1. *Lássuk be, hogy ha $p > q > r$ prímek, és $|G| = pq$ vagy $|G| = pqr$, akkor G p-Sylowja normálosztó!*

Megoldás: Ha $|G| = pq$, akkor $|Syl_p(G)| \equiv 1 \pmod{p}$ és $|Syl_p(G)| \mid q$ miatt $|Syl_p(G)| = 1$, tehát a p-Slylow normálosztó.

Legyen most $|G| = pqr$. Mivel $|Syl_p(G)| \mid qr$, a p-Sylowok száma $1, q, r$ vagy qr lehet. Ha 1, akkor a p-Sylow normálosztó. q vagy r nem lehet, mert $q, r < p$, és $|Syl_p(G)| \equiv 1 \pmod{p}$.

Tehát marad az az eset, amikor $|Syl_p(G)| = qr$. A p-Sylowok prímrendűek, így diszjunktak, tehát ebben az esetben a p-edrendű elemek száma $(p-1)qr = pqr - qr$, így az összes többi elem egy qr elemszámú részhalmazt alkot. Ez tartalmazza az összes q-Sylowot, viszont nem fér bele $q+1$ darab q-Sylow, mert azok legalább $1 + (q-1)(q+1) = q^2 > qr$ elemet fednének le. Így csak egyetlen q-Sylow lehet: $Q \lhd G$. A G/Q faktorcsoport rendje pr, ezért ebben a p-Sylow normálosztó. Legyen ez a p-Sylow $H/Q \lhd G/Q$. Az őséképe $H \lhd G$ rendje $|H/Q| \cdot |Q| = pq$, ezért H p-Sylowja, $P \lhd H$. Ebből következik, hogy $P \operatorname{char} H \lhd G$, így $P \lhd G$, ellentmondva a $|Syl_p(G)| = qr$ feltevésnek.

2. *Legyenek $p > q > r$ prímek, és $|G| = pqr$. Bizonyítsuk be, hogy pqr-nek minden pozitív d osztójához van G-nek d-edrendű részcsoportja.*

Megoldás: 1 és pqr rendű részcsoport nyilván van, és p, q, r rendű is a Sylow-tétel (vagy akár a Cauchy-tétel) miatt. Az előző feladat szerint a p-Sylow, P normálosztó, így a G/P-ben létező q-adrendű és r-edrendű részcsoport őselképe G-ben ad pq rendű és pr rendű részcsoportot. Végül qr rendű részcsoport létezik a Schur-Zassenhaus-tétel miatt: a $P \lhd G$ normálosztónak van komplementuma.

3*. *Milyen p és q prímekre van olyan p^2q rendű csoport, amelynek nincs pq rendű részcsoportja?*

Megoldás: Legyen $|G| = p^2q$, és tegyük fel, hogy G-ben nincs pq rendű részcsoport. Legyen $Q \in Syl_q(G)$. Ekkor $|N_G(Q)| = p^2q, pq$ vagy q . Az első esetben $Q \lhd G$, így G/Q-ban a Cauchy-tétel miatt létező p-edrendű részcsoport őselképe pq rendű részcsoport lenne. A másodikban a normalizátor lenne pq rendű. Tehát csak az utolsó lehetséges. Ekkor viszont $|Syl_q(G)| = p^2$, és a q-Sylowok prímrendűek, így diszjunktak, tehát G-ben $(q-1)p^2 = p^2q - p^2$ darab q-adrendű elem van, és a maradék p^2 elembe csak egyetlen p-Sylow fér. Legyen $P \lhd G$ ez a p-Sylow. P nem lehet ciklikus, mert akkor $C_p \cong P_1 \operatorname{char} P \lhd G$ $\Rightarrow P_1 \lhd G$, és G/P_1-ben van q-adrendű részcsoport, amelynek őselképe G-ben pq rendű lenne.

Marad az az eset, amikor $C_p \times C_p \cong P \lhd G$, és P-ben nincs G-nek p-edrendű normálosztója (mert az azzal vett faktorcsoport q-adrendű részcsoportjának őselképe G-ben az előző esethez hasonlóan pq rendű részcsoportot adna). Ekkor $G = P \rtimes Q$. P egy multiplikatívan írt kétdimenziós vektortér $\mathbb{F}_p$ fölött, Q generátoreleme pedig a konjugálással lineáris transzformációként hat rajta. Pontosan akkor lesz megfelelő a kapott szemidirekt szorzat, ha ennek a lineáris transzformációnak nincs sajátvektora.

