14. FÉLCSOPORTOK ÉS CSOPORTOK

Azt mondjuk, hogy $\circ$ egy **kétváltozós** (vagy binér) **művelet** a H halmazon ha a H-nak tetszőleges a és b elemeire értelmezve van egy a és b által egyértelműen meghatározott $a \circ b$-vel jelölt H-beli elem, amelyet legtöbbször az a és b szorzatának (ritkábban összegének, uniójának vagy metszetének) nevezünk. A H elemeinek és a $\circ$ műveleti jelnek a többszöri alkalmazásával, valamint zárójelek megfelelő beiktatásával különböző hosszúságú jelsorozatokat készíthetünk, amelyek között lesznek ún. szorzatok. Az $x, y, z \in H$ elemekkel

$$((x \circ y) \circ (y \circ z)) \circ y \text{ egy 5 hosszúságú szorzat,}$$

$$((z \circ x) \circ x) \circ (y \circ (x \circ z)) \text{ egy 6 hosszúságú szorzat, de}$$

$$z) \circ (x((\circ \circ xyx()))z \circ \text{ nem értelmezhető szorzatként.}$$

A szorzatokat az alábbiakban úgy fogjuk értelmezni, hogy azokban felismerhető legyen a $\circ$ műveletek H-beli elvégzésének egy olyan sorrendje, amely elvezet egy egyértelműen meghatározott végeredményhez. Egy adott szorzat esetében a műveletek elvégzésének a sorrendje persze nem lesz egyértelműen megmondható, pl. az $(x \circ y) \circ (z \circ x)$-ben háromszor szereplő $\circ$ műveletre vonatkozóan csak annyi kötöttségünk van, hogy a középső helyen állót kell utoljára elvégezni, az $x \circ y$ és $z \circ x$ elvégzésének a sorrendje lényegtelen a végeredményt illetően.

14.A.Definíció. A H halmazon értelmezett $\circ$ kétváltozós műveleti jelre nézve a **szorzatokat** az alábbi elemi lépések véges számú egymás utáni alkalmazásával kapjuk.
(i) a H halmaz elemeit egy hosszúságú és tetszőleges $x, y \in H$ elemekre $x \circ y$-t kettő hosszúságú szorzatnak tekintjük,
(ii) ha $x \in H$ és f egy $k \geq 2$ valamint g egy $l \geq 2$ hosszúságú szorzat, akkor $x \circ (f)$ és $(f) \circ x$ egy-egy $k+1$ hosszúságú szorzat, továbbá $(f) \circ (g)$ egy $k+l$ hosszúságú szorzat.
Két szorzat formálisan akkor egyenlő, ha a bennük szereplő jelek és H-beli elemek balról jobbra haladva rendre megegyeznek: tehát $x \circ (y \circ z)$ és $(x \circ y) \circ z$ formálisan különböznek. Bármely szorzatról egyértelműen megmondható, hogy annak felírásakor utolsóként a fenti (i) és (ii) lépések közül melyiket alkalmaztuk, sőt ebben az utolsó lépésben felhasznált rövidebb szorzatokra (x-re, y-ra, f-re és g-re) is egyértelműen visszakövetkeztethetünk. Az (i) és (ii) lépések természetes módon megadják a szorzat H-beli értékét is: pl. ha az f szorzat értéke $a \in H$ és a g szorzat értéke $b \in H$ volt, akkor $(f) \circ (g)$-nek az értéke $a \circ b \in H$. Egy szozat H-beli értékének a jelölésére maga a szorzat szolgál, pl. a $(3+2)+3$ szorzat (amit ebben az esetben összegnek illik nevezni) értéke a $\mathbb{Z}$-ben $(3+2)+3 = 8$. A különböző szorzatok közötti egyenlőségjel minden esetben a szorzatok H-beli értékeire vonatkozik majd nem pedig azok formális egyezőségére. Érdemes megjegyezni, hogy a $\circ$ műveleti jelet kétféleképpen is használtuk: egyrészt írásjelként a szorzatok elkészítéséhez, másrészt a H halmazon adott konkrét kétváltozós műveletként. A műveleti jelnek ez a kettős használata még akkor sem szokott félreértést okozni, hogy ha nem csak egy H halmazon, hanem esetleg más halmazokon is adva vannak konkrét kétváltozós műveletek és azokra is ugyanazt a jelet alkalmazzuk, pl. a számok és a mátrixok összeadására egyaránt a $+$-t használjuk.♡

A fenti definícióval kapcsolatban a következő fontos észrevételt tehetjük. Egy $n \geq 3$ hosszúságú h szorzatban a baloldali és a jobboldali zárójelek száma egyaránt $n-2$, továbbá a h-t bárhol kettévágva a vágástól balra eső részben a baloldali zárójelek száma nem kisebb mint az ugyanebben a részben lévő jobboldali zárójelek száma.

$$(((x \circ z) \circ z) \circ \overset{\text{vágás}}{\Big|} y) \circ ((x \circ y) \circ z)$$

Valóban, ha a fenti tulajdonság az f és g minden baloldali vágatára teljesül, akkor nagyon könnyen ellenőrízhető, hogy az $x \circ (f)$, $(f) \circ x$ és az $(f) \circ (g)$ szorzatok baloldali vágataira is érvényben marad, hogy bennük a baloldali zárójelek száma nem kisebb mint a jobboldaliaké.
Az $n \geq 1$ egészre jelölje T_n azon (n hosszúságú) szorzatok számát, amelyekben a H-beli $x_1, x_2, ..., x_n$ elemek mindegyike pontosan egyszer és pontosan ebben a sorrendben (balról jobbra) szerepel. A T_n-eket **Catalan-számoknak** nevezzük. Az $n = 4$ esetben felsoroljuk az összes ilyen szorzatot, azaz megadjuk az összes értelmes zárójelezését az $x_1 \circ x_2 \circ x_3 \circ x_4$ formális jelsorozatnak:

$$((x_1 \circ x_2) \circ x_3) \circ x_4,\ (x_1 \circ (x_2 \circ x_3)) \circ x_4,\ x_1 \circ ((x_2 \circ x_3) \circ x_4),$$

$$x_1 \circ (x_2 \circ (x_3 \circ x_4)),\ (x_1 \circ x_2) \circ (x_3 \circ x_4)\ .$$

14.1.Állítás. *$T_1 = T_2 = 1$ és az $n \geq 2$ egészre*

$$T_{n+1} = \sum_{k=1}^{n} T_k T_{(n+1)-k}\ .$$

Bizonyítás. Egy olyan h szorzat felírására, amelyben az $x_1, x_2, ..., x_n, x_{n+1} \in H$ elemek mindegyike pontosan egyszer és pontosan ebben a sorrendben szerepel a következő lehetőségeink vannak: $x_1 \circ (f)$, $(g) \circ x_{n+1}$ és $(u) \circ (v)$, ahol f és g hosszúsága $n \geq 2$, az u egy $k \geq 2$ hosszúságú és v egy $(n+1)-k \geq 2$ hosszúságú szorzat. Balról jobbra haladva az f-ben az $x_2, x_3, ..., x_n, x_{n+1}$, g-ben az $x_1, x_2, ..., x_n$, u-ban az $x_1, x_2, ..., x_k$ és v-ben az $x_{k+1}, x_{k+2}, ..., x_n, x_{n+1}$ elemeket kell, hogy találjuk. Nyilvánvaló, hogy a szóbajöhető f-ek és g-k száma egyaránt T_n, az u megválasztására T_k és a v megválasztására $T_{(n+1)-k}$ lehetőségünk van. Tehát adott $2 \leq k \leq n-1$ egészre $T_k T_{(n+1)-k}$ különböző olyan $(u) \circ (v)$ alakú $n+1$ hosszúságú h szorzat létezik, amelyben az u hosszúsága pontosan k. A fentiek alapján és $T_1 = 1$-re való tekintettel megkapjuk T_{n+1}-re a kívánt rekurzív összefüggést.

□□□

Megjegyzés. Igazolni lehet, hogy $T_{n+1} = \frac{1}{n+1}\binom{2n}{n}$.

14.B.Definíció. Az $x_1, x_2, ..., x_n \in H$ elemek balra normált szorzatán az alábbi H-beli elemet értjük: $[x_1] = x_1$, $[x_1, x_2] = x_1 \circ x_2$ és $n \geq 3$ esetén

$$[x_1, x_2, ..., x_n] = (...((x_1 \circ x_2) \circ x_3) \circ ... \circ x_{n-1}) \circ x_n\ .$$

Hasonlóan értelmezhető a jobbra normált szorzat. Azt mondjuk, hogy a H halmazon adott $\circ$ kétváltozós művelet **asszociatív**, ha $(x \circ y) \circ z = x \circ (y \circ z)$ teljesül tetszőleges $x, y, z \in H$ elemekre.♡

14.2.Állítás. *Legyen $h(x_1, x_2, ..., x_n)$ egy tetszőleges olyan szorzat a $\circ$ asszociatív művelettel, amelyben az $x_1, x_2, ..., x_n \in H$ elemek mindegyike pontosan egyszer és pontosan ebben a sorrendben szerepel. Ekkor $h(x_1, x_2, ..., x_n) = [x_1, x_2, ..., x_n]$ teljesül a H-ban.*

Bizonyítás. Az $n = 1$ esetben $h(x_1)$ csak x_1 és az $n = 2$ esetben $h(x_1, x_2)$ csak $x_1 \circ x_2$ lehet, tehát $h(x_1) = [x_1]$ és $h(x_1, x_2) = [x_1, x_2]$ nyilvánvalóan teljesül. Ha $n = 3$ akkor $h(x_1, x_2, x_3)$ kétféle lehet: $(x_1 \circ x_2) \circ x_3$ vagy $x_1 \circ (x_2 \circ x_3)$. Az első esetben $(x_1 \circ x_2) \circ x_3 = [x_1, x_2, x_3]$ a balra normált szorzat definíciója szerint igaz, a második estben $x_1 \circ (x_2 \circ x_3) = [x_1, x_2, x_3]$ az asszociatívitás miatt teljesül. A továbbiakban legyen $n \geq 3$ és tételezzük fel állításunk igazságát minden $1 \leq k \leq n$ egészre. Tekintsünk most egy olyan $h(x_1, x_2, ..., x_n, x_{n+1})$ szorzatot amelyben az $x_1, x_2, ..., x_n, x_{n+1} \in H$ elemek mindegyike pontosan egyszer és pontosan ebben a sorrendben

szerepel. A szorzat definíciója szerint a $h(x_1, x_2, ..., x_n, x_{n+1})$ felírására a következő lehetőségeink vannak: $x_1 \circ (f)$, $(g) \circ x_{n+1}$ és $(u) \circ (v)$, ahol f és g hosszúsága $n \geq 2$, az u egy $k \geq 2$ hosszúságú és v egy $(n+1)-k \geq 2$ hosszúságú szorzat. Balról jobbra haladva az f-ben az $x_2, x_3, ..., x_n, x_{n+1}$, g-ben az $x_1, x_2, ..., x_n$, u-ban az $x_1, x_2, ..., x_k$ és v-ben az $x_{k+1}, x_{k+2}, ..., x_n, x_{n+1}$ elemeket kell, hogy találjuk. Az indukciós feltevésünk szerint az $f = [x_2, x_3, ..., x_n, x_{n+1}]$ és $g = [x_1, x_2, ..., x_n]$, valamint az $u = [x_1, x_2, ..., x_k]$ és $v = [x_{k+1}, x_{k+2}, ..., x_n, x_{n+1}]$ egyenlőségek teljesülnek a H-ban. Nyilvánvalóan elegendő az alábbi

$$[x_1, x_2, ..., x_k] \circ [x_{k+1}, x_{k+2}, ..., x_n, x_{n+1}] = [x_1, x_2, ..., x_n, x_{n+1}]$$

egyenlőséget igazolni (beleértve a $k = 1$ és $k = n$ egészeket is). A balra normált szorzat definícióját az assszociatívitást és az indukciós feltevést újra felhasználva adódik, hogy

$$[x_1, x_2, ..., x_k] \circ [x_{k+1}, x_{k+2}, ..., x_n, x_{n+1}] = [x_1, x_2, ..., x_k] \circ ([x_{k+1}, x_{k+2}, ..., x_n] \circ x_{n+1}) =$$

$$([x_1, x_2, ..., x_k] \circ [x_{k+1}, x_{k+2}, ..., x_n]) \circ x_{n+1} = [x_1, x_2, ..., x_n] \circ x_{n+1} = [x_1, x_2, ..., x_n, x_{n+1}].$$

