03/08/2011

מרצה: מיכאל מגרלי
מייל: megereli@math.biu.ac.il
אתר: www.math.biu.ac.il/~megereli

ספר מומלץ: מבנים אלגבריים - או"פ.

הרצאה 1 - אלגברה מופשטת

הגדרה: נניח ש-X קבוצה לא ריקה. פונקציה $X\times X \xrightarrow{w} X$

$(a,b)\mapsto w(a,b)$ = $a\cdot b$, $a+b$, $a*b$, $a\oplus b$ — סימונים אפשריים

סימון: (X,w) או $(X,\cdot)$ ...

הזוג נקרא מבנה אלגברי.

הערה: $(\mathbb{N},+)$ $(\mathbb{N},\cdot)$ מבנים.

הפרש - ב-$\mathbb{N}$ לא מוגדר היטב.

לעומת זאת, $(\mathbb{Z},-)$ כן מוגדר היטב ולכן מבנה אלגברי.

הגדרות נוספות:

1) קומוטטיביות: מבנה אלגברי $(X,\cdot)$ נקרא קומוטטיבי (חילופי) אם $x\cdot y = y\cdot x$, $\forall x,y\in X$

למשל: $(\mathbb{Z},-)$ לא קומוטטיבי. $Mat_{n\times n}(\mathbb{R})$ (מטריצות מעל $\mathbb{R}$) לא קומוטטיבי לגבי כפל אבל כן לגבי חיבור.

2) אסוציאטיביות: מבנה נקרא אסוציאטיבי אם $(x\cdot y)\cdot z = x\cdot(y\cdot z)$

⇓

2* שדרוג: אסוציאטיביות מוכללת: אין השפעה של סוגריים במכפלה של כל n איברים מ-X.

$n=3$: = ②

3) אגודה: מבנה אלגברי (אסוציאטיבי) נקרא אגודה או חבורה למחצה (semigroup).

למשל: $(Mat_{n\times n}(\mathbb{R}),+)$, $(\mathbb{N},\cdot)$, $(\mathbb{N},+)$, $(Mat_{n\times n}(\mathbb{R}),\cdot)$, $(P(X),\cap)$ ...

כן אגודות.

$(\mathbb{Z},-)$ לא אגודה.

4) איבר ניטרלי: איבר z במבנה $(X,\cdot)$ נקרא ניטרלי אם $x\cdot z = z\cdot x = x$ $\forall x\in X$

בד"כ ניטרלי מסומן כ-e.

$\cdot$	... I, 1, 1
$+$	... 0, 0

Generated by CamScanner from intsig.com

הרבה מסמנים אותו גם דרך e $\boxed{x\cdot e = e\cdot x = x}$

טענה: ניטרלי יש לכל היותר אחד.

הסבר: נניח ש- e, e' ניטרליים

$$e = e\cdot e' = e'$$

5) אגודה עם ניטרלי נקראת **מונואיד** (monoid)

דוג: $(P(X), \cap)$ מונואיד עם $e := X$

$(\mathbb{N}, +)$ לא מונואיד (רק אגודה). $\{1,2,\dots\}$

6) **חזקות, כפולות** באגודה $(X, \cdot)$.

$a^n := \underbrace{a\cdot a \cdots a}_{n}$, $n\in\mathbb{N}$.

כללים:
- חזקה: $\boxed{(a^n)^m = a^{nm}}$ $\boxed{a^{n+m} = a^n\cdot a^m}$ $a\in X$, $n,m\in\mathbb{N}$

דוגמה: נגדיר מבנה $(X, \cdot)$. $X=\{a,b\}$, $a\neq b$

·	a	b
a	b	b
b	a	a

$$a^2\cdot a = b\cdot a = a$$
$$\neq \qquad \neq$$
$$a\cdot a^2 = a\cdot b = b$$

⇓

שים לב! X לא אגודה!

אם נתונה אגודה $(X, +)$

- **כפולה:** $na := \underbrace{a+a+\dots+a}_{n}$

כללים: $\boxed{m(na) = (mn)a}$ $\boxed{(n+m)a = na+nm}$

- במונואיד $(X, \cdot)$ מגדירים גם $a^0 = e$
- במונואיד $(X, +)$ עם ניטרלי 0_X. $0a = 0_X$

⇐

$(X,\cdot)$	$a^0 = e$
$(X,+)$	$0\cdot a = 0_X = e$

7) **הופכי (נגדי):** במונואיד $(X,\cdot)$ איבר $a\in X$ נקרא **הפיך** אם קיים $b\in X$ כך שמתקיים $\boxed{a\cdot b = b\cdot a = e}$

הערה: אם $a\cdot b = e$ אז אומרים ש- a הפיך מימין.
$b\cdot a = e$ משמאל.

- במונואיד $(X,+)$ $a+b=b+a=0_X$.

בהגדרה + קומוטטיבי.

טענה (יחידות של ההופכי)

במונואיד $(X,\cdot)$ לכל $a\in X$ יש לכל היותר הפוך אחד.

הסבר: נניח $b,b'\in X$ הפוכים ל-a.

מתקיים
$$\begin{cases} a\cdot b=b\cdot a=e \\ a\cdot b'=b'\cdot a=e \end{cases}$$

$a\cdot b=e$ (כפל ב-b')

ניטרלי $\left(\left(\begin{matrix} b'(a\cdot b)=b'\cdot e \\ (b'\cdot a)\cdot b=b' \end{matrix}\right)\right)$ אסוציאטיבי

$e\cdot b=b'$
$\Downarrow$
$b=b'$ כנדרש

מסמנים הפוך ל-a בדרך a^{-1}.

אם הפעולה היא חיבור אז: $-a$ (נסמן $-a$)

(8) מונואיד $(X,\cdot)$ שבו כל האיברים הפיכים נקרא חבורה - Group

כלומר: א) אסוציאטיביות

ב) קיום ניטרלי $=$ חבורה.

ג) כל איבר הפיך

(9) חבורה קומוטטיבית נקראת גם **חבורה אבלית** (Abel)

דוגמאות: + $\mathbb{C}$ $\mathbb{R}$ $\mathbb{Q}$ $\mathbb{Z}$ $5\mathbb{Z}$ $\{0\}$ כן חבורה (אבלית)

· $\mathbb{R}_+=\mathbb{R}\cap(0,\infty)$ $\mathbb{Q}_+=\mathbb{Q}\cap(0,\infty)$ $\{1\}$ כן חבורה (אבלית)

$\mathbb{C}^*:=\mathbb{C}\setminus\{0\}$ $\mathbb{R}^*:=\mathbb{R}\setminus\{0\}$

מונואיד אבל לא חבורה: $(\mathbb{R},\cdot)$, $(Mat_{n\times n}(\mathbb{R}),\cdot)$ לא.

$n=1$

* $GL_n(\mathbb{R}) := \{A\in Mat_{n\times n}(\mathbb{R}) \mid det(A)\neq 0\}$ General Leaner Group

שקול להפיכות מטריצה

$(GL_n(\mathbb{R}),\cdot)$ **חבורה** היא אבלית $\Leftarrow$ $n=1$ (ואז היא $\mathbb{R}^*$)

- במונואיד $(X,+)$ $a+b=b+a=0_X$.

אסוציאטיבי + קומוטטיבי

טענה: (יחידות של ההופכי)

במונואיד $(X,\cdot)$ לכל $a\in X$ יש לכל היותר הופכי אחד.

הוכחה: נניח $b,b'\in X$ הופכים ל-a.

מתקיים
$$\begin{cases} a\cdot b=b\cdot a=e \\ a\cdot b'=b'\cdot a=e \end{cases}$$

$a\cdot b=e$ (נכפיל ב-b')

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

אסוציאטיבי $\left(\left((b'\cdot a)\cdot b=b'\right)\right)$ ניטרלי

$$e\cdot b=b'$$
$$\Downarrow$$
$b=b'$ מש"ל

מסמנים הפיך ל-a ע"י a^{-1}.

אם הפעולה היא חיבור אז: $-a$ (נגדי a-ל)

8) מונואיד $(X,\cdot)$ שבו כל האיברים הפיכים נקרא חבורה - Group.

ציינו: א) אסוציאטיביות

ב) קיום ניטרלי $=$ חבורה.

ג) כל איבר הפיך

9) חבורה קומוטטיבית נקראת גם חבורה אבלית (Abel)

דוגמאות: $+$ $\mathbb{C}$ $\mathbb{R}$ $\mathbb{Q}$ $\mathbb{Z}$ $5\mathbb{Z}$ $\{0\}$ כן חבורה (אבלית)

$\cdot$ $\mathbb{R}_+=\mathbb{R}\cap(0,\infty)$ $\mathbb{Q}_+=\mathbb{Q}\cap(0,\infty)$ $\{1\}$ כן חבורה (אבלית)

$\mathbb{C}^*:=\mathbb{C}\setminus\{0\}$ $\mathbb{R}^*:=\mathbb{R}\setminus\{0\}$

מונואיד אבל לא חבורה: $(\mathbb{R},\cdot)$, $(Mat_{n\times n}(\mathbb{R}),\cdot)$ לא $n=1$

$*$ $GL_n(\mathbb{R}):=\{A\in Mat_{n\times n}(\mathbb{R}) \mid det(A)\neq 0\}$ General Leaner Group

$\Downarrow$ שקול להפיכות מטריצה

$(GL_n(\mathbb{R}),\cdot)$ חבורה היא אבלית $\Leftrightarrow$ $n=1$ (זה $\mathbb{R}^*=$)

Generated by CamScanner from intsig.com

דוגמא חשובה: $(\mathbb{Z}_n, \oplus)$ חבורה אבלית (ואף ציקלית) עם n איברים.

הגדרת $\mathbb{Z}_n$: "שאריות מודולו n"

n=2: $\mathbb{Z}_2 = \{[0],[1]\}$

חיבור מודולו 2: $[2\mathbb{Z}]$

$\oplus$	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

$[0] := 2\mathbb{Z}$ $\quad U = \mathbb{Z}$

$[1] := 2\mathbb{Z}+1$ $\quad U = \mathbb{Z}$.

כפל $[2\mathbb{Z}+1]$

$\odot$	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

באופן כללי: מגדירים יחס $\equiv$ ב-$\mathbb{Z}$

$a \equiv b \bmod n \overset{\text{def}}{\iff}$ (הגדרה) $n \mid a-b$ (n מחלק את a-b)

$\Updownarrow$

$\frac{a-b}{n} \in \mathbb{Z}$

$\Updownarrow$

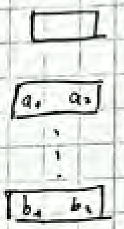
ל-a ול-b יש שאריות מודולו n.

תרגיל:

$\equiv$ יחס שקילות (על n) בקבוצה $\mathbb{Z}$.

יש n מחלקות שקילות:

חלוקה של $\mathbb{Z}$:
$$\begin{cases} [0] := n\mathbb{Z} \\ [1] := n\mathbb{Z}+1 \\ \vdots \\ [n-1] := n\mathbb{Z}+(n-1) \end{cases}$$



$$\boxed{[a]=[b] \iff a \equiv b \bmod n}$$

הגדרת החיבור $\oplus$ והכפל $\odot$ ב-$\mathbb{Z}_n$:

$[a] \oplus [b] := [a+b]$ (+ ב-$\mathbb{Z}$, $\oplus$ ב-$\mathbb{Z}_n$)

$[a] \odot [b] := [a \cdot b]$ (· ב-$\mathbb{Z}$, $\odot$ ב-$\mathbb{Z}_n$).

$[a]=[a]_7=\bar{a}=a$

<u>תרגיל:</u> אין תלות בנציגים.

$a_1 \equiv a_2 \mod n$
$b_1 \equiv b_2 \mod n$ $\Leftarrow$ $a_1+b_1 \equiv a_2+b_2$
$a_1 b_1 \equiv a_2 \cdot b_2$

לכן הפעולות מוגדרות היטב.

$(\mathbb{Z}_n, \bullet)$ חבורה אבלית

* אסוצ' + קומוט' נובע מהתכונות של + ב-$\mathbb{Z}$.
* ניטרלי $[0]$
* הנגדי ל- $[a]$ שווה $[-a]$ $(=[n-a])$

<u>טענה:</u> $(\mathbb{Z}, \odot)$ <u>מונואיד קומוטטיבי</u>

* אסוצ' + קומו'
* ניטרלי $[1]$.

<u>תזכורת:</u> $(\mathbb{Z}_n, \oplus, \odot)$ שדה $\Leftrightarrow$ $n=p$ ראשוני.

↗ באופן כללי זה "חוג".

- $(\mathbb{Z}_n, \oplus)$ <u>חבורה ציקלית</u> כי כל איבר $[a] \in \mathbb{Z}_n$ שווה לכפולה של איבר מסוים

$\boxed{[a]=a[1]}$

<u>דוגמא:</u> ב- $(\mathbb{Z}_3, \oplus)$

$[1]$
$[2] = [1] \oplus [1]$
$[0] = [1] \oplus [1] \oplus [1]$

$[1]$ הוא "יוצר" של החבורה. יש כאן "מעגל":

$[1] \oplus [1] \oplus [1] \oplus [1] = [1]$

<u>הגדרה:</u> חבורה $(X, \cdot)$ (קרויה <u>ציקלית</u>) אם קיים איבר $a \in X$ כך שכל איבר $x \in X$ שווה לחזקה מסוימת של a.

כ"א $X = \{a^k \mid k \in \mathbb{Z}\}$ ואומרים ש-a יוצר של X.

<u>הערה חשובה:</u> X חבורה, לכן a הפיך ב-X ואז מותר להשתמש גם בחזקות שליליות.

Generated by CamScanner from intsig.com

הגדרה: נניח $(X,\cdot)$ מונואיד, a הפיך ב-X.

אז מגדירים $a^{-k} := (a^{-1})^{k} \overset{\text{(תרגיל)}}{=} (a^{k})^{-1}$ $k>0$ שלם.

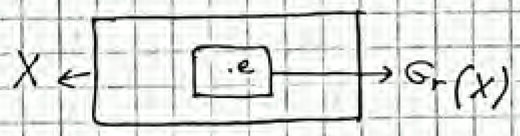
אז ניתן להרחיב את הכללים הנ"ל עבור חזקות $k\in\mathbb{Z}$.

משפט: נניח $(X,\cdot)$ מונואיד. נסמן $Gr(X) := \{a\in X \mid a \text{ הפיך ב-} X\} \subseteq X$

אז $(Gr(X),\cdot)$ חבורה. (נקרא "חבורת ההפיכים של X").

(צמצום הפעולה)

הוכחה:



1. e נמצא בתוך $Gr(X)$ מתי $e\cdot e=e \Rightarrow e^{-1}=e$.

2. $a,b\in Gr(X) \Rightarrow (a\cdot b)^{-1} = b^{-1}\cdot a^{-1}$ (סגירות)

כי $(a\cdot b)\cdot(b^{-1}\cdot a^{-1}) = (b^{-1}\cdot a^{-1})(a\cdot b) = e$

$$\Downarrow$$

$$\boxed{a,b\in Gr(X) \Rightarrow a\cdot b\in Gr(X)}$$

3. $a=(a^{-1})^{-1} \Rightarrow a^{-1}\in Gr(X) \Rightarrow a\in Gr(X)$.

צריך קיבוץ

1. איבר ניטרלי 2. סגירות 3. איברים הופכיים.

ואסוציאטיביות תכונה תורשתית מ-X.

$$\Downarrow$$

$Gr(X)$ חבורה.

משל

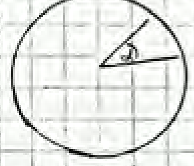
דוגמאות:

$(X,\cdot)$	$Gr(X)$	
$Mat_{n\times n}(\mathbb{R})$	$GL_n(\mathbb{R})$	
$(\mathbb{Z},\cdot)$	$\Omega_2 := \{-1,1\}$	נראה בהמשך
$(P(X),\cap)$	$(\{X\},\cap)$	

דוגמה חשובה של חבורות ציקליות

$\mathbb{T} = \{z \mid \|z\| = 1\} \supset \Omega_n = \{z \in \mathbb{C} \mid z^n = 1\}$

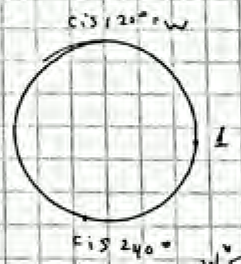
$z = \cos\alpha + i\sin\alpha = cis\,\alpha$



$\Omega_1 = \{1\}$

$\Omega_2 = \{1, -1\}$

$\Omega_3 = \{w, w^2, 1\}$, $w = cis\,120°$



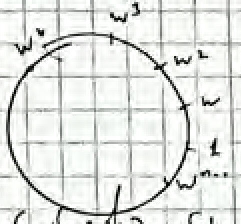
$\Omega_4 = \{i, -1, -i, 1\} = \{w, w^2, w^3, 1\}$, $w = cis\,90°$

$\vdots$

$\Omega_n = \{w, w^2, \dots, w^{n-1}, 1\}$

$w = cis\left(\frac{360°}{n}\right) = e^{i\frac{2\pi}{n}}$

$(cis\,\alpha)^n = cis\,n\alpha$



טענה: $(\Omega_n, \cdot)$ חבורה אבלית (ואף ציקלית)

(כי: $1 \in \Omega_n$, $z \in \Omega_n \Leftarrow z^{-1} \in \Omega_n$. הכל מתקיים ב-$\Omega_n$.)

אחד מהיוצרים האפשריים של Ω_n הוא $w = cis\left(\frac{360°}{n}\right) = e^{i\frac{2\pi}{n}}$

הערה:

$(\Omega_n, \cdot) = \{w^1, w^2, \dots, w^{n-1}, 1\}$

$\cong$ — איזומורפיזם

$(\mathbb{Z}_n, \oplus) = \{[1], [2], \dots, [n-1], [0]\}$

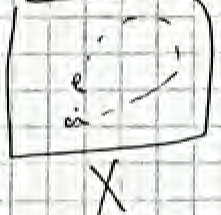
$\langle w \rangle = \{w^k\}_{k \in \mathbb{Z}} = \Omega_n$

$\langle [1] \rangle = \{k \cdot [1]\}_{k \in \mathbb{Z}} = \mathbb{Z}_n$ — סימון לחבורה ציקלית

סימון: נניח X חבורה, $a \in X$.

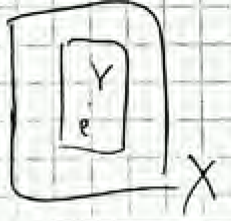
$\langle a \rangle = \{a^k\}_{k \in \mathbb{Z}}$

תת חבורה של X (ציקלית) הנוצרת ע"י a.



תת ציקלית $\langle a \rangle$

הגדרה: נניח Y תת קבוצה לא ריקה בחבורה X.
אומרים ש-Y תת חבורה של X (ונסמן $Y \leq X$), אם Y מבנה לגבי פעולת הכפל כך ש-Y גם חבורה.



דוגמאות: + $\{0\} \le 5\mathbb{Z} \le \mathbb{Z} \le \mathbb{R}$

$(\mathbb{N}\cup\{0\},+) \subset (\mathbb{Z},+)$

רק מונואיד (לא תת חבורה).

דוגמאות של חבורות ציקליות אינסופיות:

לשבי $\langle 5\rangle := \{5^k\}_{k\in\mathbb{Z}} \le \mathbb{Q}^*$

תת ציקלית אינסופית $A=\begin{pmatrix}1&1\\0&1\end{pmatrix}$

$$\langle A\rangle = \{A^k\}_{k\in\mathbb{Z}} = \left\{\begin{pmatrix}1&k\\0&1\end{pmatrix}\right\}_{k\in\mathbb{Z}} \le GL_2(\mathbb{Q})$$

$$\cong (\mathbb{Z},+)$$

הגדרה: X חבורה, $a\in X$

סדר של a מוגדר

$$O(a)=|a| := \begin{cases}\min\{k\in\mathbb{N} \mid a^k=e\} \\ \infty & \text{אם אין } k \text{ כזה}\end{cases}$$

"Order"

דוגמאות:

① $X=\Omega_{10}$ $\quad O(w)=10 \quad O(w^2)=5 \quad O(2)=\infty$

② $X=\mathbb{Q}^*$

③ $X=(\mathbb{Z},+)$ $\quad O(1)=\infty,\ O(3)=\infty$

הערה: נוכיח בהמשך של חבורה ציקלית אינסופית $\cong (\mathbb{Z},+)$ כל חבורה
ציקלית עם n איברים $\cong (\mathbb{Z}_n,\oplus_n)$

תכונות:

[1] $O(a)=1 \iff a=e$

[2] $O(a)=2 \Rightarrow a=a^{-1}$

$$O(a)=2 \iff \begin{cases}a=a^{-1}\\ a\ne e\end{cases}$$

[3] אם G חבורה ציקלית עם n איברים. אז לכל $g\in G$ מתקיים $g^n=e$

$O(a)=n$ $\quad \{e,a,\dots,a^{n-1}\}$ (n איברים!)

הסבר: קיים $a\in G$ כך ש- $\langle a\rangle = G = \{a^k\}_{k\in\mathbb{Z}}$. לכן כל $g\in G$ שווה ל- a^k

$\exists k \quad g^n=(a^k)^n=a^{kn}=(a^n)^k=e^k=e$

להשלמת החסבר מספיק להוכיח שהאיברים $e,a,a^2,\dots,a^{n-1}$ רק שונים.

אם נניח $a^i=a^j$ (לכן $i<j$) $\quad a^{j-i}=e \quad 0<j-i<n \in \mathbb{N}$

סתירה להגדרת הסדר. מש"ל

Hofit Marzouk

04/08/2011

המשך - סדר

טענה: נניח X חבורה, $a\in X$. הוכח $O(a)|m \Leftrightarrow a^m=e$.

הסבר: $(\Leftarrow)$ $n=O(a)|m$.

$\exists q\in\mathbb{Z}$ $m=nq$

$a^m=a^{nq}=(a^n)^q=e^q=e$.

$(\Rightarrow)$: נחלק m ב-n: $m=nq+r$, r שארית $0\le r<n$.

שקול להוכיח $r=0$:

$r=m-nq$

$a^r=a^{m-nq}=a^m\cdot(a^n)^{-q}=e\cdot e^{-q}=e$.

מכאן נובע ש-$r=0$.

אחרת נקבל ש- $0<r<n$ ו- $a^r=e$, בסתירה למינימליות של $n=O(a)$. משל

טענה: (חוק הצמצום)

נניח ש-a הפיך במונואיד X. אז ניתן "לצמצם" ב-a.

כלומר

$a\cdot x=a\cdot y \Rightarrow x=y$.

$x\cdot a=y\cdot a \Rightarrow x=y$.

הסבר: a הפיך, לכן קיים a^{-1}. $a\cdot x=a\cdot y$

$a^{-1}(a\cdot x)=a^{-1}(a\cdot y)$

$(a^{-1}\cdot a)\cdot x=(a^{-1}\cdot a)\cdot y$

$x=y$ משל

- באופן דומה II.

טענה: (משוואה אלמנטרית)

אם a הפיך במונואיד X אז לכל "משוואה אלמנטרית"

(בצד: פתרון יחיד, אפשר פתרון?)

I $a\cdot x=y$ $x=?$

II $x\cdot a=y$

יש פתרון יחיד והוא שווה

I $x=a^{-1}\cdot y$

II $x=y\cdot a^{-1}$

הסבר: $a\cdot x=y \Leftrightarrow a^{-1}(a\cdot x)=a^{-1}\cdot y \Leftrightarrow \boxed{x=a^{-1}\cdot y}$ I

יש יחידות!

