1) באגודה X סופית יש לפחות אדמ' אחד.

<u>הוכחה:</u> כיוון ש-X סופית קיימת לה $K \leq X$ תת-אגודה מינימלית (כך ש: $\emptyset \neq K_1 \leq K \rightarrow K_1 = K$) יהא $a \in K$ אזי $aK = \{ak : k \in K\} \leq K$ אבל K מינימלית ולכן aK=K.

מכאן שהקבוצה $A = \{k \in K, ak = a\}$ אינה ריקה.

נשים לב כי $A \leq K$, נראה סגירות:

$$k_1, k_2 \in A : ak_1 = a, ak_2 = a \rightarrow ak_1k_2 = ak_2 = a \rightarrow k_1 * k_2 \in K$$

שוב מתוך המינימליות נסיק כי A=K, מכאן שיש לפחות אדמ' אחד.

2) מופיע בסוף.

3) משפט ווילסון – Wilson

מספר טבעי $n > 1$ הוא מספר ראשוני אם"ם $(n-1)! \equiv (-1)(mod\ n)$

<u>הוכחה</u>

<u>בכיוון האחד</u>: עבור $n = p > 1$ ראשוני חבורת אוילר היא: $U_p = 1, 2, ..., p-1$. כל איבר $a \in U_p$ ההפוך לעצמו מקיים: $a^2 - 1 = (a-1)(a+1) \equiv 0 \pmod p$ כלומר: $a \equiv \pm 1 \pmod p$. מכאן שלמעט ± 1 לכל איבר יש הופכי שהוא אחר ממנו. לכן כיוון שהחבורה אבלית, במכפלת האיברים $m = (p-1)!$ האיבר היחיד שאינו מצטמצם (ע"י סידור כל איבר ליד ההופכי שלו) הוא: $m = p - 1 \equiv (-1) \pmod p$.

<u>בכיוון ההפוך</u>: נניח בשלילה כי n אינו ראשוני. אם $n = 4$ קל לבדוק כי: $(4-1)! = 6 \equiv 2 \pmod 4$. סתירה.

עבור $n > 4$: כיוון ש- n אינו ראשוני, ישנו לפחות מספר אחד $1 < a \leq n-1$ שמחלק את n.

אם: $a = \sqrt{n}$ אזי: $4 < n \Leftarrow 2 < a \Leftarrow 2a < a^2 = n$ כלומר $a, 2a$ מופיעים כ"א במכפלה $(n-1)!$ ומכפלתם מאפסת אותה בסתירה לנתון.

אחרת (a אינו שורש של n) מתקיים: $\exists 0 < a \neq b < n : a \cdot b \equiv 0 \pmod n$. לכן ab מופיע במכפלה: $(n-1)!$ ושוב מאפס אותה בסתירה לנתון.

4) **משפט לגרנז':** תהא G חבורה סופית, אזי לכל ת"ח $H \leq G$ מתקיים $[G:H] = \frac{|G|}{|H|}$

הוכחה לקבוצה של רוני ביתן:

לכל $a \in G$ נגדיר את ההעתקה $\varphi_a = H \to Ha$

ההעתקה חח"ע שכן $h_1 a = h_2 a \Rightarrow h_1 = h_2$

וברור שהיא על (מעצם הגדרתו) ולכן $|H| = |Ha|$.

כיוון שהקוסטים הם מחלקות שקילות, G הוא איחוד זר שלהם ולכן $|G| = [G:H]|H|$

<u>הוכחה לקבוצה של מגרל:</u>

<u>משפט לגרנז'</u>

נניח $(G,\cdot)$ חבורה, $H \leq G$ אז.

① $\biguplus_{g\in G} gH = G$ "חלוקה"

② $g_1H = g_2H \iff g_1^{-1}g_2 \in H \overset{def}{=} g_1 \overset{L}{\equiv} g_2 \bmod H$

③ $|G| = |H|\cdot[G:H]$

(<u>תזכורת:</u> $[G:H] \overset{def}{=} |G/H|$ האינדקס של H ב-G)

<u>הוכחה</u>

<u>רעיון להוכחה:</u>

$$G = \overbrace{\boxed{H}\quad \boxed{g_1H}\quad \boxed{g_2H}\ \cdots\ \boxed{g_kH}}^{[G:H]}$$

<u>שלב א'</u>

נוכיח $\overset{L}{\equiv}$ יחס שקילות ב-G.

