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 múlt század első felében keletkezett, a magasabbfokú egyenletek gyökjelekkel való megoldhatósága kapcsán. 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 múlt század végén és ennek a századnak az 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.

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.

Typeset by $\mathcal{AMS}$-TEX

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 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 egy-két nemtriviális eredmény is helyet kapjon. Remélem, hogy a csoportelmélet megismerése minden olvasónak kellemes, maradandó élményt nyújt majd.

I. Részcsoportok

Legyen G egy csoport. A csoportműveletet (amit szorzásnak nevezünk) egymás mellé írás jelöli, a^{-1} pedig az a elem (kétoldali) inverze. A szorzás művelete általában nem kommutatív, erre a számolásoknál ügyelnünk kell (például szorzat inverzének kiszámításakor a sorrend megfordul: igazoljuk, hogy $(xy)^{-1} = y^{-1}x^{-1}$ bármely $x, y \in G$-re). Csoportban mindkét oldalról érvényes az egyszerűsítési szabály, hiszen minden elemnek van kétoldali inverze.

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. Ezeket triviális részcsoportoknak nevezzük.

1.1. 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:

1.2. 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. Gyakorlásul érdemes belátni, hogy a komplexusszorzás asszociatív, továbbá egy H nem üres részhalmaz akkor és csak akkor részcsoport, ha $HH^{-1} \subseteq H$.

Emlékezzünk vissza, hogy a G csoport elemeinek számát G rendjének nevezzük, és $|G|$-vel jelöljük.

1.3. 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 P 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.

1.4. 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. $\square$

1.5. 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. $\square$

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 a szerinti *baloldali mellékosztályának* 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 $|G| = |H| \cdot |G : H|$.

Természetesen az előző bekezdésben elmondottak igazak a jobboldali mellékosztályokra is. 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 $|G|/|H|$), de igaz végtelen csoportokra is. 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.

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. Megjegyezzük, hogy az index 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 $|\mathbb{Z}^+ : n\mathbb{Z}^+| = n$.

Legyen $g \in G$, és H a g összes hatványainak halmaza (negatív kitevőket is megengedve). Az így kapott 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:

1.6. Következmény. *Véges csoport minden elemének rendje osztója a csoport rendjének.*

Érdemes visszaemlékezni, hogyan következik ebből az állításból az Euler-Fermat tétel. További következmény, hogy ha egy G csoport rendje egy p prím, és H részcsoportja G-nek, akkor H rendje csak 1 vagy p lehet. Az első esetben $H = \{e\}$, a másodikban $H = G$. Tehát prímrendű csoportnak csak a két triviális részcsoportja van. Megfordítva, tegyük fel, hogy G-nek csak a két triviális részcsoportja van, és legyen $e \neq g \in G$. Ekkor $\langle g \rangle \neq \{e\}$, és így $\langle g \rangle = G$ (azaz G ciklikus). Ha g rendje végtelen, akkor g^2-nek nem hatványa g, és ezért $\langle g^2 \rangle$ nemtriviális részcsoport, ami a feltételnek ellentmond. Ezért $|g| = n$, ahol n pozitív egész. Legyen p prímosztója n-nek. Ekkor a hatvány rendjére tanult képletből kapjuk, hogy $h = g^{n/p}$ rendje p. Ezért $\langle h \rangle$ prímrendű részcsoport, ami csak G lehet. Így G prímrendű. Beláttuk tehát a következőt:

1.7. Következmény. *Egy G csoportnak pontosan akkor van két részcsoportja (a két triviális részcsoport), ha G prímrendű. Ilyenkor G ciklikus csoport (és ezért kommutatív).*

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

1.8. 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. □

1.9. 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 φ 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.

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

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). 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 $\varphi(d)$. □

Vegyük észre, hogy 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.

