamma_{c-j}\xi^j / \xi^j \le Z(G/\xi^j)$$

(כי $[\gamma_{c-j}\xi^j, G] \le \xi^j$ ו- $\xi^j \le \gamma_{c-j}\xi^j$)

ממשפט ההתאמה $\gamma_{c-j}\xi^j \le \xi^{j+1}$ ולכן

$$\gamma_{c-j} \le \xi^{j+1}$$

הגדרה: חבורה G נקראת <u>נילפוטנטית</u> אם הסדרה המרכזית העולה עולה ל- G (יש $c \in \mathbb{N}$ עבורו $\xi^c(G) = G$) או הסדרה המרכזית היורדת יורדת ל- $\{e\}$ (יש $c \in \mathbb{N}$ רק ש- $\gamma_{c+1}(G) = \{e\}$).
c המינימלי נקרא <u>מחלקת הנילפוטנטיות</u> של G.

<u>דוגמאות</u>

א) G נילפוטנטית ממחלקה 1 אמ"מ G אבלית, שהרי G אבלית אמ"מ $G = \xi^1(G) = Z(G)$

ב) G נילפוטנטית ממחלקה 2 אמ"מ

$$\gamma_2(G) = G' \le Z(G) = \xi^1(G)$$

בפרט חבורה לא אבלית מסדר p^3 היא ממחלקה 2.

משפט: חבורת-p (סופית) היא נילפוטנטית.

הוכחה: יהי $\xi^i(G) \neq G$ אז $G/\xi^i(G)$ חבורת p

ולכן $Z(G/\xi^i(G)) \neq 1$ ולכן $\xi^i(G) \neq \xi^{i+1}(G)$

מכיוון ש- G סופית בשלב מסוים נקבל $G = \xi^c(G)$. ☺

משפט:

א) חבורה נילפוטנטית היא פתירה

ב) אם $G \neq \{1\}$ נילפוטנטית אז $Z(G) \neq \{e\}$

הוכחה:

א) מאינדוקציה מראים ש- $G^{(i)} \leq \gamma_i(G)$ כאשר $G^{(i)}$ החבורה הנגזרת ה- i.

ב) עבור G כנ"ל $\gamma_{c+1}(G) = \{1\}$, $\gamma_c(G) \neq \{1\}$ עבור c כלשהו. מהמשפט שהוכחנו $\gamma_c(G) \leq \xi^1(G) = Z(G)$

$\Leftarrow$ $Z(G) \neq \{1\}$. ☺

דוגמה: S_3 חבורה פתירה כי $S_3 \rhd A_3 \rhd \{1\}$ סדרה נורמלית! - $S_3/A_3 \cong \mathbb{Z}_2$; $A_3/\{e\} \cong \mathbb{Z}_3$.

מאידך S_3 אינה נילפוטנטית כי $Z(S_3) = \{1\}$.

כנ"ל, עבור S_4 ש- $S_4 \rhd A_4 \rhd V \rhd e$ פתירה אבל לא נילפוטנטית כי $Z(S_4) = 1$.

טענה: (תרגיל)

א) אם G נילפוטנטית $H \leq G$ אז H נילפוטנטית.

ב) אם G נילפוטנטית $H \lhd G$ אז G/H נילפוטנטית.

דוגמה: $G = S_3$ $H = A_3$ אז $A_3 \cong \mathbb{Z}_3$ נילפוטנטית.

$S_3/A_3 \cong \mathbb{Z}_2$ נילפוטנטית אבל G אינה נילפוטנטית.

דוגמה: יהי F שדה; $U_n(F)$ חבורת המטריצות האוניפוטנטיות.

אם F שדה סופי אז $U_n(F)$ חבורת p ולכן נילפוטנטית.

אפשר להראות שזה נכון גם לשדה F אינסופי.

(23) 11.12.07

ת' מבנים

<u>משפט</u>: G חבורה ; $a,b\in G$ מסדר 2.
אז קיים n כך ש- $\langle a,b\rangle \cong D_{2n}$

D_{2n} היא חבורת הסימטריות של מצולע בן n צלעות.
מה זה מצולע עם שתי צלעות? לא ממש ברור
למרות שגם בודקים סימטריות של קטע $[-1,1]$
יש היגיון במה שקורה שם...

<u>תזכורת</u>:

(א) G חבורה. הסדרה המרכזית היורדת מוגדרת ע"י

$$\gamma_0(G)=G$$
$$\gamma_{i+1}(G)=[\gamma_i(G),G]$$

(ב) הסדרה המרכזית העולה מוגדרת ע"י

$$\zeta^{i+1}(G)/\zeta^i(G)=Z(G/\zeta^i(G))$$
$$\zeta^0(G)=\{e\}$$

(ג) יש $c\in\mathbb{N}$ כך ש- $\gamma_{c+1}(G)=\{e\}$ אמ"מ $\zeta^c(G)=G$

<u>הגדרה</u>: חבורה G שעבורה קיים $c\in\mathbb{N}$ כך ש- $\gamma_{c+1}(G)=\{e\}$ נקראת נילפוטנטית

<u>טענה</u>: אם H,K נילפוטנטיות אז $H\times K$ נילפוטנטית

<u>הוכחה</u>: אפשר להראות באינדוקציה ש-

$$\gamma_i(H\times K)=\gamma_i(H)\times\gamma_i(K)$$

ואז המקסימום מבין ה- c-ים שמתאימים ל- H,K יתאים ל- $H\times K$. ☺

<u>מסקנה</u>: מכפלה קרטזית של חבורות p (לא דווקא אותו p) היא נילפוטנטית.

טענה: תהי G חבורה. אזי התנאים הבאים שקולים

א) $G \cong H_1 \times \dots \times H_n$

ב) $H_1, \dots, H_n$ תת חבורות נורמליות של G כך ש- $G = \langle \bigcup_{i=1}^{n} H_i \rangle$, $\{e\} = H_i \cap \langle \bigcup_{j \neq i} H_j \rangle$

ג) $H_1, \dots, H_n$ ב- G לכל $a \in G$ הצגה יחידה כ- $a = h_1 h_2 \cdots h_n$, $h_i \in H_i$

הוכחה:

(א ⟸ ב, ג) נזהה את H_i עם תת החבורה $\{e\} \times \dots \times \{e\} \times H_i \times \{e\} \times \dots \times \{e\}$ ומשם מקבלים תת חבורות נורמליות (קל להראות). ברור ש- $G = \langle \bigcup H_i \rangle$ כי $(h_1, \dots, h_n) = (h_1, e, \dots, e) \cdot \ldots \cdot (e, \dots, e, h_n)$

ו- $e = H_i \cap \langle \bigcup_{j \neq i} H_j \rangle$.

קל גם לראות שההצגה היא יחידה.

(ב ⟸ ג) ברור ש- $G = \langle \bigcup H_i \rangle = H_1 \cdots H_n$

⟸ לכל $a \in G$ קיימת הצגה $a = h_1 \cdots h_n$.

נניח ש- $\bar{h}_1 \bar{h}_2 \cdots \bar{h}_n = a = h_1 h_2 \cdots h_n$.

⟸ $H_1 \ni \bar{h}_1^{-1} h_1 = \bar{h}_2 \cdots \bar{h}_n (h_2 \cdots h_n)^{-1} \in \langle \bigcup_{j \neq 1} H_j \rangle$

⟸ $\bar{h}_1^{-1} h_1 = e$ ⟸ $\bar{h}_1 = h_1$

⟸ $h_2 \cdots h_n = \bar{h}_2 \cdots \bar{h}_n$. ועכשיו באינדוקציה $\bar{h}_i = h_i$ לכל $1 \le i \le n$.

(ג ⟸ א) נגדיר העתקה $\varphi : G \longrightarrow H_1 \times \dots \times H_n$

$a \longmapsto (h_1, \dots, h_n)$

כאשר $a = h_1 h_2 \cdots h_n$ ההצגה היחידה של a.

לפי ההנחה φ מוגדר היטב והוא חח"ע ועל. רק צריך להראות שזה הומומורפיזם.

אם $h_j h_i = h_i h_j$ לכל i, j אז נסיים כי:

$$h_1 \cdots h_n \bar{h}_1 \cdots \bar{h}_n = h_1 \bar{h}_1 \cdots h_n \bar{h}_n \longmapsto (h_1 \bar{h}_1, \dots, h_n \bar{h}_n) =$$

$$= (h_1, \dots, h_n)(\bar{h}_1, \dots, \bar{h}_n)$$

אז נראה שכל שני איברים מתחלפים:

$$[h_i,h_j] = \overbrace{h_i \underbrace{h_j h_i^{-1}}_{} h_j^{-1}}^{\in H_i} \in H_i \cap H_j \qquad (h_i h_j h_i^{-1} \in H_j)$$

נניח ש- $a \in H_i \cap H_j$, אז $h_j = a = h_i$.

$\Leftarrow$ $h_i^{-1} h_j = e$. אבל ל- e יש הצגה יחידה $\Leftarrow$ $h_i = h_j = e$ $\Leftarrow$ $[h_i,h_j] = e$

$\Leftarrow$ h_i , h_j מתחלפים. (:

יהי F שדה. $U_n(F)$ חבורת המטריצות האוניפוטנטיות $n\times n$. אם F סופי אז $q=|F|=p^e$ אז $|U_n(F)| = q^{\frac{n(n-1)}{2}}$ ולכן $U_n(F)$ חבורת p ובפרט נילפוטנטית.

<u>טענה</u>: לכל שדה F $U_n(F)$ נילפוטנטית.

<u>הוכחה</u>: נגדיר $E_{ij}(\lambda)$ המטריצה שכולה אפסים פרט למקום ה- i,j שבו יש λ.

נגדיר $e_{i,j}(\lambda) = I_n + E_{ij}(\lambda)$.

$$e_{ij}(\lambda) = \begin{pmatrix} 1 & & \lambda \\ & \ddots & \vdots \\ & & 1 \end{pmatrix}$$

כפל משמאל ב- $e_{ij}(\lambda)$ של מטריצה A שקול להוספת λ פעמים השורה ה- j לשורה ה- i.

$$U = \begin{pmatrix} 1 & a_{12} & a_{13} & \cdots & a_{1n} \\ & 1 & a_{23} & \cdots & a_{2n} \\ & & & \ddots & \\ & 0 & & & 1 \end{pmatrix}$$

בתהליך דירוג גאוס של U מחסירים כפולות של שורה j משורה i עבור $i<j$ וזה שקול לכפל במטריצות $e_{ij}(\lambda)$ עבורן $\lambda \in F$; $i<j$

<u>הערה</u>: $(e_{ij}(\lambda))^{-1} = e_{ij}(-\lambda)$

קיבלנו ש- $e_{i_1j_1}(\lambda_1)\cdots e_{i_nj_n}(\lambda_n)\, u = I$

$\Leftarrow$ $u = e_{i_nj_n}(-\lambda_n)\cdots e_{i_1j_1}(-\lambda_1)$

$\Leftarrow$ האוסף $\{e_{ij}(\lambda)\}_{i<j,\ \lambda\in F}$ יוצר את $U_n(F)$.