① $g \overset{L}{\equiv} g \bmod H$ כי $g^{-1}g = e \in H$ (רפלקסיביות)

② $g_1 \equiv g_2 \Rightarrow g_2 \equiv g_1$ (סימטריות)

<u>הסבר:</u> $g_1^{-1}g_2 \in H \Rightarrow (g_1^{-1}g_2)^{-1} \in H \Rightarrow g_2^{-1}g_1 \in H$

③ $\begin{cases} g_1 \equiv g_2 \\ g_2 \equiv g_3 \end{cases} \Rightarrow g_1 \equiv g_3$ (טרנזיטיביות)

<u>הסבר:</u> $\begin{cases} g_1^{-1}g_2 \in H \\ g_2^{-1}g_3 \in H \end{cases} \overset{\text{סגירות}}{\Rightarrow} g_1^{-1}g_3 = (g_1^{-1}g_2)(g_2^{-1}g_3) \in H$

לפי תכונה בסיסית של יחס שקילות ($X = \biguplus_{x\in X}[x]$)

$G = \biguplus_{g\in G}[g]$ חלוקה כאשר

$[g] = \{x\in G \mid g \overset{L}{\equiv} x \bmod H\} = \{x\in G \mid g^{-1}x \in H\} = \{x \in G \mid x \in gH\} = gH$

לכן $[g] = gH$ ולכן:

① $G = \biguplus_{g\in G} gH$ וגם ②

<u>שלב ב'</u>

$|gH| = |H|$ כי $gH = L_g(H)$ כאשר $S_G \ni L_g : G \to G$ הפיכה

<u>תזכורת</u>

L_g חח"ע ועל ולכן שומרת על עוצמת הקבוצה. אז ...

③ $|G| = |H|\cdot[G:H]$ (...) מ.ש.ל.

5) משפט אוילר

$$\forall a \in \mathbb{Z}^*, n \in \mathbb{N} : (a,n)=1 \Rightarrow a^{\varphi(n)} \equiv 1 (mod\ n)$$

<u>הוכחה</u>

$$(a,n)=1 \Rightarrow a \equiv a' \in U_n \Rightarrow a^{\varphi(n)} \equiv a'^{|U_n|} = 1$$

6) משפט האיזומורפיזם הראשון:

אם $\varphi: G \to H$ אפימורפיזם אז קיים איזומורפיזם $\psi: G/_{\ker(\varphi)} \cong H$ כך ש $\varphi = \psi \circ \nu$ כאשר $\nu: G \to G/_{\ker(\varphi)}$ הוא ההומומורפיזם הטבעי.

<u>הוכחה:</u>

נסמן $K = \ker(\varphi)$ ונגדיר את ההעתקה $\psi: G/K \to H$ ע"י $\psi(Ka) = \varphi(a)$

צ"ל שההעתקה מוגדרת היטב כלומר שהתמונה של Ka לא תלויה בבחירת הנציג.

$$Ka = Kb \Leftrightarrow ab^{-1} \in K \Leftrightarrow \varphi(ab^{-1}) = 1_H \Leftrightarrow \varphi(a) = \varphi(b)$$

נבדוק שψ הומומורפיזם, נעזר בעובדה כי $K \lhd G$:

$$\psi(Ka * Kb) = \psi(Kab) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(Ka)\psi(Kb)$$

כעת נבדוק כי ψ חח"ע:

$$\ker(\psi) = \{Ka: a \in G\ |\varphi(a) = 1_H\} = \{Ka: a \in K\} = \{K\}$$

נתון כי φ על כלומר $\forall h \in H \exists a: \exists a \in G: \varphi(a) = h$

לכן מתוך ההגדרה של ψ המקור של h יהיה Ka תחת ψ.

