03/08/2011

מרצה: מיכאל מגרל

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

$$X \times X \xrightarrow{w} X$$

$$(a,b) \mapsto w(a,b) = a\cdot b,\quad a+b,\quad a*b \qquad a \oplus b$$

סימונים אפשריים

(X, w) או $(X, \cdot)$ . . .

הזוג נקרא מבנה אלגברי.

דוגמה: $(N,+)$ $(N,\cdot)$ מבנים.

הפרש - ב-N לא מוגדר היטב.

לעומת זאת, $(Z,-)$ כן מוגדר היטב ולכן מבנה אלגברי.

הגדרות נוספות:

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

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

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

$$\Downarrow$$

2* **משפט:** **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: $(Mat_{n\times n}(R),+)$, $(N,\cdot)$, $(N,+)$, $(Mat_{n\times n}(R),\cdot)$, $(P(X),\cap)$ ...

הן אגודות.

$(Z,-)$ לא אגודה.

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

בדרך כלל ניטרלי מסומן כ-e

$\cdot$	$\dots I,\ 1,\ 1$
$+$	$\dots \mathbb{0},\ 0$

הרבה מסמנים אותו גם דרך e $x\cdot e = e\cdot x = x$

טענה: ניטרלי יש לכל היותר אחד.

הסבר: נניח ש- e, e' ניטרליים

$$e\cdot e' = e,\quad e\cdot e' = e' \Rightarrow e = e'$$

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

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

$(\mathbb{N}, +)$ לא מונואיד (רק אגודה). $\{1,2,3,\dots\}$

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

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

כללים:

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

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

·	a	b
a	b	b
b	a	a

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

שימו לב! X לא אגודה!

אם נתונה אגודה $(X,+)$

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

הכללים: $m(na)=(mn)a$, $(n+m)a = na+nm$

- 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 (inverse):** במונואיד $(X,\cdot)$ איבר $a\in X$ נקרא **הפיך** אם קיים $b\in X$ כך שמתקיים $a\cdot b = b\cdot a = e$

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

- במונואיד $(X,+)$ $a+b=b+a=0_X$.

אסוציאטיבי + קומוטטיבי.

טענה (יחידות של ההופכי)

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

הסבר: נניח $b,b'\in X$ הפוכים ל-a.

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

$a\cdot b=e$ (נכפיל ב-b')

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

$e\cdot b=b'$

$\Downarrow$

$b=b'$ יחיד

מסמנים הפיך ל-a ע"י a^{-1}.

אם הפעולה היא **חיבור** אזי $-a$ (נסמן $-a$).

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

תנאים: א) אסוציאטיביות

ב) קיום ניטרלי   =   חבורה.

ג) כל איבר הפיך

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

דוגמאות: $+$ $\mathbb{C}$ $\mathbb{R}$ $\mathbb{Q}$ $\mathbb{Z}$ $2\mathbb{Z}$ $\{0\}$ 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

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

(שקול להפיכות מטריצה)

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

- במונואיד $(X,+)$ $a+b=b+a=0_x$

חיבורי + קומוטטיבי

טענה (יחידות של ההופכי)

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

הסבר: נניח $b,b'\in X$ הפוכים ל-a.

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

$a\cdot b=e$ (נכפיל ב-b')

$$b'(a\cdot b)=b'\cdot e \quad \text{(נייטרלי)}$$
$$(b'\cdot a)\cdot b=b' \quad \text{(אסוציאטיבי)}$$

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

מסמנים הפיך ל-a דרך a^{-1}.

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

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

ציון: א) אסוציאטיביות
ב) קיום נייטרלי = חבורה.
ג) כל איבר הפיך

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

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

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

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

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

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

⇓ שקול להפיכות מטריצה

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

Generated by CamScanner from intsig.com

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

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

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

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

חיבור מודולו 2 : $2\mathbb{Z}$

$[0] := 2\mathbb{Z}$ $\qquad \bigcup = \mathbb{Z}$

$[1] := 2\mathbb{Z}+1$ $\qquad \bigcup = \mathbb{Z}$

כפל

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

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

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

$$\Updownarrow$$

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

$$\Updownarrow$$

ל-a ול-b יש שארית מודולו n.

תרגיל:

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

יש n מחלקות שקילות:

חלוקה של $\mathbb{Z}$:

$[0] := n\mathbb{Z}$

$[1] := n\mathbb{Z}+1$

$\vdots$

$[n-1] := n\mathbb{Z}+(n-1)$

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

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

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

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

Generated by CamScanner from intsig.com

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

תרגיל: אין תלות בנציגים.

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

לכן הפעולות מוגדרות היטב.

$(\mathbb{Z}_n, \oplus)$ חבורה אבלית

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

טענה: $(\mathbb{Z}, \odot)$ מונואיד קומוטטיבי.

* אסוצ' + קומ'
* נייטרלי $[1]$.

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

↑ באופן כללי זה "חוג".

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

$$[a] = a[1]$$

למשל: ב-$(\mathbb{Z}_3, \oplus)$

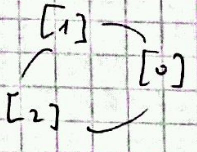
$[1]$

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

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

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

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



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

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

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

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

אז מגדירים $a^{\alpha} := (a^{-1})^{(-\alpha)} = (a^{-\alpha})^{-1}$ $\alpha<0$ שלם.

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

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? $e\cdot e=e \Leftarrow e^{-1}=e$.

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

צריך קיום

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

ואסוציאטיביות תבוא תורשתית מ-X.

$\Downarrow$

$Gr(X)$ חבורה.

מש"ל

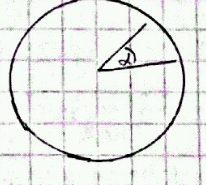
דוגמאות:

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

דוגמה חשובה של חבורות ציקליות

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

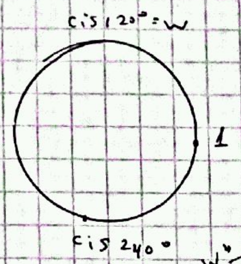
$z = \cos\alpha + i\sin\alpha = cis\,\alpha$



$\Omega_1 = \{1\}$

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

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



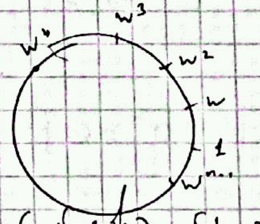
$\Omega_4 = \{i, -1, -i, 1\} = \{w, w^2, w^3, 1\}$, $w = cis\,90°$

$\vdots$

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

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

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



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

ניכר: $\mathbb{1}$, $z \in \Omega_n \Leftarrow z^{-1} \in \Omega_n$. הם מההגדרה של Ω_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

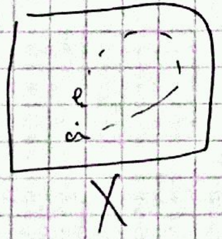
$(\mathbb{Z}_n, \oplus) = \{[1], [2], \dots, [n-1], [0]\}$

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

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

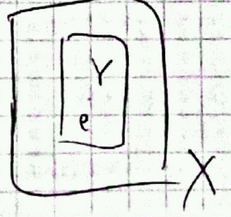
סימון: נניח X חבורה, $a \in X$.

$\langle a \rangle := \{a^k\}_{k \in \mathbb{Z}}$ תת חבורה של X (ציקלית) הנוצרת ע"י a.



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 הצמצום כך ש-Y גם חבורה.



Generated by CamScanner from intsig.com

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

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

(רק מונואיד (לא תת חבורה)   חבורה

דוגמאות של חבורות ציקליות אינסופיות:

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

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

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

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

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

② $X = \mathbb{Q}^*$

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

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

תכונות: [1] $O(a) = 1 \iff a = e$

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

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

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

הסבר: קיים $a \in G$ כך ש- $O(a) = n$, $\langle a \rangle = G = \{a^k\}_{k\in\mathbb{Z}} = \{e, a, \ldots, a^{n-1}\}$ (n איברים!) 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 ההסבר מספיק להוכיח שהאיברים $e, a, a^2, \ldots, a^{n-1}$ הם שונים.

אם נניח $a^i = a^j$ (בה"כ $i < j$). אז $a^{j-i} = e$, $0 < j-i < n$, $\in \mathbb{N}$

סתירה להגדרת הסדר. משיך.

Hofit Marzouk

04/08/2011

המשך - סדר

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

הסבר: $(\Leftarrow)$: $n:=O(a)|m$.

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

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

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

נשקול 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 $n=O(a)$ מש"ל

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}.

$$a\cdot x=a\cdot y$$

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

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

$x=y$. מש"ל

-באופן דומה II.

טענה: (משוואה אלמנטרית)

[illegible]

אם a הפיך במונואיד X אז לכל "משוואה אלמנטרית"

I $\quad a\cdot x=y$

$x=?$

II $\quad x\cdot a=y$

יש פתרון יחיד והוא שווה:

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

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

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

יש יחידות!

Generated by CamScanner from intsig.com

דוגמא: $[5]_{54} \cdot x = [3]_{54}$.

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

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

$[5]\odot[11] = [55]_{54} = [1]$ (בגלל הופכי)

קומוטטיבי

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

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

״גישה אחרת״:

לפתור בשלמים $5x = 3 \mod 54$, $x \in \mathbb{Z}$.

דרך א: ישר מהדוגמא 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: $x \equiv 33 \mod 54$

$\Updownarrow$

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

מונואיד וחבורה של פונקציות.

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

מונואיד לגבי פעולת הרכבה.

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

$Map(X,X) \ni f_2\circ f_1$ $\downarrow$ מוגדר.

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

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

$1_X = id_X = id$ ״ניטרלי״

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

הסימון: $S_X := Gr(Map(X,X))$.

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

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

הערה: X סופי $\Leftarrow$ אז מספיק לבדוק רק אחד מהתנאים: חח״ע או על.

במקרה פרטי של $X:=\{1,2,\dots,n\}$ (סימן 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: $S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = e, \; \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = a \right\}$

·	e	a
e	e	a
a	a	e

n=3: $|S_3| = 6$

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

- לחשב 2 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!

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

$$\sigma\circ a \neq a\circ\sigma$$

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

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

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

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

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

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

Generated by CamScanner from intsig.com

__דוגמא גם:__ G חבורה בעלת סדר קטן מ-6 קומוטטיבית. (סדר = מספר איברים)

__תרגיל:__

במונואיד Map(N,N) קיימים איברים הפיכים רק מצד אחד.

__הסבר:__

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

$f(n) = n+1$.

חח"ע אבל לא על ($f^{-1}(n)$ צריך להיות 0, שלא נמצא ב-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 מס' יתאים

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

כלומר לא חח"ע ולכן הפיכה רק מימין.

בקשר למונואידים (ולא רק)

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

לדוגמה: ① $a=e$ בכל מונואיד.

② $0\in(\mathbb{R},\cdot)$

③ $[6]\in(\mathbb{Z}_{30},\odot)$

③ $X=\{1,2,3\}$ $Map(X,X)$

מס' איברים $3^3 = Map$.

$f_1=\begin{pmatrix}1&2&3\\1&1&1\end{pmatrix}$ $\qquad f_1(x)=1 \quad \forall x\in X$

$g=\begin{pmatrix}1&2&3\\1&1&3\end{pmatrix}$ $\qquad f_1{}^2=f_1,\ g^2=g.$

הערה: בחבורה יש 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 $Y:=X\cup\{e\}$ $\quad(e\notin X)$

נרחיב את הפעולה:

$x_1\cdot x_2 \quad \forall x_1,x_2\in X$

$e\cdot x=x \quad \forall x\in X$

$e\cdot e=e$

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

הגדרה (הזזות) נניח $a\in X$.

נגדיר $l_a: X\to X$. $l_a(x)=a\cdot x$

$r_a: X\to X$. $r_a(x)=x\cdot a$

הזזות, transformations.

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

תכונות:

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. לכל $a\in \mathcal{O}_r(X)$. $l_a:X\to X$ חח"ע ועל.

הסבר:

1. ברור.
2. $(\Leftarrow)$: אם l_a על אזי קיים $x\in X$ עם e. $l_a(x)=e$ כלומר $a\cdot x=e$
כלומר x הפיך מימין.
$(\Rightarrow)$: נניח שקיים $x\in X$ כך ש- $a\cdot x=e$. לכל $y\in X$ 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. כנ"ל.
4. ③ ∧ ② ⟸ ④.

תרגיל: נניח X מונואיד סופי כך שאפשר לצמצם על כל איבר משמאל.
הוכח ש-X חבורה.

הערה: אם X לא סופי אז לא תמיד!
לדוג' $X:=\mathbb{N}\cup\{0\}$ + . מונואיד "עם צמצום". לא חבורה.
$a+x=a+y\Rightarrow x=y$

הערה: לכל אגודה סופית יש לפחות אידמפוטנט אחד.
(לא נכון לאינסופי, $(X:=(\mathbb{N},+))$

כמה מבוא מתורת המספרים הבסיסית (שצריך לדעת):

1. התחלקות ב-$\mathbb{Z}$
2. חילוק עם שארית.
3. מס' ראשוני: $p\geq 2$ כך ש-p מתחלק ב-1 ו-p.
4. המשפט היסודי של האריתמטיקה (פירוק לראשוניים):

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

$p_1,p_2,\dots,p_m$ גורמים ראשוניים של a. $i_1,i_2,\dots,i_m\in\mathbb{N}$ 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 $a = p_1 \cdot p_2 \cdot p_3 \cdots p_k + 1$ אז (4) קיים פירוק לראשוניים עבור a. לכן קיים p_i ראשוני

כך ש- $p_i | a \Leftarrow p_i \in P$

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

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

מש"ל

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

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

(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 $\overset{def}{\iff} (a,b) = 1$

(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 גם דרך למצוא u,v ("הצבה אחורנית")

(10) משוואה לינארית $ax + by = c$

$x,y,a,b,c \in \mathbb{Z}$

פתירה בשלמים $\iff (a,b)|c$ $\quad$ (קיים (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 $(a,b)|c$, צ"ל $c = (a,b) \cdot q$

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

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

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

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

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

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

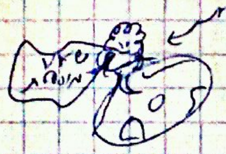
$\Leftarrow (a,b) = 1$. מש"ל

⑤ **משפט אוקלידס:** יש אינסוף ראשוניים.

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

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- $p_i | a \Rightarrow p_i \in P$.