Lineáris algebrában a magasabb dimenziós altereket úgy lehetett megkapni, hogy több vektorral generáltunk alteret. Mi felel meg ennek a konstrukciónak csoportoknál? Itt is triviálisan bizonyítható, hogy részcsoportok metszete is részcsoport. Ezért itt is teljesül, hogy bárhogy is adunk meg egy $X \subseteq G$ részhalmazt, van egy X-et tartalmazó legszűkebb részcsoport, nevezetesen az összes X-et tartalmazó részcsoportok metszete. Az X-et tartalmazó legszűkebb részcsoport neve az X *által generált részcsoport.*

Lineáris algebrában a generált részcsoport elemeire egyszerű képletet bizonyítottunk. Ha az $X = \{g\}$ egy egyelemű halmaz, akkor hasonlóan egyszerű a csoportelméleti képlet is (g hatványait kapjuk). A nemkommutatív esetben azonban a képlet elbonyolódik. A következő állítást nagyon ajánlom gyakorló feladatnak.

1.10. 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 soktényezős 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 már lényegében azonos a lineáris algebrában tanult formulával. Az X részhalmazt G *generátorrendszerének* nevezzük (illetve azt mondjuk, hogy X generálja G-t), ha $\langle X \rangle = G$.

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).

II. 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.

A matematikában sokszor megtörténik az, hogy egy G csoport elemei maguk nem feltétlenül permutációi az X halmaznak, mégis G elemei "hatnak" az X halmazon, azaz $g \in G$ és $x \in X$ esetén lehet a $g * x \in X$ elemről beszélni. Például ha G az egybevágósági transzformációk csoportja a síkon, X pedig a sík négyzeteinek a halmaza, akkor értelme van annak, hogy egy F egybevágóság az N négyzetet "elviszi" az N' négyzetbe, vagyis hogy $F * N = N'$ (ezt szokásosabb, de nem precíz az $F(N) = N'$ alakban írni).

Ennek alapján 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

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

és ha e jelöli G egységelemét, akkor bármely $x \in X$ esetén

$$e * x = x\,.$$

Ezekből a szabályokból adódik, hogy g^{-1} "inverz leképezésként" hat, azaz

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

Természetesen a legtipikusabb példa az, amikor $G \leq S_X$, azaz G maga permutációkból áll, és $g * x = g(x)$.

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

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

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 *tranzitívan hat X-en.*

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.

2.1. Tétel. *Legyen G a véges X halmazon ható csoport. 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, és G hat a kocka X csúcshalmazán (hiszen egybevágóság csúcsot csúcsba visz).

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 2.1. 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

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

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 $|G(x)| = |G : G_x|$. $\square$

III. Izomorfizmus

A *homomorfizmus,* miként a többi struktúránál is, *művelettartó leképezést* jelent. Csoportok esetében azonban elegendő a szorzattartást feltenni. Valóban, ha $\varphi : G \to H$ szorzattartó, azaz $\varphi(ab) = \varphi(a)\varphi(b)$ teljesül minden $a, b \in G$-re, akkor

$$e_H\varphi(e_G) = \varphi(e_G) = \varphi(e_Ge_G) = \varphi(e_G)\varphi(e_G)\,,$$

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

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

azaz $\varphi(g^{-1}) = (\varphi(g))^{-1}$, és így φ inverzet inverzbe visz, vagyis az inverzképzés műveletét is tartja.

Izomorfizmus alatt bijektív homomorfizmust értünk. A G és H csoportok izomorfak, ha van közöttük izomorfizmus, ennek jele $G \cong H$. Az izomorf csoportok tulajdonságai megegyeznek, hiszen a csoportelméleti fogalmakat a műveletek segítségével definiáljuk, márpedig izomorf csoportokban "ugyanazok" a műveletek. Gyakorlásképpen érdemes igazolni, hogy ha $\varphi : G \to H$ izomorfizmus, akkor g és $\varphi(g)$ rendje mindig megegyezik, részcsoport képe izomorfizmusnál részcsoport, mellékosztályé mellékosztály, és így tovább. A híres Steinitz-féle *izomorfia-elv* azt mondja ki, hogy az algebrában egymással izomorf struktúrákat nem különböztetünk meg (vagyis olyan tulajdonságokat vizsgálunk, amelyek izomorf struktúrákban ugyanakkor teljesülnek).

