1. *Legyen g egy csoportelem, g rendje $o(g) = n$, és $k, m \in \mathbb{Z}$. Lássuk be, hogy*
a) $g^m = 1 \Leftrightarrow n \mid m$;
b) $o(g^k) = \dfrac{n}{(n,k)}$.
Fogalmazzuk meg és bizonyítsuk be a megfelelő állításokat végtelen rendre!

Megoldás: a) $\Rightarrow$: Osszuk el az m-et maradékosan n-nel: $m = nq + r$. Ekkor $1 = g^m = (g^n)^q g^r = 1^q g^r = g^r$, de $r < n$, tehát $r = 0$, így $n \mid m$.
$\Leftarrow$: $m = qn \Rightarrow g^m = (g^n)^q = 1^q = 1$.
b) Az a) rész miatt $(g^k)^m = g^{km} = 1 \Leftrightarrow n \mid km \Leftrightarrow \frac{n}{(n,k)} \mid \frac{k}{(n,k)} m \Leftrightarrow \frac{n}{(n,k)} \mid m$, mivel $\frac{n}{(n,k)}$ és $\frac{k}{(n,k)}$ relatív prímek. Így a g^k legkisebb 1 értékű pozitív hatványa az $\frac{n}{(n,k)}$-adik.
Végtelen rendre a megfelelő állítások: Ha $o(g) = \infty$, akkor
$g^m = 1 \Leftrightarrow m = 0$;
$o(g^k) = \infty$, ha $k \neq 0$, és 1, ha $k = 0$.
Az első nyilvánvaló a végtelen rend definíciójából, a második pedig az elsőből következik: ha $(g^k)^m = g^{km} = 1$, akkor $km = 0$, így $k \neq 0$ esetén m csak 0 lehet, tehát $o(g^k) = \infty$, míg $k = 0$ esetén $g^k = g^0 = 1$ rendje 1.

Definiáljuk az $AB = \{ ab \mid a \in A,\ b \in B \}$ és $A^{-1} = \{ a^{-1} \mid a \in A \}$ komplexusműveleteket egy G csoport részhalmazain.

2. *Bizonyítsuk be, hogy $\mathcal{P}(G)$ egységelemes félcsoport, de A^{-1} általában nem az A inverze a komplexusszorzásra nézve.*

Megoldás: $A, B, C \subseteq G$-re $(AB)C = \{ ab \mid a \in A,\ b \in B \}C = \{(ab)c \mid a \in A,\ b \in B,\ c \in C \} = \{ a(bc) \mid a \in A,\ b \in B,\ c \in C \} = A(BC)$, tehát $\mathcal{P}(G)$ félcsoport. Az $\{ 1 \}$ halmaz egységelemként hat: $\{ 1 \} A = \{ 1a \mid a \in A \} = \{ a \mid a \in A \} = A$, és ugyanígy a másik sorrendben. Ebből következik, hogy más egységelem nem lehet a félcsoportban, és B akkor inverze A-nak, ha $AB = BA = \{ 1 \}$. Az üreshalmaznak nyilván nincs inverze, mert az mindent az üreshalmazba szoroz, de még ha azt ki is hagynánk ($\mathcal{P}(G) \setminus \{ \emptyset \}$ is zárt a szorzásra), az 1-nél több elemű halmazoknak nyilván nincs inverze: ha $g, h \in A$ különböző elemek, és $AB = \{ 1 \}$, akkor $B \neq \emptyset$, és B minden eleme g-nek és h-nak is inverze, ami nem lehet.

3. *Lássuk be, hogy egy $\emptyset \neq H \subseteq G$ részhalmazra*
$H \leq G \Leftrightarrow (HH = H$ és $H^{-1} = H) \Leftrightarrow (HH \subseteq H$ és $H^{-1} \subseteq H)$.