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

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

מש"ל

⑥ $gcd(a,b) = (a,b)$ $lcm = [a,b]$

$$\boxed{[a,b] \cdot (a,b) = ab}$$

⑦ אלגוריתם אוקלידס - למצוא את (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 $\overset{def}{=}$ $(a,b)=1$

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

אלגוריתם אוקלידס מספק גם דרך למצוא u,v "וההצבה אחורנית"

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

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

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

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

Generated by CamScanner from intsig.com

$a|b \Leftarrow \begin{cases} a|bc \\ (a,c)=1 \end{cases}$ (2)

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

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

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

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

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

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

ב) $a=[150]\in(\mathbb{Z}_{250},\oplus)$ $O([50]_{250})$

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

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

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

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

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

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

(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 הלמה של הלוק, מלמה (12) שוויונים (2)

מ-(1) ועם $\frac{n}{(n,k)}\mid t$ 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 $(\mathbb{Z}_n, \odot)$

דוגמא: $\varphi(100) = ?$

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 - צירוף "קרוב" לינארי של כולו" טענה (11), $(a,n) = 1$

את כל השלבים עשינו בצורה שקולה, ולכן נקבל $(a,n) = 1 \iff [a] \in U_n$ מש"ל

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

מקרים: $n = p$ ראשוני: $U_p = \{[1], [2], \dots, [p-1]\}$ 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: $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m}$

$$\varphi(n) = \varphi(\;) = \varphi(p_1^{k_1})\varphi(p_2^{k_2})\cdots\varphi(p_m^{k_m}) = (p_1^{k_1} - p_1^{k_1-1})\cdots$$

זרים זה לזה

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

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

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

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

8.8.2011
הרצאה III

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

למשל: ב-Ω_4 האיברים הנ"ל הם w, w^3.

תשובה על השאלה: $\varphi(n)$. $|x|$ = $card(x)$ עוצמה

הסברי: $w^k = b \in \Omega_n$, $\exists k$. $1 \le k \le n$ $|a|$ סדר.(n)

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

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

(מס' איברים מתחת ל-$|o(b)|$; "שונים" מתחת לקבוצה)

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

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

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

למשל: מ-Ω_p, p ראשוני, 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

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

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

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

זאת הרשימה של תת חב' ב-$\mathbb{Z}$ כאשר $a \in \mathbb{Z}$ (טבעי שלם).

2. $a\mathbb{Z} \leq b\mathbb{Z} \iff b \mid a$

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

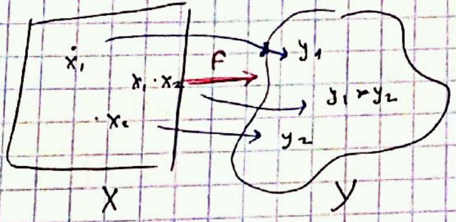
4. $a\mathbb{Z} \cap b\mathbb{Z} = [a,b]\mathbb{Z}$.

הומומורפיזמים:

הגדרה: ① נניח $(X, \cdot)$, $(Y, *)$ חבורות.

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

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



2. אם f (גם) חח"ע, אז אומרים **מונומורפיזם**. (הומומורפיזם)

3. אם f הומומורפיזם על ($Im(f) = f(X) = Y$ כ"א) אז אומרים **אפימורפיזם**,

4. f נקרא **איזומורפיזם** אם f מונו + אפי. (f הומ' + 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 הומ' (אפי, מונו, איזו)

גם ("   ")

במ"א 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' $X \to Y$. סימון: $X \cong Y$

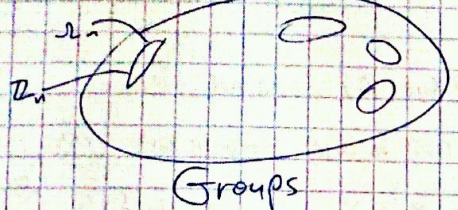
הערה:

$X \simeq X$

$X \simeq Y \iff Y \simeq X$

$Y \simeq Z$ ו- $X \simeq Y \iff X \simeq Z$

קל להוכיח בגלל התכונות הנ"ל.



(4)

★ ≃ יחס שקילות

לכן $\{Groups\}$ = מחולק למחלקות שקילות. לא קבוצה!!

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

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

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

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

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

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

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

הסבר: אינדוקציה + תכונות 5+6.

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

הסבר: אם $O(x) = n$ אז $x^n = e_x$ ⇐ (5 ו-7) $f(x^n) = f(e_x)$

$f(x)^n = e_y$. מש"ל.

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

הערה: בעצם מספיק f מונו' (למה?)

הערה 2: 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) $Im f = f(X) \le Y$

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

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

הסבר: לבדוק.

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

(לבדוק צג חבורה) $(Aut(X), \circ) \le (S_X, \circ)$ חבורה סימטרית

שאלה: מה זה $Aut(\mathbb{Z})$?

(12) איזומורפיזם שומר על תכונות קומוטטיביות, ציקליות.

נניח אם $X \xrightarrow{f} Y$ איזו: $Y = f(X)$

קומוט׳:

$\forall y_1, y_2 \in Y$

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

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

(הוס׳ f ; קומו׳)

תרגיל: הוכח 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

$\cong$

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

Ω_2

$\Omega_2 \xrightarrow{f} G$ איזו

$1 \to I$

$-1 \to J$

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

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

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

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

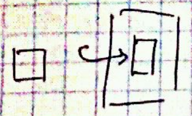
$f(x) = 5^x$

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

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

Generated by CamScanner from intsig.com

(5 $S_5 \to S_3$ קיים שיכון.



״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)

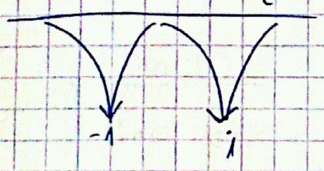
__אומרים:__ ״שיכון״ של חבורה לתוך חבורה שניה.

__שימו לב:__ לכל מיפוי $f: X \to Y$, $f_*: Y \to f(X)$ על.

(6 $(\mathbb{R}^*, \cdot) \xrightarrow{f} (S_2, \cdot)$

$S_2 = \{1, -1\}$

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



לא __איזומורפיזם__. f לא חח״ע הפרעה

בדיקה 4 מקרים (סימנים)

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

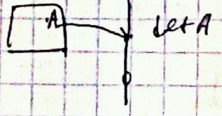
+	+
+	-
-	+
-	-

(7 (מונואידים) $(\underset{\text{מטריצות}}{Mat(\mathbb{R})}, \cdot) \to (\mathbb{R}, \cdot)$, $f = \det$

$f(A) = \det(A)$

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

f הומומורפיזם של מונואידים. מצמצם לקבל (אם) הומומורפיזם של חבורות.



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

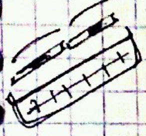
(8 אופי $(\mathbb{Z}, +) \xrightarrow{f} (\mathbb{Z}_n, \oplus)$

f ברור $a \xrightarrow{f} [a]_n$

$f(a+b) = [a+b]_n$ ← הגדרה

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

Holit Harzouki



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

הוכחה: 1 נגדיר

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

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

f הומו':

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

הוכחה 2:

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

אם נניח שלא: $k_1>k_2$

$$f(k_1)=f(k_2)$$
$$a^{k_1}=a^{k_2}$$
$$\exists k_1-k_2\in\mathbb{N} \quad a^{k_1-k_2}=e$$

בסתירה ל $O(a)=\infty$ משל.

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

שוני: $i\equiv j \bmod n \iff a^i=a^j$

הסבר:

$$a^i=a^j \iff a^{i-j}=e$$
$$\Updownarrow \text{ תרגיל}$$
$$i\equiv j \bmod n \iff n\mid i-j$$

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

תרגיל+הס'

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

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

f מוגדר היטב בגלל (*) כי $[i]=[j] \iff a^i=a^j$. משל.

Generated by CamScanner from intsig.com

תוצאה

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

<u>הסבר:</u>

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

קוסטים / משפט Lagrange

<u>הגדרה:</u> נניח $H \le G$

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

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

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

ב. קבוצת מנה של H ב-G היא $G/H := \{aH : a\in G\}$

<u>למשל:</u>

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

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

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

סימון: $[G:H] := |G/H|$ <u>למשל</u> $[\mathbb{Z}:3\mathbb{Z}]=3$

משפט Lagrange:

נניח $H\le G$ 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) $|G| = |H|\cdot[G:H]$

<u>תוצאות:</u>

(1) לכל G <u>סופית</u>, $H\le G$ מתקיים $|H| \mid |G|$ $\overset{3}{\Leftarrow}$ (4) לכל G חבורה סופית, מתקיים לכל $x\in G$, $x^{o(G)}=e$

$\overset{3}{\Leftarrow}$ $|G:H| \mid |G|$

(2) לכל G <u>סופית</u> ולכל $x\in G$ מתקיים $|o(x)| \mid |G|$ (הסבר)

<u>הסבר:</u> $n=|o(x)|=|H|$, $H\le G$: $\langle x\rangle = \langle e, x, x^2, \dots, x^{n-1}\rangle$ במילים, הסדר של איבר X שווה לסדר של תת החבורה $\langle x\rangle$. | G סופית $\Leftarrow$ לכל איבר $x\in G$ קיים סדר סופי! $\Leftarrow$ $m=nq$ מתאים. $e=(x^n)^q=x^{nq}=x^{|G|}$. תוצאה 2 $\Leftarrow$ $o(x)\mid G$, $|G|=m$, $o(x)=n$

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

<u>הסבר:</u>

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

(כי $O(a)=|G|=p$). קיבלנו ש- G ציקלית עם p איברים.

לפי משפט המיון, $G\cong\mathbb{Z}_p$. <u>מש"ל</u>.

<u>הגדרה:</u> ת"ח $H\leq G$ נקראת <u>נורמלית</u> ב- G אם $aH=Ha$ $\forall a\in G$

<u>סימון:</u> $H\trianglelefteq G$

<u>דוגמה של ת"ח לא נורמלית:</u> $G=S_3=\langle a,\sigma\rangle$ ש- $3!=6$ איברים.

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

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

ת"ח, אבל לא נורמלית.

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

<u>תכונות:</u>

(1) אם G אבלית אז כל ת"ח היא נורמלית.

$ah=ha\Rightarrow aH=Ha$ $\forall h\in H$ $\forall a\in G$

(2) כל חבורה G מקיימת $G\trianglelefteq G$, $\{e\}\trianglelefteq G$

<u>המרכז:</u> $C(G)=Z(G):=\{g\in G:\forall x\in G,\ xg=gx\}$.

(כל האיברים הקומ') $C(G)\trianglelefteq G$

<u>הסבר ל- $G\trianglelefteq G$:</u> צ"ל: $Ga=aG$ $\forall a\in G$

שימו לב: $\begin{cases}aG=G\\Ga=G\end{cases}$ תמיד.

$aG=l_a(G)=G$, כי a הפיכה.

<u>משפט Euler II (או תזכורת):</u>

לכל $(a,n)=1$ ולכל $a\in\mathbb{N}$ מתקיים $a^{\varphi(n)}\equiv 1\bmod n$

<u>הוכחה:</u> $(a,n)=1$ $\overset{\text{משפט Euler I}}{\Longrightarrow}$ $[a]_n\in(U_n,\cdot):=G$ חבורת אוילר

לפי מסקנה 4 (קודם) $[a]_n^{|U_n|}=[1]_n$.

וגם: $|U_n|=\varphi(n)$, ולכן (קודם) $a^{\varphi(n)}\equiv 1\bmod n$.

<u>מש"ל</u>

משפט פרמה: (הקטן)

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

הוכחה:

שני מקרים:

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

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

משל.

תרגיל:

לחשב שתי ספרות אחרונות של: 202

א. 39078653

ב. 39078659^{999}

רמזים:

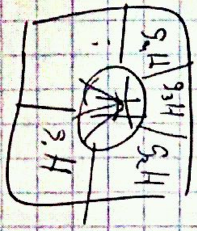
א. $\varphi(100)=40$

ב. $[53]^{-1}_{100}=17$

Generated by CamScanner from intsig.com

10/08/2011 - דגה

הרצאה IV



משפט Lagrange -

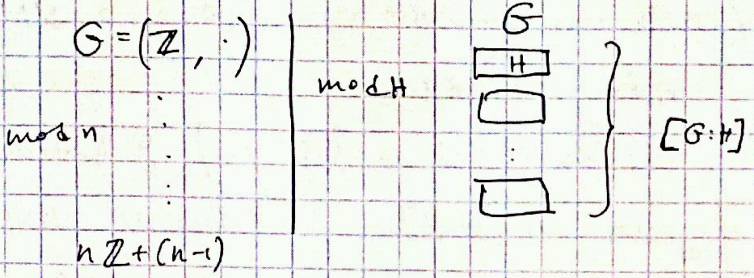
נניח $H \le G$ אזי

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

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

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

הוכחה: הרעיון:



(נגדיר יחס "מודולו H" ב-G ע"י $g_1\equiv g_2 \mod H$ $\overset{def}{\iff}$ $g_1^{-1}g_2\in H$

מוכיחים שזה יחס שקילות בקבוצה G:

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

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

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

$\parallel$

$g_2^{-1}g_1\in H \Rightarrow g_2\equiv g_1 \mod H$

ג) טרנזיטיביות: $\begin{cases} g_1\equiv g_2 \\ g_2\equiv g_3\end{cases} \Rightarrow g_1\equiv g_3$.

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

$\parallel$

$g_1^{-1}g_3\in H \Rightarrow g_1\equiv g_3$.

הוכחנו ש- $\equiv_H$ יחס שקילות (תכונה בסיסית של יחס שקילות)

$\Downarrow$

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

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

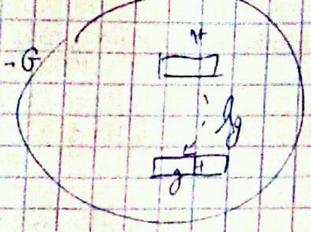
קיבלנו $[g]=gH$ קוסט של g ← מחלקה של g. לכן הוכחנו (1). $G=\bigcup_{g\in G} gH$

Generated by CamScanner from intsig.com

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

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

אז: $|gH|=|H|$ $\forall g\in G$



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

כאשר $G \xrightarrow{\ell_g} G$

$x \mapsto gx$

ℓ_g חח״ע כי g הפיך (ואז תמונת ℓ_g ... או שוו.)

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

נובע מההפיכות של g (ניתן לצמצם כי g איבר בחבורה).

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

<u>הערה:</u> משפט לגרנז' גם "בגרסה ימנית", כי $g_1\equiv g_2 \pmod H$ מימין $\overset{def}{\iff} g_1\cdot g_2^{-1}\in H$

$[G:H]$ שווה בשני המקרים הנ״ל.

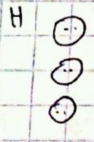
הסבר ישיר (בלי לגרנז'): $\{gH\}_{g\in G} \xrightarrow{\varphi} \{Hg\}_{g\in G}$

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

φ חח״ע ועל.

