

תהא $H \leq G$ ת"ח.

הגדרה

האינדקס של ת"ח H ב G :
מס' המח' השמאליות של H ב G := $m[G : H]$

הוכחנו בשיעור שעבר:

$$\frac{|G|}{|H|} = [G : H] \text{ אי } H \leq G \text{ ת"ח, אזי}$$

הערה חשובה

$$\frac{|G|}{|H|} = [G : H] \text{ באותו אופן ניתן להוכיח, במקרה הנ"ל, מס' המחלקות הימניות של } H \text{ ב } G$$

מסקנה 1

מס' המח' הימניות = מס' המחלקות השמאליות של H ב G .

מסקנה 2

הסדר של תת חבורה (בחבורות סופיות) מחלק את הסדר של החבורה.

מסקנה 3

תהא G חבורה סופית, לכל $g \in G$, $|G| \mid o(g)$

הוכחה

$$o(g) = |\langle g \rangle| \text{ ולפי מסקנה 2 הסדר של כל תת חבורה מחלק את הסדר של } G.$$

מסקנה 4

תהא G חבורה סופית. אזי $g^{|G|} = e \forall g \in G$

הוכחה

לפי משפט לגרנג' מתקיים:

$$|G| = |\langle g \rangle| \cdot [G : \langle g \rangle] = o(g) \cdot [G : \langle g \rangle]$$

בפרט $|G| \mid o(g)$ מסקנה 3 לעיל, לכן $o(g)$ סופי - מה שמחלק מס' סופי הוא סופי. ואז, לפי תרגיל מהשיעור הקודם אם $o(g)$ סופי אזי $o(g) = \min \{n \in \mathbb{N} : g^n = e\}$ בפרט: עבור $o(g)$ סופי כי $o(g)$ מספר שאם מעלים אותו בחזקה מקבלים $g^{o(g)} = e$ ולכן

$$g^{|G|} = g^{o(g) \cdot [G : \langle g \rangle]} = \left(g^{o(g)}\right)^{[G : \langle g \rangle]} = e^{[G : \langle g \rangle]} = e$$

ממסקנה 4 נובע משפט ידוע בתורת המספרים:

משפט פרמה הקטן

יהי p ראשוני. לכל $\alpha \in \mathbb{Z}$ $\alpha^p \equiv \alpha \pmod{p}$

הוכחה

מקרה א' אם $p \mid \alpha$ אזי $\alpha^p \equiv 0 \pmod{p}$ ומתקיים $\alpha^p \equiv \alpha \pmod{p}$

מקרה ב' אם $p \nmid \alpha$ כלומר $\alpha \pmod{p} = r$ כאשר $0 < r < p$ שלם

עובדה קלה אם $\alpha \pmod{p} = r$ אזי $\alpha^p \pmod{p} = r^p \pmod{p}$. הוכחה: תרגילורמז: $\alpha^p = (qp + r)^p \equiv r^p \pmod{p}$

לכן מספיק להוכיח $r^p \equiv r \pmod{p}, \forall 0 < r < p$

תזכורת \mathbb{F}_p שדה עם חיבור וכפל מודולו p ולכן $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ תבורה ביחס לכפל מודולו p

כעת $r \in \mathbb{F}_p^*$ ולכן $|\mathbb{F}_p^*| = p - 1$. לפי מסקנה 4: $r^{p-1} \equiv 1 \pmod{p}$ ונקבל $r^p \equiv r \pmod{p}$ ■

השלמה (בנושא מחלקות)

טענה

תהא G תבורה, $H \leq G$. לכל $a, b \in G$:

$$b^{-1}a \in H \iff aH = bH \quad (i)$$

$$ab^{-1} \in H \iff Ha = Hb \quad (ii)$$

נוכיח את (i) כאשר ההוכחה של (ii) זהה

$$\begin{aligned} a^{-1}b \in H \iff \exists h \in H \quad a^{-1}b = ah \iff b = ah \iff aH = bH \iff \\ b^{-1}a = (a^{-1}b)^{-1} = h^{-1} \in H \end{aligned}$$

$$\begin{aligned} aH = (bh)H \iff a = bh \iff \exists h \in H \quad b^{-1}a \in hH \iff \\ b^{-1}a \in H \iff b(hH) = bh \end{aligned}$$

תת תבורה נורמלית

הגדרה

תהא G תבורה, $H \leq G$ תת תבורה נורמלית (תח"נ) אם $gH = Hg, \forall g \in G$ סימון $H \trianglelefteq G$

דוגמאות

1. G אבליה. כל ת"ח H היא נורמלית.
2. G חבורה כלשהי. $\{e\} \trianglelefteq G$ כי $\{e\}g = g = g\{e\} \forall g \in G$.
3. לכל חבורה G , $G \trianglelefteq G$ כי $Gg = G = Gg \forall g \in G$.
דוגמאות 2 ו 3 נקראות תח"נ טריוויאליות.
4. לכל חבורה G המרכז $Z(G)$ היא תח"נ.
הוכחה: $\forall g \in G \quad gZ(G) = \{gx : x \in Z(G)\} = \{xg : x \in Z(G)\} = Z(G)g$
- 5.

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

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

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

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

קיבלנו $gH \neq Hg$, מכאן H אינה תח"נ של G .

6. $G = GL_n(\mathbb{R})$ תח"נ של G :

$$GL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R}) \quad (\alpha)$$

$$\{I_n\} \trianglelefteq GL_n(\mathbb{R}) \quad (\beta)$$

$$Z(GL_n(\mathbb{R})) = \{rI_n : r \in \mathbb{R}^*\} \trianglelefteq GL_n(\mathbb{R}) \quad (\gamma)$$

טענה

$$SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R}), \forall 1 \leq n$$

הוכחה

טענה 1

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

הוכחה לטענת עזר 1

לפי טענה משיעור קודם $B \in A \cdot SL_n(\mathbb{R})$ אם"ם $A \cdot SL_n(\mathbb{R}) = B \cdot SL_n(\mathbb{R})$ אם"ם לפי הטענה בהשלמה לעיל $B^{-1}A \in SL_n(\mathbb{R})$ אם"ם $\det(B^{-1}A) = 1$ אם"ם לפי משפט

המכפלה) $\det(B^{-1}) \det A = 1$ אם"ם $\frac{1}{\det B} \det A = 1$ אם"ם $\det A = \det B$ משל

טענה 1

טענה 2

לכל $A \in GL_n(\mathbb{R})$

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

הוכחה

זהה - השלם

לבסוף

טענה 1 + טענה 2 \Leftrightarrow טענה.