תזכורת:

1) תהי G חבורה, $g\in G$. תהי $S\subseteq G$ תת-קבוצה. אזי $|S| = |gSg^{-1}|$

$(gSg^{-1}) = \{gxg^{-1} \mid x\in S\}$ $\quad \begin{pmatrix} x \mapsto gxg^{-1} \\ g^{-1}yg \leftarrow\!\shortmid y \end{pmatrix}$

2) תהי G p-חבורה סופית (p ראשוני, $|G|=p^k$) תהי G פועלת על קבוצה סופית A. יהי $Fix(A)=\{a\in A : g*a=a\}$

אזי $|Fix(A)| \equiv |A| \mod p$

3) תהי G חבורה, $H\leq G$ תת חבורה. אזי G פועלת על הקבוצת המחלקות G/H

אכן, יהי $g*aH=gaH$. הפעולה מוגדרת היטב. אכן,

אם $aH=bH$ $(a,b\in G)$ אזי ק"מ $h\in H$ כך ש $b=ah$

כלומר, $gb=gah \Rightarrow gbH=gaH$. והפעולה מוגדרת היטב.

4) G פועלת על קבוצה A. תהי H תת חבורה של G. אזי מקבלים פעולה של H על A על ידי צמצום. לכל $h\in H$, $h*a$ כבר מוגדר כי $h\in G$

למשל: S_n פועלת על $\{1,\dots,n\}$, A_n גם פועלת

הגדרה: תהי G חבורה סופית, יהי p ראשוני. אזי $|G|=p^k m$ כאשר $k\geq 0$ ו- $p\nmid m$

למשל אם $p=5$ $|G|=800=5^2\cdot 32$ $(k=2, m=32)$

תת חבורה $P\leq G$ נקראת תת חבורה p-סילו (p-Sylow) אם $|P|=p^k$

(P הינה p-חבורה הכי גדולה שיכולה להיות תת חבורה של G (לפי לגראנז'))

משפטי סילו:

תהי G חבורה סופית, p ראשוני. $|G|=p^k m$ $(p\nmid m)$

1) ל-G יש תת חבורת סילו. לכל $H\leq G$ תת חבורה של G, כך ש H הינה p-חבורה. אזי קיימת תת-חבורת p-סילו P כך ש $H\leq P$

2) כל שתי תתי חבורות p-סילו צמודות זו לזו. כלומר, תהיינה $P,Q\leq G$ תתי חבורות p-סילו. אזי קיים $g\in G$ כך ש $Q=gPg^{-1}$

3) יהי n_p מספר תתי החבורות p-סילו של G
אזי $n_p\equiv 1 \bmod p$ וגם $n_p|m$

קונמה:

$G=S_4$, $p=3$, $|G|=24=3^1\cdot 8$

יש ל-G 4 תתי חבורות מסדר 3:

$\langle(1\,2\,3)\rangle$ $\langle(1\,2\,4)\rangle$ $\langle(1\,3\,4)\rangle$ $\langle(2\,3\,4)\rangle$

ואכן $n_3\equiv 1 \bmod 3$, $n_3|8 \Leftarrow n_3=1 \vee n_3=4$

הוכחה של סילו 1:

נוכיח משפט יותר חזק:

תהי $H\leq G$ תת חבורה מסדר $|H|=p^l$, כאשר $0\leq l<k$

אזי קיימת חבורה $H\leq K\leq G$ כך ש $|K|=p^{l+1}$

נשים לב שטענה זו גוררת את משפט סילו 1

תהי $H\leq G$ p-תת חבורה, $|H|=p^l$

אם $l=k$, אז H כבר תת חבורת p-סילו וסיימנו

אחרת נפעיל את הטענה מספר פעמים $H\leq K_1\leq\ldots\leq K_{k-l}$

הוכחה:

אם $p\nmid|G|$ אזי תת החבורה הטריוויאלית הינה תת חבורה p-סילו. נניח $p\,||G|$

נטפל במקרה שבו $H \trianglelefteq G$ נורמלית. אזי G/H הינה חבורה
וכן $|G/H| = \frac{|G|}{|H|} = \frac{p^k m}{p^l}$. הנחנו כי $l < k$, לכן $p \mid |G/H|$
לפי משפט קושי, יש תת חבורה $L \leq G/H$ מסדר p. בפרט
$p = [L : \{e_{G/H}\}]$
תהי $\varphi : G \to G/H$ ההטלה הטבעית. לפי משפט האיזו הרביעי
קיימת תת חבורה $H \leq K \leq G$ כך ש $L = \varphi(K)$.
ההתאמה הזאת שומרת אינדקסים. לכן