Generated by CamScanner from intsig.com

דוגמה $[5]_{54} \cdot x = [3]_{54}$

משוואה במונואיד $(\mathbb{Z}_{54}, \odot)$.

לפי הטענה ⇐ $x = [5]^{-1} \odot [3] = [11] \cdot [3] = [33]$

$[5] \odot [11] = [55]_{54} = [1]$ (בדקו הפוך:)

יש קומוטטיביות

$[5]^{-1} = [11]$

תשובה: $x = [33]_{54} \in \mathbb{Z}_{54}$ פתרון יחיד!

״גישה אחרת״

לפתור בשלמים

$5 \cdot x = 3 \mod 54$, $x \in \mathbb{Z}$

דרך א׳: ישר מהמשוואה נקבל $x \in \{54k+33 \mid k \in \mathbb{Z}\}$ אינסוף פתרונות.

דרך ב׳:

$5x \equiv 3 \mod 54$

$11 \cdot 5x \equiv 11 \cdot 3 \mod 54$

$55x \equiv 33 \mod 54$

$1 \cdot x \equiv 33 \mod 54$

תשובה: $x \equiv 33 \mod 54$

⇕

$x \in \{54k+33 \mid k \in \mathbb{Z}\}$

מונואיד וחבורה של פונקציות.

נניח $X \neq \emptyset$ נסמן $Map(X,X) := \{f : X \to X\} = X^X$

מונואיד לגבי פעולת ההרכבה.

$X \xrightarrow{f_1} X \xrightarrow{f_2} X$

$Map(X,X) \ni f_2 \circ f_1$ ← מוגדר.

$(f_2 \circ f_1)(x) := f_2(f_1(x))$

* $(f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3)$

* $f \circ id = id \circ f = f$

$1_X = id_X = id =$ ״יחידה״.

הגדרה: ״חבורה סימטרית״ מעל קבוצה X היא חבורת ההפיכים של המונואיד $(Map(X,X), \circ)$.

הסימון: $S_X := Gr(Map(X,X))$.

קל לבדוק ש- $S_X = \{f : X \to X \mid f$ חח״ע ועל$\}$ ״התמורות״

$\exists g : \; f \circ g = g \circ f = id$

הערה: X סופי ⟵ אז מספיק אחד מהתנאים: חח״ע או על.

במקרה פרטי של

$X := \{1,2,\dots,n\}$ נסמן S_n

ז"א

$$S_n = \left\{ \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \;\middle|\; i_k \in \{1,\dots,n\} \text{ שונים} \right\}$$

מס' איברים = מס' תמורות = $n!$

n=1: $S_1 := \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} = e \right\}$ חבורה טריוויאלית.

n=2: $S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = e \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = a \right\}$

·	e	a
e	e	a
a	a	e

n=3: $|S_3| = 6$

$$\left\{ e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad a\circ\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \dots \right\}$$

-נחשב עוד איברים אחרים באמצעות a, σ למשל

$$a\circ\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

מתחילים מימין!

$1 \xrightarrow{\sigma} 2 \xrightarrow{a} 3$

$$\boxed{\sigma\circ a \neq a\circ\sigma}$$

$1 \xrightarrow{a} 2 \xrightarrow{\sigma} 1$

תרגיל: להשלים את הרשימה ולבנות את הטבלה רק של החישובים $\begin{pmatrix} 1 & 2 & 3 \\ 1 & & \end{pmatrix}$ הם דרך e, a, σ

שימו לב:

$O(\sigma) = 2 \qquad \sigma^2 = e$

$O(a) = 3 \qquad a^3 = e$

לפעמים נוח יותר לכתוב

$\sigma := (1,2)$

$a := (1,2,3)$

מחזורים = ציקלים

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

למשל ב-S_5

$2 \to 5 \to 4 \to 2$ $\qquad$ $1 \to 3 \to 1$

הערה: ראינו שחבורה S_3 לא קומוטטיבית. זה נכון עבור S_n $\Leftarrow$ $n \geq 3$.

צריך לזכור: ∄ חבורה בעלת סדר קטן מ-6 קומוטטיבית. (סדר = מספר איברים)

תרגיל:

במונואיד $Map(\mathbb{N},\mathbb{N})$ קיימים איברים הפיכים רק מצד אחד.

הסבר:

$$f := \begin{pmatrix} 1 & 2 & 3 & \cdots \\ 2 & 3 & 4 & \cdots \end{pmatrix}$$

$f(n) = n+1$.

ז"א

חח"ע אבל לא על ($f^{-1}(1)$ צריך להיות 0, שלא נמצא ב-$\mathbb{N}$).

ולכן הפיכה רק משמאל.

נראה גם h הפיכה רק מימין: למשל

$$h := \begin{pmatrix} 1 & 2 & 3 & \cdots \\ ? & 1 & 2 & \cdots \end{pmatrix}$$

$$h(n) = \begin{cases} n-1 & n \geq 2 \\ ? & n=1 \end{cases}$$

כל מי שיהיה

ולכן אם $h(1)=k$ אז ל-$h^{-1}(k)$ יהיו שני ערכים $(1, k+1)$.

כלומר לא חח"ע ולכן הפיכה רק מימין.

Generated by CamScanner from intsig.com

בקשר לצמצומים (ולא רק)

הגדרה: איבר a במונואיד X נקרא ==idempotent== אם מתקיים $a^2=a$.

דוגמא:
① $a=e$ בכל מונואיד.
② $0\in(\mathbb{R},\cdot)$
③ $[6]\in(\mathbb{Z}_{30},\odot)$
④ $X=\{1,2,3\}$ $Map(X,X)$

$f_1=\begin{pmatrix}1&2&3\\1&1&1\end{pmatrix}$ מס' איברים ב- $Map = 3^3$.

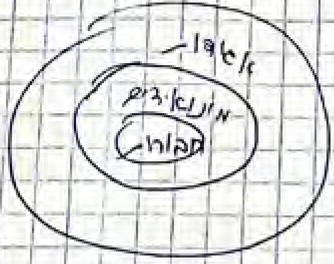
$f_1(x)=1 \quad \forall x\in X$

$g=\begin{pmatrix}1&2&3\\1&1&3\end{pmatrix}$

$f_1^2=f_1, \quad g^2=g$.

הערה: בחבורה ה-idempotent רק e.

שאלה:
א. מתי אגודה משוכנת לתוך מונואיד? תמיד!
ב. מתי מונואיד שוכן לתוך חבורה? לא תמיד!



שאלה:
נתונה אגודה X נרצה למצוא מונואיד $Y\subset X$
פעולה ב-X היא פעולת צמצום מ-Y
נגדיר $Y:=X\cup\{e\}$ $(e\notin X)$
נרחיב את הפעולה:

$$\begin{cases} x_1\cdot x_2 & \forall x_1,x_2\in X \\ e\cdot x=x & \forall x\in X \\ e\cdot e=e \end{cases}$$

קל להראות שהפעולה הזו ב-Y היא אסוציאטיבית וש-e ניטרלי.
לכן קיבלנו ש $(Y,\cdot)$ מונואיד שמרחיב את $(X,\cdot)$.

הגדרה ==(הזזות)==: נניח $a\in X$.
נגדיר $l_a: X\to X \quad l_a(x)=a\cdot x$
$r_a: X\to X \quad r_a(x)=x\cdot a$

הזזות, transformations.

יש לזה משמעות גאומטרית ב- $(\mathbb{R}^2,+)$ -

Generated by CamScanner from intsig.com

<u>תכונות:</u>

במונואיד $(X,\cdot)$, $a\in X$.

1. $l_e = r_e = id_X$.
2. $l_a: X\to X$ על $\Leftrightarrow$ a הפיך מימין
3. $l_a: X\to X$ חח"ע $\Leftrightarrow$ ניתן לצמצם ב-a משמאל
4. אם $a\in \mathcal{O}_r(X)$ $l_a: X\to X$ חח"ע ועל.

<u>הסבר:</u>

1. ברור.
2. $(\Leftarrow)$: אם l_a על אזי קיים $x\in X$ כך ש-$l_a(x)=e$ כלומר $a\cdot x=e$ כלומר x הפיך מימין.

$(\Rightarrow)$: נניח שקיים $x\in X$ כך ש-$a\cdot x=e$. אם $y\in X$ ניקח $z:=x\cdot y\in X$.

כי $l_a(z)=l_a(x\cdot z)=a\cdot(x\cdot y)=(a\cdot x)\cdot y=e\cdot y=e$

3. דומה.
4. ③ ו-② $\Leftarrow$ ④.

<u>תרגיל:</u> נניח X מונואיד <u>סופי</u> כך שאפשר לצמצם <u>בכל</u> איבר משמאל. הוכח ש-X חבורה.

<u>הערה:</u> אם <u>X לא סופי</u> אז לא תמיד!

$X:=\mathbb{N}\cup\{0\}$ לגבי + . מונואיד "עם צמצום". <u>לא חבורה</u>.

$a+x=a+y \Rightarrow x=y$

<u>הערה:</u> כל אגודה <u>סופית</u> יש לפחות אידמפוטנט אחד.

(לא נכון לאינסופי , $X:=(\mathbb{N},+)$)

<u>כמה ע' בבוא מתורת המספרים הבסיסית</u> (שצריך לדעת):

① התחלקות ב-$\mathbb{Z}$

② חילוק עם שארית

③ <u>מס ראשוני:</u> $p\geq 2$ כך ש-p מתחלק ב-1 ו-p.

④ המשפט היסודי של האריתמטיקה (פירוק לראשוניים):

$\forall a\geq 2 \qquad a=p_1^{i_1}\cdot p_2^{i_2}\cdot\ldots\cdot p_m^{i_m}$

$p_1,p_2,\ldots,p_m$ גורמים ראשוניים של a, $i_1,\ldots,i_m$ הפירוק הוא יחיד עד כדי סדר

Generated by CamScanner from intsig.com

(5) משפט אוקלידס: יש אינסוף ראשוניים

הוכחה: אם נניח שיש רק מספר סופי $P = \{p_1, p_2, \dots, p_k\}$

נניח $a = p_1 p_2 p_3 \cdots p_k + 1$ אז (4) קיים פירוק לראשוניים עבור a. לכן קיים p_i האומר:

כלומר $p_i | a \Leftarrow p_i \in P$

נקבל $a = p_1 p_2 \cdots p_i \cdots p_k + 1$

$\begin{cases} 1 = a - p_1 p_2 \cdots p_i \cdots p_k \\ p_i | a \end{cases} \Rightarrow p_i | 1 \Rightarrow$ סתירה!

מש"ל

(6) $\gcd(a,b) = (a,b)$, $lcm = [a,b]$

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

(7) אלגוריתם אוקלידס - למציאת (a,b)

(8) $\begin{cases} t|a \\ t|b \end{cases} \Rightarrow t|(a,b) \wedge t|(c_1 a + c_2 b)$

הגדרה: a,b זרים $\overset{def}{\Longleftrightarrow} (a,b) = 1$

(9) משפט: לכל $a,b \in \mathbb{Z}$ קיימים $u,v \in \mathbb{Z}$ כך ש- $u \cdot a + v \cdot b = (a,b)$.

אלגוריתם אוקלידס מספק גם דרך למצוא u,v "והצגה ליניארית"

(10) משוואה לינארית $ax+by=c$, $x,y,a,b,c \in \mathbb{Z}$

פתירה בשלמים (x,y) $\Longleftrightarrow (a,b)|c$

הסבר: $(\Leftarrow)$: $\begin{cases} (a,b)|a \\ (a,b)|b \end{cases} \Rightarrow (a,b)|(ax+by) \Rightarrow (a,b)|c$.

$(\Rightarrow)$: נתון $(a,b)|c$, כלומר $c = (a,b)q$

לפי משפט (9): $(a,b) = u \cdot a + v \cdot b$, $\exists u,v \in \mathbb{Z}$

נכפול ב-q. נקבל $(a,b) \cdot q = a(uq) + b(vq)$ כלומר $a(uq) + b(vq) = c$

$(x,y) = (uq, vq)$ מקיים את המשוואה. מש"ל

(11) $(a,b) = 1 \Longleftrightarrow$ קיימים $u,v \in \mathbb{Z}$ כך ש- $ua+vb=1$.

הסבר: $(\Rightarrow)$: מקבלים ישר מ-9.

$(\Leftarrow)$: אם $\begin{cases} c|a \\ c|b \end{cases} \Rightarrow c|(ua+vb) \Rightarrow c|1 \Rightarrow c=1$ (כי c מחלק) $\Rightarrow (a,b) = 1$ מש"ל.

(5) **משפט אוקלידס:** יש אינסוף ראשוניים. $P = \{p_1, p_2, \dots, p_k\}$

הוכחה: אם נניח שיש רק מספר סופי

ניקח $a = p_1 \cdot p_2 \cdot p_3 \cdots p_k + 1$. לפי (4) קיים פירוק לראשוניים עבור a. לכן קיים p_i ראשוני

כך ש- $p_i | a \Leftarrow p_i \in P$

נקבל $a = p_1 \cdot p_2 \cdots p_i \cdots p_k + 1$

$$\begin{cases} 1 = a - p_1 \cdot p_2 \cdots p_i \cdots p_k \\ p_i | a \end{cases} \Leftarrow p_i | 1 \Leftarrow \text{סתירה}$$

מש"ל

(6) $\gcd(a,b) = (a,b)$, $\text{lcm} = [a,b]$

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

(7) אלגוריתם אוקלידס - למציאת (a,b)

(8) $\begin{cases} t|a \\ t|b \end{cases} \Leftarrow t|(a,b) \wedge t|(c_1 a + c_2 b)$

הגדרה: a,b זרים $\overset{def}{\Leftrightarrow} (a,b) = 1$

(9) **משפט:** אם $a,b \in \mathbb{Z}$ קיימים $u,v \in \mathbb{Z}$ כך ש- $u \cdot a + v \cdot b = (a,b)$

אלגוריתם אוקלידס מספק דרך למצוא u,v "והצגה לינארית"

(10) משוואה לינארית $ax + by = c$, $x,y,a,b,c \in \mathbb{Z}$

פתירה בשלמים $\Leftrightarrow (a,b)|c$?(x,y)

הסבר: $(\Leftarrow)$: $\begin{cases} (a,b)|a \\ (a,b)|b \end{cases} \Leftarrow (a,b)|(ax+by) \Leftarrow (a,b)|c$

$(\Rightarrow)$: נתון $(a,b)|c$, כלומר $c = (a,b) \cdot q$

לפי משפט (9): $(a,b) = u \cdot a + v \cdot b$, $\exists u,v \in \mathbb{Z}$

נכפיל ב- q. נקבל $(a,b) \cdot q = a(uq) + b(vq)$ כלומר $a(uq) + b(vq) = c$

$(x,y) = (uq, vq)$ מקיים את המשוואה. מש"ל

(11) $(a,b) = 1 \Leftrightarrow$ קיימים $u,v \in \mathbb{Z}$ כך ש- $ua + vb = 1$

הסבר: $(\Leftarrow)$: מקבלים ישר מ-(9).

$(\Rightarrow)$: אם $\begin{cases} c|a \\ c|b \end{cases} \Leftarrow c|(ua+vb) \Leftarrow c|1 \Leftarrow (c \in \mathbb{N})\ c = 1$

$\Leftarrow (a,b) = 1$. מש"ל

(12) $a \mid b \Leftarrow \begin{cases} a \mid bc \\ (a,c)=1 \end{cases}$

(13) $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right)=1$

משפט: נניח G חבורה, $a\in G$, $O(a)=n$.

$$O(a^k)=\frac{n}{(n,k)}$$

דוגמה: $G=\Omega_{120}$, $a:=w\in G$, $k=100$

$$O(w^{100})=\frac{O(w)}{(O(w),100)}=\frac{120}{(\underset{120}{O(w)},100)}=6.$$

תרגיל 10: $O(w^{250})$ $w\in\Omega_{1400}$

ב) $O([150]_{250})$ $a=[150]\in(\mathbb{Z}_{250},\oplus)$

ג) $cis\,9^\circ\in\mathbb{T}=\{z\in\mathbb{C} \mid |z|=1\}$

הוכחה של המשפט: צ"ל א) $(a^k)^{\frac{n}{(n,k)}}=e$

ב) מינימלי ← $\frac{n}{(n,k)}\le t \Leftarrow \begin{cases}(a^k)^t=e \\ t\in\mathbb{N}\end{cases}$

א) $(a^k)^{\frac{n}{(n,k)}}=(a^n)^{\frac{k}{(n,k)}}=e^{\frac{k}{(n,k)}}=e$. $\frac{k}{(n,k)}\in\mathbb{Z}$

ב) נניח $\begin{cases} a^{kt}=e \\ t\in\mathbb{N}\end{cases}$. מספיק להראות $\frac{n}{(n,k)} \mid t$.

לפי הגדרה של הלוק נקבל $a^{kt}=e \Leftarrow kt=nq$ $\exists q\in\mathbb{Z}$

(1) $\frac{k}{(n,k)}\cdot t=\frac{kt}{(n,k)}=\boxed{\frac{n}{(n,k)}}\cdot q$

(2) $\left(\frac{k}{(k,n)}, \frac{n}{(k,n)}\right)=1$ לפי הגדרה של הלוק, מלמה (12) משוואונים (2)

1) ו־(1) נקבל $\frac{n}{(n,k)} \mid t$. מש"ל.

Generated by CamScanner from intsig.com

Euler's function — פונקציית אוילר

שאלה: סימון: φ, $U_n := Gr(\mathbb{Z}_n, \odot) = ?$

$\varphi(n) := |Gr(\mathbb{Z}_n, \odot)| = ?$

מספר האיברים ההפיכים ב $(\mathbb{Z}_n, \odot)$

למשל: $\varphi(100) = ?$

משפט I Euler

$$U_n := \{[k] \in \mathbb{Z}_n \mid (k,n) = 1\}$$

הוכחה: $[a] \in U_n$.

קיים $[b] \in U_n$ כך ש $[a] \odot [b] = [1]$.

שקול: קיים b: $[ab] = 1$

שקול: קיים ...: $ab \equiv 1 \mod n$

שקול: קיים ...: $ab - 1 = nq$ $\quad \exists q \in \mathbb{Z}$

שקול: $ab + (-q) \cdot n = 1$

מכאן - לפי "קריטריון כלל" טענה (11), $(a,n) = 1$

את כל המעברים עשינו בצורה שקולה, לכן קיבלנו $(a,n)=1 \Leftrightarrow [a] \in U_n$ שקול

שאלה II חישוב יעיל של $\varphi(n) = |U_n|$.

מקרים: $n = p$ ראשוני: $U_p = \{[1], [2], \ldots, [p-1]\}$ לכן $\varphi(p) = p - 1$.

$n = p^2$ כאשר p ראשוני:

~~0~~ 1 2 3 . . ~~p~~ . . . ~~2p~~ . . . ~~3p~~ . . . . p^2-1

$$\varphi(p^2) = p^2 - p$$

$n = p^k$: $\varphi(p^k) = p^k - p^{k-1}$, p ראשוני

טענת עזר: $(a,b) = 1$, $a,b \in \mathbb{N}$ אז $\varphi(ab) = \varphi(a)\varphi(b)$

מקרה כללי: $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$

$$\varphi(n) = \varphi(\ldots) \underset{\text{טענת עזר}}{=} \varphi(p_1^{k_1})\varphi(p_2^{k_2})\cdots\varphi(p_m^{k_m}) = (p_1^{k_1} - p_1^{k_1-1}) \cdots$$

$$\cdots(p_m^{k_m} - p_m^{k_m-1}) = \frac{n}{n}(\ )\cdots(\ ) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right)$$

למשל: $\varphi(100) = 100 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$.

$100 = 2^2 \cdot 5^2$

שאלה: הוכח שמספר יוצרים ב Ω_n שווה ל $\varphi(n)$?

8.8.2011

הרצאה III

שאלה: כמה איברים מקיימים $\Omega_n = \langle b \rangle$ בחבורה Ω_n?

למשל: ב-Ω_4 האיברים הנ"ל הם w, w^3.

תשובה לשאלה: $\varphi(n)$ עוצמה $|x| = ord(x)$

הסבר: $w^k = b \in \Omega_n$ מתאים $\exists k$ $|a|$ סדר(a).

שימו לב: $\Omega_n = \langle b \rangle \iff o(b) = n$.

הערה: $o(b) = n \iff \langle b \rangle = \{e, b, \dots, b^{n-1}\} \iff |o(b)| = n$

(שונים – n איברים)

אחרת אין מינימליות של n. ($a^i = a^j$, $i > j$ $\Rightarrow$ $a^{i-j} = e$, $0 < i-j < n$)

$$\iff \begin{cases} o(b) = o(w^k) = \frac{o(w)}{(o(w),k)} \\ o(b) = n \end{cases} \iff \frac{n}{(n,k)} = n \iff \boxed{(n,k)=1}$$

מספר איברים כאלה $1 \le k \le n$ שווה בדיוק ל-$\varphi(n)$. משפט.

למשל: אם p ראשוני, ב-Ω_p יש p-1 כאלה.

שאלה: כיצד למצוא הופכי ב-$(\mathbb{Z}_n, \odot)$ עבור $[a] \in \mathbb{Z}_n$ (אם הוא קיים)?

כבר יודעים: מתי קיים!

לפי משפט Euler: $\iff (a,n) = 1$.

דוגמה: לפתור $1053x \equiv 6 \mod 100$

שקול לפתור $[1053]_{100} \cdot x = [6]_{100}$

שקול: $[53]_{100} \cdot x = [6]_{100}$ כי $1053 \equiv 53 \mod 100$

$[1053]_{100} = [53]_{100}$

לכן צריך למצוא $[53]^{-1}_{100} = ?$ קיים כי $(53, 100) = 1$.

$(100,53) = (53,47) = (47,6) = (6,5) = 1$

הצבה אחורית ← אלגוריתם אוקלידס

$17 \cdot 53 + (-9) \cdot 100 = 1$

$u \cdot 53 + v \cdot 100 = 1 \quad \exists u,v \in \mathbb{Z}$

מכאן $17 \cdot 53 \equiv 1 \mod 100 \Rightarrow [17]_{100}[53]_{100} = [1]_{100} \Rightarrow [53]^{-1} = [17]$

Generated by CamScanner from intsig.com

Generated by CamScanner from intsig.com

תת חבורות של $\mathbb{Z}$:

תכונות:

① $\mathbb{Z} = a\mathbb{Z} = \{\dots, -a, 0, a, 2a, \dots\}$

כאשר הרשימה של תת ח-$\mathbb{Z}$ נראית $a\in\mathbb{Z}$ (מסגה שלם).

② $a\mathbb{Z} \leq b\mathbb{Z} \Leftrightarrow b|a$

③ $a\mathbb{Z} + b\mathbb{Z} = (a,b)\mathbb{Z}$

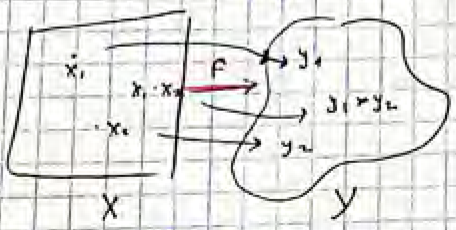
④ $a\mathbb{Z} \cap b\mathbb{Z} = [a,b]\mathbb{Z}$

הומומורפיזמים:

הגדרה: תהיינה $(X,\cdot)$, $(Y,*)$ חבורות.