קל לראות ש- $E_{ij}(\lambda)\cdot E_{kl}(\mu) = \delta_{jk}E_{il}(\lambda\mu)$

$$e_{ij}(\lambda)\, e_{kl}(\mu) = (I+E_{ij}(\lambda))(I+E_{kl}(\mu)) = I + E_{ij}(\lambda) + E_{kl}(\mu) + \delta_{jk}E_{il}(\lambda\mu)$$

$$[e_{ij}(\lambda), e_{kl}(\mu)] = (I+E_{ij}(-\lambda)+E_{kl}(-\mu)+\delta_{jk}E_{il}(\lambda\mu))(I+E_{ij}(\lambda)+E_{kl}(\mu)+\delta_{jk}E_{il}(\lambda\mu)) = I - \delta_{il}E_{kj}(\lambda\mu) + \delta_{jk}E_{il}(\lambda\mu)$$

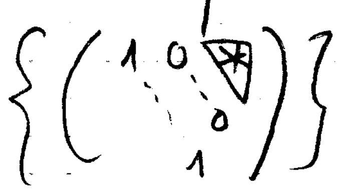
$$\Rightarrow [e_{ij}(\lambda), e_{kl}(\mu)] = \begin{cases} I & j\neq k \quad i\neq l \\ e_{kj}(\lambda\mu) & j\neq k \quad i=l \\ e_{il}(\lambda\mu) & i\neq l \quad j=k \end{cases}$$

האפשרות $i=l$, $j=k$ לא קיימת כי אז $i<j=k<l=i$

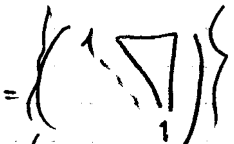
במקרה $i=l$, $j\neq k$ אז $k<i<j$ בפרט $k+1<j$

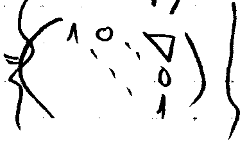
במקרה $i\neq l$, $j=k$ אז $i<j<l$ בפרט $i+1<l$

$\Leftarrow$ $U_n'(F) = G' = [G,G]$ נוצר ע"י איברים $e_{ij}(\lambda)$ כאשר $i+1<j$. לכן

$G' =$ 

באינדוקציה $\gamma_{i+1}(G) = [\gamma_i(G), G]$ נוצר ע"י $e_{ij}(\lambda)$ עבור $i+r<j$

$\gamma_1(G) =$ 

$\gamma_2(G) =$ 

$\vdots$

$\gamma_n(G) = \{I\}$ $\Rightarrow$ G נילפוטנטית

$T_n(F)$ = מטריצות הפיכות משולשיות עליונות
$D_n(F)$ = מטריצות הפיכות אלכסוניות.

נגדיר הומומורפיזם $\varphi : T_n(F) \to D_n(F)$ ע"י

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ & a_{22} & & \vdots \\ 0 & & \ddots & \\ & & & a_{nn} \end{pmatrix} \longmapsto \begin{pmatrix} a_{11} & & 0 \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix}$$

$\operatorname{Ker}\varphi = U_n(F)$.

$D_n(F)$ אבלית ובפרט נילפוטנטית ופתירה

$U_n(F)$ נילפוטנטית ולכן פתירה.

$T_n/U_n \cong D_n \Leftarrow T_n$ פתירה.

אבל T_n לא נילפוטנטית. אפשר לראות
ש- $[T_n, T_n] = U_n$ אבל $[U_n, T_n] = U_n$

$\Leftarrow U_n = \gamma_2(T_n) = \gamma_3(T_n) = \dots$

$\Leftarrow$ הסדרה מתייצבת ולכן T_n לא נילפוטנטית.

<u>טענה</u>: אין חבורה פשוטה מסדר 12

<u>הוכחה</u>: נזכיר שאם p ראשוני, חבורת p-סילו יחידה אז היא נורמלית.

$12 = 2^2 \cdot 3 \Leftarrow$ מספר חבורות 3-סילו הוא 1 או 4
נניח שחבורת 3-סילו אינה יחידה. אז יש 4 חבורות 3 סילו. החיתוך של שתי חבורות 3-סילו הוא טריוויאלי. $\Leftarrow$ ב- G יש $2\cdot 4 = 8$ איברים מסדר 3.
אם יש יותר מחבורת 2-סילו יחידה אז יש 3.
החיתוך של שתי חבורות 2-סילו מכיל לכל היותר 2 איברים. $\Leftarrow$ יש יותר מ-3 איברים מסדר 2 או 4.
יחד עם היחידה נקבל שב- G יש לפחות 13 איברים וזו סתירה.

הוכחה אלטרנטיבית לקיום תת חבורת p-סילו לחבורה G:

<u>למה</u> תהי G חבורה ונניח של-G יש תת חבורת p-סילו.
תהי $H\leq G$. אז גם ל-H יש תת חבורה p-סילו.

<u>הוכחה:</u> תת חבורת p-סילו P היא חבורה מסדר p^{s} רק ש-$p\nmid[G:P]$. בתרגול הוכחנו שאם $P,H\leq G$ מתקיים

$$[P:H]=\sum_{i=1}^{n}[H:H\cap g_i^{-1}Pg_i]$$

$p\nmid[G:P]$ לכן יש i עבורו $p\nmid[H:H\cap g_iPg_i^{-1}]$. $H\cap g_iPg_i^{-1}$ תת חבורת-p (כי היא תת חבורה של $g_iPg_i^{-1}$) ו-$p\nmid[H:H\cap g_iPg_i^{-1}]$ ⟸ $H\cap g_iPg_i^{-1}$ היא תת חבורת p-סילו של H.

(:

<u>הוכחת משפט סילו:</u> בתרגול ראינו שמטריצות התמורות ב-$GL_n(F)$ הן תת חבורה איזומורפית ל-S_n. לכן ממשפט קיילי כל חבורה ניתן לשכן ב-$GL_n(F)$ עבור n כלשהו. נבחר $F=\mathbb{Z}_p$. ראינו בעבר ש-$|GL_n(\mathbb{Z}_p)|=p^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}(p^i-1)$ ⟸ $U_n(\mathbb{Z}_p)$ היא תת חבורה p-סילו של $GL_n(\mathbb{Z}_p)$. (כי הסדר שלה $p^{\frac{n(n-1)}{2}}$).
מהלמה גם ל-G יש תת חבורת p-סילו.

(:

(26) 18.12.07
תר׳ מבנים

תזכורת והשלמות - חבורות אבליות

<u>הגדרה:</u> חבורה אבלית A נקראת חופשית על קבוצה $A \supseteq X$ אם כל פונקציה $f: X \to G$ לתוך חבורה אבלית G ניתנת להרחבה באופן יחיד להומומורפיזם $\varphi: A \to G$.

<u>טענה:</u> התנאים הבאים שקולים:

(א) A חופשית על X

(ב) כל $g \in A$ ניתן לכתיבה באופן יחיד כ- $g = \sum m_i x_i$ $m_i \in \mathbb{Z}$ $x_i \in X$ (X בסיס)

(ג) $A \cong \bigoplus_{i \in I} \mathbb{Z}$ (במקרה הסופי $A \cong \mathbb{Z}^n$)

<u>הערה:</u> יהיו $\{G_i\}_{i \in I}$ חבורות. אז

$$\prod_{i \in I} G_i = \{ f: I \to \bigcup G_i \ : \ f(i) \in G_i \ \forall i \}$$

$$\bigoplus_{i \in I} G_i = \{ f: I \to \bigcup G_i \ : \ f(i) = e_{G_i} \ \text{פרט למספר סופי של אינדקסים שבהם } f(i) \in G_i \}$$

במקרה של מכפלה / סכום ישר סופיים ההגדרות מתלכדות.

<u>משפט:</u> תהי A חבורה אבלית חופשית על בסיס $\{a_1, \dots, a_n\}$, $B \leq A$ תת חבורה. אז יש בסיס $\{\bar{\alpha}_1, \dots, \bar{\alpha}_n\}$ של A כך ש- $B = \langle m_1 \bar{\alpha}_1, \dots, m_k \bar{\alpha}_k \rangle$ עבור $k \leq n$ ו- $m_1 | m_2 | \dots | m_k$.

<u>דוגמאות:</u> (1) $A = \mathbb{Z}^2$ עם הבסיס הסטנדרטי. $B = \{(m,m) : m \in \mathbb{Z}\}$ אז

$\bar{\alpha}_1 = (1,1)$, $\bar{\alpha}_2 = (1,0)$ בסיס ל- A

$B = \langle 1 \cdot \bar{\alpha}_1 \rangle$!

(2) $A = \mathbb{Z}^2$ $B = \{(m,n) : 2 | (m+n)\}$. ק. לראות ש- B תת חבורה.
אפשר לבחור למשל $\bar{\alpha}_1 = (-1,1)$ $\bar{\alpha}_2 = (1,0)$ $B = \langle 1\bar{\alpha}_1 \rangle \oplus \langle 2\bar{\alpha}_2 \rangle$!

למעשה $m_1\bar{\alpha}_1,\dots,m_k\bar{\alpha}_k$ בסיס ל-B כי אם $\sum k_i m_i \bar{\alpha}_i = 0$ אז $k_i m_i = 0$ לכל i כי $\bar{\alpha}_1,\dots,\bar{\alpha}_n$ בסיס. ולכן $k_i=0$ לכל i ב-A.

למה: כל חבורה אבלית נוצרת סופית G היא מנה A/B עבור A חופשית על קבוצה X כלשהי.

הוכחה: יהיו $g_1,\dots,g_n$ יוצרים של G. נגדיר העתקה מהקבוצה $\{x_1,\dots,x_n\}$ ל-$\{g_1,\dots,g_n\}$ ע"י $x_i \mapsto g_i$. תהי A החבורה החופשית על $\{x_1,\dots,x_n\}$ אז ניתן להרחיב להומומורפיזם $\varphi: A\to G$ שהוא הומומורפיזם על כי כל היוצרים מתקבלים. נסמן $B=\ker\varphi$ אז $A/B \cong G$ ☺

למה: יהיו $G_1,\dots,G_k$ חבורות ותהיינה $H_i \triangleleft G_i$. אז

$$\prod_{i=1}^{k} H_i \triangleleft \prod_{i=1}^{k} G_i$$

ומתקיים

$$\prod_{i=1}^{k} G_i \Big/ \prod_{i=1}^{k} H_i \cong \prod_{i=1}^{k} G_i/H_i$$

הוכחה: נורמליות:

$$(g_1\dots g_k)^{-1}(h_1\dots h_k)(g_1\dots g_k) =$$
$$= (g_1^{-1}hg_1,\dots,g_k^{-1}hg_k) \in \prod H_i$$

כעת נגדיר הומומורפיזם: $\varphi: \prod G_i \to \prod G_i/H_i$

$$(g_1\dots g_k) \longmapsto (g_1H_1,\dots,g_kH_k)$$

ברור ש-φ על! $\ker\varphi = \prod H_i$.

$$\Rightarrow \prod G_i / \prod H_i \cong \prod G_i/H_i$$

☺

מסקנה: אם A חופשית על $\alpha_1,\dots,\alpha_n$ ו-$B\le A$ חופשית על $m_1\alpha_1\dots m_k\alpha_k$ כאשר $m_1|m_2|\cdots|m_k$ אז מתקיים

$$A/B = \bigoplus_{i=1}^{n}\langle\alpha_i\rangle \Big/ \left(\bigoplus_{i=1}^{k}\langle m_i\alpha_i\rangle \oplus \bigoplus_{i=k+1}^{n}\{0\}\right) \cong \bigoplus_{i=1}^{k}\langle\alpha_i\rangle/\langle m_i\alpha_i\rangle \oplus \bigoplus_{i=k+1}^{n}\langle\alpha_i\rangle \cong \bigoplus_{i=1}^{k}\mathbb{Z}/m_i\mathbb{Z} \oplus \bigoplus_{i=k+1}^{n}\mathbb{Z}$$

לכן G חבורה אבלית נוצרת סופית איזומורפית
לחבורה מהצורה הנ"ל.
אם החבורה אבלית סופית אז היא איזומורפית לחבורה
מהצורה $\mathbb{Z}/m_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/m_k\mathbb{Z}$

<u>למה</u>: חבורה אבלית סופית היא מכפלה של חבורות p-סילו
שלה.

