# BEVEZETÉS A CSOPORTELMÉLETBE

Írta: Kiss Emil

## Bevezetés

Egy idegen bolygó lakói üzenetet küldenek a többi civilizációnak, melyben be akarnak számolni kultúrájuk fejlettségéről. A prímszámokat persze mindenki ismeri, aki az adást fogni tudja, azokat kár elküldeni. Végülis az üzenet így kezdődik:

$$60, 168, 360, 504, 660, 1092, 2448, 2520, 3420, 4080, 5616, 6048, 6072, 7800, 9828, 12180,$$
$$14880, 20160, 20160, 25308, 25920, \ldots$$

Meg tudja-e fejteni ezt az emberiség? A válasz 1980 óta igenlő. Ekkor bizonyították ugyanis be (több mint húszéves munka eredményeként) a híres *klasszifikáció* tételét. Ez az eredmény ugyan egy csoportelméleti tétel, de máris számos alkalmazása van, elsősorban a kombinatorikában, de más területeken is. Az eredmény több matematikus munkája, és a bizonyítás (melynek teljes publikációja most készül) kb. tízezer oldal (telehintve nagyszerű ötletekkel).

A csoportelmélet a XIX. század első felében keletkezett, N. H. Abel és E. Galois munkássága nyomán. A kutatásokat az a probléma inspirálta, hogy meg lehet-e oldani a magasabbfokú egyenleteket gyökképlet segítségével. Kiderült, hogy a legalább ötödfokú polinomok gyökeit általában nem lehet olyan képlettel felírni, melyekben a négy alapműveleten kívül még a gyökvonás is szerepelhet. Ennek bizonyításához *permutációcsoportokat* vizsgáltak, azaz olyan csoportokat, melyeknek elemei permutációk, a művelet pedig ezek kompozíciója.

A XIX. század végén és a XX. század elején kezdődött az absztrakt csoportok szerkezetének vizsgálata. A feladat az, hogy lehetőség szerint minden csoportnak áttekintsük a szerkezetét, olyan struktúratételeket bizonyítsunk, amelyek alapján az alkalmazásokban felmerülő kérdésekre válaszolni lehet. Ez először a véges kommutatív, más néven Abel-csoportokra sikerült. Az ezekre vonatkozó tétel azt mondja ki, hogy minden véges Abel-csoport áttekinthető módon felépíthető nagyon szép szerkezetű (úgynevezett ciklikus) csoportokból.

A nemkommutatív csoportok szerkezete lényegesen bonyolultabb. Itt is reménykedhetünk azonban abban, hogy a csoport összeáll kisebb, ismert szerkezetű építőkövekből. Ezek az építőkövek az úgynevezett *egyszerű csoportok*. A klasszifikáció tétele éppen ezeknek a teljes leírását tartalmazza. Érdemes már most beleolvasni az utolsó fejezetbe, és nézegetni az ott szereplő táblázatokat.

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

A következőkben ki fog derülni a most elmondottak precíz értelme. Ajánlom kiegészítésül a Fuchs: Algebra jegyzetet (melynek II. fejezete foglalkozik csoportokkal), feladatgyűjteményként pedig Czédli-Szendrei-Szendrei: Absztrakt algebrai feladatok című művét.

Hogyan érdemes olvasni ezt a jegyzetet? A matematikában sok olyan könnyű állítás van, aminek a bizonyítását csak akkor lehet megérteni, ha valaki maga végzi el a megfelelő számolást. Tipikusan ilyen például új definíciók egyszerű következményeinek a kiszámolása, továbbá ellenpéldák ellenőrzése. Ezért az alábbiakban „érdemes meggondolni" szöveggel címkézett állításokat valóban számoljuk ki.

Igyekeztem leírni, mit miért csinálunk, melyik definíció, illetve tétel mögött milyen tartalom húzódik meg. Ezeket az elveket előadáson nehéz jegyzetelni, most itt az alkalom, hogy mindenki elgondolkozhasson rajtuk. A későbbi eredmények megértéséhez (és a vizsgakérdések megválaszolásához) éppen az így szerzett szemlélet segít. *A fogalmak mögött meghúzódó filozófiát, az algebrai fogalomalkotási módokat, szemléletet egy tanárnak sokszor fontosabb ismernie, mint magukat a konkrét eredményeket.*

A csoportelmélet az algebra egyik legszebb fejezete. Sajnos a matematika bármely mély ágára igaz, hogy sok erőfeszítésbe kerül, amíg az alapfogalmak megértésén túljutunk, és a szépségek csak ezután következnek. Éppen ezért igyekeztem, hogy az alábbiakban egykét nemtriviális eredmény is helyet kapjon. Remélem, hogy a csoportelmélet megismerése minden olvasónak kellemes élményt nyújt majd.

## I. Amit már mindannyian tudunk

Ebben a fejezetben átismételjük a csoport és az elemrend fogalmát. Egy $G$ halmazt akkor nevezünk csoportnak, ha értelmezve van benne egy kétváltozós (rendszerint szorzással, vagy egymás mellé írással jelölt) művelet a következő tulajdonságokkal:

(1) A művelet *asszociatív*, azaz $(gh)k = g(hk)$ teljesül tetszőleges $g, h, k \in G$ esetén.
(2) A műveletnek van kétoldali *egységeleme*, azaz egy olyan $e$ elem, hogy $eg = ge = g$ minden $g \in G$-re. Az egységelem könnyen láthatóan egyértelműen meghatározott.
(3) Erre az egyértelműen meghatározott egységelemre nézve minden elemnek van kétoldali *inverze*, azaz minden $g \in G$-hez van olyan $h \in G$, hogy $gh = hg = e$.

Nem nehéz belátni, hogy az asszociativitás következményeképpen akármilyen hosszú véges szorzat értéke is független a zárójelezéstől, ezért a zárójeleket elhagyjuk. A műveletet persze nemcsak szorzással jelölhetjük, például számok vagy vektorok összeadásakor a $+$ jelet szokás használni. Ilyenkor az egységelem helyett nullelemet, az inverz helyett ellentettet mondunk. Néha szokás az egységelem/nullelem helyett a neutrális elem kifejezést használni, ami mindenfajta műveletre jó. Hasznos gyakorló feladat annak megmutatása, hogy már egy baloldali egységelem és az erre vett balinverzek létezése magával vonja, hogy csoportot kapunk. Szintén hasznos észrevenni, hogy az inverz elemmel való szorzás segítségével az $ag = bg$ illetve $ga = gb$ egyenlőségek mindegyikéből $a = b$ következik, vagyis minden csoportban érvényes az *egyszerűsítési szabály*.

Ha a csoportművelet jele a szorzás, vagy egymás mellé írás, akkor a $g$ elem inverzét $g^{-1}$ jelöli (míg ellentett esetében a $-g$ jelölés használatos). Vigyázzunk, a szorzásnál számít a tényezők sorrendje! Így például szorzat inverzének kiszámításakor a sorrend megfordul: $(gh)^{-1} = h^{-1}g^{-1}$ bármely $g, h \in G$-re. Ha mégis igaz, hogy $gh = hg$ tetszőleges $g, h \in G$-re, akkor *kommutatív*, vagy *Abel-csoportról* beszélünk.

Az egész, a racionális, a valós, a komplex számok csoportot alkotnak az összeadásra. Ugyanígy tetszőleges $R$ gyűrű (speciálisan test) is. Ezt a csoportot $R$ *additív csoportjának* nevezzük, és $R^+$-szal jelöljük. Hasonlóképpen csoport minden vektortér is az összeadásra.

A számelméletben tanult gyűrűk közül emeljük ki azt, amit akkor használunk, amikor „modulo $n$" számolunk valamilyen $n$ pozitív egészre. Ennek elemei a $0, 1, \ldots, n-1$ számok, az összeadás és a kivonás pedig abban különbözik az egész számokra ismert szokásos műveletektől, hogy az eredménynek még vesszük az $n$-nel való osztási maradékát. A kapott gyűrű jele $\mathbb{Z}_n$. Például a $\mathbb{Z}_7$ gyűrűben az 5 és a 4 elemek összege 2, szorzatuk 6, az 5 ellentettje az összeadásra a 2, inverze a szorzásra a 3. (Számelméleti kurzusokon lényegében ugyanez a gyűrű sokszor olyan formában szerepel, hogy elemei nem számok, hanem maradékosztályok modulo $n$.)

Ha adott egy gyűrű, akkor az elemei a szorzásra általában nem alkotnak csoportot, mert a nullának nem lesz inverze. De például a nem nulla valós számok már csoportot alkotnak a szorzásra. Általában ha $R$ egységelemes gyűrű, akkor az $R$ invertálható elemei csoportot alkotnak a szorzásra, ennek neve $R$ *multiplikatív csoportja*, jele $R^\times$. Ha $R$ test, akkor ez az $R$ összes nem nulla eleméből áll.

Az előbbi fogalom nagyon fontos speciális esete a $\mathbb{Z}_n^\times$ csoport. Könnyű látni, hogy a $\mathbb{Z}_n$ gyűrű egy eleme pontosan akkor invertálható, ha relatív prím $n$-hez (tehát a $\mathbb{Z}_n$ gyűrű akkor és csak akkor test, ha $n$ egy prímszám). A $\mathbb{Z}_n^\times$ csoport elemszáma tehát a számelméletből ismert Euler-függvény, aminek a jele $\varphi(n)$. (A számelméletben sokszor a „modulo $n$ redukált maradékosztályok multiplikatív csoportja" elnevezést használják lényegében ugyanerre a csoportra.)

Ha az $R$ gyűrű egy $V$ vektortér összes lineáris transzformációjából áll, akkor az $R^\times$ csoportra szokásosabb a $GL(V)$ jelölést használni. Hasonlóan, ha $T$ test, akkor a $T^{n\times n}$ mátrixgyűrű multiplikatív csoportját $GL(n,T)$ jelöli (ez tehát az invertálható $n \times n$-es mátrixok csoportja a szorzásra). Rövidítésként $GL(n,\mathbb{Z}_p)$ helyett $GL(n,p)$-t írunk, ha $p$ prím. A $G$ és $L$ betűk a General Linear group (általános lineáris csoport) elnevezésből származnak. Ez a csoport általában nem kommutatív.

Nemkommutatív csoportot alkotnak a permutációk is a kompozícióra. Ezekről a csoportokról a determinánsképzés kapcsán tanultunk. Ha $X$ halmaz, akkor az $X$-et önmagára képező bijekciókat permutációknak nevezzük. Ezek csoportját a kompozíció (vagyis az egymás után alkalmazás) műveletére $S_X$ jelöli, neve: *szimmetrikus csoport.* Az $S_{\{1,2,\ldots,n\}}$ helyett $S_n$-et írunk. Ha $X$ elemszáma $n$, akkor általában $n$*-edfokú* szimmetrikus csoportról beszélünk. Vigyázzunk arra, hogy az $f \circ g$ kiszámításakor először a $g$-t, azután az $f$-et kell végrehajtani (ennek a furcsaságnak az az oka, hogy a leképezéseket balra, a leképezett elem elé írjuk). A kompozíció műveletét sokszor egyszerűen szorzásnak hívjuk majd.

Az egyik legfontosabb típusú permutáció a *ciklus.* Legyen $x_1, x_2, \ldots, x_k \in X$. Ekkor $(x_1 x_2 \ldots x_k)$ azt a permutációt jelöli, ami „körbeviszi" az elemeket: $x_1$-et elviszi $x_2$-be, ezt $x_3$-ba, és így tovább, $x_{k-1}$-et $x_k$-ba, végül $x_k$-t visszahozza $x_1$-be, az $X$ halmaz többi elemét pedig fixen hagyja, vagyis önmagába viszi. A megadott ciklus *hossza* a $k$ szám. Beláttuk, hogy véges $X$ halmaz esetén minden permutáció egyértelműen felírható páronként diszjunkt ciklusok szorzataként. A diszjunkt szó azt jelenti, hogy a ciklusokban nincs közös elem, vagyis ebben a felírásban minden elemet legfeljebb egy ciklus mozgathat. A kettő hosszú ciklusok neve *transzpozíció*, ezek szorzataként minden permutáció előáll. Például

egy $k$ hosszú ciklust többféleképpen fel lehet írni $k-1$ transzpozíció szorzataként.

Ha $X$ véges, akkor $S_X$ minden eleméhez hozzárendeltük az *előjelét*, ami $\pm 1$ lehet. Az 1 előjelű permutációkat párosnak, a $-1$ előjelűeket páratlannak is mondjuk. Az $f$ permutáció előjelét $sg(f)$ jelöli. Az előjelképzés tulajdonságait foglalja össze az alábbi tétel, amit korábban beláttunk.

**1.1. Tétel.** *Legyen $X$ véges halmaz.*

(1) *$S_X$ elemei között a páratlan hosszú ciklusok párosak, a páros hosszú ciklusok páratlanok.*
(2) *Szorzat előjele az előjelek szorzata: $sg(f \circ g) = sg(f)sg(g)$. Inverz előjele ugyanaz, mint az eredeti permutációé.*

Nagyon fontos megjegyzés, hogy ennek a tételnek a birtokában elfelejthetjük az előjel bonyolult, inverziókat számolgató definícióját, ezt soha már nem fogjuk használni! A fenti tétel ugyanis egyértelműen meghatározza minden permutáció előjelét, és a lényeg az, hogy ilyen tulajdonságú $sg$ függvény *létezik*. Ha ezt a létezést be tudnánk bizonyítani máshogy, egyszerűbben is, mint inverziókra gondolva, akkor az inverzió fogalmát meg sem kellene soha említeni. Egy matematikai objektum tulajdonságai mindig fontosabbak, mint az őt létrehozó konstrukció technikai részletei.

A tételből következik, hogy a páros permutációk is csoportot alkotnak a kompozícióra nézve. Ennek neve *alternáló csoport*, jele $A_X$. Beláttuk, hogy ennek elemszáma $S_X$ elemszámának a fele, vagyis $n$ elemű $X$ halmaz esetén $n!/2$.

A $G$ csoport elemeinek számát $G$ rendjének nevezzük, és $|G|$-vel jelöljük. Definiálni fogjuk a $g \in G$ elem egész kitevős hatványainak fogalmát. Ha $n$ pozitív egész szám, akkor $g^n$ jelöli azt az $n$ tényezős szorzatot, melynek minden tényezője $g$. A $g^0$ az egységelemet jelenti. Végül a szorzat inverzének képletéből kapjuk, hogy $(g^n)^{-1} = (g^{-1})^n$. Ezt az elemet $g^{-n}$ jelöli. Jó gyakorló feladat megmutatni a $g^n g^m = g^{n+m}$ és a $(g^n)^m = g^{nm}$ azonosságokat (a negatív kitevőkre is figyeljünk!). Vigyázzunk, a $(gh)^n = g^n h^n$ összefüggés általában nem érvényes, de persze akkor igen, ha $g$ és $h$ felcserélhetők, azaz ha $gh = hg$.

Egy $g$ elem különböző hatványainak számát a $g$ *rendjének* nevezzük, ennek jele $|g|$ (de sokszor, különösen ha $g$ egy szám, az $o(g)$ jelölést használjuk). A $g$ rendje pozitív egész szám, vagy pedig a $\infty$ jel, ha $g$-nek végtelen sok hatványa van. Felhívjuk a figyelmet ennek az általános fogalomnak két nagyon fontos speciális esetére. Ha a csoport az $n$-edik komplex egységgyökök csoportja a szorzásra, akkor az egységgyököknél tanult rend fogalmát, a $\mathbb{Z}_n^\times$ csoport esetében pedig a számelméletben tanult rend fogalmát kapjuk. Az alábbi tétel összefoglalja a rendről már korábban bizonyított állításokat.

**1.2. Tétel.** *Legyen $G$ csoport, $g \in G$, és $i, j, n$ egészek.*

(1) *A $g$ rendje akkor és csak akkor végtelen, ha $g$ bármely két (különböző egész kitevőjű) hatványa különböző.*
(2) *Ha $|g|$ véges, akkor $g^i = g^j \iff i \equiv j\ (|g|)$. Speciálisan $g^n = e$ akkor és csak akkor, ha $g$ rendje osztója az $n$ kitevőnek. Ezért a $g$ rendje a legkisebb olyan pozitív egész, amelyre $g$-t emelve az egységelemet kapjuk.*
(3) *A hatvány rendjének képlete: $|g^n| = |g|/(|g|, n)$.*

A tétel bizonyítása elemi számolás, amit már tanultunk. Szeretném azonban felhívni a figyelmet egy összefüggésre. Legyen $g \in G$, és tekintsük azokat az $n$ egészeket, melyekre $g^n = e$. Könnyű látni, hogy ezek a $\mathbb{Z}$ gyűrű egy ideálját alkotják (vö. a 2.8. Tétel bizonyítása). Mivel $\mathbb{Z}$ euklideszi gyűrű, ez az ideál főideál, és könnyű látni, hogy a $g$ rendje generálja (ha ez véges, $|g| = \infty$ esetén pedig a nulla generálja). Ez az észrevétel lerövidíti a tétel bizonyítását. Általában a maradékos osztás sokszori alkalmazása helyett elegánsabb ezt csak egyszer tenni, amikor belátjuk, hogy euklideszi gyűrű főideálgyűrű, és azután mindig ezt a tételt alkalmazni. Ez persze nagyobb matematikai érettséget követel az olvasótól.

Végül megemlítjük, hogy a szimmetrikus csoportban könnyű az elemrendeket kiszámítani. Tanultuk, hogy egy $k$ hosszú ciklus rendje $k$, és általában egy elem rendje a diszjunkt ciklusokra bontásában szereplő ciklushosszak legkisebb közös többszöröse.

## II. Részcsoportok

Egy $G$ csoport vizsgálatakor sokszor segít, ha olyan részhalmazait nézzük, melyek maguk is csoportok $G$ műveleteire nézve. Az így kapott csoportokat $G$ *részcsoportjainak* nevezzük. A $H \leq G$ jelölés azt jelenti, hogy $H$ részcsoportja $G$-nek. Minden csoportnak részcsoportja önmaga, valamint az egységelemből álló $\{e\}$ részcsoport. Ezek a triviális részcsoportok.

**2.1. Állítás.** *A $G$ csoport egy $H$ részhalmaza akkor és csak akkor részcsoport, ha nem üres, és zárt $G$ műveleteire nézve, azaz*

(1) $a, b \in H \implies ab \in H$,
(2) $a \in H \implies a^{-1} \in H$.

A bizonyítás (akárcsak az alterek, részgyűrűk esetében) azon múlik, hogy a csoportot definiáló azonosságok $H$ elemeire is automatikusan teljesülnek. Jó gyakorló feladat belátni, hogy egy nem üres $H$ részhalmaz pontosan akkor részcsoport, ha $a, b \in H \implies ab^{-1} \in H$ teljesül, továbbá, hogy egy részcsoport egységeleme meg kell hogy egyezzen $G$ egységelemével.