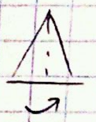
<u>תרגיל:</u> למצוא את כל הקוסטים השמאליים והימניים במקרים הבאים:

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



$[G:H]=3$

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



<u>המשך השאלה על תת״ח בחבורה ציקלית:</u>

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

מצאנו שכל תת״ח בחבורה ציקלית <u>אינסופית</u> $G=\langle a\rangle$, $o(a)=\infty$

$\{H=\langle a^m\rangle\}=Sub(G)$

m טבעי שלם. subgroups

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

$O(a)=n<\infty$.

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

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

② **יחידות:** לכל $m|n$ יש רק תת-חבורה אחת H: $|H|=m$.

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

הוכחה: נקח 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 שיש $K\le G$ ו- $|K|=m$.

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

לפי המשפט על תת-חבורות ציקליות: K גם ציקלית, לכן $\langle a^s\rangle=K$, $\exists s\in\mathbb{N}$

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

מכאן $(n,s)=\frac{n}{m}$.

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

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

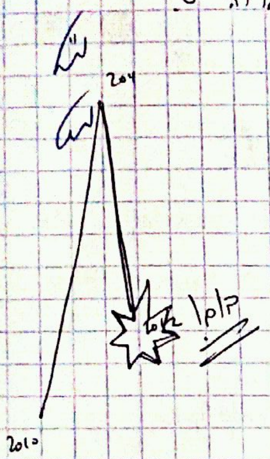
הוכחנו $a^{\frac{n}{m}}\in K$. מש"ל

תרגיל: למצוא את כל תת-חבורות של G

א) Ω_{10}

ב) $\mathbb{Z}_{15}$

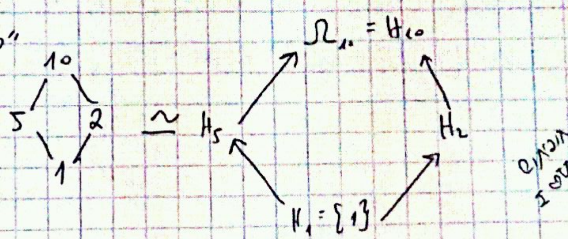
לבד



Generated by CamScanner from intsig.com

הערה: "סריג של ת"ח"

"סריג המחלקים"



משפט Wilson: (Bhaskara VIII הודו)

עבור $n \geq 2$ טבעי מתקיים

$n \mid (n-1)!+1 \iff n=p$ ראשוני

הוכחה: $(\Leftarrow)$: נניח p ראשוני. צ"ל $p \mid (p-1)!+1$

כרעיון להוכחה ניקח מקרה $p=7$.

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

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

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

$1\cdot2\cdot3\cdot4\cdot5\cdot6 \equiv 6 \mod 7$

באופן כללי: צ"ל: $p \mid (p-1)!+1$

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

שקול להוכיח: $(p-1) \mod p = 1\cdot2\cdot3\cdot4\cdots(p-2)\cdot(p-1)$

נספר כל איבר עם ההופכי שלו. יש לזכור ש- $(\mathbb{Z}_p, \oplus, \odot)$ שדה

לכן לכל $[a]_p \neq [0]_p$ יש הופכי

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

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

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

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 נראה

נהיה פה זמן מה..

תן לי דקה להבין אלך שוב..

זין מכון

$① \cdot 2 \cdots (p-2)(p-1) \equiv ① \cdot 1 \cdot (p-1) = (p-1) \bmod p$

הוכחת ⟸: נתון $n \mid (n-1)! + 1 \Leftarrow u \cdot n = (n-1)! + 1$ מספיק $\exists u \in \mathbb{Z}:$ לתשובה?

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

ולכן לפי משפט $(n,k) = 1$ $\forall k \in \mathbb{N}: k < n$ ⟸ $n = p$ ראשוני.

חבורת מנה:

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

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

Lotit Marzouk:)

(2) אז $\varphi: G \to G/H$

$g \mapsto gH$ הומומורפיזם

(3) $\ker \varphi = H$

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

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

($H = \{e, (1,2)\} \le S_3$ כי לא תמיד נכון)

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

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

מהשוויון $(aH) \cdot (bH) = (ab)H$ נובע שאין תלות בנציגים של המחלקה

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

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

צ"ל $(G/H, *)$ מבנה אלגברי:

המבנה בעצם חבורה | אסוציאטיביות $*$ נובעת מאסוציאטיביות של $(G, \cdot)$.

ניטרלי: $[e] = H \in G/H$ ⟸ e ניטרלי ב-G

$[e] = H$ ניטרלי ב-$(G/H, *)$

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

(2) φ על: ברור כי לכל $gH \in G/H$

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

φ הומומורפיזם:

$\forall a, b \in G$

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

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

Generated by CamScanner from intsig.com

(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:

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

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

הערה: $H\leq G$.

התנאים הבאים שקולים:

(א) $\forall g\in G:\ gH=Hg$ (הגדרה)

⇕

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

⇓

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

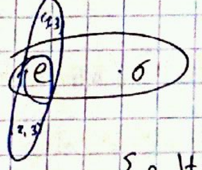
⇑ שינוי משתנה g^{-1} במקום g.

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

$h\in H$

דוגמא: $H=\{e,(1\,2)\}\leq G=S_3$

$\sigma \quad \not\trianglelefteq \quad \sigma$

$H=$ 

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

$geg^{-1}=e$.

3 מ"ח $H\ntrianglelefteq G$

הערה: הצמדה ע"י g בחבורה G היא

$\alpha_g : G\to G$

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

תכונות:

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

הסבר:

הומו':

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

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 $\alpha_g(x_1)=\alpha_g(x_2)$

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

$\Downarrow$

$x_1=x_2$ מש"ל.

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

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

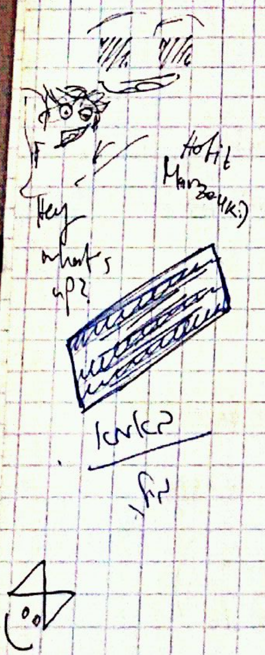
לגבי פעולת ההרכבה?

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

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

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

(4) בחבורה אבלית $\Leftarrow$ לכל g $\alpha_g = id_G$.



דוגמה: אוטומורפיזמים לא פנימיים:

(א) $(\mathbb{C}, +)$ $z \mapsto \bar{z}$ אוט' (של שדה)

$a+bi \mapsto a-bi$

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

(ב) $G = \Omega_3 \times \Omega_3$

$G \xrightarrow{f} G$

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

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

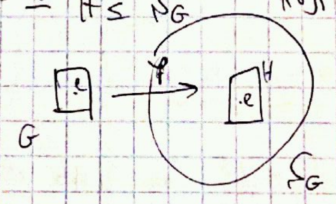
משפט Cayley (קיילי):

כל חבורה G איזומורפית לתת חבורה של S_G.

$\Downarrow$

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

הסבר התוצאה: מהמשפט ישר נקבל שקיימת תת $H \leq S_G$ $G \cong H$



נשים לב שבצורה שקולה: קיים מיפוי $G \to S_G$:

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

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

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

לין

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

$\gamma \circ \varphi$

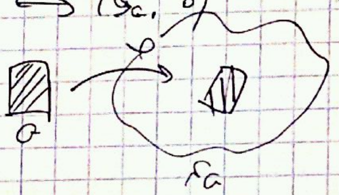
(מונומורפיזם · שיכון)

<u>רעיון</u> הטבלה של חבורה $G=\{g_1=e, g_2, \dots, g_n\}$

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

<u>הוכחה של משפט קיילי:</u>

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



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

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

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 $l_a(x)=y$

$\Downarrow$

$l_a \in S_G$.

<u>l_a הומו':</u>

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

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

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

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

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

הערה:

ל חבורה $\mathbb{R}^n$ ← חבורה מסוימת, איזומורפי

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

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

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

__רעיון ההסבר:__ לפי משפט קיילי,

$$G \overset{\varphi}{\hookrightarrow} S_n$$

לכן מספיק להראות:

$$S_n \hookrightarrow O_n(\mathbb{R})$$

$e_1, e_2, \dots, e_n$ בסיס סטנדרטי של $\mathbb{R}^n$.

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

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

וכו'

__מסקנה:__ כל חבורה סופית ניתנת לייצג בחבורה אורתוגונלית.

__חבורות של סימטריות:__

נניח $A \subseteq \mathbb{R}^n$.

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

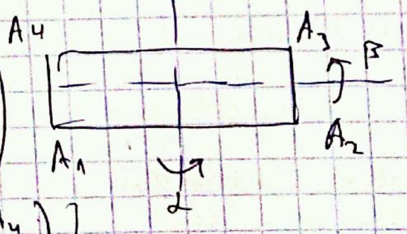
__כלומר__ ב"א

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

__דוגמאות:__

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

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



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

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

$n=1$: __טענה__

__נניח שקודם אחד:__ אוטופלו.

כל סיבוב שלא מולבן - בשמו: ואחד.

__משל.__

Generated by CamScanner from intsig.com

K_4:

*	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]				
[illegible]				
[illegible]				
[illegible]				

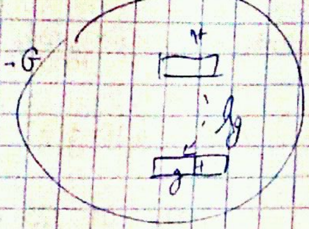
[illegible]

Generated by CamScanner from intsig.com

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

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

צ"ל: $|gH|=|H|$ $\forall g\in G$



$gH = l_g(H)$

כאשר $G\xrightarrow{l_g}G$

$x\mapsto gx$

l_g חח"ע כי g הפיך (ואז התמונה של l_g ... או שיו'.)

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

נובע מהפיכות של g (ניתן לצמצם כל איבר בחבורה).

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

הערה: משפט לגרנג' גם "בגירסה ימנית", ע"י מגדירים $g_1\equiv g_2(\text{mod } H)$ (משמאל) $\overset{def}{\Leftrightarrow} g_1\cdot g_2^{-1}\in H$

$[G:H]$ שווה בשני המקרים (הנ"ל)

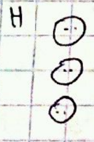
הסבר ישיר: (בלי לגרנג'): $\{gH\}_{g\in G}\xrightarrow{\varphi}\{Hg\}_{g\in G}$

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

φ חח"ע +על.

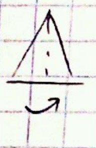
תרגיל: למצוא את כל הקוסטים השמאליים והימניים במקרים הבאים:

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



$[G:H]=3$

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



σ שיקוף

a סיבוב

המשך השאלה על ת"ח בחבורה ציקלית:

תזכורת: ת"ח של ציקלית גם ציקלית (משפט).

מצאנו שכל ת"ח בחבורה ציקלית אינסופית $G=\langle a\rangle$, $o(a)=\infty$

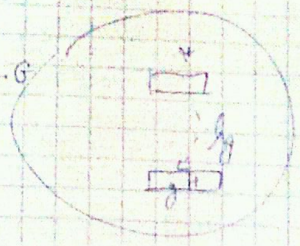
$\{H=\langle a^m\rangle\}=Sub(G)$

m טבעי/שלם. ← Subgroups

(ד) בחר מחלוקה $g_1 H = g_2 H \iff [g_1] = [g_2] \iff g_1 \equiv_H g_2 \iff g_1^{-1} \cdot g_2 \in H$

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

מסקנה: $|gH| = |H|$ $\forall g \in G$



$\left[gH = l_g(H) \right]$

כלומר $G \xrightarrow{l_g} G$

$x \longmapsto gx$

l_g חח"ע כי g הפיך (ראו תכונות של l_g ... או ישיר.)

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

נובע מהפיכות של g (עיין לצמצם כפל איבר בחבורה).

מכל העובדות שהתקבלו: $|G| = |H| \, [G:H]$

הערה: משפט לגרנז' גם "בגרסה ימנית", כלומר $g_1 \equiv g_2 \pmod{H}$ ימני $\overset{def}{\iff} g_1 \cdot g_2^{-1} \in H$

$[G:H]$ שווה בשני המקרים הנ"ל

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

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

φ חח"ע ועל.

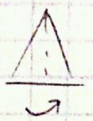
תרגיל: למצוא את כל הקוסטים השמאליים והימניים במקרים הבאים:

① $G = S_3$ $\le$ $H = \{e, (1,2)\}$

H ⊙ ⊙ ⊙

$[G:H] = 3$

② $G = D_3$ $\le$ $H = \{e, \sigma\}$



σ שיקוף

a סיבוב

המשך השאלה על ת"ח בחבורה ציקלית:

תזכורת: ת"ח של ציקלית גם ציקלית (משפט).

מצאנו שלת"ח בחבורה ציקלית אינסופית $G = \langle a \rangle$, $o(a) = \infty$.

$\{H = \langle a^m \rangle\} = Sub(G)$

m טבעי שלם. Subgroups

מקרה של חבורה ציקלית סופית: G עם $\langle a\rangle = G$

$O(a) = n < \infty$

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

קיום: (1) לכל $m \mid n$ קיימת תת חבורה H של G עם $|H| = m$.

יחידות: (2) לכל $m \mid n$ יש רק תת חבורה אחת H עם $|H| = m$.

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

הוכחה: נוכיח תחילה בהמשך שכל תת חבורה H של G היא ציקלית.

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

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

בדיקה:

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

קלקל

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

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

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

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

מכאן $(n,s) = \frac{n}{m}$.

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

$(n,s) = u\cdot n + v\cdot s$ אוקלידס, $\exists u,v \in \mathbb{Z}$

כי $a^s \in K$

הוכחנו $a^{\frac{n}{m}} \in K$. מש"ל

תרגיל: למצוא את כל תת חבורות

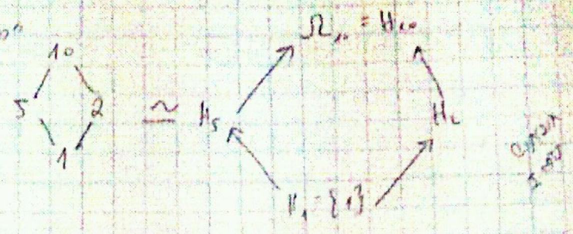
לבד

(א) Ω_{10}

(ב) $\mathbb{Z}_{15}$

הערה: "סריג של עיון"

"סריג המחלקים"



משפט Wilson (Bhaskara VIII ההודי)

עבור $n \geq 2$ טבעי מתקיים

$n = p$ ראשוני $\iff n \mid (n-1)! + 1$

הוכחה: $(\Leftarrow)$: נניח p ראשוני. צ"ל $p \mid (p-1)! + 1$

כרעיון להוכחה ניקח מקרה $p=7$.

