1. א) נוכיח שחבורה G סופית אם ורק אם יש לה מספר סופי של תת-חבורות.

$\Leftarrow$) נניח כי G סופית, בגודל n איברים. כל תת-חבורה הינה תת-קבוצה עם תכונות נוספות (סגירות לכפל והפכים). אך ל-G יש 2^n תת-קבוצות, שזה מספר סופי. לכן יש מספר סופי של תת-חבורות.

$\Rightarrow$) נניח שיש מספר סופי של תת-חבורות. כל איבר $g\in G$ יוצר תת-חבורה ציקלית $\langle g\rangle$, ולפי ההנחה ל-G יש מספר סופי של תת"ח ציקליות.
תהי H תת-חבורה ציקלית. אם $H\cong\mathbb{Z}$ אזי ל-H יש שני יוצרים ±1. אם $H\cong\mathbb{Z}_n$ אזי ל-H יש $\varphi(n)$ יוצרים (אם לא זוכרים את זה, מספיק להגיד של-H יש לא יותר מ-n יוצרים, שהרי היא עצמה בגודל n איברים בלבד).

בכל מקרה, כל איבר של G הינו יוצר של תת"ח ציקלית. אבל יש לנו מספר סופי של תת"ח ציקליות, ולכל אחת מהן מספר סופי של יוצרים. לכן ל-G יש רק מספר סופי של איברים, והיא סופית.

<u>הערה</u> השאלה הזאת הופיעה במבחן במבנים אלגבריים השנה שעברה!

ב) הטענה לא נכונה. לדוגמא, נתבונן בחבורה $G=\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\cdots$ (מכפלה קרטזית של $\aleph_0$ עותקים של $\mathbb{Z}_2$). ברור שלכל $g\in G$ מקיים $g^2=e=([0],[0],\ldots)$, לכן $o(g)\le 2$, אבל G אינסופית.

דוגמא אחרת: $G=\mathbb{Q}/\mathbb{Z}$. החבורה הזאת אינסופית, שהרי יש אינסוף מספרים רציונליים בקטע $[0,1)$, וכל אחד שייך למחלקה אחרת של $\mathbb{Q}/\mathbb{Z}$ (כי ההפרש בין שני מספרים שונים בקטע הזה קטן מ-1, לכן לא ב-$\mathbb{Z}$).
אבל יהי $g=\frac{m}{n}\mathbb{Z}\in\mathbb{Q}/\mathbb{Z}$ אזי $g^n=m\mathbb{Z}=0\cdot\mathbb{Z}=e_{\mathbb{Q}/\mathbb{Z}}$
ולכן $o(g)=n$ (יש לזכור שהפעולה הינה חיבור, למרות שרושמים אותה בכפל).
לכן $o(g)$ סופי לכל $g\in G$.

<u>שאלה 2</u> א) יהי $g\in G\setminus\{e\}$ ונניח בשלילה כי g צמוד ל-g^{-1}. אזי קיים $h\in G$ כך ש- $g^{-1}=hgh^{-1}$. תהי $conj(g)$ מחלקת הצמידות של g, ויהי $k\in conj(g)$. אזי קיים $a\in G$ כך ש- $k=aga^{-1}$. נשים לב כי

$$k^{-1}=(aga^{-1})^{-1}=ag^{-1}a^{-1}=a(hgh^{-1})a^{-1}=(ah)g(ah)^{-1}\in conj(g).$$

כלומר, $conj(g)$ סגור להפכים. אך כל $k\in conj(g)$ מקיים $k\neq k^{-1}$. אכן, אם $k=k^{-1}$ אזי $k^2=e$, לכן $o(k)|2$. אבל $o(k)\neq 1$, כי $\{e\}$ הינה מחלקת צמידות בפני עצמה ולכן $k\neq e$, ואילו $o(k)=2$ לא יתכן כי $o(k)\,|\,|G|$ לפי לגרנז', אך הנחנו כי $|G|$ אי-זוגי. לכן $k\neq k^{-1}$ לכל $k\in conj(g)$.