Vigyázzunk, hogy az inverzet ne felejtsük el megvizsgálni, például ha $G = \mathbb{Z}^+$ (az egész számok csoportja az összeadásra), akkor a pozitív egészek halmaza zárt az összeadásra, de mégsem részcsoport. Véges csoportok esetében viszont nem kell az inverzzel törődnünk, mert ha $a \in H$ rendje $n$, akkor $a^{-1} = a^{n-1} \in H$, hiszen $H$ zárt a szorzásra. Így beláttuk a következőt:

**2.2. Állítás.** *Ha $G$ minden eleme véges rendű, speciálisan ha $G$ véges, akkor $G$ minden nem üres, szorzásra zárt részhalmaza részcsoport.*

Vektorterek esetében az $U$ és $W$ alterek összegén az $U + W = \{u + w \mid u \in U, w \in W\}$ halmazt értettük. Ennek általánosításaként legyenek $X$ és $Y$ tetszőleges részhalmazai egy $G$ csoportnak. Ekkor $XY = \{xy \mid x \in X, y \in Y\}$ az $X$ és $Y$ *komplexus-szorzata.* Az elnevezés onnan származik, hogy egy csoport részhalmazait néha komplexusnak is nevezik. Ha speciálisan $X = \{a\}$ egy egyelemű halmaz, akkor $\{a\}Y$ helyett egyszerűen $aY$-t írunk. Hasonlóan definiálhatjuk a komplexus-inverz fogalmát az $X^{-1} = \{x^{-1} \mid x \in X\}$ képlettel. Ha $H$ részcsoport, akkor persze $HH = H^{-1} = H$. Gyakorlásul érdemes belátni, hogy a komplexusszorzás asszociatív, továbbá egy $H$ nem üres részhalmaz akkor és csak akkor részcsoport, ha $HH^{-1} \subseteq H$.

**2.3. Lagrange tétele.** *Véges csoport minden részcsoportjának rendje osztója a csoport rendjének.*

Mielőtt a bizonyításba kezdenénk, meg kell ismerkednünk a partíció és az ekvivalencia-reláció fogalmával. Legyen $X$ egy halmaz, és osszuk fel $X$-et nem üres, diszjunkt halmazok egyesítésére. Egy ilyen felosztást $X$ egy *partíciójának* nevezünk, a benne szereplő halmazokat pedig a partíció osztályainak.

Egy $X$ halmazon akkor értelmezünk relációt, ha $X$ bármely két elemére megmondjuk, hogy azok relációban vannak-e, vagy sem. Ilyen reláció például az oszthatóság, vagy a $\leq$ reláció az egész számok halmazán. (Egy $R$ reláció tehát általában az $X \times X$ Descartes-szorzat egy tetszőleges részhalmaza: pontosan azokból a párokból áll, melyekre a reláció teljesül.) Azt, hogy $a$ és $b$ relációban áll, $a\ R\ b$ (vagy $(a,b) \in R$) jelöli.

Ha az $X$ halmaznak adott egy partíciója, akkor készítsünk belőle egy $R$ relációt a következőképpen: két elem akkor van relációban, ha azonos osztályhoz tartoznak. Ez a reláció nyilván *reflexív* ($a\ R\ a$ minden $a \in X$-re), *szimmetrikus* ($a\ R\ b \implies b\ R\ a$ minden $a,b \in X$-re) és *tranzitív* ($a\ R\ b$ és $b\ R\ c \implies a\ R\ c$ minden $a,b,c \in X$-re). Azokat a relációkat, melyek rendelkeznek e három tulajdonsággal, *ekvivalencia-relációnak* nevezzük.

Tehát minden partíció meghatároz egy ekvivalencia-relációt. A megfordítás is igaz: minden ekvivalencia-reláció meghatároz egy partíciót. Noha ez az állítás igen egyszerű, lépten-nyomon alkalmazzák, mert a matematikában igen gyakran fordulnak elő partíciók.

**2.4. Állítás.** *Legyen $R$ ekvivalencia-reláció az $X$ halmazon. Tetszőleges $a \in X$ esetén legyen $R_a$ azoknak az $X$-beli $x$ elemeknek a halmaza, melyekre $a\ R\ x$. Ekkor az $R_a$ halmazok az $X$ egy partícióját adják.*

*Bizonyítás.* Az $R_a$ halmazok között lehetnek egyenlők; az állítást úgy kell érteni, hogy az $R_a$ halmazok közül bármely kettő vagy egyenlő, vagy diszjunkt, és egyesítésük kiadja $X$-et. Ez utóbbi állítás nyilván következik $R$ reflexivitásából ($a \in R_a$ minden $a$-ra). Most tegyük fel, hogy $R_a$ és $R_b$ nem diszjunkt, be kell látni, hogy egyenlőek. Legyen $c \in R_a \cap R_b$, megmutatjuk, hogy $R_a = R_c = R_b$. Valóban, $c \in R_a$ miatt $a\ R\ c$, és mivel $R$ szimmetrikus és tranzitív, minden $x$-re igaz, hogy $a\ R\ x \iff c\ R\ x$. Ezért $R_a = R_c$. Az $a$ és $b$ szerepét felcserélve $R_b = R_c$ adódik. □

**2.5. Állítás.** *Legyen $G$ csoport és $H \leq G$. Ekkor az $a\ R\ b \iff a^{-1}b \in H$ képlet ekvivalencia-relációt definiál $G$ alaphalmazán.*

*Bizonyítás.* Valóban, $R$ reflexív, hiszen $a^{-1}a = e \in H$. Ha $a^{-1}b \in H$, akkor a szorzat inverzére vonatkozó képlet miatt $H \ni (a^{-1}b)^{-1} = b^{-1}a$, ezért $R$ szimmetrikus. Végül ha $a^{-1}b \in H$ és $b^{-1}c \in H$, akkor $a^{-1}c = a^{-1}bb^{-1}c \in H$, vagyis $R$ tranzitív. Tehát $R$ ekvivalencia-reláció. □

Mik lesznek $R$ osztályai? Ha $a \in G$, akkor $a$ osztályát azon $x \in G$ elemek alkotják, melyekre $a\ R\ x$, azaz $a^{-1}x \in H$, vagyis $x \in aH$. Tehát beláttuk, hogy az $aH$ halmazok, ahol $a$ befutja $G$-t, a $G$ egy partícióját adják.

Hány eleme van az $aH$ halmaznak? Ugyanannyi, mint $H$-nak, hiszen a $h \leftrightarrow ah$ nyilván kölcsönösen egyértelmű megfeleltetés $H$ és $aH$ között (az egyszerűsítési szabály miatt). Ezért $G$ elemszámát úgy kaphatjuk meg, hogy $H$ elemszámát megszorozzuk az osztályok számával. Tehát $|H|$ osztója $|G|$-nek, és így Lagrange tételét bebizonyítottuk.

Az ebben a bizonyításban szereplő fogalmak annyira fontosak, hogy külön nevük is van. Az $aH$ halmazt a $H$ részcsoport szerinti *baloldali mellékosztálynak* nevezzük (hasonlóan $Ha$ jobboldali mellékosztály). Azt láttuk tehát be, hogy két $H$-szerinti baloldali mellékosztály vagy megegyezik, vagy diszjunkt, és a baloldali mellékosztályok uniója $G$. A különböző $H$ szerinti bal mellékosztályok számát a $H$ részcsoport $G$-beli *indexének* nevezzük, és $|G : H|$-val jelöljük. Ha tehát $G$ véges, akkor $|G| = |H| \cdot |G : H|$.

Az előző bekezdésben elmondottak igazak a jobboldali mellékosztályokra is. Az általában nem igaz, hogy a baloldali és a jobboldali mellékosztályok ugyanazok. (Gyakorlásképpen érdemes kiszámolni az $S_3$ csoport $\{id, (12)\}$ részcsoportja szerinti bal és jobb mellékosztályokat.) Ezért tulajdonképpen a $H$ szerinti bal- illetve jobbindex fogalmát kellett volna definiálnunk. Ez a két szám azonban megegyezik. Ez véges csoportnál azonnal világos az imént bizonyított tételből (hiszen mindkettő $|G|/|H|$).

Az index azonban lehet véges akkor is, ha a csoport maga végtelen! Például ha $n\mathbb{Z}^+$ jelöli az $n$-nel osztható egészekből álló részcsoportot $\mathbb{Z}^+$-ban, akkor $|\mathbb{Z}^+ : n\mathbb{Z}^+| = n$. Ilyenkor is igaz az, hogy a baloldali és a jobboldali index megegyezik. Valóban, ha $K = aH$ egy baloldali mellékosztály $H$ szerint, akkor $K^{-1} = Ha^{-1}$ egy jobboldali mellékosztály. Azonnal látszik, hogy az így megadott megfeleltetés a bal illetve jobb mellékosztályok halmaza között bijektív.

Legyen $g \in G$, és $H$ a $g$ összes hatványainak halmaza (negatív kitevőket is megengedve). Az így kapott (nyilván kommutatív) részcsoportot a $g$ által generált részcsoportnak nevezzük és $\langle g \rangle$-vel jelöljük. Ennek rendje $g$ hatványainak a száma, azaz definíció szerint a $g$ elem rendje. Ezért Lagrange tételének következménye az alábbi állítás:

**2.6. Következmény.** *Véges csoport minden elemének rendje osztója a csoport rendjének. Minden csoportelemet a csoport rendjére, mint kitevőre emelve az egységelemet kapjuk.*

Érdemes meggondolni, hogy ezt az eredményt a $\mathbb{Z}_n^\times$ csoportra alkalmazva az Euler-Fermat tételt kapjuk.

Egy $G$ csoportot *ciklikus*nak nevezünk, ha egy alkalmas elemének a hatványaiból áll.

**2.7. Tétel.** *Egy $G$ csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha $G$ prímrendű. Ilyenkor $G$ ciklikus csoport (és így kommutatív).*

*Bizonyítás.* Tegyük fel, hogy $G$-nek pontosan két részcsoportja van. Ekkor $|G| > 1$ és így $G$-nek létezik $e$-től különböző eleme. Minden ilyen $g$ elemre $\langle g \rangle \neq \{e\}$, azaz a feltétel miatt $\langle g \rangle = G$. Tehát $G$ ciklikus. A $g$ rendje nem lehet végtelen, mert egy ilyen elem hatványai páronként különbözők, tehát $e \neq g^2$ nem generálná $G$-t. Ha $|g| = n$, akkor legyen $p$ prímosztója $n$-nek. A hatvány rendjének képlete miatt $h = g^{n/p}$ rendje $p$. Így $e \neq h$ is generálja $G$-t, azaz $G$ prímrendű. Megfordítva, ha $G$ rendje egy $p$ prím, és $H$ részcsoportja $G$-nek, akkor $H$ rendje csak 1 vagy $p$ lehet, tehát $H = \{e\}$, illetve $H = G$. □

Ha egy csoport nem prímrendű, de ciklikus, akkor ugyan vannak valódi részcsoportjai, de ezek mind ciklikusak lesznek.

**2.8. Tétel.** *Ciklikus csoport minden részcsoportja is ciklikus.*

*Bizonyítás.* Legyen $G = \langle g \rangle$ és $H \leq G$. Tekintsük azokat az $n$ egészeket, melyekre $g^n \in H$:

$$I = \{n \in \mathbb{Z} \mid g^n \in H\}\,.$$

Azonnal látjuk, hogy $I$ ideál $\mathbb{Z}$-ben. Valóban, ha $m,n \in I$, akkor $g^m \in H$ és $g^n \in H$, és így $g^{m+n} = g^m g^n \in H$, vagyis $m+n \in I$. Ha pedig $n \in I$ és $z \in \mathbb{Z}$, akkor $g^n \in H$, vagyis $g^{nz} = (g^n)^z \in H$ (hiszen $H$ zárt a hatványozásra), vagyis $nz \in I$. Tehát $I$ ideál. Mivel $\mathbb{Z}$ euklideszi gyűrű, $I$ a tanult tétel szerint főideál, vagyis van olyan $r$ egész, hogy $I$ éppen $r$ többeseiből áll. Így $g^n \in H$ akkor és csak akkor, ha $r \mid n$, vagyis ha $g^n$ hatványa $g^r$-nek. Tehát $H$ pontosan $g^r$ hatványaiból áll, és ezért ciklikus. □

**2.9. Állítás.** *Ha $G$ véges ciklikus csoport, és $d$ osztója $G$ rendjének, akkor $G$-nek pontosan $\varphi(d)$ darab $d$ rendű eleme, és pontosan egy darab $d$ rendű részcsoportja van (itt $\varphi$ az Euler-függvény).*

*Bizonyítás.* Legyen $|G| = n$ és $G = \langle g \rangle$. Minden $d$ rendű részcsoport elemeire igaz, hogy a $d$-edik hatványuk $e$. Keressük meg először ezeket az elemeket.

$$(g^i)^d = e \iff g^{id} = e \iff n \mid id \iff n/d \mid i\,.$$

Ezek az elemek tehát $h = g^{n/d}$ hatványai, és így $d$ darab van belőlük. Ezért az egyetlen $d$ rendű részcsoport éppen ezeknek a halmaza (ezzel mellesleg új bizonyítást kaptunk az előző állításra véges csoportok esetén). A $d$ rendű elemek tehát $h$ hatványai között vannak. A hatvány rendjére vonatkozó képlet szerint

$$|h^j| = \frac{|h|}{(|h|, j)} = \frac{d}{(d, j)}\,,$$

és ez pontosan akkor $d$, ha $(d, j) = 1$, az ilyen $j$-k száma pedig $\varphi(d)$. □

Mivel az $n$-edik komplex egységgyökök csoportja ciklikus (hiszen a $2\pi/n$ szögű egységgyök generálja), ezért a fenti állítás speciális eseteként kapjuk, hogy a primitív $n$-edik egységgyökök száma $\varphi(n)$.

A most használt „generálás" kifejezés emlékeztet a lineáris algebrában használt fogalomra. Ott generált altérről, és lineáris kombinációk halmazáról, most pedig hatványok halmazáról volt szó. Mi e két dologban a közös?

A kulcsot az a lineáris algebrában bizonyított és használt észrevétel adja meg, amely szerint az $X$ által generált altér a *legszűkebb* $X$-et tartalmazó altér, azaz minden $X$-et tartalmazó altérnek része. Ugyanez a tulajdonság csoportokra is igaz: ha $G$ tetszőleges csoport, és $g \in G$, akkor $\langle g \rangle$ a legszűkebb $g$-t tartalmazó részcsoport. Valóban, ha a $H$ részcsoport tartalmazza $g$-t, akkor tartalmazza $g$ hatványait, vagyis $\langle g \rangle$-t. Ezért a „$g$ által generált részcsoport" elnevezés összevág a lineáris algebrában használt fogalommal. Lássuk akkor, hogy általában mit is jelent a generálás.

**2.10. Definíció.** *Tetszőleges $A$ struktúra (csoport, gyűrű, vektortér, algebra) esetén az $X \subseteq A$ által generált részstruktúra (részcsoport, részgyűrű, altér, részalgebra) a legszűkebb $X$-et tartalmazó részstruktúra, jele $\langle X \rangle$. Az $X$ részhalmazt $A$ generátorrendszerének nevezzük (illetve azt mondjuk, hogy $X$ generálja $A$-t), ha $\langle X \rangle = A$.*

A legszűkebb szó tehát azt jelenti, hogy $\langle X \rangle$ része minden, $X$-et tartalmazó részstruktúrának. Megjegyezzük, hogy a generálás fogalma még ennél is általánosabb, hiszen például

gyűrű esetén generált ideálról is beszélhetünk, ez az adott részhalmazt tartalmazó legszűkebb ideál.

A fenti definíció csak akkor értelmes, ha *egyértelműen létezik* ez a bizonyos legszűkebb részstruktúra. Az egyértelműség nyilvánvaló, hiszen ha két legszűkebb ilyen részstruktúra lenne, akkor azok egymást tartalmaznák. A létezés oka a következő.

**2.11. Állítás.** *Részstruktúrák metszete is részstruktúra (végtelen soké is).*

A bizonyítás azon múlik minden esetben, hogy csak a zártságot kell ellenőrizni, mert az azonosságok automatikusan öröklődnek. Ez az állítás természetesen ideálokra (továbbá balideálokra, jobbideálokra) is érvényes.

**2.12. Állítás.** *Az $X$ által generált résztruktúra egyértelműen létezik, mint az összes $X$-et tartalmazó részstruktúra metszete.*

Valóban, az $X$-et tartalmazó részstruktúrák metszete is részstruktúra, és ez a metszet része minden tényezőjének, azaz tényleg az $X$-et tartalmazó legszűkebb részstruktúra.

A generált részcsoport tehát létezik, de ahhoz, hogy az elemeit konkrétan kiszámíthassuk, a fenti konstrukció nem alkalmas. Ahogy a vektorterek esetében a generálást lefordítottuk a lineáris kombinációk nyelvére, ezt meg kell tennünk csoportok esetében is.

**2.13. Állítás.** *Legyen $G$ csoport és $X \subseteq G$.*

(1) *$\langle X \rangle$ a $G$ azon elemeiből áll, melyek felírhatók az $X$ elemeiből és azok inverzeiből képzett sokténye zős szorzatként ($X$ minden eleme többször is felhasználható).*

(2) *Ha $G$ kommutatív és $X = \{g_1, \ldots, g_n\}$, akkor*

$$\langle X \rangle = \{g_1^{k_1} \ldots g_n^{k_n} \mid k_1, \ldots, k_n \in \mathbb{Z}\}\,.$$

Az Abel-féle esetbeli képlet lényegében azonos a lineáris algebrában tanult formulával, csak az egész együtthatós lineáris kombinációban együttható helyett kitevőt kell írni, hiszen nem összeadás, hanem szorzás a művelet. Az általános eset annyiban más, hogy az egyes generátoroknak nem kell „egymás mellett" lenniük. Például a $\langle g, h \rangle$ egy tipikus eleme $g^{-2}h^6gh^2gh^2gh^{-3}$. Ezeket a szorzatokat már igen nehéz áttekinteni, ezért a két elemmel generált csoportok szerkezete igen bonyolult lehet. Gyakorlásul érdemes belátni, hogy az $\{(12), (12\ldots n)\}$ halmaz generátorrendszer az $n$-edfokú szimmetrikus csoportban. Tehát már két elemmel is akármekkora véges csoportot generálhatunk (míg lineáris algebrában a két elemmel generált alterek legfeljebb kétdimenziósak lehetnek).