Tegyük fel például, hogy G ciklikus csoport, melynek rendje n. Ha G a g elem hatványaiból áll, akkor a g hatványkitevőivel modulo n kell számolni, azaz "ugyanúgy", mint a $\mathbb{Z}_n^+$ csoport elemeivel. Tehát a $\varphi(i) = g^i$ leképezés műveletttartó, és így izomorfizmus $\mathbb{Z}_n^+$ és G között. Ha G végtelen ciklikus csoport, akkor pedig ugyanez a megfeleltetés $\mathbb{Z}^+$ és G között lesz izomorfizmus. Ezért

3.1. 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 általános ciklikus csoport helyett tehát mindig számolhatunk e konkrét csoportokban. Természetesen ez a megfeleltetés nem mindig nyilvánvaló. Ha például $G = \mathbb{Z}_p^\times$, ahol p prím, akkor a tanult tételek szerint G ciklikus, és így $\mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}^+$. 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. Vagy például azt az állítást, hogy ciklikus csoport minden részcsoportja ciklikus, elég lenne a $\mathbb{Z}^+$ és a $\mathbb{Z}_n^+$ csoportokra bizonyítani.

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. Viszonylag könnyen belátható, hogy más hatodrendű csoport nincs, azaz 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. Némi számolással belátható, hogy negyedrendű csoportból is csak kettő van. Látni fogjuk majd, hogy általában a prím-négyzet elemszámú csoportok száma is kettő.

Ahhoz, hogy ezt a sort folytathassuk, egyrészt tételeket, másrészt példákat kell kitalálnunk. Csoportok megadására már eddig is több módszert láttunk. Tanultunk az S_n szimmetrikus és az A_n alternáló csoportról. Tudjuk azt is, hogy ha R gyűrű, akkor az összeadásra nézve csoport (ezt a csoportot R^+ jelöli, és R additív csoportjának hívjuk). Ha R egységelemes, akkor R invertálható elemei csoportot alkotnak a szorzásra, melynek neve R multiplikatív csoportja, jele $R^\times$. Így keletkeztek a $\mathbb{Z}_n^+$ és a $\mathbb{Z}_n^\times$ csoportok.

Ha speciálisan az R gyűrű egy V vektortér összes lineáris transzformációjából áll (azaz $R = \mathrm{Hom}(V)$), 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). A G és L betűk a General Linear group (általános lineáris csoport) elnevezésből származnak.

Megadhatunk csoportokat 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 második táblázat az úgynevezett *kvaterniócsoportot* adja meg.

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

Ez a csoport a későbbiekben fontos lesz, 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).

Láthatjuk, hogy a táblázat minden sora (és minden oszlopa) a csoport elemeinek egy permutációja. Ez nyilván minden G csoportra igaz. 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:

3.2. 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.

IV. 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 a paritásképzés : $S_n \to \mathbb{Z}_2^+$). 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.

Szeretnénk tehát áttekinteni a G csoporton értelmezhető homomorfizmusokat. A lineáris algebrában minden $A : V \to W$ lineáris leképezéshez hozzárendeltük a magterét. Ennek ismerete a dimenziótétel miatt meghatározza $\mathrm{Im}(A)$ dimenzióját, és mivel egyenlő dimenziós vektorterek izomorfak, ezzel $\mathrm{Im}(A)$-t izomorfia erejéig meghatároztuk.

Nézzük most meg, hogy ha $\varphi : G \to H$ csoporthomomorfizmus, akkor a "mag" ismerete meghatározza-e izomorfia erejéig a "képet". Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor, miként lineáris algebrában, legyen

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

a φ *magja* (ez nyilván részcsoport G-ben), és

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

a φ *képe* (ez nyilván részcsoport H-ban). Ha φ szürjektív, vagyis ha $\mathrm{Im}(\varphi) = H$, akkor azt mondjuk, hogy φ 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 $\varphi : K \to H$ leképezés, ami K minden eleméhez önmagát rendeli, nyilván csoporthomomorfizmus, melynek képe K. Az azonban nem igaz, hogy G minden részcsoportja egy alkalmas homomorfizmus magja. Valóban, ha $a \in \mathrm{Ker}(\varphi)$ és g tetszőleges eleme G-nek, akkor

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(a)\varphi(g^{-1}) = \varphi(g)e_H\varphi(g)^{-1} = e_H\,,$$

vagyis $a \in \mathrm{Ker}(\varphi) \implies ghg^{-1} \in \mathrm{Ker}(\varphi)$. Márpedig ez a tulajdonság nem teljesül minden részcsoportra, például az S_3 csoport $\{id, (12)\}$ részcsoportjára sem (ezt érdemes ellenőrizni).