$$[K:H] = [\varphi(K) : \varphi(H)] = [L : \{e_{G/H}\}] = p$$

לכן, $|K| = p|H| = p^{l+1}$ וסיימנו

אם H אינה נורמלית?
G/H לא חבורה ולכן לא נוכל להשתמש במשפט קושי.
נזכר במנרמל $N_G(H) = \{g \in G : \forall h \in H : ghg^{-1} \in H\}$
הוכחנו כבר ש $H \trianglelefteq N_G(H)$, לכן חבורת המנה $N_G(H)/H$ מוגדרת
אם הסדר שלה מתחלק ב- p. אזי, לפי משפט קושי נקבל תת
חבורה $L \leq N_G(H)/H$ מסדר p. כמו מקודם לפי משפט האיזו
4 נקבל: $H \leq K \leq N_G(H) \leq G$ כך ש $[K:H] = p$ וסיימנו

נותר להוכיח שאם $H \leq G$ תת חבורה מסדר p^l, $0 \leq l < k$ אזי
$p \mid |N_G(H)/H|$?
נתבונן בפעולה של H על קבוצת המחלקות G/H.
(זו הפעולה מהצמצום של הפעולה של G על G/H, המוכרת בתחילת
השיעור) $h * gH = hgH$
נמצא את נקודות השבת:

$gH \in Fix(G/H) \iff h*gH=gH$ $h\in H$ לכל $\iff hgH=gH$ $h\in H$ לכל $\iff$

$\iff g^{-1}hg \in H$ $h\in H$ לכל $\iff g^{-1}\in N_G(H) \iff g\in N_G(H)$

הוכחנו כי $Fix(G/H)=N_G(H)/H$

אם $H=\{e\}$ אזי $N_G(H)=G$, לכן $N_G(H)/H \simeq G$ ואז $p\,|\,|G|$.

אחרת $l\geq 1$ לכן $p\,|\,|H|$. לפי הטענה שהזכרנו בתחילת השיעור,

$|N_G(H)/H| = |Fix(G/H)| \equiv |G/H| \bmod p$

אבל $p\,|\,|G/H|=p^{k-l}m$ (כי הנחנו $l<k$) ולכן,

$|N_G(H)/H| \equiv |G/H| \equiv 0 \bmod p \Rightarrow p\,|\,|N_G(H)/H|$

הערה בדרך הוכחנו:

טענה:

תהי G חבורה, $H\lneq G$ תת-p חבורה, נניח $p\,|\,[G:H]$ אזי

$N_G(H)\supsetneq H$

הוכחה למשפט סילו 2:

תהיינה $P,Q\leq G$ שתי תת-חבורות p-סילו. כלומר $|P|=|Q|=p^k$

(נשים לב שבדרך כלל שתי תת חבורות מאותו סדר לא חייבות להיות צמודות. לדוגמא: $G=S_4$ $H=\{e,(12)(34),(13)(24),(14)(23)\}$

$k=\langle(1234)\rangle$

אזי $|H|=|k|=4$, אבל $H\trianglelefteq S_4$, לכן H,k לא צמודות)

בחזרה להוכחה:

נתבונן בפעולה של P על קבוצת המחלקות G/Q: $\pi * gQ = \pi gQ$

עבור $\pi\in P$ $gQ\in {}^{G}/_{Q}$. P הינה p-חבורה ולכן
$|Fix({}^{G}/_{Q})|\equiv|{}^{G}/_{Q}| \mod p$

אבל, $|{}^{G}/_{Q}| = \frac{|G|}{|Q|} = \frac{p^k m}{p^k} = m$

לכן $p\nmid|{}^{G}/_{Q}|$ ולכן $p\nmid|Fix({}^{G}/_{Q})|$. בפרט $Fix({}^{G}/_{Q})\neq\emptyset$. אזי קיימות נקודות שבת.

תהי $gQ\in Fix({}^{G}/_{Q})$ נק' שבת של הפעולה הנ"ל

אזי $gQ = \pi * gQ = \pi gQ$ לכל $\pi\in P$ זה אומר $g^{-1}\pi g\in Q$ לכל $\pi\in P$

כלומר, $g^{-1}Pg\subseteq Q$ אבל אלה שתי קבוצות סופיות מאותה עוצמה p^k

לכן $g^{-1}Pg = Q \Leftarrow Q=gPg^{-1}$, כמו שצריך

מסקנה של משפט סילו 2:

תהי G חבורה, p ראשוני. יהי n_p מספר תת חבורות p-סילו. אזי
$P\trianglelefteq G \Longleftrightarrow n_p=1$

הוכחה:

($\Rightarrow$) נניח $n_p=1$. כלומר, יש רק תת חבורה p-סילו אחת, P.