7) כל חבורה סופית G איזומורפית לתת חבורה של S_G

<u>הוכחה</u>

נגדיר את ההעתקה $\varphi : G \to S_G$ ע"י $a \mapsto l_a$ כאשר $l_a(x) = ax$ (תמורה של אברי G).

l_a היא אכן תמורה שכן זו העתקה חח"ע $G \to G$.

$$\forall x, y \in G : ax = ay \Rightarrow x = y$$

ומתוך סופיות זוהי גם על.

נבדוק שימור פעולה של φ, כלומר נראה כי:

$$\varphi(ab) \stackrel{?}{=} l_a \circ l_b$$

$$\forall x \in G \ \varphi(ab)(x) = abx = l_a\big(l_b(x)\big) = (l_a \circ l_b)(x)$$

ולכן הומו', נבדוק חח"ע

$$\ker(\varphi) = \{a \in G : l_a = id\} = \{a \in G : ax = x\} = \{e\}$$

ולכן בסה"כ φ מונו' כלומר $G \cong \varphi(G) \leq S_G$

8) מופיע בסוף.

9) נוסחת המחלקה

תהא G חבורה סופית, אזי:

$$|G| = |Z(G)| + \sum_{\substack{x\ represent \\ \notin Z(G)}} \frac{|G|}{|C(x)|}$$

הוכחה

נתייחס לפעולת הצמדה של G לעצמה

$$\forall x \in G : Stb(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = gx\} = C(x)$$

$$\forall x \in G : |G * x| = [G : stb(x)] = \frac{|G|}{|C(x)|}$$

$$|G| = \sum_{x\ rep} |G * x| = \sum_{x\ rep} \frac{|G|}{|C(x)|} \underbrace{=}_{\text{במרכז כל איבר הוא מחלקת צמידות של עצמו כלומר באורך1}} |Z(G)| + \sum_{\substack{x\ rep \\ \neq Z(G)}} \frac{|G|}{|C(x)|}$$

G איחוד זר של מחלקות צמידות, ולכן

$$|G| = \sum_{x\ rep} |G * x| = \sum_{x\ rep} \frac{|G|}{|C(x)|} \underbrace{=}_{\substack{\text{במרכז}\\ \text{כל}\\ \text{איבר}\\ \text{הוא}\\ \text{מחלקת צמידות}\\ \text{של עצמו}\\ \text{כלומר באורך}1}} |Z(G)| + \sum_{\substack{x\ rep\\ \neq Z(G)}} \frac{|G|}{|C(x)|}$$

10) משפט (למת) Burnside

תהא G חבורה סופית הפועלת על קבוצה סופית X. מספר המסלולים שG יוצרת ב-X הוא

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g|$$

הוכחה

הרעיון הוא לבנות "טבלת נקודות שבת" ולמלא אותה באמצעות הפונקציה:

$$T(g,x) = \begin{cases} 0 & g * x \neq x \\ 1 & g * x = x \end{cases}$$

נספור את כל ה-1 בטבלה, לא משנה לפי עמודות או שורות.

$$\sum_{g \in G} |X_g| = \sum_{x \in X} |Stb(x)| = \sum_{i=1}^{k} \sum_{x \in G * x_i} |Stb(x_i)| = \sum_{i=1}^{k} |G * x_i| \frac{|G|}{|G * x_i|} = \sum_{i=1}^{k} |G| = |G|k$$

11) משפט סילו 1:

תהא G חבורה מסדר $p^n m$ כאשר p ראשוני, $n, m \in \mathbb{N}$. אזי קיימת ת"ח p-סילו, הינו ת"ח מסדר p^n.

הוכחה

נראה באינדוקציה על $|G|$.

בדיקת התחלה: $|G| = p$ אז G עצמה p-סילו.

הנחה: הטענה נכונה עבור כל G מסדר $|G| < p^n m$

צ"ל: נכונה עבור $|G| = p^n m$

ישנם שני ממקרים בלבד:

א) קיימת ת"ח $H \leq G$ כך ש: $|H| = p^n m_1$, $m_1 < m$. לפי הנחת האינדוקציה יש בתוך H ת"ח p-סילו ב-G.