*Bizonyítás.* Csak a 2.13. Állítás (1) részét látjuk be, hiszen ennek (2) nyilván speciális esete. Legyen $H$ az $X$ által generált részcsoport, $K$ pedig az (1)-ben leírt szorzatoknak a halmaza. Azt kell belátni, hogy $H = K$.

$K \subseteq H$. A $H$ részcsoport, amely $X$-et tartalmazza. Tehát tartalmazza az $X$ elemeinek inverzeit, és az $X \cup X^{-1}$ elemeiből képzett szorzatokat is, azaz $K$ valamennyi elemét.

$H \subseteq K$. Elegendő belátni, hogy $K$ egy $X$-et tartalmazó részcsoport, mert akkor $H$, mint a legszűkebb $X$-et tartalmazó részcsoport, része lesz $K$-nak. Az $X$ elemei, mint egytényezős szorzatok, elemei $K$-nak. Nyilván $K$ zárt a szorzásra, hiszen két bonyolult szorzatot egymás mellé írva egy ugyanilyen fajta, csak még bonyolultabb szorzatot kapunk. Az egységelem is benne van $K$-ban, mint üres szorzat. Végül a szorzat inverzének képletét alkalmazva látjuk, hogy $K$ az inverzképzésre is zárt. □

## III. Permutációcsoportok

Legyen $X$ halmaz. Az $S_X$ szimmetrikus csoport részcsoportjait *permutációcsoportnak* nevezzük. Az $X$ halmaz elemeit néha *pontoknak* hívjuk. Ez az elnevezés a geometriából származik, hiszen például nagyon fontos permutációcsoport az, amit a sík egybevágósági (vagy hasonlósági) transzformációi alkotnak.

Tegyük fel, hogy $G \leq S_X$, és definiáljunk egy $\sim_G$ relációt az $X$-en a következő képlettel:

$$x \sim_G y \iff \exists g \in G : g(x) = y\,.$$

Azaz két elem relációban áll, ha az egyiket a másikba át lehet vinni $G$ egy elemével. Például legyen $X$ a sík, és $G$ az origó körüli forgatások csoportja. Ekkor $P \sim_G Q$ nyilván akkor és csak akkor igaz, ha $P$ és $Q$ egyforma távolságra van az origótól.

Azonnal látszik, hogy $\sim_G$ ekvivalencia-reláció. Valóban, $x \sim_G x$ (hiszen az egységelem $x$-et önmagába viszi); ha $x \sim_G y$, akkor $y \sim_G x$ (hiszen ha $g(x) = y$, akkor $g^{-1}(y) = x$); végül ha $x \sim_G y$ és $y \sim_G z$, akkor $x \sim_G z$ (hiszen ha $g(x) = y$ és $h(y) = z$, akkor $(hg)(x) = z$). A $\sim_G$ relációhoz tartozó partíció osztályait $G$ *orbitjainak* nevezzük. Az előző (forgatásos) példában az orbitok az origó körüli körök. Az $x \in X$ elemet tartalmazó orbitot szokás az $x$ elem orbitjának is nevezni, jele $G(x)$. Ha $X$ egyetlen orbitból áll, akkor azt mondjuk, hogy $G$ *tranzitív* $X$*-en.*

Gyakorlásképpen érdemes bebizonyítani, hogy ha $g \in S_X$, akkor a $g$ által generált $\langle g \rangle$ részcsoport orbitjai épp a $g$ ciklusfelbontását adják.

Ha $x \in X$ adott, akkor tekinthetjük azokat a $g$ elemeket $G$-ben, melyek $x$-et fixen hagyják (azaz $g(x) = x$). Ezek nyilván részcsoportot alkotnak $G$-ben, melynek neve *az* $x$ *pont* $G$*-beli stabilizátora,* jele $G_x$.

**3.1. Tétel.** *Legyen* $G \leq S_X$. *Ekkor tetszőleges* $x \in X$*-re* $|G(x)| = |G : G_x|$.

Tehát egy orbit elemszáma, vagy *hossza* épp a stabilizátorának indexe. A tétel bizonyítását könnyebb megérteni, ha előbb egy alkalmazást mutatunk be: kiszámoljuk, hány szimmetriája van a kockának.

Legyen tehát adva egy kocka a térben, $G$ pedig azoknak az egybevágósági transzformációknak a halmaza, melyek a kockát önmagába képzik. Nyilván $G$ részcsoportja a sík egybevágóságcsoportjának, de ha $X$ jelöli a kocka csúcsainak halmazát, akkor tekinthető $G$ az $S_X$ részcsoportjának is, hiszen egybevágóság csúcsot csúcsba visz, és ha egy egybevágósági transzformációt a kocka csúcsain ismerünk, akkor már a tér minden pontjának a képét is ki tudjuk számítani.

A kocka bármely két csúcsa egymásba vihető alkalmas egybevágósággal. Valóban: két szomszédos csúcsot ki lehet cserélni például egy síkra tükrözéssel, és ilyen lépések sorozatával bármely csúcsból bármely csúcsba eljuthatunk. Azaz a $G$ csoport tranzitívan hat a kocka csúcsain. Ha $A$ jelöli az egyik csúcsot, akkor tehát az iménti tétel miatt $|G(A)| \cdot |G_A| = |G|$. Mivel $A$ orbitja az összes csúcsok halmaza, $|G(A)| = 8$. Ezért elegendő $G_A$ rendjét meghatározni.

Legyen tehát $g$ egy olyan egybevágóság, mely az $A$ csúcsot fixen hagyja, és legyen $B$, $C$, $D$ az $A$ csúcs három szomszédja. Mi lehet a $B$ csúcs képe $g$-nél? Mivel $g$ egybevágóság, a $g(B)g(A)$ távolság meg kell hogy egyezzen az $AB$ távolsággal. Tehát $g(B)$ élhossznyi

távolságra van $g(A) = A$-tól. Ilyen csúcs három van: $B$, $C$ és $D$. A testátló körüli két 120 fokos forgatás $B$-t elviszi $C$-be is és $D$-be is, ezért a $B$ elem orbitja a $G_A$ csoportnál éppen $G_A(B) = \{B, C, D\}$. A tételt most a $G_A$ csoportra alkalmazva azt kapjuk, hogy $|G_A(B)| \cdot |(G_A)_B| = |G_A|$. Így $|G| = 8 \cdot 3 \cdot |(G_A)_B|$. Tehát elég azokat az egybevágóságokat megszámolni, melyek az $A$ pontot is és a $B$ pontot is fixen hagyják.

Ha most $g$ ilyen, akkor a $C$ pont képe már csak $D$ lehet ($B$ nyilván nem). Másrészt az $AB$-n átmenő átlósíkra való tükrözés fixen hagyja $A$-t és $B$-t, és kicseréli $C$-t $D$-vel. Ezért a $(G_A)_B$ csoportban $C$ orbitja kételemű, és a tételt mégegyszer alkalmazva azt kapjuk, hogy $|G| = 8 \cdot 3 \cdot 2 \cdot |((G_A)_B)_C|$. Végül ha egy egybevágóság fixen hagyja $A$-t, $B$-t és $C$-t is, akkor $D$-t is, és könnyen láthatóan a tér minden pontját is. Ezért $|((G_A)_B)_C| = 1$, vagyis a kockának 48 szimmetriája van.

Hasonló technikával érdemes kiszámolni, hogy egy szabályos $n$-szögnek $2n$ szimmetriája van ($n$ tükrözés és $n$ forgatás). Ezeknek a csoportját $D_n$ jelöli, ez az $n$-edfokú *diédercsoport*. A szabályos tetraédernek 24 szimmetriája van, vagyis a csúcsok bármely permutációja megvalósítható alkalmas egybevágósági transzformációval.

Lássuk most akkor a 3.1. Tétel bizonyítását. Azt kell belátni, hogy $G(x)$ rendje ugyanaz, mint $G_x$ indexe. Mivel $G(x) = \{g(x) \mid g \in G\}$, ehhez azt célszerű megvizsgálni, hogy mely $g'$ elemek viszik $x$-et ugyanabba a pontba, mint $g$. Nyilván

$$g'(x) = g(x) \Longleftrightarrow (g^{-1}g')(x) = x \Longleftrightarrow g^{-1}g' \in G_x \Longleftrightarrow g' \in gG_x \,.$$

Tehát az ilyen $g'$ elemek egy $G_x$ szerinti baloldali mellékosztályt alkotnak. Vagyis az a megfeleltetés, ami a $g(x)$ ponthoz a $gG_x$ mellékosztályt rendeli, bijekció. Ezért valóban $|G(x)| = |G : G_x|$. $\square$

A matematikában sokszor megtörténik az, hogy egy $G$ csoport elemei maguk nem permutációi az $X$ halmaznak, mégis $G$ elemei „hatnak" az $X$ halmazon. Például a kocka esetében beszélhetünk arról is, hogy az egybevágóságok a kocka éleit, lapjait, vagy testátlóit permutálják. Egy egybevágósági transzformáció a tér pontjain értelmezett függvény, tehát nem szakaszokat permutál. De mondhatjuk azt, hogy ha $F$ egybevágóság, akkor az $\overline{AB}$ szakaszt $F$ „vigye" az $\overline{F(A)F(B)}$ szakaszba. Ezt jelölhetjük a következőképpen: $F * \overline{AB} = \overline{F(A)F(B)}$.

Általában azt mondjuk, hogy a $G$ csoport az $X$ halmazon *hat*, ha minden $g \in G$ és $x \in X$ esetén beszélhetünk a $g * x \in X$ elemről (formálisan: értelmezve van egy $* : G \times X \to X$ leképezés) úgy, hogy bármely $g, h \in G$ és $x \in X$ esetén

$$g * (h * x) = (gh) * x$$

(azaz $G$ elemeinek szorzata szorzatpermutációként hat), és ha $e$ jelöli $G$ egységelemét, akkor bármely $x \in X$ esetén

$$e * x = x$$

(vagyis az egységelem identikusan hat $X$-en). Ezekből a szabályokból adódik, hogy $g^{-1}$ inverz leképezésként hat, azaz

$$g * x = y \Longleftrightarrow g^{-1} * y = x \,.$$

Az eddig tárgyaltakat speciális esetként kapjuk, ha $G \leq S_X$, azaz $G$ maga permutációkból áll, és $g * x = g(x)$. A dolog kicsit hasonló ahhoz, ahogy egy vektortér elemeit az alaptest elemeivel szorozzuk (ellenőrizzük, hogy ilyenkor a test multiplikatív csoportja tényleg hat a vektortéren a fenti értelemben).

Az orbit és stabilizátor fogalma az általános esetben is ugyanúgy definiálható. Ha $G$ hat $X$-en, akkor a $\sim_G$ ekvivalencia-relációt az $X$-en az

$$x \sim_G y \iff \exists g \in G : g * x = y\,.$$

képlet definiálja (ennek osztályai lesznek az orbitok), az $x \in X$ stabilizátora pedig azokból a $g$ elemekből áll, melyekre $g * x = x$. Most is igaz, hogy az $x$-et tartalmazó orbit hossza egyenlő a stabilizátorának indexével, és a bizonyítás szó szerint ugyanaz, mint az imént.

**3.2. Tétel.** *Legyen $G$ a véges $X$ halmazon ható csoport. Ekkor tetszőleges $x \in X$-re $|G(x)| = |G : G_x|$.*

*Bizonyítás.* Nyilván

$$g' * x = g * x \iff (g^{-1}g') * x = x \iff g^{-1}g' \in G_x \iff g' \in gG_x\,.$$

Tehát az $x$-et $g * x$-be vivő $g'$ elemek egy $G_x$ szerinti baloldali mellékosztályt alkotnak. Vagyis az a megfeleltetés, ami a $g * x$ ponthoz a $gG_x$ mellékosztályt rendeli, bijekció az $x$ orbitja és $G_x$ baloldali mellékosztályainak halmaza között. □

Gyakorlásul érdemes belátni, hogy a kocka szimmetriacsoportja tranzitívan hat az élek halmazán, és minden él stabilizátora négyelemű. Hasonlóképpen a lapok halmazán is tranzitív a hatás, itt a stabilizátor nyolcelemű, olyan mint a négyzet szimmetriacsoportja.

## IV. Izomorfizmus

A csoportelmélet célja az, hogy a csoportok szerkezetét felderítse. Nem az a kérdés, hogy mik egy adott csoport elemei, hanem az, hogy a művelet hogyan működik rajtuk.

Például ha egy ciklikus csoport rendje végtelen, akkor elemei $g^n$ alakban írhatók, és két elemét úgy lehet összeszorozni, hogy a kitevőket összeadjuk. Tehát a csoport elemei helyett egész számokkal számolunk. Akkor pedig felesleges a csoportot $\mathbb{Z}^+$-tól megkülönböztetni. Azt mondhatjuk, hogy a két csoport lényegében ugyanaz. Hasonlóképpen ha $G$ egy $n$-edrendű ciklikus csoport, akkor elemei $g^n$ alakúak, és a kitevőkkel modulo $n$ kell számolni. Ezt a csoportot tehát a $\mathbb{Z}_n^+$ csoporttal tekinthetjük azonosnak.

Természetesen az nem mindig látszik egy csoporton, hogy ciklikus-e. Például a $\mathbb{Z}_5^\times$ csoportról esetleg nem vesszük azonnal észre, hogy a 2 hatványaiból áll. De ha már észrevettük, akkor a számolás nagyon egyszerűvé válik ebben a csoportban. Ez az észrevétel az alapja a binom kongruenciák megoldására a számelméletben tanult eljárásnak. Ugyanis ha $p$ prím, akkor van primitív gyök mod $p$, és ez pontosan azt jelenti, hogy a $\mathbb{Z}_p^\times$ csoport ciklikus. Ahhoz, hogy ezt az izomorfizmust megadhassuk, meg kell keresnünk egy primitív gyököt mod $p$. Ha azonban csak olyan kérdés merül fel, hogy például hány 13 rendű elem van $\mathbb{Z}_p^\times$-ben, akkor nem kell primitív gyököt keresni, hanem a 13 rendű elemeket elég a $\mathbb{Z}_{p-1}^+$ csoportban megszámolni, ami sokkal egyszerűbb feladat.

Fogalmazzuk meg pontosan, mikor is tekinthetünk két csoportot azonosnak. A végtelen ciklikus csoportban $g^n$ helyett $n$-nel akarunk számolni. Ezt az teszi lehetővé, hogy ez a megfeleltetés kölcsönösen egyértelmű, másrészt „ugyanúgy kell számolni $n$-nel, mint $g^n$-nel", vagyis a $g^n g^m$ szorzat kiszámítása az $n+m$ összeg kiszámításával egyenértékű, a csoport két eleme helyett a nekik a másik csoportban megfelelő elemekkel végezhetjük el a műveletet. Képlettel ezt úgy írhatjuk fel, hogy a $\psi(g^n) = n$ leképezés teljesíti a $\psi(g^n g^m) = \psi(g^n) + \psi(g^m)$ tulajdonságot, vagyis *művelettartó*. A művelettartó leképezéseket (tetszőleges struktúrák esetén) *homomorfizmusnak* nevezzük. Lineáris algebrában ezek a lineáris leképezések. *Izomorfizmus* alatt bijektív homomorfizmust értünk. A $G$ és $H$ csoportok izomorfak, ha van közöttük izomorfizmus, ennek jele $G \cong H$. Az eddig ciklikus csoportokról elmondottakat az új nyelven következőképpen fogalmazhatjuk meg.

**4.1. Állítás.** *Egy csoport akkor és csak akkor ciklikus, ha izomorf a $\mathbb{Z}^+$ illetve a $\mathbb{Z}_n^+$ csoportok valamelyikével (ahol $n$ pozitív egész).*

Az izomorf csoportok tulajdonságai megegyeznek, hiszen a csoportelméleti fogalmakat a műveletek segítségével definiáljuk, márpedig izomorf csoportokban „ugyanazok" a műveletek. Első lépésként vegyük észre, hogy a szorzattartásból az „egységelem-tartás" és az „inverztartás" is következik. Valóban, ha $\psi : G \to H$ szorzattartó, azaz $\psi(ab) = \psi(a)\psi(b)$ teljesül minden $a, b \in G$-re, akkor

$$e_H \psi(e_G) = \psi(e_G) = \psi(e_G e_G) = \psi(e_G)\psi(e_G)\,,$$

és így $\psi(e_G) = e_H$ az egyszerűsítési szabály miatt. Így az egységelem képe mindenképpen az egységelem. Ekkor viszont

$$e_H = \psi(e_G) = \psi(g g^{-1}) = \psi(g)\psi(g^{-1})\,,$$

azaz $\psi(g^{-1}) = (\psi(g))^{-1}$, és így $\psi$ inverzet inverzbe visz, vagyis az inverzképzés műveletét is tartja. Gyakorlásképpen érdemes igazolni, hogy ha $\psi : G \to H$ izomorfizmus, akkor $g$ és $\psi(g)$ rendje mindig megegyezik, részcsoport képe izomorfizmusnál részcsoport, mellékosztályé mellékosztály, és így tovább.

Mivel az izomorf csoportok tulajdonságai ugyanazok, nem is érdemes megkülönböztetni őket egymástól. Ez a híres Steinitz-féle *izomorfia-elv*. Például tudjuk, hogy az összes tízelemű ciklikus csoport egymással izomorf. Ezért **a** tízelemű ciklikus csoportról beszélhetünk. Az izomorfia a csoportok között természetesen ekvivalencia-reláció. Például a tizedrendű ciklikus csoportok egy izomorfia-osztályt alkotnak.

Amikor a véges csoportok osztályozásáról beszélünk, akkor azt szeretnénk, hogy izomorfia erejéig az összes véges csoportot felsoroljuk, lehetőleg olyan áttekinthető szerkezetű alakban, hogy a felmerülő kérdéseket könnyen megválaszolhassuk. Már az eddigi eredményeink is lehetővé teszik, hogy ezt a felsorolást elkezdjük. Nyilván bármely két egyelemű csoport izomorf, tehát egyelemű csoportból (izomorfia erejéig) egyetlen darab van. Láttuk, hogy minden prímrendű csoport ciklikus, és azt is, hogy az azonos rendű ciklikus csoportok izomorfak. Ezért 2, 3, 5, és 7 rendű csoportokból is egy-egy van.

Kimaradt a sorból a 4 és a 6. Vannak-e ilyen rendű csoportok? Természetesen igen, hiszen a $\mathbb{Z}_n^+$ csoport rendje $n$, azaz *minden pozitív $n$-re van $n$-edrendű csoport.* Vannak-e ezekkel nem izomorf, azaz nem ciklikus 4 illetve 6 rendű csoportok?

A válasz könnyebb 6-ra: az $S_3$ csoportnak is 6 a rendje, de nem kommutatív, és ezért nem is lehet ciklikus. Számolással belátható, hogy más hatodrendű csoport nincs, azaz izomorfia erejéig összesen kettő van.