פונקציה $f: X \to Y$ נקראת ==הומומורפיזם== אם f "שומרת" על הפעולה, כלומר

$$f(x_1 \cdot x_2) = f(x_1) * f(x_2) \quad \forall x_1, x_2 \in X$$



① אם f (גם) הומומורפיזם חח"ע, אז אומרים ==מונומורפיזם==.

② אם f הומומורפיזם על (כלומר $Im(f)=f(X)=Y$) אז אומרים ==אפימורפיזם==.

③ f נקרא ==איזומורפיזם== אם f מונו + אפי. (f הומו + חח"ע + על).

תכונות בסיסיות:

① לכל חבורה X, $id: X \to X$ איזומורפיזם (גם ==אוטומורפיזם==).

הגדרה: $X \xrightarrow{f} X$ איזומורפיזם של חבורה X על עצמה ==אוטומורפיזם==

② הרכבה של הומו (אפי, מונו, איזו)

גם ("____")

במילים אחר

$$X \xrightarrow{f_1} Y \xrightarrow{f_2} Z$$

$f_2 \circ f_1$

③ $X \xrightarrow{f} Y$ איזו $\Leftarrow$ $X \xleftarrow{f^{-1}} Y$ איזו

הגדרה: אומרים ש-Y, X איזומורפיות

אם קיים איזו $X \to Y$. ונסמן: $X \cong Y$

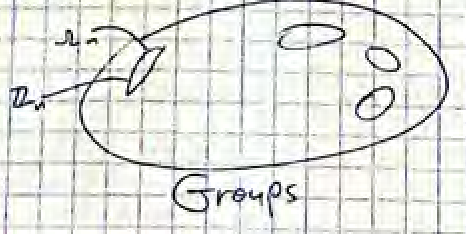
Generated by CamScanner from intsig.com

הערה: $X \simeq X$

$y \simeq x \iff x \simeq y$

$x \simeq z \Leftarrow x \simeq y \wedge y \simeq z$

קל לבדוק בעזרת התכונות הנ"ל



4) $\simeq$ יחס שקילות

לכן $\{Groups\}$ = איחוד של מחלקות שקילות... זרות קבוצות!!

5) לכל הומומורפיזם $X \xrightarrow{f} Y$ מתקיים $f(e_x)=e_y$.

הסבר: $f(e_x)^2 = f(e_x)f(e_x) = f(e_x \cdot e_x) = f(e_x)$

ז"א $f(e_x)$ אידמפוטנט ב-Y, לכן $f(e_x)=e_y$. ⇐ $b^2=b \Rightarrow b=e_Y$

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

הסבר: $f(x) * f(x^{-1}) = f(x \cdot x^{-1}) = f(e_x) = e_y$ //

$f(x^{-1}) * f(x) = \dots = e$

7) $f(x^k) = f(x)^k \quad \forall k \in \mathbb{Z}$

הסבר: אינדוקציה + תכונות 5+6.

8) $O(f(x)) \le O(x) \quad \forall x \in X$

הסבר: אם $O(x)=n$ אז $x^n = e_x \overset{5 \text{ מ'}}{\Rightarrow} f(x^n) = f(e_x)$

$f(x)^n = e_y$. משל.

9) אם f איזו' אז $\forall x \in X \; O(f(x)) = O(x)$.

הערה: בעצם מספיק f חח"ע (למה?)

הערה: כל תכונה אלגברית נשמרת ע"י איזומורפיזם (סדר, ציקליות, וכו'...)

10) $X \xrightarrow{f} Y$ הומו'.

א) $H \le X \Rightarrow f(H) \le Y$

ב) $\Downarrow$ $Im f = f(X) \le Y$

תמונה הפוכה:

ג) $G \le Y \Leftarrow f^{-1}(G) \le X =: \{x \in X \mid f(x) \in G\}$.

ג) $\Downarrow$ $\ker f \le X := f^{-1}(e_y) = \{x \in X \mid f(x) = e_y\}$.

Generated by CamScanner from intsig.com

הסבר: לבדוק

(11) לכל חבורה X : $\mathrm{Aut}(X) := \{ f: X \to X \ : \ f \text{ איזומורפיזם} \}$

$(\mathrm{Aut}(X), \circ) \leq (S_X, \circ)$ חבורה סימטרית (לבדוק צד תת חבורה)

שאלה: מה זה $\mathrm{Aut}(\mathbb{Z})$?

(12) איזומורפיזם שומר על תכונות קומוטטיביות, ציקליות.

נניח ש $X \xrightarrow{f} Y$ איזו׳
$= f(X)$

קומו׳:

$\forall y_1, y_2 \in Y$

$y_1 * y_2 = f(x_1) * f(x_2) = f(x_1 \cdot x_2)$

$y_2 * y_1 = f(x_2) * f(x_1) = f(x_2 \cdot x_1)$

תרגיל: הראו ש-Y ציקלי כאשר X ציקלי.

דוגמאות:

1) $G = \{I, J\}$

$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$J := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$

$\cdot$	I	J
I	I	J
J	J	I

$\simeq$

$\cdot$	1	-1
1	1	-1
-1	-1	1

Ω_2

$\Omega_2 \xrightarrow{f} G$

$1 \to I$

$-1 \to J$

איזו׳

2) $\mathbb{R}^* \simeq GL_1(\mathbb{R})$

3) $G = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \middle| \ n \in \mathbb{Z} \right\}$ לגבי כפל מטריצות $\simeq (\mathbb{Z}, +)$

$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \overset{f}{\mapsto} n$

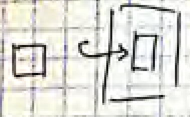
4) $(\mathbb{R}^+, \cdot) \simeq (\mathbb{R}, +)$, $\mathbb{R}^+ = (0, \infty)$ (חיובים)

$f(x) = 5^x$

$f(x_1 + x_2) = 5^{x_1 + x_2} = 5^{x_1} \cdot 5^{x_2} = f(x_1) \cdot f(x_2)$

Generated by CamScanner from intsig.com

5) $S_3 \to S_5$ קיים מונו.

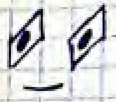


"שיכון" $\begin{pmatrix} 1 & 2 & 3 \\ i_1 & i_2 & i_3 \end{pmatrix} \xrightarrow{\varphi} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i_1 & i_2 & i_3 & 4 & 5 \end{pmatrix}$

φ הומו. חח"ע (לא על)

אומרים: "שיכון" של חבורה לתוך חבורה שניה.

סימולים: לכל מונו $f: X \to Y$, $f_*: X \to f(X)$ איזו.

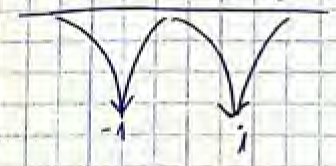


6) $(\mathbb{R}^*, \cdot) \xrightarrow{f} (\Omega_2, \cdot)$

$\Omega_2 = \{1, -1\}$

$f = sgn$

$$f(x) = \begin{cases} +1 & x>0 \\ -1 & x<0 \end{cases}$$



לא איזומורפיזם, כי על + שמור על הפעולות

בדיקה 4 מקרים (סימנים)

$$f(x_1 \cdot x_2) = f(x_1)\, f(x_2)$$

+ +
+ −
− +
− −

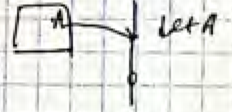
7) (מונואידים) $(Mat_{n\times n}(\mathbb{R}), \cdot) \to (\mathbb{R}, \cdot)$,

$f = det$

$f(A) = det(A)$

$f(A_1 \cdot A_2) = det(A_1 \cdot A_2) = det(A_1)\, det(A_2)$

f הומומורפיזם של מונואידים, בצמצום לקבל הומומורפיזם של חבורות.



$GL_n(\mathbb{R}) \xrightarrow{det} \mathbb{R}^*$

8) אפי $(\mathbb{Z}, +) \xrightarrow{f} (\mathbb{Z}_n, \oplus)$

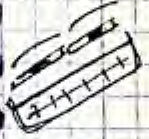
על ברור $a \xrightarrow{f} [a]_n$

$f(a+b) = [a+b]_n$

הגדרה ← $[a+b]_n = [a] \oplus [b]$

$f(a) + f(b) = [a] \oplus [b]$

Generated by CamScanner from intsig.com



משפט - מיון חבורות ציקליות:

נניח G חבורה ציקלית עם יוצר a, כלומר $\langle a \rangle = G$.

① קיים אפי $f: \mathbb{Z} \to G$

② אם G אינסופית (שקול $O(a)=\infty$) st $\mathbb{Z} \cong G$.

③ אם $O(a) \neq \infty$ אזי $\mathbb{Z}_n \cong G$.

הוכחה: ① (על)

$$\mathbb{Z} \xrightarrow{f} G$$
$$k \mapsto a^k \quad \forall k \in \mathbb{Z}$$

$$\langle a \rangle = \{a^k\}_{k\in\mathbb{Z}} \overset{\text{נתון}}{=} G \Rightarrow \text{f על}$$

f הומו:

$$f(k_1+k_2) = a^{k_1+k_2}$$
$$f(k_1)\cdot f(k_2) = a^{k_1}\cdot a^{k_2}$$

הוכחה ②:

אחרי ① מספיק ש- $\mathbb{Z}\xrightarrow{f} G$ חח"ע.

אם נניח שלא: $k_1 > k_2$, $f(k_1)=f(k_2)$

$$a^{k_1} = a^{k_2}$$
$$a^{k_1-k_2} = e \qquad \exists k_1-k_2 \in \mathbb{N}$$

בסתירה ל $O(a)=\infty$. מש"ל.

③ אם $O(a)=n<\infty$ אזי כפי שהסברנו קודם $G=\{e,a,a^2,\ldots,a^{n-1}\}$

שונים. $\boxed{i \equiv j \bmod n \iff a^i = a^j}$

הסבר:

$$a^i = a^j \iff a^{i-j}=e$$
$$\Updownarrow \quad \boxed{\text{לגרנג'}}$$
$$i \equiv j \bmod n \iff n \mid i-j$$

$$G = \{e, a, a^2, \ldots, a^{n-1}\}$$
$$\mathbb{Z}_n = \{[0],[1],[2],\ldots,[n-1]\}$$

$\boxed{\text{חח"ע + על}}$

$$f([k]) = a^k$$

הומו' $\begin{cases} f([k_1]\oplus[k_2]) = f([k_1+k_2]) = a^{k_1+k_2} \\ f([k_1])\cdot f([k_2]) = a^{k_1}\cdot a^{k_2} = a^{k_1+k_2} \end{cases}$

f מוגדרת היטב כאן כי (*) $[i]=[j] \iff a^i = a^j$. מש"ל.

Generated by CamScanner from intsig.com

תוצאה

אם G חבורה ציקלית אינסופית ($G = \langle a \rangle$) אז כל תתי החבורות של G הן $\langle a^m \rangle$ (m טבעי).

הסבר:

$$\mathbb{Z} \simeq G$$

$$m\mathbb{Z} \leq \mathbb{Z}, \quad \langle a^m \rangle = \{a^{mk}\}_{k \in \mathbb{Z}} \leq G$$

קוסטים / משפט Lagrange

הגדרה: נניח $H \leq G$

א) קוסט (מחלקה) של H ב-G לגבי איבר $a \in G$:

$$a \cdot H := \{a \cdot h : h \in H\} \quad \text{(שמאלי)}$$

$$H \cdot a := \{h \cdot a : h \in H\} \quad \text{(ימני)}$$

ב) קבוצת המנה של H ב-G היא:

$$G/H := \{aH : a \in G\}$$

למשל:

$G = \mathbb{Z}, \quad H = 3\mathbb{Z}$

$$\mathbb{Z}/3\mathbb{Z} = \{a + 3\mathbb{Z} \mid a \in \mathbb{Z}\} = \{[0]_3, [1]_3, [2]_3\}$$

ג) האינדקס של H ב-G מוגדר כעוצמה של קבוצת המנה G/H.

סימון: $[G:H] := |G/H|$ **למשל:** $[\mathbb{Z} : 3\mathbb{Z}] = 3$.

משפט Lagrange:

נניח $H \leq G$ אזי:

(1) $G = \bigcup_{g \in G} gH$ ($g_1H = g_2H$ או $g_1H \cap g_2H = \emptyset$)

(2) $g_1H = g_2H \iff g_1^{-1} \cdot g_2 \in H$

(3) $|G| = |H| \cdot [G:H]$

תוצאות:

(1) לכל G סופית, $H \leq G$ מתקיים $|H| \mid |G|$ $\overset{3}{\Rightarrow}$ (לכל H תת חבורה מתקיים) $|H| \mid |G|$; לכל $x \in G$, $x^{o(G)} = e$

$\overset{3}{\Rightarrow} [G:H] \mid |G|$

(2) לכל G סופית ולכל $x \in G$ מתקיים $|o(x)| \mid |G|$

הסבר: $n = |o(x)| = |H|$, $H \leq G$, $H = \langle x \rangle = \{e, x, x^2, \dots, x^{n-1}\}$. במילים, הסדר של איבר x שווה לסדר של תת החבורה $\langle x \rangle$. | לכן לכל $x \in G$ (הסבר) G סופית $\Leftarrow$ $o(x) \mid G$, $|G| = m$, $o(x) = n$ $\Leftarrow$ $m = nq$, $x^{|G|} = x^{nq} = (x^n)^q = e$

[illegible]

(3) אם $|G|=p$ ראשוני אז $G \simeq \mathbb{Z}_p$

הסבר:

נתון $|G|=p\in\mathbb{Z}$. קיים $e\neq a\in G$ כך ש- $|O(a)| \mid |G|=p$, $1\neq |O(a)|$, לכן $\langle a\rangle = G$,
(כי $O(a)=|G|=p$) ולכן G ציקלית עם p איברים.

לפי משפט מיון, $G\simeq \mathbb{Z}_p$. מש"ל.

הגדרה: תת חבורה $H\le G$ נקראת **נורמלית** ב-G אם $aH=Ha$ $\forall a\in G$

סימון: $H \trianglelefteq G$

דוגמה של תת חבורה לא נורמלית: $G=S_3=\langle a,\sigma\rangle$ יש $3!=6$ איברים.

$a=(1\,2\,3)$, $\sigma=(1\,2)$

$H:=\{e,\sigma\}\le S_3$.

תת חבורה, אבל לא נורמלית.

$\{a, a\sigma\} = aH \neq Ha = \{a,\sigma a\}$

תכונות:

(1) אם G אבלית אז כל תת חבורה היא נורמלית. $ah=ha \Rightarrow aH=Ha$ $\forall h\in H$, $\forall a\in G$

(2) לכל חבורה G מתקיים $G\trianglelefteq G$, $\{e\}\trianglelefteq G$

המרכז: $C(G)=Z(G):=\{g\in G : \forall x\in G,\ xg=gx\}$
(כל האיברים הקומו')
$C(G)\trianglelefteq G$

הסבר ל- $G\trianglelefteq G$: צריך: $Ga=aG$ $\forall a\in G$

שימו לב: $aG=G$, $Ga=G$ תמיד.

$aG=l_a(G)=G$, כי a הפיך.

משפט Euler II (או הכללה):

לכל $(a,n)=1$ מתקיים $a^{\varphi(n)}\equiv 1 \mod n$

הוכחה: חבורת אוילר $[a]_n\in(U_n,\cdot) =: G$ $\overset{\text{I Euler Gen}}{\Longleftrightarrow}$ $(a,n)=1$

לפי לגרנז' נקבל $[a]_n^{|U_n|}=[1]_n$

ידוע: $|U_n|=\varphi(n)$, ולכן נקבל $a^{\varphi(n)}\equiv 1 \mod n$

מש"ל

משפט פרמה: (הקטן)

יהי p ראשוני. לכל $a \in \mathbb{Z}$ מתקיים $a^p \equiv a \mod p$

הוכחה:

שני מקרים:

(1) אם $(a,p)=1$ אז $a^{p-1} = a^{\varphi(p)} \equiv 1 \mod p$ $\Leftarrow$ $a^p \equiv a \mod p$

(2) $a \equiv 0 \mod p$. (קל) $0^p \equiv 0 \mod p$, $0=0$.

מש"ל

תרגיל:

לחשב שתי ספרות אחרונות:

א. 39078653^{202}

ב. 39078659^{559}

רמזים:

א. $\varphi(100) = 40$

ב. $[53]_{100}^{-1} = 17$

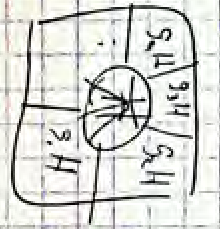
יום ד' 10/08/2011

הרצאה IV

משפט Lagrange

נניח $H \leq G$ אז:

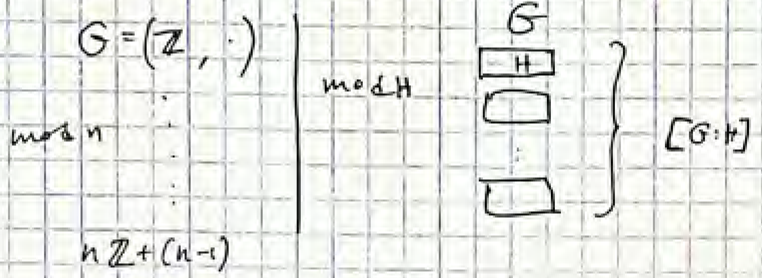
(1) $G = \dot{\bigcup}_{g \in G} gH$ איחוד זר ($g_1H \cap g_2H = \emptyset$ או $g_1H = g_2H$)



(2) $g_1H = g_2H \iff g_1^{-1}g_2 \in H$

(3) $|G| = |H| \cdot [G:H]$

הוכחה: הרעיון:



נגדיר יחס "שקילות" H ב-G ע"י $g_1 \equiv g_2 \bmod H$ **def** $g_1^{-1}g_2 \in H$

נבדוק שזה יחס שקילות בקבוצה G:

(א) רפלקסיביות: $g \equiv g \bmod H$. הסבר: $g^{-1}g = e \in H$

(ב) סימטריות: $g_1 \equiv g_2 \bmod H \Leftarrow (g_1^{-1}g_2)^{-1} \in H$

הסבר: $g_1^{-1}g_2 \in H \underset{H \leq G}{\Rightarrow} (g_1^{-1}g_2)^{-1} \in H$

$$(g_1^{-1}g_2)^{-1} = g_2^{-1}g_1 \in H \Rightarrow g_2 \equiv g_1 \bmod H$$

(ג) טרנזיטיביות:

$$\begin{cases} g_1 \equiv g_2 \\ g_2 \equiv g_3 \end{cases} \Rightarrow g_1 \equiv g_3$$

$$\begin{cases} g_1^{-1}g_2 \in H \\ g_2^{-1}g_3 \in H \end{cases} \underset{H \leq G}{\Rightarrow} (g_1^{-1}g_2)\cdot(g_2^{-1}g_3) \in H$$

$$(g_1^{-1}g_2)\cdot(g_2^{-1}g_3) = g_1^{-1}g_3 \in H \Rightarrow g_1 \equiv g_3$$

הוכחנו ש- $\equiv_H$ יחס שקילות (משפט בסיסי של יחס שקילות)

$$\Downarrow$$

$$G = \dot{\bigcup}_{g \in G} [g]$$

$[g] := \{x \in G \mid g \equiv x \bmod H\}$ מחלקה של G

$$[g] = \{x \in G \mid g \equiv x \bmod H\} = \{x \in G \mid g^{-1}x \in H\} = \{x \in G \mid x \in gH\} = gH$$

קיבלנו $[g] = gH$ קוסט של g ← מחלקה של g. לכן הוכחנו (1). $G = \dot{\bigcup}_{g \in G} gH$

Generated by CamScanner from intsig.com

(2) המשך מההוכחה. $g_1H=g_2H \iff [g_1]=[g_2] \iff g_1 \equiv_H g_2 \iff g_1^{-1}\cdot g_2 \in H$

נוכיח $|g_1H|=|g_2H|=|H|$ $\forall g_1,g_2\in G$.

מספיק: $|gH|=|H|$ $\forall g\in G$

$$\boxed{gH = l_g(H)}$$

כאשר $G \xrightarrow{l_g} G$

$x \mapsto gx$

l_g חח"ע כי g הפיך (ואז תמונת l_g ... או שוויון.)

$x_1 \neq x_2 \Rightarrow g\cdot x_1 \neq g\cdot x_2$

נובע מהפיכות g (ניתן לצמצם כי איבר בחבורה)

מה העובדה שהתקבלו: $|G|=|H|\cdot[G:H]$

הערה: משפט לגרנג' גם "בצד ימני", כי מגדירים (משמאל) $g_1 \equiv g_2$ $\overset{def}{\iff}$ $g_1\cdot g_2^{-1}\in H$

ש-$[G:H]$ שווה בשני המקרים הנ"ל

הסבר ישיר: (בלי לגרנג'):

$$\{gH\}_{g\in G} \xrightarrow{\varphi} \{Hg\}_{g\in G}$$

$\forall g\in G$ $\quad gH \to Hg^{-1}$

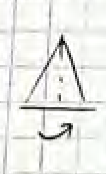
φ חח"ע ועל.

תרגיל: למצוא את כל הקוסטים השמאליים והימניים במקרים הבאים:

(1) $G=S_3 \geq H=\{e,(1,2)\}$

$[G:H]=3$

(2) $G=D_3 \geq H=\{e,\sigma\}$



σ שיקוף

a סיבוב

המשך השאלה על תת חבורה ציקלית:

תזכורת: תת חבורה של ציקלית גם ציקלית (משפט).

מצאנו שתת חבורה ציקלית אינסופית $G=\langle a\rangle$, $O(a)=\infty$

$\{H=\langle a^m\rangle\} = Sub(G)$ ($m\geq 0$ שלם, Subgroups)

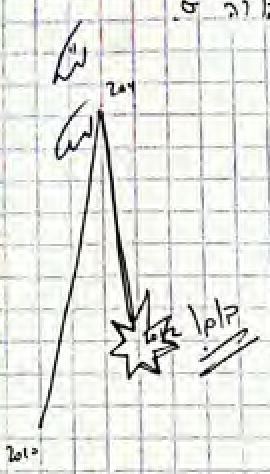
מקרה של חבורה ציקלית סופית G, כך ש- $\langle a\rangle = G$

$O(a)=n<\infty$

משפט: נניח $O(a)=n<\infty$, $\langle a\rangle=G$

קיום: (1) לכל $m|n$ קיימת תת חבורה H כך ש- $|H|=m$.

יחידות: (2) לכל $m|n$ יש בדיוק תת חבורה **אחת** H, $|H|=m$.



הערה: שימו לב לפי משפט לגרנז' סדר של תת חבורה H בהכרח מחלק סדר של חבורה G.

הוכחה: נזכיר בחשבון בהמשך שכל תת חבורה H של G היא ציקלית.