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

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

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

$6 \equiv (1)\,2\cdot3\cdot4\cdot5\cdot(6) \mod 7$

באופן כללי: צ"ל: $p \mid (p-1)! + 1$

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

שקול להוכיח: $(p-1) \mod p = (1)\cdot2\cdot3\cdot4\cdots(p-2)\cdot(p-1)$

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

לכל $[a]_p \neq [0]_p$ יש הופכי

אם
אם רק
ורק אם נרצה
נהיה פה זמן מחר.
תן לי דקה להגיע אליך שוב..

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

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

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

חבורה לגבי כפל

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

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

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

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

דין מראן

① $2 \cdot \ldots (p-2)(p-1) \equiv ① \; 1\cdot(p-1) \equiv (p-1) \bmod p$

הוכחת משפט ... לכן $n \mid (n-1)!+1$ ⟸ $\exists u \in \mathbb{Z}: u\cdot n = (n-1)!+1$ (מספיק)

[<] לתשובה?

לכן $v_k = \frac{-(n-1)!}{k}$ ... $k<n$ ... $u \cdot n - (n-1)! = 1$

$u\cdot n + v_k k = 1$ ... $(n,k)=1$ ... $\forall k \in \mathbb{N}: k<n$ ... u_k

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) $\varphi: G \to G/H$ אפי
$g \mapsto gH$ [ההטלה]

(3) $\ker\varphi = H$

Ofit Marzouk :)

הוכחה: נוכיח קודם ש $(aH)\cdot(bH) = (ab)H$ (כפל ב-G. זה לא $*$)

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

(תת קבוצה של S_3 ... $H = \{e,(1,2)\} \le G$ ... 4)

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

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

מהשוויון $(aH)\cdot(bH) = (ab)H$

נובע שאין תלות בנציגים של המחלקה

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

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

לכן $(G/H, *)$ מבנה אלגברי.

המבנה הוא חבורה:

אסוציאטיביות $*$ נובע — מאסוציאטיביות של $(G,\cdot)$.

ניטרלי: $[e] = H \in G/H$ · e ניטרלי ב-G ⟸

$[e] = H$ ניטרלי ב $(G/H, *)$

הופכי ל $[a] = aH \in G/H$:

$[a]^{-1} = [a^{-1}] = a^{-1}H \in G/H$

(2) 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)

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

מש"ל

דוגמאות:

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

$\trianglerighteq$

$H=n\mathbb{Z}$

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

משפט: $H\leq G$

התנאים הבאים שקולים:

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

⇕

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

⇕

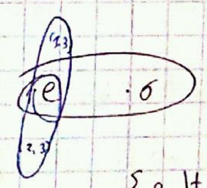
(ג) $gHg^{-1}\subseteq H \quad \forall g\in G$

⇑ שינוי משתנה g^{-1} במקום g.

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

דוגמה: $H=\{e,(1,2)\}\leq G=S_3$

$\sigma \quad \ntrianglelefteq \quad \sigma$

$H=$ 

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

$geg^{-1}=e$.

$\Leftarrow$ נ"ח $H\ntrianglelefteq G$

הגדרה: הצמדה ע"י g בחבורה G היא

$\alpha_g: G\to G$

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

תכונות:

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

הסבר:

הומ':

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

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

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

(2)

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

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

לשני פעולת הרכבה?

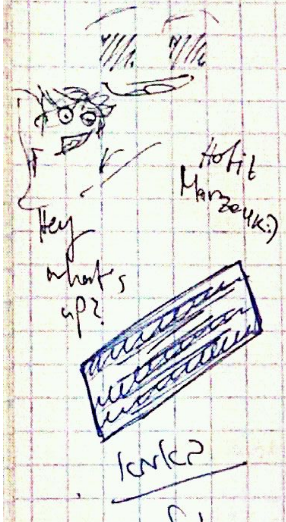
$$\alpha_{g_1} \circ \alpha_{g_2} = \alpha_{g_1 g_2}$$

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

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

⇓

(4) בחבורה אבלית – לכל g, $\alpha_g = id_G$.



<u>דוגמה:</u> אוטומורפיזמים לא פנימיים:

(1) $(\mathbb{C}, +)$ $\quad z \mapsto \bar{z}$ $\quad$ אוט' (של שדה)

$a+bi \mapsto a-bi$

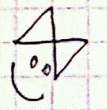
$f \ne id_{\mathbb{C}}$.

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

$G \xrightarrow{f} G$

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

אוטו' (לבדוק) $\ne id_G$. לכן <u>לא פנימי</u>.



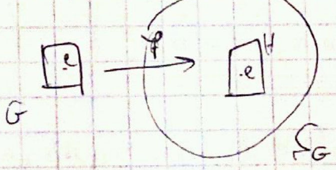
משפט Cayley (קיילי):

לכל חבורה G איזומורפית לתת חבורה של S_G.

⇓

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

<u>הסבר התוצאה:</u> מהמשפט ישר נקבל שקיימת ת"ח $\quad G \cong H \le S_G$



<u>נשים לב שזה שקול:</u> קיים מונו' $G \to S_G$:

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

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

Generated by CamScanner from intsig.com

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

מיון

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

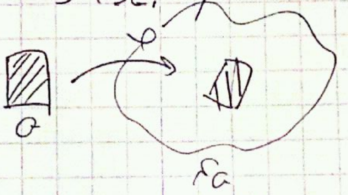
$\gamma \circ \varphi$ — מונומורפיזם (שיכון)

מיון: 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				

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 ש-φ מונומו׳.

קודם כל φ מוגדרת נכון: $l_a \in S_G$ $\forall a \in G$, והפיכה!!

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׳:

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

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

φ חח״ע: נ.ב. $a \neq b \Rightarrow l_a \neq l_b$ (כלומר $\varphi(a) \neq \varphi(b)$)

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

הערה:

{איזומטריות לינאריות של $\mathbb{R}^n$} חבורה מטריצות, איזומורפיזם

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

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

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

ניתן משכן להוכיח: $S_n \hookrightarrow O_n(\mathbb{R})$

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

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

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

...

מסקנה: כל חבורה סופית ניתנת לשכן בחבורה אורתוגונלית.

חבורות של סימטריות:

נניח $A \subseteq \mathbb{R}^n$.

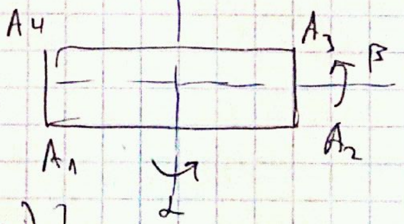
$$Sym(A) := \left\{ \mathbb{R}^n \xrightarrow{f} \mathbb{R}^n \;\middle|\; \begin{array}{r} \text{א) } f \text{ על} \\ \text{ב) } f \text{ שומר מרחקים} \\ \text{ג) } f(A) = A \end{array} \right\}$$

ב) ז"א $\forall u, v \in \mathbb{R}^n \quad \|f(u) - f(v)\| = \|u - v\|$

דוגמאות:

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

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



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

ונח: תוצאה.

נניח קבוצה אחת: אינסופית.

כל פעם שלוקחים מהלך כזה: ואז—

משהו.

Generated by CamScanner from intsig.com

15/08/2011

תרגול V

המשך סימטריות

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

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

(Hofit Marzuk)

הגדרה: תת קבוצה A בחבורה G נקראת <u>קבוצת יוצרים</u> של G,

(סימון $\langle A\rangle = G$), 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: הגדרה שקולה: $\langle A\rangle = G$, כאשר מגדירים $\langle A\rangle$ כתת חבורה ב-G הנוצרת ע"י A

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

שימו לב:

תת החבורה הקטנה ביותר שמכילה את A →

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

הגדרה: "<u>הדרגה</u> של G"

$$\mathrm{rank}(G) = \min\{ |A| \mid \langle A\rangle = G \}$$

תכונות:

(א) ברור: $\mathrm{rank}(G) \le |G|$.

<u>הסבר:</u> ניקח $A := G$

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

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

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

$A = \{a, b\}$

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

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

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

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

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

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

$(0 \le c_1, c_2, c_3 \le 2$ (או)

Generated by CamScanner from intsig.com

הערה כללית: אם החבורה היא $(G,+)$ אז:

$$\langle A\rangle = \{ k_1a_1 + k_2a_2 + \dots + k_na_n \mid a_i \in A,\ k_i \in \mathbb{Z} \}$$

מקרה פרטי של ההגדרה הנ"ל עבור פעולה חיבורית.

ⓐ $G = \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$.

$\text{rank}(G) = 3$

$$g = k_1e_1 + k_2e_2 + k_3e_3, \quad k_i \in \mathbb{Z}$$

ⓑ $\text{rank}(\mathbb{Z}^n) = n$

דוגמה חשובה:

$\text{rank}(D_n) = 2$.

τ - שיקוף
a - סיבוב

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

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

⚠ τ אחד מהשיקופים. כל שיקוף הסדר שווה ל-2. כלומר

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

$\Downarrow$

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

$\Downarrow$

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

$$D_n = \langle \underbrace{a,\tau}_{\text{יוצרים}} \mid \underbrace{a^n = e,\ (a^k\tau)^2 = e}_{\text{יחסים}} \rangle \quad \boxed{0\le k\le n-1}$$

$n \ge 3$

$\Downarrow$

$\text{rank}(D_n) = 2$.

הגדרה: חבורה G נקראת נוצרת סופית (נ"ס)
אם קיימת תת קבוצה <u>סופית</u> A כך ש $\langle A\rangle = G$.
כלומר אם $\text{rank}(G) < \infty$ סופי.

למשל:

ⓐ כל חבורה סופית היא נ"ס (כי $\text{rank}(G) \le |G|$)

ⓑ $\mathbb{Z}^{100}$

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

תכונות נוספות של S_n

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

1) S_n קומוטטיבית $\Longleftrightarrow$ $n \in \{1,2\}$

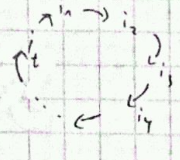
2) $|S_n| = n!$

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

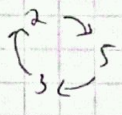
שיכון טבעי $S_n \hookrightarrow S_m$ $\forall n \le m$

הגדרה: עגל (או מחזור) באורך t

סימון: $\underbrace{(i_1\ i_2\ i_3\ \dots\ i_t)}_{\text{שונים}} \in S_n$, $t \le n$ 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: $(2,4)$ $\quad (i,j)$ "חילופים" $(i,j)^2 = e$. $\quad i \neq j$

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

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:

$1 \xrightarrow{\alpha} 3 \xrightarrow{\alpha} 7 \to 2 \to 6$ (חוזר ל-1) $\qquad 4 \to 10$ (חוזר) $\qquad 5 \to 14 \to 12$ (חוזר)

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

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

Generated by CamScanner from intsig.com

תכונות:

א) sign תמיד הומומורפיזם

$$\forall \alpha,\beta \in S_n \qquad sign(\alpha\circ\beta) = sign(\alpha)\cdot sign(\beta)$$

sign אפימורפיזם $\Leftrightarrow n \geq 2$

ב)

$$sign(i_1,\dots,i_t) = \begin{cases} 1 & t=2k-1 \\ -1 & t=2k \end{cases}$$

למשל:

$sign(2,5) = sign(i,j) = -1$

$sign(2,5,3) = 1$

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

$sign(e) = 1$

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

ד)

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

הסבר:

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

($\mathbb{Z}_2$ אבלי!)

ה) הגרעין של sign:

$Ker(sign) = \{$ 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: צ"ל $ker f = H \trianglelefteq X$

שקול להוכיח $x h x^{-1} \in H \qquad \forall h \in H \ \forall x \in X$

שקול להוכיח: $f(xhx^{-1}) = e_Y$

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

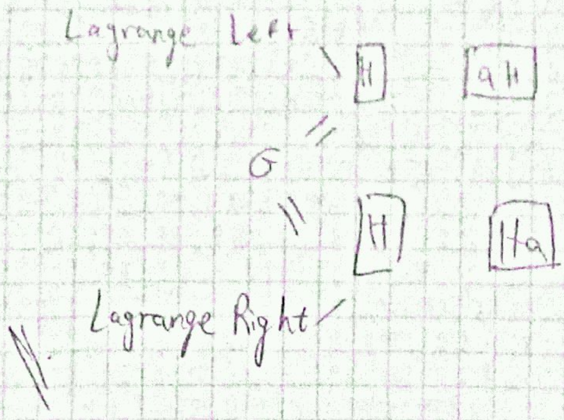
דרך אחרת להוכיח ש- $A_n \trianglelefteq S_n$ נורמלית מהטענה הבאה:

טענה: באופן כללי

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

Generated by CamScanner from intsig.com

נושא: ניקה Hפ



$[S_n : A_n] = 2$

הוכחה:

$S_n = \boxed{A_n} \cup \boxed{\tau A_n}$

$\tau := (1,2)$

A_n ↓ זוגיים; τA_n ↓ אי זוגיים — 2 קוסטים

$|A_n| = |\tau A_n|$

$\Downarrow$

$[S_n : A_n] = 2$

מס' התמורות הזוגיים → $\boxed{|A_n| = \frac{n!}{2}}$ ∎

⑧ **הצמדה ב- S_n:**

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

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

דוגמה: $\sigma = (2,4)$

$g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \in S_4$

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

מסקנה: $g\sigma g^{-1} = \sigma$

שקול: $g\sigma = \sigma g$ (מתחלפים).

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

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

מסקנה: הצמדה לא משפיעה על האורך של עגול ועל "הטיפוס" של תמורה. (מבנה)

אם $\alpha = \sigma_1 \sigma_2 \cdots \sigma_r$ מכפלה של ציקלים

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

למשל:

g_1 $\quad \alpha = (2,4)(1,5,3)$

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

מסקנה: לפי הטענה, כל גרעין תהיה נורמלית. ההפך גם נכון!

ט"ל: כל $G \trianglerighteq H$ אפשר להציג כגרעין של הומומורפיזם מתאים.

זה נובע ממשפט חבורת מנה.