Ha a rend 4, akkor is tudunk találni nem-ciklikus csoportot, ilyen például $\mathbb{Z}_8^\times$. Ebben a csoportban ugyanis minden elem négyzete az egységelem, azaz nincs negyedrendű elem. Az egységelemtől különböző három elem közül bármely kettő szorzata a harmadik. Ezt a csoportot, és a vele izomorfakat Klein-csoportnak nevezzük. Némi számolással belátható, hogy negyedrendű csoportból csak ez a kétféle van. Látni fogjuk majd, hogy általában a prím-négyzet elemszámú csoportok száma is kettő.

A nyolcelemű csoportok felsorolásához definiálnunk kell a *kvaterniócsoport* fogalmát. Egy csoportot nemcsak valamiféle „szabály" segítségével adhatunk meg, hanem úgy is, hogy felsoroljuk az elemeket, és megmondjuk az összes szorzatot. Ezt célszerű táblázatosan végezni, úgy, hogy a $g$ elem sorának és a $h$ elem oszlopának a metszéspontjába írjuk a $gh$ elemet. Ezt a táblázatot Cayley-táblázatnak nevezzük. Példaként álljon itt a négyzet szimmetriacsoportjának Cayley-táblázata (mint $S_4$ egy részcsoportja). Aki ezt a táblázatot leellenőrzi, egy életre megtanulja a permutációszorzást...

| $D_4$ | $id$ | (1234) | (13)(24) | (1432) | (12)(34) | (24) | (14)(23) | (13) |
|---|---|---|---|---|---|---|---|---|
| $id$ | $id$ | (1234) | (13)(24) | (1432) | (12)(34) | (24) | (14)(23) | (13) |
| (1234) | (1234) | (13)(24) | (1432) | $id$ | (13) | (12)(34) | (24) | (14)(23) |
| (13)(24) | (13)(24) | (1432) | $id$ | (1234) | (14)(23) | (13) | (12)(34) | (24) |
| (1432) | (1432) | $id$ | (1234) | (13)(24) | (24) | (14)(23) | (13) | (12)(34) |
| (12)(34) | (12)(34) | (24) | (14)(23) | (13) | $id$ | (1234) | (13)(24) | (1432) |
| (24) | (24) | (14)(23) | (13) | (12)(34) | (1432) | $id$ | (1234) | (13)(24) |
| (14)(23) | (14)(23) | (13) | (12)(34) | (24) | (13)(24) | (1432) | $id$ | (1234) |
| (13) | (13) | (12)(34) | (24) | (14)(23) | (1234) | (13)(24) | (1432) | $id$ |

A következő táblázat a kvaterniócsoportot definiálja.

| $Q$ | $1$ | $i$ | $j$ | $k$ | $-1$ | $-i$ | $-j$ | $-k$ |
|---|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $i$ | $j$ | $k$ | $-1$ | $-i$ | $-j$ | $-k$ |
| $i$ | $i$ | $-1$ | $k$ | $-j$ | $-i$ | $1$ | $-k$ | $j$ |
| $j$ | $j$ | $-k$ | $-1$ | $i$ | $-j$ | $k$ | $1$ | $-i$ |
| $k$ | $k$ | $j$ | $-i$ | $-1$ | $-k$ | $-j$ | $i$ | $1$ |
| $-1$ | $-1$ | $-i$ | $-j$ | $-k$ | $1$ | $i$ | $j$ | $k$ |
| $-i$ | $-i$ | $1$ | $-k$ | $j$ | $i$ | $-1$ | $k$ | $-j$ |
| $-j$ | $-j$ | $k$ | $1$ | $-i$ | $j$ | $-k$ | $-1$ | $i$ |
| $-k$ | $-k$ | $-j$ | $i$ | $1$ | $k$ | $j$ | $-i$ | $-1$ |

A szorzást a következőképpen lehet megjegyezni. Az 1 az egységelem, a $-1$-gyel való szorzás mindenkit az ellentettjére változtat. Az $i$, $j$, $k$ mindegyike úgy viselkedik, mint a komplex $i$ szám, azaz négyzetük $-1$. Egymással ezeket úgy szorozzuk, hogy az $\{i, j, k\}$ „körön" sorrendben haladva bármely kettő szorzata a harmadik, visszafelé haladva pedig bármely kettő szorzata a harmadik ellentettje. Természetesen itt ellenőrizni kell az asszociativitást (ez elvileg $8^3$ egyenlőség vizsgálatát jelenti).

Nyolcelemű csoport ötféle van, három kommutatív (ezek szerkezetéről később lesz szó), $D_4$ és $Q$. Ez utóbbiak nem kommutatívak, és nem izomorfak, mert a másodrendű elemek száma $Q$-ban csak egy, $D_4$-ben pedig 5.

Az egyszerűsítési szabály miatt tetszőleges $G$ csoport Cayley-táblázatának minden sora (és minden oszlopa) a csoport elemeinek egy permutációja. Jelölje $\psi(g)$ a $g$ elem sorához tartozó permutációt (azaz legyen $[\psi(g)](x) = gx$). Ez $G$ elemeit permutálja, azaz $\psi(g) \in S_G$. A kapott $\psi : G \to S_G$ megfeleltetés szorzattartó, azaz $\psi(gh) = \psi(g) \circ \psi(h)$. Valóban, tetszőleges $x \in G$ esetén

$$\psi(gh)(x) = ghx = g(hx) = \psi(g)(hx) = \psi(g)(\psi(h)(x)) = (\psi(g) \circ \psi(h))(x)\,.$$

Továbbá $g \neq h$ esetén $\psi(g) \neq \psi(h)$ (sőt, ez a két permutáció egyetlen helyen sem egyezik meg, hiszen az oszlopok is permutációk). Ezért a $\psi : G \to S_G$ leképezés injektív csoporthomomorfizmus. Ezzel beláttuk, hogy a Cayley-táblázat soraihoz tartozó permutációk $G$-vel izomorf részcsoportot alkotnak $S_G$-ben. Másképp fogalmazva:

**4.2. Cayley tétele.** *Minden csoport izomorf egy permutációcsoporttal.*

E tétel szerint elég lenne csak permutációcsoportokat vizsgálni (mint Galois korában tették). A Cayley-reprezentáció vizsgálata azonban csak ritkán segít a csoport szerkezetének feltárásában.

## V. Homomorfizmus

Láttuk, hogy izomorfizmus segítségével az egyik csoportban bizonyított eredményeket más csoportokra is átvihetjük. Az olyan homomorfizmusok is fontosak, melyek nem izomorfizmusok. Sokszor előfordul ugyanis, hogy egy nagy, bonyolult $G$ csoportnak van egy homomorfizmusa egy egyszerű szerkezetű $H$ csoportra (ilyen például az előjelképzés : $S_n \to \mathbb{Z}_2^+$). Így a $G$-re vonatkozó kérdések egy részét $H$-ban számolva is megválaszolhatjuk. Például azt a tényt, hogy (12) nem áll elő hármasciklusok szorzataként, az előjel vizsgálatával láthatjuk azonnal át. A homomorfizmus valószínűleg a matematika legfontosabb fogalma. Sőt, az életben (folyamatok modellezésekor) is azt tesszük, hogy a lényeges dolgokat megragadjuk, és csak azokat vizsgáljuk, azaz „homomorfizmust" (a lényeget megtartó leképezést) készítünk egy már kezelhető struktúrába (a modellbe).

Szeretnénk áttekinteni a $G$ csoporton értelmezhető homomorfizmusokat. Ez nehezebb feladat, mint a lineáris algebrában, ahol minden homomorfimust egy mátrixszal megadhatunk. A lineáris algebrában minden $A : V \to W$ lineáris leképezéshez hozzárendeltük a magterét. Ennek ismerete a dimenziótétel miatt meghatározza $\mathrm{Im}(A)$ dimenzióját, és ezzel a kép, mint vektortér szerkezetét. Nézzük meg, hogy ha $\psi : G \to H$ csoporthomomorfizmus, akkor a „mag" ismerete meghatározza-e izomorfia erejéig a „képet".

Ha $\psi : G \to H$ egy csoporthomomorfizmus, akkor, miként lineáris algebrában, legyen

$$\mathrm{Ker}(\psi) = \{a \in G \mid \psi(a) = e_H\} \leq G$$

a $\psi$ *magja* (ez nyilván részcsoport $G$-ben), és

$$\mathrm{Im}(\psi) = \{\psi(a) \mid a \in G\} \leq H$$

a $\psi$ *képe* (ez nyilván részcsoport $H$-ban). Ha $\psi$ szürjektív, vagyis ha $\mathrm{Im}(\psi) = H$, akkor azt mondjuk, hogy $\psi$ a $H$-**ra** (és nem $H$-**ba**) képez.

Könnyű látni, hogy $H$ minden részcsoportja előáll alkalmas homomorfizmus képeként. Valóban, ha $K \leq H$, akkor az a $\psi : K \to H$ leképezés, ami $K$ minden eleméhez önmagát rendeli, nyilván csoporthomomorfizmus, melynek képe $K$. Nézzük meg, magja lesz-e minden részcsoport is egy alkalmas homomorfizmusnak.

Tegyük fel, hogy $N \leq G$ a $\psi$ homomorfizmus magja. Ha $h \in \mathrm{Im}(\psi)$, akkor $G$ mely elemei képződnek $h$-ra? Legyen $\psi(g) = h$, ekkor

$$\psi(g') = h \Longleftrightarrow \psi(g') = \psi(g) \Longleftrightarrow \psi(g^{-1}g') = e_H \Longleftrightarrow g^{-1}g' \in \mathrm{Ker}(\psi) = N \Longleftrightarrow g' \in gN\,.$$

Tehát $h$-ra épp a $gN$ mellékosztály elemei képződnek.

Ez az eredmény gyanús! Mi okozza azt az aszimmetriát, hogy *bal* mellékosztály jött ki? A dolgok természete, vagy a mi számolási módszerünk? A $\psi(g') = \psi(g)$ összefüggést ebben a számolásban balról szoroztuk $\psi(g^{-1})$-gyel. Most szorozzuk jobbról.

$$\psi(g') = h \Longleftrightarrow \psi(g') = \psi(g) \Longleftrightarrow \psi(g'g^{-1}) = e_H \Longleftrightarrow g'g^{-1} \in \mathrm{Ker}(\psi) = N \Longleftrightarrow g' \in Ng\,.$$

Most az jött ki, hogy $h$-ra épp az $Ng$ mellékosztály elemei képződnek. Tehát $gN = Ng$ minden $g \in G$ elemre. Így az $N$ szerinti jobb- és baloldali mellékosztályok megegyeznek. Ez a tulajdonság nem teljesül minden részcsoportra, például az $S_3$ csoport $\{id, (12)\}$ részcsoportjára sem. Tehát ez a részcsoport nem lesz homomorfizmusnak magja.

Vigyázzunk, $gN = Ng$ nem jelenti azt, hogy $N$ minden eleme felcserélhető $g$-vel, hanem csak azt, hogy minden $n \in N$-hez van olyan $n' \in N$, hogy $gn = n'g$, és fordítva, minden $n$-hez van olyan $n''$, hogy $ng = gn''$. Példaként ellenőrizzük ezt a tulajdonságot az $S_3$ csoportban, ha $N = \{id, (123), (132)\}$ és $g = (12)$.

Az, hogy az $N$ szerinti jobb és bal mellékosztályok megegyeznek, formálisan csak annyit jelent, hogy minden $g$-hez van olyan $g'$, hogy $gN = Ng'$. Ebből azonban következik, hogy $gN = Ng$. Valóban, $g \in gN = Ng'$, és nyilván $g \in Ng$, vagyis az $Ng$ és $Ng'$ mellékosztályok nem diszjunktak, tehát egyenlőek.

A $G$ csoport egy $N$ részcsoportját akkor nevezzük *normális részcsoportnak,* vagy *normálosztónak,* ha egy alkalmas, $G$-n értelmezett homomorfizmusnak a magja (jelölés: $N \lhd G$).

**5.1. Tétel.** *A $G$ csoport $N$ részcsoportja akkor és csak akkor normálosztó, ha a szerinte vett bal- és jobboldali mellékosztályok megegyeznek.*

*Bizonyítás.* Tegyük fel, hogy az $N \leq G$ részcsoportra $gN = Ng$ teljesül minden $g \in G$ esetén. Szeretnénk egy olyan $\psi : G \to H$ homomorfizmust konstruálni, melynek magja $N$. Ahhoz, hogy ezt megtehessük, tegyük fel, hogy a célt sikerült elérni, és vizsgáljuk meg, hogy milyen a kapott $\psi$ és $H$. Így ki fog derülni, hogyan kell őket megkonstruálni. Azért, hogy az alábbiakban ne keveredjenek össze a bizonyítás valódi lépései a motivációval, a konstrukció során egy $K$ csoportot, és egy $\varphi : G \to K$ homomorfizmust fogunk építeni, melynek magja $N$ lesz.

A $H$ „felesleges", azaz $\mathrm{Im}(\psi)$-n kívüli elemeit nem akarjuk megkonstruálni, ezért ezeket elhagyva feltehetjük, hogy $\psi$ szürjektív. Láttuk, hogy ha $h \in H$, akkor pontosan egy $N$ szerinti mellékosztály elemei képződnek $h$-ra. Azaz $H$ elemei kölcsönösen egyértelmű

megfeleltetésben állnak az $N$ szerinti mellékosztályokkal. Így megvannak már a keresett $K$ csoport elemei: ezek legyenek az $N$ szerinti mellékosztályok; és megvan a keresett $\varphi$ leképezés is, ennek nyilván a $g$ elemhez az ő mellékosztályát, azaz a $gN = Ng$ halmazt kell rendelnie.

Hogyan kaphatjuk meg a $G$-beli szorzás ismeretében a $h_1, h_2 \in H$ elemek szorzatát? Ha $\psi(g_1) = h_1$ és $\psi(g_2) = h_2$, akkor

$$h_1 h_2 = \psi(g_1)\psi(g_2) = \psi(g_1 g_2)\,,$$

vagyis a $h_1 h_2$ szorzatnak a $g_1 g_2 N$ mellékosztály felel meg. Ezért a $K$ csoportban két mellékosztály szorzatát a

$$(g_1 N) \cdot (g_2 N) = g_1 g_2 N$$

képlettel kell, hogy definiáljuk. Azt várjuk, hogy csoportot kapunk, és a $\varphi(g) = gN$ leképezés csoporthomomorfizmus, melynek magja $N$.

Még a csoportaxiómák ellenőrzése **előtt** van egy probléma. Szabad-e így a műveletet definiálnunk? A problémát a következő hasonlat világítja meg. Az, hogy „narancsszín", egy értelmes fogalom: ez tetszőleges narancsnak a színét jelenti. Hasonlóan azonban nem definiálhatjuk az „autószín" fogalmát, hiszen az autók színe nem egyforma.

Másik köznapi példa a következő. Ha adott a gyerekek halmazán egy kétváltozós reláció, és van két iskolai osztályunk, akkor megpróbálhatjuk értelmezni a relációt a két osztály között is a következő módon: kiveszünk egy-egy gyereket mindkét osztályból, és megnézzük, hogy ők ketten relációban vannak-e. Például ha a reláció az, hogy „idősebb korosztályhoz tartozik", akkor ez a teszt (normális esetben) ugyanazt az eredményt fogja adni, bárhogy is veszünk ki egy-egy gyereket, és így értelmes arról beszélni, hogy a 7/B idősebb korosztályhoz tartozik, mint a 6/A. De a fenti definíció alapján értelmetlen arról beszélni, hogy az egyik osztály „jobb tanuló", mint a másik, hiszen abból, hogy Jancsi a 7/A-ból jobb tanuló, mint Juliska a 6/B-ből még nem következik, hogy a 7/A-ban mindenki jobb tanuló, mint a 6/B-ben.

Amikor a $g_1 N$ és $g_2 N$ mellékosztályokat akarjuk összeszorozni, akkor a probléma hasonló: ugyanazt az eredményt kapjuk-e, ha e két mellékosztályt másik elemmel adjuk meg. Be kellene látni, hogy a szorzat csak a mellékosztálytól függ, nem pedig a $g_i$ elemektől. Vagyis, hogy

$$g_1 N = g_1' N \text{ és } g_2 N = g_2' N \implies g_1 g_2 N = g_1' g_2' N\,.$$

Ha ez igaz, akkor a szorzás definíciója értelmes.

A fenti következtetés nem igaz tetszőleges részcsoportra (például az $S_3$ csoport $\{id, (12)\}$ részcsoportjára sem). Ha azonban $gN = Ng$ minden $g \in G$-re, akkor

$$g_1 g_2 N = g_1 g_2' N = g_1 N g_2' = g_1' N g_2' = g_1' g_2' N\,,$$

azaz a szorzás a $K$ halmazon jóldefiniált. Az összes többi tulajdonság triviálisan teljesül: a szorzás nyilván asszociatív, az egységelem $eN = N$, a $gN$ inverze $g^{-1}N$ (ez ismét nem függ $g$-től, csak a mellékosztálytól), és $\psi$ is nyilvánvalóan szorzástartó. Nyilván $g \in \mathrm{Ker}(\psi)$ akkor és csak akkor, ha $gN = eN$, vagyis ha $g \in N$. Azaz $\mathrm{Ker}(\psi) = N$, és ezzel a tételt beláttuk. □

A most konstruált csoportot a $G$ csoport $N$ szerinti *faktorcsoportjának* nevezzük, és $G/N$-nel jelöljük. Ha $G$ véges, akkor persze $|G/N| = |G : N| = |G|/|N|$. A $\varphi : g \mapsto gN$ leképezés neve *természetes homomorfizmus.*

Az iménti gondolatmenet során az is kiderült, hogy ha $\psi : G \to H$ tetszőleges homomorfizmus, és $N = \mathrm{Ker}(\psi)$, akkor $\mathrm{Im}(\psi)$ elemei kölcsönösen egyértelmű, művelettartó megfeleltetésben állnak a $K = G/N$ csoport elemeivel (a $\psi(g)$ elemnek a $gN = Ng$ felel meg), vagyis, hogy $\mathrm{Im}(\psi) \cong K = G/N$. Azaz:

**5.2. Homomorfizmus-tétel.** *Ha $\psi : G \to H$ homomorfizmus, akkor* $\mathrm{Im}(\psi) \cong G/\mathrm{Ker}(\psi)$.

Ez az állítás a dimenziótétel csoportelméleti analogonja. Maga a faktorcsoport az algebra egyik legfontosabb fogalma. A faktorcsoportban az osztályok elemeivel (úgynevezett reprezentánsokkal) kell tehát számolni. Minél ügyesebben választjuk ezeket a reprezentánsokat, annál egyszerűbb a számolás.