יהי $g\in G$. אזי $gPg^{-1}\leq G$ היא תת חבורה p-סילו כי: $|gPg^{-1}|=|P|$

אבל יש רק אחת ולכן $gPg^{-1}=P$ לכל $g\in G$ כלומר $P\trianglelefteq G$

($\Leftarrow$) תהי $P\leq G$ תת חבורה p-סילו. נניח $P\trianglelefteq G$. תהי $Q\leq G$ תת חבורה p-סילו אחרת. אזי $Q=gPg^{-1}$ עבור $g\in G$ מתאים, לפי משפט סילו 2.

אבל $P\trianglelefteq G \Rightarrow P=Q \Rightarrow n_p=1$

הוכחה של סילו 3:

תהי $Syl_p(G)$ הקבוצה של תתי החבורות p-סילו של G

G פועלת על $Syl_p(G)$ ע"י הצמדה. $g*P=gPg^{-1}$

לפי משפט סילו 2, הפעולה הנ"ל טרנזיטיבית. לכן יש רק מסלול אחד

והגודל שלו הוא $|Syl_p(G)|=n_p$

תהי $P\in Syl_p(G)$ תת חבורה p-סילו של G. לפי משפט מסלול מייצב:

$n_p=|Syl_p(G)|=|G*P|=[G:G_P]$

כאשר G_P הוא המייצב $G_P=\{g\in G: g*P=P\}$

ואכן: $g\in G_P \iff g*P=gPg^{-1}=P \iff g\in N_G(P)$

אנחנו יודעים כי $P\le N_G(P) \Rightarrow p^k \mid |N_G(P)| \Rightarrow |N_G(P)|=p^k m'$

כאשר $p\nmid m'$

לכן $[G:N_G(P)]=\frac{p^k m}{p^k m'}=\frac{m}{m'}$. ולכן $n_p=[G:N_G(P)] \mid m$

נשאר להוכיח כי $n_p\equiv 1 \bmod p$

תהי P תת חבורה p-סילו, ונתבונן בפעולה של P על $Syl_p(G)$

על ידי הצמדה (צמצום של הפעולה הקודמת) $\pi * Q=\pi Q\pi^{-1}$

עבור $\pi\in P$, $Q\in Syl_p(G)$

נשים לב כי $P\in Syl_p(G)$ הינה נקודת שבת של הפעולה. אכן:

$\pi P\pi^{-1}=P$ לכל $\pi\in P$

תהי $Q\in Syl_p(G)$ נקודת שבת. אז', $\pi * Q=\pi Q\pi^{-1}=Q$ לכל $\pi\in P$

$\Leftarrow$ $\pi\in N_G(Q)$ לכל $\pi\in P$ $\Leftarrow$ $P\le N_G(Q)$

לכן P תת חבורה p-סילו של $N_G(Q)$ (אכן $|N_G(Q)| \mid |G|$ לפי לגרנז'

ולכן $N_G(Q)$ לא יכול להתחלק בשום חזקה של p שגדולה מ- $|P|=p^k$)

ואבל גם $Q\le N_G(Q)$. לכן P,Q שתיהן תתי החבורות p-סילו של

המנרמל $N_G(Q)$. ואבל $Q\trianglelefteq N_G(Q)$. לכן, לפי ההוכחה הקודמת, ל $N_G(Q)$

יש רק תת חבורה p-סילו אחת. לכן $P=Q$

אז Q הייתה נקודת שבת שרירותית של הפעולה של P על

$Syl_p(G)$. ולכן יש רק נקודת שבת אחת $|Fix(Syl_p(G))|=1$.

אך P ה"א p חבורה לכן לפי הטענה מתחילת השיעור

$$n_p = |Syl_p(G)| \equiv |Fix(Syl_p(G))| \mod p$$

לכן $n_p \equiv 1 \mod p$

הגדרה: תהי G חבורה. G נקראת פשוטה אם אין לה תתי חבורות נורמליות מלבד G, $\{e\}$

(אם $H \trianglelefteq G$, אזי אפשר לקוות לחקור את G על ידי חקירת החבורות הייתר קטנות $H, G/H$)

טענה:

יהיו p, q שני ראשוניים שונים, $p<q$. תהי G חבורה מסדר pq^k כאשר $k \geq 1$. אזי G לא פשוטה.