הוכחנו כי $conj(g)$ מתפרק בזוגות $\{k,k^{-1}\}$, לכן יש בה מספר זוגי של איברים. לפי משפט מסלול-מייצב, $|conj(g)|=[G:C_G(g)]$, והמספר הינו מחלק את $|G|$ לפי לגרנז'. לכן $|G|$ גם זוגי, בסתירה להנחה.

ב) יהי $\varphi:G\to G$ הומומורפיזם כלשהו, יהי $h=[g_1,g_2]\in G'$ קומוטטור. אזי

$$\varphi(h)=\varphi(g_1g_2g_1^{-1}g_2^{-1})=\varphi(g_1)\varphi(g_2)\varphi(g_1^{-1})\varphi(g_2^{-1})=\varphi(g_1)\varphi(g_2)\varphi(g_1)^{-1}\varphi(g_2)^{-1}$$
$$=[\varphi(g_1),\varphi(g_2)]\in G'.$$

זה לא מספיק, כי איבר שרירותי $k\in G'$ אינו בהכרח קומוטטור. אבל G' נוצרת על ידי הקומוטטורים לפי הגדרה. לכן k הינו מכפלה של קומוטטורים (והפכיהם, אבל הפכי של קומוטטור הינו גם קומוטטור). כלומר,

$$k=[g_1,g_2][g_3,g_4]\cdots[g_{2r-1},g_{2r}].$$

לכן, $\varphi(k)=\varphi([g_1,g_2])\cdots\varphi([g_{2r-1},g_{2r}])$ וכבר הוכחנו כי $\varphi([g_{i-1},g_i])\in G'$ לכל i. כיוון ש-G' תת-חבורה וסגורה לכפל, זה אומר $\varphi(k)\in G'$.

אז הראנו כי $\varphi(G')\subseteq G'$ לכל φ (הוכחנו את הטענה, והוכחנו בשיעור שהתמונה של תת-חבורה תחת הומומורפיזם היא תת-חבורה). זה אומר ש-G' אופיינית במלואה ב-G.

ג) יהי $G=\mathbb{Z}_2\times S_3$. המרכז הינו

$$Z(G)=Z(\mathbb{Z}_2)\times Z(S_3)=\mathbb{Z}_2\times\{id\}.$$

נגדיר הומומורפיזם $\varphi:G\to G$ על ידי $\varphi([a],\sigma)=([0],(1\,2)^a)$.

נשים לב כי φ מוגדר היטב כי $o((12))=2$ ולכן $(12)^a$ תלוי רק במחלקת השקילות של a מודולו 2. בנוסף, φ הומומורפיזם כי

$$\varphi(([a],\sigma)\cdot([b],\tau)) = \varphi([a+b],\sigma\tau) = ([0],(12)^{a+b}) = ([0],(12)^a(12)^b) = ([0],(12)^a)([0],(12)^b) = \varphi(([a],\sigma))\,\varphi(([b],\tau)).$$

עכשיו, $([1], id)\in Z(G)$, אבל $\varphi(([1], id)) = ([0],(12)) \notin Z(G)$, לכן $Z(G)$ אינה אופיינית במלואה ב-G.

שאלה 3

א) נשים לב כי $|S_{2p}| = (2p)! = 1\cdot 2\cdot 3\cdots (p-1)\cdot p\cdot (p+1)\cdots 2p$. הגורמים היחידים שמתפרקים ב-p הם $p, 2p$. כיוון שהנחנו $2<p$, כל אחד משני המספרים $p,2p$ מתחלק ב-p אך לא ב-p^2.
לכן, $p^2m = (2p)!$, כאשר $p\nmid m$. לכן העוצמה של תת-חבורת p-סילו של S_{2p} הינה p^2, והוכחנו בהרצאה שכל חבורה מסדר p^2 הינה אבלית.