A G csoport egy N részcsoportját akkor nevezzük *normális részcsoportnak,* vagy *normálosztónak,* ha egy alkalmas, G-n értelmezett homomorfizmusnak a magja (jelölés: $N \triangleleft G$). A gag^{-1} szorzatot az *a elem g-vel vett konjugáltjának* nevezzük. Beláttuk tehát, hogy minden normálosztó zárt G bármely elemével való konjugálásra. Meg fogjuk mutatni, hogy ennek az állításnak a megfordítása is igaz. Előbb azonban fogalmazzuk át a kapott feltételt.

4.1. Állítás. *A G csoport N részcsoportjára ekvivalensek az alábbiak.*

(1) *N zárt a konjugálásra (azaz $a \in H$, $g \in G$ esetén $gag^{-1} \in H$).*
(2) *Minden $g \in G$ elemre $gN = Ng$ (azaz az N szerinti jobb és bal mellékosztályok megegyeznek).*

Bizonyítás. Valóban, ha N zárt a konjugálásra, akkor $gNg^{-1} \subseteq N$. Ez igaz g helyett 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 konjugáltságra való zártság 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). □

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 $g \in Ng$, azaz az Ng és Ng' mellékosztályok nem diszjunktak, tehát egyenlőek.

4.2. Tétel. *A G csoport N részcsoportja akkor és csak akkor normálosztó, ha zárt a konjugálásra.*

Bizonyítás. Tegyük fel, hogy az $N \leq G$ részcsoport zárt a G elemeivel való konjugálásra. Szeretnénk egy olyan $\varphi : G \to H$ homomorfizmust konstruálni, melynek magja N. Ahhoz, hogy ezt megtehessük, tegyük fel, hogy a célt sikerült elérni, és vizsgáljuk meg, hogy milyennek kell lennie a kapott φ-nek és H-nak, hogy kiderüljön, hogyan kell őket megkonstruálni.

A H “felesleges” elemeit elhagyva feltehetjük, hogy a keresett φ szürjektív. Először is a $H = \mathrm{Im}(\varphi)$ csoportot kellene megtalálni. Ha $h \in H$, akkor G mely elemei képződnek h-ra? Legyen $\varphi(g) = h$, ekkor

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

Tehát h-ra épp a gN mellékosztály elemei képződnek. Azaz H elemei kölcsönösen egyértelmű megfeleltetésben állnak az N szerinti baloldali mellékosztályokkal. Hogyan kaphatjuk meg a G-beli szorzás ismeretében a $h_1, h_2 \in H$ elemek szorzatát? Ha $\varphi(g_1) = h_1$ és $\varphi(g_2) = h_2$, akkor

$$h_1h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1g_2)\,,$$

vagyis a h_1h_2 szorzatnak a g_1g_2N mellékosztály felel meg.

Konstruáljunk tehát egy K csoportot, melynek elemei éppen a G csoport N szerinti baloldali mellékosztályai, két mellékosztály szorzatát pedig a

$$(g_1N) \cdot (g_2N) = g_1g_2N$$

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

Még a csoportaxiómák ellenőrzése **előtt** van egy probléma. Szabad-e így a műveletet definiálnunk? Lássunk először egy példát a mindennapi életből. 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 Lolka az 7/A-ból jobb tanuló, mint Bolka a 6/B-ből még nem következik, hogy az 7/A-ban mindenki jobb tanuló, mint a 6/B-ben.

Amikor a g_1N és g_2N 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

$$g_1N = g_1'N \text{ és } g_2N = g_2'N \implies g_1g_2N = g_1'g_2'N\,.$$

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 N zárt a konjugálásra, azaz, mint láttuk, $gN = Ng$ minden $g \in G$-re, akkor

$$g_1g_2N = g_1g_2'N = g_1Ng_2' = g_1'Ng_2' = g_1'g_2'N\,,$$

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 ψ 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. Mivel az N szerinti bal és jobb mellékosztályok ugyanazok, ezért ugyanazt a csoportot kapjuk akkor is, ha jobb mellékosztályokkal dolgozunk. Ha G véges, akkor persze $|G/N| = |G : N| = |G|/|N|$.