תוצאה:

אין חבורות פשוטות מסדר $375 = 3 \cdot 5^3$

הוכחה:

לפי סילו 3, $n_q \equiv 1 \mod q$

$n_q | p \Rightarrow n_q = 1$ או $n_q = p$

אבל $q<p$, לכן $p \equiv 1 \mod q \Rightarrow n_q = 1$

לכן ל-G יש תת חבורה Q סילו נורמלית. לכן G אינה פשוטה

תזכורת:

תהי G חבורה, $N \trianglelefteq G$, $H \trianglelefteq N$ אזי H לא בהכרח נורמלית ב- G. ראינו את הדוגמא:

$G = A_4$

$N = \{e, (12)(34), (13)(24), (14)(23)\}$

$H = \{e, (12)(34)\}$

$N \trianglelefteq G$, $H \trianglelefteq N$ אבל $H \ntrianglelefteq G$ (A_4 אינה פשוטה)

טענה:

תהי G חבורה, $N \trianglelefteq G$ תת חבורה נורמלית. תהי $P \leq N$ תת חבורה p-סילו של N (לאו דווקא p-סילו של G). נניח $P \trianglelefteq N$ אזי $P \trianglelefteq G$

הערה: אם לא היינו מניחים P p סילו של N, הטענה לא הייתה נכונה

הוכחה:

יהי $g \in G$. צריך להוכיח $gPg^{-1} = P$

הנחנו כי $N \trianglelefteq G$ נורמלית, לכן סגורה להצמדה. לכן $gPg^{-1} \leq N$

ולכן gPg^{-1} הינה תת חבורת p-סילו של N. אבל לפי ההנחה

ל-N יש רק תת חבורה p-סילו אחת, כי יש לה תת חבורה p-סילו

נורמלית. ולכן $gPg^{-1} = P$

טענה:

תהי G חבורה מסדר 30, אזי ל-G יש תת חבורה 5-סילו נורמלית

הוכחה:

$|G| = 30 = 5 \cdot 6$, לכן כל תת חבורה 5-סילו של G היא מסדר $5^1 = 5$

לפי משפט סילו 3, $n_5 \equiv 1 \bmod 5$, $n_5 | 6$

לכן $n_5 = 1$ או $n_5 = 6$. אם $n_5 = 1$ אזי אכן יש תת חבורה 5-סילו

נורמלית. נניח בשלילה כי $n_5 = 6$

זה אומר שיש 6 תתי חבורות 5-סילו. כל אחת מסדר 5

לכן, לכל אחת יש 4 איברים מסדר 5 וגם e.

תהיינה P, Q תתי חבורות 5-סילו שונות. אזי $|P \cap Q| = 1$ לפי לגרנז'

(אם $|P \cap Q| = 5$, אזי $P = P \cap Q = Q$ בסתירה להנחה שהן שונות)

לכן ב-G $6 \cdot 4 = 24$ איברים מסדר 5

נבחן כמה תתי חבורות 3-סילו יש ב-G. $|G| = 30 = 3 \cdot 10$

$n_3 \equiv 1 \mod 3$ $n_3 | 10$ $\Leftarrow$ $n_3 = 1, 10$

אם $n_3 = 10$ יש עשר תתי חבורות 3-סילו. בכל אחת 3 איברים

כלומר, e ו-2 איברים מסדר 3. כמו מקודם החיתוכים טריוויאלים

לכן יש $2 \cdot 10 = 20$ איברים שונים מסדר 3

עכשיו יש חבורה G מסדר 30. יש ב-24 איברים מסדר 5

וגם 20 איברים מסדר 3 - לא ייתכן. לכן $n_3 \neq 10$ $\Leftarrow$ $n_3 = 1$

תהי P תת חבורה 5-סילו, Q תת חבורה 3 סילו

ולכן PQ הינה תת חבורה של G

$PQ = \{\pi q : \pi \in P, q \in Q\}$

לפי משפט האיזו' השני $PQ/Q \simeq P/P\cap Q$

אך $P \cap Q = \{e\}$ לפי לגרנג' $\Leftarrow$ $\frac{|P|}{|P\cap Q|} = \frac{5}{1} = 5 = \frac{|PQ|}{|Q|}$ $\Leftarrow$ $|PQ| = 15$

לכן $[G:PQ] = \frac{30}{15} = 2$ ולכן $PQ \trianglelefteq G$. זה אומר ש PQ סגורה

להצמדה. אז PQ מכילה את P, לכן PQ מכילה את כל

תתי החבורות 5-סילו, שכולן צמודות ל-P. אך בין P והצמודות

שלה יש 24 איברים מסדר 5. אין מקום לכולם בתוך PQ

מסדר 15. בסתירה. לכן $n_5 \neq 6$, ולכן $n_5 = 1$

לכן, ל G יש תת חבורה 5 סילו נורמלית.