□□□

14.C.Definíció. Ha $\circ$ egy kétváltozós asszociatív művelet a H halmazon, akkor a $(H, \circ)$ párost **félcsoportnak** nevezzük. Gyakran előfordul, hogy a $\circ$ műveletre nem szükséges külön utalást tennünk, ilyenkor a H-ra önállóan is használhatjuk a félcsoport elnevezést. A 14.2. Állítás szerint egy $(H, \circ)$ félcsoport $x_1, x_2, ..., x_n \in H$ elemeire a zárójelek és műveleti jelek nélkül felírt $x_1x_2...x_n$ sorozatnak egyértelműen megadható a H-beli jelentése úgy mint a $x_1 \circ x_2 \circ ... \circ x_n$ jelsorozat egy tetszőleges értelmes zárójelezése által meghatározott H-beli szorzat elem, pl. $x_1x_2...x_n = [x_1, x_2, ..., x_n]$. Egy $x \in H$ elemnek az $n \geq 1$ egész kitevőjű hatványát az $x^n = xx...x$ (itt x pontosan n-szer szerepel) szorzat értelmezi.♡

A továbbiakban félcsoportokban mellőzhetjük a $\circ$ vagy más műveleti jel használatát, elegendő a szorzat megadásához a benne szereplő elemek egymás után írása. Mindaddig tehetjük ezt, amíg egyetlen műveletünk van, amennyiben a H halmazon egyidejüleg több (asszociatív) művelet is adott akkor csak egy előre kijelölt műveletnek lehet a jelét az algebrai kifejezésekből elhagyni a többire mindenképpen szükséges a műveleti jel kiírása, pl. az $a, b, c \in \mathbb{Z}$ számokkal felírt $(ab + c)ac(bc + a) + abc$ kifejezésben a szokásos módon a szorzás műveleti jelét nem tüntettük fel. Ismét a 14.2. Állítást alkalmazva kapjuk a következőket:

$$(x_1x_2...x_n)(x_{n+1}x_{n+2}...x_{n+m}) = x_1x_2...x_{n+m} \ ,$$

$$x^n x^m = x^{n+m} \ , \ (x^n)^m = x^{nm}.$$

14.D.Definíció. A $(H, \circ)$ félcsoportban

1. az $x, y \in H$ elemeket **felcserélhetőeknek** nevezzük, ha $xy = yx$;
2. teljesül a **kommutatívitás**, ha bármely két elem felcserélhető, azaz ha $xy = yx$ minden $x, y \in H$ elemre;
3. az $e \in H$ elemet **egységnek** nevezzük, ha $ex = xe = x$ minden $x \in H$ elemre;
4. a $c \in H$ elemet **centrálisnak** nevezzük, ha $cx = xc$ minden $x \in H$ elemre (az egységek centrálisak); a H centrális elemeinek halmazát jelölje $\xi(H)$;
5. az $x \in H$ elemmel **balról egyszerűsíthetünk**, ha tetszőleges $u, v \in H$ elemekre az $xu = xv$ egyenlőség csak az $u = v$ esetben teljesülhet (hasonlóan értelmezzük a jobbról egyszerűsíthetőséget).♡

A $(H, \circ)$ félcsoport felcserélhető $x, y \in H$ elemeire

$$(xy)^n = x^n y^n.$$

Ha $(H, \circ)$ kommutatív, akkor az $x_1, x_2, ..., x_n \in H$ elemek tetszőleges $x_{\pi(1)}, x_{\pi(2)}, ..., x_{\pi(n)}$ átrendezésére (permutációjára) teljesül a szorzatok alábbi egyenlősége

$$x_{\pi(1)} x_{\pi(2)} ... x_{\pi(n)} = x_1 x_2 ... x_n \ .$$

Egy félcsoportban nem létezhet két egymástól különböző egység: az $e_1, e_2 \in H$ egységekre $e_1 x = x$ és $y e_2 = y$, ahonnan $x = e_2$ és $y = e_1$ választással azonnal kapjuk, hogy $e_1 = e_2$. Értelmes tehát azt mondani, hogy $(H, \circ, e)$ egy egységelemes félcsoport, az egységelemes félcsoportot **monoidnak** nevezzük. Az egységet 1 jelöli a legtöbbször, de ha egy kommutatív félcsoportban a műveleti jel + akkor az egységet 0-val szokás jelölni, pl. $(\mathbb{Z}, +, 0)$ egységelemes kommutatív félcsoport (azaz kommutatív monoid).

14.E.Definíció. A $(H, \circ, 1)$ monoidban egy $x \in H$ elem **balinverze** minden olyan $x' \in H$ elem, amelyre $x'x = 1$. A **jobbinverzek** az $xx'' = 1$ tulajdonságú $x'' \in H$ elemek. Az $x \in H$ elem (kétoldali) **inverze** minden olyan elem, amelyik egyidejűleg balinverze is és jobbinverze is x-nek.♡

Ha $x' \in H$ balinverze és $x'' \in H$ jobbinverze az $x \in H$ elemnek, akkor

$$x' = x' \circ 1 = x' \circ (x \circ x'') = (x' \circ x) \circ x'' = 1 \circ x'' = x''.$$

Tehát egy x elemnek nem létezhet két egymástól különböző inverze és így az inverz létezése esetén jogosultak vagyunk az x^{-1} jelölésre: $x^{-1}x = xx^{-1} = 1$. Előfordulhat, hogy egy elemnek végtelen sok balinverze van (ilyenkor jobbinverze nem létezhet). Ha x-nek van balinverze (jobbinverze), akkor az x elemmel lehet balról (jobbról) egyszerűsíteni: ha az $x, u, v, h \in H$ elemekre $xu = xv = h$, akkor az $x' \in H$ balinverzet használva kapjuk, hogy

$$u = 1 \circ u = (x'x)u = x'(xu) = x'h = x'(xv) = (x'x)v = 1 \circ v = v,$$

továbbá azt, hogy az $u = x'h$ elem kielégíti az $xu = h$ egyenletet. Az inverzekkel való számolás (könnyen ellenőrízhető) szabályait az alábbiakban adjuk meg egy $(H, \circ, 1)$ monoid inverzekkel rendelkező $x, y \in H$ elemeire és az $n \geq 1$ egészre:

$$(x^{-1})^{-1} = x, \ (xy)^{-1} = y^{-1}x^{-1}, \ (x^n)^{-1} = (x^{-1})^n.$$

14.F.Definíció. A $(G, \circ, 1)$ monoidot **csoportnak** nevezzük, ha minden $x \in G$ elemnek létezik az $x^{-1} \in G$ inverze. Ilyenkor egy $x \in G$ elemet és az $A, B, H \subseteq G$ részhalmazokat tekintve

1. az $n \geq 1$ egészre legyen $x^{-n} = (x^n)^{-1} = (x^{-1})^n$ és $x^0 = 1$;
2. értelmezzük G-nek az $A^{-1} = \{a^{-1} \mid a \in A\}$, $xA = \{xa \mid a \in A\}$, $Ax = \{ax \mid a \in A\}$ és $AB = \{ab \mid a \in A, b \in B\}$ (nyilvánvaló, hogy $\{x\}A = xA$ és $A\{x\} = Ax$) részhalmazait;
3. a $H \leq G$ jelölést alkalmazzuk és azt mondjuk, hogy H **részcsoportja** G-nek, ha $1 \in H$ és H zárt a szorzásra valamint az inverz képzésére nézve: tetszőleges $u, v \in H$ elemekre $uv \in H$ és $u^{-1} \in H$ (a $\varnothing \neq H \subseteq G$ részhalmaz pontosan akkor részcsoportja G-nek, ha $HH \subseteq H$ és $H^{-1} \subseteq H$); egy $H \leq G$ részcsoportra $(H, \circ, 1)$ önállóan is csoport;

4. a $H \lhd G$ jelölést alkalmazzuk és azt mondjuk, hogy H **normális részcsoportja** G-nek, ha $H \leq G$ részcsoport és H zárt a G elemeivel való konjugálásra nézve: tetszőleges $h \in H$ és $g \in G$ elemre $g^{-1}hg \in H$ ($g^{-1}xg$-t nevezzük az x elem g-vel való **konjugáltjának**).♡

14.3.Állítás. *Egy $(G, \circ, 1)$ csoport $x, y \in G$ elemeire és a $H, N \subseteq G$ részhalmazokra az alábbiak teljesülnek.*

1. *Az $x \in G$ elemmel lehet jobbról is és balról is egyszerűsíteni.*
2. *$x^k x^l = x^{k+l}$ és $(x^k)^l = x^{kl}$ tetszőleges $k, l \in \mathbb{Z}$ egészekre.*
3. *$\langle x \rangle = \{..., x^{-l}, ..., x^{-3}, x^{-2}, x^{-1}, 1, x, x^2, ..., x^k, ...\} \leq G$ részcsoport.*
   *Ha létezik olyan $z \in G$ elem, amelyre $\langle z \rangle = G$, akkor G-t **ciklikusnak** nevezzük, minden ciklikus csoport kommutatív.*
4. *Részcsoportok tetszőleges metszete is részcsoport.*
5. *$H \leq G \iff HH^{-1} \subseteq H$.*
6. *$H \leq G \iff H^{-1}H \subseteq H$.*
7. *Amennyiben $H \leq G$, akkor: $N \leq G$ és $N \subseteq H \iff N \leq H$.*
8. *Amennyiben $H \leq G$, akkor $x \in xH$, $|xH| = |H|$ és*
   $xH = yH \iff x \in yH \iff y \in xH \iff x^{-1}y \in H \iff y^{-1}x \in H \iff xH \cap yH \neq \varnothing$.
   *Az $xH \subseteq G$ részhalmazt nevezzük az x **elem H szerinti baloldali mellékosztályának**.*
9. *Amennyiben $H \leq G$, akkor $x \in Hx$, $|Hx| = |H|$ és*
   $Hx = Hy \iff x \in Hy \iff y \in Hx \iff xy^{-1} \in H \iff yx^{-1} \in H \iff Hx \cap Hy \neq \varnothing$.
   *A $Hx \subseteq G$ részhalmazt nevezzük az x **elem H szerinti jobboldali mellékosztályának**.*
10. *$\{1\} \lhd G$ és $G \lhd G$.*
    *Ha G-nek csak ez a két (ún. **triviális**) normális részcsoportja van ($H \lhd G \iff H = \{1\}$ vagy $H = G$), akkor G-t **egyszerűnek** nevezzük; a triviálistól különböző részcsoportot **valódinak** nevezzük.*
11. *A G centrális elemeinek halmaza G-nek normális részcsoportja: $\xi(G) \lhd G$.*
12. *Amennyiben G kommutatív, akkor G-nek minden $H \leq G$ részcsoportja normális részcsoport is: $H \lhd G$.*
13. *Normális részcsoportok tetszőleges metszete is normális részcsoport.*
14. *Amennyiben $H \leq G$, akkor $H \lhd G \iff gH = Hg$ teljesül minden $g \in G$ elemre.*
15. *Amennyiben $H \lhd G$, akkor $AH = HA$ tetszőleges $A \subseteq G$ részhalmazra.*
16. *Amennyiben $H \lhd G$ továbbá az $u, v \in G$ elemekre $uH = xH$ és $vH = yH$, akkor $uvH = xyH$.*
17. *Amennyiben $H \leq G$, $N \lhd G$ és $N \subseteq H$, akkor $N \lhd H$.*

18. *Amennyiben $H \leq G$ és $N \lhd G$, akkor $N \cup H \subseteq NH = HN$ és $NH = HN \leq G$ részcsoport, továbbá $N \lhd NH = HN$ és $N \cap H \lhd H$.*

Bizonyítás.

