משפט

$a,b\in G$,$H\le G$

א. מתקיים $aH=bH$ או $aH\cap bH=\emptyset$

ב. $aH=H$ אם ורק אם $a\in H$

משפט

$H\le G$, $a,b\in G$, $a^{-1}b\in H$ אזי $aH=bH\Leftrightarrow b^{-1}a\in H$ (יחס שקילות - $\Leftrightarrow a^{-1}b\in H$) [וכנ"ל לגבי $Ha=Hb\Leftrightarrow ba^{-1}H$]

אפשר להגדיר יחס שקילות $a\sim b\Leftrightarrow a^{-1}b\in H$ ואז המחלקות השמאליות הן מחלקות השקילות.

מסקנה

אם $G\le H$ אזי $G=\biguplus xH=\biguplus Hx$ (xH מחלקות שמאליו של H ב-G). ניתן לסמן איחוד זר גם בתור $\coprod$

תרגיל $H\le G$. הוכיחו $Hg_1=Hg_2\Leftrightarrow g_1\in Hg_2$

הגדרה

תהי G חבורה, $X\subseteq G$.

$$X^{-1}=\left\{x^{-1}:x\in X\right\}$$

תרגיל

מה זה $(Hg)^{-1}$ כאשר $g\in G,H\le G$?

פתרון

$$(Hg)^{-1}=\left\{(hg)^{-1}:h\in H\right\}=\left\{g^{-1}h^{-1}:h\in H\right\}=g^{-1}\left\{h^{-1}:h\in H\right\}=g^{-1}H$$

הערה $H^{-1}=H$

הגדרה

$[G:H]$=אינדקס של תת חבורה H בחבורה G=מספר המחלקות השמאליות של H ב-G=מספר המחלקות הימניות.

את השוויון (בין מספר המחלקות ימניות למספר השמאליות) רואים לפי התרגיל.

משפט לגרנג'

אם G סופית ו$H \leq G$ אזי $|G| = |H| [G : H]$

מסקנה

אם G $K \leq H \leq G$ אזי $[G : K] = [G : H] [H : K]$

דרך הוכחה $|G| = |H| [G : H]$ - להציב $|H| = |K| [H : K]$
$|G| = [G : K] |K|$

תרגיל בית

$|G| = 20$, מה הגדלים האפשריים של תת-חבורות?

משפט

אם G סופית ו$g \in G$ אזי $o(g) \mid |G|$

מסקנה

$$g^{|G|} = e$$

$$|G| = d \cdot o(g)$$

$$g^{|G|} = \left(g^{o(g)}\right)^d = e^d = e$$

המשפט הקטן של פרמה

יהי p ראשוני, אזי לכל $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$

"הוכחה" אם מביטים ב$U_p = \{1, ..., p-1\}$ אזי $|U_p| = p - 1$ ואז לכל $a \in U_p$,
$a^p = a \Leftarrow a^{p-1} = 1 = e$

דוגמה

$$3^7 \equiv 3 \pmod{7}$$

$$13^{41} \equiv 13 \pmod{100}$$

$$|U_{100}| = 40, 5 \cdot 4 \cdot 2 \cdot 1 = 40$$

תרגיל

הראו כי חבורה היא מסדר זוגי $\Leftrightarrow$היא כוללת איבר מסדר 2.

פתרון

$\Leftarrow$ $G=\{e\}\cup\underbrace{\{a,a^{-1}\}}_{2}\cup\underbrace{\{b,b^{-1}\}}_{2}\cup\ldots$ - אם מניחים שאין בG איבר מסדר 2, אזי $2\nmid|G|$

$\Rightarrow$ $2=o(g)\mid|G|$

תרגיל

תהי G חבורה מסדר $2p$(כאשר p ראשוני). הוכח כי לG יש איבר מסדר p.

פתרון

כל איבר בG הוא מסדר 1, 2, p או $2p$. אם יש איבר מסדר p אז סיימנו. אם יש איבר $a\in G$ מסדר $2p$ אזי a^2 הוא מסדר p וסיימנו.

$$e=a^{2p}=\left(a^2\right)^p$$

הסדר של a^2 צריך לחלק את $p\Leftarrow$ $o\left(a^2\right)=p$ו$o\left(a^2\right)=1$ לא יעזור לנו כי אז $o(a)=2$).
נניח בשלילה כי כל אברי G השונים מהיחידה הם מסדר 2. $2p>4$. אז ניקח שני איברים מסדר 2 בG שונים, $a,b\in G$.

$$\langle a,b\rangle=\{1,a,b,ab\}=H$$

$$4=|H|\mid|G|=2p$$

$\Leftarrow$סתירה$\Leftarrow$לא כל האיברים של G הם מסדר 2.

הערה ab מסדר 2 $\Leftarrow e=\left(ab\right)^2=abab\Leftarrow a=bab\Leftarrow ab=ba\Leftarrow a$ וb מתחלפים.