Így a kérdés arra redukálódik, hogy milyen p-re és q-ra van olyan $A \in \mathbb{F}_p^{2\times 2}$ mátrix, amelynek nincs sajátértéke $\mathbb{F}_p$-ben, és amelyre $A^q = I$. Ha $m(x)$ a mátrix minimálpolinomja, akkor $m(x) \mid x^q - 1$. $m(x)$ másodfokú, mert nincs gyöke $\mathbb{F}_p$-ben, és osztója a másodfokú karakterisztikus polinomnak. Így $m(x)$ gyökei az $\mathbb{F}_{p^2}$ multiplikatív csoportjában generátorelemek, és q-adrendűek, így $q \mid p^2 - 1$, de $q \nmid p - 1$, tehát $q \mid p + 1$. Ez a feltétel ekvivalens azzal, hogy q páratlan, és $q \mid p + 1$. Ez valóban elegendő ahhoz, hogy megfelelő lineáris transzformációt találjunk ($\mathbb{F}_{p^2}$ additív csoportján a kapott $\alpha \in \mathbb{F}_{p^2}$ elemmel való szorzás pontosan ilyen lineáris transzformáció).

4. *Legyen G véges csoport. Bizonyítsuk be, hogy G akkor és csak akkor ciklikus, ha minden m pozitív egészre az $x^m = 1$ egyenletnek G-ben legföljebb m megoldása van!*

Megoldás: Ha $G = \langle a \rangle$ n-edrendű ciklikus csoport, akkor $1 \le k \le n$-re $(a^k)^m = 1 \Leftrightarrow n \mid km \Leftrightarrow \frac{n}{(n;m)} \mid k\frac{m}{(n;m)} \Leftrightarrow \frac{n}{(n;m)} \mid k$, tehát a megoldások az a^k hatványok, ahol $k = \frac{jn}{(n;m)}$, $j = 1, 2, \ldots, (n;m)$. Így a megoldásszám $(n;m) \le m$.

Tegyük fel, hogy G-ben minden $x^m = 1$ egyenletnek legföljebb m megoldása van. Ekkor G minden H részcsoportja normálosztó, sőt karakterisztikus részcsoport, ugyanis H elemei kielégítik az $x^{|H|} = 1$ egyenletet, és így a feltétel miatt más elem nem elégíti ki ezt. Ebből következik, hogy G minden Sylow-részcsoportja normálosztó, és így G a különböző prímosztókhoz tartozó Sylow-részcsoportjainak direkt szorzata. Természetesen a részcsoportok is öröklik a feltételt, így elég p-csoportokra belátni, hogy ciklikusak, mert akkor G relatív prím rendű ciklikus csoportok direkt szorzata, tehát maga is ciklikus lesz.

Legyen P p-csoport a megadott feltétellel, és $|P| = p^n$. P-nek van p^{n-1}-edrendű részcsoportja (van valódi normálosztója, mert $Z(P) \ne 1$, és a faktorcsoport p indexű részcsoportjának ősképe p indexű P-ben). Mivel ezen a részcsoporton kívül más elem nem elégíti ki az $x^{p^n} = 1$ egyenletet, tetszőleges külső elem p^n rendű, így generálja P-t.

5. *Határozzuk meg a következő csoportok automorfizmuscsoportját!*

a) D_4 *b)* Q *kvaterniócsoport* *c)* S_4

Megoldás: a) Legyen $G = \langle f, t \rangle \cong D_4$, ahol f a $90°$-os forgatás, és t valamelyik tükrözés. Ekkor minden $f \mapsto f' = f^{\pm 1}$, $t \mapsto t' = tf^k$ $(k = 0, 1, 2, 3)$ automorfizmust ad, mert ugyanazt a szemidirekt szorzatot generálják: f képe 4-edrendű, t képe másodrendű, és $t'f't' = (f')^{-1}$. Így $|\operatorname{Aut} D_4| = 8$. Ez a csoport nem Abel, mert pl. a $\sigma : f \mapsto f^{-1}$, $t \mapsto t$ és $\tau : f \mapsto f$, $t \mapsto tf$ automorfizmusok nem felcserélhetők ($\sigma\tau : t \mapsto tf$, míg $\tau\sigma : t \mapsto tf^{-1}$), és nem lehet a quaterniócsoport, mert $\operatorname{Inn} D_4 \cong D_4/Z(D_4) \cong C_2 \times C_2$ részcsoportja az automorfizmuscsoportnak, viszont Q-nak csak egy másodrendű eleme van. Tehát $\operatorname{Aut} D_4 \cong D_4$.