1. Ha az $u, v \in G$ elemekre $xu = xv$ teljesül, akkor az egyenlőség mindkét oldalát balról szorozva az $x^{-1} \in G$ inverz elemmel az alábbiakat kapjuk:

$$u = 1u = (x^{-1}x)u = x^{-1}(xu) = x^{-1}(xv) = (x^{-1}x)v = 1v = v.$$

2. Ha $k \geq 1$ és $l \geq 1$, akkor a 14.C.Definíció után tett megjegyzések értelmében az $x^k x^l = x^{k+l}$ és $(x^k)^l = x^{kl}$ egyenlőségek teljesülnek. Ha $k \geq 1$, $l \leq -1$ és $k \geq |l| = -l$, akkor az előbb igazolt esetet, a 14.E.Definíció utáni megállapításokat és a 14.F.Definíció 1.részét használva kapjuk az alábbiakat

$$x^k x^l = (x^{k+l}x^{-l})x^l = (x^{k+l}(x^l)^{-1})x^l = x^{k+l}((x^l)^{-1}x^l) = x^{k+l}1 = x^{k+l},$$

$$(x^k)^l = ((x^k)^{-l})^{-1} = (x^{-kl})^{-1} = x^{kl}.$$

   A további lehetséges esetek áttekintését az olvasóra bízzuk.

3. $1 = x^0 \in \langle x \rangle$ és ha $u, v \in \langle x \rangle$, akkor $u = x^k$, $v = x^l$ teljesül alkalmas $k, l \in \mathbb{Z}$ egészekre. Most az előbbi 2.rész alapján $uv = x^k x^l = x^{k+l} \in \langle x \rangle$ és $u^{-1} = (x^k)^{-1} = x^{-k} \in \langle x \rangle$ adódik. A $\langle z \rangle$ kommutatívitása $z^k z^l = z^{k+l} = z^{l+k} = z^l z^k$ következménye.

4. A $H_\gamma \leq G$ (itt $\gamma \in \Gamma$) részcsoportokra $1 \in H_\gamma$, ahonnan $1 \in \bigcap_{\gamma\in\Gamma} H_\gamma$ következik. Ha $u, v \in \bigcap_{\gamma\in\Gamma} H_\gamma$, akkor $u, v \in H_\gamma$ minden $\gamma \in \Gamma$ indexre, ami a részcsoport tulajdonságai miatt az $uv \in H_\gamma$ és az $u^{-1} \in H_\gamma$ tartalmazásokat eredményezi tetszőleges $\gamma \in \Gamma$ indexre. Tehát $uv \in \bigcap_{\gamma\in\Gamma} H_\gamma$ és $u^{-1} \in \bigcap_{\gamma\in\Gamma} H_\gamma$.

5. A HH^{-1} bármely eleme egy uv^{-1} alakban írható szorzat, ahol $u, v \in H$. Mivel $H \leq G$, ezért előbb a $v^{-1} \in H$ tartalmazást, majd innen az $uv^{-1} \in H$ tartalmazást kapjuk. Tehát $HH^{-1} \subseteq H$.

   Amennyiben $HH^{-1} \subseteq H$ és $v \in H$ tetszőleges, akkor $1 = vv^{-1} \in HH^{-1}$ miatt előbb $1 \in H$, majd $v^{-1} = 1v^{-1} \in HH^{-1}$ miatt $v^{-1} \in H$ adódik. Ha $u \in H$ egy további elem, akkor $v^{-1} \in H$ és $uv = u(v^{-1})^{-1} \in HH^{-1}$ miatt az $uv \in H$ tartalmazást kapjuk.

6. Az 5.részhez hasonlóan igazolható.

7. A $(H, \circ, 1)$ csoportban az 1 egység elem azonos a G-beli egység elemmel, továbbá az elemek szorzása és inverzének képzése is megegyezeik a G-belivel.

   Legyen most $N \leq G$ és $N \subseteq H$, ekkor $N \leq G$ miatt $1 \in N$ teljesül. Az $x, y \in N$ elemekre $N \leq G$ miatt $xy \in N$ és $x^{-1} \in N$ teljesül, ami a $(H, \circ, 1)$ csoportról elmondottak alapján azt jelenti, hogy $N \leq H$ részcsoport a $(H, \circ, 1)$ csoportban is.

   Amennyiben $N \leq H$ részcsoportja a $(H, \circ, 1)$ csoportnak, akkor $1 \in N$, továbbá az $x, y \in N$ elemekre $xy \in N$ és $x^{-1} \in N$ teljesül. A $(H, \circ, 1)$ csoportról elmondottak alapján ez azt jelenti, hogy $N \leq G$ részcsoport a $(G, \circ, 1)$ csoportban is.

8. $1 \in H$ miatt $x = x1 \in xH$ és egy $h \in H$ elemre a $h \longmapsto xh$ hozzárendelés bijektív $H \longrightarrow xH$ függvényt értelmez, ahonnan $|xH| = |H|$ adódik. A fenti hozzárendelés szürjektív, hiszen xH minden eleme xh alakban írható. Az injektívitás abból következik, hogy $xh_1 = xh_2$ esetén az 1.rész szerint x-el lehet balról egyszerűsíteni (itt $h_1, h_2 \in H$).

   Ha $xH = yH$, akkor $x \in xH$ miatt $x \in yH$ is teljesül.

   Ha $x \in yH$, akkor $x = yh$ valamilyen $h \in H$ elemre és a h^{-1} inverz elemmel való jobbról szorzás az $xh^{-1} = y$ egyenlőséghez, illetve $h^{-1} \in H$ miatt az $y \in xH$ tartalmazáshoz vezet.

   Ha $y \in xH$, akkor $y = xg$ valamilyen $g \in H$ elemre, ahonnan az x^{-1} inverz elemmel való balról szorzás az $x^{-1}y = g$ egyenlőséghez, illetve $g \in H$ miatt az $x^{-1}y \in H$ tartalmazáshoz vezet.

   Ha $x^{-1}y \in H$, akkor $y^{-1}x = y^{-1}(x^{-1})^{-1} = (x^{-1}y)^{-1} \in H$, hiszen H zárt az inverz képzésére.

   Ha $y^{-1}x \in H$, akkor $x \in xH$ és $x = y(y^{-1}x) \in yH$ miatt $x \in xH \cap yH$ is teljesül.

   Ha $xH \cap yH \neq \varnothing$, akkor kiválasztva egy tetszőleges $z \in xH \cap yH$ elemet $z = xa = yb$ teljesül alkalmas $a, b \in H$ elemekkel, ami az $x = za^{-1} = yba^{-1}$ egyenlőséget eredményezi. Most egy $h \in H$ elemre $ba^{-1}h \in H$ miatt az $xh = yba^{-1}h \in yH$ tartalmazást kapjuk, ami azt jelenti, hogy $xH \subseteq yH$. Hasonlóan látható a fordított $yH \subseteq xH$ tartalmazás is.

9. A 8.részhez hasonlóan igazolható.

10. $G \lhd G$ nyilvánvaló, az $\{1\} \lhd G$ igazolásához elég a következőket megjegyezni: $1 \cdot 1 = 1$, $1^{-1} = 1$ és $g^{-1}1g = g^{-1}g = 1$ tetszőleges $g \in G$ elemre.

11. Ha $c, c_1, c_2 \in \xi(G)$, akkor tetszőleges $x \in G$ elemre

$$(c_1c_2)x = c_1(c_2x) = c_1(xc_2) = (c_1x)c_2 = (xc_1)c_2 = x(c_1c_2) \text{ és}$$

$$c^{-1}x = (c^{-1}x)cc^{-1} = c^{-1}(xc)c^{-1} = c^{-1}(cx)c^{-1} = (c^{-1}c)xc^{-1} = xc^{-1}.$$

   Tehát c_1c_2 és c^{-1} centrális elemek, azaz $c_1c_2 \in \xi(G)$ és $c^{-1} \in \xi(G)$.

   Ha $g \in G$, akkor

$$g^{-1}cg = g^{-1}(cg) = g^{-1}(gc) = (g^{-1}g)c = c \in \xi(G).$$

12. A kommutatívitás miatt tetszőleges $h \in H$ és $g \in G$ elemekre

$$g^{-1}hg = g^{-1}(hg) = g^{-1}(gh) = (g^{-1}g)h = h \in H.$$

13. Amennyiben $g \in G$ és $h \in \bigcap_{\gamma\in\Gamma} H_\gamma$ a $H_\gamma \lhd G$ (itt $\gamma \in \Gamma$) normális részcsoportokra, akkor $h \in H_\gamma$ minden $\gamma \in \Gamma$ indexre. A normális részcsoport tulajdonságai miatt $g^{-1}hg \in H_\gamma$ minden $\gamma \in \Gamma$ indexre. Tehát $g^{-1}hg \in \bigcap_{\gamma\in\Gamma} H_\gamma$, ami azt jelenti, hogy $\bigcap_{\gamma\in\Gamma} H_\gamma \lhd G$.

14. Egy $h \in H$ elemre $gh = (gh)g^{-1}g = (ghg^{-1})g \in Hg$, hiszen a $H \lhd G$ normális részcsoportra $ghg^{-1} = (g^{-1})^{-1}h(g^{-1}) \in H$. Tehát $gH \subseteq Hg$ és a fordított $Hg \subseteq gH$ tartalmazást is hasonlóan igazolhatjuk.

   Legyen most $gH = Hg$ tetszőleges $g \in G$ elemre, ekkor egy $h \in H$ elemre $hg \in Hg$ miatt $hg \in gH$, azaz $hg = gh'$ valamilyen $h' \in H$ elemmel. Így $g^{-1}hg = g^{-1}gh' = h' \in H$, ami azt jelenti, hogy $H \lhd G$ normális részcsoport.

15. A 14.rész felhasználásával kapjuk, hogy tetszőleges $A \subseteq G$ részhalmazra

$$AH = \bigcup_{g \in A} gH = \bigcup_{g \in A} Hg = HA.$$

16. Ha $uH = xH$ és $vH = yH$, akkor $u \in uH$ és $v \in vH$ miatt $u = xh_1$ és $v = yh_2$ teljesül alkalmas $h_1, h_2 \in H$ elemekkel. Így

$$uv = xh_1yh_2 = x(yy^{-1})h_1yh_2 = xy(y^{-1}h_1y)h_2 \in xyH,$$

mert a $H \lhd G$ normális részcsoportban $y^{-1}h_1y \in H$ miatt $(y^{-1}h_1y)h_2 \in H$ teljesül. A 8.rész figyelembe vételével kapjuk, hogy $uvH = xyH$.

17. Mivel $N \lhd G$ miatt N zárt a G elemeivel való konjugálásra, ezért N nyilvánvalóan zárt a G-nél szűkebb H-nak az elemeivel való konjugálásra is, tehát $N \leq H$ miatt (ez a 7.rész alapján igaz) $N \lhd H$ is teljesül.

18. Legyen $H \leq G$ és $N \lhd G$, ekkor $1 \in H$ és $1 \in N$ miatt $N \subseteq NH$ és $H \subseteq NH$, továbbá a 15.rész szerint $NH = HN$. Most az $x_1y_1 \in HN$ és az $x_2y_2 \in HN$ elemekre (itt $x_1, x_2 \in H$, $y_1, y_2 \in N$ és az $y_1x_2 \in Nx_2$ elemre $Nx_2 = x_2N$ miatt $y_1x_2 = x_2y_1'$ teljesül valamilyen $y_1' \in N$ elemmel) $x_1x_2 \in H$ és $y_1'y_2 \in N$ miatt

$$x_1y_1x_2y_2 = x_1x_2y_1'y_2 \in HN,$$

továbbá $y_1^{-1} \in N$ és $x_1^{-1} \in H$ alapján

$$(x_1y_1)^{-1} = (y_1)^{-1}(x_1)^{-1} \in NH = HN.$$

Tehát HN zárt a szorzásra és az inverz képzésére, ezért $HN \leq G$ részcsoport. Mivel $N \lhd G$ és $N \subseteq NH$, ezért a 17.rész szerint $N \lhd NH$.

$N \cap H \leq G$ és $N \cap H \subseteq H$ miatt a 7.rész alkalmazásával kapjuk, hogy $N \cap H \leq H$. Mivel N is és nyilvánvalóan maga H is zárt a H elemeivel való konjugálásra, ezért $N \cap H$ zárt lesz a H elemeivel való konjugálásra, tehát $N \cap H \lhd H$.