תזכורת: אם $H \trianglelefteq G$ אזי $(G/H, *)$ חבורה (שנקראת חבורת מנה)

אז $p: G \to G/H$, $g \mapsto gH$

$\ker p = H$

משפט: לכל חבורה G מתקיים (Y חבורה)

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

דוגמאות נוספות של תת"ח נורמליות:

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

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

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

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

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

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

(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) $[G:H] = 2 \Rightarrow H \trianglelefteq G$

למשל:

א) $A_n \trianglelefteq S_n$

ב) $\langle a \rangle = \{e, a, \ldots, a^{n-1}\} =: C_n \trianglelefteq D_n$ $\quad (n \geq 3)$

$\quad n \qquad 2n$

ג) $D_n / C_n \cong \Omega_2$

Generated by CamScanner from intsig.com

(ד)

Hofit Marzouk :)

<u>שאלה:</u> מה הן התמונות האפימורפיות של חבורה נתונה G?
(עד כדי איזומורפיזמים)

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

<u>דוגמא</u>: הטלה טבעית $G \xrightarrow{p} G/H$ אפי

<u>תשובה</u>: כל תמונה אפימורפית היא באה בדרך של חבורת מנה.

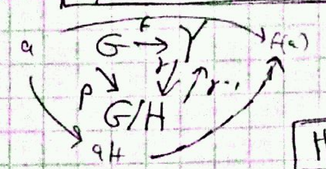
Hofit Marzouk :)

<u>משפט Noether</u> (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



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

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

<u>הוכחה</u>: <u>בניית γ</u>: (הגדיר)

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

<u>הערה</u>: 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!

<u>הוכחה</u> $f(a_1) = f(a_2) \Leftarrow a_1H = a_2H$ (כאשר $a_1H = [a_1]$, $a_2H = [a_2]$). מכאן $\gamma([a_1]) = \gamma([a_2]) \Leftarrow [a_1] = [a_2]$ (כאשר $\gamma([a_1]) = f(a_1)$, $\gamma([a_2]) = f(a_2)$).

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

γ פונ' <u>על</u>: זה נובע מהבניה של γ, כי אם $y \in Y$ אז קיים $x \in G$ ע"כ $f(x) = y$ (כי f על).

מצד שני

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

$xH \mapsto y$. הוכחנו על!!

$[x] = xH$

$[y] = yH$

<u>הומומורפיזם γ:</u>

צריך γ: $\gamma: G/H \to Y$

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

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

<u>מהכאן:</u>

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

$$\| \text{ הומ׳ } f$$

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

הוכחנו γ איזומורפיזם

$f = \gamma \circ p$ ישר מההגדרה.

משל.

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

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

$$|Y| \,\big|\, |G|$$

<u>הסבר</u>: לפי לגרנז':

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

$|G/H| = |Y|$

$\|$

$[G:H]$

מצד שני, ממשפט האיזו I:

כאשר $H = \ker f$

בהכרח $|Y| \,\big|\, |G|$. משל.

<u>תוצאה 3</u>: לכל הומומורפיזם $G \xrightarrow{f} Y$ מתקיים:

$$\boxed{Im f \cong G/\ker f}$$

<u>דוגמה 1</u>: למצוא תמונות אפימורפיות של:

(א) $\mathbb{Z}$

(ב) $\mathbb{Z}_{15}$

(ג) D_3

<u>תשובה:</u>

א) {חבורות ציקליות}. <u>הסבר:</u> ציקלית כי $\{\mathbb{Z}/H \mid H \trianglelefteq \mathbb{Z}\}$

אבליות ←

$$= \{\mathbb{Z}/H \mid H \leq \mathbb{Z}\}$$

$$= \{\mathbb{Z}/H \mid n\mathbb{Z} \quad n \in \{0,1,2,\dots\}\}$$

$n=0$: $\mathbb{Z}/\{0\} \cong \mathbb{Z}$

$n=1$: $\mathbb{Z}_1 = \mathbb{Z}/\mathbb{Z} \cong \Omega_1 = \{1\}$

$n \geq 2$: $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$

בגלל משפט מיון חבורות ציקליות (קב) את התשובה.

ב) $\{\mathbb{Z}_n \mid n|15\}$

ת״י (נורמליות כי $\mathbb{Z}_n$) $H \trianglelefteq \mathbb{Z}_n$

$\|H\|$	G/H חבורה ציקלית (כי תמונה של ציקלית היא ציקלית)
1	$\mathbb{Z}_{15}/\{0\} \cong \mathbb{Z}_{15}$
3	$[15:3]=5$ $\mathbb{Z}_5$
5	$\mathbb{Z}_3$
15	$\mathbb{Z}_1$

ג) <u>תשובה:</u> $\{D_3, \mathbb{Z}_1, \mathbb{Z}_2\}$

(Ω_1) (Ω_2)

<u>הסבר:</u> {תמונות אפימורפיות של D_3}

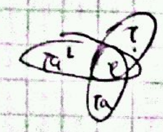
$$= \{D_3/H \mid H \trianglelefteq D_3\}$$

$$= \left\{D_3/H \;\middle|\; H=\{e\},\ H=D_3,\ H=C_3\right\}$$

$D_3/\{e\} \cong D_3$

$D_3/D_3 \cong \mathbb{Z}_1$

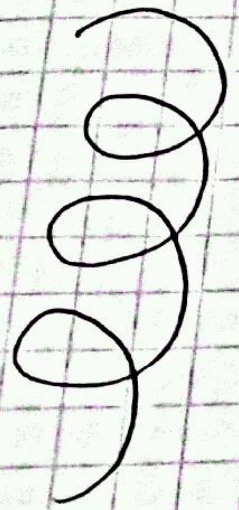
$D_3/C_3 \cong \mathbb{Z}_2$



לא נורמלי ←

<u>תת חבורות 2 איברים הם:</u> $\{e,\tau\}$ (H_1), $\{e,\tau a\}$ (H_2), $\{e,\tau a^2\}$ (H_3)

דוגמא 2: הוכח ש $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$



פתרון: למצוא $\cong$ ע"י משפט איזו' I.

צ"ל למצוא 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 ו'
הרצאה VI

ב' 8.29 יש שיעור השלמה
ב-9:00

תזכורת: $\mathbb{R}/\mathbb{Z} \simeq \mathbb{T}$

$\mathbb{R} \to \mathbb{T}$, $f(t) = cis(2\pi t)$, $\ker f = \mathbb{Z}$, $\mathbb{R}/\ker f$

תרגול: $\mathbb{T} := \{ z \in \mathbb{C} \mid \|z\| = 1 \}$

הוכח $\mathbb{R}^2/\mathbb{Z}^2 \simeq \mathbb{T}^2$

טורוס - 2 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-$\mathbb{T}$"

לא קיים (בכלל) קיים n כך ש z^n שייך לאפס

הערה: $O_2(\mathbb{R}) \geq \left\{ \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \right\} \simeq \mathbb{T} \leq \mathbb{C}^*$

של מט' אורתוגונליות 2 x 2

$0 \leq \alpha \leq 2\pi$

לחבורת סיבובים

תרגיל: הוכח שלכל n קיים מונומורפיזם $\mathbb{Z}_n \hookrightarrow O_2(\mathbb{R})$ (או Ω_n).

הערה לגבי מ.ג: "במשחק 15" המצב הנתון $\sigma \in S_{15}$ הוא פתיר $\iff \sigma \in A_{15}$ (זוגי!)

$S_n = \langle (12), (12\ldots n) \rangle$, $\text{rank}(S_n) = 2$, $|S_n| = n!$ *

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \hookrightarrow S_8$

$\text{rank}(\mathbb{Z}_2^3) = 3 > \text{rank}(S_8) = 2$

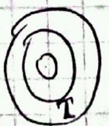
עוד תרגילים לגבי משפט האיזו' I

הוכח:

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



חבורת מנה של האיברים הם מעגלים

משפט האיזומורפיזם II:

נניח $A \leq G$, $H \trianglelefteq G$ אזי:

① $AH \leq G$, $H \trianglelefteq AH$, $A \cap H \trianglelefteq A$

② $AH/H \simeq A/A\cap H$

רעיון ההוכחה של ②:

מבוסס על משפט האיזו' I. מגדירים $f: A \to AH/H$, $\ker f = A\cap H$

$f(a) = aH$

דוגמה: $(4\mathbb{Z}+6\mathbb{Z})/6\mathbb{Z} \cong 4\mathbb{Z}/4\mathbb{Z}\cap 6\mathbb{Z}$

מצד אחד: $(4\mathbb{Z}+6\mathbb{Z})/6\mathbb{Z} = 2\mathbb{Z}/6\mathbb{Z}$

ציקלי עם 3 אלמנטים

מצד שני: $4\mathbb{Z}/4\mathbb{Z}\cap 6\mathbb{Z} = 4\mathbb{Z}/12\mathbb{Z}$

שהוא איזומורפי ל- $\mathbb{Z}_3$

מסקנה: מתקיים $[AH:H] = [A:A\cap H]$ (מסקנה ממשפט איזו' II.)

משפט האיזומורפיזם III: (הצמצום)

נניח $H \trianglelefteq G$, $N \trianglelefteq G$, $N \leq H$ אזי:

$$\left((G/N)/(H/N)\right) \cong G/H$$

דוגמה: $(\mathbb{Z}/24\mathbb{Z})/(6\mathbb{Z}/24\mathbb{Z}) \cong \mathbb{Z}/6\mathbb{Z}$

תכונות של מכפלה קרטזית של חבורות:

אם X, Y חבורות אז מגדירים מכפלה קרטזית של חבורות בצורה הבאה:

$X \times Y := \left\{ (x,y) \;\middle|\; \begin{matrix} x\in X \\ y\in Y \end{matrix} \right\}$ קבוצה

הפעלה רכיב רכיב: $(x_1,y_1)*(x_2,y_2) := (x_1x_2, y_1y_2)$

Generated by CamScanner from intsig.com

דוגמה: $K_4 \simeq \Omega_2 \times \Omega_2$ $(\mathbb{R}^2,+)$

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 "סכום ישר" של חבורות.

וגם לאוסף $\{X_i\}_{i\in I}$ של חבורות, I קבוצה (לא מגבלה על העוצמה)

$$\prod_{i\in I} X_i = \left\{ I \xrightarrow{f} \bigcup_{i\in I} X_i \ ,\ f(i)\in X_i \right\}$$

$$f := (x_i)_{i\in I} \ ,\quad x_i = f(i) \in X_i$$

$$\boxed{(x_i)_{i\in I} * (x_i')_{i\in I} = (x_i \cdot x_i')_{i\in I}}$$

$\left(\prod_{i\in I} X_i, *\right)$ חבורה.

סגירות: $(x_i)_{i\in I} * (x_i')_{i\in I} = (x_i \cdot x_i')_{i\in I}$

ניטרלי: $(e_i)_{i\in I}$ e_i ניטרלי של X_i

הפכי: ל־ $(x_i)_{i\in I}$ שווה ל־ $(x_i^{-1})_{i\in I}$.

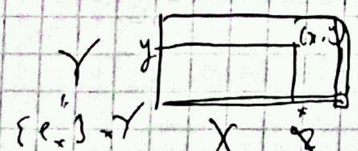
דוגמאות: (א) $(\mathbb{R},+)^n = (\mathbb{R}^n,+)$

(ב) $(\mathbb{R}^{\mathbb{N}},+)$ חבורה של סדרות עם חיבור רגיל

$$\underset{\text{חיבור}}{\mathbb{Z}_2^{\mathbb{N}}} \simeq \Omega_2 := \left\{ (x_n)_{n\in\mathbb{N}} \ \middle|\ x_n \in \{-1,1\} \right\}$$
כפל

ניטרלי ל־ $X*Y$ שווה $e_{X*Y} = e = (e_X, e_Y)$

הטלות:



$X*Y \xrightarrow{\pi_1} $, $X*Y \xrightarrow{\pi_2}$

$\pi_1(x,y) = x$ $\pi_2(x,y) = y$

באופן כללי: $x \in \prod_{i\in I} X_i \xrightarrow{\pi_{i_0}} X_{i_0}$

$$\pi_{i_0}(x_i),\ \pi_{i_0}\left((x_i)_{i\in I}\right) = x_{i_0}$$

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 ש $X \times Y$: $\ker \pi$

תכונה חשובה: $\prod_{i\in I} X_i$ אבלי $\Leftrightarrow$ X_i אבלי

הקשר והסבר:

$$X_{i_0} \longrightarrow \prod_{i\in I} X_i$$

$$x \mapsto (x_i)_{i\in I} \quad \begin{cases} x_i = e_i & i \neq i_0 \\ x_{i_0} = x & i = i_0 \end{cases}$$

הערה: אם $\prod X_i$ ציקלי $\Leftarrow$ X_i ציקלי $\forall i$

הסבר: תכונה קודמת ואם תיחשב ציקלי, גם ציקלי

דוגמה: Ω_2 ציקלי אבל $\Omega_2 \times \Omega_2$ לא ציקלי.

הערה: נוכיח בהמשך $\mathbb{Z}_n \times \mathbb{Z}_m$ ציקלי $\Leftrightarrow (n,m)=1$

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.

$$X \times Y \longrightarrow$$

להשלים!

תוצאה:

$$\{e_X\}\times Y \trianglelefteq X\times Y$$

$$X\times \{e_Y\} \trianglelefteq X\times Y$$

$$X\times Y / \{e_X\}\times Y \simeq X$$

~~$X\times Y / X\times\{e_Y\}$~~

$$X\times Y / X\times \{e_Y\} \simeq Y$$

תכונה:

אם $G:=X\times X$ הפונקציה

$$G\xrightarrow{\varphi} G$$
$$(x_1,x_2)\mapsto(x_2,x_1)$$

חילוף רכיבים (מיקום רכיב) [illegible]

היא אוטומורפיזם.

הכלל:

$G:=X\times\cdots\times X=X^n$. לכל תמורה $\sigma\in S_n$ מגדירים אוט'

$G\xrightarrow{\varphi_\sigma}G$: $\varphi_\sigma(x_1,\dots,x_n)=(x_{\sigma(1)},x_{\sigma(2)},\dots,x_{\sigma(n)})$

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, אז' $\prod X_i\xrightarrow{f=\prod_{i\in I}f_i}\prod Y_i$

$(x_i)_{i\in I}\mapsto(f_i(x_i))_{i\in I}$ גם הומומורפיזם (הוכחה קלה)

דוגמאות

① א. הוכח שקיים איזו' $\mathbb{Z}_{15}\times D_3\simeq\Omega_{15}\times D_3$

$$\mathbb{Z}_{15}\xrightarrow{f_1}\Omega_{15}$$

$$D_3\xrightarrow{f_2=id}D_3$$

2 הוכח $S_3\times\Omega_{25}\simeq C_{25}\times D_3$ אם ידוע ש $S_3\simeq D_3$

הסדר: איזו' $S_3\xrightarrow{f_1}D_3$, איזו' $\Omega_{25}\xrightarrow{f_2}C_{25}$ (שניהם ציקליות מאותו 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׳

$$C_{25}\xrightarrow{f_1=h_2\circ h_1} C_5$$

$$C_{25}\xrightarrow{h_1} C_{25}/H \xrightarrow[\cong]{h_2} C_5$$

משפט $H\le C_{25}$, $|H|=5$

$$D_n\xrightarrow{sign}\Omega_2 \qquad D_{100}\xrightarrow{f_2=\text{"sign"}}\Omega_2=\{1,-1\}$$

סיבובים $a^i\to 1$

שיקופים $a^i\tau\to -1$

ו־S_3 אפשר לשלוח אפי׳ את כולו לאיבר היחידה

(ע״כ 3 ...)

$$S_3\times D_{100}\times C_{25}\xrightarrow{f} C_5\times\Omega_2$$

$$f(x,y,z)=(f_1(z),\ sign(y))$$

משפט פירוק של חבורות

תהי $(G,\cdot)$ חבורה. התנאים הבאים שקולים:

1. $G\cong X\times Y$.

