

$g \in G$, חבורה G

מסדר g $\circ(g) = \min\{n \in \mathbb{N} \mid g^n = e\}$ $\circ(g) = \infty$

הוא מסדר $\langle g \rangle$ $\circ(g) = |\langle g \rangle|$

אם $\circ(g)$ סופי, אז $n \equiv m \pmod{\circ(g)} \Leftrightarrow g^n = g^m$

במקרה $(m=0)$, $g^n = e \Leftrightarrow n \equiv 0 \pmod{\circ(g)} \Leftrightarrow \circ(g) \mid n$

טענה (משעור קובץ):

יהי $n \geq 1$, $a \in \mathbb{Z}$, אזי הסדר של $[a] \in \mathbb{Z}_n$ (חסר חילוק) הוא

$$\circ([a]) = \frac{n}{\gcd(a,n)}$$

הוכחה:

$\circ(g) \mid k \Leftrightarrow [a]^k = e = [0] \Leftrightarrow [ka] = [0] \Leftrightarrow ka \equiv 0 \pmod{n} \Leftrightarrow n \mid ka, kn$

$\Leftrightarrow n \mid \gcd(ka, kn) \Leftrightarrow n \mid k \cdot \gcd(a, n) \Leftrightarrow \exists c \in \mathbb{Z} : nc = k \cdot \gcd(a, n) \Leftrightarrow$

$\Leftrightarrow \underbrace{\frac{n}{\gcd(a,n)}}_{\in \mathbb{Z}} c = k \Leftrightarrow \frac{n}{\gcd(a,n)} \mid k \Leftrightarrow \underbrace{\circ([a])}_{\text{(הוכחה)}} \mid k$

$$\circ([a]) = \frac{n}{\gcd(a,n)}$$

השקרה: תהי G חבורה, $H \leq G$ תת חבורה. נגדיר שני יחסים \sim על G .

$$g_1 \sim_l g_2 \Leftrightarrow g_1^{-1} g_2 \in H$$

$$g_1 \sim_r g_2 \Leftrightarrow g_2 g_1^{-1} \in H$$

השקרה \sim_l נקראת אבליזציה אם לכל $g_1, g_2 \in G$ מתקיים $g_1 g_2 = g_2 g_1$

השקרה \sim_r נקראת אבליזציה אם לכל $g_1, g_2 \in G$ מתקיים $g_1 g_2 = g_2 g_1$

טענה:

שני היחסים מההגדרה הם יחסים שקילות

הוכחה:

$g \sim g \Leftrightarrow g^{-1}g = e \in H$ רגל היסודיות: $g \in G$ יהי

$g_1 \sim g_2 \Leftrightarrow g_1^{-1}g_2 \in H \Leftrightarrow (g_1^{-1}g_2)^{-1} \in H \Leftrightarrow$ סימטריה: יהיו $g_1, g_2 \in G$

$\Leftrightarrow g_2^{-1}g_1 \in H \Leftrightarrow g_2 \sim g_1$

טרנזיטיביות: יהיו $g_1, g_2, g_3 \in G$ כך ש $g_1 \sim g_2, g_2 \sim g_3$

$g_1 \sim g_2 \wedge g_2 \sim g_3 \Leftrightarrow g_1^{-1}g_2, g_2^{-1}g_3 \in H \Leftrightarrow g_1^{-1}g_2g_2^{-1}g_3 = g_1^{-1}g_3 \in H \Leftrightarrow$

$\Leftrightarrow g_1 \sim g_3$

הגדרה: מחלקות שקילות של היחס \sim נקראות מחלקות שקילות

משמאל של H ב- G (משמאל coset)

מחלקות השקילות של היחס \sim נקראות מחלקות שקילות

מימין של H ב- G

א"ק נגזרות מחלקות משמאל (כל המחלקות יהיו מחלקות משמאל כל עוד?
 ד"ו נכתב אחרת)

$\Leftrightarrow \exists h \in H: g^{-1}x = h \Leftrightarrow g^{-1}x \in H \Leftrightarrow g \sim x$ יהי $g \in G$ קבוע

$\Leftrightarrow \exists h \in H: x = gh$

לכן המחלקה של g היא $\{x = gh: h \in H\} = gH$

מחלקות מימין בינו $\{x = hg: h \in H\} = Hg$

הצורה aH או Ha אבסולוטי, אבל המחלקות מימין אמת למחלקות משמאל

(1) G חבורה. $H = G$ אזי לכל $g_1, g_2 \in G$, $g_1^{-1}g_2 \in G$ ולכן $g_1 \sim g_2$ לכל $g_1, g_2 \in G$.
 עכ"ל יש רק מחלקה אחת.