□□□

14.4.Állítás. *Ha egy $(G, \circ, 1)$ csoportban $H_1 * H_2$ jelöli a $H_1 \leq G$ és $H_2 \leq G$ részcsoportok $H_1 \cup H_2$ unióját tartalmazó valamennyi részcsoportnak a metszetét, akkor*

$$H_1 \cup H_2 \subseteq H_1 * H_2 \leq G \quad , \quad H_2 * H_1 = H_1 * H_2$$

és tetszőleges $N \leq G$ részcsoportra

$$H_1 \cup H_2 \subseteq N \Longleftrightarrow H_1 * H_2 \subseteq N,$$

továbbá

$$H_1 * H_2 = \{x_1y_1x_2y_2...x_ny_n \mid n \geq 1 \text{ és } x_1, x_2, ..., x_n \in H_1 \text{ és } y_1, y_2, ..., y_n \in H_2\}.$$

Amennyiben $H_1 \lhd G$ (vagy $H_2 \lhd G$), akkor $H_1 * H_2 = H_1H_2 = H_2H_1$.

Bizonyítás. A $H_1 \cup H_2 \subseteq H_1 * H_2$ tartalmazás nyilvánvaló következménye a $H_1 * H_2$ értelmezésének. Mivel a G részcsoportjainak tetszőleges metszete is részcsoport (lásd a 14.3.Állítás 4.részét),

ezért $H_1 * H_2 \leq G$. A $H_2 * H_1 = H_1 * H_2$ egyenlőség egyszerűen annak a következménye, hogy $H_1 \cup H_2 = H_2 \cup H_1$. Az $N \leq G$ részcsoportra a tartalmazásoknak az $H_1 \cup H_2 \subseteq N \iff H_1 * H_2 \subseteq N$ ekvivalenciája szintén a $H_1 * H_2$ értelmezésének köszönhető.
Tekintsük az ($H_1 * H_2$-beli) $x_1, x_2, ..., x_n \in H_1$ és $y_1, y_2, ..., y_n \in H_2$ elemeket, ekkor $H_1 * H_2$-nek a (G-beli) szorzásra való zártsága miatt

$$x_1y_1x_2y_2...x_ny_n \in H_1 * H_2,$$

ahonnan az

$$M = \{x_1y_1x_2y_2...x_ny_n \mid n \geq 1 \text{ és } x_1, x_2, ..., x_n \in H_1 \text{ és } y_1, y_2, ..., y_n \in H_2\}$$

halmazra az $M \subseteq H_1 * H_2$ tartalmazás adódik.
Most belátjuk, hogy M olyan részcsoportja G-nek, amelyre $H_1 \cup H_2 \subseteq M$. Így az eddigiek alapján előbb a $H_1 * H_2 \subseteq M$ tartalmazást, majd a kívánt $H_1 * H_2 = M$ egyenlőséget kapjuk.
Mivel $y_1 = 1 \in H_2$ miatt tetszőleges $x_1 \in H_1$ elemre $x_1 = x_11 = x_1y_1 \in M$, ezért $H_1 \subseteq M$. A $H_2 \subseteq M$ tartalmazás is hasonlóan látható. Az M-beli

$$x_1y_1x_2y_2...x_ny_n \text{ és } x'_1y'_1x'_2y'_2...x'_my'_m$$

elemek (itt $x'_1, x'_2, ..., x'_m \in H_1$ és $y'_1, y'_2, ..., y'_m \in H_2$) szorzatára

$$(x_1y_1x_2y_2...x_ny_n)(x'_1y'_1x'_2y'_2...x'_ny'_n) = x_1y_1x_2y_2...x_ny_nx'_1y'_1x'_2y'_2...x'_my'_m \in M$$

nyilvánvalóan teljesül. Az $x_{n+1} = 1 = y_0$ elemek beiktatásával az M-beli $x_1y_1x_2y_2...x_ny_n$ elem inverzére

$$(x_1y_1x_2y_2...x_ny_n)^{-1} = y_n^{-1}x_n^{-1}...y_2^{-1}x_2^{-1}y_1^{-1}x_1^{-1} = x_{n+1}y_n^{-1}x_n^{-1}...y_2^{-1}x_2^{-1}y_1^{-1}x_1^{-1}y_0 \in M$$

teljesül, hiszen $x_{n+1}, x_n^{-1}, ..., x_2^{-1}, x_1^{-1} \in H_1$ és $y_n^{-1}, ...y_2^{-1}, y_1^{-1}, y_0 \in H_2$. Tehát $M \leq G$ részcsoport.
Mivel a H_1H_2 szorzat elemei x_1y_1 alakban írhatóak egy $x_1 \in H_1$ és egy $y_1 \in H_2$ elemmel, ezért $H_1H_2 \subseteq H_1 * H_2$. Amennyiben $H_1 \lhd G$, akkor a 14.3.Állítás 18.része szerint $H_1 \cup H_2 \subseteq H_1H_2 = H_2H_1 \leq G$, ahonnan az eddigiek alapján a $H_1 * H_2 \subseteq H_1H_2$ tartalmazás, illetve a $H_1 * H_2 = H_1H_2$ egyenlőség következik.

□□□

14.5.Állítás. *Ha egy $(G, \circ, 1)$ csoportban a $H \subseteq G$ véges részhalmazra $1 \in H$ és H zárt a szorzásra nézve (tetszőleges $u, v \in H$ elemekre $uv \in H$), akkor $H \leq G$ részcsoport.*

Bizonyítás. Legyen $h_1, h_2, ..., h_n$ egy olyan felsorolása H összes elemeinek, hogy $1 \leq i < j \leq n$ esetén $h_i \neq h_j$. Tetszőleges $u \in H$ elemre $uh_1, uh_2, ..., uh_n$ is egy teljes felsorolása H elemeinek, hiszen az $i \neq j$ egészekre az $uh_i = uh_j$ egyenlőségből a balról való egyszerűsíthetőség miatt $h_i = h_j$ következne. Mivel az $\{uh_i \mid 1 \leq i \leq n\}$ elemei között szerepelnie kell az 1-nek is, ezért u-nak létezik jobbinverze: $uu'' = 1$ teljesül valamely $u'' = h_i$ elemre. Hasonlóképpen az előbbi u''-nek is létezik egy jobbinverze: $u''v = 1$ valamelyik $v \in H$ elemre. Az u'' elemnek az u balinverzére és v jobbinverzére $u = v$, ami azt jelenti, hogy u'' kétoldali inverze az u-nak: $u^{-1} = u'' \in H$.

□□□

Következmény. *Ha egy $(G, \circ, 1)$ csoportban az $x \in G$ elemre $\{1, x, x^2, ..., x^k, ...\} \subseteq G$ véges részhalmaz, akkor $\{1, x, x^2, ..., x^k, ...\} \leq G$ részcsoport és $\langle x \rangle = \{1, x, x^2, ..., x^k, ...\}$.*

14.G.Definíció. Ha egy $(G, \circ, 1)$ csoport $x \in G$ eleméhez van olyan $k \geq 1$ egész, amelyre $x^k = 1$, akkor a legkisebb ilyen tulajdonságú

$$d = \min\{k \mid k \geq 1 \text{ egész és } x^k = 1\}$$

számot nevezzük az x **elem rendjének**. Ha $x^k \neq 1$ minden $k \geq 1$ egészre, akkor azt mondjuk, hogy az x **elem végtelen rendű**.♡

14.6.Állítás. *Ha egy $(G, \circ, 1)$ csoportban az $x \in G$ elem rendje d, akkor $x^k = x^l$ teljesülése ekvivalens azzal, hogy a $k - l$ különbség osztható d-vel: $x^k = x^l \Longleftrightarrow d \mid k - l$. Továbbá*

$$\langle x \rangle = \{1, x, x^2, ..., x^{d-1}\},$$

ami azt jelenti, hogy az $\langle x \rangle \leq G$ részcsoport d elemű. Az $\left\langle x^k \right\rangle \subseteq \left\langle x^l \right\rangle$ tartalmazás teljesülése most ekvivalens azzal, hogy k osztható $\text{lnko}(d, l)$-el: $\left\langle x^k \right\rangle \subseteq \left\langle x^l \right\rangle \Longleftrightarrow \text{lnko}(d, l) \mid k$.
Ha az $x \in G$ elem végtelen rendű, akkor tetszőleges $k \neq l$ egész kitevőkre $x^k \neq x^l$ (tehát ilyenkor $\langle x \rangle \leq G$ végtelen részcsoport). Az $\left\langle x^k \right\rangle \subseteq \left\langle x^l \right\rangle$ tartalmazás teljesülése most ekvivalens azzal, hogy k osztható l-el: $\left\langle x^k \right\rangle \subseteq \left\langle x^l \right\rangle \Longleftrightarrow l \mid k$. Véges csoport minden eleme véges rendű.

Bizonyítás. Ha $d \mid k - l$, akkor $k - l = dt$ teljesül valamilyen $t \in \mathbb{Z}$ egész számra, ahonnan a 14.3.Állítás 2.részének figyelembe vételével előbb $x^{k-l} = x^{dt} = (x^d)^t = 1^t = 1$, majd $x^k = x^{k-l}x^l = 1x^l = x^l$ adódik. Ha $d \nmid k - l$, akkor maradékos osztással a $k - l = dt + r$ egyenlőséget kapjuk, ahol $1 \leq r \leq d - 1$. Most

$$x^{k-l} = x^{dt+r} = x^{dt}x^r = (x^d)^t x^r = 1^t x^r = x^r \neq 1,$$

ahonnan $x^k \neq x^l$ következik. Tehát $\{1, x, x^2, ..., x^{d-1}\}$ elemeinek száma pontosan d.
Az $\langle x \rangle$ tetszőleges eleme x^k alakban írható valamilyen $k \in \mathbb{Z}$ egész kitevővel. Maradékos osztással a $k = dt + l$ egyenlőséget kapjuk (itt $0 \leq l \leq d - 1$), ahonnan a már igazoltak szerint

$$x^k = x^l \in \{1, x, x^2, ..., x^{d-1}\},$$

következik. Így előbb az $\langle x \rangle \subseteq \{1, x, x^2, ..., x^{d-1}\}$ tartalmazáshoz, majd a kívánt egyenlőséghez jutunk.
Mivel $\left\langle x^k \right\rangle \subseteq \left\langle x^l \right\rangle \Longrightarrow x^k \in \left\langle x^l \right\rangle$, ezért $x^k = (x^l)^t = x^{lt}$ teljesül valamilyen $t \in \mathbb{Z}$ egész kitevőre. A korábban igazoltak szerint a $d \mid k - lt$ oszthatóságnak teljesülnie kell. Most $k - lt = dm$, illetve $k = dm + lt$ valamilyen $m \in \mathbb{Z}$ egész számra, ahonnan a kívánt $\text{lnko}(d, l) \mid k$ oszthatóság azonnal adódik.
Ha viszont az $\text{lnko}(d, l) \mid k$ oszthatóság teljesül, akkor léteznek olyan $m, t \in \mathbb{Z}$ egész számok, amelyekre $k = dm + lt$. Most

$$x^k = x^{dm+lt} = x^{dm}x^{lt} = (x^d)^m x^{lt} = 1^m x^{lt} = (x^l)^t \in \left\langle x^l \right\rangle,$$

ahonnan $\left\langle x^k \right\rangle \subseteq \left\langle x^l \right\rangle$ következik.
Ha az $x \in G$ elem végtelen rendű, akkor a $k \neq l$ egész kitevőkre az $x^k = x^l$ egyenlőségből x^{-l}-el való (jobbról vagy balról) szorzás után az $x^{k-l} = 1$ ellentmondáshoz jutunk. Tehát a $k \neq l$ egész kitevőkre $x^k \neq x^l$, azaz $\langle x \rangle$ elemeinek száma végtelen.
Mivel $\left\langle x^k \right\rangle \subseteq \left\langle x^l \right\rangle \Longrightarrow x^k \in \left\langle x^l \right\rangle$, ezért $x^k = (x^l)^t = x^{lt}$ teljesül valamilyen $t \in \mathbb{Z}$ egész kitevőre. Az előbbiek szerint a $k = lt$ egyenlőségnek teljesülnie kell, ami az $l \mid k$ oszthatóságot jelenti.
Ha viszont az $l \mid k$ oszthatóság teljesül, akkor létezik olyan $t \in \mathbb{Z}$ egész szám, amelyre $k = lt$. Így $x^k = x^{lt} = (x^l)^t \in \left\langle x^l \right\rangle$, ahonnan $\left\langle x^k \right\rangle \subseteq \left\langle x^l \right\rangle$ következik.