2. קיימות תת׳ X,Y (לא בהכ׳ נורמליות) כך ש:

א. $Y\trianglelefteq G \wedge X\trianglelefteq G$

ב. $X\cap Y=\{e_G\}$

ג. $X\cdot Y=G$

הוכחה

$\boxed{1}\Rightarrow\boxed{2}$

א. ראינו בהרצאה: $X\cong X\times\{e_Y\}\trianglelefteq X\times Y \wedge Y\cong\{e_X\}\times Y\trianglelefteq X\times Y$

ב. $X\times\{e_Y\}\cap\{e_X\}\times Y=\{(e_X,e_Y)\}=e_{X\times Y}\overset{\text{איז׳}}{=}e_G$

ג. יהי $g=(x,y)\in G$, $g=(x,e_y)*(e_x,y)$

$\qquad\in X \qquad \in Y$

2 ⟸ 1

נוכיח תחילה: שמתקיים $xyx^{-1}y^{-1}=e \iff xy=yx \quad \forall x\in X,\ \forall y\in Y$

הגדרה
יהיו $x,y\in G$ מגדירים <u>קומוטטור</u> של (x,y): $[x,y]:=xyx^{-1}y^{-1}\in G$

נבדוק ש $[x,y]=xyx^{-1}y^{-1}=e$

$$xyx^{-1}y^{-1}=(xyx^{-1})y^{-1}\underset{Y\trianglelefteq G}{\in} Y$$

$$xyx^{-1}y^{-1}=x(yx^{-1}y^{-1})\underset{X\trianglelefteq G}{\in} X$$

לכן

$$[x,y]\in X\cap Y \underset{(2)}{=}\{e\}$$

הוכחנו (*) $\boxed{xy=yx \quad \forall x\in X,\ y\in Y}$

נגדיר

$$X\times Y\xrightarrow{\ \varphi\ }G$$

$$(x,y)\longmapsto x\cdot y$$

② ⟸ φ <u>על</u>

ג) <u>φ הומ':</u>

$$\varphi((x_1,y_1)*(x_2,y_2))=\varphi(x_1x_2,\ y_1y_2)=(x_1x_2)(y_1y_2)=x_1x_2y_1y_2$$

$$\varphi(x_1,y_1)\cdot\varphi(x_2y_2)=(x_1y_1)\cdot(x_2\cdot y_2)=x_1(y_1x_2)y_2\underset{(*)}{=}x_1x_2y_1y_2$$

✓

ד) <u>חח"ע</u>, צריך להוכיח שהגרעין הוא טריוויאלי:

$$\ker\varphi=\{(x,y)\in X\times Y:\varphi(x,y)=e\}=\{(x,y)\in X\times Y: xy=e\}$$

$$=\{\quad : x=y^{-1}\}=\{\quad : x=y=e\}$$

(האיבר היחיד בחיתוך הוא e)

$$=\{(e,e)\}=\{e_{X\times Y}\}$$

Generated by CamScanner from intsig.com

משפט הקרטזיון (ציקליות של המכפלה)

התנאים שקולים:

1. $C_m \times C_n$ ציקלית (ולכן איזומורפית C_{mn})
2. $(m,n)=1$

הוכחה

$1 \Leftarrow 2$

אם נניח בשלילה ש $(m,n)=d>1$ נראה שלכל איבר $g\in C_m\times C_n$

מתקיים $O(g) < mn$

$g=(x,y)\in C_m\times C_n$

$x\in C_m \Leftarrow O(x)\,|\,m$

$y\in C_n \Leftarrow O(y)\,|\,n$

$$g^{\frac{mn}{d}}=(x,y)^{\frac{mn}{d}}=((x,e)\cdot(e,y))^{\frac{mn}{d}}$$

$$=\left(x^{\frac{mn}{d}},y^{\frac{mn}{d}}\right)=\left((x^m)^{\frac{n}{d}},(y^n)^{\frac{m}{d}}\right)=(e,e)=e$$

מכאן $O(g)\le \frac{mn}{d} < mn$

$1 \Rightarrow 2$

נשתמש במשפט הפירוק עבור חבורה $G=C_{mn}$

C_{mn} ציקלית עם mn איברים.

לפי משפט מיון ת"ח בחבורה ציקלית קיימות ת"ח $X\le C_{mn}$ עם m איברים

$Y\le C_{mn}$ עם n איברים

נראה כי מתקיימים התנאים א, ב, ג במשפט הפירוק:

א. ברור $\left\{ \begin{array}{l} X\trianglelefteq C_{mn} \\ Y\trianglelefteq C_{mn} \end{array}\right.$ כי C_{mn} אבלית (ציקלית)

ב. $X\cap Y=\{e\}$ כי

$X\cap Y\le X \Rightarrow |X\cap Y|\,\big|\,|X|=m$

לגרנז'

$X\cap Y\le Y \Rightarrow |X\cap Y|\,\big|\,|Y|=n$

ניון כי $(m,n)=1$ ולכן $|X\cap Y|=1 \Leftarrow X\cap Y=\{e\}$

↑ $X\cap Y$ ת"ח ולכן $e\in X\cap Y$ בהכרח

Generated by CamScanner from intsig.com

ג. צ"ל $X\cdot Y=C_{mn}$

נניח a יוצר של C_{mn}. $X\cdot Y\subseteq C_{mn}$ כמובן, כי אלו ת"ח.

נותר להוכיח $C_{mn}\subseteq X\cdot Y$, שקול להוכיח $a\in X\cdot Y$:

$$a^n\in X=\langle a^n\rangle$$

מכיון ש $o(X)=m=o(a^n)$

$$a^m\in Y=\langle a^m\rangle$$

לפי משפט אוקלידס קיימים $u,v\in\mathbb{Z}$ כך ש

$$u\cdot m+v\cdot n=1 \longleftarrow 1=(m,n)$$

$$a=a^1=a^{um+vn}= \text{[struck through]}$$

$$=a^{vn+um}=\underbrace{(a^n)^v}_{\in X}\cdot\underbrace{(a^m)^u}_{\in Y}\in X\cdot Y \quad \checkmark$$

מש"ל

-הפסקה-

<u>תוצאה:</u> $\mathbb{Z}_m\times\mathbb{Z}_n\cong\mathbb{Z}_{mn} \iff (m,n)=1$.

מכאן לכל $(m,n)=1$ המערכת פתירה

$$\begin{cases} x\equiv a_1 \mod m \\ x\equiv a_2 \mod n\end{cases}$$

<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

$$\begin{cases} x\equiv a_1 \mod m_1 \\ x\equiv a_2 \mod m_2 \\ \vdots \\ x\equiv a_t \mod m_t\end{cases}$$

הא פתירה.

והפתרון מודולו $m=m_1m_2\cdots m_t$ הוא יחיד.

<u>הכללה:</u> $\mathbb{Z}_m\cong\mathbb{Z}_{m_1}\times\mathbb{Z}_{m_2}\times\cdots\times\mathbb{Z}_{m_t}$, $(m_i,m_j)=1$

$m=\prod_{i=1}^{t} m_i$

$$[k]\mapsto([k]_{m_1},[k]_{m_2},\ldots,[k]_{m_t})$$

Generated by CamScanner from intsig.com

מיון חבורות אבליות (סופיות):

1. כל חבורה אבלית סופית $\cong$ מכפלה (סופית) של חבורות ציקליות (סופיות)
2. כל חבורה אבלית נ"ס $\cong$ מכפלה סופית של חבורות ציקליות.

$\Downarrow$

דוג':

$$\mathbb{Z}_{40}\times\mathbb{Z}\times\mathbb{Z}_{36}\times\mathbb{Z}_{8}\times\mathbb{Z}_{125}\times\mathbb{Z}$$

3. G חבורה אבלית נ"ס היא תמונה אפימורפית של $\mathbb{Z}^n$

הערה: אפשר להוכיח בלי משפט האיזו' I (לבדוק!) (A).

שאלה: כמה חבורות אבליות קיימות (עד כדי $\cong$) עם n איברים?
ואיך נבנה אותן? A

דוגמאות: G אבלית. $|G|=n$.

א) $n=p$ ראשוני. $G\cong C_p$ (תוצאה מ-Lagrange)
אחת! (עד כדי $\cong$).

ב) $n=p^2$.

$C_{p^2} \rightarrow$ $2=2$

$C_p\times C_p \rightarrow$ $2=1+1$

2 חבורות. (עד כדי $\cong$)

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 סוגים.

ד) $n=p^5$

$5=5$

$5=4+1$

$5=3+1+1$

$5=2+2+1$

$5=2+1+1+1$

$5=1+1+1+1+1$

$p(5)=7$

למשל, C_{p^5} A

מס' חלוקות

$$m_1\ge m_2\ge\dots\ge m_t\ge 1$$

$$m=m_1+\dots+m_t$$

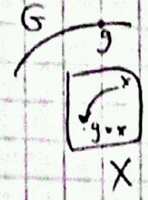
Generated by CamScanner from intsig.com

[illegible]

<u>הגדרה:</u> פעולה (action) של חבורה G על קבוצה $X\neq\emptyset$ היא פונקציה

$$G\times X\xrightarrow{\alpha}X$$

$$(g,x)\mapsto g*x=\alpha(g,x)$$



כך שמתקיים:

$\boxed{A_1}$ $\quad e*x=x \quad \forall x\in X$

$\boxed{A_2}$ $\quad g_1*(g_2*x)=(g_1g_2)*x$

אז אומרים: X הוא G-מרחב (G-space) (G,X,α) או (G,X)

> <u>הערה:</u> במקרה של α רציף עם G, X <u>מרחבים טופולוגיים</u> אז (קבל) 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 $[x]:=\{y\in X \mid y=g*x \ \exists g\in G\}=G*x$

ב) אומרים פעולה טרנזיטיבית (הומוגנית) 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 $\quad$ G^x $\quad$ 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 $\quad F:=\{G \text{ נק' שבת של}\}=\bigcap_{g\in G}X_g$

<u>הערה 1:</u> באופן דומה מגדירים פעולה מימין $\quad X\times G\to X$.

(זה חשוב בפעולות מעל פונקציות).

2) מגדירים גם פעולה של מונואיד (אגודה) אז מתקיים רק $\boxed{A_2}$.

דוגמאות:

1) נניח $(G,\cdot)$ חבורה.

נגדיר פעולה של G מעל $X:=G$.

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

שים ♥

א) (2) הכללה של (1) $(H=\{e\})$

ב) הפעולה ב-(2) (וכן גם ב-(1)) טרנזיטיבית. לא $tH\in G/H$ $t*H=tH$.

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! ואין נקודת שבת.

3) הצמדות:

לכל חבורה G ניקח $X:=G$ ונגדיר: $G\times G\to G$

$$(g,x)\mapsto g*x:=gxg^{-1}\ (\in G)$$

$$e*x=exe^{-1}=x \quad \boxed{A_1}$$

$$g_1*(g_2*x)=g_1(g_2xg_2^{-1})g_1^{-1}=(g_1g_2)*x \quad \boxed{A_2}$$

✓

כאן נקודות שבת = המרכז של G:

$$F=\{x\in G \mid \forall g\in G: g*x=x\}=\{x\in G\mid \forall g\in G: gxg^{-1}=x\}=$$

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

⇐ הערה: פעולת הצמדה של G מעל G ($G\times G\to G$) היא טריוויאלית (היא מציבה לוקלי) אמ"ם G אבלית.

במקרה הפרטי של $G = S_n$:

א= מס' מסלולים (= מס' מחלקות צמידות ב-S_n) שווה $k = p(n)$.

למשל: $n=5$,

$p(5) = 7$. ההסבר בנוסחה של הצמדות ב-S_n: $g(i_1, i_2, \dots, i_n)g^{-1} = (g(i_1), \dots, g(i_n))$ הטיפוס נשמר.

תשובה: תמיד קיים $g \in S_n$ כך שאפשר להגיע לכל האיברים באותו טיפוס

$x = (1\ 2\ 3\ 4\ 5)$

$[x] = \{(i_1, i_2, i_3, i_4, i_5)\}$

למשל: $y = (3\ 5\ 1\ 4\ 2)$ (x-מאותה מחלקה)

ניקח
$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$$
אז $y = gxg^{-1}$ 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 ($G \in$, $e \in$)

$X := Sub(G)$

$$G \times Sub(G) \to Sub(G)$$

$$(g, H) \mapsto gHg^{-1}$$
$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$

הצמדה = אוטומורפיזם → מעביר תת"ח לתת"ח

A_1

A_2

שימו לב: הפעולה הצמדה $F = \{H \le G \mid H \trianglelefteq G\}$ נקודות שבת הן תת"ח נורמליות ב-G.

5) נניח $G \times X \xrightarrow{\alpha} X$ פעולה. (נגדיר)

$G \times P(X) \xrightarrow{\alpha} P(X)$

$(g, A) \mapsto g * A := \{g * a \mid a \in A\}$

A_1 ≙

A_2

6) **דוגמת מפתח:**

נניח X קבוצה לא ריקה, $G = S_X$ חבורה סימטרית

(מגדירים) **פעולה טבעית:**

$S_X \times X \to X$

$(g, x) \mapsto g * x = g(x)$

A_1 ≙

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 מושרה $G \times X \to X$

$(g, x) \mapsto g(x)$

הערה: כל פעולה $G \times X \to X$ היא בעצם פעולה שבאה דרך צמצום של דוגמה מהסוג $S_X \times X \to X$

הסבר: (דומה למשפט קיילי): (נגדיר "הזזה"

$\alpha_g : X \to X \in S_X$

$x \mapsto g * x$

כי $\alpha_g^{-1} = \alpha_{g^{-1}}$

אז נגדיר $G \xrightarrow{\varphi} S_X$ (הומומורפיזם קיילי) הומומורפיזם

$g \mapsto \alpha_g$

לאו תמיד מונומורפיזם.