<u>הוכחה</u>: לכל p ראשוני המחלק את סדר החבורה, חבורת
p-סילו נורמלית (כי G אבלית) ולכן יחידה.
נסמן את כל החבורות p-סילו (של ה-p-ים השונים)
ב- $P_1,\dots,P_k$. אז $P_1\cdots P_k = G$ כי $|P_1\cdots P_k| = |G|$
כי אם $p^r \,\|\, |G|$ אז $p^r \,\|\, |P_1\cdots P_k|$ בנוסף
$P_i \cap \prod_{j\neq i} P_j = \{e\}$ (משיקולים של סדר איברים). ☺

<u>טענה</u>: נניח ש-A אבלית סופית ו- $|A| = p^r$ p ראשוני
אז $A \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_k}\mathbb{Z}$ כאשר $r_i \geq 1$, $\sum r_i = r$
ו- $r_1 \geq \dots \geq r_k$.
נניח ש- $A \cong \mathbb{Z}/p^{s_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{s_l}\mathbb{Z}$.
נראה באינדוקציה על סדר החבורה ש- $k = l$ ו- $r_i = s_i$ לכל i.
עבור G אבלית נגדיר $G^{(p)} = \{g \in G : pg = 0\}$. זאת
תת חבורה של G (כי G אבלית).
קל לראות שאם $G = G_1 \times \dots \times G_k$ אז $G^{(p)} = G_1^{(p)} \times \dots \times G_k^{(p)}$
נשים לב ש-

$$\frac{\mathbb{Z}/p^{r_i}\mathbb{Z}}{\left(\mathbb{Z}/p^{r_i}\mathbb{Z}\right)^{(p)}} \cong \mathbb{Z}/p^{r_i-1}\mathbb{Z}$$

כי נגדיר הומומורפיזם $\varphi : \mathbb{Z}/p^{r_i}\mathbb{Z} \to \mathbb{Z}/p^{r_i-1}\mathbb{Z}$ ע"י $g \mapsto pg$
ואז $\operatorname{Ker}\varphi = \left(\mathbb{Z}/p^{r_i}\mathbb{Z}\right)^{(p)}$ ולכן

$$A/A^{(p)} = \frac{\mathbb{Z}/p^{r_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_k}\mathbb{Z}}{\left(\mathbb{Z}/p^{r_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_k}\mathbb{Z}\right)^{(p)}} \cong$$

$$\cong \mathbb{Z}/p^{r_1-1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{r_k-1}\mathbb{Z}$$

כנ"ל עבור הפירוק השני:

$$A/A^{(p)} \cong \mathbb{Z}/p^{s_1-1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{s_k-1}\mathbb{Z}$$

מהנחת האינדוקציה הפירוק של $A/A^{(p)}$ יחיד. לכן $k=l$ ו- $s_i-1=r_i-1 \Rightarrow s_i=r_i$

<u>מסקנה:</u>

מספר החבורות האבליות מסדר p^r הוא מספר האפשרויות לרשום את r כסכום $r=r_1+\dots+r_k$ כאשר $r_k \geq \dots \geq r_1$. נסמן מספר זה ב- $\sigma(r)$ (פונקציית החלוקה). נשים לב שזה לא תלוי ב- p, אלא רק ב- r.

<u>דוגמה:</u> חבורות אבליות מסדר $2^6=64$. מהן החלוקות האפשריות?

$1+1+1+1+1+1$	$\mathbb{Z}_2 \times \dots \times \mathbb{Z}_2$
$1+1+1+1+2$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$
$1+1+2+2$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4$
$2+2+2$	$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4$
$1+1+1+3$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8$
$1+2+3$	$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8$
$3+3$	$\mathbb{Z}_8 \times \mathbb{Z}_8$
$1+1+4$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{16}$
$2+4$	$\mathbb{Z}_4 \times \mathbb{Z}_{16}$
$1+5$	$\mathbb{Z}_2 \times \mathbb{Z}_{32}$
6	$\mathbb{Z}_{64}$

<u>מסקנה:</u> אם G חבורה אבלית ו- $|G|=p_1^{r_1}\cdots p_k^{r_k}$ אז מספר חבורות מסדר זה הן $\sigma(r_1)\cdots\sigma(r_k)$

הגדרה: Q היא חבורה עם 8 איברים הנוצרת ע"י a,b רק כך ש- $a^4=1$ $b^2=a^2$ $bab^{-1}=a^{-1}$

$$Q \cong \left\langle \begin{pmatrix}0&i\\i&0\end{pmatrix}, \begin{pmatrix}0&1\\-1&0\end{pmatrix} \right\rangle$$

טענה: חבורה לא אבלית מסדר 8 איזומורפית ל- Q או ל- D_4.

מסקנה: החבורות מסדר $2^3=8$ הן Q, D_4 וכן $\mathbb{Z}_8$, $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$, $\mathbb{Z}_2\times\mathbb{Z}_4$

הוכחת הטענה: כל האיברים מסדר 2 אז G אבלית וכן אין איבר מסדר 8 כי אז היא ציקלית ואבלית.
לכן יש איבר מסדר 4 a. $\langle a\rangle \triangleleft G$ (כי $[G:\langle a\rangle]=2$)
$G/\langle a\rangle \cong \mathbb{Z}_2$. יהי $b\notin\langle a\rangle$. מכיוון שחבורת המנה מסדר 2 (ציקלית) $b^2\langle a\rangle=(b\langle a\rangle)^2=\langle a\rangle \Leftarrow b^2\in\langle a\rangle$.
אם $b^2=a$ אז b מסדר 8 ו- G ציקלית. כנ"ל אם $b^2=a^3=a^{-1}$.

אם $H\triangleleft G$ $\lvert G/H\rvert=[G:H]$ לכן אם $g\in G$ אז $(gH)^{[G:H]}=H$ לכן $g^{[G:H]}\in H$

לכן האפשרויות הן $b^2=a^2$ או $b^2=1$.
$\langle a\rangle\triangleleft G \Leftarrow bab^{-1}=a^i$
לגבי i: $o(bab^{-1})=o(a)$ $o(a^2)=2$ $o(1)=1$
$bab^{-1}=a,a^{-1} \Leftarrow$
$\left((bab^{-1})^k=bab^{-1}bab^{-1}\dots bab^{-1}=ba^kb^{-1}=1 \Leftarrow a^k=1\right)$
אם $bab^{-1}=a$ אז $ba=ab$ אבל $G=\langle a,b\rangle$ ו- G לא אבלית.
לכן יש בדיוק שתי אפשרויות:

(א) $bab^{-1}=a^{-1}$ $b^2=a^2$ $a^4=1$ $\Leftarrow G\cong Q$

(ב) $bab=a^{-1}$ $b^2=1$ $a^4=1$ $\Leftarrow G\cong D_4$

(29) 25.12.07
ת' מבנים

חוגים

חוג R הוא קבוצה עם שתי פעולות $+,\cdot$ כך ש- R חבורה אבלית ביחס לחיבור, הכפל אסוציאטיבי ומתקיימת דיסטריבוטיביות:
$$(a+b)c = ac+bc$$
$$a(b+c) = ab+ac$$

__הגדרה:__ חוג עם יחידה הוא חוג R עם איבר $1\neq 0$ שמקיים $1a = a1 = a$ לכל $a\in R$.

__הגדרה:__ חוג נקרא קומוטטיבי אם $ab=ba$ לכל $a,b\in R$

__הגדרה:__ חוג R עם יחידה נקרא חוג חילוק אם לכל $0\neq a\in R$ יש $b\in R$ כך ש- $ab=ba=1$.

__הגדרה:__ $a\in R^{0\neq}$ נקרא מחלק אפס משמאל אם קיים $0\neq b\in R$ כך ש $ab=0$. באופן דומה מוגדר מחלק אפס מימין.
בחוג קומוטטיבי נקרא ל-a מחלק 0.
חוג (קומוטטיבי) ללא מחלקי אפס נקרא תחום שלמות.

__הערה:__ בתחום שלמות R מתקיים $ac=bc$ עבור $c\neq 0$ אזי $a=b$ (תכונת הצמצום) (תרגיל!)

__הגדרה:__ $S\subseteq R$ ייקרא תת חוג אם הוא חוג ביחס לפעולות המושרות מ- R

__דוגמאות__

1. $\mathbb{Z}$ עם כפל וחיבור הרגילים. זה חוג קומוטטיבי עם יחידה וזה גם תחום שלמות. אבל זה לא חוג חילוק.
2. F שדה הוא חוג קומוטטיבי שהוא גם חוג חילוק
שאלה מעניינת: האם יש חוג חילוק קומוטטיבי שאינו שדה?
3. $\mathbb{Z}_n$ עבור $n\in\mathbb{N}$ עם חיבור וכפל מודולו n.

האיברים ההפיכים ב-$\mathbb{Z}_n$ הם $\mathbb{Z}_n^*$

אם n לא ראשוני אז $\mathbb{Z}_n$ אינו חוג חילוק. $\mathbb{Z}_n$
אינו תחום שלמות אם n לא ראשוני, כי אם $n=pq$
אז $p,q\in\mathbb{Z}_n$ הם מחלקי אפס.

(1) חוג הפולינומים מעל שדה F - $F[X]$ או באופן יותר
כללי, פולינומים מעל חוג R - $R[X]$

$$R[X]=\left\{\sum_{i=0}^{n}a_ix^i : a_i\in R,\ n\in\mathbb{N}\right\}$$

פורמלית אפשר גם להגדיר את זה ע"י קבוצת כל הסדרות של איברי R רק שהחל ממקום מסוים הן קבועות אפס.

$$\sum a_ix^i=\sum b_ix^i \iff a_i=b_i \text{ לכל } i$$

$$\sum a_ix^i+\sum b_ix^i=\sum(a_i+b_i)x^i$$

$$\left(\sum a_ix^i\right)\left(\sum b_ix^i\right)=\sum_i\sum_{j=0}^{i}a_jb_{i-j}$$

זהו חוג קומוטטיבי אמ"מ R קומוטטיבי וזה תחום שלמות אמ"מ R תחום שלמות (תרגיל)
נשים לב ש-R הוא תת חוג של $R[X]$.

<u>הגדרה:</u> דרגה של פולינום $f=\sum a_ix^i$ הוא האינדקס המקסימלי i שעבורו $a_i\neq 0$.
(נסמן את הדרגה ב-$\deg(f)$. $\deg(0)=-\infty$

אם R תחום שלמות אז $\deg(f+g)\le\max(\deg f,\deg g)$
$\deg(fg)\underset{\downarrow}{=}\deg f+\deg g$

לא בהכרח נכון אם R לא תחום שלמות

בפרט אם f הפיך אז $0=\deg(1)=\deg(f)+\deg(f^{-1})$
$\Leftarrow \deg f=0 \Leftarrow f\in R$.

<u>מסקנה:</u> איבר ב-$R[X]$ הוא הפיך אמ"מ הוא ב-R^* (= האיברים ההפיכים ב-R)

לא תמיד אפשר לזהות פולינומים כביטויים פורמליים עם פולינומים כפונקציות על R.
למשל, $x^p - x \in \mathbb{Z}_p[x]$, אז $\alpha^p - \alpha = 0$ לכל $\alpha \in \mathbb{Z}_p$
אבל $x^p - x$ אינו פולינום האפס.

אפשר להגדיר באופן אינדוקטיבי:
$$R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n]$$
ביטוי ב- $R[X_1, \dots, X_n]$ נתון כ- $\sum a_{\nu_1 \dots \nu_n} X_1^{\nu_1} \dots X_n^{\nu_n}$
כאשר $a_{\nu_1 \dots \nu_n} \in R$. ביטוי מהצורה $X_1^{\nu_1} \dots X_n^{\nu_n}$
נקרא <u>מונום</u>. הדרגה של מונום היא $\sum_{i=1}^{n} \nu_i$. כל איבר
ב- $R[X_1 \dots X_n]$ הוא צירוף ליניארי של מונומים
עם מקדמים ב- R.
פולינום ב- n משתנים ייקרא <u>הומוגני</u> אם הדרגה
של כל המונומים המופיעים בהצגה שלו שווה.

<u>דוגמה</u>: $x^2 + xy + y^2$ פולינום הומוגני ב- x וב- y.