(1) נניח $m|n$. $H=\langle a^{\frac{n}{m}}\rangle$ (קיום)

מספיק להוכיח: $|H|=m$. שקול להוכיח: $O(a^{\frac{n}{m}})=m$

בדיקה:

$$O\left(a^{\frac{n}{m}}\right)=\frac{O(a)}{\left(O(a),\frac{n}{m}\right)}=\frac{n}{\left(n,\frac{n}{m}\right)}=\frac{n}{\frac{n}{m}}=m$$

(2) **יחידות:** נניח תת חבורה $K\leq G$ ו- $|K|=m$

צריך: $H=K$. שקול להוכיח: $H\subseteq K$. שקול להוכיח: $a^{\frac{n}{m}}\in K$

לפי המשפט על תתי חבורות ציקליות $\in$ K אז ציקלית לכן $\langle a^s\rangle=K$, $\exists s\in\mathbb{N}$

$$\underset{m}{\overset{\parallel}{|K|}}=O(a^s)=\frac{n}{(n,s)}$$

מכאן $(n,s)=\frac{n}{m}$.

$$a^{\frac{n}{m}}=a^{(n,s)}=a^{u\cdot n+v\cdot s}=(a^n)^u\cdot(a^s)^v=e(a^s)^v\in K$$

$(n,s)=u\cdot n+v\cdot s$ איקלידס, $\exists u,v\in\mathbb{Z}$; כי $a^s\in K$

לכן $a^{\frac{n}{m}}\in K$. מש"ל

תרגיל: למצוא את כל תת חבורות של G

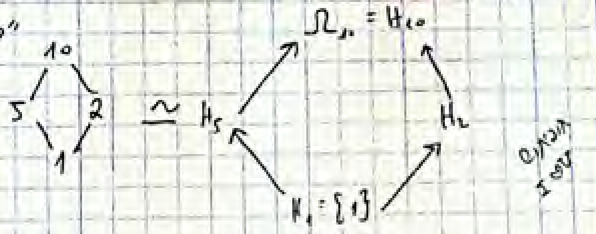
(ג) Ω_{10}

(ד) $\mathbb{Z}_{15}$

לבד

הערה: "סריג של תת..."

"סריג המחלקים"



משפט Wilson: (VIII Bhasmara הודו)

עבור $n \geq 2$ טבעי מתקיים

n ראשוני $\iff n \mid (n-1)! + 1$

הוכחה: $(\Leftarrow)$: נניח p ראשוני $p \geq 3$. $p \mid (p-1)! + 1$

כרעיון להוכחה ניקח מקרה $p=7$.

$7 \mid 1\cdot2\cdot3\cdot4\cdot5\cdot6 + 1$

שקול להוכיח $0 \equiv (1\cdot2\cdot3\cdot4\cdot5\cdot6) + 1 \mod p$

$p-1 \equiv 1\cdot2\cdot3\cdot4\cdot5\cdot6 \mod p$

$6 \equiv ① 2\cdot3\cdot4\cdot5\cdot⑥ \mod 7$

אם
אם רק
ורק אם נוכיח
נהיה פה עם אחד.
חוץ מ-1 ו-$p-1$
הגענו לאחד
שכל...

באופן כללי: **צ"ל:** $p \mid (p-1)! + 1$

שקול להוכיח $(p-1)! \equiv p-1 \mod p$

שקול להוכיח: $① \cdot 2 \cdot 3 \cdot 4 \cdots (p-2) \cdot (p-1) \equiv (p-1) \mod p$

נזכיר כי איבר עם ההופכי שלו. ידוע ש- $(\mathbb{Z}_p, \oplus, \odot)$ שדה

לכל $[a]_p \neq [0]_p$ יש הופכי

חשוב שלכל איבר ששונה מ-$[1]$ או $[p-1]$ ההופכי שונה ממנו מתקיים:

$[a^{-1}] = [a]^{-1} \iff a = [1] \vee [a] = [p-1]$

$\forall [a] \in \mathbb{Z}_p^{*} = \{[1], \ldots, [p-1]\} = V_p$
חבורה לכפל

$[x]^{-1} = [x]$

$[x]^2 = [1] = [1]^2$

$([x] - [1]) \cdot ([x] + [1]) = [0]$

$[x] = [1]$ או $[x] = -[1] = [-1] = [p-1]$

Generated by CamScanner from intsig.com

$1 \cdot 2 \cdots (p-2)(p-1) \equiv 1 \cdot 1 \cdot (p-1) = (p-1) \mod p$ מין מבחן

הוכחת משפט: נתון $\exists u \in \mathbb{Z}:\ u \cdot n = (n-1)! + 1 \Leftarrow n \mid (n-1)! + 1$ לצמצם/בצ?

$u \cdot n - (n-1)! = 1$ $u_k \cdot n + v_k \cdot k = 1$ $1 \le k < n$ ונקבל שלכל $\forall k \in \mathbb{N}, k < n$ $v_k = \frac{-(n-1)!}{k}$ (סמן

$v_k = \forall k \in \mathbb{N}: k < n$ $(n,k) = 1$ לינקלי משפט ... מתקיים:

חבורת מנה:

משפט: נניח $H \trianglelefteq G$ (H תת חבורה נורמלית ב-G) אז:

(1) $(G/H, *)$ חבורה לגבי כפל קוסטים $\boxed{aH * bH := (ab)H}$

(2) אזי $\varphi: G \to G/H$, $g \mapsto gH$ — הומומורפיזם

(3) $\ker\varphi = H$

הוכחה: נוכיח קודם ש $(aH)(bH) = (ab)H$ (כפל ב-G, לא כמו $*$)

$\{(ab)h \mid h \in H\}$ $\{(ah_1)\cdot(bh_2) \mid h_1, h_2 \in H\}$ (חבורות לא תמיד זה נכון $H = \{e, (1,2)\} \le S_4$)

$$(aH)(bH) = (aH)\cdot(Hb) = a(H \cdot H)\cdot b = a(Hb) = a(bH) = (ab)H$$

(נורמלי $bH = Hb$; סגירות; $H \trianglelefteq G$; נורמלי)

מהשוויון $(aH)\cdot(bH) = (ab)H$ נוכיח שהפעולה מוגדרת היטב:

$a'H = aH$, $b'H = bH$ $\Leftarrow$ $a'H \cdot b'H = aH \cdot bH = (ab)H$

$a'H * b'H = \ldots = aH * bH$

לכן $(G/H, *)$ מבנה אלגברי.

המבנה בעצם חבורה: אסוציאטיביות — נובעת מ-אסוציאטיביות של $(G, \cdot)$.

ניטרלי: $[e] = H \in G/H$ הוא ניטרלי ב-$(G/H, *)$, $[e] = H$.

הופכי ל-$[a] = aH \in G/H$: $[a]^{-1} = [a^{-1}] = a^{-1}H \in G/H$

(ב) φ על: ברור כי לכל $gH \in G/H$, $\varphi(g) = gH = [g]$

φ הומומורפיזם: $\forall a, b \in G$

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

$\varphi(a) * \varphi(b) = aH * bH$ (def)

(3)

$\ker\varphi = \{x\in G \mid \varphi(x)=[e]=H\} = \{x\in G \mid xH=H\} = \{x\in G \mid x\in H\} = H$

מש"ל

דוגמא:

$G=(\mathbb{Z},+)$

$H=n\mathbb{Z} \trianglelefteq G$

$(G/H,\times) = (\mathbb{Z}/n\mathbb{Z},\times) = (\mathbb{Z}_n,\oplus)$

הגדרה: $H\le G$.

התנאים הבאים שקולים:

(א) $\forall g\in G:\ gH=Hg$ (הגדרה)

(ב) $\forall g\in G:\ gHg^{-1}=H$ (הצמדה ע"י g משאירה H במקום.)

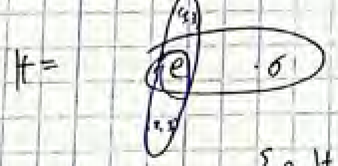
⇓

(ג) $\forall g\in G\quad gHg^{-1}\subseteq H$

⇑ שינוי משתנה g^{-1} במקום g.

(ד) $\forall g\in G,\ h\in H \quad ghg^{-1}\in H$

דוגמא: $H=\{e,(1\,2)\}\le G=S_3$, $H \ntrianglelefteq G$



מסלול הצמדה של H: $\{gHg^{-1} \mid g\in G\}=\{H_1,H_2,H_3\}$

$geg^{-1}=e$

3 מ"ח $H\ntrianglelefteq G$

הגדרה: הצמדה ע"י g בחבורה G היא

$\alpha_g: G\to G$

$\alpha_g(x)=gxg^{-1}$. $x\in G$ משתנה. "g קבוע"

תכונות:

(1) α_g אוטומורפיזם (נקרא "אוטומורפיזם פנימי")

הסבר:

הומ:

$\alpha_g(x_1 x_2) = g(x_1 x_2)g^{-1}$

$\alpha_g(x_1)\cdot\alpha_g(x_2) = (gx_1g^{-1})\cdot(gx_2g^{-1})$

על: יהי $y\in G$ ניקח $x=g^{-1}yg\in G$ אז $\alpha_g(x)=y$

חח"ע: $x_1\neq x_2$ צ"ל: $g(x_1)\neq g(x_2)$.

אם נניח $\alpha_g(x_1)=\alpha_g(x_2)$

$gx_1g^{-1} = gx_2g^{-1}$

$\Downarrow$

$x_1=x_2$. מש"ל.

Generated by CamScanner from intsig.com

אוטומורפיזמים פנימיים $\quad Inn(G) = \{\alpha_g\}_{g \in G}$ (2)

$$Inn(G) \le Aut(G) \le S_G$$

לפי כלל ההרכבה

$$\alpha_{g_1} \circ \alpha_{g_2} = \alpha_{g_1 g_2}$$

(3)

$$g \in Z(G) \iff \alpha_g = id$$

$$Z(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$$

(4) בחבורה אבלית $\alpha_g = id_G$.

דוגמה: אוטומורפיזמים לא פנימיים:

אז (G) שדה

(1) $(\mathbb{C}, +)$

$z \mapsto \bar{z}$

$a+bi \mapsto a-bi$

$f \neq id_{\mathbb{C}}$.

(2) $G = S_3 \times S_3$

$G \xrightarrow{f} G$

$(x,y) \to (y,x)$

אוטומ' (לבדוק) $\neq id_G$. לכן לא פנימי

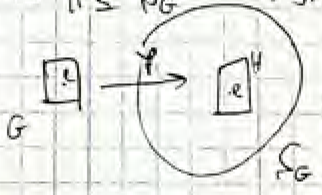
משפט Cayley (קיילי)

כל חבורה G איזומורפית לתת חבורה של S_G.

⇓

תוצאה: כל חבורה סופית G עם $n = |G|$ איברים "משוכנת" לתוך S_n.

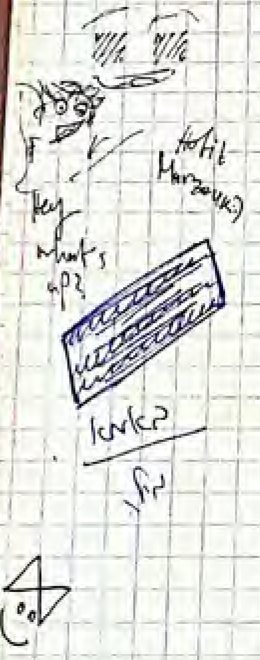
הסבר התוצאה: מהמשפט יש לנו שקיימת תת $H \le S_G$, $G \cong H$



נשים לב שבאופן שקול:

$$S_G = \{G \xrightarrow{f} G \ \text{חח"ע ועל}\} = \left\{\begin{pmatrix} g_1 = e, & g_2, & \dots, & g_n \\ g_{i_1}, & g_{i_2}, & \dots, & g_{i_n} \end{pmatrix}\right\} \quad \text{קיים מיפוי } G \to S_G:$$

$$S_n = \left\{\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}\right\}$$



קל לבדוק שיש איזומורפיזם טבעי $S_G \xrightarrow{\gamma} S_n$

לין

$$G \xrightarrow{\varphi \text{ שיכון}} S_G \xrightarrow{\gamma} S_n$$

$\gamma \circ \varphi$ (מונומורפיזם · שיכון)

<u>דימוי</u> הטבלה של חבורה

$$G = \{g_1 = e, g_2, \dots, g_n\}$$

	g_1	g_2	…	g_n
g_1				
⋮				
g	gg_1	…	…	gg_n
⋮				
g_n				

<u>הוכחה של משפט קיילי:</u>

צ"ל שקיים מונו'

$$(G, \cdot) \xrightarrow{\varphi} (S_G, \circ)$$

נגדיר $\varphi: G \to S_G$,$\varphi(a) = l_a$ ונוכיח שזה מונומורפיזם.

<u>קודם כל φ מוגדרת היטב:</u> $l_a \in S_G$,$\forall a \in G$,הוכחנו!!

l_a <u>חח"ע</u>: $x_1 \neq x_2 \Rightarrow ax_1 \neq ax_2$

l_a <u>על</u>: לכל $y \in G$ ניקח $x := a^{-1}y$ אז $l_a(x) = y$

⇓

$l_a \in S_G$.

<u>l_a הומו':</u>

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

$$\varphi(a \cdot b) = l_{ab}$$

$$\varphi(a) \circ \varphi(b) = l_a \cdot l_b$$

<u>φ חח"ע</u>: נניח $a \neq b$ ⇐ $l_a \neq l_b$ (כאשר $l_a = \varphi(a)$, $l_b = \varphi(b)$)

$$l_a \neq l_b \Leftarrow \begin{cases} x = e & l_a(e) = a \cdot e = a \\ & l_b(e) = b \cdot e = b \end{cases}$$

($a \neq b$)

Generated by CamScanner from intsig.com

הערה:

חבורה $\{$אוטומורפיזמים לינאריים של חבורה $\mathbb{R}^n\}$ חבורה מטריצות, איזומורפית

$\{$מטריצות אורתוגונליות $n\times n\} = O_n(\mathbb{R}) \leq GL_n(\mathbb{R})$

כל חבורה סופית G עם n איברים היא משוכנת לתוך $O_n(\mathbb{R})$.

רעיון ההסבר: לפי משפט קיילי, $G \overset{\varphi}{\hookrightarrow} S_n$

וכן משכן להלן: $S_n \hookrightarrow O_n(\mathbb{R})$

$e_1, e_2, \dots, e_n$ הבסיס הסטנדרטי של $\mathbb{R}^n$.

$$S_n \ni \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \overset{\text{בסיס סטנדרטי של } \mathbb{R}^n}{\longleftrightarrow} \begin{pmatrix} e_1 & e_2 & \cdots & e_n \\ e_{i_1} & e_{i_2} & \cdots & e_{i_n} \end{pmatrix}$$

$$\begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad (1,2) \mapsto \begin{pmatrix} e_1 & e_2 & e_3 \\ e_2 & e_1 & e_3 \end{pmatrix} \longleftrightarrow \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in O_n(\mathbb{R})$$

כו'.

מסקנה: כל חבורה סופית ניתנת לשיכון בחבורה אורתוגונלית.

חבורות של סימטריות:

יהי $A \subseteq \mathbb{R}^n$.

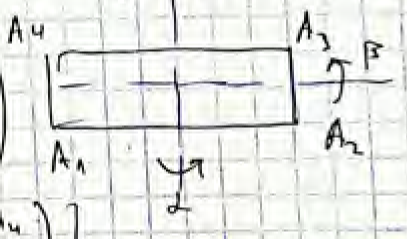
$$Sym(A) := \left\{ \mathbb{R}^n \xrightarrow{f} \mathbb{R}^n \;\middle|\; \begin{array}{l} \text{(1) חח"ע ועל} \\ \text{(2) } f \text{ שומרת מרחקים} \\ \text{(3) } f(A)=A \end{array} \right\}$$

(2) זה אומר: $\forall u,v \in \mathbb{R}^n \quad \|f(u)-f(v)\| = \|u-v\|$

דוגמאות:

(1) $A \subseteq \mathbb{R}^2$ = מצולע משוכלל. $Sym(A) = D_n$

(2) $A =$ ▭ מלבן ב-$\mathbb{R}^2$ שאינו ריבוע. $Sym(A) = K_4 \cong V_4$ "חבורת Klein"



$$K_4 = \left\{ e = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_1 & A_2 & A_3 & A_4 \end{pmatrix}, \alpha = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_2 & A_1 & A_4 & A_3 \end{pmatrix}, \beta = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_4 & A_3 & A_2 & A_1 \end{pmatrix}, \gamma = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_3 & A_4 & A_1 & A_2 \end{pmatrix} \right\}$$

[illegible]

[illegible]

[illegible]

[illegible]

Generated by CamScanner from intsig.com

[illegible]

Generated by CamScanner from intsig.com

Generated by CamScanner from intsig.com

(ד) בחור מהמלנחה $g_1H = g_2H \iff [g_1] = [g_2] \iff g_1 \equiv_H g_2 \iff g_1^{-1} \cdot g_2 \in H$

נזכור $|g_1H| = |g_2H| = |H|$ $\forall g_1, g_2 \in G$

מיל: $|gH| = |H|$ $\forall g \in G$

$gH = \ell_g(H)$

כלשי: $G \xrightarrow{\ell_g} G$

$x \longmapsto gx$

ℓ_g חח"ע כי g הפיך (יאו תכונות ℓ_g ... או שי.)

$x_1 \neq x_2 \Rightarrow gx_1 \neq gx_2$

נובע מהפיכות g (ניתן לצמצם בכל איבר בחבורה)

מה העובדות שהתקבלו: $|G| = |H| \cdot [G:H]$

הערה: משפט לגרנז' גם "קוסטים ימניים", אז $g_2 = g_1 h$ (משמאל) $\overset{def}{\iff} g_1^{-1} g_2 \in H$

ש

$[G:H]$ שווה בשני המקרים הנ"ל

הסבר שיר: (בלי לגרנז'): $\{gH\}_{g \in G} \xrightarrow{\varphi} \{Hg\}_{g \in G}$

$\forall g \in G$ $gH \rightarrow Hg^{-1}$

φ חח"ע ועל.

תרגיל: למצוא את כל הקוסטים השמאליים והימניים במקרים הבאים:

① $G = S_3 \geq H = \{e, (1,2)\}$

$[G:H] = 3$

② $G = D_3 \geq H = \{e, \sigma\}$ σ שיקוף, a סיבוב

<u>המשך השאלה על תת חבורה ציקלית:</u>

<u>תזכורת:</u> תת של ציקלית גם ציקלית (משפט).

מצאנו שתת חבורה ציקלית <u>אינסופית</u>, $G = \langle a \rangle$, $o(a) = \infty$

$Sub(G) = \{H = \langle a^m \rangle\}$ — Subgroups; $m \geq 0$ שלם.

Artin

Herstein

מקרה של חבורה ציקלית סופית G ויהי e , $\langle a\rangle = G$

$O(a) = n < \infty$

משפט: נניח ש $O(a)=n<\infty$, $\langle a\rangle=G$

קיום: (1) אם $m|n$ אז קיימת תת חבורה H של G ו- $|H|=m$.

יחידות: (2) לכל $m|n$ קיימת רק תת חבורה אחת H עם $|H|=m$

הערה: שימו לב לפי המשפט לגרנז' סדר של תת חבורה H מחלק סדר של חבורה G.

הוכחה: נזכר בהמשך כי כל תת חבורה H של G היא ציקלית.

(1) נניח $m|n$. $H=\langle a^{\frac{n}{m}}\rangle$ (קיום)

מספיק להוכיח: $|H|=m$. שקול להוכיח: $O(a^{\frac{n}{m}})=m$

בדיקה:

$$O\left(a^{\frac{n}{m}}\right)=\frac{O(a)}{\left(O(a),\frac{n}{m}\right)}=\frac{n}{\left(n,\frac{n}{m}\right)}=\frac{n}{\frac{n}{m}}=m$$

(2) **יחידות:** נניח שיש $K\le G$ ו $|K|=m$.

נוכיח: $H=K$. שקול להוכיח: $H\subseteq K$. שקול להוכיח: $a^{\frac{n}{m}}\in K$

לפי המשפט של תתי ציקליות $\in$ K אם ציקלית לכן $\langle a^s\rangle=K$, $\exists s\in\mathbb{N}$

$$|K| = O(a^s) = \frac{n}{(n,s)}$$

$|K| = m$.

מכאן $(n,s)=\frac{n}{m}$.

$$a^{\frac{n}{m}}=a^{(n,s)}=a^{u\cdot n+v\cdot s}=(a^n)^u\cdot(a^s)^v=e(a^s)^v\in K$$

$(n,s)=un+vs$, $\exists u,v\in\mathbb{Z}$ (אוקלידס) ; כי $a^s\in K$

הוכחנו $a^{\frac{n}{m}}\in K$. **סוף**

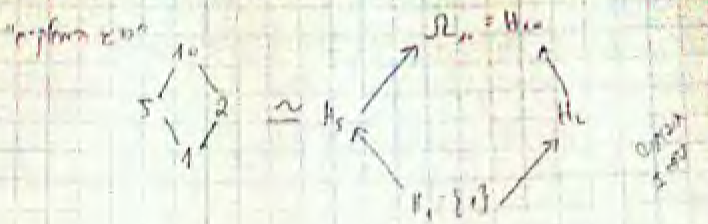
תרגיל: למצוא את כל תתי חבורה

(א) Ω_{10}

(ב) $\mathbb{Z}_{15}$

לבד

הערה: "סריג של ..."



משפט Wilson

(VIII Bhaskara הודו)

עבור שלם טבעי מתקיים

$n \mid (n-1)! + 1 \iff n =$ ראשוני

הוכחה: $(\Leftarrow)$: נניח p ראשוני $p \geq 3$. $p \mid (p-1)! + 1$

כרעיון להוכחה ניקח מקרה $p=7$

$7 \mid 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 + 1$

שקול למה $0 \equiv (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6) + 1 \mod p$

$p-1 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \mod p$

$6 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \mod 7$

באופן כללי: צ"ל: $p \mid (p-1)! + 1$

שקול להוכיח ש- $(p-1)! \equiv p-1 \mod p$

שקול להוכיח ש- $(p-1) \mod p$: $1 \cdot 2 \cdot 3 \cdot 4 \cdots (p-2) \cdot (p-1) = (p-1)$

נסדר כל איבר עם ההופכי שלו. ידוע לנו ש- $(\mathbb{Z}_p, \oplus, \odot)$ שדה

לכל $[a]_p \neq [0]_p$ יש הופכי

חשוב שלכל איבר ששונה מ $[1]$ או $[p-1]$ ההופכי שונה ממנו מתקיים:

$[a^{-1}] = [a]^{-1} \iff a = [1] \vee [a] = [p-1]$

$\forall [a] \in \mathbb{Z}_p^* = \{[1], \dots, [p-1]\} = V_p$

חבורה לגבי כפל

$[x]^{-1} = [x]$

$[x]^2 = [1] = [1]^2$

$([x] - [1]) \cdot ([x] + [1]) = [0]$

$[x] = [1]$ או $[x] = -[1] = [-1] = [p-1]$

אם
אם רק
ורק אם נב...

יהיה סה"כ מחו...

תוך דקה
להוציא ...
שוב...

זין מראן

① 2. $(p-1)(p-1) = ① \cdot 1 \cdot (p-1) \cdot (p-1) \bmod p$

הוכחת ניש׳ יחין

$\exists u \in \mathbb{Z}: u \cdot n = (n-1) + [n \mid (n-1)] + 1$

$u \cdot n - (n-1) = 1$

$v_k = \frac{(n-1)}{n}$ ... $k \in n$ ... $1 \le k \le n$

$u \cdot n + v_n k = 1$, $(n,k) = 1$, $\forall k \in \varphi: k \in n$

חבורת מנה

משפט: נניח $H \trianglelefteq G$ (H תת-חבורה נורמלית ב-G)

(1) $(G/H, *)$ חבורה לגבי הפעולה: $aH * bH := (ab)H$

(2) $\varphi: G \to G/H$, $g \mapsto gH$ — הומומורפיזם

(3) $\ker\varphi = H$

הוכחה: נוכיח קודם ש- $(aH)(bH) = (ab)H$ (כפל ב-G של $*$)

$\{(ab)h \mid h \in H\}$ = $\{(ah_1)\cdot(bh_2) \mid h_1, h_2 \in H\}$ (הכפל הקבוצתי)

$H = \{e, u, u^2\} \le G$, 4

$(aH)(bH) = (aH)\cdot(Hb) = a(H\cdot H)\cdot b = a(Hb) = a(bH) = (ab)H$

($bH = Hb$ נורמלי; $H \trianglelefteq G$)

מהמשוואה $(aH)\cdot(bH) = (ab)H$

נוכיח שאין תלות בנציגים של המחלקה

$a'H = aH$, $b'H = bH$ $\Leftarrow$ $a'H \cdot b'H = aH \cdot bH = (ab)H$

$a'H * b'H = aH * bH$

כי $(G/H, *)$ מבנה אלגברי.