ב) לא קיימת ת"ח $H \leq G$ מסדר $p^n m_1$, $m_1 < m$.

כלומר כל ת"ח היא מסדר $p^{n_1 < n} m$. באופן כללי יתכן גם: $m_1 \leq m$

$$\forall H \leq G : p | [G:H] = \frac{|G|}{|H|}$$

מכאן ע"פ נוסחת המחלקה:

$$p^n m = \underbrace{|G|}_{\substack{\text{מתחלק} \\ p\text{ב}}} = |Z(G)| + \underbrace{\sum_{\substack{x\ rep \\ \notin Z(G)}} [G:C(x)]}_{\substack{\text{מתחלק} \\ p\text{ב}}} \Rightarrow \ p \mid |Z(G)| \Rightarrow Z(G) \neq \{e\}$$

כעת כיוון $Z(G)$ אבלית ו $p \mid |Z(G)|$ קיים איבר מסדר p (טענה קודמת),נשים לב כי:

$$(a \in Z(G)) \ \ H = < a > \lhd G$$

$$|G/_H| = \frac{p^n m}{p} = p^{n-1} m$$

ע"פ הנחת האינדוקציה, יש ל$G/_H$ תת-חבורה p-סילו, כלומר $\exists A \leq G/_H$ כך ש: $|A| = p^{n-1}$

$$H \lhd G \Rightarrow \text{קיים אפי}: \nu: G \to G/_H \ , \qquad g \mapsto gH$$

נסמן: $A^* = \nu^{-1}(A) \leq G$. נמצם את ν ל:

$$\nu_0: A^* \to A$$

$$e \in A \Rightarrow \ker(\nu) = \ker(\nu_0) = H$$

לפי משפט איזו' 1:

$$A^*/_{\ker(\nu_0)} = A^*/_H \cong A$$

$$|A^*| = |H||A| = pp^{n-1} = p^n$$

12) משפט סילו 2:

תחת התנאים של משפט סילו 1 $(|G| = p^n m, (p,m) = 1)$:

א) כל ת"ח $H \le G$ מסדר p^k כאשר $1 \le k \le n$ מוכלת באיזשהי ת"ח p-סילו.
ב) כל שני ת"ח p-סילו הם צמודות.

הוכחה

תהא $H \le G$ עם $|H| = p^k$.

קבוצת ת"ח p- סילו= Syl_p

ע"פ משפט סילו 1:

$$Syl_p \neq \phi$$

תהא $P \in Syl_p$ ונגדיר פעולה $H \times G/_p \to G/_p$ ע"י $(h, xP) \mapsto hxP$

פעולת H מחלקת את איברי $G/_P$ למסלולים זרים. נזכר כי H היא חבורת p, ולכן:

$$m = |G/_P| = \sum_{x\ rep} |H * xp| = \sum_{x\ rep} [H : Stb(xp)] = \sum_{x\ rep} p^{r_x}$$

<u>אבל</u> $(m,p) = 1$ ולכן בהכרח לפחות $r_x = 0$ עבור x אחד, כלומר קיימת לפחות נקודת שבת אחת, כלומר קיים xP כל שלכל $h \in H$

$$hxP = xP \Leftrightarrow x^{-1}hxP = x^{-1}xP = P \Leftrightarrow x^{-1}hx \in P \Leftrightarrow h \in xPx^{-1} \Rightarrow H \subseteq xPx^{-1}$$

$$|xPx^{-1}| = |P| = p^n$$

ב)

ע"פ סעיף קודם בפרט לכל $P_1 \in SyL_p(G)$ (מסדר p^n) ולכל בחירה התחלתית של $P_2 \in SyL_p(G)$ קיים x כך כלשהו כך ש: $P_1 \subseteq xP_2x^{-1}$.

אבל $|P_1| = p^n = |P_2| = |xP_2x^{-1}|$ ולכן $P_1 = xP_2x^{-1}$.

(ההצמדה לא משנה את גודל הקבוצה!).