Az iménti gondolatmenet során azonban az is kiderült, hogy ha $\varphi : G \to H$ tetszőleges homomorfizmus, akkor $\mathrm{Im}(\varphi)$ elemei kölcsönösen egyértelmű, művelettartó megfeleltetésben állnak a K csoport elemeivel, vagyis, hogy $\mathrm{Im}(\varphi) \cong K = G/N$. Azaz:

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

Ez az állítás tehát a dimenziótétel csoportelméleti analogonja. Maga a faktorcsoport az algebra egyik legfontosabb fogalma. A faktorcsoportban általában az osztályok elemeivel (úgynevezett reprezentánsokkal) célszerű számolni.

4.4. Állítás. *Legyen $N \triangleleft G$ 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, $(gN)^n = eN \Longleftrightarrow g^n \in N$, és k a legkisebb ilyen pozitív n. □

Hasonlóan igazolható az is, hogy egy tetszőleges elem rendje többszöröse az elem bármely homomorfizmusnál vett képe rendjének.

Minden csoportban nyilván normálosztó a két triviális részcsoport. Ha egy csoportnak csak két normálosztója van, akkor a csoportot *egyszerű csoportnak* nevezzük (az egyelemű csoportot tehát nem tekintjük egyszerűnek).

4.5. 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 az 1.7. Következmény szerint pontosan a prímrendű ciklikus csoportok. □

V. Feloldható csoportok

Minden véges G csoportot "fel lehet építeni" egyszerű csoportokból a következőképpen. Vegyünk egy $N \neq G$ normálosztót G-ben, ami *maximális*, azaz nincs G-nek N-et tartalmazó normálosztója (persze N-en és G-n kívül).

5.1. Állítás. *Ha N maximális normálosztó G-ben, akkor G/N egyszerű csoport.*

Bizonyítás. Tegyük fel, hogy $K \triangleleft (G/N)$. A G/N elemei N szerinti mellékosztályok, K elemei ezek közül valók. Jelölje L a K elemeinek unióját, ez tehát G részhalmaza. Belátjuk, hogy $L \triangleleft G$.

Ha $g, h \in L$, akkor $gN, hN \in K$ (az L definíciója miatt). Mivel $K \leq G/N$, e két elem szorzata, azaz $ghN \in K$. Ezért $gh \in L$. Hasonlóan igazolható, hogy L zárt az inverzképzésre és a G elemeivel való konjugálásra (igen jó gyakorló feladat elvégezni ezeket a számolásokat). Így L tényleg normálosztó G-ben.

Nyilván $N \leq L \leq G$, és így N maximalitása miatt $L = N$ vagy $L = G$. Az első esetben $|K| = 1$, a másodikban $K = G/N$. Tehát G/N egyszerű. □

Igaz, és hasonlóan bizonyítható az állítás megfordítása is: ha G/N egyszerű, akkor N maximális normálosztó. Valójában azt láttuk be, hogy G/N normálosztói megfelelnek az N-et tartalmazó G-beli normálosztóknak. Gyakorlásul igazoljuk, hogy ugyanez részcsoportokra is igaz, és az egymásnak megfelelő részcsoportok indexe ugyanaz (vagyis az előző bizonyítás jelölésével $|G/N : K| = |G : L|$).

Ha tehát G véges csoport és $N = N_1$ maximális normálosztó G-ben, akkor G/N_1 egyszerű csoport. Legyen most N_2 maximális normálosztója N_1-nek. Ekkor persze N_1/N_2 is egyszerű csoport. Az eljárást folytatva előbb-utóbb elfogy a G csoport, vagyis $N_k = \{e\}$ lesz valamilyen k-ra. Így egy olyan "láncot" kaptunk:

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

ahol az N_i/N_{i+1} faktorcsoportok mindegyike egyszerű. Tehát G-t egyszerű csoportokból "raktuk össze".

Általában 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 *kompozíciólláncának* nevezzük.