□□□

14.7.Állítás. *Egy $(G, \circ, 1)$ ciklikus csoport minden részcsoportja ciklikus, azaz ha $G = \langle z \rangle$ valamilyen $z \in G$ elemre és $H \leq G$, akkor létezik olyan $h \in H$ elem, amelyre $H = \langle h \rangle$.*

Bizonyítás. Tekintsük az alábbi

$$k = \min\{t \in \mathbb{Z} \,|t \geq 1 \text{ és } z^t \in H\}$$

egész számot, ami $H \neq \{1_G\}$ esetén létezik. Valóban, ha egy $0 \neq t \in \mathbb{Z}$ egészre $z^t \in H$, akkor $z^{-t} = (z^t)^{-1} \in H$ is teljesül, ami azt jelenti, hogy a fenti halmaz nem üres. Mivel $z^k \in H$ miatt a $\langle z^k \rangle \subseteq H$ tartalmazás nyilvánvaló, ezért a $H = \langle z^k \rangle$ egyenlőség igazolásához elegendő megmutatni, hogy $H \subseteq \langle z^k \rangle$. Most H-nak egy tetszőleges eleme z^l alakban írható, amennyiben ezt az $l \in \mathbb{Z}$ egész számot maradékosan osztjuk k-val, akkor az $l = km + r$ egyenlőséghez jutunk valamilyen $0 \leq r \leq k-1$ maradékkal. Ha $r \neq 0$, akkor $z^k \in H$ és $z^l \in H$ figyelembe vételével a

$$z^r = z^{km-l} = (z^k)^m (z^l)^{-1} \in H$$

tartalmazást kapjuk, ami ellentmond k minimalitásának. Tehát $r = 0$, ahonnan

$$z^l = z^{km} = (z^k)^m \in \langle z^k \rangle$$

adódik.

□□□

14.H.Definíció. Egy $(G, \circ, 1)$ csoport $x_\gamma \in G, \gamma \in \Gamma$ elemeiről azt mondjuk, hogy a $H \leq G$ **részcsoportra nézve baloldali reprezentánsoknak egy teljes rendszerét** alkotják, ha

$$\bigcup_{\gamma \in \Gamma} x_\gamma H = G.$$

Az $x_\gamma \in G, \gamma \in \Gamma$ elemek pontosan akkor alkotják a $H \leq G$ részcsoportra nézve baloldali reprezentánsoknak egy teljes rendszerét, ha

$$\{x_\gamma H \mid \gamma \in \Gamma\} = \{xH \mid x \in G\}.$$

Valóban, ha $\bigcup\limits_{\gamma \in \Gamma} x_\gamma H = G$, akkor tetszőleges $x \in G$ elemre $x \in x_\gamma H$ teljesül valamilyen $\gamma \in \Gamma$ indexre, ahonnan a 14.3.Állítás 8.része szerint $xH = x_\gamma H$ következik. A 14.3.Állítás 8.részének ismételt figyelembe vételével az $\{x_\gamma H \mid \gamma \in \Gamma\} = \{xH \mid x \in G\}$ egyenlőségből

$$\bigcup_{\gamma \in \Gamma} x_\gamma H = \bigcup_{x \in G} xH = G$$

következik.
Abban az esetben, amikor még tetszőleges $\gamma, \delta \in \Gamma, \gamma \neq \delta$ indexekre $x_\gamma H \neq x_\delta H$ is teljesül **baloldali reprezentánsoknak egy teljes irredundáns rendszeréről beszélünk**. Az ún. kiválasztási axióma segítségével igazolható, hogy bármely $H \leq G$ részcsoportra nézve létezik baloldali reprezentánsoknak teljes irredundáns rendszere. A megfelelő jobboldali fogalmakat hasonlóan értelmezhetjük. Amennyiben $H \lhd G$ normális részcsoport, akkor $x_\gamma H = H x_\gamma$ miatt a baloldali és a jobboldali fogalmak egybe esnek, ezért ilyenkor csak reprezentánsok (teljes, illetve teljes irredundáns) rendszeréről beszélünk.♡

14.8.Állítás (Lagrange tétele). *Egy $(G, \circ, 1)$ véges csoportban bármely $H \leq G$ részcsoportra nézve a baloldali reprezentánsoknak tetszőleges $x_\gamma \in G, \gamma \in \Gamma$ teljes irredundáns rendszerére teljesül, hogy $|\Gamma|\,|H| = |G|$.*

Tehát H elemeinek száma osztója G elemszámának és a H részcsoportra nézve a baloldali reprezentánsoknak bármely teljes irredundáns rendszerének a számossága $|\Gamma| = \frac{|G|}{|H|}$.

Bizonyítás. A baloldali reprezentánsoknak bármely teljes $x_\gamma \in G, \gamma \in \Gamma$ rendszerére az

$$\bigcup_{\gamma\in\Gamma} x_\gamma H = G.$$

egyenlőség teljesül. Amennyiben a fenti rendszer irredundáns, akkor tetszőleges $\gamma, \delta \in \Gamma, \gamma \neq \delta$ indexekre $x_\gamma H \neq x_\delta H$, ami a 14.3.Állítás 8.része szerint azt is jelenti, hogy ilyenkor $x_\gamma H \cap x_\delta H = \varnothing$. Tehát a G halmaz megkapható a páronként diszjunkt $x_\gamma H \subseteq G, \gamma \in \Gamma$ részhalmazainak az egyesítéseként, ahonnan az elemszámokra

$$\sum_{\gamma\in\Gamma} |x_\gamma H| = |G|$$

adódik. A 14.3.Állítás 8.része szerint $|x_\gamma H| = |H|$ minden $\gamma \in \Gamma$ indexre, ami az előbbi egyenlőséget figyelembe véve a kívánt $|\Gamma|\,|H| = |G|$ összefüggést szolgáltatja.

□□□

14.9.Következmény. *Ha egy véges $(G, \circ, 1)$ csoportban $|G| = n$ és az $x \in G$ elem rendje d, akkor d osztója n-nek: $d \mid n$. Továbbá $x^n = 1$.*

Bizonyítás. A 14.6.Állítás szerint most az

$$\langle x\rangle = \{1, x, x^2, ..., x^{d-1}\} \leq G$$

részcsoport d elemű. A 14.8.Állítást alkalmazva kapjuk, hogy d osztója n-nek: $n = dm$. Tehát $x^n = x^{dm} = (x^d)^m = 1^m = 1$.

□□□

14.10.Következmény. *Egy $(G, \circ, 1)$ nem triviális csoportra ($G \neq \{1\}$) az alábbiak ekvivalensek.*

1. *$H \leq G$ esetén $H = \{1\}$ vagy $H = G$ (azaz G-nek csak triviális részcsoportjai vannak).*
2. *G ciklikus és a $|G|$ elemszám véges és prím.*
3. *A $|G|$ elemszám véges és prím.*

Bizonyítás.

(1) $\Longrightarrow$ (2) : A feltételünk szerint bármely $x \in G$ elem esetén az $\langle x\rangle \leq G$ részcsoportra $\langle x\rangle = \{1\}$ vagy $\langle x\rangle = G$ teljesül. Ha x-et 1-től különbözőnek választjuk (ezt $G \neq \{1\}$ miatt megtehetjük), akkor csak az $\langle x\rangle = G$ egyenlőség teljesülhet. Tehát G ciklikus.

Ha x végtelen rendű, akkor $x^2 \neq 1$ miatt a $H = \langle x^2\rangle \leq G$ részcsoportra $H \neq \{1\}$ és a 14.6.Állítás szerint $\langle x\rangle \not\subseteq \langle x^2\rangle$, azaz $H = \langle x^2\rangle \neq \langle x\rangle = G$. Ellentmondásba kerültünk a feltevésünkel, ezért x rendje valamilyen véges $d \geq 1$ egész szám.

Amennyiben d nem prím, akkor $d = d_1 d_2$ bizonyos $d_1 \geq 2$ és $d_2 \geq 2$ egész számokra. Most $x^{d_1} \neq 1$ miatt a $H = \left\langle x^{d_1}\right\rangle \leq G$ részcsoportra $H \neq \{1\}$ és mivel $d_1 = \text{lnko}(d, d_1)$ nem osztója 1-nek, ezért a 14.6.Állítás szerint $\langle x\rangle \not\subseteq \left\langle x^{d_1}\right\rangle$, azaz $H = \left\langle x^{d_1}\right\rangle \neq \langle x\rangle = G$. Ellentmondásba kerültünk a feltevésünkel, ezért $d = |\langle x\rangle| = |G|$ prím.

(2) $\Longrightarrow$ (3) : Nyilvánvaló.

(3) $\Longrightarrow$ (1) : A 14.8.Állítás szerint egy $H \leq G$ részcsoport $|H|$ elemszáma osztója a $|G|$ elemszámnak, ez utóbbi most prím. Tehát $|H| = 1$ vagy $|H| = |G|$, az első esetben $H = \{1\}$ a második esetben $H = G$ teljesül.

□□□

14.11.Állítás. *Ha egy véges $(G, \circ, 1)$ csoportban a $H \leq G$ részcsoportra $\frac{|G|}{|H|} = 2$, akkor H normális részcsoportja G-nek: $H \lhd G$.*

Bizonyítás. Legyen $x_\gamma \in G, \gamma \in \Gamma$ a H részcsoportra nézve baloldali reprezentánsoknak egy teljes irredundáns rendszere, ekkor a 14.8.Állítás szerint $|\Gamma| = \frac{|G|}{|H|}$. Tehát a fenti rendszer két elemből áll, amelyeket jelölhetünk x_1-el és x_2-vel. Most $x_1H \cup x_2H = G$ és $x_1H \cap x_2H = \varnothing$, továbbá tételezzük fel, hogy $1 \in x_1H$ (a másik lehetséges eset $1 \in x_2H$ nem igényel külön vizsgálatot). A 14.3.Állítás 8.része alapján $x_1H = H$, továbbá egy $g \in G$ elemre $g \notin H$ esetén (ekkor $g \in x_2H$) $gH = x_2H$ és a 14.3.Állítás 9.része alapján még $H \cap Hg = \varnothing$ is teljesül. Az utóbbi egyenlőségből és abból, hogy $H \cup x_2H = G$ a $Hg \subseteq x_2H = gH$ tartalmazást kapjuk. Tehát $g \in G \setminus H$ esetén $g^{-1}Hg \subseteq g^{-1}(gH) = H$, amennyiben $g \in H$, akkor $g^{-1}Hg \subseteq H$ nyilvánvalóan teljesül.

□□□

14.I. Definíció. Legyen $H \lhd G$ a $(G, \circ, 1_G)$ csoport normális részcsoportja, értelmezzük a $xH = Hx$, $x \in G$ alakú mellékosztályok

$$G/H = \{xH \mid x \in G\}$$

halmazán a következő kétváltozós műveletet: $x, y \in G$ esetén legyen

$$(xH) * (yH) = xyH.$$

A 14.3.Állítás 16.részéből következik, hogy ha az $u, v \in G$ elemekre $uH = xH$ és $vH = yH$, akkor $uvH = xyH$. Tehát a $*$ művelet megadása a mellékosztályok G/H halmazán korekt, azaz nem függ a reprezentánsok választásától. Könnyen igazolható az is, hogy az előbbi kétváltozós művelettel $(G/H, *, H)$ egy csoport, amelyet a G csoport H normális részcsoport szerinti **faktor csoportjának** nevezünk. A $H = 1_GH \in G/H$ mellékosztály egységelem, amelyre az $1_{G/H}$, vagy az egyszerűbb 1 jelölést alkalmazzuk. Nyilvánvaló, hogy $(xH)^{-1} = x^{-1}H$. Ha G véges, akkor reprezentánsoknak egy tetszőleges $x_\gamma \in G, \gamma \in \Gamma$ teljes irredundáns rendszerét választva

$$|G/H| = |\{xH \mid x \in G\}| = |\{x_\gamma H \mid \gamma \in \Gamma\}| = |\Gamma| = \frac{|G|}{|H|}$$

adódik. ♡

14.12.Állítás. *Legyen $H \lhd G$ a $(G, \circ, 1)$ csoport egy normális részcsoportja.*

1. *Egy $N \leq G$ részcsoportra az*

$$N/H = \{xH \mid x \in N\} \subseteq G/H$$

halmaz részcsoportot alkot a G/H faktor csoportban: $N/H \leq G/H$. Ha $N \lhd G$ normális, akkor $N/H \lhd G/H$.