b) Q automorfizmusait meghatározza az i és a j képe, mivel ezek generálják Q-t, és i képe $\pm i, \pm j, \pm k$ közül akármelyik lehet, j képe pedig bármelyik negyedrendű, amely nincs benne i képének generátumában (könnyen ellenőrizhető, hogy $i\varphi$, $j\varphi$ és $k\varphi = (i\varphi) \cdot (j\varphi)$ ezek után kielégítik ugyanazokat a szorzási szabályokat, mint i, j, k. Tehát $|\operatorname{Aut} Q| = 24$. Most belátjuk, hogy ez a csoport izomorf S_4-gyel. Ehhez elég megadni egy szürjektív homomorfizmust az S_4-be, ami az elemszámok egyenlősége miatt izomorfizmus is lesz. A Q csoport automorfizmusai permutálják az $A_1 = \{\{i, j, k\}, \{-i, -j, -k\}\}$, $A_2 = \{\{i, j, -k\}, \{-i, -j, k\}\}$, $A_3 = \{\{i, -j, k\}, \{-i, j, -k\}\}$, $A_4 = \{\{-i, j, k\}, \{i, -j, -k\}\}$ halmazokat. Ezeken a $\sigma : i \mapsto j$, $j \mapsto -i$, $k \mapsto j(-i) = k$ automorfizmus az (A_1, A_4, A_2, A_3) 4-ciklussal hat, a $\tau : i \mapsto -i$, $j \mapsto k$, $k \mapsto (-i)k = j$ automorfizmus pedig az (A_1, A_4) transzpozícióval. Mivel ezek ketten kigenerálják az egész szimmetrikus csoportot, a kapott $\operatorname{Aut} Q \to S_{\{A_1, A_2, A_3, A_4\}} \cong S_4$ homomorfizmus szürjektív.

c) $\operatorname{Aut} S_4 \ge \operatorname{Inn} S_4 \cong S_4/Z(S_4) = S_4/1 \cong S_4$. Másrészt $\operatorname{Aut} S_4$-nek nem lehet 24-nél több eleme, ugyanis a négyelemű $V = \langle (..)(..) \rangle \operatorname{char} S_4$ csoportot minden automorfizmus helyben hagyja, és $\operatorname{Aut} V \cong \operatorname{Aut}(C_2 \times C_2) \cong S_3$, és V minden másodrendű eleméhez pontosan két olyan negyedrendű elem van S_4-ben, amelynek négyzete az adott elem. Tehát a V egy tetszőleges automorfizmusához, legföljebb $2 \cdot 2 = 4$-féle képe lehet az $a = (1234)$ és $b = (1324)$ elemeknek. Ez összesen maximum 24 lehetőség, s mivel V ezzel a két negyedrendű elemmel együtt kigenerálja S_4-et (az V és a kigenerál egy D_4-gyel izomorf 2-Sylowot, s mivel ebben csak két negyedrendű elem van,

b ezen kívül van, így $\langle V, a, b\rangle$ csak az egész S_4 lehet), S_4-nek összesen legföljebb 24 automorfizmusa van. Így $\operatorname{Aut} S_4 = \operatorname{Inn} S_4 \cong S_4$.

6. *Legyen $H < G$, $\Omega = \{ Hx \mid x \in G\}$, és $\varphi : G \to S_\Omega$ a G elemeivel való jobbszorzás mint Ω-n vett csoporthatás. Bizonyítsuk be, hogy φ magja G-nek H-ban levő legnagyobb normálosztója!*

Megoldás: $Hxg = Hx \Leftrightarrow Hxgx^{-1} = H \Leftrightarrow xgx^{-1} \in H \Leftrightarrow g \in H^x$, tehát $\operatorname{Ker}\varphi = \bigcap_{x\in G} H^x$. Ez nyilván benne van H-ban (az $x = 1$-gyel vett konjugáltjában), normálosztó, mert homomorfizmus magja, és ha $N \lhd G$-re $N \le H$, akkor $N = N^x \le H^x$ minden $x \in G$-re, így $N \le \operatorname{Ker}\varphi$, tehát $\operatorname{Ker}\varphi$ a G legnagyobb H-ban levő normálosztója.