Három dologra nagyon vigyáznunk kell. Először is, ez az egyszerű csoportokból való "összerakás" távolról sem egyértelmű. Ha ismerjük a lánc egyszerű faktorcsoportjait, az még nem határozza meg G szerkezetét. Például végezzük el ezt az eljárást a két hatelemű csoportra:

$$\{e\} \lhd \{id, (123), (132)\} \lhd S_3$$
$$\{e\} \lhd \{0, 2, 4\} \lhd \mathbb{Z}_6^+\,.$$

Mindkét esetben a faktorcsoportok elemszáma (alulról kezdve) 3 illetve 2. Azaz a kapott egyszerű csoportok ugyanazok S_3 és $\mathbb{Z}_6^+$ esetén ($\mathbb{Z}_3^+$ és $\mathbb{Z}_2^+$), és e két hatelemű csoport mégsem izomorf.

A második dolog, amire vigyáznunk kell, hogy a kapott N_i csoportok nem lesznek általában 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! Példaként végezzük el eljárásunkat az A_4 alternáló csoportra.

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

és itt $\{id, (12)(34)\}$ nem lesz normálosztó A_4-ben (ezt is jó gyakorlás ellenőrizni).

Végül vigyáznunk kell arra is, hogy ez a fajta felbontás általában nem egyértelmű. Például a $\mathbb{Z}_6^+$ csoportnál eljárhatunk így is:

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

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

A G csoportot *feloldhatónak* nevezzük, ha van olyan normállánca, melyben a szereplő faktorcsoportok mindegyike Abel. Ha G véges, akkor ezzel ekvivalens feltétel, hogy G-nek van olyan kompozíciólánca, melynek faktorai prímrendűek. Ez könnyen következik abból a már bizonyított tényből, hogy minden egyszerű Abel-csoport prímrendű (végezzük el a bizonyítást). A Jordan-Hölder tétel szerint ekkor a többi kompozícióláncban is minden faktor prímrendű.

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:

5.2. 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). A megfordítás abból következik, hogy

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

Ekkor ugyanis S_n-nek kompozíciólánca lesz $\{e\} \triangleleft A_n \triangleleft S_n$, azaz ilyenkor S_n tényleg nem feloldható. Az 5.3. Tétel bizonyítása szintén megtalálható a Fuchs-jegyzetben.

Feloldható csoportokra másik fontos példa a prímhatványrendű csoportok. 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, ez nyilván feloldható.

5.4. Tétel. *Ha p prím, akkor minden véges p-csoport feloldható.*

Mielőtt bebizonyítanánk ezt az állítást, vizsgáljuk meg, hogyan lehet megkeresni egy G csoport normálosztóit. Tudjuk, hogy ezek azok a részcsoportok, amelyek a konjugálásra zártak. Ha tehát $g \in G$, akkor legyen

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

Ezzel a G csoportnak egy önmagán való hatását definiáltuk. Valóban, 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 orbitokat G *konjugált osztályainak* nevezzük. Tehát két elem akkor van egy konjugált osztályban, ha G egy alkalmas elemével egymásba konjugálhatók. Ezért

5.5. Állítás. *Egy részcsoport akkor és csak akkor normálosztó, ha konjugált osztályok egyesítése.*

Hogyan lehet meghatározni a konjugált elemosztályokat? Alkalmazzuk a 2.1. Tételt a most vizsgált hatásra. Azt kapjuk, hogy ha $x \in G$, akkor x orbitjának, azaz konjugált elemosztályának a rendje éppen az x stabilizátorának az indexe. Mi az x stabilizátora? Azon $g \in G$ elemek halmaza, melyek x-et fixen hagyják, azaz melyekre $gxg^{-1} = x$, vagyis $gx = xg$. Ezt a részcsoportot, tehát az x elemmel felcserélhető G-beli elemek halmazát, az x elem G-beli *centralizátorának* nevezzük, és $C_G(x)$-szel jelöljük. A 2.1. Tétel tehát a következőt adja:

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

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. Ha ugyanis y és z mindketten felcserélhetők G összes elemével, akkor yz (és y^{-1}) is, hiszen ekkor

$$g(yz) = ygz = (yz)g\,.$$

Nyilvánvalóan $Z(G) \lhd G$, hiszen $Z(G)$ (egyelemű) konjugált osztályok egyesítése. Hasonló okokból $Z(G)$ minden részcsoportja normálosztó G-ben.