המבנה בעצם חבורה: אסוציאטיביות נובעת מזו של $(G, \cdot)$

נייטרלי: $[e] = H \in G/H$, e נייטרלי ב-G

$[e] = H$ נייטרלי ב-$(G/H, *)$

הופכי ל- $[a] = aH \in G/H$: $[a]^{-1} = [a^{-1}] = a^{-1}H \in G/H$

(2) φ על: כי לכל $gH \in G/H$

$\varphi(g) = gH = [g]$

φ הומו׳:

$\forall a, b \in G$

$\varphi(ab) = \varphi(a)\varphi(b) = (ab)H$ // def

$\varphi(a) * \varphi(b) = aH * bH$

(3)

$\ker\varphi = \{x\in G \mid \varphi(x)=[e]=H\} = \{x\in G \mid xH=H\} = \{x\in G \mid x\in H\} = H$ מש"ל

דוגמאות:

$G=(\mathbb{Z},+)$

$H=n\mathbb{Z}$

$(G/H,\times)=(\mathbb{Z}/n\mathbb{Z},\times)=(\mathbb{Z}_n,\oplus)$

הגדרה: $H\leq G$

התנאים הבאים שקולים:

(א) $\forall g\in G \quad gH=Hg$ (הגדרה)

⇕

(ב) $\forall g\in G \quad gHg^{-1}=H$ (הצמדה ע"י g משאירה H במקום)

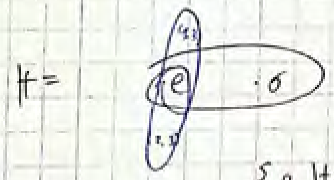
⇕

(ג) $\forall g\in G \quad gHg^{-1}\subseteq H$

שני משמעות ע"י g במקום g.

(ד) $\forall g\in G,\ h\in H \quad ghg^{-1}\in H$

דוגמה: $H=\{e,(1\,2)\}\leq G=S_3$



מסלול הצמדות של H: $\{gHg^{-1}\mid g\in G\}=\{H_1,H_2,H_3\}$

$geg^{-1}=e$ $\quad H\ntrianglelefteq G$

הערה: הצמדה ע"י g בחבורה G היא $\alpha_g: G\to G$

$\alpha_g(x)=gxg^{-1}$ $\quad x\in G$ משתנה, g קבוע.

תכונות:

(1) α_g אוטומורפיזם (אוטומורפיזם "פנימי")

הוכחה:

הומו: $\alpha_g(x_1x_2)=g(x_1x_2)g^{-1} = (gx_1g^{-1})\cdot(gx_2g^{-1}) = \alpha_g(x_1)\cdot\alpha_g(x_2)$

על: יהי $y\in G$ ניקח $x=g^{-1}yg\in G$ אז $\alpha_g(x)=y$

חח"ע: $x_1\neq x_2$ צ"ל: $g(x_1)\neq g(x_2)$.

אם נניח $\alpha_g(x_1)=\alpha_g(x_2)$

$gx_1g^{-1}=gx_2g^{-1}$

$\Downarrow$

$x_1=x_2$ סתירה.

(1)

אוטומורפיזמים פנימיים . $Inn(G) = \{\alpha_g\}_{g\in G}$

$$Inn(G) \trianglelefteq Aut(G)$$ ≤ S_G

לצריכות הרכבה

$$\alpha_{g_1} \circ \alpha_{g_2} = \alpha_{g_1 g_2}$$

$$g \in Z(G) \iff \alpha_g = id_G$$

(3)

$$Z(G) = \{g \in G \mid gx = xg \quad \forall x \in G\}$$

(4) בחבורה אבלית $\alpha_g = id_G$ ∀

דוגמה אוטומורפיזמים לא פנימיים :

(5) $(\mathbb{C}, +)$

$z \mapsto \bar{z}$ אוט' (לא שגר)

$a+bi \mapsto a-bi$

$f \neq id_{\mathbb{C}}$.

(6) $G = \Omega_3 \times \Omega_3$

$G \xrightarrow{f} G$

$(x,y) \to (y,x)$

אוטומ' (לבדוק) $\neq id_G$. לכן לא פנימי.

משפט Cayley (קיילי)

כל חבורה G איזומורפית לתת חבורה של S_G.

⇓

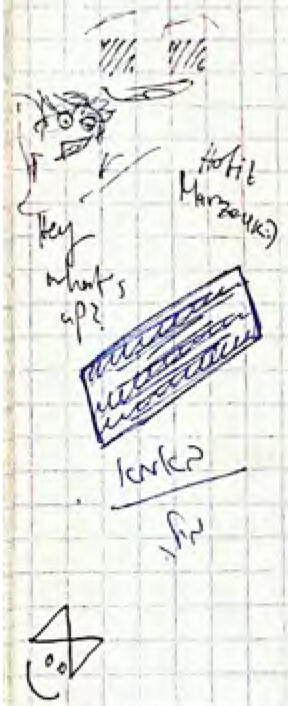
תוצאה: כל חבורה סופית G עם $n=|G|$ איברים "משוכנת" לתוך S_n.

הסבר התוצאה: מהמשפט ישר נקבל שקיימת ת"ח $H \leq S_G$, $G \cong H$

נשים לב שבכה שקול: קיים מיפוי $G \to S_G$:

$$S_G = \{G \xrightarrow{f} G \text{ חח"ע ועל}\} = \left\{\begin{pmatrix} g_1 = e, & g_2, & \dots & g_n \\ g_{i_1} & g_{i_2} & \dots & g_{in} \end{pmatrix}\right\}$$

$$S_n = \left\{\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}\right\}$$



קל לבדוק שזו איזומורפיזם לכן $G \xrightarrow{\varphi} S_n$

$G \xrightarrow{\text{איזו'}} S_G \xrightarrow{f} S_n$

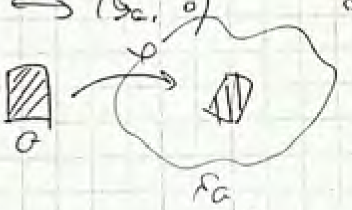
$f\cdot\varphi$ מונומורפיזם

טיפ: הטבלה של חבורה $G=\{g_1=e, g_2, \dots, g_n\}$

	g_1	g_2	$\dots$	g_n
g_1				
$\vdots$				
g	gg_1	$\dots$	$\dots$	gg_n
$\vdots$				
g_n				

הוכחה של משפט קיילי:

צ"ל שקיים מונו' $(G,\cdot) \xrightarrow{\varphi} (S_G, \circ)$



נגדיר $\varphi: G\to S_G$, $\varphi(a)=l_a$ ונוכיח כי מונו'.

קודם כל φ מוגדר נכון: $l_a \in S_G$ $\forall a\in G$, הפיך!!

l_a חח"ע: $x_1\neq x_2 \Rightarrow ax_1\neq ax_2$

l_a על: לכל $y\in G$ ניקח $x:=a^{-1}y$ אז $l_a(x)=y$

$\Downarrow$

$l_a\in S_G$.

l_a הומו':

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

$$\varphi(a\cdot b)=l_{ab} = l_a\cdot l_b = \varphi(a)\circ\varphi(b)$$

φ חח"ע: צ"ל: $a\neq b \Rightarrow l_a\neq l_b$ ($l_a=\varphi(a)$, $l_b=\varphi(b)$)

$$l_a\neq l_b \Leftarrow \begin{cases} x=e & l_a(e)=a\cdot e=a \\ & \neq \\ & l_b(e)=b\cdot e=b \end{cases}$$

הערה

{איזומטריות ליניאריות של $\mathbb{R}^n$} חבורה מטריצות, אורתוגונליות

החבורה $O_n(\mathbb{R}) \leq GL_n(\mathbb{R})$ = {מטריצות אורתוגונליות}

כל חבורה סופית עם n איברים היא משוכנת לתוך $O_n(\mathbb{R})$.

הוכחה: לפי משפט קיילי $G \xhookrightarrow{\varphi} S_n$

לכן מספיק להראות: $S_n \hookrightarrow O_n(\mathbb{R})$

$e_1, e_2, \dots, e_n$ הבסיס הסטנדרטי של $\mathbb{R}^n$.

$$S_n \ni \alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \xleftrightarrow{\text{בסיס סטנדרטי של } \mathbb{R}^n} \begin{pmatrix} e_1 & e_2 & \cdots & e_n \\ e_{i_1} & e_{i_2} & \cdots & e_{i_n} \end{pmatrix}$$

$$\begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad (1,2) \mapsto \begin{pmatrix} e_1 & e_2 & e_3 \\ e_2 & e_1 & e_3 \end{pmatrix} \leftrightarrow \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in O_n(\mathbb{R})$$

...

מסקנה: כל חבורה סופית ניתנת לשיכון בחבורה אורתוגונלית.

חבורות של סימטריות:

נניח $A \subseteq \mathbb{R}^n$.

$$Sym(A) := \left\{ \mathbb{R}^n \xrightarrow{f} \mathbb{R}^n \;\middle|\; \begin{array}{l} \text{(א) } f \text{ על} \\ \text{(ב) } f \text{ שומר מרחקים} \\ \text{(ג) } f(A) = A \end{array} \right\}$$

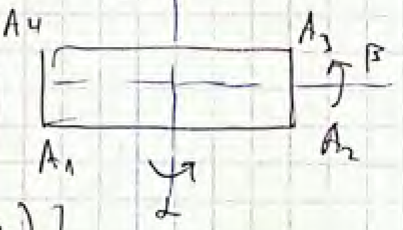
כלומר: $\forall u, v \in \mathbb{R}^n \quad \|f(u) - f(v)\| = \|u - v\|$

דוגמאות

(1) $A \subseteq \mathbb{R}^2$ = מצולע משוכלל. $Sym(A) = D_n$

(2) $A = $ ▭ מלבן ב-$\mathbb{R}^2$ לא ריבוע $Sym(A) = K_4$ "חבורת Klein"

V_4 ״



$$K_4 = \left\{ e = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_1 & A_2 & A_3 & A_4 \end{pmatrix}, \alpha = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_2 & A_1 & A_4 & A_3 \end{pmatrix}, \right.$$

$$\left. \beta = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_4 & A_3 & A_2 & A_1 \end{pmatrix}, \gamma = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_3 & A_4 & A_1 & A_2 \end{pmatrix} \right\}$$

ובכן: תרגיל

בניית תת-חבורה: אתגר.

לכל הסבר על השאלה: ואתר.

משהו.

Generated by CamScanner from intsig.com

Generated by CamScanner from intsig.com

15/08/2011

גיליון V

המשך סימטריות

חבורת קליין K_4 היא משוכנת באופן טבעי לתוך $S_4 \cong S_{\{A_1,A_2,A_3,A_4\}}$

חבורת D_n (סימטריות של מצולע משוכלל עם n קודקודים), היא משוכנת לתוך $S_n \cong S_{\{A_1,\dots,A_n\}}$

הגדרה: תת קבוצה A בחבורה G נקראת קבוצת יוצרים של G,
(סימון $G = \langle A \rangle$), אם כל איבר $g \in G$ אפשר להציג בצורה

$$g = a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n}$$

$$a_i \in A$$

$$k_i \in \mathbb{Z}$$

הערה: שקולה להגדרה $G = \langle A \rangle$, כאשר מגדירים $\langle A \rangle$ כתת חבורה ב-G הנוצרת ע"י A

$$\langle A \rangle = \left\{ a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n} \;\middle|\; \begin{matrix} a_i \in A \\ k_i \in \mathbb{Z} \end{matrix} \right\} \leq G$$

שימו לב:

תת החבורה הקטנה ביותר שמכילה את A →

$$\boxed{\langle A \rangle = \bigcap \{ H \leq G \mid A \subseteq H \}}$$

הגדרה: $\text{rank}(G) = \min \{ |A| \mid \langle A \rangle = G \}$ "הדרגה של G"

תכונות:

(א) ברור: $\text{rank}(G) \leq |G|$.

הסבר: ניקח $A := G$

(ב) $\text{rank}(G) = 1 \iff G$ ציקלית

(ג) $\text{rank}(K_4) = 2$ $\quad K_4 \cong \Omega_2 \times \Omega_2$ (חבורה כפלית)

$a = (-1,1) \quad (1,-1) = b$

$A = \{a, b\}$

$\langle A \rangle = \Omega_2 \times \Omega_2$

(ד) $G = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ $\quad (G, +)$

$e_1 = ([1],[0],[0])$

$e_2 = ([0],[1],[0])$

$e_3 = ([0],[0],[1])$

$g = c_1 e_1 + c_2 e_2 + c_3 e_3$ $\quad c_i \in \mathbb{Z}$ (כל)

$(0 \leq c_1, c_2, c_3 \leq 2$

Generated by CamScanner from intsig.com

קומוטטיבית: אם החבורה היא $(G,+)$ אז:

$$\langle A \rangle = \{ k_1 a_1 + k_2 a_2 + \dots + k_n a_n \mid a_i \in A,\ k_i \in \mathbb{Z} \}$$

מקרה פרטי של החבורה הנ"ל נקרא פעולה חיבורית.

(ג) $G = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$

$$g = k_1 e_1 + k_2 e_2 + k_3 e_3 \qquad k_i \in \mathbb{Z}$$

$rank(G) = 3$

(1) $rank(\mathbb{Z}^n) = n$.

דוגמה חשובה:

$rank(D_n) = 2$.

τ - שיקוף
a - סיבוב

$$D_n = \begin{cases} e \quad a \quad a^2 \quad \dots \quad a^{n-1} & \text{סיבובים} \\ \tau \quad a\tau \quad a^2\tau \quad \dots \quad a^{n-1}\tau & \text{שיקופים} \end{cases}$$

$a = R_{\frac{2\pi}{n}}$, $O(a) = n$.

⚠ τ אחד מהשיקופים. לכל שיקוף הסדר שווה ל-2. כ"א

$(a^k\tau)^2 = e$

⇓

$a^k\tau \cdot a^k\tau = e \quad / (a^{-k} \cdot \tau^{-1})$

$\tau a^k = a^{-k} \cdot \tau^{-1}$

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

$$\boxed{\tau \cdot a^k = a^{n-k} \cdot \tau = a^{-k} \cdot \tau}$$

$$D_n = \langle \underbrace{a, \tau}_{\text{יוצרים}} \mid \underbrace{a^n = e,\ (a^k\tau)^2 = e}_{\text{יחסים}} \rangle$$ [illegible]

⇓

$n \geq 3$

$rank(D_n) = 2$.

הגדרה: חבורה G [illegible] נוצרת סופית (נ"ס) אם קיימת תת קבוצה **סופית** A כך ש $\langle A \rangle = G$.

כ"א אם $rank(G) = \infty$ סופי.

למשל:

(א) כל חבורה סופית היא נ"ס (כי $rank(G) \leq |G|$)

(ב) $\mathbb{Z}^{100}$

(ג) **לא נ"ס:** $(\mathbb{Q},+)$, $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R},+)$

Generated by CamScanner from intsig.com

תכונות נוספות של S_n

תזכורת: (משפט Cayley) כל חבורה סופית עם n איברים משוכנת בתוך S_n.

① S_n לא קומוטטיבית $n \notin \{1,2\}$. ($n \geq 3$)

② $|S_n| = n!$

③ $\dots \hookrightarrow S_n \hookrightarrow S_{n+1} \hookrightarrow S_{n+2} \hookrightarrow \dots$

שיכון טבעי $S_n \hookrightarrow S_m$ $\forall n \leq m$.

הגדרה: עגל (או מחזור) באורך t

סימון: $\underbrace{(i_1\ i_2\ i_3\ \dots\ i_t)}_{\text{שונים}} \in S_n$, $t \leq n$ המשמעות:

למשל: $\alpha = (2, 5, 3) \in S_7$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \| & \downarrow & \downarrow & \| & \downarrow & \| & \| \\ 1 & 5 & 2 & 4 & 3 & 6 & 7 \end{pmatrix}$$

④ t = אורך העגל = הסדר של $\alpha = (i_1, \dots, i_t)$

למשל: $(2,4)$ (i,j) "חילופים" $i \neq j$. $(i, j)^2 = e$.

$\alpha = (2,5,3)$, $O(\alpha) = 3$

הערה: $(i) = e$ עגל באורך 1.

⑤ **טענה:** כל תמורה $\alpha \in S_n$ היא שווה למכפלה של מחזורים זרים.

הגדרה: $\sigma_1 = (i_1, i_2, \dots, i_t)$

$\sigma_2 = (j_1, j_2, \dots, j_k)$

זרים אם $\{i_1, i_2, \dots, i_t\} \cap \{j_1, j_2, \dots, j_k\} = \emptyset$.

למשל $(1,5,4,8)$ ו- $(2,3)$ זרים.

דוגמה:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 3 & 6 & 7 & 10 & 14 & 1 & 2 & 13 & 15 & 4 & 11 & 5 & 8 & 12 & 9 \end{pmatrix} =$$

$= \sigma_1 \sigma_2 \sigma_3 \sigma_4 \sigma_5 \sigma_6$

האלגוריתם:

$1 \xrightarrow{\alpha} 3 \xrightarrow{\alpha} 7 \to 2 \to 6$ $\quad 4 \to 10$ $\quad 5 \to 14 \to 12$

$\sigma_1 = (1, 3, 7, 2, 6)$ $\quad \sigma_2 = (4, 10)$ $\quad \sigma_3 = (5, 14, 12)$

$\sigma_4 = (8, 13)$ $\quad \sigma_5 = (9, 15)$ $\quad \sigma_6 = (11)$

Generated by CamScanner from intsig.com

תכונות

א) sign תמיד הומומורפיזם

$\text{sign}(\alpha\circ\beta) = \text{sign}(\alpha)\,\text{sign}(\beta) \quad \forall \alpha,\beta \in S_n$

sign אפימורפיזם $\Leftrightarrow n \geq 2$

ב)

$$\text{sign}(i_1,\dots,i_t) = \begin{cases} 1 & t = \text{אי-זוגי} \\ -1 & t = \text{זוגי} \end{cases}$$

למשל:

$\text{sign}(2,5) = \text{sign}(i,j) = -1$

$\text{sign}(2,5,3) = 1$

$(2,5,3) = \underbrace{(2,5)(5,3)}_{\text{2 חילופים}}$

$\text{sign}(e) = 1$

ג) $\text{sign}(\alpha^m) = \text{sign}(\alpha)^m \quad \forall m \in \mathbb{Z}$

ד) $\boxed{\text{sign}(\alpha g \alpha^{-1}) = \text{sign}(g)}$

הסבר:

$\text{sign}(g)\cdot\text{sign}(\alpha)\cdot\text{sign}(g)^{-1} = \text{sign}(g)\cdot\text{sign}(g)^{-1}\cdot\text{sign}(\alpha)$

$\mathbb{Z}_2$ אבלי!

ה) הגרעין של sign:

$\text{Ker}(\text{sign}) = \{\text{תמורות זוגיות}\} = A_n$

תמיד: $A_n \quad S_n$

טענה: באופן כללי כל גרעין $\ker f \leq X$ של הומומורפיזם $f: X \to Y$ הוא תת חבורה נורמלית ב-X, צ"ל $\boxed{\ker f \trianglelefteq X}$

הסבר: יהי $\ker f = H \leq X$

שקול להוכיח $xhx^{-1} \in H \quad \forall h \in H,\ \forall x \in X$

שקול להוכיח: $f(xhx^{-1}) = e_Y$

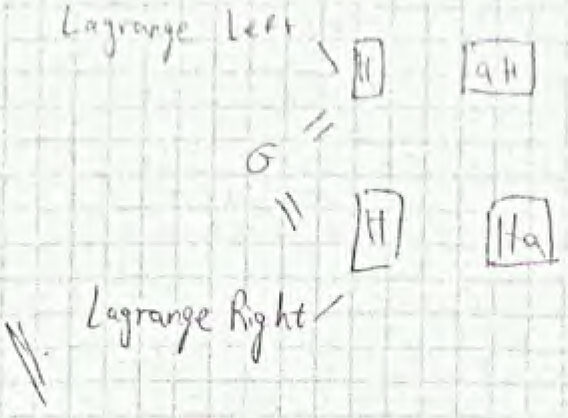
בדיקה: $f(xhx^{-1}) = f(x)f(h)f(x)^{-1} = f(x)\cdot e_Y \cdot f(x)^{-1} = e_Y$.

דרך אחרת שהוכחת ש- $A_n \trianglelefteq S_n$ נורמלית מהטענה:

טענה: באופן כללי $\boxed{H \trianglelefteq G \Leftarrow [G:H] = 2}$

Generated by CamScanner from intsig.com

הרצאה: נוקה 11 פג



$$[S_n : A_n] = 2$$

הוכחה:

$$S_n = \boxed{A_n} \cup \boxed{\tau A_n} \qquad \tau := (1,2)$$

A_n ← זוגיים; τA_n ← אי זוגיים — 2 קוסטים

$$|A_n| = |\tau A_n|$$
$$\Downarrow$$
$$[S_n : A_n] = 2$$

מס' האיברים הזוגיים ← $\boxed{|A_n| = \frac{n!}{2}}$

⑧ הצמדה ב- S_n:

נניח $\sigma = (i_1, i_2, \dots, i_m)$ מעגל. $g \in S_n$ $g\sigma g^{-1} = ?$

תשובה: $g\sigma g^{-1} = (g(i_1), g(i_2), \dots, g(i_m))$

דוגמה: $\sigma = (2,4)$ ב- S_4

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

$$g(2,4)g^{-1} = (g(2), g(4)) = (4,2) = (2,4)$$

מסקנה: $g\sigma g^{-1} = \sigma$

שקול: $g\sigma = \sigma g$ (מתחלפים).

$$\alpha = (3,2,4)$$

$$g\alpha g^{-1} = g(3,2,4)g^{-1} = (g(3), g(2), g(4)) = (1,4,2)$$

מסקנות: הצמדה לא משפיעה על האורך של מעגל אלא "הטיפוס" של תמורה (מבנה).

3.3

Generated by CamScanner from intsig.com

אם σ_i ... $\alpha = \sigma_1 \sigma_2 \cdots \sigma_m$ מכפלה של מחזורים

$$g\alpha g^{-1} = g(\sigma_1\sigma_2 \cdots \sigma_m)g^{-1} = (g\sigma_1 g^{-1})(g\sigma_2 g^{-1}) \cdots (g\sigma_m g^{-1})$$

למשל:

$$\alpha = (2,4)(1,5,3)$$

$$g\alpha g^{-1} = (i_1, j_2)(i_1, i_2, i_3)$$

(רווחה 2.1)

מסקנה: לפי הטענה, כל אוסף תת"ח נורמלית. ההפך לא נכון!