ב) תהי $P\le S_{2p}$ תת-חבורת p-סילו. לפי המיון של חבורות אבליות סופיות, $P\cong\mathbb{Z}_{p^2}$ או $P\cong\mathbb{Z}_p\times\mathbb{Z}_p$. אך $P\cong\mathbb{Z}_{p^2}$ לא יתכן, כי ב-S_{2p} אין איבר מסדר p^2. לכן כל איבר לא-טריוויאלי ב-P הינו מסדר p, כלומר הינו מעגל מאורך p או מכפלה של שני מעגלים זרים כאלה.
זה נותן לנו מוטיבציה לחפש מעגלים זרים מאורך p. אכן, יהיו לדוגמא $a=(1\,2\,3\cdots p)$, $b=(p+1\ p+2\cdots 2p)$. אזי a,b זרים, לכן מתחלפים. לכן

$$\langle a,b\rangle = \{a^ib^j : 0\le i,j<p\}\le S_{2p}.$$

קל לראות שכל האיברים האלה שונים, לכן $|\langle a,b\rangle| = p^2$ ולכן $\langle a,b\rangle$ הינה תת-חבורת p-סילו של S_{2p}. הוכחנו לעיל כי תת-חבורות p-סילו של S_{2p} אינן ציקליות, לכן אי אפשר ליצור אותן על ידי איבר אחד. זה אומר שהקבוצה המייצרת $\{a,b\}$ חייבת להיות מינימלית.

ג) נשים לב כי G הינה תת"ח p-סילוב יחידה של עצמה. לפי משפט קושי, קיים איבר $g\in G$ כך ש- $p=o(g)$, ולכן תת"ח $\langle g\rangle\le G$ מסדר p. אך כפי ההוכחה של המשפט הראשון של סילוב, הוכחנו שאפשר להכניס את $\langle g\rangle$ לשרשרת של תת-חבורות

$$H_1=\langle g\rangle\le H_2\le H_3\le\cdots\le H_{n-1}\le H_n=G,$$

כאשר $|H_i|=p^i$. לכן, קיימת תת"ח $H_{n-1}\le G$ מסדר p^{n-1}. האינדקס שלה הינו $\frac{p^n}{p^{n-1}}=p$. כיוון שזה הראשוני היחיד, ובפרט הכי הקטן, שמחלק את $|G|$, ניתן להסיק על פי משפט מן התרגול כי $H_{n-1}\trianglelefteq G$.

פתרון אחר: נעשה אינדוקציה על n. אם $n=1$, אזי $\{e\}\trianglelefteq G$ הינה תת"ח נורמלית (הוכחנו בהרצאה כי התת"ח הטריוויאלית תמיד נורמלית) מסדר $p^{n-1}=1$. זה בסיס האינדוקציה.

כיוון ש-G p-חבורה, ידוע כי $Z(G)$ לא טריוויאלי. כיוון שהמרכז תמיד תת"ח נורמלית, מקבלים חבורת מנה $G/Z(G)$ מסדר p^k, כאשר $0\le k<n$.

אם $k\neq 0$, אזי באינדוקציה קיימת תת"ח $L\trianglelefteq G/Z(G)$ מסדר p^{k-1}, כלומר מאינדקס p. לפי משפט האיזומורפיזם הרביעי, $L=K/Z(G)$, כאשר $K\trianglelefteq G$ הינה תת"ח נורמלית מאינדקס p, כלומר מסדר p^{n-1}. אזי K הינה התת"ח שחיפשנו.

נשאר לטפל במקרה $k=0$, כלומר $Z(G)=G$. זה אומר כי G אבלית. כיוון שכל תת"ח של חבורה אבלית הינה נורמלית, צריך רק להוכיח שקיימת תת"ח מסדר p^{n-1}. לפי המיון של חבורות אבליות סופיות,

$$G\cong\mathbb{Z}_{p^{n_1}}\times\mathbb{Z}_{p^{n_2}}\times\cdots\times\mathbb{Z}_{p^{n_r}}$$

כאשר $n_1+\cdots+n_r=n$. התת"ח

$H=p\mathbb{Z}_{p^{n_1}}\times\mathbb{Z}_{p^{n_2}}\times\cdots\times\mathbb{Z}_{p^{n_r}}$ עובדת.

שאלה 4 א) יהי $g\in HK$ קבוע, נסמן $A=\{(h,k)\in H\times K : g=hk\}$. נשים לב כי ל-$A$ אין מבנה של חבורה, לכן אין משמעות לחפש איזומורפיזם בין A לבין $H\cap K$. פשוט נבנה פונקציה חח"ע ועל בין שני הקבוצות האלה.

