1. *Legyenek A és B a G csoport részcsoportjai. Lássuk be, hogy az $AB = \{\, ab \mid a \in A,\ b \in B \,\}$ komplexusszorzat akkor és csak akkor részcsoport, ha $AB = BA$.*

Megoldás: A részcsoport definíciójából következik, hogy egy nem üres $H \subseteq G$ részhalmaz akkor és csak akkor részcsoport, ha $HH \subseteq H$ és $H^{-1} \subseteq H$, vagy ekvivalens módon: ha $HH = H$ és $H^{-1} = H$ (az elsőben $h = 1h$ mutatja a másik irányú tartalmazást, a másodikban pedig a $H^{-1} \subseteq H$ tartalmazásból az elemek invertálásával következik, hogy $H \subseteq H^{-1}$ is igaz). A bizonyításban felhasználjuk azt is, hogy tetszőleges $A, B \subseteq G$ részhalmazra $(AB)^{-1} = \{(ab)^{-1} \mid a \in A,\ b \in B\} = \{\, b^{-1}a^{-1} \mid a \in A,\ b \in B \,\} = B^{-1}A^{-1}$.
Tegyük fel, hogy $A, B, AB \leq G$. Ekkor $AB = (AB)^{-1} = B^{-1}A^{-1} = BA$.
Most tegyük fel, hogy az A, B részcsoportokra $AB = BA$. Ekkor $ABAB = AABB = AB$, és $(AB)^{-1} = B^{-1}A^{-1} = BA = AB$. Tehát $AB \leq G$.

2. *Legyen A és B a G véges csoport két részcsoportja. Bizonyítsuk be, hogy $|AB| = \dfrac{|A| \cdot |B|}{|A \cap B|}$.*

Megoldás: Az $\{(a, b) \mid a \in A,\ b \in B\}$ Descartes-szorzatnak $|A| \cdot |B|$ eleme van. Ha aszerint osztályozzuk a Descartes-szorzat elemeit, hogy az ab szorzat mivel egyenlő, akkor (a, b) és (a', b') pontosan akkor vannak egy osztályban, ha $ab = a'b'$, azaz $(a')^{-1}a = b'b^{-1}$. Mivel ez utóbbi elem A-ban és B-ben is benne van, ha ezt az elemet x-nek hívjuk, akkor $x \in A \cap B$, és $a' = ax^{-1}$, míg $b' = xb$, vagyis $(a', b') = (ax^{-1}, xb)$. Tehát pontosan annyi elem van egy osztályban, mint ahány eleme van $A \cap B$-nek. Az ab szorzat pedig $|AB|$-féle értéket vehet föl, így $|A| \cdot |B| = |A \cap B| \cdot |AB|$, amiből következik a feladat állítása.

3. *Legyen $a, b \in G$, és $o(a), o(b) < \infty$. Bizonyítsuk be, hogy ha $ab = ba$, akkor*
a) $o(ab) \mid [o(a), o(b)]$,
b) és ha emellett $\langle a \rangle \cap \langle b \rangle = 1$ (pl. mert $(o(a), o(b)) = 1$), akkor $o(ab) = [o(a), o(b)]$.
Lássuk be, hogy ha $ab \neq ba$, akkor még az a) állítás sem feltétlenül igaz.

Megoldás: Legyen $o(a) = m$ és $o(b) = n$
a) Mivel $ab = ba$, $(ab)^{[m,n]} = a^{[m,n]}b^{[m,n]}$, és az utóbbi $1 \cdot 1 = 1$, ugyanis $m \mid [m, n]$ és $n \mid [m, n]$. Ebből következik, hogy $o(ab) \mid [m, n]$.
b) Legyen $o(ab) = k$. Az a) részben láttuk, hogy $k \mid [m, n]$. Fordítva, ha $\langle a \rangle \cap \langle b \rangle = 1$, akkor $1 = (ab)^k = a^k b^k \Rightarrow a^k = b^{-k} \in \langle a \rangle \cap \langle b \rangle = 1 \Rightarrow a^k = b^k = 1 \Rightarrow m, n \mid k \Rightarrow [m, n] \mid k$. Tehát $o(ab) = k = [m, n]$.
Viszont ha D_4-ben f a 90°-os forgatás, t pedig az egyik tükrözés, akkor tf is tükrözés (a 45°-kal elforgatott tengelyre), tehát másodrendű, viszont $t(tf) = t^2 f = f$ negyedrendű. Tehát $o(t(tf)) = 4$ nem osztója $[o(t), o(tf)] = [2, 2] = 2$-nek.