<u>דוגמה</u>
נגדיר $\tau : \mathbb{C} \to \mathbb{C}$, $z \to \bar{z}$. החוג $\mathbb{C}^{\tau}[X]$ כחבורה
אבלית, זהה לפולינומים מעל $\mathbb{C}$, ונגדיר $zX = X\bar{z}$
וכפל לאיברים כלליים נגדיר בעזרת דיסטריבוטיביות.
זה נקרא חוג פולינומים מפותל. זה <u>לא</u> חוג קומוטטיבי.
נכפול למשל כמה איברים.

$$(5 + iX)(3 + (1+i)X + 2iX^2) =$$
$$= 15 + 5(1+i)X + 5 \cdot 2i X^2 + iX \cdot 3 + \underbrace{iX(1+i)X}_{= i(1-i)X^2 = (1+i)X^2} + \underbrace{iX \cdot 2iX^2}_{= i(-2i)X^3 = 2X^3}$$

המשך דוגמאות

- R חוג. $M_n(R)$ חוג המטריצות $n\times n$ מעל R עם חיבור וכפל מטריצות.

עבור $n>1$ זה חוג לא קומוטטיבי ולא חוג חילוק.

נניח ש-R קומוטטיבי עם יחידה. ניתן להגדיר עבור $A\in M_n(R)$ את $\det A$ כרגיל $\det A=\sum_{\sigma\in S_n} sgn\,\sigma \prod_{i=1}^{n} a_{i\sigma(i)}$

הדטרמיננטה מקיימת את כל התכונות שהיא מקיימת מעל שדה (כפל בסקלר, סכום שורות וכן הלאה).

בפרט גם $\det(AB)=\det A\det B$

ונוסחת פיתוח לפי שורה: $\det A=\sum_{j=1}^{n}(-1)^{i+j}a_{ij}A_{ij}$

$$A_{ij}=\left|\begin{matrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{in} \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn}\end{matrix}\right|$$

הדטרמיננטה של המטריצה המתקבלת מ-A השמטת את השורה ה-i והעמודה ה-j

$\sum_{j=1}^{n}(-1)^{k+j}a_{ij}A_{kj}=|A|\delta_{ik}$.

מגדירים כרגיל את $adj\,A$ ע"י $(Adj A)_{ij}=(-1)^{i+j}A_{ji}$

אז $\det A\cdot I_n=(Adj A)A=A\,Adj A$

אם $\det A\in R$ איבר הפיך אז A הפיך ו- $A^{-1}=(\det A)^{-1}Adj A$

מאידך, אם A הפיכה אז $\det A\cdot\det A^{-1}=\det I_n=1$

לכן $\det A\in R$ איבר הפיך.

אז A הפיכה ב-$M_n(R)$ אמ"מ $\det A$ הפיכה ב-R.

למשל $A\in M_n(\mathbb{Z})$ אמ"מ $\det A=\pm 1$.

$A\in M_n(F[x])$ הפיכה אמ"מ $\det F\in F^*$.

- $\mathbb{H}$ חוג הקווטרניונים של המילטון

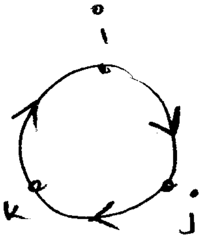
$\mathbb{H}=\{a+bi+cj+dk \ : \ a,b,c,d\in\mathbb{R}\}$

i,j,k הם סתם סימנים.

נאמר ש- $a+bi+cj+dk=a'+b'i+c'j+d'k$ אמ"מ $a=a'$, $b=b'$, $c=c'$, $d=d'$

החיבור מוגדר באופן הבא:

$$(a+bi+cj+dk)+(a'+b'i+c'j+d'k) = a+a'+(b+b')i+(c+c')j+(d+d')k$$



הכפל מוגדר באופן הבא:

$$i^2=j^2=k^2=-1$$

$$ij=k \quad jk=i \quad ki=j$$

$$ji=-k \quad kj=-i \quad ik=-j$$

ועבור איברים כלליים נגדיר את הכפל בעזרת דיסטריבוטיביות.

$$(a+bi+cj+dk)(e+fi+gj+hk)=$$
$$= ae+afi+agj+ahk+$$
$$+bei-bf+bgk-bhj+$$
$$+cej-cfk-cg+chi+$$
$$+dek+dfj-dgi-dh=$$
$$=(ae-bf-cg-dh)+(af+be+ch-dg)i+$$
$$+(ag-bh+ce+df)j+(ah+bg-cf+de)k$$

$1\in\mathbb{H}$ הוא היחידה בחוג.

$\mathbb{H}$ לא קומוטטיבי.

נניח $x=a+bi+cj+dk\in\mathbb{H}$. נגדיר הצמוד $\bar{x}=a-bi-cj-dk$

אז $x\cdot\bar{x}=a^2+b^2+c^2+d^2$ (תרגיל)

בפרט, אם $x\neq 0$ אז $\mathbb{R}\ni x\cdot\bar{x}\neq 0$ ולכן יש לו הופכי.

ואז $\frac{\bar{x}}{x\bar{x}}=x^{-1}$ אז לכל איבר $\mathbb{H}\ni x\neq 0$ יש הופכי וזה אומר שיש לנו חוג חילוק שאינו קומוטטיבי!

<u>הגדרה:</u> יהי R חוג. נגדיר את R^{op} להיות החוג שבקבוצה שלו ביחס לחיבור זהה ל-R ובכפל $a*_{op}b=b*_R a$

<u>דוגמה:</u> יהי $R=M_n(F)$ עבור שדה F ונגדיר $\varphi: R\to R^{op}$ ע"י $A\mapsto A^t$.

אז φ הומומורפיזם כי $(AB)^t = B^tA^t = A^t * B^t$

מאידך φ כמובן הפיכה $\varphi\circ\varphi = Id$ $\Leftarrow$ φ איזומורפיזם.

עוד דוגמאות

- $\mathbb{Z}\sqrt{2} = \{a+b\sqrt{2}\}_{a,b\in\mathbb{Z}}$ זה תת חוג של $\mathbb{R}$

הסגירות לחיבור היא טריוויאלית.

גם את הסגירות לכפל אפשר לראות מחישוב ישיר:

$$(a+b\sqrt{2})(c+d\sqrt{2}) = \underbrace{(ac+2bd)}_{\in\mathbb{Z}} + \underbrace{(ad+bc)}_{\in\mathbb{Z}}\sqrt{2}$$

- $\mathbb{Z}[i] = \{a+bi : a,b\in\mathbb{Z}\}$ חוג השלמים של גאוס

זה תת חוג של $\mathbb{C}$.

- תהי S קבוצה $R = \{$ אוסף תת הקבוצות של S $\}$

ונגדיר חיבור וכפל באופן הבא:

$$X+Y = X\Delta Y = X\cup Y \setminus X\cap Y$$

$$X\cdot Y = X\cap Y$$

$$0 = \emptyset$$

$$1 = S$$

זה חוג קומוטטיבי עם יחידה. ומתקיים $X^2 = X$

לכל $X\in R$. (נקרא חוג בוליאני).

(32) 1.1.08
ת' אמנים
שנה אזרחית טובה!

פריקות בתחומים

<u>המשפט היסודי של האריתמטיקה</u>: לכל $n \in \mathbb{Z}$ יש פירוק $n = \pm p_1 \cdots p_k$ כאשר p_i ראשוניים והפירוק יחיד עד כדי שינוי סדר האיברים

<u>הגדרות</u>: יהי R תחום שלמות ויהיו $a,b \in R$

- נאמר ש-a <u>מחלק</u> את b ונסמן $a|b$ אם $b = ac$ עבור $c \in R$ כלשהו
- a <u>מחלק ממש</u> את b אם $b = ac$ ו- a, c אינם הפיכים.
- a <u>אי-פריק</u> אם a לא הפיך ואין ל-a אף מחלק ממש.
- נאמר ש-a <u>חבר</u> של b ונסמן $a \sim b$ אם $a|b$ ו- $b|a$. (זה קורה אמ"מ $a = bu$ ו- u הפיך)

<u>הגדרה</u>: R תחום שלמות יקרא <u>תחום פריקות חד-ערכית</u> (פח"ע) אם:

1) פריקות: לכל $a \in R$ יש פירוק $a = p_1 \cdots p_n$ כאשר p_i איברים אי פריקים.
2) חד ערכיות: אם מתקיים גם $a = q_1 \cdots q_m$ אז $n = m$ ואם נסדר נכון את האיברים אז $q_i \sim p_i$ לכל i.

<u>הגדרה</u>: תחום R יקרא <u>תחום ראשי</u> אם כל אידיאל הוא ראשי, כלומר מהצורה aR עבור $a \in R$.

<u>משפט</u>: תחום ראשי הוא תחום פח"ע

! <u>הערה</u>: ההפך לא בהכרח נכון. יש תחומי פח"ע שאינם ראשיים, למשל $\mathbb{Z}[X]$ או $F[X,Y]$.

מסקנה מהמשפט: אם $R=S[X]$ כאשר S תחום פ"ע
אז גם R תחום פ"ע.

פריקות חד-ערכית נובעת מכך שבתחום ראשי כל איבר אי פריק p מקיים את התכונה שאם $p|ab$ אז $p|a$ או $p|b$.

לא קשה, תחום פריקות הוא תחום פ"ע אמ"מ כל אי פריק מקיים תכונה זו.
לאיברים המקיימים תכונה זו קוראים ראשוניים.
נשים לב שראשוניים הם תמיד אי-פריקים אבל אי-פריק הוא לא בהכרח ראשוני.

דוגמה $R=\mathbb{Z}[\sqrt{-5}]$. בחוג זה מתקיים
$$2\cdot3=6=(1-\sqrt{-5})(1+\sqrt{-5})$$
אפשר לראות ש- $1+\sqrt{-5}$, $1-\sqrt{-5}$, $2,3$ אי"פ $\mathbb{Z}[\sqrt{-5}]$
אינו תחום פ"ע. כמו כן, $2,3,1-\sqrt{-5},1+\sqrt{-5}$ אינם ראשוניים.

הגדרה: תחום שלמות R ייקרא חוג אוקלידי אם יש העתקה $d: R\setminus\{0\}\longrightarrow \mathbb{N}\cup\{0\}$ כך שמתקיים:

(א) לכל $a,b\in R$ $d(a)\le d(ab)$

(ב) לכל $a,b\in R$ קיימים $q,r\in R$ כך שמתקיים $b=qa+r$; $r=0$ או $d(r)<d(a)$

ראינו שמתקיים

חוג אוקלידי $\overset{\Longrightarrow}{\not\Longleftarrow}$ חוג ראשי $\overset{\Longrightarrow}{\not\Longleftarrow}$ תחום פ"ע

דוגמאות: $\mathbb{Z}$, $F[X]$, $\mathbb{Z}[i]$

משפט: $\mathbb{Z}[i]$ חוג אוקלידי כאשר

$$|x|^2 = d(x) = d(a+bi) = a^2+b^2$$

הוכחה: צריך להראות שמתקיימות שתי התכונות

(א) תרגיל

(ב) יהיו $a,b \in \mathbb{Z}[i]$. נניח ש- $b = aw$ כאשר $w = x+iy \in \mathbb{C}$. קיימים $m,n \in \mathbb{Z}$ כך ש-

$$x = m+x_0 \qquad y = n+y_0$$

כאשר $-\frac{1}{2} \le x_0, y_0 < \frac{1}{2}$.

נבחר $q = m+ni$ ונסמן $r = b - qa \in \mathbb{Z}[i]$

אם נראה ש- $d(r) < d(a)$ נקבל את הדרוש.

$$d(r) = r^2 = |b-qa|^2 = |aw-qa|^2 =$$

$$= |a(x+iy) - a(m+ni)|^2 = |a|^2 |x_0 + iy_0|^2 \le$$

$$\le \frac{1}{2}|a|^2 < |a|^2 = d(a)$$

לכן $b = qa+r$ מקיים את התכונה הנדרשת. ☺

מסקנה: $\mathbb{Z}[i]$ תחום פא"ר

הערה: האיברים ההפיכים ב- $\mathbb{Z}[i]$ צריכים לקיים $|u|^2 = 1$ (מכפליות הנורמה). לכן, אם $u = x+iy$ אז $|u|^2 = x^2+y^2 = 1 \Leftarrow y=0, x=\pm 1$ או $x=0, y=\pm 1$. כלומר האיברים ההפיכים הם $\{\pm 1, \pm i\}$

דוגמה: $2 \in \mathbb{Z}$ ראשוני אבל $2 = (1+i)(1-i)$

פירוק של 2 ב- $\mathbb{Z}[i]$ $\Leftarrow$ 2 אינו ראשוני ב- $\mathbb{Z}[i]$

לעומת, 3 הם ראשוני גם ב- $\mathbb{Z}$ וגם ב- $\mathbb{Z}[i]$.