7. *Bizonyítsuk be, hogy nincs 120 elemű egyszerű csoport!*

Megoldás: Tegyük fel, hogy van: G egyszerű, és $|G| = 120$. Ekkor $|Syl_5(G)| \mid 24$, és $|Syl_5(G)| \equiv 1 \pmod 5$, így $|Syl_5(G)| = 1$ vagy 6. De 1 nem lehet, mert G egyszerű, így 6 darab 5-Sylow van. Legyen H egy 5-Sylow normalizátora. Ekkor $|G : H| = 6$, és a H mellékosztályain reprezentálva kapunk egy $\varphi : G \to S_6$ homomorfizmust. Ennek a magja H-ban van, és normálosztó, így G egyszerűsége miatt csak 1 lehet, vagyis $G \cong \operatorname{Im}\varphi \le S_6$. Feltehetjük, hogy maga G részcsoportja S_6-nak. $G \cap A_6 \lhd G$, így G egyszerűsége miatt vagy $G \le A_6$, de akkor $|A_6 : G| = 3$, és A_6-nak nincs 6-nál kisebb indexű valódi részcsoportja, vagy $G \cap A_6 = 1$, de akkor $|S_6| \ge |G| \cdot |A_6| = 120 \cdot |A_6|$ ismét ellentmondás. Tehát nem létezik ilyen G csoport.

8. *Bizonyítsuk be, hogy $Z(S_n) = 1$, ha $n \ge 3$.*

Megoldás: Legyen $1 \ne g \in S_n$. Ekkor van olyan $\alpha \ne \beta$, hogy $\alpha g = \beta$. Mivel $n \ge 3$, van még az alaphalmaznak egy α-tól és β-tól különböző γ eleme. Legyen $h = (\beta\gamma)$. Ha ezzel megkonjugáljuk g-t, a kapott g^h elem αh-t βh-ba viszi, azaz $g^h : \alpha \mapsto \gamma$, így $g^h \ne g$, és ezért $g \notin Z(S_n)$.

9. *Mutassuk meg, hogy minden tranzitív kommutatív permutációcsoport reguláris, azaz az egységelemtől különböző elemei fixpontmentesek.*

Megoldás: Legyen $1 \ne g$, és tegyük fel, hogy g-nek van fixpontja: $Fix(g) \ne \emptyset$. Ekkor tetszőleges h elemre és $\alpha \in Fix(g)$-re $gh = hg$ miatt $(\alpha h)g = \alpha hg = \alpha gh = \alpha h$, tehát $Fix(g)h \subseteq Fix(g)$. De akkor $Fix(g)$ nem triviális orbit lenne, ellentmondva a csoport tranzitivitásának.

10. *Hányféleképpen lehet kiszínezni egy szabályos nyolcszög csúcsait pirossal és kékkel, ha pontosan három csúcsnak lehet piros a színe, és*

a) a forgatással egymásba vihető színezéseket azonosnak tekintjük, illetve

b) a forgatással vagy tükrözéssel egymásba vihető színezéseket azonosnak tekintjük.

Megoldás: Mindkét esetben elegendő megszámolni az összes ($\binom{8}{3}$ darab) színezésen a megengedett szimmetriák orbitjait, tehát a színezések olyan osztályait, amelyeket azonosnak tekintünk. Ehhez a fixpontok átlagát kell kiszámítani az a) kérdésnél az $\langle f\rangle \cong C_8$ permutációcsoportra, a b) kérdésnél pedig az $\langle f, t\rangle \cong D_8$ csoportra.

a) Az identikustól különböző forgatások nem vihetik önmagába semelyik színezést, mert ahhoz a piros csúcsokból páros soknak kellene lennie. Így az orbitok száma $(1 \cdot \binom{8}{3} + 7 \cdot 0)/8 = 7$.

b) Az átlóra való tükrözéseknek $2 \cdot 3 = 6$ fixpontjuk van (egy piros csúcsnak a tengelyre kell kerülnie, a másik kettőnek a három merőleges átló egyikének két végpontjára), az oldalközéppontokat összekötő tengelyekre való tükrözéseknek 0. Így az orbitok száma $(1 \cdot 56 + 7 \cdot 0 + 4 \cdot 6 + 4 \cdot 0)/16 = 5$.