נבחר זוג ספציפי $h\in H$, $k\in K$, כך ש- $g=hk$. הוא קיים כי $g\in HK$

לכן שיש יותר מזוג אחד כזה. אולם נבחר אחד. נשים לב שאם $x\in H\cap K$,
אזי בפרט $x\in H$, $x^{-1}\in K$ (כי K סגורה תחת הפכים) ומקיים
$(hx)(x^{-1}k)=hk=g$.

כלומר, $(hx,x^{-1}k)\in A$ אז נגדיר פונקציה

$$f: H\cap K\longrightarrow A$$
$$f(x)=(hx,x^{-1}k)$$

אני טוען כי f חח"ע ועל.

<u>f חח"ע</u> יהיו $x,y\in H\cap K$ כך ש-$f(x)=f(y)$ אזי $(hx,x^{-1}k)=(hy,y^{-1}k)$ ובפרט $hx=hy$. מצמצמים את h, ומקבלים $x=y$.

<u>f על</u> יהי $(h',k')\in A$ יהי $x=h^{-1}h'$, כך ש- $h'=hx$.
כיוון ש-$g=h'k'$, רואים כי $k'=(h')^{-1}g=(hx)^{-1}g=x^{-1}h^{-1}g=x^{-1}h^{-1}hk=x^{-1}k$.

בפרט, $x=h^{-1}h'=k(k')^{-1}$. מזה נובע כי $x\in H\cap K$. והוכחנו כי $(h',k')=(hx,x^{-1}k)=f(x)$. לכן f על.
סך הכל הוכחנו כי $|A|=|H\cap K|$ כמו שנדרש.

ב) לפי ההנחה, $\gcd(|H|,[G:H])=1$. כיוון ש- $K\trianglelefteq G$, ניתן להיעזר במשפט האיזומורפיזם השני ולהוכיח כי $HK/K\cong H/H\cap K$. בפרט, הסדרים של שני חבורות המנה האלה שווים, לכן $\frac{|H|}{|H\cap K|}=\frac{|HK|}{|K|}$, ולכן $[K:H\cap K]=\frac{|K|}{|H\cap K|}=\frac{|HK|}{|H|}$.

תחת ההנחות שלנו, $HK\le G$ ת"ח, לכן לפי לגרנז' קיים $m\in\mathbb{Z}$ כך ש- $|G|=m|HK|$, ובפרט $\frac{|G|}{|H|}=m\frac{|HK|}{|H|}$, כלומר $[K:H\cap K]\mid[G:H]$. אך $|H\cap K|\mid|H|$ לפי לגרנז'. כיוון של-$|H|$ ול-$|G/H|$ אין מחלקים משותפים, כך גם של-$|H\cap K|$ ול-$[K:H\cap K]$ אין. לכן $\gcd(|H\cap K|,[K:H\cap K])=1$, ו- $H\cap K$ הינה ת"ח הול של K.
באופן דומה מטפלים במחצית השנייה של הסעיף. לפי הנ"ל, $|HK/K|=\frac{|HK|}{|K|}=\frac{|H|}{|H\cap K|}$, לכן $|H|\,\big|\,|HK/K|$. מצד שני, $H\le HK$ ת"ח,
לכן $|HK|=m'|H|$ עבור $m'\in\mathbb{Z}$ מתאים, לכן

$$\left[{}^{G}\!/_{K}:{}^{HK}\!/_{K}\right]=\frac{\frac{|G|}{|K|}}{\frac{|HK|}{|K|}}=\frac{|G|}{|HK|}=\frac{|G|}{m'|H|}\Rightarrow m'\left[{}^{G}\!/_{K}:{}^{HK}\!/_{K}\right]=[G:H]\Rightarrow\left[{}^{G}\!/_{K}:{}^{HK}\!/_{K}\right]\Big|[G:H].$$

לכן גם $\gcd\left(\left[{}^{G}\!/_{K}:{}^{HK}\!/_{K}\right],\left|{}^{HK}\!/_{K}\right|\right)=1$, ולכן ${}^{HK}\!/_{K}$ הינה ת"ח הול של ${}^{G}\!/_{K}$.