נניח ש- $3 = (a+ib)(c+id)$ אז

$$9 = (a^2+b^2)(c^2+d^2)$$

עבור $a,b,c,d \in \mathbb{N}$ וזה לא יתכן.

משפט:

(א) יהי $p\in\mathbb{Z}$ ראשוני, אז או ש-p ראשוני גם ב-$\mathbb{Z}[i]$ או ש- $p=\pi\cdot\bar{\pi}$ כאשר π ראשוני ב-$\mathbb{Z}[i]$

(ב) אם $\pi\in\mathbb{Z}[i]$ ראשוני-גאוס אז $\pi\bar{\pi}$ ראשוני ב-$\mathbb{Z}$ או ריבוע של ראשוני ב-$\mathbb{Z}$.

(ג) $p\in\mathbb{Z}$ הוא ראשוני גאוס אמ"מ $p\equiv 3 \pmod 4$

(ד) התנאים הבאים שקולים:

(i) $p=\pi\bar{\pi}$ כאשר π ראשוני גאוס

(ii) $p=a^2+b^2$ עבור $a,b\in\mathbb{Z}$

(iii) למשוואה $x^2\equiv -1 \pmod p$ יש פתרון

(iv) $p=2$ או $p\equiv 1 \pmod 4$

הערה: לראשוני ב-$\mathbb{Z}$ נקרא ראשוני ולראשוני ב-$\mathbb{Z}[i]$ נקרא ראשוני גאוס.

הוכחה:

(א) יהי $p\in\mathbb{Z}$ ראשוני. $p\in\mathbb{Z}[i]$ לכן יש ראשוני גאוס π רק ש- $\pi|p$. אז $\bar{\pi}|p$ (כי $p=\bar{p}=\bar{\pi}\bar{a}$ אם $p=\pi a$). לכן $\pi\bar{\pi}|p^2$ אבל $\pi\bar{\pi}\in\mathbb{Z}$.
אם $p\sim\pi$ אז p ראשוני גאוס. אם לא, אז π מחלק ממש את p ולכן $\pi\bar{\pi}$ מחלק ממש את $p^2 \Rightarrow p=\pi\bar{\pi}$.

(ב) יהי π ראשוני גאוס. נניח ש- $\pi\bar{\pi}=n\in\mathbb{N}$. נפרק את n ב-$\mathbb{Z}$, לגורם פירוק ב-$\mathbb{Z}[i]$ (לא בהכרח למכפלת אי פריקים). לכן π מחלק את אחד הגורמים במכפלה, $\pi|p$. לכן $\pi\bar{\pi}|p^2$ ולכן $\pi\bar{\pi}=p^2$ או $p=\pi\bar{\pi}$ ראשוני.

(ג) נוכיח (ג) ו-(ד). אם p ראשוני גאוס אז הוא לא מכפלת איברים $\pi\bar{\pi}$ ולכן מהשקילות בין (i) ו-(iv) נקבל $p\not\equiv 1 \pmod 4$ ו- $p\not\equiv 2 \pmod 4$

③ (i) ⟸⟹ (ii)

אם $p=\pi\bar{\pi}$ כאשר $\pi=a+bi$ אז $p=a^2+b^2$

ואם $p=a^2+b^2$ אז עבור $\pi=a+bi$ $p=\pi\bar{\pi}$.

(i) ⟸⟹ (iii)

ראשית, נטען ש- $\mathbb{Z}[i]\cong\mathbb{Z}[x]/(x^2+1)$

האידיאל הראשי שנוצר ע"י x^2+1

נתבונן בהומומורפיזם $\varphi:\mathbb{R}[x]\longrightarrow\mathbb{R}[i]=\mathbb{C}$

$f(x)\longrightarrow f(i)$

קל לראות שזה אכן הומומורפיזם.

$(x^2+1)\subseteq\ker\varphi$ שהרי $f(x)(x^2+1)\longmapsto f(i)\cdot 0=0$

$\mathbb{R}[x]$ חוג ראשי.

x^2+1 אי פריק ב- $\mathbb{R}[x]$. בחוג ראשי אידיאל הנוצר ע"י איבר אי פריק a הוא מקסימלי כי אם $(a)=I\subsetneq R$ אז $I=(b)$; $b|a$. אבל a אי-פריק לכן $b\sim a$ ⟸ $(a)=(b)$ לכן (x^2+1) מקסימלי ⟸ $\ker\varphi=(x^2+1)$

לכן אם נגדיר $\varphi:\mathbb{Z}[x]\to\mathbb{Z}[i]$ ע"י $f(x)\to f(i)$

אז $f(i)=0 \Rightarrow x^2+1\mid f(x)$ לכן $\ker\varphi=(x^2+1)$

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

<u>למה:</u> יהי p ראשוני. התנאים הבאים שקולים

(א) p ראשוני גם ב $\mathbb{Z}[i]$

(ב) $\mathbb{Z}[i]/(p)$ שדה

(ג) x^2+1 אי פריק ב- $\mathbb{Z}_p[x]$

<u>הערה:</u> (p) הוא אוסף האיברים $a+bi$ כך ש- $p|a,b$

<u>הוכחה:</u>

(א⟸⟹ב) $\mathbb{Z}[i]$ תחום ראשי. לכן אם p ראשוני אז (p) אידיאל מקסימלי לכן $\mathbb{Z}[i]/(p)$ שדה. (אם R חוג קומוטטיבי עם יחידה; $M\triangleleft R$ אידיאל מקסימלי אז R/M שדה כי אז ל R/M אין אידיאלים לא טריוויאליים ולפי התרגיל R/M שדה).

מאידך, אם R/I שדה אז אין ב- R/I
אידיאלים לא טריוויאלים ולכן ממשפט ההתאמה
I מקסימלי.
(ג $\Leftrightarrow$ ב) נתבונן ב- $\mathbb{Z}[x]/(x^2+1,p)$
מצד אחד,

$$\mathbb{Z}[x]/(x^2+1,p) \cong \mathbb{Z}[x]/(x^2+1)\Big/(p) \cong \mathbb{Z}[i]/(p)$$

מצד שני,

$$\mathbb{Z}[x]/(x^2+1,p) \cong \mathbb{Z}_p[x]/(x^2+1)$$

$\mathbb{Z}_p[x]/(x^2+1)$ הוא שדה אמ"מ x^2+1 אי-פריק
ב- $\mathbb{Z}_p[x]$. לכן $\mathbb{Z}[i]/(p)$ שדה אמ"מ x^2+1
אי פריק ב- $\mathbb{Z}_p$. מש"ל.
נתבונן להוכחת השקילות (i) $\Leftrightarrow$ (iii)
p ראשוני גאוס אמ"מ x^2+1 "פריק ב- $\mathbb{Z}_p[x]$.
אמ"מ יש לו שורש $a^2+1 \equiv 0 \pmod p$ אמ"מ
$a^2 \equiv -1 \pmod p$ ולכן יש ל $x^2 \equiv -1 \pmod p$ פותרון
אמ"מ p ראשוני גאוס.

(35) 8.1.08

ת' מבנים

<u>תזכורת:</u>

(א) $p\in\mathbb{Z}$ ראשוני הוא ראשוני גאוסי או $p=\pi\bar{\pi}$ עבור π ראשוני גאוסי

(ב) אם π ראשוני גאוסי אז $\pi\bar{\pi}\in\mathbb{N}$ ראשוני או ריבוע ראשוני.

(ג) התנאים הבאים שקולים:

(i) $p=\pi\bar{\pi}$ ראשוני גאוסי

(ii) $p=a^2+b^2$

(iii) למשוואה $x^2\equiv -1 \pmod{p}$ יש פתרון

(iv) $p=2$ או $p\equiv 1 \pmod{4}$

<u>הוכחה:</u> (המשך)

(ד) $(i \Leftrightarrow iii)$

<u>למה:</u> עבור p ראשוני התנאים הבאים שקולים:

(א) p ראשוני גאוסי (אמ"מ $\mathbb{Z}[i]/(p)$ שדה)

(ב) x^2+1 אי פריק ב- $\mathbb{Z}_p[x]$

<u>הוכחת הלמה:</u> נזכיר $\mathbb{Z}[i]\cong\mathbb{Z}[x]/(x^2+1)$

נתבונן באידיאל הנוצר ע"י p, x^2+1 ב- $\mathbb{Z}[x]$.

$$I=(p,x^2+1)=\{f(x)p+g(x)(x^2+1) : f,g\in\mathbb{Z}[x]\}$$

ניקח את העתקה $\mathbb{Z}[x]\to\mathbb{Z}[x]/p\mathbb{Z}[x]$. לאן עובר I תחת ההטלה הטבעית?

$$I\mapsto (x^2+1)\mathbb{Z}[x]/p\mathbb{Z}[x]$$

נשים לב ש- $\mathbb{Z}[x]/p\mathbb{Z}[x]\cong\mathbb{Z}_p[x]$

ממשפט האיזומורפיזם השני נקבל ש-

$$\mathbb{Z}[x]/I\cong\frac{\mathbb{Z}[x]/p\mathbb{Z}[x]}{(x^2+1)\mathbb{Z}[x]/p\mathbb{Z}[x]}\cong\mathbb{Z}_p[x]/(x^2+1)\mathbb{Z}_p[x]$$

כעת נתבונן בהעתקה $\mathbb{Z}[x]\to\mathbb{Z}[x]/(x^2+1)\cong\mathbb{Z}[i]$

אז $I\mapsto p\mathbb{Z}[x]/(x^2+1)$

לכן $\mathbb{Z}[x]/I \cong \mathbb{Z}[x]/(x^2+1) \Big/ p\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i]/(p)$

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

אגף ימין הוא שדה אמ"מ p אי פריק ב- $\mathbb{Z}[i]$

אגף שמאל הוא שדה אמ"מ x^2+1 אי פריק ב $\mathbb{Z}_p[X]$

וזה אמ"מ ל- x^2+1 אין שורש ב- $\mathbb{Z}_p[X]$ (כי אם הוא פריק אז $x^2+1=(x-a)(x-b)$ ו a,b שורשים)

לכן p ראשוני גאוס אמ"מ x^2+1 אי פריק ב- $\mathbb{Z}_p[X]$ מ.ש.ל למה

לפת p אינו ראשוני גאוס אמ"מ x^2+1 פריק ב- $\mathbb{Z}_p[X]$ אמ"מ יש פתרון למשוואה $x^2 \equiv -1 \pmod p$.

(iii $\Leftrightarrow$ iv)

יש פתרון ל- $x^2 \equiv -1 \pmod p$ אמ"מ $p=2$ או $p \equiv 1 \pmod 4$

אם $p=2$ אז $1^2 \equiv -1 \pmod 2$ לכן אפשר להניח ש- $p \neq 2$.

<u>למה:</u>

(א) $a \in \mathbb{Z}$ פתרון למשוואה $x^2 \equiv -1 \pmod p$ אמ"מ a איבר מסדר 4 מודולו p.

(ב) יש איבר מסדר 4 ב- $\mathbb{Z}_p^*$ אמ"מ $p \equiv 1 \pmod 4$

<u>הוכחת הלמה:</u>

(א) אם $\bar{a}$ איבר מסדר 4 ב- $\mathbb{Z}_p$ אז $\bar{a}^2$ איבר מסדר 2. איבר מסדר 2 ב- $\mathbb{Z}_p$ מקיים $x^2-1=0$
$(x-1)(x+1)$

לכן האיבר היחיד מסדר 2 הוא -1 ולכן $\bar{a}^2=-1$ או $a^2 \equiv -1 \pmod p$. ובכיוון ההפוך אם $\bar{a}^2 \equiv -1 \pmod p$ אז $\bar{a}^4 \equiv 1 \pmod p$ ולכן ל- a יש סדר 4 ב- $\mathbb{Z}_p$.