5.7. Állítás. *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. $\square$

Legyen végül P tetszőleges p-csoport, és készítsük el P tetszőleges kompozícióláncát. Ebben a faktorok rendje osztója $|P|$-nek, azaz mindegyik ilyen F faktorcsoport egyszerű p-csoport. Az előző tétel szerint $Z(F)$ nem csak az egységelemből áll. Mivel $Z(F) \lhd F$, és F egyszerű, azt kapjuk, hogy $Z(F) = F$, azaz F Abel. De minden kommutatív egyszerű csoport prímrendű, így F rendje p. Ez a P kompozícióláncának minden faktorára igaz, tehát P feloldható. Így az 5.4. Tételt beláttuk.

Most már részben törleszteni tudjuk egy korábbi adósságunkat is.

5.8. Tétel. *Minden prímnégyzet rendű csoport kommutatív.*

Bizonyítás. Legyen P egy p^2 rendű csoport, ahol p prím. Ekkor $Z(P)$ elemszáma az előző tétel 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 $h \in G - Z(P)$. Ekkor $gh = hg$, hiszen g a centrumban van. Ezért a

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

halmaz egy kommutatív részcsoportja P-nek. A H részcsoport bővebb $Z(P)$-nél (hiszen a prímrendű $Z(P)$-t már g hatványai is kiadják), és 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. $\square$

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).

Érdemes még a konjugálással kapcsolatban két dolgot megjegyezni.

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

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

leképezés a G csoportot önmagára képző izomorfizmus.

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

Speciálisan tehát ez az 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:

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

($g \in G$, $A \in X$). 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, azaz 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 tételt láttuk tehát be:

5.10. 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 $H \leq N_G(H)$.

VI. 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. Ez könnyen kiderül az alábbi tétel felhasználásával:

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 $N \lhd G$. $\square$

Mivel az A_5 egyszerű csoport, nem lehet benne kettő indexű, azaz 30 rendű részcsoport. 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.

6.2. 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: az 1.9. Állítás szerint $n_H = 1$ (tetszőleges q esetén). Ezért a következő állítást kapjuk:

6.3. 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 6.2. 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. Ha az itt szereplő *különböző* mellékosztályok száma 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 tm_A, ahol m_A egy p-vel osztható szám. Ezért

$$|X| = tn_G + tpx_G\,,$$

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

Ugyanez a gondolatmenet a H csoportra is elmondható:

$$|X| = tn_H + tpx_H\,,$$

ahol x_H valamilyen egész szám. A két egyenlőséget összevetve és t-vel osztva éppen a 6.2. Lemma állítása adódik. $\square$

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

6.4. 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:

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

Láttuk, hogy 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 $P' \triangleleft N_G(P')$, és így beszélhetünk a hP' elem rendjéről az $N_G(P')/P'$ faktorcsoportban (vö. 4.4 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 $h \in P'$. $\square$

Foglaljuk össze az eddig bizonyítottakat.

6.5. 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 6.3. 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.

VII. Véges Abel-csoportok

A Sylow-tételek csak a kiindulópontját jelentik annak az útnak, ami a klasszifikációhoz vezet. Van azonban a csoportelméletnek egy viszonylag lezárt fejezete is: a véges Abel-csoportokra ugyanis sikerült struktúratételt bizonyítani.

A lineáris algebrában az oszlopvektorokkal viszonylag könnyen tudunk számolni, ezért fontos az a tétel, hogy minden véges dimenziós vektortér izomorf a T^n vektortérrel (ahol T az alaptest). Ezekkel az oszlopvektorokkal a műveleteket komponensenként végezzük. Ugyanezt akkor is megtehetjük, ha az egyes komponensek csoportokból valók.

Legyenek tehát $G_1, \ldots, G_n$ tetszőleges csoportok. Ekkor a $G_1 \times \cdots \times G_n$ halmazon definiálhatjuk a komponensenkénti műveleteket:

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

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). Így csoportot kaptunk, melyet a $G_1, \ldots, G_n$ csoportok *direkt szorzatának nevezünk,* és $G_1 \times \cdots \times G_n$-nel jelölünk. 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:

7.1. Állítás. *A $G_1 \times \cdots \times G_n$ direkt szorzat tetszőleges elemének rendje a komponensek 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. □

7.2. 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 $(m,n) = 1$, $|g| = n$, $|h| = m$. $\square$

