תהא $H \leq G$ ת"ח.

הגדרה

האינדקס של ת"ח H בG:
מס' המח' השמאליות של H בG=: $m\left[G:H\right]$

הוכחנו בשיעור שעבר:

משפט לגרנג' תהא G חבורה וספית, $H \leq G$ ת"ח, אזי $\frac{|G|}{|H|} = \left[G:H\right]$

הערה חשובה

באותו אופן ניתן להוכיח, במקרה הנ"ל, מס' המחלקות הימניות של H בG= $\frac{|G|}{|H|}$

מסקנה 1

מס' המח' הימניות=מס' המחלקות השמאליות של H בG.

מסקנה 2

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

מסקנה 3

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

הוכחה

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

מסקנה 4

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

הוכחה

לפי משפט לגרנג' מתקיים:

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

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

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

ממסקנה 4 נובע משפט ידוע בתורת המספרים:

משפט פרמה הקטן

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

הוכחה

מקרה א' אם $p \mid \alpha$ אזי $p \mid \alpha^p$ ומתקיים $\alpha^p \mathrm{mod} p = \alpha \mathrm{mod} p = 0$

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

עובדה קלה אם $\alpha \mathrm{mod} p = r$ אזי $\alpha^p \mathrm{mod} p = r^p \mathrm{mod} p$. <u>הוכחה</u>: תרגיל]רמז: $\alpha^p = (qp+r)^p$ $\alpha = qp + r$[

לכן מספיק להוכיח $\forall 0 < r < p$, $r^p \mathrm{mod} p = r$

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

כעת $r \in \mathbb{F}_p^*$ ולכן $\left|\mathbb{F}_p^*\right| = p - 1$. לפי מסקנה 4: $r^{\left|\mathbb{F}_p^*\right|} \mathrm{mod} p = 1 \Leftarrow r^{p-1} \mathrm{mod} p = 1$.
נכפיל את שני האגפים בr(בחבורה $\mathbb{F}_p^*$, כלומר בכפל מודולו p) ונקבל $r^p \mathrm{mod} p = r \mathrm{mod} p = r$ ■

השלמה(בנושא מחלקות)

טענה

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

(i) $aH = bH$ אמ"ם $b^{-1}a \in H$

(ii) $Ha = Hb$ אמ"ם $ab^{-1} \in H$

נוכיח את (i) כאשר ההוכחה של (ii) זהה

$\Leftarrow$ $aH = bH \Leftarrow b = be = \in aH \Leftarrow b = ah$ $\exists h \in H$ ואז $a^{-1}b \in G$ ולכן $b^{-1}a = \left(a^{-1}b\right)^{-1} = h^{-1} \in H$.

$\Rightarrow$ נניח $b^{-1}a \in H$ אז $\exists h \in H$ $b^{-1}a \in h$ ואז $a = bh$ ואז $aH = (bh)H = b(hH) = bh$

תת חבורה נורמלית

הגדרה

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

דוגמאות

1. G אבלית. כל ת"ח H היא נורמלית.
2. G חבורה כלשהי. $\{e\} \trianglelefteq G$ כי $\forall g \in G$ $g\{e\} = g = \{e\}g$.
3. לכל חבורה G, $G \trianglelefteq G$ כי $\forall g \in G$ $gG = G = Gg$.
דוגמאות 2 ו3 נקראות תח"נ טריוויאליות.
4. לכל חבורה G המרכז $Z(G)$ היא תח"נ.
<u>הוכחה</u>: $\forall g \in G$ $gZ(G) = \{gx : x \in Z(G)\} = \{xg : x \in Z(G)\} = Z(G)g$
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:

(א) $GL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$

(ב) $\{I_n\} \trianglelefteq GL_n\{\mathbb{R}\}$

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

טענה

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

הוכחה

טענה 1

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

הוכחה לטענת עזר 1

לפי טענה משיעור קודם $B \in A \cdot SL_n(\mathbb{R})$ אמ"ם $A \cdot SL_n(\mathbb{R}) = B \cdot SL_n(\mathbb{R})$ אמ"ם לפי הטענה בהשלמה לעיל $B^{-1}A \in SL_n(\mathbb{R})$ אמ"ם $\det\left(B^{-1}A\right) = 1$ אמ"ם(לפי משפט המכפלה) $\det\left(B^{-1}\right)\det A = 1$ אמ"ם $\frac{1}{\det B}\det A = 1$ אמ"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 $\Leftarrow$ טענה.