חזרה לפעולה: דרך $S_X \times X \to X$

$G \times X \to X$

$(g, x) \mapsto \varphi(g)(x)$

דוגמה: $X=\{1,2,3,4,5,6\}$

$G=\langle(1,2),(3,4,5)\rangle \leq S_6$ עם פעולה טבעית

למצוא: מסלולים G_x, X_g, F

פתרון:

$$G=\left\{\begin{matrix} e, & (3,4,5)=a, & (3,5,4)=a^2 \\ \tau=(1,2), & \tau a, & \tau a^2 \end{matrix}\right\} \leq S_6 \qquad |G|=6$$

מסלולים: $[x]=\{g*x\}_{g\in G}$

מסלולים = k:

- $(1 \cdot 2)$: $[1]=\{1,2\}=[2]$
- $(3 \cdot 4 \cdot 5)$: $[3]=\{3,4,5\}=[4]=[5]$
- (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

בסה"כ: 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

סה"כ: 18

הערה: קיבלנו

$$\begin{cases} \sum_{x \in X} |G_x| = 18 \\ \sum_{g \in G} |X_g| = 18 \end{cases}$$

כלומר באופן כללי:

$$\sum |G_x| = \sum |X_g|$$

משפט Burnside

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g|$$

(k ↓ מס' מסלולים)

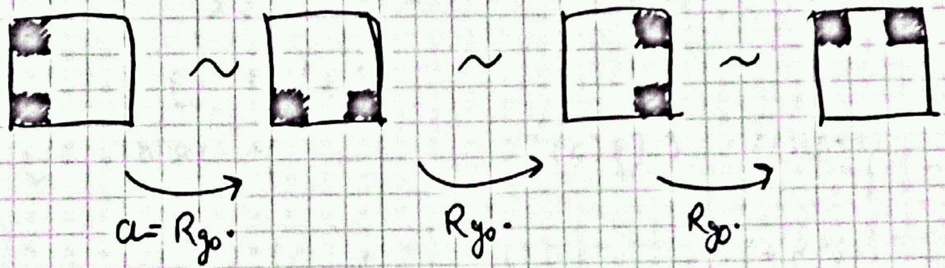
נוכיח בהמשך

בדוגמה $k = \frac{1}{6} \cdot 18 = 3$

שאלה קומבינטורית:

"דוגמה על הלוח":

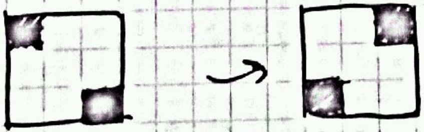
כמה לוחות 3×3 קיימים (עד כדי סיבובים) אם מותר לצבוע ב-2 צבעים קבועים (ש"ל)



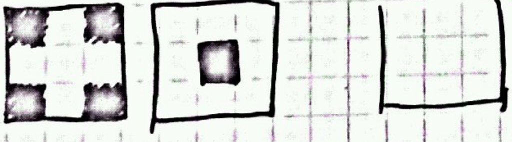
אורך המסלול שווה ל-4.

בחבורה $G = C_4$ יש 4 אלמנטים.

דוגמה למסלול מאורך 2:



דוגמאות למסלול מאורך 1 (נק' שבת):

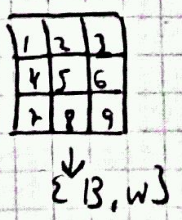


בניית המודל: בונים פעולה כאשר $G = C_4$, 4 אלמנטים

$$X = \{\underbrace{1,2,3,4,5,6,7,8,9}_{Y}\} \xrightarrow{f} \{B, W\}]$$

$$|X| = 2^9.$$

הרעיון



השלב הראשון:

Generated by CamScanner from intsig.com

$G \times Y \to Y$ — יש פעולה טבעית — דוגמה מהתרגול:

$(g,y) \mapsto g * y$

$\langle a \rangle = G = \{e, a, a^2, a^3\}$ $\boxed{e * y = y}$

$a = R_{90^\circ}$ — אם נסובב ב-90° כל קודקוד יעבור ל...

$R_{90^\circ} = a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 1 & 8 & 5 & 2 & 9 & 6 & 3 \end{pmatrix} = (1\,7\,9\,3)(2\,4\,8\,6)$

$R_{180^\circ} = a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \end{pmatrix} = (1\,9)(2\,8)(3\,7)(4\,6)$

$R_{270^\circ} = a^{-1} = a^3 = \begin{pmatrix} \\ \end{pmatrix} = (3\,9\,7\,1)(6\,8\,4\,2)$

פעולה: $G \times Y \to Y$ אינדוק — מגדירים פעולה

$X \times G \to X$

$(f, g) \mapsto f * g$

נגדיר $f * g$ מוגדרת כ-

$(f * g)(y) = f(g(y))$

$\forall y \in Y$

$f * e = f$ $\boxed{A}$ ✓

$(f * g_2) * g_1 = f * (g_2 g_1)$ $\boxed{A}$ ✓

מספר מסלולים:

$k = \frac{1}{|G|} \cdot \sum_{g \in G} |X_g| = \frac{(2^9 + 2^3 \cdot 2 + 2^5)}{4} = 140$

$g \in G$	X_g	$\|X_g\|$
e	$X_e = X$	2^9
a		2^3
a^2		2^5
$a^{-1} = a^3$	$X_{g^{-1}} = X_g$	2^3

שאלה: לפתור שאלה דומה עם לוח 4x4 ב-3 צבעים לגבי פעולת חבורה D_4.
(ניתן סיבובים ושיקופים).

תכונות בסיסיות של פעולות

תהי $G \times X \xrightarrow{\alpha} X$ פעולה.

① $X = \dot{\bigcup}_{x \in X} [x]$ (איחוד זר של המסלולים)

הסבר: נגדיר יחס שקילות ב-X

$x \sim y \overset{def}{\iff} y = g * x$, $\exists g \in G$

לבדוק שהיחס הוא יחס שקילות. Δ

② $G_x \le G$. הסבר: Δ

③ $g * x = y \Rightarrow g G_x g^{-1} = G_y$

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 $g * x = y \Rightarrow x = g^{-1} * y$)

לכן $ghg^{-1} \in G_y$. אז הוכחנו $g G_x g^{-1} \subseteq G_y$.

באופן דומה אפשר להוכיח $\supseteq$

תרגיל.

④ $g * x = y$ (כלומר $x \sim y$) $\Rightarrow |G_x| = |G_y|$

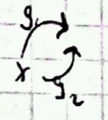
⑤ $X_e = X$, $X_{g^{-1}} = X_g$

⑥ $\forall g_1, g_2 \in G$ $\quad g_1 \equiv g_2 \mod G_x \iff g_1 * x = g_2 * x$

$\Updownarrow$ ← תרגיל

$g_1^{-1} g_2 \in G_x$

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

$$\boxed{f(g * x) = g * f(x)}$$

$\forall g \in G$

$\forall x \in X_1$

$$\begin{array}{ccc} G * X_1 & \longrightarrow & X_1 \\ f \downarrow & & \downarrow f \\ G * X_2 & \longrightarrow & X_2 \end{array}$$

אומרים ש-f <u>איזומורפיזם</u> אם f <u>הומומ' + חח"ע ועל</u>.

$$\begin{array}{ccc} G * X_1 & \rightarrow & X_1 \\ \updownarrow & & \updownarrow \\ G * X_2 & \rightarrow & X_2 \end{array}$$

(7) **משפט (מיון פעולות טרנזיטיביות):**

כל פעולה $G * X \to X$ עם מסלול 1 [illegible] הוא איזומורפית לפעולה

$G * G/H \to G/H$ כאשר $H := G_x$ (אם נבחר $x \in X$).

<u>הוכחה:</u> $y \in X$, $y = g * x$

g_1, g_2

נבחר $x_0 \in X$

$gG_x \simeq$

$G/G_x \ni G_x$

נגדיר f איזו'

$X = [x] = \{g * x\}_{g \in G}$

(נזכיר

$$f: X \to G/G_x$$

$$y = g*x \mapsto gG_x$$

מוגדר היטב כי

(6) $g_1 \equiv g_2 \mod G_x \iff y = g_1 * x = g_2 * x$

$\Downarrow$

$g_1G_x = g_2G_x$

Afit Marzouki

$\oplus G \cong L_2(\mathbb{R})$

Dana Vaknin red 22

חח"ע: נובע שוב מאותה תבנית (6)

על: לכל $gG_x \in G/G_x$ ניקח $X \ni y := g*x$

$f(y) = gG_x$

הומומורפיזם: צ"ל: "f שומרת על הפעולה"

צ"ל: $f(t*y) = t*f(y)$ $\quad \forall t \in G,\ \forall y \in X$

$$f(t*y) = f(t*(g*x)) = f((tg)*x) = (tg)G_x$$

$$t*f(y) = t*f(g*x) = t*gG_x = t(gG_x)$$

מש"ל

(8) משפט: לכל חבורה סופית G ופעולה של G על X מתקיים:

$$|G| = |[x]|\cdot|G_x|$$

מכאן מסקנה: $|[x]| \mid |G|$

הסבר של: אם $G*X \to X$ פעולה, $x \in X$ אז נגביל לפעולה המצומצמת

$G*[x] \to [x]$ מעבר!

לפי המשפט הקודם:

$$\begin{array}{ccc} G*[x] & \to & [x] \\ \updownarrow & & \updownarrow \\ G*G/G_x & \to & G/G_x \end{array} \cong$$

ולכן $|[x]| = |G/G_x| \overset{\text{לגראנז'}}{=} \frac{|G|}{|G_x|}$

$|G| = |[x]|\,|G_x|$

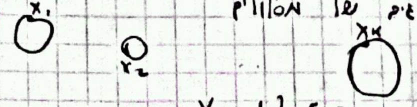
מש"ל

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

$|X| = |[x_1]| + |[x_2]| + \dots + |[x_n]| = \sum_{i=1}^{n} |[x_i]|$ מצד שני לפי (8):

$\Leftarrow$ $|[x_i]| = [G : G_{x_i}]$.

מכאן $\Leftarrow$ $|X| = \sum_{i=1}^{n} [G : G_{x_i}]$.

מש"ל

שאלה: כמה איברים מתחלפים עם $a = (5\ 2\ 3)$ בחבורה S_4?

10) לכל חבורה סופית G מתקיים

$$|G| = |Z(G)| + \sum_{j=1}^{m} [G : C_{x_j}]$$

$x_1, \dots, x_m$ נציגי מחלקות צמידות ב-G, רק ל-$x_i \notin Z(G)$.

הגדרה: הצנטרליזטור של $x \in G$

$C_x := \{ g \in G \mid gx = xg \}$ (ממרכז x)

= מייצב של x לגבי פעולת הצמדה $G \times G \to G$.

הסבר של הנוסחה:

$$|G| = |C(G)| + \sum_{j=1}^{m} |[x_j]| \underset{(8)}{=} |C(G)| + \sum_{j=1}^{m} [G : C_{x_j}]$$

($C(G)$ = מסלולים נקודתיים ב-G)

11) **מסקנה:** אם $|G| = p^n$, ו-p ראשוני, אזי המרכז חייב להיות לא טריוויאלי ($|Z(G)| \neq 1$, כלומר)

הסבר: מ-(10)

$$|G| = |C(G)| + \sum_{j=1}^{m} [G : C_{x_j}]$$

$[G : C_{x_j}]$ מתחלק ב-p לכל j ⇐ מתחלק ב-p, מתחלק ב-p ולכן $|C(G)| \neq 1$ מש"ל

24/08/2011

VIII

שיעור השלמה ב 28.8
9:00

שאלה: כמה איברים מתחלפים עם התמורה $(5,2,3)$ ב-S_7?

פתרון: $C_a = G_a =: \{g\in G \mid gag^{-1}=a\} = \{g\in G \mid ga=ag\}$

(G_a – מייצב)

$G=S_7$ פועלת על עצמה דרך הצמדה.

נוסחה:
$$\boxed{|G_a| = \frac{|G|}{|[a]|}}$$

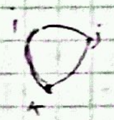
$\Downarrow$

$$|C_a| = \frac{|S_7|}{|[(5,2,3)]|} = \frac{7!}{?}$$

$$[(5,2,3)] = \{(i,j,k) \mid i,j,k\in\{1,\dots,7\}\} = \binom{7}{3}\cdot\frac{3!}{3} =$$

המסלול = מחלקת צמידות

$=$ מס' מעגלים מאורך 3 ב-S_7 $= (i,j,k)=(k,i,j)=(j,k,i) =$



התשובה:
$$|C_a| = \frac{7!}{\binom{7}{3}\cdot\frac{3!}{3}}$$

טענה 1: נניח G חבורת-p. (כלומר $|G|=p^n$, $n\in\mathbb{N}$).

נניח $G\times X\to X$ פעולה. אז תמיד מתקיים:

X_0 פ.מ: $|F| \equiv |X| \mod p$.

הוכחה: $X = \biguplus_{x\in X}[x] = \biguplus_{i=1}^{k}[x_i]$.

$x_1,\dots,x_k$ נציגים של מסלולים.

$$|X| = \sum_{i=1}^{k} |[x_i]|$$

$$|X| = |F| + \sum_{j=1}^{m} |[x_j]| = |F| + \sum_{j=1}^{m}[G:G_{x_j}] \qquad (|[x_j]|>1)$$

$$[G:G_{x_j}] \equiv 0 \mod p \quad \Leftarrow \quad \begin{cases} ([G:G_{x_j}]\neq 1) \\ [G:G_{x_j}] \mid |G| = p^n \end{cases}$$

$\Downarrow$

$$|F| \equiv |X| \mod p$$ ■

משפט: לכל $|G|=p^n$ $\Rightarrow$ $p \mid |C(G)|$ (ולכן $|C(G)|\neq 1$)

p ראשוני, $n\in\mathbb{N}$

טענה 2: נניח G חבורת-p, $G \times X \to X$ פעולה, $p \nmid |X|$.
אזי יש נקודת שבת (שקול: $F \neq \emptyset$).

הוכחה: לפי טענה 1

$$\begin{cases} |F| \equiv |X| \mod p \\ p \nmid |X| \iff |X| \not\equiv 0 \mod p \end{cases}$$

$$\Downarrow$$

$$|F| \not\equiv 0 \mod p$$

$$\Downarrow$$

$$|F| > 0 \text{ בפרט}.$$

מש"ל

משפטי סילו (Sylow)

הגדרות:

(א) G חבורת-p $\underset{def}{\iff}$ $|G| = p^n$, p ראשוני, $n \in \mathbb{N}$.