A számelméletben bebizonyítottuk, hogy ha m és n relatív prím pozitív egészek, akkor létezik egy olyan $f : \mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \to \mathbb{Z}_{nm}^\times$ bijekció, hogy tetszőleges $a, a' \in \mathbb{Z}_n^\times$ és $b, b' \in \mathbb{Z}_m^\times$ esetén

$$f(a *_n a', b *_m b') = f(a,b) *_{nm} f(a',b')\,.$$

Ez az összefüggés mostani fogalmainkkal éppen azt jelenti, hogy f izomorfizmus a $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times$ és a $\mathbb{Z}_{nm}^\times$ csoportok között.

7.3. Tétel. *Ha m és n relatív prím pozitív egészek, akkor $\mathbb{Z}_n^\times \times \mathbb{Z}_m^\times \cong \mathbb{Z}_{nm}^\times$.*

A $\mathbb{Z}_n^\times$ csoport generátorelemeit primitív gyöknek neveztük modulo n. Milyen n-ekre létezik primitív gyök? Beláttuk, hogy ha n prím, akkor létezik. A mostaniak alapján egy negatív eredményt is igazolhatunk. Ha ugyanis $\mathbb{Z}_{nm}^\times$ ciklikus, akkor 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. Beláttuk tehát a következő állítást.

7.4. Következmény. *Ha modulo n létezik primitív gyök, akkor n vagy prímhatvány, vagy egy prímhatvány kétszerese.*

További számelméleti 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.

Legyen $G = A \times B$. 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:

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

(hasonló tulajdonságokat fedezhettünk fel alterek körében is, amikor direkt összegről beszéltünk). Ezeknek a tulajdonságoknak a bizonyítása nagyon egyszerű, és igencsak javallott gyakorlófeladat.

A fenti tulajdonságok megléte már elegendő ahhoz, hogy direkt szorzatot kapjunk.

7.5. 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 ψ leképezés, melyet a $\psi((a,b)) = ab$ képlet definiál, bijekció az $A \times B$ és G között. Még azt kell belátnunk, hogy ψ 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. $\square$

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 $A, B \lhd G$.

Az eddigiek alkalmazásaként megmutatjuk, hogy minden 15 rendű csoport ciklikus. A Sylow-tételeknél tanult gondolatmenetet alkalmazva, azaz 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 is 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.

7.6. 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 ez azt jelenti, hogy ha a G csoportot kétféleképpen is sikerült felbontani prímhatványrendű ciklikus csoportok direkt szorzatára, akkor bárhogy is veszünk egy q prímhatványt, a q elemszámú tényezők száma a két felbontásban ugyanaz 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).

Mostani tudásunk birtokában már többet mondhatunk a kis elemszámú csoportokról. A prímrendűeket és a prímnégyzet rendűeket már elintéztük. Nyolcadrendű csoportból a fentiek szerint 3-féle kommutatív van, és be lehet látni, hogy ezeken kívül két nemizomorf nyolcadrendű csoport van: a kvaterniócsoport, és a D_4 diédercsoport (azaz a négyzet szimmetriacsoportja). 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.

VIII. Egyszerű csoportok

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 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 múlt 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 század elején vetette fel Burnside híres problémáját, hogy van-e páratlan rendű nemkommutatív egyszerű csoport. Noha akkoriban már több mély módszer létezett egyszerű csoportok vizsgálatára, a kérdés sokáig nyitott maradt. 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:

8.1. Feit-Thompson Tétel. *Minden nemkommutatív egyszerű csoport rendje páros.*

A bizonyítás (W. Feit, J. G. Thompson, Solvability of groups of odd order, *Pacific J. Math.*, **13** (1963), 775-1029) több, mint 250 oldal.

Ezután már nem sokáig váratott magára az egyszerű csoportok teljes 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. A klasszifikációnak ez 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, azaz 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.

8.2. 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).

8.3. 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) $PSL(4,2)\cong A_8$.

8.4. Tétel. *Legyen*

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

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 (az 1.9. Állítás bizonyítása szerint) éppen d. $\square$

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.

8.5. Tétel. *Legyen p prím, és tekintsük az $S_{\{0,1,\ldots,p-1\}}$ 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.*

8.6. 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.

8.7. 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.

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