4. *Bizonyítsuk be, hogy ciklikus csoport minden részcsoportja ciklikus, és Z_n-ben minden $d \mid n$-hez egyetlen d-elemű részcsoport van.*

Megoldás: Legyen $G = \langle a \rangle$ ciklikus csoport, és $1 \neq H \leq G$. Legyen k a legkisebb pozitív egész, amelyre $a^k \in H$ (ilyen van, mert $H \neq 1$, és H zárt az inverzre). Belátjuk, hogy ez az elem generálja H-t.
Vegyük a H egy tetszőleges a^m elemét, és osszuk el m-et maradékosan k-val: $m = kq + r$, ahol $0 \leq r < k$. Ekkor $a^m = (a^k)^q \cdot a^r$, és itt a^m és $(a^k)^q$ is H-beli, így $a^r = a^m(a^k)^{-q} \in H$, ami ellentmond k minimalitásának, kivéve, ha $r = 0$. Tehát $a^m = (a^k)^q \in \langle a^k \rangle$ a H minden a^m elemére, vagyis $H = \langle a^k \rangle$.

Ha most $G \cong Z_n$, akkor azt tudjuk az 1/9-es feladatból, hogy minden $d \mid n$-re van d-edrendű részcsoport, $H := \langle a^{n/d} \rangle$. Bármely d-edrendű részcsoport Z_d-vel izomorf, mert az előzőek szerint ciklikus, tehát tudjuk róla, hogy minden elemének a d-edik hatványa 1. Viszont az $x^d = 1$ egyenletnek G-ben csak d megoldása van: $0 \le k < n$-re $(a^k)^d = 1 \Leftrightarrow n \mid kd \Leftrightarrow \frac{n}{d} \mid k \Leftrightarrow k = 0, \frac{n}{d}, \frac{2n}{d}, \ldots, \frac{(d-1)n}{d}$, ezért csak egyetlen d-edrendű részcsoport van Z_n-ben.

5. *Határozzuk meg a következő csoportok összes részcsoportját!*

$$D_8 \text{ (a négyzet szimmetriacsoportja)}, \qquad Z_{16}, \qquad Z_{12}$$

Megoldás: Z_{16}-ban és Z_{12}-ben az előző feladat szerint a csoport rendjének minden osztójához egyetlen olyan rendű részcsoport van, tehát Z_{16}-ban egy-egy 1, 2, 4, 8 és 16 rendű ciklikus részcsoport (és ezek a tartalmazásra nézve láncot alkotnak, mert a részcsoportokra is igaz, hogy van bennük osztó elemszámú részcsoport), Z_{12}-ben pedig $1, 2, 3, 4, 6, 12$ rendűből van egy-egy.
D_8-ban legyen a 90°-os forgatás f, és az egyik tükrözés t. Ekkor

$$D_8 = \{\, 1, f, f^2, f^3, t, tf, tf^2, tf^3 \,\}.$$

(Irányításváltó és irányítástartó egybevágóság szorzata irányításváltó, tehát ha t-vel megszorozzuk a forgatásokat, négy különböző tükrözést, tehát az összes tükrözést megkapjuk.)
Legyen $H \le D_8$. Ha $f \in H$, akkor bármelyik tükrözést hozzárakva, ezek kigenerálják az összes elemet, így ilyen részcsoportból csak D_8 és $\langle f \rangle \cong Z_4$ van. Most tegyük fel, hogy $f \notin H$ (és akkor persze $f^{-1} \notin H$). Ekkor a négy tükrözésből nem tartalmazhat két szomszédost, mert azok kigenerálják f-et: $(tf^k)^{-1} tf^{k+1} = f^{-k} t t f^{k+1} = f^{-k} f^{k+1} = f$, így H legföljebb két tükrözést tartalmazhat, és azok sem szomszédosak (és együtt kigenerálják az f^2-et): $\{\, 1, t, tf^2, f^2 \,\}$ és $\{\, 1, tf, tf^3, f^2 \,\}$ valóban részcsoportok (az ellenőrzéshez használjuk, hogy $tft = f^{-1}$), és minden $\neq 1$ elemük másodrendű, tehát $\mathbb{F}_2^2$-vel izomorfak. Ha egyetlen tükrözést tartalmaz a H, és nincs benne f^2 sem (ui. azok ketten az előbbi két részcsoport egyikét generálnák), akkor az csak egy másodrendű ciklikus részcsoport lehet, amelyet egyetlen tükrözés alkot az egységelemmel együtt. Végül ha nincs benne sem tükrözés, sem f, akkor $H = \langle f^2 \rangle \cong Z_2$ vagy $H = 1$.
Tehát a következő részcsoportok vannak D_8-ban:

$$D_8,\ \langle f \rangle,\ \langle t, f^2 \rangle,\ \langle tf, f^2 \rangle,\ \langle t \rangle,\ \langle tf \rangle, \langle tf^2 \rangle, \langle tf^3 \rangle,\ \langle f^2 \rangle,\ 1,$$