**5.3. Állítás.** *Legyen $N \lhd G$ és $g \in G$. Ekkor a $gN \in G/N$ elem rendje a legkisebb olyan pozitív $k$ egész, melyre $g^k \in N$, és végtelen, ha ilyen $k$ nem létezik.*

*Bizonyítás.* Valóban, $(gN)^n = eN \iff g^n \in N$, és $k$ a legkisebb ilyen pozitív $n$. □

Hasonlóan igazolható az is, hogy ha egy $g$ elem képe egy homomorfizmusnál $h$, akkor $h$ rendje osztója $g$ rendjének.

## VI. Hogyan keressünk normálosztót?

Van egy nagyon egyszerű eset, ami azonban gyakran előfordul, ezért célszerű ismerni.

**6.1. Állítás.** *Tetszőleges csoportban minden 2 indexű részcsoport normálosztó.*

*Bizonyítás.* Ha $|G : N| = 2$, akkor $G$-nek két baloldali mellékosztálya van $N$ szerint. Az egyik $N$, a másik tehát $N$ komplementuma, azaz $G - N$. Ugyanez azonban a jobboldali mellékosztályokra is igaz. Tehát a baloldali és a jobboldali mellékosztályok halmaza is $\{N, G - N\}$. Ezért $N \lhd G$. □

Az általános esetben úgy érhetünk célt, ha a $gN = Ng$ feltételt átfogalmazzuk.

**6.2. Lemma.** *A $G$ csoport $N$ részcsoportja akkor és csak akkor normálosztó, ha minden $a \in N$, $g \in G$ esetén $gag^{-1} \in N$.*

*Bizonyítás.* A lemma feltételét komplexusokkal úgy írhatjuk fel, hogy $gNg^{-1} \subseteq N$. Ez igaz minden $g$-re, tehát $g^{-1}$-re is, azaz $g^{-1}Ng \subseteq N$, ahonnan balról $g$-vel, jobbról $g^{-1}$-gyel szorozva $N \subseteq gNg^{-1}$ adódik. Tehát a lemma feltétele azzal ekvivalens, hogy $gNg^{-1} = N$ minden $g \in G$-re. Ez pedig pontosan akkor igaz, ha $gN = Ng$ (csak $g$-vel, illetve a megfordításhoz $g^{-1}$-gyel kell jobbról szorozni). □

A $gag^{-1}$ szorzatot *az $a$ elem $g$-vel vett konjugáltjának* nevezzük. Az előző lemma tehát azt mondja, hogy a normálosztók pontosan a konjugálásra zárt részcsoportok. A konjugált képlete a lineáris algebrában a bázistranszformációt írta le, ami a teljes mátrixalgebra önmagára való izomorfizmusát létesítette. A konjugálás csoportok esetében is izomorfizmus lesz, és ennek fontos következményei vannak (például konjugáláskor az elemrend nem változik meg).

**6.3. Állítás.** *Ha $G$ csoport és $g \in G$, akkor a*

$$\psi_g : x \mapsto gxg^{-1}$$

*leképezés a $G$ csoportot önmagára képző izomorfizmus.*

*Bizonyítás.* $\psi_g(x)\psi_g(y) = gxg^{-1}gyg^{-1} = gxyg^{-1} = \psi_g(xy)$. Mivel a $g$-vel való konjugálás inverze a $g^{-1}$-gyel való konjugálás, ezért a konjugálás bijekció. □

Lineáris algebrában két mátrixot hasonlónak nevezünk, ha ugyanannak a lineáris transzformációnak a mátrixai, csak más-más bázisban. Ez ekvivalencia-reláció (és a cél az volt, hogy adott mátrixhoz megtaláljuk a hozzá hasonlók közül a legszebb, lehetőleg diagonális alakú mátrixot). A bázistranszformáció képlete miatt ezt az ekvivalencia-relációt a konjugálás adja meg.

Egy $G$ csoportban az $a$ és $b$ elemeket akkor nevezzük konjugáltaknak, ha van olyan $g \in G$, melyre $gag^{-1} = b$. Ez is ekvivalencia-reláció lesz. Valóban, $eae^{-1} = a$ miatt minden elem konjugált önmagával, a szimmetria abból következik, hogy $b = gag^{-1}$ esetén $a = (g^{-1})b(g^{-1})^{-1}$ (vagyis ha a $g$ elem „odakonjugál", akkor az inverze „visszakonjugál"), végül a tranzitivitás abból következik, hogy ha $g$ az $a$-t $b$-be konjugálja, $h$ pedig a $b$-t $c$-be, akkor a $hg$ elem $a$-t $c$-be konjugálja.

Az így kapott osztályokat a $G$ *konjugált osztályainak* nevezzük. A 6.2 Lemma tehát úgy fogalmazható, hogy *egy $N$ részcsoport akkor és csak akkor normálosztó $G$-ben, ha a $G$ néhány konjugált osztályának egyesítése.* Normálosztók kereséséhez tehát célszerű a csoportot konjugált osztályokra bontani. Ehhez viszont jó lenne tudni, hány eleme van egy adott $a$ elem konjugált osztályának.

Tekintsük azokat a $g \in G$ elemeket, amelyek $a$-val felcserélhetők, azaz amelyekre $ga = ag$ teljesül. Ezek a $g$ elemek az $a$ elem $G$-beli *centralizátorát* alkotják, melynek jele $C_G(a)$.

Az $a$ elem centralizátora részcsoport. Ha ugyanis $g$ és $h$ mindketten felcserélhetők $a$-val, akkor $gh$ is, hiszen ekkor

$$a(gh) = gah = (gh)a\,.$$

Továbbá ha $ag = ga$, akkor mindkét oldalról $g$ inverzével szorozva $g^{-1}a = ag^{-1}$ adódik. Azaz $g^{-1} \in C_G(a)$.

**6.4. Állítás.** *A $G$ véges csoport $a$ elemének éppen annyi különböző konjugáltja van $G$-ben, mint az $a$ centralizátorának indexe, azaz $|G : C_G(a)|$. Speciálisan minden konjugált osztály elemszáma osztója $G$ rendjének.*

*Bizonyítás.* Legyen $b = gag^{-1}$. Vizsgáljuk meg, mely $h$ elemek konjugálják még az $a$-t $b$-be. Nyilván

$$hah^{-1} = gag^{-1} \iff g^{-1}ha = ag^{-1}h \iff g^{-1}h \in C_G(a) \iff h \in gC_G(a)\,.$$

Tehát az $a$-t $b$-be vivő $h$ elemek egy $C_G(a)$ szerinti baloldali mellékosztályt alkotnak. Vagyis az a megfeleltetés, ami a $b$ elemhez a $gC_G(a)$ mellékosztályt rendeli, bijekció az $a$ konjugált osztálya és $C_G(a)$ baloldali mellékosztályainak halmaza között. □

Remélem, többen fejcsóválva olvassák az eddigieket, mert felismerték, hogy egy korábbi bizonyítást mondtunk el mégegyszer. Már az a mód is szemet kell szúrjon, ahogy a konjugált osztályokat definiáltuk, hiszen azt mondtuk: $a$ és $b$ egy osztályban van, ha $G$ egy eleme konjugálással az egyiket a másikba *viszi*. A megfeleltetés a konjugált osztály elemei és egy részcsoport szerinti mellékosztályok között pedig teljesen ugyanaz, mint mikor az orbitok elemszámát vizsgáltuk meg.

A fenti számolásokat tehát el lehet kerülni, ha definiáljuk a csoport önmagán való hatását konjugálás segítségével. Ha $g \in G$, akkor legyen $X = G$, és

$$g * x = gxg^{-1} \quad (x \in G)\,.$$

Ezzel tényleg hatást kaptunk: ha $g, h, x \in G$, akkor

$$(gh) * x = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = g * (h * x)\,,$$

ha pedig $e$ a $G$ egységeleme, akkor

$$e * x = exe^{-1} = x\,.$$

Az ebből a hatásból keletkező orbitok $G$ konjugált osztályai egy elem stabilizátora pedig nyilvánvalóan a centralizátora. A 6.4. Állítás tehát következik a 3.2. Tételből.

Könnyű számolás mutatja (jó gyakorlófeladat ezt elvégezni), hogy az $S_n$ csoportban két elem akkor és csak akkor konjugált, ha ciklusfelbontásuk „egyforma" (azaz ugyananyi, ugyanolyan hosszú ciklus szerepel bennük).

Külön figyelmet érdemelnek az egyelemű konjugált osztályok. Az $x$ elem osztálya akkor és csak akkor ilyen, ha $x$ centralizátorának indexe 1, azaz ha ez a centralizátor az egész csoport, vagyis ha $x$ felcserélhető $G$ minden elemével. Az ilyen elemek halmazát $G$ *centrumának* nevezzük, és $Z(G)$-vel jelöljük.

$Z(G)$ nyilván részcsoportja $G$-nek (ez közvetlen számolással is látható, vagy pedig abból következik, hogy a centrum nyilván az összes elem centralizátorainak a metszete). Nyilvánvalóan $Z(G) \triangleleft G$, hiszen $Z(G)$ (egyelemű) konjugált osztályok egyesítése. Hasonló okokból $Z(G)$ minden részcsoportja normálosztó $G$-ben.

Mostanáig csak átfogalmazásokat végeztünk. Az algebrában gyakran megtörténik, hogy ilyen egyszerű lépések sorozatával olyan tételig jutunk el, aminek a bizonyítását mégsem tudnánk olyan könnyen kitalálni. Most is ez a helyzet, lényegében minden eszközünk megvan ahhoz, hogy megértsük a prímnégyzet rendű csoportok szerkezetét.

Legyen $p$ prímszám. Azt mondjuk, hogy a $G$ véges csoport *$p$-csoport*, ha $G$ rendje $p$-nek hatványa. Az egyelemű csoportot minden $p$-re $p$-csoportnak tekintjük.

**6.5. Tétel.** *Ha $p$ prím és $P$ nem egyelemű $p$-csoport, akkor $Z(P)$ sem egyelemű.*

*Bizonyítás.* Bontsuk fel $P$-t konjugált elemosztályainak uniójára. Vonjuk egybe az egyelemű osztályokat, ezek $P$ centrumát alkotják. Ha $K_1, \ldots, K_m$ a többi konjugált osztály, akkor tehát

$$|P| = |Z(P)| + |K_1| + \cdots + |K_m|$$

(ezt $P$ *osztályegyenletének* nevezzük).

Tudjuk, hogy $K_i$ elemszáma osztója $P$ rendjének, és mivel $|K_i| > 1$, azt kapjuk, hogy $|K_i|$ osztható $p$-vel. Mivel $|P|$ is osztható $p$-vel, az osztályegyenletből kapjuk, hogy $|Z(P)|$ is osztható $p$-vel. Ekkor pedig $Z(P)$ nem lehet egyelemű. □

**6.6. Következmény.** *Minden prímnégyzet rendű csoport kommutatív.*

*Bizonyítás.* Legyen $P$ egy $p^2$ rendű csoport, ahol $p$ prím. Ekkor $Z(P)$ elemszáma az előző tétel és Lagrange tétele szerint vagy $p$, vagy $p^2$. Az utóbbi esetben készen vagyunk, hiszen $Z(P)$ kommutatív, az előbbit kell kizárnunk. Legyen $e \neq g \in Z(P)$, és $h \in G$, $h \notin Z(P)$. Ekkor $gh = hg$, hiszen $g$ a centrumban van. Ezért a

$$H = \langle g, h \rangle = \{g^n h^m \mid n, m \in \mathbb{Z}\}$$

halmaz egy kommutatív részcsoportja $P$-nek. A $H$ részcsoport tartalmazza $Z(P)$-t (hiszen a prímrendű $Z(P)$-t már $g$ hatványai is kiadják), sőt, a $h$ elem miatt bővebb $Z(P)$-nél. Így $H$ rendje csakis $p^2$ lehet. Ezért $H = P$, vagyis $P$ Abel. Ekkor azonban $Z(P) = P$, azaz a centrum mégsem $p$ rendű. Ez az ellentmondás bizonyítja az állítást. □

Gyakorlásul általánosítsuk a mostani gondolatmenetet, és igazoljuk, hogy ha egy $G$ véges csoportban $G/Z(G)$ ciklikus, akkor $G$ Abel (és így $G/Z(G)$ az egyelemű csoport).

A konjugálás, mint izomorfizmus, részcsoportot részcsoportba visz. Ha $H \leq G$, akkor a $gHg^{-1}$ részcsoportot a $H$ részcsoport $G$-vel vett konjugáltjának nevezzük. Ahogy sikerült egy elem konjugáltjait megszámolni, ugyanúgy megszámolhatjuk egy tetszőleges részhalmaz konjugáltjait is. Legyen $X$ a $G$ összes részhalmazainak halmaza, és hasson $X$-en $G$ a konjugálással:

$$g * A = gAg^{-1}$$

($g \in G$, $A \subseteq G$). Most tehát a „pontok" maguk is halmazok. Könnyen ellenőrizhető, hogy hatást kaptunk. Ha $A \in X$, akkor az $A$ konjugáltjainak a száma éppen az $A$ orbitjának az elemszáma, vagyis az $A$ stabilizátorának az indexe. Az $A$ stabilizátora azokból a $g \in G$ elemekből áll, melyekre $gAg^{-1} = A$ (vagyis átrendezve $gA = Ag$). Ezt a részcsoportot az $A$ részhalmaz *normalizátorának* nevezzük, és $N_G(A)$-val jelöljük. Tehát az $A$ normalizátora az $A$-val *mint halmazzal* felcserélhető elemekből álló részcsoport. A következő eredményt láttuk be:

**6.7. Állítás.** *A $G$ véges csoport $A$ részhalmazának éppen annyi különböző konjugáltja van $G$-ben, mint az $A$ normalizátorának indexe, azaz $|G : N_G(A)|$. Speciálisan $A$ konjugáltjainak száma osztója $G$ rendjének.*

Gyakorlásul lássuk be, hogy ha $H \leq G$, akkor $N_G(H)$ a legnagyobb olyan részcsoportja $G$-nek, melyben $H$ normálosztó (innen származik a normalizátor elnevezés). Természetesen ilyenkor $H \leq N_G(H)$.

## VII. Egyszerű és feloldható csoportok

Minden csoportban nyilván normálosztó a két triviális részcsoport. Ha egy csoportnak csak ez a két normálosztója van, akkor a csoportot *egyszerű csoportnak* nevezzük (az egyelemű csoportot tehát nem tekintjük egyszerűnek). Bizonyos értelemben minden véges csoport felépíthető egyszerű csoportok segítségével, és ezért az egyszerű csoportok meghatározása a csoportelmélet alapvető feladata.

**7.1. Állítás.** *A kommutatív egyszerű csoportok éppen a prímrendű csoportok.*

*Bizonyítás.* Valóban, kommutatív csoportban $gN = Ng$ mindig teljesül, ezért minden részcsoport normálosztó. Ezek a csoportok tehát azok, aminek csak a két triviális részcsoportja van, vagyis a 2.7. Következmény szerint pontosan a prímrendű ciklikus csoportok. □

**7.2. Állítás.** *Ha $p$ prím, akkor a véges egyszerű $p$-csoportok éppen a prímrendű csoportok.*

*Bizonyítás.* Ha $P$ egyszerű $p$-csoport, akkor a 6.5. Tétel miatt $|Z(P)| > 1$. Mivel $Z(P) \lhd P$, és $P$ egyszerű, ezért $Z(P) = P$, vagyis $P$ kommutatív. Ezért az előző állítást alkalmazhatjuk. □

Nemkommutatív egyszerű csoportot nem is olyan könnyű találni. Egy ilyen csoport rendjének Burnside egy nevezetes tétele szerint legalább három különböző prímosztója kell, hogy legyen, és ez a rend a Feit-Thompson tétel (10.1) szerint biztosan páros szám. A legkisebb nemkommutatív véges egyszerű csoportnak hatvan eleme van, és ezt a csoportot már nagyon jól ismerjük.

**7.3. Tétel.** *Az $A_n$ alternáló csoport $n \geq 5$ esetén nemkommutatív egyszerű csoport.*

A tétel bizonyítása megtalálható a Fuchs-jegyzetben. A véges egyszerű csoportok osztályozásáról a X. Fejezetben lesz részletesebben szó.

Ha adott egy $G$ csoport, ami nem egyszerű, akkor vegyünk egy nemtriviális $N$ normálosztót, és tekintsük az $N$ és $G/N$ csoportokat. Ha még ezek sem egyszerűek, folytassuk az eljárást. Ha $G$ véges, akkor előbb-utóbb már csupa egyszerű csoporthoz jutunk. A kapott egyszerű csoportok sokat elárulnak $G$ szerkezetéről. Kicsit pontosabban, $G$ *normálláncának* nevezzük $G$ részcsoportjainak egy olyan sorozatát, melyre

$$\{e\} = N_k \lhd N_{k-1} \lhd \ldots \lhd N_2 \lhd N_1 \lhd N_0 = G\,.$$

Ha az összes $N_i/N_{i+1}$ faktorcsoport egyszerű, akkor az ilyen láncot $G$ *kompozícióláncának* nevezzük, ezeket az egyszerű faktorcsoportokat pedig $G$ *kompozíció-faktorainak.*

Például az $A_4$ alternáló csoport esetén a következő láncot kaphatjuk:

$$\{e\} \lhd \{id, (12)(34)\} \lhd \{id, (12)(34), (13)(24), (14)(23)\} \lhd A_4\,.$$

Megjegyezzük, hogy $\{id, (12)(34)\}$ nem lesz normálosztó $A_4$-ben (ezt jó gyakorlás ellenőrizni). Láthatjuk tehát, hogy a kapott $N_i$ részcsoportok általában nem lesznek $G$ normálosztói (csak annyit tudunk, hogy $N_i \lhd N_{i-1}$, azaz mindegyik $N_i$ az előzőben lesz normálosztó). A $\lhd$ reláció általában nem tranzitív!

A normállánc, sőt a kompozíciólánc sem egyértelmű általában. Például a $\mathbb{Z}_6^+$ csoportnál eljárhatunk kétféleképpen is:

$$\{e\} \lhd \{0,3\} \lhd \mathbb{Z}_6^+\,, \qquad \{e\} \lhd \{0,2,4\} \lhd \mathbb{Z}_6^+\,.$$

A kompozíció-faktorok mindkét lánc esetében $\mathbb{Z}_2^+$ és $\mathbb{Z}_3^+$. Általában is igaz, hogy *ha a felbontást másképp végezzük, akkor ugyanazok az egyszerű csoportok jönnek ki kompozíció-faktorokként, csak esetleg más sorrendben.* Ez Jordan-Hölder nevezetes tétele (a bizonyítás megtalálható a Fuchs: Algebra jegyzetben).