13) משפט סילו 3

עבור חבורה G נסמן $n_p = \left|Syl_p(G)\right|$

א) $n_p = [G: N_G(P)]$

ב) $n_p \equiv 1(mod\ p)$

ג) $n_p = (1+kp)|_m$ כאשר $k \in \mathbb{N} \cup \{0\}, (m,p) = 1, m = \frac{|G|}{p^n}$

הוכחה

א) נגדיר את הפעולה $G \times Syl_p(G) \to Syl_P(G)$ ע"י $(g,P) \mapsto g * P = gPg^{-1}$.

ע"פ משפט סילו 2 הפעולה היא הומוגנית (יש מסלול אחד).

לכן $n_p = |G * P| = [G: Stb(P)] = [G: N_G(P)]$

כי $Stb(P) = \{g \in G: gPg^{-1} = P\} = N_G(P)$

ב) תהא $P \in Syl_P(G)$ ונתייחס לצמצום של פעולת ההצמדה לפעולת P בלבד. כעת הפעולה כבר לא בהכרח הומוגנית!

$$P \times Syl_p(G) \to Syl_g(G) : (p, P_1) \mapsto pP_1p^{-1}$$

גודל כל מסלול: $\forall Q \in Syl_g(G) :\ |P * Q| = [P: Stb(Q)]$ מחלק את $|P| = p^n$, כלומר אורך כל מסלול הוא מאורך 1 או חזקה של p.

ומכאן ע"פ נוסחת המחלקה הכללית:

$$\left|Syl_g(G)\right| = |X| = |F| + \sum_{\substack{Q\ rep \\ \notin F}} [P: Stb(Q)] = \frac{p^n}{p^{r<n}}$$

ונקבל כי $|F| \equiv n_p(mod\ p)$

אנו נראה כי $F = \{P\}$ (P היא נקודת השבת היחידה).

מצד אחת $P \in F$ שכן: $P * P = \{pPp^{-1} : p \in P\} = \{P\}$

מצד שני, יהי $Q \in Syl_g(G)$ כך ש$Q \in F$, אזי $P \leq N_G(Q)$ שכן Q היא נקודת שבת תחת הצמדה של אברי P:

$\forall p \in P: pQp^{-1} = Q$ ולכן $P, Q \leq N_G(Q)$.

קבלנו שתי ת"ח p-סילו ב$N_G(Q)$. אבל $Q \lhd N_G(Q)$ ולכן היא היחידה, כלומר $P = Q$.

<u>מסקנה:</u>

$$|\mathrm{F}| = 1 \Rightarrow \mathrm{n_p} \equiv |F|(mod\ p) = 1$$

ג) ע"פ לגראנז':

$$[G: P] = \frac{|G|}{|P|} = \frac{|G|}{|N_G(p)|}\frac{|N_G(P)|}{|P|} = [G: N_G(P)][N_G(P): P]$$

$$\Rightarrow n_p|_{\frac{|G|}{|P|} = m}$$

צריך להזכיר שעפ"י סעיף א': $n_p = \left[G : N_G\left(P\right)\right]$.

14) כל חבורת p פתירה

טענת עזר

תהא G חבורת p מסדר p^n (p ראשוני), אזי לכל $1 \leq k \leq n$ קיימת ת"ח נורמלית ב-G מסדר p^k.

הוכחת טענת העזר

באינדוקציה על $|G| = p^n$

התחלה: אם $|G| = p$ אז ניקח את G עצמה.

הנחה: נניח שהטענה נכונה לכל G כך ש$|G| < p^n$, צ"ל עבור $|G| = p^n$.

בחבורת p המרכז $Z(G)$ לא טריוויאלי.

כחבורה אבלית ב$Z(G)$ יש איבר a מסדר p.

נסמן $H =< a >$. כיוון ש$H \leq Z(G)$, $H \lhd G$. נתבונן באפימורפיזם הטבעי $\nu: G \to G/_H, g \mapsto gH$.

ע"פ לגראנז' $|G/_H| = p^{n-1}$ ולכן עפ"י ההנחה לכל $1 \leq k \leq n$ קיימת ת"ח נורמלית $A \lhd G/_H$, $|A| = p^{k-1}$.