és az izomorfiatípusuk rendre:

$$D_8,\ Z_4,\ \mathbb{F}_2^2,\ \mathbb{F}_2^2, Z_2, Z_2, Z_2, Z_2, Z_2, 1.$$

6. *Bizonyítsuk be, hogy bármely végtelen csoportnak végtelen sok részcsoportja van.*

Megoldás: Vegyük észre, hogy egy ciklikus csoportban csak véges sok olyan elem van, ami generálja a teljes csoportot. Véges csoportra ez nyilvánvaló, ha pedig $o(a) = \infty$, akkor $a \in \langle a^k \rangle$ esetén $\exists m \in \mathbb{Z}$: $a^{km-1} = 1$, azaz $km = 1$, és így $k = \pm 1$. Tehát ha az elemeket osztályozzuk aszerint, hogy melyek generálják ugyanazt a részcsoportot, akkor a végtelen sok elem végtelen sok különböző osztályba kerül, vagyis már ciklikus részcsoportból is végtelen sok van.

7. *a) Lássuk be, hogy $(\mathbb{Q},+)$ minden végesen generált részcsoportja ciklikus (elég megmutatni, hogy tetszőleges, két elemmmel generált részcsoportja egy elemmel is generálható).*

b) Bizonyítsuk be, hogy $(\mathbb{Q},+)$-nak nincs minimális generátorrendszere, sőt, minden generátorrendszerből tetszőleges elem elhagyható.*

Megoldás: a) Vegyünk két elemet $(\mathbb{Q},+)$-ban: $\frac{a}{b}$, $\frac{c}{d}$ $(a,b,c,d\in\mathbb{Z}, b,d\neq 0)$. Ekkor $\frac{a}{b}=\frac{ad}{bd}$ és $\frac{c}{d}=\frac{cb}{bd}$. Tudjuk, hogy $(\mathbb{Z},+)$ minden részcsoportja ciklikus, így van olyan $m\in\mathbb{Z}$, hogy $\langle ad,cb\rangle=\langle m\rangle$ a $\mathbb{Z}$-ben, amiből következik, hogy $\langle\frac{ad}{bd},\ \frac{cb}{bd}\rangle=\langle\frac{m}{bd}\rangle$.
Így teljes indukcióval bizonyíthatjuk, hogy minden n elemmel generált részcsoport is ciklikus: $n=1,2$-re láttuk, és ha $\langle r_1,\dots,r_n\rangle=\langle s\rangle$, akkor $\langle r_1,\dots,r_n,r_{n+1}\rangle=\langle s,r_{n+1}\rangle$ szintén ciklikus.

b) $(\mathbb{Q},+)$ nyilván nem ciklikus, mert egy tört egész számszorosai (egyszerűsített alakban) legföljebb akkora nevezőjűek, mint ő maga.
Legyen a egy generátorrendszer eleme, és H a többi elem generátuma. A H tetszőleges nemnulla elemét és a-t is fel lehet szorozni nem nulla egész számmá, és így ugyanazzá az egésszé is (pl. a két egész szorzatává), így $\exists m\in\mathbb{Z}$, hogy $ma\in H$.
Most tetszőleges $r\in\mathbb{Q}$-ra $\frac{r}{m}$ felírható $\frac{r}{m}=ka+h$ alakban, ahol $k\in\mathbb{Z}$ és $h\in H$, mert H az a-val együtt már generálja az egész $\mathbb{Q}$-t. De akkor $r=kma+mh\in H+H=H$, vagyis minden $r\in\mathbb{Q}$ benne van H-ban, azaz $H=\mathbb{Q}$.