Megoldás: A harmadik feltétel a részcsoport definíciójából közvetlenül adódóan ekvivalens az elsővel, továbbá a másodikból nyilván következik a harmadik. Azt kell még belátnunk, hogy az elsőből következik a második. Az egyik irányú tartalmazások már megvannak. Másrészt, ha $H \leq G$, akkor $1 \in H$, ezért minden $h \in H$-ra $h = 1 \cdot h \in HH$, vagyis $H \subseteq HH$. Továbbá nemcsak $H^{-1} \subseteq H$, hanem mivel H zárt az inverzre, minden $h \in H$-ra $h = (h^{-1})^{-1} \in H^{-1}$, vagyis $H \subseteq H^{-1}$ is igaz.

4. *Mutassuk meg, hogy $A, B \leq G$-re AB akkor és csak akkor részcsoport G-ben, ha $AB = BA$.*

Megoldás: Felhasználhatjuk a 3. feladat összefüggéseit. Ha A, B, AB mindegyike részcsoport, akkor $AB = (AB)^{-1} = \{(ab)^{-1} \mid a \in A,\ b \in B \} = \{ b^{-1}a^{-1} \mid a \in A,\ b \in B \} = B^{-1}A^{-1} = BA$.

Fordítva, ha $AB = BA$, akkor $(AB)(AB) = A(BA)B = A(AB)B = (AA)(BB) = AB$, és $(AB)^{-1} = B^{-1}A^{-1} = BA$ ugyanúgy, mint az előbb (ebben csak a komplexusműveletek definícióját és az A, B részcsoportságát használtuk), és a feltevés miatt $BA = AB$, tehát $(AB)^{-1} = AB$. Így a 3. feladat szerint $AB \leq G$.

5. *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 $(a', b') = (ax^{-1}, xb)$. Fordítva, minden $x \in A \cap B$-re (ax^{-1}, xb) benne van a Descartes-szorzatban. 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.

6. *Bizonyítsuk be, hogy egy részcsoportnak ugyanannyi jobb oldali mellékosztálya van, mint bal oldali mellékosztálya. Adjunk meg köztük egy természetes bijekciót!*

Megoldás: Tetszőleges Hg jobb mellékosztályra $(Hg)^{-1} = g^{-1}H^{-1} = g^{-1}H$ az inverz elemhez tartozó bal mellékosztály. Mivel a komplexusokra igaz, hogy $(A^{-1})^{-1} = A$, ez bijekciót ad a jobb és bal mellékosztályok között.

7. *Milyen rendű elemek vannak a D_n diédercsoportban, és melyikből hány darab?*

Megoldás: Az n darab tükrözés mindegyike másodrendű, a forgatások pedig egy n-edrendű ciklikus csoportot alkotnak, tehát ezek között minden $d|n$ pozitív egészre pontosan $\varphi(d)$ darab d-edrendű van.

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

Megoldás: Tegyük fel, hogy a csoportnak van egy végtelen rendű g eleme. Ekkor $\langle g^k \rangle \neq \langle g^m \rangle$, amennyiben $k \neq m$ pozitív számok, mert különben $g^k \in \langle g^m \rangle$ miatt $g^k = g^{mx}$, azaz $g^{k-mx} = 1$ valamely $x \in \mathbb{Z}$-re, így $k - mx = 0$ lenne, azaz $m \mid k$, és ugyanígy $k \mid m$, tehát $k = m$ lenne. Tehát ilyenkor már $\langle g \rangle$-nek is van végtelen sok részcsoportja.
Ha csak véges rendű elemek vannak, akkor tudjuk, hogy csak véges sokan generálhatják ugyanazt a (ciklikus) részcsoportot, tehát végtelen sok ciklikus részcsoportnak kell lennie.