ה) $|\mathbb{Z}_p^*|=p-1$

אם יש איבר מסדר 4 ב- $\mathbb{Z}_p^*$ אז $4 \mid |\mathbb{Z}_p^*|$
ולכן $p\equiv 1 \pmod 4$.
אם $p\equiv 1 \pmod 4$ אז $4 \mid |\mathbb{Z}_p^*|$.
נתבונן בתת-חבורה 2-סילו H של $\mathbb{Z}_p^*$. כי
חבורה מסדר 4 לפחות, לכן יש איבר $H \ni a \neq -1,1$
רק שסדר a הוא 2^n וכו'
לכן אפשר למצוא ב-H איבר מסדר 4 (חזקה מתאימה של a)

☺

<u>דוגמא</u> $\mathbb{Z}[\sqrt{-5}]$ אינו תחום פ.ר.י.
$2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$
נראה ש- 2, 3, $1\pm\sqrt{-5}$ אי פריקים.
נניח $2=ab$ אז $4=|a|^2|b|^2$
$4=(a_1^2+5a_2^2)(b_1^2+5b_2^2)$
אם $a_1^2+5a_2^2=1$ (כלומר $a_1=\pm 1$ $a_2=0$)
אז $a=\pm 1$ הפיך (כנ"ל גם b).
$a_1^2+5a_2^2=2$ לא יתכן. לכן אין פירוק לא טריוויאלי של 2.
עבור 3 כנ"ל. כי $3=ab$ אז או ש- a הפיך או
ש- $a_1^2+5a_2^2=3$ וזה לא יתכן.

הרחבות שדות

יהי F שדה ויהי $f(x)\in F[x]$ אי פריק (מדרגה n) יהי R החוג
$F[x]/(f)$. ההעתקה הטבעית $F[x]\to F[x]/(f)$
מצומצמת ל- F היא חח"ע. לכן אפשר לזהות את F
עם תמונתה - תת חוג של R.
אפשר לחשוב על R כמרחב וקטורי מעל F.

R חבורה אבלית חיבורית. כפל אומר $r \in R$ ב-$a \in F$ יהיה פשוט הכפל ב-R : ar.

תכונות המרחב הוקטורי נובעות מתכונות החוג.

יתר על כן $\dim_F R = n$. נראה שאם $\bar{X}$ תמונת X ב-R אז $1, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1}$ בסיס ל-R מעל F.

פורש: יהי $g(x) \in F[X]$ אז $g(x) = q(x)f(x) + r(x)$ ואשר $\deg r < n$. לכן $\overline{g(x)} = \bar{0} + \overline{r(x)}$

$r(x) = \sum_{i=0}^{n-1} a_i x^i \Rightarrow \overline{g(x)} = \sum_{i=0}^{n-1} a_i \bar{x}^i$.

בת"ל: נניח $\sum_{i=0}^{n-1} a_i \bar{x}^i = \bar{0}$ אז $\sum_{i=0}^{n-1} a_i x^i \in (f(x))$

$f(x)$ מדרגה n ואם הוא מחלק את אגף שמאל אז אגף שמאל הוא 0.

נניח ש-$f(x)$ פולינום אי פריק. אז $(f(x))$ אידיאל מקסימלי ולכן $L = F[X]/(f(x))$ הוא שדה.

ב-L מתקיים $f(\bar{x}) = \overline{f(x)} = 0$. לכן $\bar{x}$ שורש של הפולינום ב-L.

דוגמה: $x^2+1 \in \mathbb{R}[X]$ אי פריק לכן $\mathbb{R}[X]/(x^2+1)$ הוא שדה והוא ממימד 2 מעל $\mathbb{R}$. למעשה

$$\mathbb{R}[X]/(x^2+1) \cong \mathbb{C}$$

נניח ש-$F = \mathbb{Z}_p$! $f \in \mathbb{Z}_p[X]$ ממעלה n אי פריק. נקבל שדה $L = \mathbb{Z}_p[X]/(f)$ המכיל את $\mathbb{Z}_p$. L ממימד n מעל $\mathbb{Z}_p$ ולכן $|L| = p^n$.

לכן אם נוכיח שלכל $n \in \mathbb{N}$ יש פולינום ממעלה n מעל $\mathbb{Z}_p$ אי פריק נקבל שיש שדה מסדר p^n לכל n. למעשה לכל n יש שדה יחיד מסדר p^n. ההוכחה במבנים 2.

<u>דוגמה</u> $F=\mathbb{Z}_2$ $\quad f(x)=x^2+x+1$

f ממעלה 2 ולכן f אי פריק אמ"מ ל-f אין שורשים ב-$\mathbb{Z}_2$. ואכן אין לו שורשים:

$$\left.\begin{array}{l} f(0)=0+0+1=1\neq 0 \\ f(1)=1+1+1=1\neq 0 \end{array}\right\} \Rightarrow f \text{ אי פריק}$$

$\Leftarrow$ $\mathbb{Z}_2[x]/(x^2+x+1)$ שדה מסדר 4.

בסיס לשדה מעל $\mathbb{Z}_2$ נתון ע"י $1, \bar{x}$. אז

$$L=\{0, 1, \bar{x}, 1+\bar{x}\}$$

$+$	0	1	$\bar{x}$	$1+\bar{x}$
0	0	1	$\bar{x}$	$1+\bar{x}$
1	1	0	$1+\bar{x}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$1+\bar{x}$	0	1
$1+\bar{x}$	$1+\bar{x}$	$\bar{x}$	1	0

$\cdot$	0	1	$\bar{x}$	$1+\bar{x}$
0	0	0	0	0
1	0	1	$\bar{x}$	$1+\bar{x}$
$\bar{x}$	0	$\bar{x}$	$1+\bar{x}$	1
$1+\bar{x}$	0	$1+\bar{x}$	1	$\bar{x}$

$$\bar{x}\cdot\bar{x}=\bar{x}^2$$

$$\bar{x}^2+\bar{x}+1=0 \Rightarrow \bar{x}^2=-\bar{x}-1=\bar{x}+1$$

$$\bar{x}(1+\bar{x})=\bar{x}+\bar{x}^2=\bar{x}+1+\bar{x}=1$$

$$(1+\bar{x})(1+\bar{x})=1+\bar{x}+\bar{x}+\bar{x}^2=1+\bar{x}+1=\bar{x}$$

<u>הגדרה:</u>

(א) עבור $a,b\in R$, d נקרא ממ"מ (gcd) אם $d|a$, $d|b$ ולכל d' כך ש-$d'|a$ ו-$d'|b$ מתקיים $d'|d$.

(ב) עבור $a,b\in R$, m נקרא כ.מ.מ (lcm) אם $a|m$, $b|m$ ולכל m' כך ש-$a|m'$ ו-$b|m'$ מתקיים $m|m'$.

gcd ו- lcm נקבעים ביחידות עד כדי כפל בהפיך.
בתחום פריקות R תמיד קיימים gcd ו- lcm.
אם $a=p_1^{e_1}\cdots p_n^{e_n}$ ו- $b=p_1^{f_1}\cdots p_n^{f_n}$ (חלק מהחזקות אולי 0) אז

$$(a,b)=\gcd(a,b)=\prod p_i^{\min(e_i,f_i)}$$

$$[a,b]=\operatorname{lcm}(a,b)=\prod p_i^{\max(e_i,f_i)}$$

$$\Rightarrow (a,b)[a,b]=ab$$

האלגוריתם של אוקלידס:
עבור $a,b\in R$ כך ש $d(a)\geq d(b)$

$$a=q_1b+r_1$$
$$b=q_2r_1+r_2$$
$$r_1=q_3r_2+r_3$$
$$\vdots$$
$$r_{m-2}=q_mr_{m-1}+r_m$$
$$r_{m-1}=q_{m+1}r_m$$

אפשר להראות ש- $r_m=\gcd(a,b)$ וגם $r_m=av+bu$
כאשר $u,v\in R$
אם $d=(a,b)$ אז $m=\frac{ab}{d}$ הכפולה המשותפת
המינימלית, כי בוודאי $a|m$ ו- $b|m$.
אם $a|m'$ ו- $b|m'$ אז $ab|(av+bu)m'$
ולכן $ab|dm'$ ⇐ $dm|dm'$ ⇐ $m|m'$.

(38) 15.1.08
ת׳ מתנים

שבוע הבא שיעור חזרה.
(נא לשלוח שאלות מראש).

חוגי חבורה

יהי R חוג ו- G חבורה. חוג החבורה

$$R[G] = \left\{ \sum_{g\in G} a_g g \ : \ a_g \in R \right\}$$

כאשר אם G חבורה אינסופית נדרוש שפרט למספר סופי של המקדמים מתאפסים.

החיבור: $\sum a_g g + \sum b_g g = \sum (a_g+b_g) g$

הכפל: $(\sum a_g g)(\sum b_g g) = \sum_{g\in G} \sum_{h\in G} a_g b_h gh =$

$$= \sum_{g\in G} \left(\sum_{g_1 g_2 = g} a_{g_1} b_{g_2} \right) g$$

זה חוג עם יחידה (אם R חוג עם יחידה)

זה חוג קומוטטיבי אמ"מ G, R קומוטטיביים.

<u>דוגמה</u> $R = F$ שדה $G = \mathbb{Z}$.

$$F[\mathbb{Z}] \cong F[X, X^{-1}]$$

ובאופן כללי $F[\mathbb{Z}^n] \cong F[X_1, X_1^{-1}, \dots, X_n, X_n^{-1}]$

<u>טענה:</u> $\mathbb{C}[\mathbb{Z}_2] \cong \mathbb{C} \oplus \mathbb{C}$ $\quad \left(\mathbb{C}[\mathbb{Z}_p] \cong \underbrace{\mathbb{C} \oplus \dots \oplus \mathbb{C}}_{p} \right)$

$$\{ a[0] + b[1] : a, b \in \mathbb{C} \}$$

<u>תזכורת:</u> יהי R חוג עם יחידה אז $e \in R$ מקיים $e^2 = e$

וכן $e \in Z(R)$. אז $R = R_1 \oplus R_2$ כאשר

$R_1 = eR$ $\quad R_2 = (1-e)R$

<u>הוכחת הטענה:</u> נחפש e כמו בתזכורת ב- $\mathbb{C}[\mathbb{Z}_2]$

$$(a[0] + b[1])^2 = a[0] + b[1]$$

$$(a^2+b^2)[0] + 2ab[1]$$

$$\Rightarrow \quad 2ab = b$$
$$a^2+b^2 = a$$
$$\Rightarrow \quad a = \tfrac{1}{2} \quad b = -\tfrac{1}{2}$$
$$\Rightarrow \quad e = \tfrac{1}{2}[0] - \tfrac{1}{2}[1]$$
$$\Rightarrow \quad 1-e = 1[0] - e = \tfrac{1}{2}[0] + \tfrac{1}{2}[1]$$
$$\Rightarrow \quad \mathbb{C}[\mathbb{Z}_2] \cong (e) \oplus (1-e)$$

$$(e) = \left\{\left(\tfrac{1}{2}[0]-\tfrac{1}{2}[1]\right)\left(a[0]+b[1]\right)\right\} =$$
$$= \left\{\frac{a-b}{2}[0] - \frac{a-b}{2}[1]\right\} =$$
$$= \{x[0]-x[1] : x \in \mathbb{C}\}$$
$$(1-e) = \{x[0]+x[1] : x \in \mathbb{C}\}$$

בשביל לסיים נותר להראות ש- $(e),(1-e) \cong \mathbb{C}$.

נגדיר איזומורפיזמים:

$$(e) \longrightarrow \mathbb{C}$$
$$a[0]-a[1] \longmapsto 2a$$

$$(1-e) \longrightarrow \mathbb{C}$$
$$a[0]+a[1] \longmapsto 2a$$

קל לראות שאלה הומומורפיזמים חיבוריים חח"ע ועל. נותר לראות שהם גם כפליים.

$$(a[0]-a[1])(b[0]-b[1]) =$$
$$= 2ab[0] - 2ab[1] \longmapsto 4ab$$

אבל $a[0]-a[1] \to 2a$ $\quad$ $b[0]-b[1] \to 2a$

וזה כפלי.