8. *Bizonyítsuk be, hogy ha n-nek pontosan k különböző prímosztója van, akkor Z_n minden minimális (azaz fölösleges elemet nem tartalmazó) generátorrendszere k-elemű.*

Megoldás: Vegyünk egy generátorrendszert, és írjuk fel a generátorelemek rendjeit. Ha $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ az n kanonikus alakja, akkor a rendek között kell lennie $p_i^{\alpha_i}$-vel oszthatónak minden i-re, mert különben a 3.a) feladat szerint nem tudnánk belőlük előállítani a csoport n-edrendű generátorelemét. Legyen g_i a generátorrendszer olyan eleme, amelynek a rendje osztható $p_i^{\alpha_i}$-vel. A g_i-nek van olyan hatványa, amelynek a rendje pontosan $p_i^{\alpha_i}$, legyen ez h_i. A 3.b) feladat alapján i-re vonatkozó teljes indukcióval bizonyíthatjuk, hogy $o(h_1\cdots h_i)=p_1^{\alpha_1}\cdots p_i^{\alpha_i}$. $i=1$-re nyilván igaz, és ha valamely i-re igaz, akkor $\langle h_1\cdots h_i\rangle\cap\langle h_{i+1}\rangle=1$ a rendek relatív prímsége miatt, tehát $o(h_1\cdots h_{i+1})=o(h_1\cdots h_i)o(h_{i+1})=p_1^{\alpha_1}\cdots p_{i+1}^{\alpha_{i+1}}$. Ezek szerint $o(h_1\cdots h_k)=n$, vagyis $h_1\cdots h_k$ generálja az egész csoportot, így $\{h_1,\dots,h_k\}$, és ebből következően $\{g_1,\dots,g_k\}$ is generátorrendszer. Ha a generátorrendszer minimális volt, akkor nem lehetett benne több elem, így nincs k-nál nagyobb elemszámú minimális generátorrendszer.
k-elemű minimális generátorrendszer viszont létezik: Z_n-ben minden i-re van $p_i^{\alpha_i}$ rendű elem, legyen ez g_i. Az előbbiek alapján $\langle g_1,\dots,g_k\rangle=Z_n$. Ha a g_i-t elhagynánk, akkor a kigenerálható elemek rendje legföljebb $\frac{n}{p_i^{\alpha_i}}$ lenne, tehát a többi elem nem generálja ki a Z_n n-edrendű generátorelemét. Így ez a részhalmaz minimális generátorrendszer Z_n-ben.

9. *Legyen p prím, és Z_{p^∞} a komplex p-hatványadik egységgyökök multiplikatív csoportja (kváziciklikus csoport). Lássuk be, hogy Z_{p^∞} minden valódi részcsoportja véges ciklikus csoport, és hogy a részcsoportok a tartalmazásra nézve láncot alkotnak.*

Megoldás: Először ellenőrizzük, hogy a p-hatványadik egységgyökök valóban részcsoportot alkotnak $\mathbb{C}^\times$-ben! Benne van az 1, zárt az inverzre, mert ha $\varepsilon^{p^k}=1$, akkor $(\varepsilon^{-1})^{p^k}=$

$(\varepsilon^{p^k})^{-1} = 1$, és ha ε p^k-adik, η p^n-edik egységgyök, ahol, mondjuk, $k \leq n$, akkor $\varepsilon\eta$ is p^n-edik egységgyök: $(\varepsilon\eta)^{p^n} = \varepsilon^{p^n}\eta^{p^n} = 1 \cdot 1 = 1$, mivel $p^k \mid p^n$.
Tudjuk, hogy egy primitív p^n-edik egységgyök kigenerál minden p^n-edik egységgyököt, és így minden p^k rendű elemet is Z_{p^∞}-ben, ahol $k \leq n$. Így ha egy részcsoportban tetszőlegesen nagy k-ra van p^k rendű elem, akkor abban az összes p-hatványadik egységgyök benne van, azaz csak a teljes csoport lehet.
Legyen $H < Z_{p^\infty}$, és ebben a legnagyobb elemrend p^n: legyen $o(h) = p^n$. Mivel ez a primitív p^n-edik egységgyök minden p^k-adik egységgyököt kigenerál, azaz a kváziciklikus csoport minden $\leq p^n$ rendű elemét, $H = \langle h \rangle \cong Z_{p^n}$. Ebből következik az is, hogy minden n-re egyetlen p^n rendű részcsoport van (a p^n-edik egységgyökök ciklikus csoportja), és a kisebb rendű benne van a nagyobb rendűben, így valóban láncot alkotnak ezek a részcsoportok.

Hf1. *Bizonyítsuk be, hogy az $\mathbb{F}_2$ fölötti invertálható 3×3-as felső háromszögmátrixok csoportja nem ciklikus.*

Hf2. *Határozzuk meg a $G = (\mathbb{Z}_{16}^*, \cdot)$ csoportra a generátorrendszerek minimális elemszámát, $d(G)$-t. Adjunk meg olyan $d(G)$ elemű generátorrendszert, amelynek elemei diszjunkt (azaz csak $\{1\}$-ben metsző) részcsoportokat generálnak, és olyat is, amelyre ez nem igaz! (A generálás bizonyításához használhatjuk a 2. feladatot.)*