(2) G חבורה. $H = \{e\}$ תת חבורה הטריוויאלית. $g_1 \sim g_2 \Leftrightarrow g_1^{-1}g_2 \in H \Leftrightarrow g_1^{-1}g_2 = e \Leftrightarrow g_1 = g_2$.
 כל מחלקה יש רק איבר אחד $g \in H = \{e\}$.

(3) $G = \mathbb{Z}$ (זרם חיבור) $H = n\mathbb{Z}$. יהיו $g_1, g_2 \in \mathbb{Z}$ אזי

$g_1 \sim g_2 \Leftrightarrow g_1^{-1}g_2 \in H = n\mathbb{Z} \Leftrightarrow -g_1 + g_2 \in n\mathbb{Z} \Leftrightarrow n | (g_2 - g_1) \Leftrightarrow g_1 \equiv g_2 \pmod{n}$
 עכ"ל מחלקות שקילות הן מחלקות שקילות מודולו n .

(4) $G = GL_n(\mathbb{R})$ $H = SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\}$ יהיו $A, B \in GL_n(\mathbb{R})$

$$A \sim B \Leftrightarrow A^{-1}B \in SL_n(\mathbb{R}) \Leftrightarrow \frac{\det B}{\det A} = 1 \Leftrightarrow \det A = \det B$$

עכ"ל המחלקה SL_n

$$A(SL_n(\mathbb{R})) = \{B \in GL_n(\mathbb{R}) : \det B = \det A\}$$

יש כתאמה חד-חד-ערכית בין המחלקות עכ"ל עכ"ל

$$r \neq 0 \Leftrightarrow \{A \in GL_n(\mathbb{R}) : \det A = r\} \quad \mathbb{R}^* = \mathbb{R} \setminus \{0\}$$

יש e שבמחלקות שקילות מיוחדות כהן, היחסים

\sim, \sim_r שווים למרות $e \in GL_n(\mathbb{R})$ לא אובדנית. זה קורה מפני

H כינה תת חבורה נורמלית.

(5) תהי A קבוצה, $G = S_A$ כלומר $G = \{f : A \rightarrow A\}$ תחב"ש

$$H = \text{stab}(a) = \{f \in S_A : f(a) = a\} \quad a \in A \quad \text{ע"ל תת חבורה}$$

תהיינה $f, g \in S_A$ אזי

$$f \sim g \Leftrightarrow f^{-1}g \in \text{stab}(a) \Leftrightarrow (f^{-1}g)(a) = f^{-1}(g(a)) = a \Leftrightarrow f(a) = g(a)$$

ע"ל הכו' f, g חבורות עכ"ל \Leftrightarrow הן שומרות את a לגותה
 יתמונה

$x \in A \leftrightarrow \{f \in S_A : f(a) = x\}$ ($H = \text{stab}(a)$) $A \leftrightarrow G/H$ יש התאמה חד־חד־ערכית ושל

סימון: G/H הקבוצה של מחלקות שקילות של G מניין
 סימון: G/H הקבוצה של מחלקות שקילות של G מניין

נתבונן ביחס מניין:

$$f \sim_r g \Leftrightarrow \exists f^{-1} \in \text{stab}(a) \Leftrightarrow \exists f^{-1}(a) = a \Leftrightarrow f^{-1}(a) = g^{-1}(a)$$

פונקציות סבוריות לפי \sim_r אם $a \sim a^{-1}$ יש את אותו המקור, פלוס
 פונקציות שולקות את אותו איבר a^{-1}

$x \in A \leftrightarrow \{f \in S_A : f(x) = a\}$ $A \leftrightarrow G/H$ יש התאמה

קונטרה:

$\begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix} \sigma \in S_3$ נראים תמורה $G = S_3 = S_{\{1,2,3\}}$

$\left. \begin{matrix} \left(\begin{matrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{matrix} \right) \left(\begin{matrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{matrix} \right) \left(\begin{matrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{matrix} \right) \\ \left(\begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{matrix} \right) \left(\begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{matrix} \right) \left(\begin{matrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{matrix} \right) \end{matrix} \right\}$ S_3 יש $6 = 3!$ איברים

$$H = \text{stab}(3) = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

$$eH = \{eh \in H\} = H$$

המחלקה e הינה מניין

מה המחלקה $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$?