A kompozíció-faktorok sok információt szolgáltatnak a csoportról, de nem határozzák meg a szerkezetét. Például az $S_3$ csoport esetén

$$\{e\} \lhd \{id, (123), (132)\} \lhd S_3$$

kompozíciólánc, a faktorok most is $\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$, mint $\mathbb{Z}_6^+$ esetében, ugyanakkor $S_3 \ncong \mathbb{Z}_6^+$.

A véges $G$ csoportot *feloldhatónak* nevezzük, ha van olyan kompozíciólánca, melyben a szereplő faktorcsoportok mindegyike prímrendű ciklikus csoport (vagyis ha a kompozíció-faktorai között nincs nemkommutatív egyszerű csoport). A feloldható csoportok fontos szerephez jutnak az egyenletek gyökképleteinek vizsgálatában (és a geometriai szerkesztések elméletében is). Az, hogy pontosan a legfeljebb negyedfokú egyenletekre van általános megoldóképlet, az alábbi tételnek a következménye:

**7.4. Tétel.** *Az $S_n$ szimmetrikus csoport akkor és csak akkor feloldható, ha $n \leq 4$.*

Az, hogy $n \leq 4$ esetén $S_n$ feloldható, a fenti példák már lényegében mutatják (gyakorlásul egészítsük ki a gondolatmenetet). Ha viszont $n \geq 5$, akkor $S_n$-nek kompozíciólánca lesz $\{e\} \lhd A_n \lhd S_n$, és így kompozíció-faktora a nemkommutatív egyszerű $A_n$ csoport.

A véges Abel-csoportok feloldhatók, hiszen kompozíció-faktoraik kommutatív egyszerű csoportok, azaz a 7.1. Állítás miatt prímrendű ciklikusak. Szintén feloldhatók a prímhatványrendű csoportok. Valóban, legyen $P$ tetszőleges $p$-csoport, és készítsük el $P$ egy kompozícióláncát. Ebben a faktorok rendje osztója $|P|$-nek, azaz mindegyik ilyen $F$ faktorcsoport egyszerű $p$-csoport. A 7.2. Állítás miatt $F$ rendje $p$. Ez a $P$ kompozícióláncának minden faktorára igaz, tehát $P$ feloldható.

Hasonló gondolatmenet mutatja, hogy minden páratlan rendű csoport feloldható (ennek bizonyításához a Feit-Thompson tételt kell felhasználni).

## VIII. A Sylow-tételek

A Lagrange-tétel megfordítása általában nem igaz. Ha $G$ véges csoport, és $d$ osztója $G$ rendjének, akkor nem feltétlenül van $G$-ben sem $d$ rendű elem, sem $d$ rendű részcsoport. Például az $A_5$ csoportban nincsen 30 rendű részcsoport, és így 30 rendű elem sem, hiszen minden kettő indexű részcsoport normálosztó a 6.1. Állítás miatt, márpedig az $A_5$ egyszerű csoport. Ha azonban $d$ egy $p$ prím hatványa, akkor mindig van $d$ rendű részcsoport, sőt ezek száma kongruens 1-gyel modulo $p$. Ez Sylow nevezetes tétele, melyet most bebizonyítunk.

**8.1. Lemma.** *Legyenek $G$ és $H$ egyforma rendű véges csoportok, és $q$ egy $p$ prím hatványa, mely osztja ezt a közös rendet. Jelölje $n_G$ illetve $n_H$ a $G$ illetve $H$ azon részcsoportjainak számát, melyek rendje $q$. Ekkor $n_G \equiv n_H (p)$.*

Ez a lemma azért jó, mert ha speciálisan $H$ a ciklikus csoport, akkor az $n_H$ értékét ismerjük: a 2.9. Állítás szerint $n_H = 1$ (tetszőleges $q$ esetén). Ezért a következő állítást kapjuk:

**8.2. Tétel.** *Ha a $p$ prím egy $q$ hatványa osztja a $G$ véges csoport rendjét, akkor van $G$-ben $q$ rendű részcsoport, és ezek száma kongruens 1-gyel modulo $p$.*

Természetesen ha tudjuk, hogy $n_G$ kongruens 1-gyel modulo $p$, akkor $n_G$ nem lehet nulla, tehát nem kell külön bebizonyítani, hogy van $q$ rendű részcsoport.

Lássuk akkor be a 8.1. Lemmát. Jelölje $X$ a $G$ összes $q$-elemű részhalmazaiból álló halmazt. Hasson $G$ az $X$-en balszorzással:

$$g * A = gA \quad (= \{ga \mid a \in A\})$$

(itt $g \in G$, $A \in X$). A „pontok" tehát ismét halmazok, és könnyen ellenőrizhetjük, hogy ez tényleg hatás.

Először vizsgáljuk azokat az orbitokat, amelyek valamelyik eleme egy $K$ részcsoport (még nem tudjuk, van-e ilyen orbit). Ekkor az orbit többi eleme $gK$ alakú, azaz ennek az orbitnak az elemei éppen a $K$ szerinti bal mellékosztályok. Ezért ennek az orbitnak az elemszáma $|G : K| = |G|/q$, és az orbitban az egyetlen részcsoport a $K$, vagyis az ilyen orbitok száma $n_G$.

Most tegyük fel, hogy az $A = \{a_1, \ldots, a_q\} \in X$ elem orbitjának egyetlen eleme sem részcsoport. Tekintsük az $A$ „pont" $G_A$ stabilizátorát. Ez azokból a $g \in G$ elemekből áll, melyekre $gA = A$. Ezért

$$A = G_A A = G_A a_1 \cup \cdots \cup G_A a_q \,,$$

vagyis az $A$ halmaz $G_A$ szerinti jobb mellékosztályok egyesítése. Jelölje az ebben az unióban szereplő *különböző* mellékosztályok számát $m_A$, akkor tehát $q = |A| = m_A \cdot |G_A|$. Ha $m_A = 1$ lenne, azaz ha $A = G_A a$ alkalmas $a \in A$ esetén, akkor az $a^{-1}A = a^{-1}G_A a$ halmaz benne van $A$ orbitjában, és részcsoport. Ez ellentmondás, tehát $m_A > 1$, és így $m_A \mid q$ miatt $m_A$ osztható $p$-vel. Az $A$ orbitjának elemszáma pedig

$$|G(A)| = |G : G_A| = \frac{|G|}{|G_A|} = \frac{|G| m_A}{q} \,.$$

Tudjuk, hogy az orbitok elemszámának összege kiadja az alaphalmaz, azaz $X$ elemszámát. Jelöljük a $|G|/q$ számot $t$-vel, akkor tehát minden részcsoportot tartalmazó orbit elemszáma $t$, és ezeknek az összhossza $n_G t$. A többi orbit hossza $t m_A$ alakú, ahol $m_A$ egy $p$-vel osztható szám. Ezért

$$|X| = t n_G + t p x_G \,,$$

ahol $x_G$ valamilyen egész szám (ami a $G$ csoporttól függ).

Ugyanez a gondolatmenet a $H$ csoportra is elmondható:

$$|X| = t n_H + t p x_H \,,$$

ahol $x_H$ valamilyen egész szám. A két egyenlőséget összevetve és $t$-vel osztva éppen a 8.1. Lemma állítása adódik. □

Legyen a $G$ véges csoport rendjének prímtényezős felbontása $|G| = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. A $p_i^{\alpha_i}$ rendű részcsoportokat a $G$ csoport *$p_i$-Sylow részcsoportjainak* nevezzük.

**8.3. Lemma.** *Legyen $G$ véges csoport, $Q \leq G$ egy $p$-hatványrendű részcsoport, $P$ pedig egy $p$-Sylow részcsoport. Ekkor van olyan $g \in G$, melyre $Q \leq gPg^{-1}$.*

*Bizonyítás.* Legyen $X$ a $P$ részcsoport $G$-beli konjugáltjainak a halmaza:

$$X = \{gPg^{-1} \mid g \in G\}\,.$$

A 6.7. Állítás miatt e halmaz elemszáma éppen $|G : N_G(P)|$. Ez a szám nyilván osztója $|G : P|$-nek (hiszen $|G : P| = |G : N_G(P)| \cdot |N_G(P) : P|$), és mivel $P$ egy $p$-Sylow, $|G : P|$ nem osztható $p$-vel. Ezért $X$ elemszáma sem osztható $p$-vel.

Hasson a $Q$ részcsoport az $X$ halmazon konjugálással, azaz $h \in Q$, $P' \in X$ esetén legyen

$$h * P' = hP'h^{-1}\,.$$

Mivel $Q$ rendje $p$-hatvány, minden stabilizátor indexe (azaz minden orbit elemszáma) szintén $p$-hatvány, tehát vagy $p$-vel osztható, vagy 1. Mivel $|X|$ nem osztható $p$-vel, van olyan orbit, aminek elemszáma 1, azaz aminek a stabilizátora a teljes $Q$. Ha ennek az orbitnak az egyetlen eleme $P' = gPg^{-1}$, akkor tehát azt kaptuk, hogy bármely $h \in Q$ esetén $hP'h^{-1} = P'$, azaz $Q \leq N_G(P')$.

Meg szeretnénk mutatni, hogy valójában $Q \leq P'$ (ezzel készen is lennénk). Tegyük fel, hogy $h \in Q$, és legyen $h$ rendje $m$ (ez a $p$ prím hatványa). Tudjuk, hogy $P' \lhd N_G(P')$, és így beszélhetünk a $hP'$ elem rendjéről az $N_G(P')/P'$ faktorcsoportban (vö. 5.3 Állítás). Mivel $h^m = e$, ezért $(hP')^m = P'$, azaz a $hP'$ elem rendje osztója $m$-nek, és így maga is $p$-hatvány. Másrészt viszont $|P'| = |P|$, ezért a $N_G(P')/P'$ faktorcsoportnak a rendje, azaz $|N_G(P')|/|P'|$ osztója $|G|/|P'| = |G|/|P|$-nek, ami nem osztható $p$-vel. Egy $p$-vel nem osztható rendű csoportban csak az egységelemnek lehet $p$-hatvány a rendje. Ezért $hP'$ az egységelem, $hP' = P'$, ami azt jelenti, hogy $h \in P'$. □

Foglaljuk össze az eddig bizonyítottakat.

**8.4. Sylow tétele.** *Legyen $G$ véges csoport, és $p$ a $G$ rendjének tetszőleges prímosztója. Ekkor igazak a következő állítások.*

(1) *Van $G$-ben $p$-Sylow részcsoport.*
(2) *$G$ minden $p$-hatványrendű részcsoportja része $G$ egy $p$-Sylow részcsoportjának.*
(3) *Bármely két $p$-Sylow részcsoport konjugált $G$-ben.*
(4) *Ha $q$ egy $G$ rendjét osztó $p$-hatvány, akkor a $q$-rendű $G$-beli részcsoportok száma kongruens 1-gyel modulo $p$.*
(5) *A $p$-Sylow részcsoportok száma osztója $|G : P|$-nek.*

*Bizonyítás.* A (4) állítás éppen a 8.2. Tétel, amiből (1) is következik. A (2) és (3) állítások az előző lemmából adódnak, hiszen $p$-Sylow részcsoport minden konjugáltja is $p$-Sylow részcsoport. Végül (5) következik (3)-ból, hiszen tudjuk, hogy egy részhalmaz konjugáltjainak száma a normalizátorának indexe, márpedig ha $P$ egy $p$-Sylow, akkor $|N_G(P) : P|$ osztója $|G : P|$-nek. □

Alkalmazásként mutassuk meg, hogy nincs 100 rendű egyszerű csoport. Valóban, legyen $G$ egy 100 rendű csoport, és jelölje $n$ az 5-Sylow részcsoportok számát $G$-ben. Ekkor az

előző tétel szerint $n \equiv 1\ (5)$, másrészt pedig $n$ osztója minden 5-Sylow indexének. Az 5-Sylowok rendje 25, és így indexük $100/25 = 4$. Ennek osztói $1, 2, 4$, és ezek közül csak az 1 kongruens 1-gyel modulo 5. Ezért $G$-ben egyetlen 5-Sylow van. Ez tehát az összes konjugáltjaival megegyezik, azaz normálosztó. Vagyis egy 100 rendű csoportban mindig van 25 rendű normálosztó, és ezért egy ilyen csoport nem lehet egyszerű.

Gyakorló feladatként igazoljuk, hogy ha egy véges csoport rendje két prím szorzata, akkor a csoport feloldható.

## IX. Véges Abel-csoportok

Ha két csoportról meg akarjuk mutatni, hogy nem izomorfak, akkor rendszerint olyan tulajdonságot keresünk, ami az egyiknek megvan, a másiknak nincs. Például ha az egyikben két negyedrendű elem van, a másikban pedig hat, akkor a két csoport biztos nem izomorf. Az ilyen tulajdonságokat *invariánsoknak* nevezzük. Az előző példában szereplő invariáns a negyedrendű elemek száma volt. De ilyen invariáns a csoport rendje is például, vagy a kommutativitás.

Sajnos az invariánsok módszere nem mindig működik. Ha adott két csoport, melyekről el akarjuk dönteni, hogy izomorfak-e, akkor végigpróbálgathatjuk az ismert invariánsokat. Ha azonban nem találunk eltérést, attól még lehet, hogy a két csoport nem izomorf. Ilyenkor új, még ismeretlen invariánsok után kutathatunk.

Példaként oldjuk meg a vektorterek izomorfiaproblémáját. Két vektortér garantáltan nem lesz izomorf, ha a dimenziójuk különböző, hiszen tanultuk, hogy egy vektortérizomorfizmus, vagyis egy bijektív lineáris leképezés bázist bázisba visz. Tehát egy nagyon hasznos invariáns a dimenzió. De más invariánsra nincs is szükség! Ha két vektortér egyenlő dimenziós, akkor az előírhatósági tétel miatt van közöttük olyan lineáris leképezés, ami bázist bázisba visz, és ez persze bijektív lesz. Vagyis *két vektortér akkor és csak akkor izomorf, ha dimenziójuk egyenlő.* Egy vektortér izomorfia-típusa tehát egyetlen invariánssal, a dimenzióval jellemezhető.

A „legegyszerűbb" $n$-dimenziós vektortér a $T$ test felett az $n$ magas oszlopvektorok $T^n$ tere. És valóban, az egész lineáris algebra kiindulópontja az, hogy tetszőleges vektortér elemei helyett a vele izomorf $T^n$ vektortérben számolunk (úgy, hogy rögzítünk egy bázist, és vesszük a vektorok koordinátáit).

Az elmondottak miatt a vektortér a lehető legegyszerűbb algebrai struktúrák közé tartozik. És noha a véges nemkommutatív csoportok szerkezete nagyon bonyolult lehet, a véges Abel-csoportokra sikerült olyan struktúratételt bizonyítani, ami majdnem olyan egyszerű számolást tesz lehetővé, mint a vektorterek esetében. Most bemutatjuk ezt az eredményt.

Hogyan általánosíthatjuk az oszlopvektor fogalmát? Ezekkel a műveleteket komponensenként végezzük. Ugyanezt akkor is megtehetjük, ha az egyes komponensek csoportokból valók. Legyenek $G_1, \ldots, G_n$ tetszőleges csoportok, és tekintsük a $(g_1, \ldots, g_n)$ sorozatokat, ahol $g_i \in G_i$ minden $i$-re. Ezeknek a sorozatoknak a halmazát $G_1 \times \cdots \times G_n$ jelöli. (A sorozatokat tipográfiai okokból nem oszlopba, mint a vektortereknél, hanem sorba írjuk.) A műveleteket komponensenként definiáljuk:

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n)$$

és

$$(g_1, \ldots, g_n)^{-1} = (g_1^{-1}, \ldots, g_n^{-1})$$

(természetesen az $i$-edik komponensben a $G_i$ csoport műveleteit kell elvégezni). Könnyű látni, hogy csoportot kaptunk, ezt a $G_1, \ldots, G_n$ csoportok *direkt szorzatának nevezzük*, és $G_1 \times \cdots \times G_n$-nel jelöljük. Az egységelem nyilván az, ahol minden komponensbe a megfelelő csoport egységelemét tesszük. Szokásos a direkt szorzatot végtelen sok komponens esetében is definiálni, de erre most nem lesz szükségünk.

A direkt szorzatban általában könnyű számolni. Illusztrációképpen igazoljuk a következő állítást:

**9.1. Állítás.** *A $G_1 \times \cdots \times G_n$ direkt szorzat tetszőleges elemének rendje a komponensei rendjeinek legkisebb közös többszöröse (és végtelen, ha a komponensek között van végtelen rendű is).*

*Bizonyítás.* Nyilván $(g_1, \ldots, g_n)^k = (g_1^k, \ldots, g_n^k)$ akkor és csak akkor az egységelem, ha minden $i$-re $g_i^k$ a $G_i$ egységeleme, azaz ha $|g_i|$ osztója $k$-nak. A legkisebb ilyen pozitív $k$ nyilván a rendek legkisebb közös többszöröse. □

**9.2. Következmény.** *A $G$ és $H$ véges csoportok direkt szorzata akkor és csak akkor ciklikus, ha $G$ és $H$ egymáshoz relatív prím rendű ciklikus csoportok.*

*Bizonyítás.* Legyen $|G| = n$ és $|H| = m$. Ha $g$ generálja $G$-t és $h$ generálja $H$-t, akkor a $(g, h)$ rendje $[n, m]$. Ha $n$ és $m$ relatív prímek, akkor ez egyenlő $nm$-el, tehát a $G \times H$ rendjével. Ezért ekkor $(g, h)$ generálja a direkt szorzatot.

Megfordítva, tegyük fel, hogy $G \times H$ ciklikus, és legyen $(g, h)$ egy generátorelem. Ekkor $g$ rendje osztója $n$-nek, $h$ rendje pedig $m$-nek. Tehát $(g, h)$ rendje (ami $nm$) osztója $[n, m]$-nek. Ez csak úgy lehet, ha $(n, m) = 1$, $|g| = n$, $|h| = m$. □

Ennek az egyszerű észrevételnek van egy nagyon érdekes számelméleti következménye. Emlékezzünk rá, hogy a $\mathbb{Z}_n^\times$ csoport generátorelemeit primitív gyöknek neveztük modulo $n$.

**9.3. Tétel.** *Ha modulo $n$ létezik primitív gyök, akkor $n$ vagy prímhatvány, vagy egy prímhatvány kétszerese.*

Hogyan lehetne ezt a tételt belátni? A számelméletben, amikor megmutattuk, hogy az Euler-függvény multiplikatív, melléktermékként az is kiderült (noha nem ezen a nyelven fogalmaztuk meg), hogy ha $m$ és $n$ relatív prím pozitív egészek, akkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$ (a részletes bizonyítás a Függelékben található).