כנ"ל עבור ההומומורפיזם השני.

למה: יהיו S, R חוגים ותהי G חבורה. נסמן $S^* = U(S)$ האיברים ההפיכים ב-S.
אז יש התאמה חח"ע בין הומומורפיזמים של חוגים $f: R[S] \to S$ לבין זוגות של הומומורפיזמים
$$\left\{ \begin{array}{ll} f_R: R \to S & \text{הומומורפיזם של חוגים} \\ f_G: G \to U(S) & \text{הומומורפיזם של חבורות.} \end{array} \right.$$

הוכחה: בהינתן f_R, f_G נגדיר
$$f\Big(\sum_{g\in G} a_g g\Big) = \sum_{g\in G} f_R(a_g) f_G(g)$$
תרגיל: זה הומומורפיזם של חוגים.
מאידך, בהינתן $f: R[G] \to S$, $f_R: R \to S$ יהיה הצמצום של f לאיברי R (כלומר האיברים מהצורה $R[1]$).
$f_G: G \to S$ יוגדר ע"י צמצום f ל-G (כלומר לקבוצת האיברים מהצורה $1\cdot g$). איברים אלה הפיכים ב-$R[G]$ לכן $f(1g) \in U(S)$.
תרגיל: אלה העתקות הפוכות.

מסקנה: אם $f: G \to H$ הומומורפיזם של חבורות אז יש הומומורפיזם של חוגים יחיד $\varphi: R[G] \to R[H]$ כך ש-φ היא הזהות על R ו-$\varphi|_G = f$!

למה: 1) תהי G חבורה, $H \le G$ סופית. נגדיר $N_H = \sum_{h\in H} h \in R[G]$. אזי $N_H \cdot N_H = |H| \cdot N_H$
ובפרט, אם $|H|$ הפיך ב-R אז $e_H = \frac{N_H}{|H|}$ אידמפוטנט ($e_H^2 = e_H$).
2) אם $H \trianglelefteq G$ (באותם תנאים) אז e_H במרכז של $R[G]$.

הוכחה: 1) נסמן $H = \{h_1, \dots, h_n\}$. אזי
$$(\Sigma h)(\Sigma h) = h_1 \Sigma h + h_2 \Sigma h + \dots + h_n \Sigma h =$$
$$= \Sigma h_1 h + \dots + \Sigma h_n h = \Sigma h + \dots + \Sigma h = |H| N_H$$

בפרט אם $|H|$ הפיך אז

$$e_H \cdot e_H = \frac{N_H}{|H|} \cdot \frac{N_H}{|H|} = \frac{|H| N_H}{|H||H|} = \frac{N_H}{|H|} = e_H$$

2) מספיק להראות ש- $N_H g = g N_H$ לכל $g \in G$

(תרגיל). ואכן

$$N_H g = (\Sigma h) g = \Sigma h \cdot g = \Sigma g g^{-1} h g$$

אבל H נורמלית ולכן $g^{-1} H g = H$

$$\Rightarrow \Sigma g g^{-1} h g \overset{!}{=} \Sigma g h = g(\Sigma h) =$$

$$= g N_H$$

(:

<u>טענה:</u> $\mathbb{C}[S_3] \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$

<u>הוכחה:</u>

(א) יש הומומורפיזם יחיד $\varphi : S_3 \to \mathbb{Z}_2$ (הומומורפיזם המנה $S_3 \to S_3/A_3 \cong \mathbb{Z}_2$).

מהלמה הראשונה יש הומומורפיזם של חוגים $f : \mathbb{C}[S_3] \to \mathbb{C}[\mathbb{Z}_2]$ שהוא העתקה מעל $\mathbb{C}$.

תרגיל: f הומומורפיזם על כי φ על

$$\left(f(\Sigma a_g g) = \Sigma a_g \varphi(g) \right)$$

נסמן $H = A_3 \triangleleft S_3$. נניח b יוצר של H. אז

מהלמה השנייה $e_H = \dfrac{[id] + [b] + [b^2]}{3}$

אידמפוטנט מרכזי.

$$f(e_H) = \frac{[0] + [0] + [0]}{3} = 1 \cdot [0] \in \mathbb{C}[\mathbb{Z}_2]$$

(כי $0 = \varphi(id) = \varphi(b) = \varphi(b^2)$ כי $H = \ker \varphi$)

$$f(1 - e_H) = f(1) - f(e_H) = 0[0]$$

(ב) נסמן $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$

אז $O(A) = 2$ $O(B) = 3$; $ABA^{-1} = B^{-1}$ (תרגיל)

$\Leftarrow$ $\langle A, B \rangle \cong S_3$

בפרט, יש הומומורפיזם $\Psi: S_3 \to GL_2(\mathbb{C}) = U(M_2(\mathbb{C}))$

לכן לפי הלמה הראשונה יש הומומורפיזם $g: \mathbb{C}[S_3] \to M_2(\mathbb{C})$.

g על: כי I_2, A, B, B^2 בתמונה של Ψ וקל לראות שהן מהוות בסיס ל- $M_2(\mathbb{C})$ ולכן g על.

לאן עובר e_H? $g(e_H) = \frac{1}{3}\left(I_2 + \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} + \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}\right) = 0$

$g(1-e_H) = I_2$

(c) נגדיר הומומורפיזם $h: \mathbb{C}[S_3] \to \mathbb{C}[\mathbb{Z}_2] \oplus M_2(\mathbb{C})$ ע"י

$h(a) = (f(a), g(a)) \quad a \in \mathbb{C}[S_3]$

ברור שזה הומומורפיזם כי זה הומומורפיזם בכל רכיב.

$$\mathbb{C}[S_3] = (e_H) \oplus (1-e_H)$$

$$\Rightarrow \ker f = (1-e_H)$$

$$\ker g = (e_H)$$

$$\ker h = \ker f \cap \ker g = \{0\}$$

⇐ ההעתקה חח"ע.

h על כי אם $(a,b) \in \mathbb{C}[\mathbb{Z}_2] \oplus M_2(\mathbb{C})$

אז יש $x \in (e_H)$ רק ש- $f(x) = a$

ויש $y \in (1-e_H)$ רק ש- $g(y) = b$

לכן $h(x+y) = (a,b)$

מכיוון ש- $\mathbb{C}[\mathbb{Z}_2] \cong \mathbb{C} \oplus \mathbb{C}$ נקבל ש-

$$\mathbb{C}[S_3] \cong \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C})$$

(41)

חוג השלמים ה-p-אדיים $\mathbb{Z}_p$ (סליחה על כפולות הסימון)

שלם p-אדי הוא טור פורמלי מהצורה $\sum_{i=0}^{\infty} a_i p^i \quad 0 \le a_i \le p-1$

$\sum a_i p^i = \sum b_i p^i$ אמ"מ $a_i = b_i$ לכל i.

<u>הערה</u>: ניתן לשכן את המספרים הטבעיים ב- $\mathbb{Z}_p$ (כי לכל מספר טבעי יש פיתוח לפי בסיס p).

<u>חיבור</u>: כמו חיבור ארוך רק בבסיס p ובאורך אינסופי.

$$\Sigma a_i p^i + \Sigma b_i p^i = \Sigma c_i p^i$$

כאשר c_i נקבע כך:

אם $a_0+b_0 < p$ אז $c_0 = a_0+b_0$

אחרת $c_0 \equiv a_0+b_0 \pmod p$ ונעביר 1 לעמודה הבאה

וכן הלאה.

דוגמה

$$a = 1 + \overset{1}{0}\cdot p + \overset{1}{0}\cdot p^2 + \ldots$$

$$b = (p-1) + (p-1)p + (p-1)p^2 + \ldots$$

$$a+b = 0 + 0\cdot p + 0\cdot p^2 + \ldots$$

באופן כללי, אם $a = \Sigma a_i p^i$ נכתוב $b = (p-1-a_i)p^i$ ואז

$a+b+1 = 0$ או $-a = b+1$

לא קשה לראות ש- $\mathbb{Z}_p$ הוא חבורה אבלית עם החיבור

ובפרט אפשר לשכן את $\mathbb{Z}$ ב- $\mathbb{Z}_p$.

כפל: כפל ארוך:

$$a = a_0 + a_1 p + a_2 p^2 + \ldots$$

$$b = b_0 + b_1 p + b_2 p^2 + \ldots$$

$$c_0 + c_1 p + c_2 p^2 + \ldots$$

$$d_1 p + d_2 p^2 + \ldots$$

$$\ddots$$

פה יש משהו טריקי: אמנם יש אינסוף שורות אבל בכל עמודה מספר סופי של מחוברים.

$$\Sigma c_i p^i = (\Sigma a_i p^i)(\Sigma b_i p^i)$$

$c_0 = a_0 b_0 \pmod p$ ואם $a_0 b_0 = c_0 + p d_1$ נשמור את d_1

$e_1 = a_1 b_0 \pmod p$ $c_1 = d_1 + e_1$ וכו' נקבל שורה אחת

וכך לכל השורות.

דוגמה

$$-1 = \Sigma (p-1)p^i = (p-1)\Sigma p^i$$

$\Leftarrow$ $\frac{1}{1-p} = \Sigma p^i$ $\Leftarrow$ $1-p$ הפיך ב- $\mathbb{Z}_p$.

אדב שני, $p\cdot\sum a_ip^i = \sum a_ip^{i+1}$ ולכן
p אינו הפיך.

אפשר לראות את הדברים הבאים:

1) $\mathbb{Z}_p$ חוג קומוטטיבי עם יחידה
2) $\mathbb{Z}_p$ תחום שלמות
3) יש הומומורפיזם $\varepsilon : \mathbb{Z}_p \to \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ע"י

$$\sum a_ip^i \longmapsto a_0 \pmod p$$

הגרעין הוא $\ker(\varepsilon) = \{\sum a_ip^i : a_0 = 0\} =$
$= p\mathbb{Z}_p$

מכיוון ש-$\mathbb{Z}/p\mathbb{Z}$ שדה נובע ש-$p\mathbb{Z}_p$ אידיאל
מקסימלי.

<u>טענה</u>: האיברים ההפיכים ב-$\mathbb{Z}_p$ הם
$\{\sum a_ip^i : a_0 \neq 0\}$

<u>מסקנה</u>: ב-$\mathbb{Z}_p$ יש אידיאל מקסימלי יחיד. למה? כי
אם $I \neq p\mathbb{Z}_p$ מקסימלי אז I מכיל איבר הפיך
ולכן $I = \mathbb{Z}_p$.

<u>הגדרה</u>: חוג R עם אידיאל מקסימלי יחיד נקרא חוג מקומי.

4) לכל $a \in \mathbb{Z}_p$ יש הצגה יחידה כ-$p^n \cdot u$ עבור
$n \in \mathbb{N}$ ו-u הפיך ב-$\mathbb{Z}_p$.
5) $a \in \mathbb{Z}$ הפיך ב-$\mathbb{Z}_p$ אמ"מ $(a,p) = 1$.
6) $\mathbb{Z}_p$ חוג ראשי והאידיאלים ב-$\mathbb{Z}_p$ הם
$\{0\}$ ו-$p^k\mathbb{Z}_p$

(42) 18.02.08
ג' מונים

שיעור חזרה

* נתון: $H \lhd G$ וכל $\sigma \in Aut(H)$ פנימי.

צ"ל: $G = H \cdot C_G(H)$

{ $C_G(H) =$ האיברים ב-G שמתחלפים עם כל H
$Z(G) =$ האיברים ב-G שמתחלפים עם כל G $= C_G(G)$ }

אנחנו צריכים להגיד איך נראים האיברים של G וכל מה שאנחנו יודעים זה איזה של H. אז צריך לקחת איבר ב-G ולקשר אותו ל-H. בוודאי הדרך לעשות זאת היא הגדרה שהם אוטומורפיזם של G..