9. *Bizonyítsuk be, hogy C_∞ minden nem triviális részcsoportja véges indexű, azaz véges sok mellékosztálya van.*

Megoldás: Tudjuk, hogy C_∞-nek minden részcsoportja ciklikus, tehát ha a nagy csoportnak generátoreleme a, akkor a részcsoporté a^n valamely $n > 0$-ra ($\langle a^0 \rangle = 1$ a triviális részcsoport, és $\langle a^{-n} \rangle = \langle a^n \rangle$). Ekkor $H = \langle a^n \rangle$ minden mellékosztályának van a^r alakú reprezentánseleme, ahol $0 \leq r < n$, ugyanis tetszőleges egész m-re az n-nel való $m = nq + r$ maradékos osztásból $a^m = (a^n)^q a^r \in Ha^r$, tehát a^m mellékosztályában a^r is benne van. Tehát a mellékosztályok száma legföljebb n. Az is igaz, hogy a mellékosztályok száma pontosan n, mert $0 \leq i, j < n$, $i \neq j$ esetén $a^{i-j} \notin \langle a^n \rangle$, vagyis $1, a, \ldots, a^{n-1}$ nem lehetnek egy mellékosztályban.

10. *Hány különböző homomorfizmus adható meg az alábbi csoportok között?*
a) $C_{10} \to C_{33}$ *b)* $C_n \to C_n$ *c)* $C_n \to C_m$ *d)* $C_\infty \to C_n$ *e)* $C_n \to C_\infty$

Megoldás: a) Legyen $C_{10} = \langle a \rangle$ és $C_{33} = \langle b \rangle$. Ha $\varphi : \langle a \rangle \to \langle b \rangle$ homomorfizmus, akkor $o(\varphi(a)) \mid o(a) = 10$, és $o(\varphi(a)) \mid |\langle b \rangle| = 33$, ezért $o(\varphi(a)) \mid (10, 33) = 1$. Tehát $\varphi(a) = 1 \Rightarrow \varphi(a^k) = 1^k = 1$ minden k-ra, vagyis csak a triviális $\equiv 1$ homomorfizmus létezik.

b) Ez a c) kérdés speciális esete: n különböző homomorfizmus van C_n-ből C_n-be, a generátorelemet C_n bármely elemébe lehet képezni.

c) Legyen $C_n = \langle a \rangle$ és $C_m = \langle b \rangle$. Az a generátorelem képe csak olyan $c \in \langle b \rangle$ lehet, amelynek a rendje osztja a rendjét. Ha viszont teljesül ez a feltétel, akkor a $\varphi : a^k \mapsto c^k$ $(k \in \mathbb{Z})$ leképezés jól definiált: $a^k = a^\ell \Rightarrow a^{k-\ell} = 1 \Rightarrow o(c) \mid n \mid k - \ell \Rightarrow c^{k-\ell} = 1 \Rightarrow c^k = c^\ell$, és művelettartó is: $\varphi(a^k a^\ell) = \varphi(a^{k+\ell}) = c^{k+\ell} = c^k c^\ell = \varphi(a^k)\varphi(a^\ell)$. Mivel C_m minden elemének a rendje osztója m-nek, csak azok jönnek szóba, amelyeknek a rendje (m, n)-nek osztója, ilyenből pedig C_m-ben pontosan (m, n) darab van, a C_m egyetlen (m, n) elemű részcsoportjában. Tehát a $C_n \to C_m$ homomorfizmusok száma (m, n).

d) Ha $C_\infty = \langle a \rangle$ és $C_n = \langle b \rangle$, akkor az a elemet C_n tetszőleges c elemébe képezhetjük az $a^k \mapsto c^k$ $(k \in \mathbb{Z})$ leképezéssel. Ez C_∞-n jól definiált, és nyilván művelettartó is. Tehát n különböző homomorfizmus van C_∞-ből C_n-be.

e) Mivel véges rendű elem csak véges rendűbe mehet, C_∞-ben pedig csak az 1 véges rendű, C_n-ből C_∞-be csak a triviális $\equiv 1$ homomorfizmus létezik.

Hf1. *Bizonyítsuk be, hogy $o(ab) = o(ba)$ egy G csoport tetszőleges a, b elemeire.* *(2 pont)*

Hf2. *Bizonyítsuk be, hogy a $\mathbb{Z}_2$ fölötti invertálható 3×3-as felső háromszögmátrixok csoportja nem ciklikus.* *(2 pont)*