Tegyük fel, hogy $\mathbb{Z}_{nm}^\times$ ciklikus. Ekkor a $\mathbb{Z}_n^\times$ és a $\mathbb{Z}_m^\times$ csoportoknak is ciklikusaknak, és relatív prím rendűeknek kell lenniük. E csoportok rendjei $\varphi(n)$ és $\varphi(m)$. De ha $n > 2$, akkor $\varphi(n)$ páros. Ezért $m$ és $n$ valamelyike 1 vagy 2 kell, hogy legyen. Ebből pedig a 9.3. Tétel nyilvánvalóan következik.

További vizsgálatokkal igazolható, hogy *pontosan akkor létezik primitív gyök modulo $n$, ha $n = 1$, 2, 4, $p^k$, $2p^k$ alakú, ahol $p$ páratlan prím.*

Ha egy csoportról sikerül belátni, hogy direkt szorzat, akkor ez jó hír, mert a szerkezetét sikerült kisebb (és ezért remélhetőleg egyszerűbb) csoportokéra visszavezetni. Tehát szeretnénk tudni, hogyan lehet felismerni, hogy egy csoport izomorf-e egy direkt szorzattal.

Ehhez kanyarodjunk vissza a lineáris algebrához. Szó volt arról, hogy a $W$ vektortér az $U$ és $V$ alterek direkt összege, ha $U+V = W$ és $U \cap V = \{0\}$. Ezek a feltételek azt garantálják, hogy $W$ minden $w$ eleme egyértelműen felírható $u+v$ alakban, ahol $u \in U$ és $v \in V$. Azaz

$W$ elemei kölcsönösen egyértelmű megfeleltetésben állnak a $(u, v)$ párokkal. Könnyű látni, hogy ha a vektortér-műveleteket ezekre a párokra komponensenként értelmezzük, akkor ez a megfeleltetés művelettartó is.

Hogyan lehetne ezt az észrevételt megfordítani? Tegyük fel, hogy $G = A \times B$, ahol $A$ és $B$ tetszőleges csoportok. Tekintsük az

$$A^* = A \times \{e_B\} = \{(a, e_B) \mid a \in A\}$$
$$B^* = \{e_A\} \times B = \{(e_A, b) \mid b \in B\}$$

halmazokat. Ezekről azonnal látható, hogy igazak az alábbiak:

$$A \cong A^* \lhd G, \quad B \cong B^* \lhd G,$$
$$A^* \cap B^* = \{(e_A, e_B)\}, \quad A^*B^* = G\,.$$

Ezeknek a tulajdonságoknak a bizonyítása nagyon egyszerű, és igencsak javallott gyakorlófeladat. Miként lineáris algebrában is, ezeknek a tulajdonságoknak a megléte már elegendő ahhoz, hogy direkt szorzatot kapjunk.

**9.4. Állítás.** *Legyen $G$ csoport, és tegyük fel, hogy $G$-ben van két normálosztó, $A$ és $B$ úgy, hogy $A \cap B = \{e\}$ és $AB = G$. Ekkor $G \cong A \times B$.*

*Bizonyítás.* A feltétel szerint $G$ minden eleme előáll $ab$ alakban, ahol $a \in A$ és $b \in B$. Ez az előállítás egyértelmű is, ha ugyanis $ab = a'b'$, ahol $a' \in A$ és $b' \in B$, akkor átrendezéssel azt kapjuk, hogy

$$a'^{-1}a = b'b^{-1}\,.$$

Itt a baloldal $A$-nak, a jobboldal $B$-nek eleme. Tehát ez az elem $A \cap B$-ben van, vagyis a feltétel szerint az egységelem. De $a'^{-1}a = e$-ből következik, hogy $a = a'$, és hasonlóan kapjuk, hogy $b = b'$.

Így tehát az a $\psi$ leképezés, melyet a $\psi((a, b)) = ab$ képlet definiál, bijekció az $A \times B$ és $G$ között. Még azt kell belátnunk, hogy $\psi$ szorzattartó. Ehhez először azt igazoljuk, hogy $a \in A$ és $b \in B$ esetén $ab = ba$. Valóban, tekintsük a $aba^{-1}b^{-1}$ elemet. Ezt kétféleképpen is átalakíthatjuk:

$$aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in B\,,$$

hiszen $B$ normálosztó, és ezért zárt az $a$-val való konjugálásra. Viszont

$$aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in A\,,$$

hiszen $A$ is normálosztó, és így zárt a $b$-vel való konjugálásra. Így $aba^{-1}b^{-1} \in A \cap B = \{e\}$, azaz átrendezéssel $ab = ba$.

Végül ha $a, a' \in A$ és $b, b' \in B$, akkor az előbbiek szerint $a'b = ba'$, és ezért

$$\psi((a,b)(a',b')) = \psi((aa', bb')) = aa'bb' = aba'b' = \psi((a,b))\psi((a',b'))\,,$$

amivel az állítást beláttuk. □

Ha nem tudjuk, hogy $AB = G$, akkor a fenti bizonyításból az adódik, hogy $AB$ részcsoport, mely izomorf $A$ és $B$ direkt szorzatával.

Ha az $S_3$ csoportban $A = \{id, (12)\}$ és $B = \{id, (123), (132)\}$, akkor valamennyi feltétel teljesül azzal az egy kivétellel, hogy $A$ nem lesz normálosztó, és természetesen nem igaz, hogy $S_3 \cong A \times B$, hiszen $A \times B \cong \mathbb{Z}_2^+ \times \mathbb{Z}_3^+ \cong \mathbb{Z}_6^+$, az $S_3$ pedig nem ciklikus, hiszen nem is kommutatív. Tehát szükséges feltenni, hogy $A, B \lhd G$.

A többtényezős direkt szorzatot is jellemezhetjük normálosztók segítségével. Legyen $G_i^*$ a $G_1 \times \cdots \times G_n$ direkt szorzat azon elemeinek a halmaza, melyek $i$-edik komponense tetszőleges eleme $G_i$-nek, a többi komponensben pedig a megfelelő csoport egységeleme áll. Nyilván $G_i^*$ a $G_i$-vel izomorf normálosztója a direkt szorzatnak. A $G_i^*$ normálosztók teljesítik, hogy

(1) szorzatuk az egész csoport;
(2) Bárhogy is veszünk $n-1$ darabot közülük, ezek szorzatának és a kimaradónak a metszete csak az egységelemből áll.

Megfordítva, könnyen igazolható, hogy az ilyen tulajdonságú normálosztók direkt szorzat felbontást adnak.

Hadd hívjam fel külön is a figyelmet arra, hogy a feltétel **nem úgy szól**, hogy bármely két $G_i^*$ metszete triviális. A vektorterekhez visszatérve, vegyünk a síkon három, origón átmenő egyenest. Ezek összege a sík, bármely kettő metszete nulla, mégsem igaz, hogy a sík ennek a három egyenesnek a direkt összege lenne, hiszen három egyenes direkt összege biztosan háromdimenziós. A teret viszont felbonthatjuk három egyenes direkt összegére, például a három koordináta-tengely segítségével, és itt valóban igaz, hogy bármely két tengely által kifeszített sík nullában metszi a harmadik tengelyt.

A vektorterek struktúratételét tehát úgy fogalmazhatjuk, hogy minden véges dimenziós vektortér előáll egydimenziós vektorterek (a $T$ test, mint önmaga felett vett vektortér) direkt szorzataként. A véges Abel-csoportok alaptétele ezzel analóg eredmény.

**9.5. A véges Abel-csoportok alaptétele.** *Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. A felbontásban szereplő adott rendű tényezők száma egyértelműen meghatározott.*

Részletesebben az egyértelműség azt jelenti, hogy ugyan a $G$ csoportot esetleg többféleképpen is sikerülhet felbontani prímhatványrendű ciklikus csoportok direkt szorzatára, de bárhogy is veszünk egy $q$ prímhatványt, a $q$ elemszámú tényezők száma mindegyik felbontásban ugyanannyi lesz.

Például legyen $G$ rendje 24. Ekkor a lehetséges tényezők rendjei éppen a 24 szám prímhatvány-osztói, azaz $2, 4, 8, 3$. Ilyen elemszámú tényezőkből kell a 24-et kikombinálni. A lehetőségek tehát a következők:

$$\mathbb{Z}_3^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_2^+, \quad \mathbb{Z}_3^+ \times \mathbb{Z}_2^+ \times \mathbb{Z}_4^+, \quad \mathbb{Z}_3^+ \times \mathbb{Z}_8^+.$$

Ezek szerint izomorfia erejéig 3 darab 24 rendű Abel-csoport van.

Ha $G$ egy $p^2$ rendű csoport, akkor, mint láttuk, kommutatív, és az alaptétel szerint kétféle lehet: $\mathbb{Z}_{p^2}^+$ és $\mathbb{Z}_p^+ \times \mathbb{Z}_p^+$. Ezzel régi ígéretünket is teljesítettük. Az alaptételt magát nem bizonyítjuk (a bizonyítás megtalálható a Fuchs: Algebra jegyzetben).

Az eddigiek alkalmazásaként megmutatjuk, hogy minden 15 rendű csoport ciklikus. A Sylow-tételeknél tanult gondolatmenetet alkalmazva, vagyis az 5- illetve 3-Sylowok számát vizsgálva az adódik, hogy mindkét Sylowból csak egy darab lehet, és ezek normálosztók. Ha tehát $G$ a csoport, és $P$, $Q$ a 3- illetve az 5-Sylow, akkor ezek normálosztók, és $P \cap Q$ egyelemű (hiszen rendje osztója a 3-nak is és az 5-nek is). Így a fentiek szerint $PQ$ részcsoport, ami izomorf $P \times Q$-val, azaz a $\mathbb{Z}_3^+ \times \mathbb{Z}_5^+ \cong \mathbb{Z}_{15}^+$ csoporttal. Mivel $G$ rendje 15, $PQ$ az egész $G$, azaz $G$ ciklikus.

Gyakorlásul érdemes ezt a gondolatmenetet általánosítani. Ha a $G$ csoport rendje $pq$, ahol $p < q$ különböző prímek, akkor mutassuk meg, hogy $G$ szükségképpen ciklikus, kivéve ha $q \equiv 1\ (p)$. Ez utóbbi esetben kissé komplikáltabb számolással belátható, hogy $pq$ rendű csoportból összesen két darab van, a ciklikus, és egy nemkommutatív.

Mostani tudásunk birtokában már többet mondhatunk a kis elemszámú csoportokról. A prímrendűeket és a prímnégyzet rendűeket már elintéztük. Nyolcadrendű csoportból ötféle van: a már említett két nemkommutatív csoporton ($D_4$, $Q$) kívül három kommutatív: $(\mathbb{Z}_2^+)^3$, $\mathbb{Z}_2^+ \times \mathbb{Z}_4^+$ és $\mathbb{Z}_8^+$. Általában is igaz, hogy prím-köb rendű csoportból pontosan öt nemizomorf van, melyből három kommutatív.

Ha a rend 10 vagy 14, akkor ez két prím szorzata, és két-két csoportot kapunk, a ciklikusakat, illetve a $D_5$ és $D_7$ diédercsoportokat. A 12 és 16 rendű csoportokat már nehezebb áttekinteni. A sort folytatva csupa feloldható csoportot fogunk kapni egészen addig, amíg a rend el nem éri a 60-at, ekkor ugyanis fellép az $A_5$, ami a legkisebb elemszámú nemkommutatív egyszerű csoport.

## X. Az egyszerű csoportok klasszifikációja

Ebben a részben, a teljesség bármiféle igénye nélkül, a véges egyszerű csoportok klasszifikációjával kapcsolatos eredményekről lesz szó. Az, hogy $A_n$ egyszerű csoport ha $n \geq 5$, már Galois számára is ismeretes volt, ezen múlik annak bizonyítása, hogy a 4-nél magasabb fokú egyenletekre nincsen gyökképlet. Ugyancsak régről (geometriából és analízisből) ismeretesek az úgynevezett klasszikus egyszerű csoportok, melyek több végtelen sorozatot alkotnak. Ezek talán legfontosabb családjával, a *projektív speciális lineáris csoportokkal (PSL$(n,q)$)* később megismerkedünk majd.

Már a XIX. században találtak olyan egyszerű csoportokat, melyek nem illettek be ezekbe a végtelen sorozatokba. Az első ötöt felfedezőjükről Mathieu-csoportoknak nevezzük. Jelük $M_{11}$, $M_{12}$, $M_{22}$, $M_{23}$ és $M_{24}$. Az index azt fejezi ki, hogy ezek az adott elemszámú halmazon ható permutációcsoportok, valójában bizonyos kombinatorikus struktúrák szimmetriacsoportjai. Azért váltak érdekessé, mert „nagyon" tranzitívak, erről később még lesz szó. A Mathieu-csoportokat az űrkutatásban is felhasználták már.

Az első mélyebb eredmények a huszadik század elején keletkeztek (Burnside, Frobenius) a *reprezentációelmélet* kialakulásával, amely lineáris algebrai eszközöket használ. Burnside ennek az elméletnek a segítségével fedezte fel azt a már említett eredményt, hogy egy nemkommutatív véges egyszerű csoport rendje legalább három különböző prímszámmal kell, hogy osztható legyen. A reprezentációelmélet fontos szerepet játszik a kémiában és a részecskefizikában is.

Burnside már akkoriban azt sejtette, hogy a véges nemkommutatív egyszerű csoportok rendje páros kell, hogy legyen. A kor eszközei azonban elégtelennek bizonyultak a sejtés bi-

zonyításához. Az 1950-es években Suzuki meghatározta az összes olyan egyszerű csoportot, melyben minden egységtől különböző elem centralizátora Abel-féle. Suzuki gondolataiból kiindulva végülis sikerült megoldani Burnside problémáját:

**10.1. Feit-Thompson Tétel.** *Minden nemkommutatív véges egyszerű csoport rendje páros kell, hogy legyen.*

A bizonyítás, ami több, mint 250 oldal (W. Feit, J. G. Thompson, Solvability of groups of odd order, *Pacific J. Math.*, **13** (1963), 775-1029), felhasználja a csoportelmélet korábbi eredményeit, például a reprezentációelméletet is.

Ezután már nem sokáig váratott magára az egyszerű csoportok klasszifikációja. Először Thompson egy újabb 600 oldalas cikkben meghatározta azokat az egyszerű csoportokat, melyek minden valódi részcsoportja már feloldható, ez utóbbi munkájáért Fields-Medalt (matematikai Nobel-díjat) kapott. A klasszifikáció az 1980-as évek elején vált teljessé.

A véges, nemkommutatív, egyszerű csoportok 17 végtelen sorozatba tartoznak, és ezen kívül van még 26 egyszerű csoport, melyek egyik sorozatnak sem tagjai. Ezeket *spóradikus* egyszerű csoportoknak nevezzük. A végtelen sorozatok egyikét az alternáló csoportok alkotják. A többi sorozatot Chevalley foglalta egységes rendszerbe. A spóradikus egyszerű csoportok listája az első táblázatban található a fejezet végén. Ide tartoznak például a már említett Mathieu-csoportok is.

Érdemes elidőzni kicsit a legnagyobb spóradikus csoportnál, mely a Monster (azaz Szörnyeteg) névre hallgat. Rendje

$$808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000\,,$$

azaz $8.08 \cdot 10^{53}$. Összehasonlításképpen néhány adat: a világegyetem nukleonjainak (protonok és neutronok) száma $3 \cdot 10^{77}$, térfogata (jelenleg) $10^{85}$ köbcenti, a Föld tömege $3.5 \cdot 10^{51}$-szerese egy proton tömegének (tehát a Monsternek sokkal több eleme van, mint ahány atomból a Föld áll), végül az ősrobbanás (azaz a világ kezdete) óta mindössze $4.7 \cdot 10^{17}$ másodperc telt el.

Ebből láthatjuk, hogy egy ekkora csoportot egyáltalán nem triviális megkonstruálni. Semmiféle számítógép nem tárolhatja például a szorzástábláját. A klasszifikációnak ez a konstrukció volt az utolsó lépése. Már tudták, hogy a Monster elemszáma csak a fenti lehet, azt is, hogy 194 konjugált osztálya kell, hogy legyen, csak azt nem tudták, hogy ilyen csoport létezik-e. Végül Griess talált egy 196884-dimenziós algebrát, melynek bizonyos szimmetriái a Monsterrel izomorf csoportot alkotnak.

Érdekes észrevenni, hogy a konjugált osztályok száma milyen kicsi a csoport rendjéhez képest. Az $M_{24}$ Mathieu-csoportnak például mindössze 26 konjugált osztálya van. Ez a csoport alapvető szerepet játszik a Monster, és sok más spóradikus egyszerű csoport szerkezetében is.

Lássuk az összes nemkommutatív egyszerű csoportot, melynek rendje egymilliónál kisebb. Ezek száma 56, melyből 39 izomorf a $PSL(2,q)$ csoporttal alkalmas $q$ prímhatványra, további három izomorf $PSL(3,q)$-val ($q = 3, 4, 5$), és egy, $A_8 \cong PSL(4,2)$. Ezt a 43 csoportot a harmadik táblázat tartalmazza, a többi 13-at a második táblázatban soroltuk fel. Itt szerepel két alternáló csoport ($A_7$, $A_9$), öt spóradikus csoport (az első három Mathieu és az

első két Janko), a maradék hat csoport pedig további végtelen sorozatoknak elemei (ezeket nem definiáljuk). Megjegyezzük, hogy két nemizomorf 20160 rendű egyszerű csoport van.

Most már itt az ideje, hogy megtudjuk, mik is ezek a $PSL(n,q)$ csoportok. Mint az eddigiekben is, jelölje $GL(n,T)$ az $n \times n$-es invertálható $T$ feletti mátrixok csoportját, ahol $T$ tetszőleges test. Ez még nem egyszerű csoport, több okból sem. Egyrészt $Z$ centruma nem triviális (könnyű kiszámolni, hogy ez a centrum éppen az egységmátrix nem nulla skalárszorosaiból áll, ezeket *skalármátrixoknak* nevezzük). Másrészt a determinánsképzés homomorfizmusa $GL(n,T)$-nek a $T$ test multiplikatív csoportjába, jelölje ennek magját, vagyis az 1 determinánsú mátrixok normálosztóját $SL(n,T)$ (speciális lineáris csoport). A $GL(n,T)/Z$ csoportnak speciális geometriai jelentése van, ahonnan a neve származik: általános projektív lineáris csoport, jele $PGL(n,T)$. Végül $PSL(n,T)$ vagy $L_n(T)$ jelöli az $SL(n,T)$ csoportnak a benne lévő skalármátrixok által alkotott normálosztó szerinti faktorcsoportját. Ha $n = 1$, akkor csoportjaink mindegyike kommutatív, ezért a továbbiakban feltesszük, hogy $n \geq 2$.