נתבונן ב$\widetilde{A} = \nu^{-1}(A)$. כיוון שν הומ', $\tilde{A} \lhd G$. ע"פ משפט איזו' I: $A \cong \widetilde{A}/_{H=\ker\nu}$ (גם בצמצום של ν ל$\tilde{A}$ הגרעין נשאר H).

ולכן $|\tilde{A}| = |H||A| = pp^{k-1} = p^k$ ■

הוכחת המשפט

ע"פ טענת העזר נוכל לבנות סדרה נורמלית

$$G \rhd G_1 \rhd G_2 \rhd \cdots \rhd \{e\}$$

כך שאם $|G| = p^n$ אז $|G_1| = p^{n-1}$ $|G_2| = p^{n-2}$,

ונקבל $G_k/_{G_{k+1}} \cong \mathbb{Z}_p$ ולכן צקלית ולכן אבלית.

משפט (מיון תת-חבורות של חבורה ציקלית סופית): תהא $G=\langle a\rangle$ חבורה ציקלית מסדר n אזי:

1. $H\le G \Leftarrow |H|\,|\,n$,
2. לכל k טבעי: $k\,|\,n$, קיימת ת"ח יחידה $H\le G$ כך ש: $|H|=k$.

הוכחה:

1. עפ"י משפט לגרנז'.
2. כל ת"ח של חבורה ציקלית היא ציקלית. כמו כן לכל $k\,|\,n$:

$$o\left(a^j\right)=k \iff k=\frac{n}{(j,n)} \iff (j,n)=\frac{n}{k}$$

עבור $j=\frac{n}{k}$ מקבלים <u>קיום</u>. באופן כללי אם: $j=\frac{n}{k}t$ אז ממילא: $a^j\in\left\langle a^{n/k}\right\rangle$ ומכאן ה<u>יחידות</u>. □

משפט (מתי מכפלה ישרה של שתי חבורות ציקליות היא חבורה ציקלית):

לכל $n,m\in\mathbb{N}$: $(n,m)=1 \iff \mathbb{Z}_n\times\mathbb{Z}_m\simeq\mathbb{Z}_{nm}$.

הוכחה:

בכיוון $\Leftarrow$ נגדיר: $\varphi:\mathbb{Z}_{nm}\to\mathbb{Z}_n\times\mathbb{Z}_m$ ע"י: $\varphi\left(x\left(\operatorname{mod} nm\right)\right)=\left(x\left(\operatorname{mod} n\right),x\left(\operatorname{mod} m\right)\right)$.

כיוון ש: $(n,m)=1$ תכונות העל וחח"ע נובעות ממשפט השאריות הסיני. נראה שימור פעולה:

$$\begin{aligned}\varphi\left((x+y)\left(\operatorname{mod} nm\right)\right)&=\left((x+y)\left(\operatorname{mod} n\right),(x+y)\left(\operatorname{mod} m\right)\right)\\&=\left(x\left(\operatorname{mod} n\right),x\left(\operatorname{mod} m\right)\right)+\left(y\left(\operatorname{mod} n\right),y\left(\operatorname{mod} m\right)\right)\\&=\varphi\left(x\left(\operatorname{mod} nm\right)\right)+\varphi\left(y\left(\operatorname{mod} nm\right)\right)\end{aligned}$$

מכאן שזהו איזומורפיזם.

בכיוון $\Rightarrow$: נתון כי: $\mathbb{Z}_n\times\mathbb{Z}_m$ ציקלית, כלומר: $\exists(a,b)\in\mathbb{Z}_n\times\mathbb{Z}_m:\ o\left((a,b)\right)=nm$.

נשים לב כי: $(a,b)^{[n,m]}=\left([n,m]a,[n,m]b\right)=(nu,mv)=(0,0)$.

אם כן: $nm=o\left((a,b)\right)\le[n,m]$ אבל זה יתכן רק כאשר: $nm=[n,m]$ ומכאן ש: $(n,m)=1$. □