Amennyiben $H \subseteq N$, akkor a $H \neq N \neq G$ esetben N/H valódi részcsoportja G/H-nak: $\{1_{G/H}\} \neq N/H \neq G/H$.

2. *Ha $\mathcal{N} \leq G/H$ egy részcsoport, akkor az*

$$\overline{\mathcal{N}} = \{x \mid x \in G \text{ és } xH \in \mathcal{N}\} \subseteq G$$

részhalmaz egy H-t tartalmazó részcsoport a G csoportban: $H \subseteq \overline{\mathcal{N}} \leq G$ (így $H \lhd \overline{\mathcal{N}}$ is teljesül). Az $\{1_{G/H}\} \neq \mathcal{N} \neq G/H$ esetben: $H \neq \overline{\mathcal{N}} \neq G$. Amennyiben $\mathcal{N} \lhd G/H$ normális, akkor $\overline{\mathcal{N}} \lhd G$.

3. *Ha az $N \leq G$ és $\mathcal{N} \leq G/H$ részcsoportokra $H \subseteq N$, akkor*

$$\overline{N/H} = N \text{ és } \overline{\mathcal{N}}/H = \mathcal{N}.$$

Bizonyítás.

1. Az $x, y \in N$ elemekkel felírt xH és yH mellékosztályokat szorozva a G/H faktor csoportban

$$(xH) * (yH) = xyH$$

adódik, ahol $xy \in N$ miatt $xyH \in N/H$. Az xH mellékosztály inverze a G/H faktor csoportban

$$(xH)^{-1} = x^{-1}H,$$

ahol $x^{-1} \in N$ miatt $x^{-1}H \in N/H$. Tehát $N/H \leq G/H$ részcsoport.

Ha $N \lhd G$, akkor G/H-nak tetszőleges uH elemére (itt $u \in G$)

$$(uH)^{-1} * (xH) * (uH) = (u^{-1}H) * (xH) * (uH) = u^{-1}xuH \in N/H,$$

mert $u^{-1}xu \in N$. Tehát $N/H \lhd G/H$.

Ha $N \neq H$ és $H \subseteq N$, akkor van olyan $z \in N$, amelyre $z \notin H$, azaz amelyre $zH \neq H$. Így $zH \in N/H$ miatt $N/H \neq \{1_{G/H}\}$.

Ha $N \neq G$ és $H \subseteq N$, akkor létezik olyan $w \in G$, amelyre $w \notin N$. Ekkor $wH \notin N/H$, hiszen $wH = xH$ teljesülése valamilyen $x \in N$ elemre a 14.3.Állítás 8.részének figyelembe vételével előbb az $x^{-1}w \in H \subseteq N$ tartalmazáshoz, majd a

$$w = x(x^{-1}w) \in N$$

ellentmondáshoz vezetne. Tehát $N/H \neq G/H$.

2. Az $x, y \in \overline{\mathcal{N}}$ elemekre $xH \in \mathcal{N}$ és $yH \in \mathcal{N}$, ahonnan $\mathcal{N} \leq G/H$ miatt

$$xyH = (xH) * (yH) \in \mathcal{N} \text{ és } x^{-1}H = (xH)^{-1} \in \mathcal{N}$$

adódik. Tehát $xy \in \overline{\mathcal{N}}$ és $x^{-1} \in \overline{\mathcal{N}}$, ami azt jelenti, hogy $\overline{\mathcal{N}} \leq G$ részcsoport. Mivel egy $h \in H$ elemre $hH = H = 1_{G/H} \in \mathcal{N}$, ezért $H \subseteq \overline{\mathcal{N}}$.

Ha $\mathcal{N} \neq \{1_{G/H}\}$, akkor van olyan $z \in G$, amelyre $H \neq zH \in \mathcal{N}$. Most $z \in \overline{\mathcal{N}}$ és $z \notin H$, azaz $\overline{\mathcal{N}} \neq H$.

Ha $\mathcal{N} \neq G/H$, akkor létezik olyan $w \in G$, amelyre $wH \notin \mathcal{N}$. Ekkor $w \notin \overline{\mathcal{N}}$, ahonnan $\overline{\mathcal{N}} \neq G$ adódik.

Ha $\mathcal{N} \lhd G/H$, akkor tetszőleges $u \in G$ elemre

$$u^{-1}xuH = (u^{-1}H) * (xH) * (uH) = (uH)^{-1} * (xH) * (uH) \in \mathcal{N},$$

ahonnan $u^{-1}xu \in \overline{\mathcal{N}}$ következik. Tehát $\overline{\mathcal{N}} \lhd G$.

3. Egy $x \in G$ elemre $x \in \overline{N/H}$ pontosan akkor teljesül, ha $xH \in N/H$, ami azzal ekvivalens, hogy $xH = gH$ valamilyen $g \in N$ elemmel. A 14.3.Állítás 8.része szerint az $xH = gH$ egyenlőségből $g^{-1}x \in H$ következik. Mivel $x = g(g^{-1}x)$, ezért $H \subseteq N$ miatt ebben az esetben $x \in N$ teljesül. Ha viszont $x \in N$, akkor $xH \in N/H$ nyilvánvalóan igaz. Tehát $\overline{N/H} = N$.

   Egy $x \in G$ elemre $xH \in \overline{\mathcal{N}}/H$ pontosan akkor teljesül, ha $xH = gH$ valamilyen $g \in \overline{\mathcal{N}}$ elemmel. Mivel $g \in \overline{\mathcal{N}}$ azzal ekvivalens, hogy $gH \in \mathcal{N}$, ezért $\overline{\mathcal{N}}/H \subseteq \mathcal{N}$. Ha viszont $xH \in \mathcal{N}$, akkor $x \in \overline{\mathcal{N}}$, ahonnan $xH \in \overline{\mathcal{N}}/H$ adódik. Tehát a fordított $\mathcal{N} \subseteq \overline{\mathcal{N}}/H$ tartalmazás is teljesül.

□□□

14.13.Állítás. *Ha egy $(G, \circ, 1)$ csoportnak a centrális elemek által alkotott $\xi(G) \lhd G$ normális részcsoport szerinti $G/\xi(G)$ faktor csoportja ciklikus, akkor G kommutatív.*

Bizonyítás. Legyen $z \in G$ olyan elem, hogy a ciklikus $G/\xi(G)$ csoportra

$$G/\xi(G) = \langle z\xi(G) \rangle ,$$

ami azt jelenti, hogy a $(z\xi(G))^k = z^k\xi(G)$, $k \in \mathbb{Z}$ hatványok a $G/\xi(G)$ faktor csoport összes elemét megadják. Tehát a mellékosztályoknak a $z^k\xi(G)$, $k \in \mathbb{Z}$ rendszere teljes, azaz a 14.H.Definícióban foglaltak szerint

$$G = \bigcup_{k\in\mathbb{Z}} z^k\xi(G).$$

Az eddigiek alapján a tetszőlegesen megválasztott $x, y \in G$ elemeket

$$x = z^n c_1 \text{ és } y = z^m c_2$$

alakban írhatjuk bizonyos $n, m \in \mathbb{Z}$ kitevőkkel és $c_1, c_2 \in \xi(G)$ centrális elemekkel. Így a $z^n z^m = z^{n+m} = z^m z^n$ egyenlőséget (lásd a 14.3.Állítás 2.részét) és a centrális elemek tulajdonságát kihasználva kapjuk, hogy

$$xy = z^n c_1 (z^m c_2) = z^n (z^m c_2) c_1 = z^{n+m} c_2 c_1 = z^m z^n c_2 c_1 = z^m c_2 z^n c_1 = yx.$$

□□□

14.J. Definíció. Azt mondjuk, hogy egy $(G, \circ, 1)$ csoport $H_i \subseteq G$, $0 \le i \le n$ részhalmazai a G-nek egy n **hosszúságú szubnormál láncát** alkotják, ha

$$\{1\} = H_0 \lhd H_1 \lhd ... \lhd H_i \lhd H_{i+1} \lhd ... \lhd H_{n-1} \lhd H_n = G.$$

A fenti szubnormál lánc **ismétlődés nélküli**, ha minden $0 \le i \le n-1$ egészre $H_i \neq H_{i+1}$. A 14.3.Állításbeli 7.rész alapján $H_i \le G$ teljesül minden $0 \le i \le n$ indexre, de $H_i \lhd G$ általában nem lesz igaz. A H_{i+1}/H_i, $0 \le i \le n-1$ faktor csoportokat nevezzük a **szubnormál lánc faktorainak**. A $(G, \circ, 1)$ csoportot **feloldhatónak** nevezzük, ha létezik olyan (véges hosszúságú) szubnormál lánca, amelynek minden faktora kommutatív. Ha G kommutatív, akkor $\{1\} = H_0 \lhd H_1 = G$ olyan $n = 1$ hosszúságú szubnormál lánc, amelynek az egyetlen $G/\{1\}$ faktora nyilvánvalóan kommutatív. Tehát minden kommutatív csoport feloldható.♡

14.14.Állítás. *Legyen $N \le G$ részcsoportja a $(G, \circ, 1)$ csoportnak.*

1. *Ha G feloldható, akkor az N csoport is feloldható.*

2. *Amennyiben $N \lhd G$ normális részcsoport és G feloldható, akkor a G/N faktor csoport is feloldható.*

3. *Amennyiben $N \lhd G$ normális részcsoport, továbbá az N és a G/N csoportok mindegyike feloldható, akkor G is feloldható.*

Bizonyítás.

1. Legyen
$$\{1\} = H_0 \lhd H_1 \lhd ... \lhd H_i \lhd H_{i+1} \lhd ... \lhd H_{n-1} \lhd H_n = G.$$
a G csoportnak a kommutatív H_{i+1}/H_i, $0 \leq i \leq n-1$ faktorokkal rendelkező szubnormál lánca. Ekkor $N \cap H_i \lhd N \cap H_{i+1}$ nyilvánvalóan teljesül minden $0 \leq i \leq n-1$ indexre és
$$\{1\} = N \cap H_0 \lhd N \cap H_1 \lhd ... \lhd N \cap H_i \lhd N \cap H_{i+1} \lhd ... \lhd N \cap H_{n-1} \lhd N \cap H_n = N \cap G = N$$
olyan szubnormál lánca lesz az N csoportnak, amelynek az $(N \cap H_{i+1})/(N \cap H_i)$, $0 \leq i \leq n-1$ faktorai szintén kommutatívak: $u, v \in N \cap H_{i+1}$ esetén
$$u(N \cap H_i) * v(N \cap H_i) = uv(N \cap H_i) = vu(N \cap H_i) = v(N \cap H_i) * u(N \cap H_i).$$
Az $uv(N \cap H_i) = vu(N \cap H_i)$ egyenlőség az $(uv)^{-1}vu \in N$ tartalmazásnak és a kommutatív H_{i+1}/H_i csoportban teljesülő
$$uvH_i = (uH_i) * (vH_i) = (vH_i) * (uH_i) = vuH_i$$
egyenlőségből a 14.3.Állítás 8.része szerint kapható $(uv)^{-1}vu \in H_i$ tartalmazásnak a következménye.