יהי $g \in G$. מכך ש-$H \lhd G$ נובע ש-$gHg^{-1} = i_g(H) = H$
לכן $i_g|_H \in Aut(H)$. לכן קיים $h \in H$ רק ש- $i_g|_H = i_h$
כלומר לכל $x \in H$ $gxg^{-1} = hxh^{-1}$. $\Leftarrow$ $(h^{-1}g)x(h^{-1}g)^{-1} = x$
$\Leftarrow$ $(h^{-1}g)x = x(h^{-1}g)$ $\Leftarrow$ $h^{-1}g \in C_G(H)$ $\Leftarrow$ $g = h\cdot(h^{-1}g) \in HC_G(H)$.

* נתון: G פשוטה ויש $1 \neq g \in G$.
צ"ל: $G = \langle g^G \rangle$ (כלומר G נוצרת ע"י מחלקת הצמידות של g ב-G).

כמובן $\langle g^G \rangle \le G$. אם נראה שהיא נורמלית אז מהפשטות של G היא או שהיא טריוויאלית או שהיא G. אבל יש $1 \neq g \in G$ ברור שהיא תהיה G.

יש טענה כללית יותר שאפשר להוכיח: $S \subseteq G$ תת קבוצה המקיימת $xSx^{-1} \subseteq S$ לכל $x \in G$ $\Leftarrow$ $\langle S \rangle \lhd G$.

נוכיח: לכל $x \in G$: $\langle xSx^{-1} \rangle = x\langle S \rangle x^{-1}$: $\langle S \rangle$ זה כל המילים שאפשר ליצור מאיברי S וההופכיים שלהם. ועכשיו ברור שזה אותו דבר כי פשוט האיברים של $\langle xSx^{-1} \rangle$ הן מילים מאותו $\langle xSx^{-1} \rangle$ אבל ה-x-ים מצטמצמים עם ה-x^{-1}-ים.

מהנתון ש-$xSx^{-1} \subseteq S$ לכל x נובע ש-$xSx^{-1} = S$ לכל x (מאותו שיקול כמו בתחילת נורמליות). עכשיו $\langle S \rangle = \langle xSx^{-1} \rangle = x\langle S \rangle x^{-1}$ וזאת תת חבורה נורמלית.

* חבורה מסדר 117 היא אבלית:

$117 = 3^2\cdot 13$ ⇐ יש שתי חבורות סילו - 3 סילו ו- 13 סילו. מספר חבורות 13-סילו הוא $1 \pmod{13}$ ומחלק את 117 ⇐ מחלק את 9. ⇐ בהכרח יש רק חבורת 13-סילו אחת.

מספר חבורות 3-סילו הוא $1 \pmod 3$ ומחלק את 13 ⇐ או שיש אחת כזו או 13.

תהי N חבורת 13-סילו של G ותהי H חבורת 3-סילו של G כלשהי. ⇐ $H\cap N=\{e\}$, $HN=G$!

$N \triangleleft G$.

ורצה להראות ש-H ו-N מתחלפות כי אז G אבלית (כי כל אחת מהן אבלית) (רק ש-3=סדר)

יהי $x\in H$ אזי $xNx^{-1}=N$ ולכן i_x אוטומורפיזם של N.

$N=\langle y\rangle$ ולכן $xyx^{-1}=y^i$. כמובן $i_x^3=i_{x^3}=id_N$.

מצד שני

$$i_x(y) = y^i$$
$$i_x^2(y) = xy^ix^{-1} = (xyx^{-1})^i = y^{i^2}$$
$$\Rightarrow i_x^3(y) = y^{i^3} = y$$

⇐ $13 / i^3-1$

רג צור הכל! הטענה הראשונה לא נכונה. ניקח $G=\langle x,y,z\rangle$ כאשר x,z מסדר 3

y מסדר 13

z מרכזי ו- $xyx^{-1}=y^3$

זו חבורה מסדר 117 שאינה אבלית.

* א) צ"ל שאין שדה F כך ש- $A_5 \hookrightarrow UT_5(F)$ (UT משולשיות עליונות)

ב) צ"ל של F ש $S_5 \hookrightarrow GL_5(F)$ (זה ברור פשוט בעזרת מטריצות תמורה: לממש השיכון הטבעי) כי $SL_5(F)$ הסימן של תמורה מתאים לדטרמיננטה של המטריצה ולכן לא הדטרמיננטות תהיינה 1).

נוכיח את (א)

נסמן ב- $UN_5(F)$ את המטריצות האוניטריות מסדר 5 מעל F.
קל לראות ש- $UN_5(F) \lhd UT_5(F)$.
ניקח למשל את ההעתקה $UT_5(F) \to (F^*)^5$ שמתאימה לכל מטריצה A את האיברים על האלכסון. זה הומומורפיזם של חבורות. נניח שקיים שדה כנ"ל. נזהה את A_5 עם התמונה שלה ואז $A_5 \subseteq UT_5(F)$. ידוע $A_5 \cap UN_5(F) \lhd A_5$
(כי $UN_5(F)$ נורמלית). $\Leftarrow$ או $A_5 \subseteq UN_5(F)$
או $A_5 \cap UN_5(F) = \{e\}$ (כי A_5 פשוטה)
ידוע נסתור את שני המקרים.
$A_5 \subseteq UN_5(F)$ לא ייתכן כי $UN_5(F)$ נילפוטנטית ; A_5 לא.
סליחה. לא דיוק את זה.
$UN_5(F)$ פתירה! $UT_5(F)/UN_5(F)$ איזומורפית (איזומורפיזם) לתת חבורה של $(F^*)^5$) ולכן $UT_5(F)$ פתירה וזה לא יכול להיות ש- A_5 איזומורפית לתת חבורה של חבורה פתירה.

שיעור חזרה על שמ'

שאלות:

① G חבורה $H\le G$ ו- $[G:H]=4$ אז G אינה פשוטה.
② האם $M_2(\mathbb{R})$ ו- $M_3(\mathbb{R})$ איזומורפיים כחוגים?
③ G חבורה הפועלת על חבורה H האם [illegible] היא תת חבורה?
④ G חבורה סופית. $H\trianglelefteq G$. $\gcd(|H|,[G:H])=1$. $K\le G$ רק ש- $|K|=|H|$. צ"ל: $K=H$.

תשובות:

① צריך למצוא תת חבורה נורמלית (לא טריוויאלית). G פועלת על המחלקות של H ב- G. G/H ולכן יש הומומורפיזם $\varphi: G\to Per(G/H)\cong S_4$. הרעיון של זה נחקה הכפל פעם לא טריוויאלי. הרי $g(g'H)=(gg')H$.
$\ker\varphi=\{g\in G : gg'H=g'H\}$
בפרט אם $g\in\ker\varphi$ אז $gH=H$ $\Rightarrow$ $\ker\varphi\subseteq H$.
אז $G\neq\ker\varphi$. ועכשיו צריך להראות שהגרעין אינו $\{e\}$.
נניח בשלילה ש- $\ker\varphi=\{e\}$. אז $G\hookrightarrow S_4$ חח"ע. כלומר G תת חבורה של S_4.
$|S_4|=24=4\cdot3\cdot2$ $\Rightarrow$ $|G|$ יכול להיות 4, 8, 12 או 24.
אם $|G|=4$ אז $G\cong\mathbb{Z}_4$ או $G\cong\mathbb{Z}_2\times\mathbb{Z}_2$ אבליות ולכן לא פשוטות.
אם $|G|=8$ אז G אבלית או $G\cong D_4$ או $G\cong Q$ ובכל אופן אלה לא פשוטות (אבליות הן פשוטות רק אם הן מסדר ראשוני, ול- D_4 יש תת חבורה נורמלית - זאת שנוצרת ע"י הסיבובים ול- Q יש תת חבורה מאינדקס 2).
אם $|G|=12$ האינדקס של H הוא 4 ולכן $G\cong A_4$ ו- A_4 אינה פשוטה כי $A_4\triangleright V=\{id,(12)(34),\dots\}$. A_4 היא ה- A_n היחידה שלא פשוטה.
אם $|G|=24$ אז $G=S_4$ ו- S_4 לא פשוטה, שהרי $A_4\triangleleft S_4$.
* אם $H\le G$ רק ש- $[G:H]=n$ אז יש $\varphi: G\to S_n$ רק ש- $\ker\varphi\le H$ ולכן אם G פשוטה אז φ שיכון של G ב- S_n.

(2) נניח ש- $\varphi: M_2(\mathbb{R}) \to M_3(\mathbb{R})$ איזומורפיזם של חוגים. אז φ משרה איזומורפיזם של מרחבים וקטוריים מעל $\mathbb{R}$: ברור ש-φ שומר על חיבור. הוא שומר גם על הכפל בסקלר כי
$\varphi(rA) = \varphi((r\,r)A) = \varphi(r\,r)\varphi(A)$
ועכשיו צריך להראות $\varphi(r\,r)\varphi(A) = r\varphi(A)$. טוב, לא מתחיל להיות מסובך. ועזבו את זה.

(4) בודאי מספיק להראות ש- $K \subseteq H$. נתבונן בחבורת המנה G/H. התמונה של K תחת ההטלה הטבעית $G \to G/H$ היא KH/H. ממשפט האיזומורפיזם השני $KH/H \cong K/K\cap H$. $|H| = |K| = |H\cap K|\,|K/H\cap K|$
$\Leftarrow$ $|H|\;|\;|KH/H|$ ומצד שני $|KH/H|\;|\;|G/H|$. לכן מהנתון נובע ש- $|KH/H| = 1$ $\Leftarrow$ $KH \subseteq H$ $\Leftarrow$ $K \subseteq H$ $\Leftarrow$ $K = H$.

מבנה הבחינה:
- 1 מתוך 2 - אשפסטים (כ- 30%)
- 2 מתוך 3 - תרגילים (כ- 40%)
- 4 מתוך 5 - שאלות קצרות (כ- 30%)

* חבורה מסדר p^2q (p, q ראשוניים) היא פתירה.
איך ניגשים לשאלה כזאת? קודם כל צריך למצוא תת חבורה נורמלית כך שהמנה אבלית ואז ננסה להמשיך את הסדרה.
נתבונן בחבורות q-סילו. נניח שיש n כאלה. אז $n | p^2$ (כי $n | p^2q$ וגם $n \nmid q$). אם $n=1$ אז יופי. נבדוק את האפשרויות האחרות. מאחר ש- $n \equiv 1 \pmod q$ אז או ש- $1+kq = p$ או ש- $1+kq = p^2$.
נניח שיש m חבורות p-סילו. אז $m=1$ או $m=q$ ובנוסף $m=1+kp$.
נניח $1+kp = q$ אז $q-1 = kp$ $\Leftarrow$ $p | q-1$. אם $p \geq q$ אז זה לא יתכן. $\Leftarrow$ $p < q$.

<u>בסיכום:</u>
א. $p \geq q$. אז יש חבורת p-סילו יחידה כי מספר חבורות p-סילו הוא 1 או q; $1+kp = q$ $\Leftarrow$ $p | q-1$ וזו סתירה.
לכן יש חבורה תקינה ונורמלית מסדר p^2 H; $|G/H| = q$

חבורה מסדר p^2 היא אבלית – לכן פתירה. חבורה מסדר q גם פתירה.
לכן G פתירה.

I $q<p$. מספר חבורות q סילו הוא 1 או p או p^2.
אם המספר הוא p נקבל ש- $p=1+kq \Rightarrow q|p-1$ וכו'
סתירה. $\Rightarrow$ או שיש 1 או שיש p^2. נניח שהמספר הוא p^2.
אז $p^2=1+kq \Rightarrow q|p^2-1 \Rightarrow q|p-1$ או $q|p+1$
(כי q ראשוני). ואמרנו לגבי $q|p-1$ ראינו קודם. אם $q|p+1$
$q>p \Rightarrow q=p+1 \Rightarrow$ מתקבל $q=3$ $p=2$ אז
$|G|<59$ ולכן סתירה. $\Rightarrow$

אם מספר חבורות q סילו הוא 1 אזי תהי נורמלית H מסדר q.
$|G/H|=p^2$ ומסיימים כמו קודם.