Mivel véges csoportokat szeretnénk kapni, célszerű a $T$ testet is végesnek választani. A Galois-elmélet keretében be fogjuk látni, hogy izomorfia erejéig minden $q$ prímhatványhoz pontosan egy $q$ elemű test létezik. Ha $T$ a $q$ elemű véges test, akkor a most definiált csoportok jelölésében $T$ helyett $q$-t írunk.

**10.2. Tétel.** *A $PSL(n,q)$ csoport egyszerű, kivéve $PSL(2,2)$ és $PSL(2,3)$.*

A tétel bizonyítása mátrixokkal való számolás, megtalálható például B. Huppert: *Endliche Gruppen* című könyvben (6.13. Tétel). Ugyanitt találhatók az alábbi hasznos izomorfizmusok bizonyításai (melyek táblázatainkból is kiolvashatók).

**10.3. Tétel.** *Az alábbi izomorfizmusok teljesülnek.*

(1) $PSL(2,2) \cong SL(2,2) = GL(2,2) \cong S_3$.
(2) $PSL(2,3) \cong A_4$.
(3) $PSL(2,4) \cong PSL(2,5) \cong A_5$.
(4) $PSL(2,7) \cong PSL(3,2)$ *(rendjük* 168*).*
(5) $PSL(2,9) \cong A_6$.
(6) $PSL(4,2) \cong A_8$.

**10.4. Tétel.** *Legyen*

$$M = (q^n - 1)(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1}) \quad \text{és} \quad d = (q-1, n)\,.$$

*Ekkor*

$$|GL(n,q)| = M\,; \quad |SL(n,q)| = |PGL(n,q)| = \frac{M}{q-1}\,; \quad |PSL(n,q)| = \frac{M}{(q-1)d}\,.$$

*Bizonyítás.* Legyen $V$ egy $n$-dimenziós vektortér a $q$ elemű $T$ test felett, és $v_1, \dots, v_n$ egy bázis. Számoljuk meg az invertálható lineáris transzformációkat. A $v_1$ képe tetszőleges nem nulla vektor lehet, ez $q^n - 1$ módon választható. A $v_2$ bárhová képződhet a $v_1$ generálta altéren kívül, ez $q^n - q$-féleképp lehetséges, és így tovább. Ezért $GL(n,q)$ rendje tényleg $M$.

A determináns a $T$ multiplikatív csoportjára képez, ezért a homomorfizmus-tétel miatt $SL(n,q)$ indexe $q-1$. Az egységmátrix nem nulla skalárszorosainak száma $q-1$, azaz $PGL(n,q)$ egy $q-1$ elemű normálosztó szerinti faktor.

Végül az utolsó állítás bizonyításához azt kell megmutatni, hogy e normálosztó 1 determinánsú elemeinek száma $d=(q-1,n)$. Ehhez meg kell számolni $T$ azon $t$ elemeit, melyekre $t^n=1$. Nyilván $t^n=1$ akkor és csak akkor, ha $t$ rendje a $T^\times$ csoportban osztója $n$-nek, és mivel $t$ rendje osztója e csoport rendjének (ami $q-1$), ez azzal ekvivalens, hogy $t$ rendje osztója $(q-1,n)=d$-nek, azaz, hogy $t^d=1$. A $T^\times$ csoport azonban (mint minden véges test multiplikatív csoportja) ciklikus, és így az ilyen elemek száma (a 2.9. Állítás bizonyítása szerint) éppen $d$. □

Végezetül néhány híres eredményt sorolunk fel, ami a klasszifikációból következik. A klasszifikáció kombinatorikai alkalmazásai során általában permutációcsoportokra vonatkozó problémák kerülnek elő. Egy permutációcsoportot *$k$-tranzitívnak* nevezünk, ha bárhogyan is választunk ki $k$ különböző pontot, a csoport alkalmas elemével ezek tetszőleges másik $k$ pontba átvihetők. A $G$ csoport egy $M$ részcsoportja *maximális részcsoport,* ha $M<G$, és nincs $G$-nek $M$-et tartalmazó részcsoportja ($M$-en és $G$-n kívül). Többszörösen tranzitív csoportban a stabilizátorok könnyen láthatóan maximális részcsoportok. Az egyszerű csoportok legtöbbjének már ismerik a maximális részcsoportjait. Hadd álljon itt egy meglepő eredmény, ami a klasszifikáció bizonyítása előtt híres sejtés volt.

**10.5. Tétel.** *Legyen $p$ prím, és tekintsük az $S_{\{0,1,\dots,p-1\}}$ szimmetrikus csoport azon részcsoportját, melyet az $ax+b$ ($a\neq 0$) alakú permutációk alkotnak (ahol az összeadást és a szorzást mod $p$ végezzük). Ekkor ez ($(p-2)!$ indexű) maximális részcsoport.*

**10.6. Tétel.** *Az $A_n$ és $S_n$ csoportokon kívül nincs olyan permutációcsoport, amely legalább hat-tranzitív lenne. Két öt-tranzitív csoport van, az $M_{12}$ és $M_{24}$ Mathieu-csoportok. A négy-tranzitív csoportok száma négy, az előző kettőn kívül még $M_{11}$ és $M_{23}$.*

Három-tranzitív csoport már végtelen sok van, de a klasszifikációból még a kettőtranzitív csoportok teljes leírása is következik.

**10.7. Tétel.** *Minden véges egyszerű csoport generálható két elemmel.*

E tétel szerint ha egy $G$ véges csoport bármely két elemmel generálható részcsoportja feloldható, akkor $G$ is feloldható, és ezt igen nehéz bizonyítani. Ugyanakkor $G$ nyilván pontosan akkor Abel, ha bármely két elemmel generált részcsoportja Abel.

Aki az alábbiaknál több információra kíváncsi, annak érdemes forgatnia a Nagy Piros Könyvet, azaz a véges egyszerű csoportok Atlaszát.

1. Táblázat. A spóradikus csoportok jele, rendje és felfedezőik.

| | | |
|---|---|---|
| $M_{11}$ | $2^4 \cdot 3^2 \cdot 5 \cdot 11$ | Mathieu |
| $M_{12}$ | $2^6 \cdot 3^3 \cdot 5 \cdot 11$ | Mathieu |
| $M_{22}$ | $2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$ | Mathieu |
| $M_{23}$ | $2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$ | Mathieu |
| $M_{24}$ | $2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$ | Mathieu |
| $J_2$ | $2^7 \cdot 3^3 \cdot 5^2 \cdot 7$ | Hall, Janko |
| $Suz$ | $2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$ | Suzuki |
| $HS$ | $2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$ | Higman, Sims |
| $McL$ | $2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$ | McLaughlin |
| $Co_3$ | $2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$ | Conway |
| $Co_2$ | $2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$ | Conway |
| $Co_1$ | $2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$ | Conway, Leech |
| $He$ | $2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$ | Held/Higman, McKay |
| $Fi_{22}$ | $2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$ | Fischer |
| $Fi_{23}$ | $2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$ | Fischer |
| $Fi'_{24}$ | $2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$ | Fischer |
| $HN$ | $2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$ | Harada, Norton/Smith |
| $Th$ | $2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$ | Thompson/Smith |
| $B$ | $2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$ | Fischer/Sims, Leon |
| $M$ | $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot$ $\cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$ | Fischer, Griess |
| $J_1$ | $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$ | Janko |
| $O'N$ | $2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$ | O'Nan/Sims |
| $J_3$ | $2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$ | Janko/Higman, McKay |
| $Ly$ | $2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$ | Lyons/Sims |
| $Ru$ | $2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$ | Rudvalis/Conway, Wales |
| $J_4$ | $2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$ | Janko/Norton, Parker, Benson, Conway, Thackray |

2. Táblázat. Az egymilliónál kisebb rendű egyszerű csoportok, I.

| | |
|---|---|
| $A_7$ | $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$ |
| $U_3(3) \cong G_2(2)'$ | $6048 = 2^5 \cdot 3^3 \cdot 7$ |
| $M_{11}$ | $7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$ |
| $U_4(2) \cong S_4(3)$ | $25920 = 2^6 \cdot 3^4 \cdot 5$ |
| $Sz(8)$ | $29120 = 2^6 \cdot 5 \cdot 7 \cdot 13$ |
| $U_3(4)$ | $62400 = 2^6 \cdot 3 \cdot 5^2 \cdot 13$ |
| $M_{12}$ | $95040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$ |
| $U_3(5)$ | $126000 = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7$ |
| $J_1$ | $175560 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$ |
| $A_9$ | $181440 = 2^6 \cdot 3^4 \cdot 5 \cdot 7$ |
| $M_{22}$ | $443520 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$ |
| $J_2$ | $604800 = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7$ |
| $S_4(4)$ | $979200 = 2^8 \cdot 3^2 \cdot 5^2 \cdot 17$ |

3. Táblázat. Az egymilliónál kisebb rendű egyszerű csoportok, II.

| | |
|---|---|
| $PSL(2,4) \cong PSL(2,5) \cong A_5$ | $60 = 2^2 \cdot 3 \cdot 5$ |
| $PSL(2,7) \cong PSL(3,2)$ | $168 = 2^3 \cdot 3 \cdot 7$ |
| $PSL(2,9) \cong A_6 \cong S_4(2)'$ | $360 = 2^3 \cdot 3^2 \cdot 5$ |
| $PSL(2,8) \cong R(3)'$ | $504 = 2^3 \cdot 3^2 \cdot 7$ |
| $PSL(2,11)$ | $660 = 2^2 \cdot 3 \cdot 5 \cdot 11$ |
| $PSL(2,13)$ | $1092 = 2^2 \cdot 3 \cdot 7 \cdot 13$ |
| $PSL(2,17)$ | $2448 = 2^4 \cdot 3^2 \cdot 17$ |
| $PSL(2,19)$ | $3420 = 2^2 \cdot 3^2 \cdot 5 \cdot 19$ |
| $PSL(2,16)$ | $4080 = 2^4 \cdot 3 \cdot 5 \cdot 17$ |
| $PSL(3,3)$ | $5616 = 2^4 \cdot 3^3 \cdot 13$ |
| $PSL(2,23)$ | $6072 = 2^3 \cdot 3 \cdot 11 \cdot 23$ |
| $PSL(2,25)$ | $7800 = 2^3 \cdot 3 \cdot 5^2 \cdot 13$ |
| $PSL(2,27)$ | $9828 = 2^2 \cdot 3^3 \cdot 7 \cdot 13$ |
| $PSL(2,29)$ | $12180 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 29$ |
| $PSL(2,31)$ | $14880 = 2^5 \cdot 3 \cdot 5 \cdot 31$ |
| $PSL(4,2) \cong A_8$ | $20160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$ |
| $PSL(3,4)$ | $20160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$ |
| $PSL(2,37)$ | $25308 = 2^2 \cdot 3^2 \cdot 19 \cdot 37$ |
| $PSL(2,32)$ | $32736 = 2^5 \cdot 3 \cdot 11 \cdot 31$ |
| $PSL(2,41)$ | $34440 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 41$ |
| $PSL(2,43)$ | $39732 = 2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 43$ |
| $PSL(2,47)$ | $51888 = 2^4 \cdot 3 \cdot 23 \cdot 47$ |
| $PSL(2,49)$ | $58800 = 2^4 \cdot 3 \cdot 5^2 \cdot 7^2$ |
| $PSL(2,53)$ | $74412 = 2^2 \cdot 3^3 \cdot 13 \cdot 53$ |
| $PSL(2,59)$ | $102660 = 2^2 \cdot 3 \cdot 5 \cdot 29 \cdot 59$ |
| $PSL(2,61)$ | $113460 = 2^2 \cdot 3 \cdot 5 \cdot 31 \cdot 61$ |
| $PSL(2,67)$ | $150348 = 2^2 \cdot 3 \cdot 11 \cdot 17 \cdot 67$ |
| $PSL(2,71)$ | $178920 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 71$ |
| $PSL(2,73)$ | $194472 = 2^3 \cdot 3^2 \cdot 37 \cdot 73$ |
| $PSL(2,79)$ | $246480 = 2^4 \cdot 3 \cdot 5 \cdot 13 \cdot 79$ |
| $PSL(2,64)$ | $262080 = 2^6 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$ |
| $PSL(2,81)$ | $265680 = 2^4 \cdot 3^4 \cdot 5 \cdot 41$ |
| $PSL(2,83)$ | $285852 = 2^2 \cdot 3 \cdot 7 \cdot 41 \cdot 83$ |
| $PSL(2,89)$ | $352440 = 2^3 \cdot 3^2 \cdot 5 \cdot 11 \cdot 89$ |
| $PSL(3,5)$ | $372000 = 2^5 \cdot 3 \cdot 5^3 \cdot 31$ |
| $PSL(2,97)$ | $456288 = 2^5 \cdot 3 \cdot 7^2 \cdot 97$ |
| $PSL(2,101)$ | $515100 = 2^2 \cdot 3 \cdot 5^2 \cdot 17 \cdot 101$ |
| $PSL(2,103)$ | $546312 = 2^3 \cdot 3 \cdot 13 \cdot 17 \cdot 103$ |
| $PSL(2,107)$ | $612468 = 2^2 \cdot 3^3 \cdot 53 \cdot 107$ |
| $PSL(2,109)$ | $647460 = 2^2 \cdot 3^3 \cdot 5 \cdot 11 \cdot 109$ |
| $PSL(2,113)$ | $721392 = 2^4 \cdot 3 \cdot 7 \cdot 19 \cdot 113$ |
| $PSL(2,121)$ | $885720 = 2^3 \cdot 3 \cdot 5 \cdot 11^2 \cdot 61$ |
| $PSL(2,125)$ | $976500 = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 31$ |

## Függelék

A $\varphi(n)$ Euler-függvény a $0, 1, \ldots, n-1$ számok közül az $n$-hez relatív prímek száma, azaz a $\mathbb{Z}_n^\times$ csoport rendje. Ebben a csoportban $*_n$ jelöli a műveletet.

**Tétel.** *Az Euler-függvény multiplikatív, azaz ha $n$ és $m$ relatív prím pozitív egészek, akkor $\varphi(nm) = \varphi(n)\varphi(m)$. Sőt, ilyenkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$ is teljesül.*

*Bizonyítás.* Legyenek $n$ és $m$ relatív prím pozitív egészek. Meg fogunk adni egy $f$ bijekciót a $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$ és a $\mathbb{Z}_{nm}^\times$ halmazok között. Ebből az Euler-függvény multiplikativitása már következik. Az izomorfia úgy fog kijönni, hogy a konstruált $f$ bijekció művelettartó is lesz.

Ha $c \in \mathbb{Z}_{nm}^\times$, akkor vegyük a $c$ szám $n$-nel való osztási maradékát, ezt jelölje $a$. Hasonlóképpen legyen $b$ a $c$ szám $m$-mel való osztási maradéka. Legyen $f(c) = (a, b)$.

A definíció szerint $0 \leq a < n$. Megmutatjuk, hogy $a$ és $n$ relatív prímek. Valóban, ha volna egy $d > 1$ közös osztójuk, akkor $a \equiv c\ (n)$ miatt $d$ osztaná $c$-t is, ami lehetetlen, mert $c$ és $nm$ relatív prímek. Ezért $a \in \mathbb{Z}_n^\times$. Ugyanígy adódik, hogy $b \in \mathbb{Z}_m^\times$. Az $f$ tehát a $\mathbb{Z}_{nm}^\times$ halmazt a $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$ halmazba képzi. Ahhoz, hogy belássuk, hogy bijektív, meg kell mutatnunk, hogy $f$ szürjektív és injektív.

Legyen $(a, b) \in \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$, és tekintsük az

$$\left.\begin{aligned} x &\equiv a\ (n) \\ x &\equiv b\ (m) \end{aligned}\right\}$$

szimultán kongruenciarendszert. Ennek a kínai maradéktétel szerint van megoldása, és ez egyértelmű modulo $nm$. Ezért pontosan egy olyan $c$ megoldás van, amelyre $0 \leq c < nm$. Belátjuk, hogy $c \in \mathbb{Z}_{nm}^\times$, azaz hogy $(c, nm) = 1$. Tegyük fel ennek ellenkezőjét. Ekkor van olyan $q$ prím, melyre $q \mid c$ és $q \mid nm$. Ezért vagy $q \mid n$, vagy $q \mid m$. Az első esetben $c \equiv a\ (n)$ miatt $q \mid a$ is teljesül, azaz $q$ közös osztója $a$-nak és $n$-nek. Ez lehetetlen, mert $a \in \mathbb{Z}_n^\times$, azaz $(a, n) = 1$. A második esetben, amikor $q \mid m$, a $(b, m) = 1$ feltétellel kapunk ellentmondást. Tehát tényleg $c \in \mathbb{Z}_{nm}^\times$. A maradékos osztás egyértelműsége miatt $f(c) = (a, b)$. Tehát $f$ tényleg szürjektív.

Az, hogy $f$ injektív, a kínai maradéktétel egyértelműségi állításából következik. Ha ugyanis $f(c) = f(c') = (a, b)$, akkor $c$ is és $c'$ is megoldása a fenti szimultán kongruenciarendszernek. Tehát $c \equiv c'\ (nm)$. Mivel $0 \leq c, c' < nm$, ezért $c = c'$. Tehát $f$ bijektív, és ezzel $\varphi$ multiplikativitását beláttuk.

A művelettartás bizonyításához tegyük fel, hogy $f(c) = (a, b)$ és $f(c') = (a', b')$. Szeretnénk kiszámítani $c$ és $c'$ (a $\mathbb{Z}_{nm}^\times$ csoportban vett) szorzatának $f$-nél vett képét, azaz a $c *_{nm} c'$ számnak a maradékát modulo $n$ és modulo $m$. A modulo $nm$ szorzás definíciója az, hogy az egész számok között kiszámított szorzatot még redukálni kell modulo $nm$. Így viszont $c *_{nm} c' \equiv cc'\ (n)$ is teljesül, tehát elegendő a $cc'$ maradékát kiszámolni. Tudjuk, hogy $c \equiv a\ (n)$ és $c' \equiv a'\ (n)$, ezért $cc' \equiv aa\ (n)$. Így $cc'$ maradéka ugyanaz, mint $aa'$ maradéka, azaz $a *_n a'$. Hasonló számolással kapjuk, hogy $c *_{nm} c'$ mod $m$ vett maradéka $b *_m b'$. Tehát $f(c *_{nm} c') = (a *_n a', b *_m b')$.

Mivel direkt szorzatban komponensenként kell szorozni, a $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$ csoportban $(a, b)$ és $(a', b')$ szorzata $(a *_n a', b *_m b')$, és így $f$ tényleg művelettartó. $\square$