2. Legyen
$$\{1\} = H_0 \lhd H_1 \lhd ... \lhd H_i \lhd H_{i+1} \lhd ... \lhd H_{n-1} \lhd H_n = G.$$
a G csoportnak a kommutatív H_{i+1}/H_i, $0 \leq i \leq n-1$ faktorokkal rendelkező szubnormál lánca. Ekkor $H_i/N \lhd H_{i+1}/N$ nyilvánvalóan teljesül minden $0 \leq i \leq n-1$ indexre és
$$\{1_{G/N}\} = H_0/N \lhd H_1/N \lhd ... \lhd H_i/N \lhd H_{i+1}/N \lhd ... \lhd H_{n-1}/N \lhd H_n/N = G/N$$
olyan szubnormál lánca lesz a G/N csoportnak, amelynek az $(H_{i+1}/N)/(H_i/N)$, $0 \leq i \leq n-1$ faktorai szintén kommutatívak: $u, v \in H_{i+1}$ esetén
$$uN(H_i/N) * vN(H_i/N) = uvN(H_i/N) = vuN(H_i/N) = vN(H_i/N) * uN(H_i/N).$$
Az $uvN(H_i/N) = vuN(H_i/N)$ egyenlőség az 1.rész bizonyításában is felhasznált $(uv)^{-1}vu \in H_i$ tartalmazásból kapható: $(uvN)^{-1} * (vuN) = (uv)^{-1}vuN \in H_i/N$.

3. Legyen
$$\{1\} = M_0 \lhd M_1 \lhd ... \lhd M_i \lhd M_{i+1} \lhd ... \lhd M_{k-1} \lhd M_k = N.$$
az N csoportnak a kommutatív M_{i+1}/M_i, $0 \leq i \leq k-1$ faktorokkal rendelkező szubnormál lánca és
$$\{1_{G/N}\} = \mathcal{N}_0 \lhd \mathcal{N}_1 \lhd ... \lhd \mathcal{N}_j \lhd \mathcal{N}_{j+1} \lhd ... \lhd \mathcal{N}_{l-1} \lhd \mathcal{N}_l = G/N.$$

a G/N csoportnak a kommutatív $\mathcal{N}_{j+1}/\mathcal{N}_j$, $0 \leq j \leq l-1$ faktorokkal rendelkező szubnormál lánca. Tekintsük a 14.12.Állítás 2.részében értelmezett

$$\overline{\mathcal{N}_j} = \{x \mid x \in G \text{ és } xN \in \mathcal{N}_j\} \leq G,\ 0 \leq j \leq l$$

részcsoportokat, ekkor

$$N = \overline{\mathcal{N}_0} \lhd \overline{\mathcal{N}_1} \lhd ... \lhd \overline{\mathcal{N}_j} \lhd \overline{\mathcal{N}_{j+1}} \lhd ... \lhd \overline{\mathcal{N}_{l-1}} \lhd \overline{\mathcal{N}_l} = G.$$

Valóban, a $g \in \overline{\mathcal{N}_{j+1}}$ és $x \in \overline{\mathcal{N}_j}$ elemekre $gN \in \mathcal{N}_{j+1}$ és $xN \in \mathcal{N}_j$, ezért a $\mathcal{N}_j \lhd \mathcal{N}_{j+1}$ viszonyra való tekintettel

$$g^{-1}xgN = (gN)^{-1} * (xN) * (gN) \in \mathcal{N}_j,$$

ahonnan $g^{-1}xg \in \overline{\mathcal{N}_j}$ adódik.

Az $\overline{\mathcal{N}_{j+1}}/\overline{\mathcal{N}_j}$, $0 \leq j \leq l-1$ faktor csoportok kommutatívak: $u, v \in \overline{\mathcal{N}_{j+1}}$ esetén

$$(u\overline{\mathcal{N}_j}) * (v\overline{\mathcal{N}_j}) = uv\overline{\mathcal{N}_j} = vu\overline{\mathcal{N}_j} = (v\overline{\mathcal{N}_j}) * (u\overline{\mathcal{N}_j}).$$

Az $uv\overline{\mathcal{N}_j} = vu\overline{\mathcal{N}_j}$ egyenlőség annak a következménye, hogy a kommutatív $\mathcal{N}_{j+1}/\mathcal{N}_j$ csoport $(uN)\mathcal{N}_j$ és $(vN)\mathcal{N}_j$ elemeire

$$(uvN)\mathcal{N}_j = (uN)\mathcal{N}_j * (vN)\mathcal{N}_j = (vN)\mathcal{N}_j * (uN)\mathcal{N}_j = (vuN)\mathcal{N}_j$$

teljesül, ami a 14.3.Állítás 8.része szerint előbb az

$$(uv)^{-1}(vu)N = (uvN)^{-1} * (vuN) \in \mathcal{N}_j$$

majd innen az $(uv)^{-1}(vu) \in \overline{\mathcal{N}_j}$ tartalmazáshoz vezet.

Végeredményben a G csoportnak a kommutatív faktorokkal rendelkező

$$\{1\} = M_0 \lhd ... \lhd M_i \lhd ... \lhd M_k = N = \overline{\mathcal{N}_0} \lhd ... \lhd \overline{\mathcal{N}_j} \lhd ... \lhd \overline{\mathcal{N}_l} = G$$

szubnormál láncához jutottunk, ami G-nek a feloldhatóságát igazolja.

□□□

14.15.Tétel. *Egy véges feloldható $(G, \circ, 1)$ csoportnak létezik olyan*

$$\{1\} = H_0 \lhd H_1 \lhd ... \lhd H_i \lhd H_{i+1} \lhd ... \lhd H_{n-1} \lhd H_n = G.$$

szubnormál lánca is, amelynek minden H_{i+1}/H_i, $0 \leq i \leq n-1$ faktora prím elemszámú ciklikus csoport.

Bizonyítás. Nyilvánvaló, hogy ha G-nek létezik kommutatív faktorokkal rendelkező szubnormál lánca, akkor az ilyen tulajdonságú szubnormál láncok között van ismétlődés nélküli is (az egymás után következő ismétlődő részcsoportokat egyszerűen el kell hagyni). Legyen

$$\{1\} = H_0 \lhd H_1 \lhd ... \lhd H_i \lhd H_{i+1} \lhd ... \lhd H_{n-1} \lhd H_n = G.$$

a G feloldható csoport kommutatív faktorokkal rendelkező ismétlődés nélküli szubnormál láncai közül a leghosszabbak egyike (a G végessége miatt ilyen található). Ha $\mathcal{N} \leq H_{i+1}/H_i$ egy valódi részcsoport (azaz $\{1_{H_{i+1}/H_i}\} \neq \mathcal{N} \neq H_{i+1}/H_i$), akkor a 14.12.Állítás 2.része szerint

$$H_i \lhd \overline{\mathcal{N}} = \{x \mid x \in H_{i+1} \text{ és } xH_i \in \mathcal{N}\} \leq H_{i+1}$$

és $H_i \neq \overline{\mathcal{N}} \neq H_{i+1}$. Mivel H_{i+1}/H_i kommutatív, ezért minden részcsoportja (így $\mathcal{N}$ is) normális, ezért a 14.12.Állítás 2.részét újra alkalmazva kapjuk, hogy $\overline{\mathcal{N}} \lhd H_{i+1}$. Az eddigiek szerint G-nek az alábbi

$$\{1\} = H_0 \lhd H_1 \lhd ... \lhd H_i \lhd \overline{\mathcal{N}} \lhd H_{i+1} \lhd ... \lhd H_{n-1} \lhd H_n = G$$

szubnormál lánca ismétlődés nélküli. A fenti szubnormál lánc szintén kommutatív faktorokkal rendelkezik. Valóban, $\overline{\mathcal{N}}/H_i \leq H_{i+1}/H_i$ miatt az $\overline{\mathcal{N}}/H_i$ faktor csoport kommutatív. A $H_{i+1}/\overline{\mathcal{N}}$ faktor is kommutatív, hiszen az $x\overline{\mathcal{N}}$ és $y\overline{\mathcal{N}}$ elemekre (itt $x, y \in H_{i+1}$)

$$(x\overline{\mathcal{N}}) * (y\overline{\mathcal{N}}) = xy\overline{\mathcal{N}} = yx\overline{\mathcal{N}} = (y\overline{\mathcal{N}}) * (x\overline{\mathcal{N}}),$$

ahol az $xy\overline{\mathcal{N}} = yx\overline{\mathcal{N}}$ egyenlőség annak a következménye, hogy a kommutatív H_{i+1}/H_i faktor csoportban

$$xyH_i = (xH_i) * (yH_i) = (yH_i) * (xH_i) = yxH_i$$

teljesül, ami a 14.3.Állítás 8.része alapján az $(xy)^{-1}(yx) \in H_i \subseteq \overline{\mathcal{N}}$ tartalmazást eredményezi (megjegyzendő, hogy $H_{i+1}/\overline{\mathcal{N}}$ a H_{i+1}/H_i csoport ún. homomorf képe).
A leghosszabb kommutatív faktorokkal rendelkező szubnormál lánctól egy hasonló tulajdonságú, de hosszabb szubnormál láncot kaptunk, ami ellentmondás. Tehát a H_{i+1}/H_i faktor csoportnak nem létezik valódi részcsoportja, ez a a 14.10.Következmény szerint azt jelenti, hogy H_{i+1}/H_i prím elemszámú ciklikus csoport.

□□□

14.K. Definíció. Azt mondjuk, hogy a (egész G_1-en értelmezett és értékeit a G_2-ben felvevő) $\lambda : G_1 \longrightarrow G_2$ függvény a $(G_1, \circ, 1)$ csoportból a $(G_2, \circ, 1)$ csoportba irányuló **(csoport) homomorfizmus**, ha $\lambda(1) = 1$ és $\lambda(xy) = \lambda(x)\lambda(y)$ teljesül tetszőleges $x, y \in G_1$ elemekre.
A λ **homomorfizmus magján** G_1-nek a

$$\ker(\lambda) = \{x \in G_1 \mid \lambda(x) = 1\} \subseteq G_1$$

részhalmazát értjük. Az injektív csoport homomorfizmust (csoport) **beágyazásnak** nevezzük. Amennyiben a λ homomorfizmus bijektív (injektív és szürjektív) függvény, akkor (csoport) **izomorfizmusnak** nevezzük. A $(G_1, \circ, 1)$ és $(G_2, \circ, 1)$ **csoportokat izomorfoknak** nevezzük és a $G_1 \cong G_2$ jelölést alkalmazzuk, ha létezik (legalább egy) a G_1-ből G_2-be irányuló csoport izomorfizmus.♡

14.16.Állítás. *Tekintsük a $(G, \circ, 1)$, $(G_1, \circ, 1)$, $(G_2, \circ, 1)$ és $(G_3, \circ, 1)$ csoportokat, az $M \lhd G$ normális részcsoportot és a G/M faktor csoportot, valamint a $\lambda : G_1 \longrightarrow G_2$ és $\mu : G_2 \longrightarrow G_3$ csoport homomorfizmusokat.*

1. *Egy $x \in G_1$ elemre a $\lambda(x) \in G_2$ képelem inverzére a $(G_2, \circ, 1)$ csoportban $(\lambda(x))^{-1} = \lambda(x^{-1})$ teljesül.*
2. *Egy $H \leq G_1$ részcsoport λ szerinti képhalmaza részcsoport G_2-ben: $\lambda(H) \leq G_2$.*
3. *Ha λ szürjektív, akkor egy $N \lhd G_1$ normális részcsoport λ szerinti képhalmaza normális részcsoport G_2-ben: $\lambda(N) \lhd G_2$.*
4. *Egy $U \leq G_2$ részcsoport λ szerinti ősképe részcsoport G_1-ben: $\lambda^{-1}(U) \leq G_1$.*
5. *Egy $V \lhd G_2$ normális részcsoport λ szerinti ősképe normális részcsoport G_1-ben: $\lambda^{-1}(V) \lhd G_1$.*

6. *A λ homomorfizmus magja normális részcsoport G_1-ben:* $\ker(\lambda) \lhd G_1$.

7. *A λ homomorfizmus pontosan akkor injektív, ha* $\ker(\lambda) = \{1\}$.