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$

יש אותה תמונה

המחלקה השלישית הינה

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

אבחנות על מחלקות

תהי G חבורה, $H \leq G$ תת-חבורה.

(1) $eH = H = He$ כלומר, H בעצמה בינה אחת המחלקות

(2) כל שאר המחלקות אינן תת-חבורות, כי הן לא מכילות את e

(3) כל המחלקות מאותה עוצמה

אכן לכל $g \in G$, $H \rightarrow gH$, $x \leftarrow g^{-1}x$, $h \mapsto gh$

לכן $H \mapsto gH$ חתך ועל ועל $|H| = |gH|$

באופן קומה עבור המחלקות מימין ונקבל $|Hg| = |H| = |gH|$

(4) $|G/H| = |G/H|$

$G/H \rightarrow G/H$, $f(gH) = Hg^{-1}$ נמבין בהצטרפים

f מוגדרת היטב: אם $gH = xH$ אזי $x \sim g$ כריג להוכיח כי $Hg^{-1} = Hx^{-1}$ וכן, $g^{-1}(x^{-1})^{-1} = g^{-1}x \in H$, $gH = xH \Rightarrow g^{-1}x \in H$, $Hg^{-1} = Hx^{-1}$ כלומר, $x^{-1} \sim g^{-1}$ (סקלים מימין) ולכן

$f: gH \mapsto Hg^{-1}$

$x^{-1}H \leftarrow Hx$

לכן f חתך ועל

הצורה תהי G חבורה, $H \leq G$ תת-חבורה, האינדקס של H ב- G

הינו העוצמה $|G/H| = |G/H|$. מסתים אותו $[G:H]$

משפט לגרנדז':

תהי G חבורה סופית, $H \subseteq G$ תת חבורה. אזי $|H| \mid |G|$

הוכחה:

נוכחנו שבכל מחלקה (משמאלו) יש $|H|$ איברים, כי הצבחות של כל המחלקות שוות. 'ה' $[G:H]$ מספר המחלקות. המחלקות הן מחלקות שקילות של יחס שקילות, לכן זרות או שוות.

$$\text{לכן } |H| \cdot [G:H] = |G| \text{ ולכן } |H| \mid |G|$$

תוצאות:

(1) תהי G חבורה סופית, $e \in G$ וזי $|G|/|H|$

הוכחה:

תהי $H = \langle g \rangle$ הנוכחו כי $|H| = |G|$. ולפי לגרנדז' $|G|/|H|$

(2) תהי G חבורה סופית. לכל $e \in G$ מתקיים $e^{|G|} = e$

הוכחה:

$e^{|G|} = e \Leftrightarrow |G| \in \text{ord}(e)$, לפי התוצאה הקודמת $|G|/|H|$

(3) 'ה' P ראשוני, תהי G חבורה מסדר P . אזי:

א) G הינה חבורה ציקלית (קיים $e \in G$ כך $\langle e \rangle = G$)

ב) תת-החבורות היחידות של G הן $\{e\}$ ו- G

הוכחה:

א) 'ה' $e \in G$ אזי $|G|/|H|$ $|H| = 1$ או $|H| = P$.

$$|H| = 1 \Leftrightarrow e = e^1 = e$$

$$|H| = P \Leftrightarrow \langle e \rangle = G$$

ב) תהי $H \subseteq G$ תת חבורה. לפי לגרנדז' $|H| \mid P$ לכן

$$|H| = 1 \Leftrightarrow H = \{e\} \text{ או } |H| = P \Leftrightarrow H = G$$

השקרה: חבורה G נקראת ציקלית אם קיים איבר $a \in G$ כך ש $\langle a \rangle = G$

איבר a כזה נקרא יוצר של G

קולומב:

\mathbb{Z} ציקלית, נוצרת על ידי 1 או -1

תכונות: תהי G ציקלית. אם $\langle a \rangle = G$ אז $\langle a^{-1} \rangle = G$

השקרה: יהי \mathbb{Z}_n מתקין באינוואזיה \mathbb{Z}_n עם פעולת כפל של המספרים.

זהו חבורה כי $\mathbb{Z}_n \neq \emptyset$, $[a] \cdot [b] = [ab]$, $[a]^{-1} = [a^{-1}]$. לכן \mathbb{Z}_n הוא הופכי

תהי $U_n = U(\mathbb{Z}_n)$. תת-חבורה של המספרים ההפיכות. לפי טענה

(מהשיעור הראשון), U_n היא חבורה (תחת כפל המספרים)

היא נקראת חבורת אוילר.