(ב) $H \leq G$ נקראת תת-חבורה-p אם H היא חבורת-p. (על G אין הגבלות).

(ג) אומרים ש-$H \leq G$ היא תת-חבורה p-סילו $\underset{def}{\iff}$ $\begin{cases} ① \ |H| = p^n \text{ תת-חבורה-}p. \\ ② \ |G| = p^n \cdot m,\ m \in \mathbb{N} \text{ כך ש } (p,m)=1 \end{cases}$

שקול: אם $H \leq K \leq G$ (H p-סילו, K p) כך ש-K תת-חבורה p $\Leftarrow$ $H=K$.

(ד) n_p = מס' תת-חבורות p-סילו.

הערה: יתכן שיש כמה תת-חבורות p-סילו. נוכיח שתמיד קיימת תת-חבורה 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-חבורה 2-סילו. $m = 5^3$

ב. $p=5$: $P_5 = C_{25} \times \{e\} \times C_5$. $m = 2^3$

הערה: בחבורה אבלית תת-חבורה p-סילו הן תמיד יחידות. לה נובע ממשפט II סילו.

2 $G = D_3$, $|G| = 6 = 2 \cdot 3$

א. $p=3$: $P_3 = C_3 \triangleleft D_3$ יחידה! $m=2$. $Syl_3(G) = \{C_3\}$

נזכיר: ממשפטי סילו נובע שתת-חבורה p-סילו $H \leq G$ היא יחידה $\iff$ $H \triangleleft G$.

ב. $p=2$: מה הן תת-חבורות עם 2 איברים? $m=3$

$n_p=$ מספר ת"ח p-סילו.

זכור: $\boxed{n_p | m}$

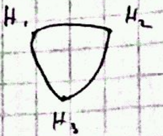
$Syl_p(G)=\{H_1, H_2, H_3\}$.

כאן זוג.

$H_1=\{e,\tau\}$

$H_2=\{e,\tau\sigma\}$

$H_3=\{e,\tau\sigma^2\}$



משפט פירוק של חבורות אבליות סופיות

נניח G חבורה אבלית סופית $|G|=p_1^{k_1}\cdots p_m^{k_m}$ (לפי גורמים ראשוניים שונים) $k_1,\dots,k_m\in N$

אזי G מתפרקת $G\simeq P_1\times\dots\times P_m$, כך ש $|P_i|=p_i^{k_i}$

(Kofit Marzouk)

__הוכחה:__ תהי $(G,+)$ חיבורית.

__טענת עזר I:__ נניח G אבלית: $|G|=m_1 m_2$ ∧ $(m_1,m_2)=1$

אזי

$G_{m_2}=m_1 G$

$G_{m_1}=m_2 G$

כאשר $mG:=\{mx \mid x\in G\}$ (כפולות) $m\in N$

$G_m=\{x\in G \mid o(x)|m\}$

__הוכחת טענה I:__ נראה $G_{m_2}=m_1 G$

$(\subseteq)$: נניח $x\in G_{m_2}$, צ"ל $x\in m_1G$

$(m_1,m_2)=1$

$\Downarrow$

$\exists u,v\in\mathbb{Z}: \ u\cdot m_1+v\cdot m_2=1$

$x=1\cdot x=(u\cdot m_1+v\cdot m_2)x=(u\cdot m_1)x+(v\cdot m_2)x=(um_1)x+0_G=(um_1)x=$

$=m_1(ux)\in m_1G$

($x\in G_{m_2} \Rightarrow m_2x=0_G$)

מכאן $x\in m_1G$.

$(\supseteq)$: נניח $x\in m_1G$ צ"ל $x\in G_{m_2}$

$\begin{cases} x=m_1 y \\ y\in G \end{cases}$

$m_2\cdot x=m_2\cdot m_1\cdot y=|G|\cdot y=0_G$

$m_2x=0_G$

$\Downarrow$

$o(x)|m_2$

$\Downarrow$

$x\in G_{m_2}$.

מש"ל

טענת עזר II: נניח G חבורה אבלית, $|G|=m_1 m_2$ ו- $(m_1,m_2)=1$

אזי
$$\boxed{G \cong m_1G \oplus m_2G}$$
$\oplus$ – סכום ישיר (מקרה פרטי של מכפלה קרטזית של חבורות).

$X = Y_1 \oplus Y_2$
$(y_1,y_2)+(y_1',y_2')$

לפי משפט פירוק חבורות שקול להוכיח ש

1. $m_1G \trianglelefteq G \ , \ m_2G \trianglelefteq G$
2. $m_1G \cap m_2G = \{0_G\}$
3. $m_1G + m_2G = G$

הוכחה: [1] ברור כי G אבלית. $mG \le G$ תמיד! (חשוב אבלית) $\Leftarrow mG \trianglelefteq G$

[2] נניח $x \in m_1G \cap m_2G$. צ"ל $x = 0_G$.

נקבל
$$\begin{cases} x\in m_1G \\ x \in m_2G \end{cases} \Rightarrow \begin{cases} o(x) \mid m_2 \\ o(x) \mid m_1 \end{cases} \Rightarrow o(x) \mid (m_1,m_2) \Rightarrow o(x) \mid 1 \Rightarrow o(x)=1$$
$$\Downarrow$$
$$x = 0_G$$

הוכחנו [2]. //

[3] נוכיח: $G = m_1G + m_2G$.

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 $\Rightarrow$ **משל!**

-הפסקה-

טענה: לכל 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.

מספיק שקיימת ת"ח-p שהיא ציקלית.

(כי אם $|H|=p^k$ ($k\in\mathbb{N}$) ו- H ציקלית $\Leftarrow$ (משפט מיון ת"ח) קיימת ת"ח $\le H$ עם p^ℓ, $\ell \le k$)

מכיוון שקיימת ת"ח-p $X \le G$, $|X| = p^k > 1$. ניקח $x\in X$ לא ניטרלי;

אזי $H := \langle x\rangle \le X \le G$ ($|H|=p^i$, $|X|=p^k$) ת"ח-p ציקלית.

$|G|$, לכן לפי משפט הפיצול (הקודם) $G \cong P \times Q$

כאשר, $|P| = p^k$ (מקס) חבורת p שהיא באופן טבעי משוכנת לתוך G.

$X := P \times \{e\} \leq G$ חבורת-p.

מצאנו!

משל.

הערה: בהמשך נוכיח שאפשר להוריד אבליות של G ואז נקבל משפט Cauchy (קושי).

משפט: לכל G חבורת p כך ש $|G| = p^n$ מתקיים:

(א) קיימת ת"ח נורמלית $H \trianglelefteq G$ עם p^{n-1} איברים

(ב) לכל $1 \leq i \leq n$ קיימת ת"ח $K \leq G$ עם $|K| = p^i$.

הוכחה:

(ב) נובע מ-(א) בקלות $G \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \dots \trianglerighteq H_{n-1}$ (סדרים p^n, p^{n-1}, p^{n-2}, …, p)

הוכחה של (א): באינדוקציה:

1) $n=1$: $|G| = p^1$. ניקח $H := \{e\}$, $|H| = p^{1-1} = 1$.

2) נניח שהטענה נכונה עבור $n-1$

3) נוכיח עבור n

תזכורת: לכל חבורת-p $p \mid |C(G)|$.

המרכז $C(G)$ היא חבורה אבלית סופית ($p \mid |C(G)|$) לכן לפי הטענה הקודמת (מקרה פרטי של משפט קושי) קיימת ת"ח $H \leq C(G)$ כך ש $|H| = p$

תכונה חשובה של מרכז: כל ת"ח $H \leq C(G)$ של המרכז היא ת"ח נורמלית של G.

לכן $H \trianglelefteq G$, $|H| = p$.

לכן G/H חבורת מנה מוגדרת היטב:

מוגדר אפי טבעי: $G \xrightarrow{f} G/H$, $g \mapsto gH$

$|G/H| \underset{\text{הגדרה}}{=} [G:H] = \frac{p^n}{p} = p^{n-1}$

שימו לב: $|H| = p$.

לכן G/H חבורה עם p^{n-1} איברים. לפי הנחת האינדוקציה קיימת ת"ח נורמלית $A \trianglelefteq G/H$ כך ש $|A| = p^{n-2}$.

הערה: מקור של ת"ח נורמלית מעביר ת"ח נורמלית לפי הומומורפיזם. לבדוק!

Generated by CamScanner from intsig.com

$$G \xrightarrow{f} G/H$$
$$\triangledown \qquad\qquad \triangledown$$
$$f^{-1}(A) \xrightarrow[\text{הצמצום}]{f_0} A$$

$\ker f_0 = \ker f = H$

$|f^{-1}(A)| = |f^{-1}(A)/H| \cdot |H| = |A| \cdot |H| = p^{n-2} \cdot p = p^{n-1}$.

<u>לסיכום:</u> מצאנו תת חבורה נורמלית $G \trianglerighteq f^{-1}(A)$ עם p^{n-1} איברים.

משלימים את האינדוקציה $\Leftarrow$ מש"ל.

<u>תוצאה:</u> לכל חבורת-p G עם p^n איברים קיימת שרשרת נורמלית עם מנות ציקליות. שרשרת נורמלית:

$$G_0 := G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \dots \trianglerighteq G_{n-1} \trianglerighteq \{e\} =: G_n$$
$$p^n \quad p^{n-1} \quad p^{n-2} \qquad p \qquad p^0=1$$

"המנות"

$G_0/G_1,\ G_1/G_2,\ \dots,\ G_{n-1}/G_n$

כולן ציקליות (עם סדר p, לפי לגרנז' ותוצאות).

<u>הגדרה:</u> חבורה G נקראת פתירה (Solvable) אם עבור G קיימת שרשרת נורמלית סופית עם מנות <u>אבליות</u>.

תוצאה
$\Downarrow$

<u>מסקנה:</u> כל חבורת-p היא חבורה פתירה. ידוע שהחבורה הכי קטנה לא פתירה היא A_5.

בהמשך נלמד דרך אחרת לקביעה של פתירות דרך הקומוטטורים $[x,y]$

<u>דוגמאות של חבורות פתירות:</u>

1) כל חבורה אבלית פתירה.

$$\left.\begin{array}{l} G_1 := \{e\} \trianglelefteq G_0 = G \\ G/\{e\} \cong G \quad \text{בלבד אחת מנה} \\ \text{אבלית} \end{array}\right\} \checkmark$$

2) $G = D_n$ (לא אבלית) $\{e\} \trianglelefteq C_n \trianglelefteq D_n$

$C_n/\{e\} \cong C_n$ (אבלית), $D_n/C_n \cong \Omega_2$ (אבלית) 2 מנות

3) $GL_2(\mathbb{R}) \geq G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| \begin{array}{l} a \neq 0 \\ a,b \in \mathbb{R} \end{array} \right\}$ <u>פתירה!</u>

<u>רמז:</u> <u>לבדוק</u>: $H \cong \mathbb{R}$, $\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| b \in \mathbb{R} \right\} = H \trianglelefteq G$,

$G/H \cong \mathbb{R}^*$ שימוש באיזו I

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: $G/H \cong \mathbb{R}^\times$, $H \cong \mathbb{R}^\times$ (שיעור 3-5)

הערה: A_5 חבורה פשוטה (כל תת"ח נורמלית הן רק $\{e\}, A_5$).
היא החבורה הקטנה ביותר שפשוטה ולא אבלית.

הערה: {פשוטות אבליות} = {ציקליות מסדר ראשוני}.

הערה: מהמשפט שהוכחנו היום $\Leftarrow$ 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.
$\Leftarrow$ $p^{n-1} \neq p^n$

$G \neq H \neq \{e\}$

H נורמלית ב-G

משפטי Sylow

Sylow I (קיום): תהי G חבורה עם $|G| = p^n \cdot m$ כאשר $(p,m)=1$, $m,n\in\mathbb{N}$.
אזי קיימת 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 $n_p :=$ #תת"ח p סילו. אזי:
א) $n_p \equiv 1 \mod p$
ב) $n_p \mid m$
ג) $n_p = [G : N(P)]$ (כאשר $P \in Syl_p(G)$).

תזכורת: $N(H) := \{ g\in G \mid gHg^{-1} = H \}$ נורמליזטור של H בתוך G.

תכונות:
(1) $H \triangleleft N(H)$
(2) $N(H)$ היא תת"ח הכי גדולה בין תת"ח K של G שמכילות את H וכך ש-H נורמליות ב-K.
(3) $N(H) =$ מייצב של נקודה H במרחב פעולה $G\times Sub(G) \to Sub(G)$, $H\in$

$$\boxed{G_H = N(H)}$$

Generated by CamScanner from intsig.com

הוכחה Sylow I: באינדוקציה לפי הסדר של G.

(א) $|G|=p$ כאן $G=\mathbb{Z}_p$.

(ב) נניח שהטענה נכונה לכל $k < p^n m$

(ג) צ"ל עבור $|G| = p^n \cdot m$

יש כאן שני מקרים:

[1] קיימת תת"ח $H \le G$ כך ש $|H| = p^n \cdot m' < p^n \cdot m = |G|$.
$(H \neq G)$

אז אפשר להשתמש בהנחת האינדוקציה (ב):

קיימת תת"ח p-סילו $P \le H$. אז P תת"ח p-סילו גם ב-G.

[2] במקרה שאין תת"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] $p \mid [G:C_{x_j}]$

(כיוון $p \mid |G|$, לכן $p \mid |C(G)|$. הוכחנו מקרה פרטי של משפט קושי. נובע שקיימת תת"ח $K \le C(G)$ כך ש $|K| = p$.

ויודעים $K \triangleleft G$ לכן חבורת מנה G/K מוגדרת היטב.

ניקח אפי' טבעי $G \xrightarrow{f} G/K$

$$m \cdot p^{n-1} = \frac{p^n \cdot m}{p} = \frac{|G|}{|K|} = [G:K] = |G/K| < |G|.$$

לפי הנחת האינדוקציה קיימת תת"ח p-סילו $Syl_p(G/K) \ni H \le G/K$

$$\begin{array}{ccc} G & \xrightarrow{f} & G/K \\ \rotatebox{90}{$\le$} & & \rotatebox{90}{$\le$} \\ f^{-1}(H) & \xrightarrow{f_0} & H \end{array}$$

(נצמצם)

הערה: המקור של תת"ח הוא גם תת"ח.

לפי לגראנז':

$\ker f = \ker f_0 = K$.

$$|f^{-1}(H)| = |f^{-1}(H)/K| \cdot |K| = |H| \cdot |K| = p^{n-1} \cdot p = p^n$$

מצאנו תת"ח p-סילו

השלמנו את האינדוקציה!

מש"ל

Generated by CamScanner from intsig.com