ציון: כל $H \trianglelefteq G$ אפשר להציג כגרעין של הומומורפיזם מתאים.

זה נותן משפט חבורת מנה.

הגדרה: אם $H \trianglelefteq G$ אז $(G/H, \cdot)$ חבורה (נקראת חבורת מנה)

אז $p: G \to G/H$

$g \mapsto gH$

$\boxed{\ker p = H}$

משפט: לכל חבורה G מתקיים (Y חבורה)

$$\{H \mid H \trianglelefteq G\} = \{\ker f \mid f: G \underset{\text{הומ'}}{\to} Y\}$$

דוגמאות נוספות של תת"ח נורמליות:

(1) $G \trianglelefteq G$ $\quad \{e\} \trianglelefteq G$

$$G/G \cong \{e\}$$

$$G/\{e\} \cong G$$

(2) $\mathbb{R}_+ \trianglelefteq \mathbb{R}^*$

$$\mathbb{R}^*/\mathbb{R}_+ \cong \Omega_2$$

$$\{\mathbb{R}_+, \mathbb{R}_-\} \qquad \{+1, -1\}$$

(3) $\{A \in M_n(\mathbb{R}) \mid \det(A) = 1\} =: SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$

הסבר:

$$SL_n(\mathbb{R}) = \ker(\det)$$

(4)

$$\boxed{H \trianglelefteq G \Leftarrow [G:H] = 2}$$

למשל:

א) $A_n \trianglelefteq S_n$

ב) (דיהדרלית) $\langle a \rangle = \{e, a, \ldots, a^{n-1}\} =: \underset{n}{C_n} \trianglelefteq \underset{2n}{D_n}$

ג) $D_n / C_n \cong \Omega_2$

Generated by CamScanner from intsig.com

(ד)

שאלה: מה הן התמונות ההומומורפיות של חבורה (תמונה של G)
(עד כדי איזומורפיזמים)

כלומר נניח $G \to Y$ אפימורפיזם
למצוא Y (עד כדי איזו)

דוגמה: העתקה טבעית $G \xrightarrow{p} G/H$ אפי

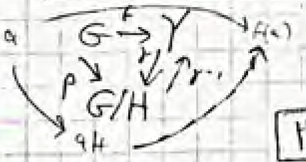
תשובה: כל תמונה אפימורפית היא בדיוק של חבורות מנה

משפט Noether (האיזומורפיזם I)

נניח $G \xrightarrow{f} Y$ אפימורפיזם בין חבורות. אז מתקיים:

① $\boxed{Y \cong G/\ker f}$

②



כאשר $G/H \xrightarrow{\gamma} Y$ איזומורפיזם

$\boxed{H := \ker f}$

$\boxed{f = \gamma \circ p}$

הוכחה: בניית γ: (הגדיר)

$$G/H \xrightarrow{\gamma} Y$$
$$aH \mapsto f(a)$$

הערה: γ מוגדר היטב כי

$$a_1H = a_2H$$
$$\Updownarrow$$
$$a_1^{-1}a_2 \in H = \ker f$$
$$\Updownarrow$$
$$f(a_1^{-1}a_2) = e_Y$$
$$\Updownarrow$$
$$f(a_1) = f(a_2)$$

מוכיח שאין תלות בנציגים!

הוכחנו $f(a_1)=f(a_2) \Leftrightarrow a_1H = a_2H$ (כלומר $[a_1]$, $[a_2]$) מכאן $[a_1]=[a_2] \Leftrightarrow \gamma([a_1]) = \gamma([a_2])$ (כלומר $f(a_1)$, $f(a_2)$)

זה מוכיח שפונקציה $\gamma: G/H \to Y$ היא חח"ע

γ על: נובע מהבנייה של γ, כי אם $y \in Y$ אז קיים $x \in G$ כך ש $f(x)=y$
(כי f על).

$$\gamma(xH) = \gamma([x]) = f(x) = y$$

מה שנדרש

$xH \to y$. הושלם.

Ufit Marzouk:)

Ufit Marzouk:)

$[x] = xH$

$[y] = yH$

γ הומומורפיזם:

$\gamma : G/H \to Y$

צריך:

$\gamma[\,[x]\cdot[y]\,] \overset{?}{=} \gamma([x]) \cdot \gamma([y]) = f(xy)$

$\gamma([x]) \cdot \gamma([y]) = f(x) \cdot f(y)$

מתקיים:

$\gamma([x] \cdot [y]) \overset{\text{הגדרה}}{=} \gamma([xy]) \overset{\text{הגדרה}}{=} f(xy)$

$\qquad \Vert$ הומו' f

$\gamma([x]) \cdot \gamma([y]) = f(x) \cdot f(y)$

הראינו γ איזומורפיזם

$f = \gamma \circ p$ ישר מההגדרה.

משל

<u>תוצאה 1</u>: כל תמונה אפימורפית של G היא $\simeq$ חבורת מנה.

<u>תוצאה 2</u>: לכל אפימורפיזם של חבורות סופי $G \xrightarrow{f} Y$ מתקיים

$$|Y| \mid |G|$$

<u>הסבר</u>: לפי לגרנז':

$|G| = [G:H] \cdot |H|$

משפט האיזומורפיזם הראשון:

$|G/H| = |Y|$

$\Vert$

$[G:H]$

כאשר $H = \ker f$

קיבלנו $|Y| \mid |G|$. משל

<u>תוצאה 3</u>: לכל הומומורפיזם $G \xrightarrow{f} Y$ מתקיים: $\boxed{\mathrm{Im} f \simeq G/\ker f}$

<u>דוגמא 1</u>: למצוא תמונות אפימורפיות של:

(א) $\mathbb{Z}$

(ב) $\mathbb{Z}_{15}$

(ג) D_3

Generated by CamScanner from intsig.com

תשובה:

א) {חבורות ציקליות} הסבר: ציקליות $\{\mathbb{Z}/H \mid H \trianglelefteq \mathbb{Z}\}$

אבליות ←

$\{\mathbb{Z}/H \mid H \leq \mathbb{Z}\}$

$\{\mathbb{Z}/H \mid n\mathbb{Z} \quad n \in \{0,1,2,\dots\}\}$

$\mathbb{Z}/\{0\} \cong \mathbb{Z}$ $\quad n=0$

$\mathbb{Z}_1 = \mathbb{Z}/\mathbb{Z} \cong \Omega_1 = \{1\}$ $\quad n=1$

$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ $\quad n\geq 2$

בגלל משפט מיון חבורות ציקליות (קב) אלו התשובה.

ב) $\{\mathbb{Z}_n \mid n|15\}$

תמיד נורמלית (כי $\mathbb{Z}_n$ אבלית) $H \trianglelefteq \mathbb{Z}_n$

$\lvert H\rvert$	G/H ציקלית (כי תמונה הומומורפית של ציקלית היא ציקלית)
1	$\mathbb{Z}_{15}/\{0\} \cong \mathbb{Z}_{15}$
3	$\mathbb{Z}_5$ $\quad [15:3]=5$
5	$\mathbb{Z}_3$
15	$\mathbb{Z}_1$

ג) תשובה: $\{D_3, \mathbb{Z}_1, \mathbb{Z}_2\}$

הסבר: {תמונות הומומורפיות} $=$

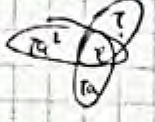
$\{D_3/H \mid H \trianglelefteq D_3\}$ $=$

$\left\{D_3/H \;\middle|\; H=\{e\},\ H=D_3,\ H=C_3\right\}$

$D_3/\{e\} \cong D_3$

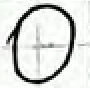
$D_3/D_3 \cong \mathbb{Z}_1$

$D_3/C_3 \cong \mathbb{Z}_2$



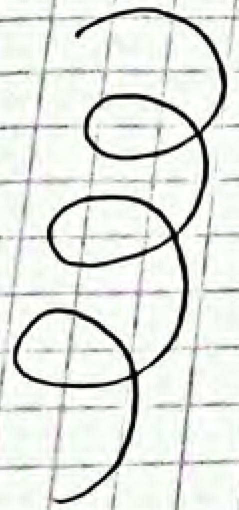
תתי חבורות 2 איברים הם: $\{e,\tau\}$ (H_1), $\{e,\tau a\}$ (H_2), $\{e,\tau a^2\}$ (H_3) — לא נורמליות

דוגמה 2: הוכח ש $\mathbb{T} \cong \mathbb{R}/\mathbb{Z}$



פתרון: נמצא $\cong$ ע"פ משפט איזו' I.

צ"ל נמצא אפי' $\mathbb{R} \xrightarrow{f} \mathbb{T}$ כך ש $\ker f = \mathbb{Z}$



$$f(t) = cis(2\pi t)$$

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{f} & \mathbb{T} \\ \downarrow & \nearrow_{\cong} & \\ \mathbb{R}/\ker f & & \end{array}$$

$$\ker f = \mathbb{Z}$$

17/08/2011

הרצאה VI

ב 8 עד 9 שיעור השלמה
9:00

תזכורת:

$\mathbb{R}/\mathbb{Z} \simeq \mathbb{T}$

דוגמה: $\mathbb{R} \to \mathbb{T}$, $f(t) = cis(2\pi t)$, $\ker f = \mathbb{Z}$, $\mathbb{T} \cong \mathbb{R}/\ker f$

$\mathbb{T} := \{ z \in \mathbb{C} \mid \|z\| = 1 \}$ S^1

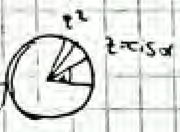
תרגיל: הוכח: $\mathbb{R}^2/\mathbb{Z}^2 \simeq \mathbb{T}^2$

טורוס - Z מימד
"צינור הגלגל"

$\mathbb{T} \geq \{ z \in \mathbb{T} \mid O(z) < \infty \} = \Omega_\infty = \bigcup_{n \in \mathbb{N}} \Omega_n \simeq \mathbb{Q}/\mathbb{Z}$

הערה: 1) $O(z) < \infty \iff \frac{\alpha}{\pi} \in \mathbb{Q}$, $z = cis\,\alpha$

2) $O(z) = \infty \iff \frac{\alpha}{\pi} \notin \mathbb{Q}$



$\langle z \rangle = \{z^n\}_{n \in \mathbb{N}} \leq \mathbb{T}$
"צפוף ב $\mathbb{T}$"

גם קשר (צפוף) קיים n כך ש z^n שרירותי

הערה: $O_2(\mathbb{R}) \geq \left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \right\} \simeq \mathbb{T} \leq \mathbb{C}^*$ ← מט' אורתוגונליות מסדר 2

$0 \leq \alpha \leq 2\pi$

תחבורת סיבובים

תרגיל: הוכח שלכל n קיים מונומורפיזם $\mathbb{Z}_n \hookrightarrow O_2(\mathbb{R})$ (או Ω_n).

הערה לגבי הבוחן: "במשחק ה "15" המצב הנתון פתיר אם"ם הפרמוטציה $\in A_{15}$ (זוגי!)

$S_n = \langle (1\,2), (1\,2 \ldots n) \rangle \rightarrow rank(S_n) = 2$, $|S_n| = n!$ *

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \hookrightarrow S_8$

$rank(\mathbb{Z}_2^3) = 3 > rank(S_8) = 2$

עוד תרגילים לגבי משפט האיזו I

תרגיל:

א. $\mathbb{R}^*/\mathbb{R}_+ \simeq \mathbb{Z}_2$ (אפשר גם בדרך אחרת)

ב. $\mathbb{C}^*/\mathbb{T} \simeq \mathbb{R}_+$

הקוסטים הם מעגלים עם מרכז בראשית הצירים

$\mathbb{C}^*/\mathbb{T}$ = חבורת מנה של האיברים הם מעגלים

משפט האיזומורפיזם II:

נניח $A \le G$, $H \trianglelefteq G$ אזי:

① $AH \le G$, $H \trianglelefteq AH$, $A \cap H \trianglelefteq A$

② $AH/H \simeq A/A\cap H$

רעיון ההוכחה של ②:

מבוסס על משפט האיזו' I. מגדירים $f: A \xrightarrow{f} AH/H$, $\ker f = A\cap H$

$f(a) = aH$ ...

דוגמה:

$$(4\mathbb{Z}+6\mathbb{Z})/6\mathbb{Z} \simeq 4\mathbb{Z}/4\mathbb{Z}\cap 6\mathbb{Z}$$

דרך אחרת:

$$(4\mathbb{Z}+6\mathbb{Z})/6\mathbb{Z} = 2\mathbb{Z}/6\mathbb{Z}$$

ציקלי עם 3 אלמנטים

:: ______

$$4\mathbb{Z}/4\mathbb{Z}\cap 6\mathbb{Z} = 4\mathbb{Z}/12\mathbb{Z}$$

שניהן איזומורפיים ל- $\mathbb{Z}_3$.

הערה: מתקיים $[AH:H] = [A:A\cap H]$ כתוצאה מאיזו' II.

משפט האיזומורפיזם III: (הצמצום)

נניח $H \trianglelefteq G$, $N \trianglelefteq G$, $N \le H$ אזי:

$$\left((G/N)/(H/N)\right) \simeq G/H$$

דוגמה: $(\mathbb{Z}/24\mathbb{Z})/(6\mathbb{Z}/24\mathbb{Z}) \simeq \mathbb{Z}/6\mathbb{Z}$

תכונות של מכפלה קרטזית של חבורות:

אם X, Y חבורות אז מגדירים מכפלה קרטזית של חבורות כחבורה

הבאה: קבוצה

$$X \times Y := \left\{ (x,y) \;\middle|\; \begin{matrix} x\in X \\ y\in Y \end{matrix} \right\}$$

הפעולה תהיה רכיבית:

$$(x_1,y_1) * (x_2,y_2) := (x_1x_2, y_1y_2)$$

דוגמה: $K_4 \simeq \Omega_2 \times \Omega_2$ $\quad (\mathbb{R}^2,+)$

הערה: אם X, Y "חיבוריות" אז $(x_1,y_1)+(x_2,y_2)=(x_1+x_2, y_1+y_2)$

באופן דומה מגדירים $\prod_{i=1}^{n} X_i : X_1 * X_2 * \dots * X_n$, n חבורות. אז אומרים "נוטציה" של חבורות.

וגם לאוסף $\{X_i\}_{i\in I}$ של חבורות, I קבוצה (לא מוגבלת, או הדוגמה)

$$\prod_{i\in I} X_i = \{ I \xrightarrow{f} \bigcup_{i\in I} X_i \ , \ f(i)\in X_i \}$$

$$f := (x_i)_{i\in I} \quad , \quad x_i = f(i) \in X_i$$

$$\boxed{(x_i)_{i\in I} * (y_i)_{i\in I} = (x_i \cdot x_i')_{i\in I}}$$

$(\prod_{i\in I} X_i , *)$ חבורה.

סגירות: $(x_i)_{i\in I} * (x_i')_{i\in I} = (x_i \cdot x_i')_{i\in I}$

נייטרלי: $(e_i)_{i\in I}$ e_i נייטרלי של X_i

הפכי ל־ $(x_i)_{i\in I}$ שווה $(x_i^{-1})_{i\in I}$.

דוגמאות: ① $(\mathbb{R},+)^n = (\mathbb{R}^n,+)$

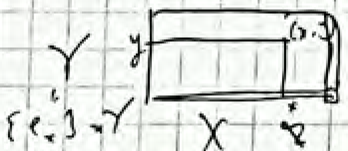
② $(\mathbb{R}^{\mathbb{N}},+)$ חבורה של סדרות עם חיבור רגיל

$$\mathbb{Z}_2^{\mathbb{N}} \underset{\text{חיבור}}{\simeq} \Omega_2 := \{ (x_n)_{n\in\mathbb{N}} \mid x_n \in \{0,1\} \}$$

(פ)

נייטרלי ל־ $X \times Y$ שווה $e_{X\times Y} = e = (e_X, e_Y)$

הטלות:



$$X \times Y \quad \pi_1 \swarrow \quad \searrow \pi_2$$

$\pi_1(x,y)=x \qquad \pi_2(x,y)=y$

באופן דומה

$$x \in \prod_{i\in I} X_i \xrightarrow{\pi_{i_0}} X_{i_0}$$

$$\pi_{i_0}(x) = \pi_{i_0}\left((x_i)_{i\in I} \right) = x_{i_0}$$

Generated by CamScanner from intsig.com

טענה: ההעתקה $\prod X_i \xrightarrow{\pi_{i_0}} X_{i_0}$ היא אפימורפיזם.

גרעין: $\ker \pi_{i_0} = \{ (x_i)_{i\in I} \mid x_{i_0} = e_{i_0} \in X_{i_0} \}$

במקרה של $X \times Y$: $\ker \pi$

תכונה חשובה: $\prod_{i\in I} X_i$ אבלית $\Leftrightarrow$ X_i אבלית.

חלק של ההסבר:

$$X_{i_0} \longrightarrow \prod_{i\in I} X_i$$

$$x \mapsto (x_i)_{i\in I} \quad \begin{cases} x_i = e_i & i \neq i_0 \\ x_{i_0} = x & i = i_0 \end{cases}$$

הערה: אם $\prod X_i$ ציקלית $\Leftarrow$ X_i ציקלית $\forall i$

הסבר: תכונה קודמת ואם תיחשב ציקלי, גם ציקלי.

דוגמא: $\mathbb{Z}_2$ ציקלית אבל $\mathbb{Z}_2 \times \mathbb{Z}_2$ לא ציקלית.

הערה: נוכיח בהמשך $\mathbb{Z}_n \times \mathbb{Z}_m$ ציקלית $\Leftrightarrow$ $(n,m)=1$

תכונה:

$$\begin{cases} X_1 \trianglelefteq X \\ Y_1 \trianglelefteq Y \end{cases} \Rightarrow X_1 \times Y_1 \trianglelefteq X \times Y$$

$$X \times Y / X_1 \times Y_1 \cong X/X_1 \times Y/Y_1$$

הסבר: משפט איזו I.

$$X \times Y \longrightarrow$$

להמשיך!

תוצאה:

$\{e_X\}\times Y \trianglelefteq X\times Y$

$X\times\{e_Y\}\trianglelefteq X\times Y$

$X\times Y/\{e_X\}\times Y\cong X$

~~$X\times Y/X\times\{e_Y\}\cong$~~

$X\times Y/X\times\{e_Y\}\cong Y$

תכונה:

אם $G:=X\times X$ הפונקציה $G\xrightarrow{\varphi}G$

$(x_1,x_2)\mapsto(x_2,x_1)$

חופית מיוחדת רק eeeeeeeeeeeee

היא אוטומורפיזם.

הכלל:

יהי $G:=X\times\cdots\times X=X^n$. לכל תמורה $\sigma\in S_n$ נגדיר את

$G\xrightarrow{\varphi_\sigma}G$: $\varphi_\sigma(x_1,\dots,x_n)=(x_{\sigma(1)},x_{\sigma(2)},\dots,x_{\sigma(n)})$

שימו לב

קיים מונומורפיזם $S_n\hookrightarrow Aut(X^n)$

$\sigma\mapsto\varphi_\sigma$

הגדרה

$\forall i\in I$ $X_i\xrightarrow{f_i}Y_i$ הומומורפיזם, אזי $\prod X_i\xrightarrow{f=\prod_{i\in I}f_i}\prod Y_i$

$(x_i)_{i\in I}\mapsto(f_i(x_i))_{i\in I}$ גם הומומורפיזם (תרגיל)

דוגמאות

① א. הוכח שקיים איזו' $\mathbb{Z}_{15}\times D_3\cong\Omega_{15}\times D_3$

$\mathbb{Z}_{15}\xrightarrow{f_1}\Omega_{15}$

$D_3\xrightarrow{f_2=id}D_3$

2 הוכח $S_3\times\Omega_{25}\cong C_{25}\times D_3$ אם ידוע ש $S_3\cong D_3$

הסבר: איזו' $S_3\xrightarrow{f_1}D_3$, איזו' $\Omega_{25}\xrightarrow{f_2}C_{25}$ (עניין בדיקות מ.שעור הסדר)

$S_3\times\Omega_{25}\xrightarrow{f}C_{25}\times D_3$

$f(x,y)=(f_2(y),f_1(x))$ (הרכבה של 2 איזו')

Generated by CamScanner from intsig.com

② הוכח שקיים אפי' $S_3\times D_{100}\times C_{25}\xrightarrow{f} C_5\times\Omega_2$

קיים אפי'

$C_{25}\xrightarrow{f_1=h_2\circ h_1} C_5$, $C_{25}\xrightarrow{h_1} C_{25}/H \xrightarrow{h_2,\ \cong} C_5$

כאשר $H\le C_{25}$, $|H|=5$

$D_n\xrightarrow{sign}\Omega_2$
סיבובים $a^i\to 1$
שיקופים $a^i\tau\to -1$

$D_{100}\xrightarrow{f_2=\text{"sign"}}\Omega_2=\{1,-1\}$

ו S_3 אפשר לשלוח לאן שבא לי, שולח את הגרעין לטריוויאלי (כולו גרעין)

$$S_3\times D_{100}\times C_{25}\xrightarrow{f} C_5\times\Omega_2$$
$$f(x,y,z)=(f_1(z),\ sign(y))$$

משפט פירוק של חבורות

יהי $(G,\cdot)$ חבורה. התנאים הבאים שקולים:

1. $G\cong X\times Y$.
2. קיימות תת' X,Y (לא בהכ' אבליות) כך ש:

א. $X\trianglelefteq G \wedge Y\trianglelefteq G$

ב. $X\cap Y=\{e_G\}$

ג. $X\cdot Y=G$

הוכחה

$\boxed{1}\Rightarrow\boxed{2}$

א. ראינו בתרגול: $X\cong X\times\{e_Y\}\trianglelefteq X\times Y \wedge Y\cong\{e_X\}\times Y\trianglelefteq X\times Y$

ב. $X\times\{e_Y\}\cap\{e_X\}\times Y=\{(e_X,e_Y)\}=e_{X\times Y}\underset{\text{איזו}}{=}e_G$

ג. יהי $g=(x,y)\in G$, $g=\underset{\in X}{(x,e_Y)}*\underset{\in Y}{(e_X,y)}$

Generated by CamScanner from intsig.com

א ⟸ ב

נוכיח תחילה שמתקיים $xyx^{-1}y^{-1}=e \iff xy=yx \quad \forall x\in X,\ \forall y\in Y$

תזכורת: יהיו $x,y\in G$ מגדירים קומוטטור של (x,y): $[x,y]:=xyx^{-1}y^{-1}\in G$

במקרה $[x,y]=xyx^{-1}y^{-1}=e$

$$xyx^{-1}y^{-1}=(xyx^{-1})y^{-1}\in Y \quad (Y\trianglelefteq G)$$

$$xyx^{-1}y^{-1}=x(yx^{-1}y^{-1})\in X \quad (X\trianglelefteq G)$$

דהיינו $[x,y]\in X\cap Y \overset{(2)}{=} \{e\}$

(*) הוכחנו $xy=yx \quad \forall x\in X,\ y\in Y$

נגדיר

$$X\times Y \xrightarrow{\varphi} G$$

$$(x,y)\mapsto x\cdot y$$

② ⟸ φ על

נוכיח φ הומ':

$$\varphi((x_1,y_1)*(x_2,y_2))=\varphi(x_1x_2,\ y_1y_2)=(x_1x_2)(y_1y_2)=x_1x_2y_1y_2$$

$$\varphi(x_1,y_1)\cdot\varphi(x_2,y_2)=(x_1y_1)(x_2y_2)=x_1(y_1x_2)y_2 \overset{(*)}{=} x_1x_2y_1y_2$$

✓

נותר, מספיק להוכיח שהגרעין הוא טריוויאלי:

$$\ker\varphi=\{(x,y)\in X\times Y:\varphi(x,y)=e\}=\{(x,y)\in X\times Y: xy=e\}$$

$$=\{\ \ : x=y^{-1}\}=\{\ \ : x=y=e\}$$

(האיבר היחיד בחיתוך הוא e)

$$=\{(e,e)\}=\{e_{X\times Y}\}$$

Generated by CamScanner from intsig.com

משפט (קריטריון לציקליות של המכפלה)

התנאים שקולים:

1. $C_m \times C_n$ ציקלית (ולכן איזומורפית ל-C_{mn})

2. $(m,n)=1$

הוכחה

1 ⇐ 2

אם נניח בשלילה ש- $(m,n)=d>1$ נוכיח שלכל איבר $g \in C_m \times C_n$

מתקיים $O(g) < mn$

$g=(x,y) \in C_m \times C_n$

$x \in C_m \Rightarrow O(x) | m$

$y \in C_n \Rightarrow O(y) | n$

$$g^{\frac{mn}{d}} = (x,y)^{\frac{mn}{d}} = ((x,e)\cdot(e,y))^{\frac{mn}{d}}$$

$$= \left(x^{\frac{mn}{d}}, y^{\frac{mn}{d}}\right) = \left((x^m)^{\frac{n}{d}}, (y^n)^{\frac{m}{d}}\right) = (e,e) = e$$

מכאן $O(g) \leq \frac{mn}{d} < mn$

2 ⇒ 1

נשתמש במשפט הפירוק עבור חבורה $G=C_{mn}$

C_{mn} ציקלית עם mn איברים.