טענה:

יהי \mathbb{Z}_n , יהי $a \in \mathbb{Z}_n$ אז $[a] \in U_n$ (הפיכה ב- \mathbb{Z}_n)

אם ורק אם $\gcd(a, n) = 1$

הוכחה:

(\Rightarrow) אם $\gcd(a, n) = 1$, אז לפי גלגוליתם אוקלידס במרחב, קיימים

$x, y \in \mathbb{Z}$ כך ש $ax + ny = 1$. לכן, $ax \equiv 1 \pmod{n}$. כלומר, $[a]$

$$[a][x] = [x][a] = [1] = e$$

לכן $[a]$ הפיכה

(\Leftarrow) תהי $[a]$ הפיכה. נק"ל כי a לא זר ל- n . כלומר, קיים

מתאם k כך ש $ka = 1$ ו- $ka \equiv 1 \pmod{n}$

יהי $[x] \in \mathbb{Z}_n$ ההופכי של $[a]$ אז $[ax] = [a][x] = e = [1]$

לכן $ax \equiv 1 \pmod{n}$ לכן $n \mid ax - 1$ ולכן קיים $y \in \mathbb{Z}$

כך ש $ax - ny = 1$ וקיבלנו $ka = 1$

בסתירה. לכן $\gcd(a, n) = 1$

האברה: ϕ היא משהי' $\phi(n)$ העוצמה של U_n . ϕ נקראת הפונקציה של אוילר

הערכה: כיוון שהאיברים של Z_n ה'ם $[1], \dots, [n]$

מקבלים ש $\phi(n) = |\{1 \leq a \leq n : \text{gcd}(a, n) = 1\}|$

לדוגמה: $\phi(6) = 2$ $\phi(5) = 4$ $\phi(4) = 2$ $\phi(3) = 2$ $\phi(2) = 1$

ה' ϕ היא פונקציה. וזו $\phi(p) = p-1$ (כל המספרים $1, \dots, p-1$ זכרים p)

ה' ϕ היא פונקציה של האוסון p .

מספר a עם זכר p $a \in Z_n \Leftrightarrow p \nmid a$ כי כן המספרים $1, \dots, p^r$

כלל זכרים p ה'ם $1, 2, \dots, p^r$ (כמה p^r p כולל)

$\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$ לכן

טענה:

ה' ϕ היא פונקציה מרובעת, $\phi(mn) = \phi(m)\phi(n)$ או ϕ זכרים, $\text{gcd}(m, n) = 1$.

הוכחה:

נוסף משהי' האגרות הסיוני

טענה: (משפט אוילר)

ה' ϕ היא משהי' $a \in Z_n$ וזו $a \in Z_n$ כן $\text{gcd}(a, n) = 1$ או $a^{\phi(n)} \equiv 1 \pmod n$

הוכחה:

נהי $G = U_n$ כיוון e $\text{gcd}(a, n) = 1$ $[a] \in U_n$. הוכחנו כי $|G| = \phi(n)$ לכן

$[a]^{\phi(n)} = [a]^{|G|} = [1]$ וכן $[a]^{\phi(n)} = e = [1]$

$a^{\phi(n)} \equiv 1 \pmod n$ לכן

כוכבה (המשפט הקטן של פירמה)

'ה' p כאלוני. 'ה' a $(\gcd(a,p)=1)$ כלומר

$$a^{p-1} \equiv 1 \pmod{p}$$

כוכבה:

מקרה פרטי של הטענה הקודמת $n=p$.

$$\varphi(n) = \prod_{i=1}^m (p_i - 1) p_i^{r_i - 1} \quad \text{כאילו} \quad n = p_1^{r_1} \dots p_m^{r_m}$$

טענה:

'ה' p, q כאלוני שונים. 'ה' $n=pq$. למה אם $\varphi(n)$ זה שקול

למכפול p, q האנשים

כוכבה:

$$\varphi(n) = (p-1)(q-1) \iff n=pq$$

כלומר $\varphi(n)$ ו- n ידועים

$$(x-p)(x-q) = x^2 - (p+q)x + pq = x^2 - (n+1-\varphi(n))x + n$$

כלל

$$\varphi(n) = (p-1)(q-1) = pq - p - q + 1 = n + 1 - p - q \iff p + q = n + 1 - \varphi(n)$$