<u>שאלה 5</u> א) נשים לב כי $144=2^4\cdot 3^2$. לכן מספר החבורות האבליות מסדר 144, עד כדי איזומורפיזם, הינו $P(4)\cdot P(2)=5\cdot 2=10$ החבורות הן

$$
\begin{array}{ccc}
\mathbb{Z}_{16}\times\mathbb{Z}_9 & \simeq & \mathbb{Z}_{144}\\
\mathbb{Z}_2\times\mathbb{Z}_8\times\mathbb{Z}_9 & \simeq & \mathbb{Z}_2\times\mathbb{Z}_{72}\\
\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_4\times\mathbb{Z}_9 & \simeq & \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_{36}\\
\mathbb{Z}_4\times\mathbb{Z}_4\times\mathbb{Z}_9 & \simeq & \mathbb{Z}_4\times\mathbb{Z}_{36}\\
\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_9 & \simeq & \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_{18}\\
\mathbb{Z}_{16}\times\mathbb{Z}_3\times\mathbb{Z}_3 & \simeq & \mathbb{Z}_3\times\mathbb{Z}_{48}\\
\mathbb{Z}_2\times\mathbb{Z}_8\times\mathbb{Z}_3\times\mathbb{Z}_3 & \simeq & \mathbb{Z}_6\times\mathbb{Z}_{24}\\
\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_4\times\mathbb{Z}_3\times\mathbb{Z}_3 & \simeq & \mathbb{Z}_2\times\mathbb{Z}_6\times\mathbb{Z}_{12}\\
\mathbb{Z}_4\times\mathbb{Z}_4\times\mathbb{Z}_3\times\mathbb{Z}_3 & \simeq & \mathbb{Z}_{12}\times\mathbb{Z}_{12}\\
\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_3 & \simeq & \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_6\times\mathbb{Z}_6
\end{array}
$$

בטור הימני מופיעים פירוקים לפי מחלקים אלמנטריים, ואילו בטור השמאלי לפי גורמים אינווריאנטיים. בכל מקרה האיזומורפיזמים נובעים מן המשפט כי $\mathbb{Z}_{mn}\simeq\mathbb{Z}_m\times\mathbb{Z}_n$ כאשר $\gcd(m,n)=1$.

ב) יהי $|G|=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ הפירוק לגורמים ראשוניים של $|G|$, כאשר $p_i\neq p_j$ אם $i\neq j$. יהי P_i תת-חבורה p_i-סילו. אזי $|P_i|=p_i^{e_i}$ ולפי ההנחה, $P_i\simeq\mathbb{Z}_{p_i^{e_i}}$. כיוון ש-$G$ אבלית, היא נילפוטנטית. לפי המשפט האחרון של השיעור האחרון, $G\simeq P_1\times P_2\times\cdots\times P_r\simeq\mathbb{Z}_{p_1^{e_1}}\times\cdots\times\mathbb{Z}_{p_r^{e_r}}$. כיוון שהסדרים של הקומפוננטות זרים, מקבלים $G\simeq\mathbb{Z}_{p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}}=\mathbb{Z}_{|G|}$, כלומר G ציקלית.

<u>פתרון אחר</u> (אם לא זוכרים משפטים על חבורות נילפוטנטיות). נתבונן בתת-חבורה $P_1P_2\cdots P_r$. כיוון שכל תת-חבורה של G נורמלית (כי G אבלית), ניתן להוכיח באינדוקציה כי $P_1\cdots P_j\simeq P_1\times\cdots\times P_j$ לכל $1\le j\le r$ (הרי $P_1\cdots P_j\cap P_{j+1}=\{e\}$ כי הסדרים זרים). לכן, התת-חבורה $P_1\cdots P_r\simeq P_1\times\cdots\times P_r\simeq\mathbb{Z}_{p_1^{e_1}}\times\cdots\times\mathbb{Z}_{p_r^{e_r}}=\mathbb{Z}_{|G|}$ ציקלית. כיוון שהסדר שלה הינו $|G|$, מקבלים $P_1P_2\cdots P_r=G$, ולכן G ציקלית.