לפי משפט ניון תת-חבורה ציקלית יש תת $X \leq C_{mn}$ עם m איברים

$Y \leq C_{mn}$ עם n איברים

נראה כי מתקיימים התנאים א,ב,ג במשפט הפירוק:

א. ברור כי $\left\{ \begin{array}{l} X \trianglelefteq C_{mn} \\ Y \trianglelefteq C_{mn} \end{array} \right.$ כי C_{mn} אבלית (ציקלית)

ב. $X \cap Y = \{e\}$ כי

$X \cap Y \leq X \Rightarrow |X \cap Y| \,\big|\, |X|=m$

$X \cap Y \leq Y \Rightarrow |X \cap Y| \,\big|\, |Y|=n$ (לגרנז')

כיון כי $(m,n)=1$ ולכן $|X \cap Y|=1 \Rightarrow X \cap Y = \{e\}$

↑

$X \cap Y$ תת חבורה ולכן $e \in X \cap Y$

ג. $X \cdot Y = C_{mn}$ ⟸

נניח a היוצר של C_{mn} בגלל $X \cdot Y \subseteq C_{mn}$, כי אלו תת"ח.

נותר להוכיח $C_{mn} \subseteq X \cdot Y$, שקול להוכיח $a \in X \cdot Y$:

$$a^n \in X = \langle a^n \rangle$$

מש"ל $O(X) = m = O(a^n)$

$$a^m \in Y = \langle a^m \rangle$$

לפי משפט אוקלידס קיימים $u, v \in \mathbb{Z}$ כך ש

$$u \cdot m + v \cdot n = 1 \longleftarrow 1 = (m, n)$$

$$a = a^1 = a^{um+vn} = \ldots$$

$$= a^{vn+um} = \underbrace{(a^n)^v}_{\in X} \cdot \underbrace{(a^m)^u}_{\in Y} \in X \cdot Y \quad \checkmark$$

מש"ל

-הפסקה-

<u>תוצאה:</u> $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn} \Leftrightarrow (m,n) = 1$.

מכאן לכל $(m,n) = 1$

$$\begin{cases} x \equiv a_1 \mod m \\ x \equiv a_2 \mod n \end{cases}$$ המערכת פתירה

<u>הפתרון:</u> $x = a_1(vn) + a_2(um)$ כאשר $un + vm = 1$

<u>הכללה:</u> "משפט השאריות הסיני" (מופשטת 2)

נתון $(m_i, m_j) = 1$ לכל $i \neq j$

אז המערכת

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \vdots \\ x \equiv a_t \mod m_t \end{cases}$$ היא פתירה.

והפתרון מודולו $m = m_1 m_2 \cdots m_t$ הוא יחיד.

<u>הכללה:</u> $\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_t}$ $\quad (m_i, m_j) = 1$

$$[k] \mapsto ([k]_{m_1}, [k]_{m_2}, \ldots, [k]_{m_t}) \qquad m = \prod_{i=1}^{t} m_i$$

Generated by CamScanner from intsig.com

מיון חבורות אבליות (סופיות):

משפט ① כל חבורה אבלית סופית ≅ מכפלה (סופית) של חבורות ציקליות (סופיות)

② כל G חבורה אבלית נ"ס ≅ מכפלה סופית של חבורות ציקליות.

דוג':

$$\mathbb{Z}_{40}\times\mathbb{Z}\times\mathbb{Z}_{32}\times\mathbb{Z}_{7^8}\times\mathbb{Z}_{125}\times\mathbb{Z}$$

③ G חבורה אבלית נ"ס היא תמונה אפימורפית של $\mathbb{Z}^n$.

הערה: אפשר להוכיח דרך משפט האיזו' I (לבדוק!) .

שאלה: כמה חבורות אבליות קיימות (עד כדי ≅) עם n איברים? ואיך נדע לבנות אותן?

דוגמאות: G אבלית. $|G|=n$

א) $n=p$ ראשוני. $G\cong C_p$ (מסקנה מ-Lagrange) אז אחת! (עד כדי ≅).

ב) $n=p^2$.

C_{p^2} → $2=2$

$C_p\times C_p$ → $2=1+1$

2 חבורות. (עד כדי ≅)

ג) $n=p^3$

C_{p^3} → $3=3$

$C_{p^2}\times C_p$ → $3=2+1$

$C_p\times C_p\times C_p$ → $3=1+1+1$

3 קב'.

ד) $n=p^5$

C_{p^5}

$5=5$

$5=4+1$

$5=3+1+1$

$5=2+2+1$

$5=2+1+1+1$

$5=1+1+1+1+1$

$p(5)=7$

לכל, מס' חלוקות

$$m_1\geq m_2\geq\dots\geq m_t\geq 1$$

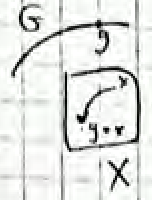
$$m=m_1+\dots+m_t$$

[illegible]

<u>הגדרה:</u> פעולה (action) של חבורה G על קבוצה $X \neq \phi$ היא פונקציה

$$G \times X \xrightarrow{\alpha} X$$

$$(g, x) \mapsto g * x = \alpha(g, x)$$



כך שמתקיים:

$\forall x \in X \quad e * x = x$ [A_1]

$g_1 * (g_2 * x) = (g_1 g_2) * x$ [A_2]

אז אומרים: X הוא G-מרחב (G-space) (G, X, α) או (G, X)

<u>הערה:</u> במקרה של α <u>רציפה</u> עם G, X <u>מרחבים טופולוגיים</u> אז (קב) הגדרה של <u>מערכת דינמית מופשטת</u>.

<u>הגדרות נוספות:</u>

נניח $\alpha: G \times X \to X$ פעולה.

א) <u>מסלול</u> (orbit) של נקודה $x \in X$ הוא $G * x$ $= \{y \in X \mid y = g * x \ \exists g \in G\} =: [x]$

ב) אומרים פעולה טרנזיטיבית (המואגית) אם קיים רק מסלול אחד.

ג) אומרים ש-$x \in X$ הוא נקודת שבת של G אם $[x] = \{x\}$.

(שקול: $g * x = x \quad \forall g \in G$).

ד) <u>מייצב</u> (stabilizer) של x:

$$Stb(x) = G_x := \{g \in G \mid g * x = x\} \leq G$$

St_x לבדוק

ה) "נקודת שבת של g" (כאן $g \in G$ קבוע)

$$X_g := \{x \in X \mid g * x = x\}$$

<u>למשל:</u>

$$X_e = X$$

$$X_{g^{-1}} = X_g$$

Fixed Point $F := \{ \text{נקודות שבת של } G \} = \bigcap_{g \in G} X_g$

<u>הערה 1:</u> באופן דומה מגדירים פעולה מימין $X \times G \to X$.

(זה חשוב בפעולות מעל פונקציות).

ב) מגדירים גם פעולה של מונואיד (אגודה) אז מתקיים רק [A_2].

Generated by CamScanner from intsig.com

דוגמאות:

1. נניח $(G,\cdot)$ חבורה.

נגדיר פעולה של G על $X:=G$.

ימנית: $G\times G\to G$, $(x,g)\mapsto x\cdot g$

שמאלית: $G\times G\to G$, $(g,x)\mapsto g\cdot x$ (לבדוק!!)

2. נניח $H\leq G$. אז מגדירים פעולה (שמאלית)

$$G\times G/H \to G/H$$

$$(g, tH)\mapsto (gt)H = g(tH)$$

$$X:=G/H = \{tH\}_{t\in G}$$

קוסטים שמאליים

שימו ♥

א. (2) הכללה של (1) $(H=\{e\})$

ב. הפעולה ב-(2) (ולכן גם ב-(1)) טרנזיטיבית. לכל $tH\in G/H$: $t*H=tH$.

ג. $F=\emptyset \iff H\neq G$

אם $G=H$ אז $G\times G/G\to G/G$

$G/G=\{tG\}_{t\in G}=\{G\}$ נקודה אחת! והיא נקודת שבת.

3. **הצמדות:**

לכל חבורה G ניקח $X:=G$ ונגדיר: $G\times G\to G$

$$(g,x)\mapsto g*x := gxg^{-1}\ (\in G)$$

A_1: $e*x = exe^{-1} = x$

A_2: $g_1*(g_2*x) = g_1(g_2xg_2^{-1})g_1^{-1} = (g_1g_2)*x$ ✓

כאן נקודות שבת = המרכז של G:

$$F=\{x\in G \mid \forall g\in G: g*x=x\} = \{x\in G\mid \forall g\in G: gxg^{-1}=x\} =$$

$$=\{x\in G\mid gx=xg\ \forall g\in G\} = Z(G)\ \ (=C(G))$$

מסקנה: פעולת הצמדה G על G ($G\times G\to G$) היא טריוויאלית (היא מעבירה כל איבר לעצמו) אמ"מ G אבלית.

במקרה הפרטי של $G=S_n$:

א = מס' מסלולים (= מס' מחלקות צמידות ב-S_n) שווה $p(n)=k$.

לדוגמה: $n=5$, $p(5)=7$.

ההסבר: בניסוח של הצמדות ב-S_n: $g(i_1,i_2,\dots,i_n)g^{-1}=(g(i_1),\dots,g(i_n))$

הטיפוס נשמר.

חשוב: תמיד קיים $g\in S_n$ כך שאפשר להגיע לכל האיברים באותו טיפוס.

$x=(1\ 2\ 3\ 4\ 5)$

$[x]=\{(i_1,i_2,i_3,i_4,i_5)\}$

לדוגמה: $y=(3\ 5\ 1\ 4\ 2)$ (צמוד ל-x)

ניקח $g=\begin{pmatrix}1&2&3&4&5\\3&5&1&4&2\end{pmatrix}$ אז $gxg^{-1}=y$ לפי הנוסחה.

טיפוס מורכב: $(i_1\ i_2\ i_3)(i_4\ i_5)=(3\ 2\ 5)(1\ 4)$

לכן מס' מחלקות צמידות = מס' טיפוסים מורכבים

$5=5$

$5=4+1$

$\vdots$

$5=3+2$

$\vdots$

$5=1+1+1+1+1$

הצמדות בתת"ח:

לכל חבורה G (סופית) $Sub(G):=\{H\le G\}$ תת"ח ב-G ($G\in$, $e\in$)

$X:=Sub(G)$

$G\times Sub(G)\to Sub(G)$

$(g,H)\mapsto gHg^{-1}$ $\quad gHg^{-1}=\{ghg^{-1}\mid h\in H\}$

הצמדה ואוטומורפיזם → מעבירה תת"ח לתת"ח

A_1

A_2

שימו לב: בפעולה הנ"ל $F=\{H\le G\mid H\trianglelefteq G\}$

נקודות שבת הן תת"ח נורמליות ב-G.

Generated by CamScanner from intsig.com

5) נניח $G \times X \xrightarrow{\alpha} X$ פעולה. (נגדיר)

$$G \times P(X) \xrightarrow{\alpha'} P(X)$$

$$(g, A) \mapsto g * A := \{g * a \mid a \in A\}$$

$\boxed{A_1}$ $\hat{\;}$

$\boxed{A_2}$

6) **דוגמא מפתח**

נניח X קבוצה לא ריקה, $G = S_X$ חבורה סימטרית.

(מגדירים **פעולה טבעית**:)

$$S_X \times X \to X$$

$$(g, x) \mapsto g * x = g(x)$$

$\boxed{A_1}$ Δ

$\boxed{A_2}$

הערה: אם $G \times X \xrightarrow{\alpha} X$ פעולה, ו- $H \leq G$ אז אפשר להגדיר את הצמצום של הפעולה: $H \times X \to X$ גם פעולה

$$(h, x) \mapsto h * x = \alpha(h, x)$$

למשל: אם $G \leq S_X$ אז מוגדרת $G \times X \to X$

$$(g, x) \mapsto g(x)$$

הערה: כל פעולה $G \times X \to X$ היא בעצם פעולה שבאה דרך צמצום של דוגמה מפתח $S_X \times X \to X$

הסבר: (דומה למשפט קיילי): נגדיר "הצגה": $\alpha_g : X \to X \in S_X$

$$x \mapsto g * x$$

כי $\boxed{\alpha_g^{-1} = \alpha_{g^{-1}}}$

אז נגדיר (הומומורפיזם קיילי) $G \xrightarrow{\varphi} S_X$ הומומורפיזם

$$g \mapsto \alpha_g$$

לא תמיד מונומורפיזם.

הערה לסעיף ה: דרך $S_X \times X \to X$

$$G \times X \to X$$

$$(g, x) \mapsto \varphi(g)(x)$$

Generated by CamScanner from intsig.com

<u>דוגמא:</u> $X = \{1,2,3,4,5,6\}$

$G = \langle (1,2), (3,4,5) \rangle \leq S_6$ עם פעולה טבעית

<u>למצוא:</u> מסלולים, G_x, X_g, F

<u>פתרון:</u>

$|G| = 6$

$$G = \left\{ \begin{matrix} e, & (3,4,5) = a, & (3,5,4) = a^2 \\ \tau^2 = (1,2) & \tau a, & \tau a^2 \end{matrix} \right\} \leq S_6$$

<u>מסלולים:</u> $[x] = \{g * x\}_{g \in G}$

k = מסלולים 3

- $(\cdot 1 \; \cdot 2) = [1] = \{1,2\} = [2]$
- $(\cdot 3 \; \cdot 4 \; \cdot 5) = [3] = \{3,4,5\} = [4] = [5]$
- $(\cdot 6) = \{6\}$

(א) $G_x := \{g \in G \mid g * x = x\}$

$x \in X$	$G_x \leq G$	$\lvert G_x \rvert$
1	$\langle a \rangle = \{e, a, a^2\}$	3
2	$\langle a \rangle$	3
3	$\langle \tau \rangle = \{e, \tau\}$	2
4	$\langle \tau \rangle$	2
5	$\langle \tau \rangle$	2
6	G	6

<u>מבחן:</u> [18]

(ב) $X_g := \{x \in X \mid g * x = x\} \subseteq X$

$g \in G$	X_g	$\lvert X_g \rvert$
e	X	6
a	$\{1,2,6\}$	3
a^2	$\{1,2,6\}$	3
τ	$\{3,4,5,6\}$	4
τa	$\{6\}$	1
τa^2	$\{6\}$	1

(18) מ.ש.ל

Generated by CamScanner from intsig.com

הערה: קיבלנו
$$\begin{cases}\sum_{x\in X}|G_x|=18\\ \sum_{g\in G}|X_g|=18\end{cases}$$

(נכון באופן כללי): $\sum|G_x| = \sum|X_g|$

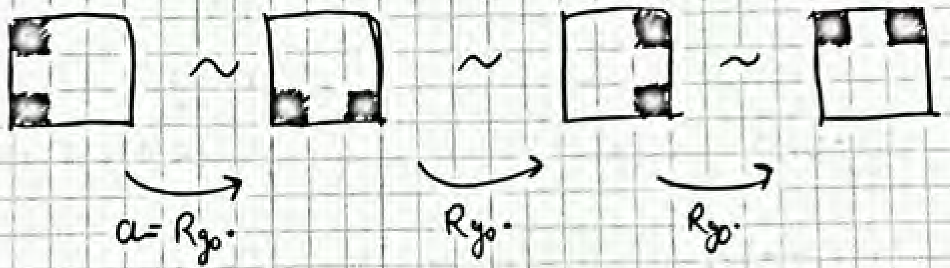
משפט Burnside (הוכחה בהמשך):
$$k=\frac{1}{|G|}\sum_{g\in G}|X_g|$$
(k ← מס' מסלולים)

בדוגמה: $k=\frac{1}{6}\cdot 18=③$

שאלה קומבינטורית:

"דוגמה של הלוחות":

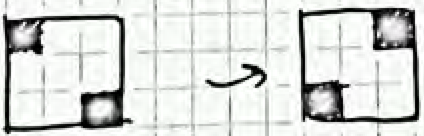
כמה לוחות 3x3 קיימים (עד כדי סיבובים) אם מותר לצבוע ב-2 צבעים קבועים (B,W)



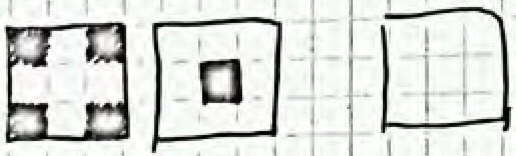
אורך המסלול שווה ל-4.

בחבורה $G=C_4$ יש 4 אלמנטים.

דוגמה למסלול מאורך 2:



דוגמאות למסלול מאורך 1 (נק' שבת):



בניית המודל: קודם פעולה כאשר $G=C_4$, 4 אלמנטים

$$X=\{\underbrace{1,2,3,4,5,6,7,8,9}_{Y}\to\{B,W\}\}$$

הרעיון:

1	2	3
4	5	6
7	8	9

$\downarrow$ $\{B,W\}$

$|X|=2^9$.

השלב הראשון:

Generated by CamScanner from intsig.com

דוגמה חשובה: יש פעולה טבעית

$G \times Y \to Y$

$(g, y) \mapsto g * y$

$\langle a \rangle = G = \{e, a, a^2, a^3\}$ $\boxed{e * y = y}$

$a = R_{90^\circ}$

[illegible]

$R_{90^\circ} = a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 1 & 8 & 5 & 2 & 9 & 6 & 3 \end{pmatrix}$ – [illegible]

$R_{180^\circ} = a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} = (1\,9)(2\,8)(3\,7)(4\,6)$

$R_{270^\circ} = a^{-1} = a^3 = \begin{pmatrix} \quad \end{pmatrix} = (3\,9\,7\,1)(6\,8\,4\,2)$

פעולה: $G \times Y \to Y$ מגדירה [illegible] פעולה

$X \times G \to X$

$(f, g) \mapsto f * g$

כאשר $f * g$ מוגדר ע"י $(f * g)(y) = f(g(y))$

$\forall y \in Y$

$f * e = f$ $\boxed{A}$ ✓

$(f * g_2) * g_1 = f * (g_2 g_1)$ $\boxed{B}$ ✓

[illegible]

$k = \frac{1}{|G|} \cdot \sum_{g \in G} |X_g| = \frac{(2^9 + 2^3 \cdot 2 + 2^5)}{4} = 140$

$g \in G$	X_g	$\lvert X_g \rvert$
e	$X_e = X$	2^9
a		2^3
a^2		2^5
$a^{-1} = a^3$	$X_{g^{-1}} = X_g$	2^3

Generated by CamScanner from intsig.com

שאלה: לפתור שאלה דומה עם לוח 4×4 ב-3 צבעים לצבעי פאות חבור – D_4.
(ציון סיבובים ושיקופים).

תכונות בסיסיות של פעולות

תהי $G\times X\xrightarrow{\alpha}X$ פעולה

① $X=\bigcup_{x\in X}[x]$ (איחוד זר של המסלולים)

הסבר: נגדיר יחס שקילות ב-X

$x\sim y \overset{def}{\iff} y=g*x$, $\exists g\in G$

($x \xrightarrow{\exists g} y$)

לבדוק שהיחס הוא יחס שקילות. ∎

② $G_x\le G$. הסבר: ∎

③ $g*x=y \Rightarrow gG_xg^{-1}=G_y$

הסבר: נניח $h\in G_x$.

צ"ל: $ghg^{-1}\in G_y$ (ואז נקבל $\subseteq$)

$$(ghg^{-1})*y \underset{A_2}{=} (gh)*(g^{-1}*y) = (gh)*x \underset{A_2}{=} g*(h*x) \underset{h\in G_x}{=} g*x=y$$

(נתון $g*x=y$, $x=g^{-1}*y$)

לכן $ghg^{-1}\in G_y$. אז הוכחנו $gG_xg^{-1}\subseteq G_y$.

באופן דומה אפשר להוכיח $\supseteq$.

משל.

④ $g*x=y$ (כלומר $x\sim y$) $\Rightarrow |G_x|=|G_y|$

⑤ $X_e=X$, $X_{g^{-1}}=X_g$

⑥ $\forall g_1,g_2\in G$ $\quad g_1\equiv g_2 \bmod G_x \iff g_1*x=g_2*x$

$\Updownarrow$ ← לבדוק

$g_1^{-1}g_2\in G_x$

הסבר:

הסבר:

$$g_1 * x = g_2 * x$$

⇕

$$g_1^{-1} * (g_1 * x) = g_1^{-1} * (g_2 * x)$$

⇕

$$(g_1^{-1} g_1) * x = (g_1^{-1} g_2) * x$$

⇕

$$x = (g_1^{-1} g_2) * x$$

⇕

$$g_1^{-1} g_2 \in G_x$$

⇕

$$g_1 \equiv g_2 \mod G_x$$

משל

הגדרה: נניח

$$G * X_1 \xrightarrow{*_1} X_1$$

פעולות

$$G * X_2 \xrightarrow{*_2} X_2$$

פונקציה $X_1 \xrightarrow{f} X_2$ נקראת הומומורפיזם של פעולות (או של G-מרחבים) אם

$$\boxed{f(g * x) = g * f(x)}$$

$\forall g \in G$

$\forall x \in X_1$

$$\begin{array}{ccc} G \times X_1 & \longrightarrow & X_1 \\ f \downarrow & & \downarrow f \\ G \times X_2 & \longrightarrow & X_2 \end{array}$$

אומרים ש-f <u>איזומורפיזם</u> אם f הומו' <u>אחד-על</u>.

$$\begin{array}{ccc} G \times X_1 & \longrightarrow & X_1 \\ \updownarrow & & \updownarrow \\ G \times X_2 & \longrightarrow & X_2 \end{array}$$

⑦ <u>משפט (מיון פעולות טרנזיטיביות):</u>

כל פעולה $G * X \to X$ עם מסלול 1 הוא איזומורפית לפעולה $G * G/H \to G/H$ כאשר $H := G_x$ (אם נבחר $x \in X$).

