

הצבור: יהי G סופי.

א. נניח $|G| = p^k$ ו- $|G| \nmid p^{k+1}$, אז יש $H \leq G$ מסדר p^k (נקראת חבורת סילוב- p).
 ב. אם $H \leq G$ מסדר p^i אז יש P סילוב- p ו- $g \in G$ כך ש: $H \leq gPg^{-1}$.
 ג. מס' חבורת סילוב- p יסומן ב- n_p . אז $n_p \equiv 1 \pmod{p}$.
 ד. $n_p = (G:N(P))$ ופירוט $n_p | (G:P)$.

עמלה: כל חבורה מסדר 132 אינה פשוטה.

הוכחה: $132 = 11 \cdot 2^2 \cdot 3$. נניח בשלילה G פשוטה, אז $n_{11} > 1$ ובנוסף $n_{11} | 12$.

$$n_{11} \equiv 1 \pmod{11}$$

ולכן $n_{11} = 12$. מכאן $12 \cdot 10 = 120$ איברים מסדר 11.

$$n_3 = 1, 4, 7, 10, 13, 16, 19, 22, 25$$

$$n_3 \equiv 1 \pmod{3}, n_3 > 1, n_3 | 44$$

$$n_3 \in \{4, 22\}$$

נניח $n_3 = 4$, ונראה שזה לא יתכן.

דבר I: $n = (G:N(P))$ כאשר P חבורת סילוב-3. לפי משפט קיילי יש

$$\psi: G \rightarrow S_n, \quad \{e\} \leq \ker \psi \leq N(P) < G$$

אבל אם $\ker \psi = \{e\}$ אז $24 \nmid |G|$ או $32 = |G|$ בסתירה. לכן $\{e\} < \ker \psi < G$

בסתירה.

דבר II: נניח בשלילה $n_3 = 4$ אז יש $8 = 4 \cdot 2$ איברים מסדר 3. סה"כ $120 + 8 = 128$

אם $n_2 > 1$ זה מוסיף יותר מ-4 איברים מסדר 2 שמתוך אלה 2^2 , וסה"כ יותר

מ-132 בסתירה.

□

לכן $n_3 = 22$. זה לא יתכן כי $120 + 22 \cdot 2 > 132$.

עמלה: יהי $|G| = pqr$ ו- $p < q < r$ ראשוניים. חבורת סילוב- p

נורמלית ב- G .

הוכחה: שלב א': צ"ל $n_r = 1$ או $n_q = 1$.

נניח בשלילה אחרת. $n_r \equiv 1 \pmod{r}$ ו- $n_q \equiv 1 \pmod{q}$. אז

$n_r = p$ נקבל $r | p-1$ בסתירה. אם $n_r = q$ ו- $r | q-1$ בסתירה.

לכן נבחנו pq איבר מסדר r .

$n_q \equiv 1 \pmod{q}$, לכן $n_q \in \{p, r, pr\}$. אם $n_q = p$, אז $q | p-1$ בסתירה.

לכן $n_q \geq 2$ ומכאן $r(q-1) \leq r$ איברים מסדר q .

אם סתירה, כי

$$\underbrace{pq(r-1)}_{r \text{ גודל}} + \underbrace{r(q-1)}_{q \text{ גודל}} = pqr - pq + (q-1)r > pqr$$

$\uparrow$
 $q-1 \geq p$
 $r > q$

על כן: נניח $n_r = 1$

יהי R תבור סתירה r , Q תבור סתירה q .
 נשאל א', $R \leq G$ או $Q \leq G$ או $RQ \leq G$.
 $|RQ| \leq r$ (לפי) $|RQ| = r$ כי $|RQ| \leq r$ ו- $r > q$.
 (גם q, r).

בנוסף $q \mid n_r(RQ)$ וכן $n_r(RQ) \equiv 1 \pmod{r}$ ולכן $n_r(RQ) = 1$.
 $RQ \leq N_G(R)$ ולכן $RQ \leq N_G(R)$ שומר.
 $n_r = \frac{|G|}{|N_G(R)|} = p$
 $\equiv 1 \pmod{r}$
 אם $|N_G(R)| = r$ איברי G , אז $|N_G(R)| \in \{r, p, pr\}$ ←
 סתירה.

אם $N_G(R) = G$ וס"מ.

היה במבחן שאלה של תבורות סתירה. תשובה לשאלה
 את השאלה החוצה במערכת! (השאלה החוצה: ישו ש כי
 התבורות ש סדר 6)

שאלה: נניח כי $|G| = p^2 q$. צ"ל G לא פאטה.

הוכחה: אחת, $n_p > 1$, $n_q > 1$, $n_p \mid q$, $n_q \mid p$.
 $p < q \Leftrightarrow p \mid q-1 \Leftrightarrow n_p = q$ אם $n_p = q$ אז $n_q = p$.
~~אם $n_q \mid p^2$ אז $n_q \in \{p, p^2\}$. אם $n_q = p^2$ אז $p = n_q \equiv 1 \pmod{q}$.~~
 $p = n_q \equiv 1 \pmod{q} \Leftrightarrow p \mid q-1 \Leftrightarrow q < p$ וסתירה. אם $n_q = p^2$ אז $n_p = q$ ו- $p^2 \mid q-1$.
 איברים מסדר q . ואם תבור סתירה p אחת כפר תורה p^2 איברים מסדר
 $1, p, p^2$ ואם $p^2 q = p^2(q-1) + p^2$. $\square$