8. *A $\mu \circ \lambda : G_1 \longrightarrow G_3$ összetett függvény is homomorfizmus.*

9. *Ha λ izomorfizmus, akkor a $\lambda^{-1} : G_2 \longrightarrow G_1$ inverz függvény is izomorfizmus.*

10. *Egy $z \in G$ elemen a $\varkappa(z) = zM$ módon értelmezett $\varkappa : G \longrightarrow G/M$ leképezés olyan szürjektív homomorfizmus, amelyre* $\ker(\varkappa) = M$.

11. *Egy $x \in G_1$ elemet használva a $G_1/\ker(\lambda)$ faktor csoport $x\ker(\lambda)$ alakú elemén*

$$\overline{\lambda}(x\ker(\lambda)) = \lambda(x)$$

módon értelmezhetünk egy $\overline{\lambda} : G_1/\ker(\lambda) \longrightarrow G_2$ függvényt, amely injektív homomorfizmus, amennyiben λ szürjektív, akkor $\overline{\lambda}$ izomorfizmus (ez utóbbi esetben $G_1/\ker(\lambda) \cong G_2$ és ezt nevezik a ***homomorfizmus tételnek****).*

12. *Egy $z \in G$ elemre az $\alpha_g(z) = g^{-1}zg$ módon értelmezett $\alpha_g : G \longrightarrow G$ leképezés izomorfizmus.*

Bizonyítás.

1. Mivel $\lambda(x^{-1})\lambda(x) = \lambda(x^{-1}x) = \lambda(1) = 1$ és $\lambda(x)\lambda(x^{-1}) = \lambda(xx^{-1}) = \lambda(1) = 1$, ezért az inverz egyértelműsége miatt $(\lambda(x))^{-1} = \lambda(x^{-1})$.

2. $\lambda(H)$-nak a $\lambda(h_1)$ és $\lambda(h_2)$ elemeire (itt $h_1, h_2 \in H$) $\lambda(h_1)\lambda(h_2) = \lambda(h_1h_2) \in \lambda(H)$, mert $h_1h_2 \in H$. Az 1.részben foglaltak szerint $\lambda(H)$-nak egy további $\lambda(h)$ elemére ($h \in H$) $(\lambda(h))^{-1} = \lambda(h^{-1}) \in \lambda(H)$, mert $h^{-1} \in H$. Tehát $\lambda(H) \leq G_2$ részcsoport.

3. A szürjektívitás miatt tetszőleges $g \in G_2$ elem $g = \lambda(u)$ alakban írható valamilyen $u \in G_1$ elemmel. Tehát $\lambda(N)$-nek egy $\lambda(h)$ elemére (itt $h \in N$)

$$g^{-1}\lambda(h)g = (\lambda(u))^{-1}\lambda(h)\lambda(u) = \lambda(u^{-1})\lambda(h)\lambda(u) = \lambda(u^{-1}hu) \in \lambda(H),$$

hiszen $N \lhd G_1$ miatt $u^{-1}hu \in N$.

4. Ha $x, y \in \lambda^{-1}(U)$, akkor $\lambda(x), \lambda(y) \in U$, ahonnan $U \leq G_2$ miatt $\lambda(xy) = \lambda(x)\lambda(y) \in U$ és $\lambda(x^{-1}) = (\lambda(x))^{-1} \in U$ adódik. Tehát $xy \in \lambda^{-1}(U)$ és $x^{-1} \in \lambda^{-1}(U)$, ami azt jelenti, hogy $\lambda^{-1}(U) \leq G_1$ részcsoport.

5. Tetszőleges $u \in G_1$ és $x \in \lambda^{-1}(V)$ elemekre

$$\lambda(u^{-1}xu) = \lambda(u^{-1})\lambda(x)\lambda(u) = (\lambda(u))^{-1}\lambda(x)\lambda(u) \in V,$$

hiszen $\lambda(x) \in V$ és $V \lhd G_2$. Tehát $u^{-1}xu \in \lambda^{-1}(V)$, azaz $\lambda^{-1}(V) \lhd G_1$.

6. Ha $x, y \in \ker(\lambda)$ és $u \in G_1$, akkor $\lambda(x) = \lambda(y) = 1$, ahonnan az alábbi

$$\lambda(xy) = \lambda(x)\lambda(y) = 1 \cdot 1 = 1 \ , \ \lambda(x^{-1}) = (\lambda(x))^{-1} = 1^{-1} = 1 \text{ és}$$

$$\lambda(u^{-1}xu) = \lambda(u^{-1})\lambda(x)\lambda(u) = (\lambda(u))^{-1} \cdot 1 \cdot \lambda(u) = (\lambda(u))^{-1}\lambda(u) = 1$$

egyenlőségek adódnak. Tehát $xy \in \ker(\lambda)$, $x^{-1} \in \ker(\lambda)$ és $u^{-1}xu \in \ker(\lambda)$,
azaz $\ker(\lambda) \lhd G_1$.

7. Az $u, v \in G_1$ elemekre

$$\lambda(u) = \lambda(v) \Longleftrightarrow \lambda(u)(\lambda(v))^{-1} = 1 \Longleftrightarrow \lambda(u)\lambda(v^{-1}) = 1 \Longleftrightarrow \lambda(uv^{-1}) = 1 \Longleftrightarrow uv^{-1} \in \ker(\lambda).$$

Tehát $\ker(\lambda) = \{1\}$ esetén $\lambda(u) = \lambda(v) \Longrightarrow uv^{-1} = 1 \Longrightarrow u = v$, ami azt jelenti, hogy λ injektív.

Ha viszont λ injektív, akkor $x \in \ker(\lambda)$ esetén $\lambda(x) = 1 = \lambda(1)$, ahonnan $x = 1$, azaz $\ker(\lambda) = \{1\}$ következik.

8. Az $1, x, y \in G_1$ elemekre $(\mu \circ \lambda)(1) = \mu(\lambda(1)) = \mu(1) = 1$ és

$$(\mu \circ \lambda)(xy) = \mu(\lambda(xy)) = \mu(\lambda(x)\lambda(y)) = \mu(\lambda(x))\mu(\lambda(y)) = (\mu \circ \lambda)(x)(\mu \circ \lambda)(y).$$

Tehát a $\mu \circ \lambda : G_1 \longrightarrow G_3$ összetett függvény homomorfizmus.

9. Azt kell igazolni, hogy $\lambda^{-1} : G_2 \longrightarrow G_1$ homomorfizmus. Az $1, g', g'' \in G_2$ elemekre az inverz függvény $\lambda \circ \lambda^{-1} = \mathrm{id}_{G_2}$ tulajdonsága miatt

$\lambda(\lambda^{-1}(1)) = 1 = \lambda(1)$ és $\lambda(\lambda^{-1}(g'g'')) = g'g'' = \lambda(\lambda^{-1}(g'))\lambda(\lambda^{-1}(g'')) = \lambda(\lambda^{-1}(g')\lambda^{-1}(g''))$

teljesül, ahonnan a λ injektívitását felhasználva kapjuk a kívánt

$$\lambda^{-1}(1) = 1 \text{ és } \lambda^{-1}(g'g'')) = \lambda^{-1}(g')\lambda^{-1}(g'')$$

egyenlőségeket.

10. Az $1, z_1, z_2 \in G$ elemekre

$$\varkappa(1) = 1M = M = 1_{G/M} \text{ és } \varkappa(z_1z_2) = z_1z_2M = (z_1M) * (z_2M) = \varkappa(z_1)\varkappa(z_2),$$

ami azt igazolja, hogy $\varkappa : G \longrightarrow G/M$ homomorfizmus. A $\varkappa$ szürjektívitása nyilvánvaló.

Ha egy $z \in G$ elemre $\varkappa(z) = 1$, akkor $zM = 1_{G/M} = M$. A14.3.Állítás 8.része szerint ez a $z \in M$ tartalmazással ekvivalens, azaz $\ker(\varkappa) = M$.

11. Ha az $x, y \in G_1$ elemekre $x\ker(\lambda) = y\ker(\lambda)$, akkor $x^{-1}y \in \ker(\lambda)$ (lásd a 14.3Állítás 8.részét). Tehát $\lambda(x^{-1}y) = 1$, ahonnan előbb

$$(\lambda(x))^{-1}\lambda(y) = \lambda(x^{-1})\lambda(y) = \lambda(x^{-1}y) = 1,$$

majd $\lambda(x) = \lambda(y)$ adódik. Ez azt jelenti, hogy $\overline{\lambda}$ megadása az $x\ker(\lambda)$ mellékosztályon megfelelő. Nyilvánvaló, hogy $\overline{\lambda}$ homomorfizmus.

Ha $\overline{\lambda}(x\ker(\lambda)) = 1$, akkor $\lambda(x) = 1$, azaz $x \in \ker(\lambda)$, illetve $x\ker(\lambda) = \ker(\lambda) = 1_{G_1/\ker(\lambda)}$ teljesül. Tehát $\ker(\overline{\lambda}) = \{1_{G_1/\ker(\lambda)}\}$, ami a már igazolt 7.részre való tekintettel azt eredményezi, hogy $\overline{\lambda} : G_1/\ker(\lambda) \longrightarrow G_2$ injektív.

A λ szürjektívitásából azonnal következik a $\overline{\lambda}$ szürjektívitása.

12. Az $1, z_1, z_2 \in G$ elemekre $\alpha_g(1) = g^{-1}1g = g^{-1}g = 1$ és

$$\alpha_g(z_1z_2) = g^{-1}z_1z_2g = g^{-1}z_1gg^{-1}z_2g = \alpha_g(z_1)\alpha_g(z_2).$$

Tehát $\alpha_g : G \longrightarrow G$ valóban homomorfizmus. Könnyen ellenőrízhető, hogy α_g-nek az inverz függvénye az $\alpha_{g^{-1}} : G \longrightarrow G$ függvény lesz. Valóban, egy $z \in G$ elemre

$$(\alpha_{g^{-1}} \circ \alpha_g)(z) = \alpha_{g^{-1}}(\alpha_g(z)) = (g^{-1})^{-1}(g^{-1}zg)g^{-1} = gg^{-1}zgg^{-1} = z$$

és teljesen hasonlóan $(\alpha_g \circ \alpha_{g^{-1}})(z) = z$ adódik.

□□□

14.17.Tétel. *Egy* $(G, \circ, 1)$ *csoport* $H \leq G$ *részcsoportjára és* $N \lhd G$ *normális részcsoportjára* $N \lhd NH = HN$ *és* $N \cap H \lhd H$*, továbbá az* NH/N *és a* $H/N \cap H$ *faktor csoportok izomorfak:* $NH/N \cong H/N \cap H$ *(ezt nevezik az* ***első izomorfizmus tételnek****).*

Bizonyítás. A 14.3.Állítás 18.része szerint $N \lhd NH = HN$ és $N \cap H \lhd H$. Értelmezzük a $\lambda : H/N \cap H \longrightarrow NH/N$ leképezést a $H/N \cap H$ faktor csoport egy $x(N \cap H)$ elemén (itt $x \in H$) az alábbi módon:

$$\lambda(x(N \cap H)) = xN.$$

Nyilvánvaló, hogy $H \subseteq NH$ miatt $x \in NH$ és amennyiben egy $x' \in H$ elemre $x'(N \cap H) = x(N \cap H)$, akkor $x^{-1}x' \in N \cap H \subseteq N$ miatt $x'N = xN$ az NH/N faktor csoportban (a 14.3.Állítás 8.részét használtuk). Tehát λ megadása az $x(N \cap H)$ mellékosztályon megfelelő. A λ olyan homomorfizmus (ez azonnal látható), amelynek a magjára

$$\ker(\lambda) = \{1_{H/N \cap H}\},$$

hiszen $x \in H$ esetén $xN = 1_{NH/N} = N$ pontosan akkor teljesül, ha $x \in N \cap H$, azaz ha $x(N \cap H) = N \cap H = 1_{H/N \cap H}$. Tehát a 14.16.Állítás 7.részére való tekintettel λ injektív. A λ szürjektív, mert az NH/N faktor csoport bármely eleme yxN alakban írható alkalmas $y \in N$ és $x \in H$ elemekkel és ilyenkor

$$\lambda(x(N \cap H)) = xN = yxN.$$

Valóban, $y \in N$ és $N \lhd G$ miatt $x^{-1}yx \in N$, ami a 14.3.Állítás 8.része szerint az $xN = yxN$ egyenlőséget eredményezi.

□□□