<u>הוכחה:</u> $y = g * x$

$X \ni x$ נבחר

$G/G_x \ni G_x$ ... gG_x ~ (נגדיר f איזו')

$$X = [x] = \{g * x\}_{g \in G}$$

(נגדיר

$$f: X \to G/G_x$$

$$y = g * x \mapsto gG_x$$

מוגדר היטב כי

(6) $$\boxed{g_1 \equiv g_2 \bmod G_x \iff y = g_1 * x = g_2 * x}$$

$\Downarrow$

$$g_1 G_x = g_2 G_x$$

Afit Marzouki

$\oplus C = L_2(R)$

Dana Vaknin red 22

<u>יחחי"ע:</u> לעבר שוב מאותה תבונה (6)

<u>על:</u> לכל $gG_x \in G/G_x$ ניקח $X \ni y := g * x$

$$f(y) = gG_x$$

<u>הומומורפיזם:</u> די"ל: "f שומרת על הפעולה"

צ"ל:

$$\boxed{f(t * y) = t * f(y)}$$

$\forall t \in G$
$\forall y \in X$

$$f(t*y) = f(t*(g*x)) = f((tg)*x) = (tg)G_x$$

$$t*f(y) = t*f(g*x) = t*gG_x = t(gG_x)$$

מש"ל

(8) <u>משפט:</u> לכל חבורה סופית G ופעולה של G מעל X מתקיים:

$$\boxed{|G| = |[x]| \cdot |G_x|}$$

מכאן <u>מסקנה:</u> $|[x]| \mid |G|$

<u>הסבר של ל:</u> אם $G * X \to X$ פעולה, $x \in X$ אז נסתכל על הפעולה המצומצמת

$G * [x] \to [x]$ מעבר!

לפי המשפט הקודם:

$$\begin{matrix} G * [x] \to [x] \\ \updownarrow \quad\quad \updownarrow \\ G * G/G_x \to G/G_x \end{matrix} \quad \cong$$

ולכן $|[x]| = |G/G_x|$

לגרנז' $\parallel$

$$\frac{|G|}{|G_x|}$$

$$|G| = |[x]| \cdot |G_x|$$

מש"ל

9) **משפט:** (נוסחת המחלקות)

לכל פעולה $G \times X \to X$ מתקיים:

$$|X| = \sum_{i=1}^{n} [G : G_{x_i}]$$

$x_1, x_2, \dots, x_n$ נציגים של מסלולים

הוכחה: לפי 1) $X = \bigcup_{x \in X} [x]$ אם $x_1, \dots, x_n$ נציגים של המסלול

מצב של זה $|X| = |[x_1]| + |[x_2]| + \dots + |[x_n]| = \sum_{i=1}^{n} |[x_i]|$ לפי 8):

$\Leftarrow$ $|[x_i]| = [G : G_{x_i}]$

מכיוון $\Leftarrow$ $|X| = \sum_{i=1}^{n} [G : G_{x_i}]$.

מש"ל

שאלה: כמה איברים מתחלפים עם $a = (5\ 2\ 3)$ בחבורה S_5?

10) לכל חבורה סופית G מתקיים:

$$|G| = |Z(G)| + \sum_{j=1}^{m} [G : C_{x_j}]$$

כאשר $x_1, \dots, x_m$ נציגים של מחלקות צמידות ב-G, כך ש- $x_j \notin Z(G)$.

הגדרה: צנטרליזטור של $x \in G$

$$C_x := \{g \in G \mid gx = xg\} \quad \text{(אקספליציט)}$$

= המייצב של x לגבי פעולת ההצמדה $G \times G \to G$.

הסבר של הנוסחה:

$$|G| = |C(G)| + \sum_{j=1}^{m} |[x_j]| \underset{8}{=} |C(G)| + \sum_{j=1}^{m} [G : C_{x_j}]$$

(מעל $C(G)$: מסלולים נקודתיים ב-G)

11) **מסקנה:** אם $|G| = p^n$, כאשר p ראשוני, אז המרכז חבורה לא טריוויאלית (כלומר $|Z(G)| \neq 1$)

הסבר: מ-10)

$$|G| = |C(G)| + \sum_{j=1}^{m} [G : C_{x_j}]$$

$[G : C_{x_j}]$ מתחלק ב-p (p מתחלק לכל אחד), $|G|$ מתחלק ב-p, לכן גם $|C(G)|$ מתחלק ב-p, ולכן שונה מ-1.

24/08/2011

VIII

שיעור השלמה ב-88 9:00

שאלה: כמה איברים מתחלפים עם התמורה $(5,2,3)$ ב-S_7?

פתרון: $\{g\in G \mid ga=ag\} = \{g\in G \mid gag^{-1}=a\} =: C_a = G_a$

(מיצב)

$G=S_7$ פועלת על עצמה דרך הצמדות

נוסחה:
$$|G_a| = \frac{|G|}{|[a]|}$$

$$\Downarrow$$

$$|C_a| = \frac{|S_7|}{|[(5,2,3)]|} = \frac{7!}{?}$$

$$[(5,2,3)] = \{(i,j,k) \mid i,j,k\in\{1,\dots,7\}\} = \binom{7}{3}\cdot\frac{3!}{3} =$$

המסלול = מחלקות צמדות

$= (i,j,k)=(k,i,j)=(j,k,i) =$ מס' מעגלים מאורך 3 ב-S_7 =

התשובה:
$$|C_a| = \frac{7!}{\binom{7}{3}\cdot\frac{3!}{3}}$$

טענה 1: נניח G חבורת-p. (כלו' $|G|=p^n$ $n\in\mathbb{N}$).

נניח $G\cdot X\to X$ פעולה. אז תמיד מתקיים:

X^G $|F| \equiv |X| \bmod p$.

הוכחה: $X = \bigcup_{x\in X}[x] = \dot{\bigcup}_{i=1}^{k}[x_i]$.

$x_1,\dots,x_k$ נציגים של מסלולים.

$$|X| = \sum_{i=1}^{k}|[x_i]|$$

$$|X| = |F| + \sum_{j=1}^{m}|[x_j]| = |F| + \sum_{j=1}^{m}[G:G_{x_j}] \qquad (|[x_j]|>1)$$

$$[G:G_{x_j}] \equiv 0 \bmod p \quad \Leftarrow \quad \begin{cases} ([G:G_{x_j}]>1) \\ [G:G_{x_j}] \mid |G| = p^n \end{cases}$$

$$\Downarrow$$

$$|F| \equiv |X| \bmod p$$

מסקנה: לכל $|G|=p^n$ (p ראשוני, $n\in\mathbb{N}$) $\Rightarrow$ $p \mid |C(G)|$ (ולכן $|C(G)|>1$)

טענה 2: נניח G חבורת-p, $G \times X \to X$ פעולה, $p \nmid |X|$

אזי יש נקודת שבת. (שקול: $F \neq \phi$).

הוכחה: מטענה 1

$$\begin{cases} |F| \equiv |X| \mod p \\ p \nmid |X| \iff |X| \not\equiv 0 \mod p \end{cases}$$

$$\Downarrow$$

$$|F| \not\equiv 0 \mod p$$

$$\Downarrow$$

$$|F| > 0$$

מש"ל

משפטי סילו (Sylow)

הגדרות:

א) G חבורת-p $\overset{def}{=}$ $|G| = p^n$, p ראשוני, $n \in \mathbb{N}$.

ב) $H \leq G$ נקראת תת-p אם H היא חבורת-p. (על G אין הגבלות)

ג) אומרים ש-$H \leq G$ היא תת-p-סילו $\overset{def}{=}$ ① $|H| = p^n$ תת-p. ② $|G| = p^n \cdot m$ ($m \in \mathbb{N}$) כך ש $(p, m) = 1$

ד) **שקול:** אם $H \leq K \leq G$ (H תת-p סילו, K תת-p) וגם K תת-p ⟸ $H = K$.
(תת-p-סילו = מקס' תת-p)

הערה: יתכן שיש כמה תתי-p-סילו. נוכיח שתמיד קיימת תת-p-סילו לכל ראשוני שמחלק את $|G|$.

דוגמאות:

[1] $G = C_{25} \times C_8 \times C_5$ (אבלית) $|G| = 25 \cdot 8 \cdot 5 = 1{,}000$.

א. $p=2$: $P_2 = \{e\} \times C_8 \times \{e\}$ תת-2-סילו. $m = 5^3$

ב. $p=5$: $P_5 = C_{25} \times \{e\} \times C_5$ $m = 2^3$

הערה: בחבורה אבלית תת-p-סילו הן תמיד יחידות. לה נובע ממשפט II סילו.

[2] $G = D_3$, $|G| = 6 = 2 \cdot 3$

א. $p=3$: $P_3 = C_3 \lhd D_3$ יחידה! $m=2$. $Syl_3(G) = \{C_3\}$

לידיעה: ממשפטי סילו נובע שתת-p-סילו $H \leq G$ היא יחידה $\iff$ $H \lhd G$

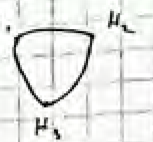
ב. $p=2$: מה לגבי תתי עם 2 איברים? $m=3$

p-חבורה = מספר איברים חזקה של p.

$H_1 = \{e, \tau\}$

$H_2 = \{e, \tau\sigma\}$

$H_3 = \{e, \tau\sigma^2\}$



יזכיר $\boxed{n_p | m}$

$Syl_2(G) = \{H_1, H_2, H_3\}$

כמון זוג.

משפט המיון של חבורות אבליות סופיות

נניח G חבורה אבלית סופית $|G| = p_1^{k_1} \cdots p_m^{k_m}$ (לפי גורמים ראשוניים שונים) $k_1, \dots, k_m \in \mathbb{N}$

אזי G מתפרקת $G \simeq P_1 \times \dots \times P_m$ כך ש- $|P_i| = p_i^{k_i}$ (Hurzeu...)

<u>הוכחה:</u> תהי $(G, +)$ חיבורית.

<u>טענת עזר I:</u> נניח G אבלית: $|G| = m_1 m_2$ ו- $(m_1, m_2) = 1$

אזי

$G_{m_2} = m_1 G$

$G_{m_1} = m_2 G$

כאשר $mG := \{mx \mid x \in G\}$ (נסמן) $m \in \mathbb{N}$

$G_m = \{x \in G \mid o(x) | m\}$

<u>הוכחת טענה I:</u> נראה $G_{m_2} = m_1 G$

$(\subseteq)$: נניח $x \in G_{m_2}$, נוכיח $x \in m_1 G$

$(m_1, m_2) = 1$

$\Downarrow$

$\exists u, v \in \mathbb{Z} : u \cdot m_1 + v \cdot m_2 = 1$

$x = 1 \cdot x = (u \cdot m_1 + v \cdot m_2) x = (u \cdot m_1) x + (v \cdot m_2) x = (u m_1) x + 0_G = (u m_1) x =$

$= m_1 (u x) \in m_1 G$

($x \in G_{m_2} \Rightarrow m_2 x = 0_G$)

מכאן $x \in m_1 G$.

$(\supseteq)$: נניח $x \in m_1 G$ נוכיח $x \in G_{m_2}$

$\Downarrow$

$\begin{cases} x = m_1 y \\ y \in G \end{cases}$

$m_2 \cdot x = m_2 \cdot m_1 \cdot y = |G| \cdot y = 0_G$

$m_2 x = 0_G$

$\Downarrow$

$o(x) | m_2$

$\Downarrow$

$x \in G_{m_2}$.

מש"ל

טענת עזר II: נניח G חבורה אבלית סופית $|G|=m_1m_2$ ו $(m_1,m_2)=1$

אזי $\boxed{G \cong m_1G \oplus m_2G}$

סכום ישר (מקרה פרטי של משפט [illegible] — של חבורות)

$X = Y_1 \oplus Y_2$
$(y_1,y_2)+(y_1',y_2')$

לפי משפט פירוק חבורות שקול להוכיח ש

1. $m_2G \trianglelefteq G \ , \ m_1G \trianglelefteq G$
2. $m_1G \cap m_2G = \{0_G\}$
3. $m_1G + m_2G = G$

הוכחה: 1 ברור כי G אבלית. $mG \leq G$ תמיד! (חשוב אבלית) $\Rightarrow mG \trianglelefteq G$

2 נניח $x \in m_1G \cap m_2G$. צ"ל $x = 0_G$

ניקח $\begin{cases} x\in m_1G \\ x\in m_2G \end{cases} \Rightarrow \begin{cases} o(x) \mid m_2 \\ o(x) \mid m_1 \end{cases} \Rightarrow o(x) \mid (m_1,m_2) \Rightarrow o(x) \mid 1 \Rightarrow o(x)=1$

$\Downarrow$

$x = 0_G$

הוכחנו 2. //

נוכיח 3: $G = m_1G + m_2G$.

נניח $x\in G$. צ"ל $x \in m_1G+m_2G$.

$(m_1,m_2)=1 \Rightarrow \exists\, u,v\in\mathbb{Z} : um_1+vm_2=1$

$$x = 1\cdot x = (um_1+vm_2)x = \underbrace{m_1(ux)}_{\in m_1G} + \underbrace{m_2(vx)}_{\in m_2G}$$

הוכחנו 3.

טענה 1 + טענה 2 + אינדוקציה $\Rightarrow$ **משפט**.

טענה: לכל (הפסקה) חבורה אבלית G ולכל p ראשוני שמחלק את $|G|$

קיים $a\in G$ כך ש- $o(a)=p$.

הוכחה: שקול להוכיח שקיימת ת"ח עם p איברים.

נראה שקיימת ת"ח-p שהיא ציקלית.

(כי אם $|H|=p^k$, $k\in\mathbb{N}$ ו H ציקלית $\Leftarrow$ קיימת ת"ח $K\le H$ עם $|K|=p$ (משפט מיון ת"ח))

נראה שקיימת ת"ח-p $X\le G$, $|X|=p^k>1$. ניקח $x\in X$ לא ניטרלי;

אזי: $\underset{p^i,\ i\in\mathbb{N}}{H := \langle x\rangle} \le \underset{p^k}{X} \le G$ ת"ח-p ציקלית.

Generated by CamScanner from intsig.com

ו-$|G|$ם, לכן לפי משפט הפירוק (הקודם) $G \simeq P \times Q$

כאשר $|P| = p^k$ מקס' חבורת p שהיא באופן טבעי משוכנת לתוך G.

$X := P \times \{e\} \le G$ חבורת-p.

מצאנו!

<u>משל</u>.

<u>הערה:</u> בהמשך נוכיח שאפשר להחריג אבליות של G ואז נקבל משפט Cauchy (קושי).

<u>משפט:</u> לכל G חבורת-p כך ש $|G| = p^n$ מתקיים:

① קיימת תת"ח נורמלית $H \trianglelefteq G$ עם p^{n-1} איברים

② לכל $1 \le i \le n$ קיימת תת"ח $K \le G$ עם $|K| = p^i$.

<u>הוכחה:</u>

② נובע מ-① בקלות: $G \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \dots \trianglerighteq H_{n-1}$

$p^n \quad p^{n-1} \quad p^{n-2} \quad \dots \quad p$

<u>הוכחה של ①:</u> <u>באינדוקציה:</u>

1) <u>$n=1$:</u> $|G| = p$. ניקח $H := \{e\}$, $|H| = p^{n-1} = 1$!

2) נניח שהטענה נכונה עבור $n-1$

3) נוכיח עבור n

<u>תזכורת:</u> לכל חבורת-p $p \mid |C(G)|$

המרכז $C(G)$ היא חבורה אבלית סופית ו-$p \mid |C(G)|$ לכן לפי הטענה הקודמת (מקרה פרטי של משפט קושי) קיימת תת"ח $H \le C(G)$ כך ש $|H| = p$

<u>תכונה חשובה של מרכז:</u> כל תת"ח $H \le C(G)$ של המרכז היא <u>תת"ח נורמלית של G</u>.

לכן $H \trianglelefteq G$ כך ש $|H| = p$.

לכן G/H <u>חבורת מנה</u> מוגדרת היטב

מוגדר באופן טבעי:

$f: G \to G/H$

$g \mapsto gH$

<u>סימון:</u> $|H| = p$.

$|G/H| = [G:H] = \frac{p^n}{p} = p^{n-1}$ (הגדרה)

לכן G/H חבורה עם p^{n-1} איברים. לפי הנחת האינדוקציה קיימת תת"ח נורמלית $A \trianglelefteq G/H$ כך ש $|A| = p^{n-2}$.

<u>הערה:</u> מקור של תת"ח נורמלית מעביר תת"ח נורמלית תחת הומומורפיזם. לבדוק! ∎

Generated by CamScanner from intsig.com

$$G \xrightarrow{f} G/H$$
$$\triangledown \qquad\qquad \triangledown$$
$$f^{-1}(A) \xrightarrow[\text{הצמצום}]{f_0} A$$

$\ker f_0 = \ker f = H$

$|f^{-1}(A)| = |f^{-1}(A)/H| \cdot |H| = |A| \cdot |H| = p^{n-2} \cdot p = p^{n-1}$.

לסיכום: מצאנו תת חבורה נורמלית $f^{-1}(A) \triangleleft G$ עם p^{n-1} איברים.

משלימים את האינדוקציה ⇐ מש"ל.

מסקנה: לכל חבורת-p G עם p^n איברים קיימת שרשרת נורמלית עם מנות ציקליות. שרשרת נורמלית:

$$G_0 := G \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_{n-1} \triangleright \{e\} =: G_n$$
$$p^n \quad p^{n-1} \quad p^{n-2} \quad \dots \quad p \quad p^0$$

"המנות"

$$G_0/G_1,\ G_1/G_2,\ \dots,\ G_{n-1}/G_n$$

כולן ציקליות (עם סדר p, לפי לגרנז' [illegible]).

הגדרה: חבורה G נקראת פתירה (Solvable) אם עבור G קיימת שרשרת נורמלית סופית עם מנות אבליות.

↓ תוצאה

מסקנה: כל חבורת-p היא חבורה פתירה. ידוע שהחבורה הכי קטנה לא פתירה היא A_5.

בהמשך נלמד דרך אחרת לבדיקה של פתירות דרך הקומוטטורים [עיין].

דוגמאות של חבורות פתירות:

1) כל חבורה אבלית פתירה.

$G_0 = G \triangleright G_1 := \{e\}$ ✓ — מנה אחת בלבד $G/\{e\} \cong G$ אבלית

2) $G = D_n$ (לא אבלית) $\{e\} \triangleleft C_n \triangleleft D_n$

$C_n/\{e\} \cong C_n$ אבלית, $D_n/C_n \cong \Omega_2$ אבלית — 2 מנות

3) $GL_2(\mathbb{R}) \geq G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| \begin{matrix} a \neq 0 \\ a,b \in \mathbb{R} \end{matrix} \right\}$ פתירה!

רמז: לבדוק: $H \cong \mathbb{R}$, $G/H \cong \mathbb{R}^*$ שימוש ב איזו I, $\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| b \in \mathbb{R} \right\} = H \triangleleft G$,

4) חבורת Heisenberg

$$GL_3(\mathbb{R}) \geq G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a,b,c \in \mathbb{R} \right\}$$

לבדוק: $G/H \cong \mathbb{R}^{\times}$, $H \cong \mathbb{R}^{\times}$ (שי"ב 3-2)

<u>הערה:</u> A_5 חבורה פשוטה (כלומר תת"ח נורמליות הן רק $\{e\}, A_5$).
היא החבורה הקטנה ביותר שפשוטה ולא אבלית.

<u>הערה:</u> {פשוטות אבליות} = {ציקליות מסדר ראשוני}

<u>הערה:</u> מהמשפט שהוכחנו היום ⟸ כל חבורת p G עם p^n איברים $n \geq 2$,
היא חבורה לא פשוטה. כי קיימת תת"ח נורמלית $H \trianglelefteq G$ עם p^{n-1} איברים.
($\Leftarrow$ p^{n-1} ...)
$\{e\} \neq H \neq G$
H נורמלית ב-G

<u>משפטי Sylow</u>

Sylow I (קיום)
נניח G חבורה עם $|G| = p^n \cdot m$ כאשר $(p,m)=1$, $m,n \in \mathbb{N}$.
אז: <u>קיימת</u> תת"ח p-סילו $P \leq G$.

Sylow II (צמידות)
א) כל תת"ח p- $H \leq G$ מוכלת בתת"ח p-סילו.
ב) כל תת"ח p-סילו צמודות ב-G.

Sylow III (כמות)
אם תת"ח p סילו $=: n_p$. אז:
א) $n_p \equiv 1 \bmod p$
ב) $n_p \mid m$
ג) $n_p = [G : N(P)]$ (כאשר $P \in Syl_p(G)$).

<u>הגדרה:</u> $N(H) := \{ g \in G \mid gHg^{-1} = H \}$ נורמליזטור של H בתוך G.

<u>תכונות:</u>
(1) $H \triangleleft N(H)$
(2) $N(H)$ היא תת"ח הכי גדולה מבין תת"ח K של G שמכילות את H וכך ש-H נורמלית ב-K.
(3) $N(H)$ = מי"צ של נקודה H במרחב פעולה $G \curvearrowright Sub(G) \to Sub(G)$, $H \in$

$$\boxed{G_H = N(H)}$$

Generated by CamScanner from intsig.com

הוכחה Sylow I: באינדוקציה לפי הסדר של G

(א) $|G|=p$ ברור. $G=P$.

(ב) נניח שהטענה נכונה לכל $k < p^n m$

(ג) צ"ל עבור $|G| = p^n m$

יש רק שני מקרים:

1. קיימת ת"ח $H \le G$ כך ש $|H| = p^n m'$ ו $p^n m' < p^n m = |G|$. $(H \neq G)$

אז אפשר להשתמש בהנחת האינדוקציה (ב):

קיימת ת"ח p-סילו $P \le H$. אז P ת"ח p-סילו גם ב-G.

2. במקרה שאין ת"ח כזאת, אז $H<G$ מקיימת $p \mid [G:H]$.

לפי נוסחת המחלקות נקבל

$$|G| = |C(G)| + \sum_{x_j \notin C(G)} [G : C_{x_j}]$$

(נציגים של המחלקות)

$x_j \notin C(G) \Rightarrow C_{x_j} \neq G$.

לכן לפי הנחה 2: $p \mid [G:C_{x_j}]$.

(תמן) $p \mid |G|$ לכן $p \mid |C(G)|$. היות הוכחנו מקרה פרטי של משפט קושי. נובע שקיימת ת"ח $K \le C(G)$ כך ש $p = |K|$.

יודעים $K \triangleleft G$ לכן חבורת מנה G/K מוגדרת היטב.

ניקח אפי' טבעי $G \xrightarrow{f} G/K$

$$p^{n-1} m = \frac{p^n m}{p} = \frac{|G|}{|K|} = [G:K] = |G/K| < |G|.$$

לפי הנחת האינדוקציה קיימת ת"ח p-סילו $H \le G/K$, $H \in Syl_p(G/K)$

$$\begin{array}{ccc} G & \xrightarrow{f} & G/K \\ \vee\!| & & \vee\!| \\ f^{-1}(H) & \xrightarrow{f_0} & H \end{array}$$

(צמצום)

תזכורת: המקור של ת"ח הוא גם ת"ח.

$\ker f = \ker f_0 = K$.

לפי לגרנז':

$$|f^{-1}(H)| = |f^{-1}(H)/K| \cdot |K| = |H| \cdot |K| = p^{n-1} \cdot p = p^n$$

מצאנו ת"ח p-סילו

השלמנו את האינדוקציה!

שש"ל

Generated by CamScanner from intsig.com