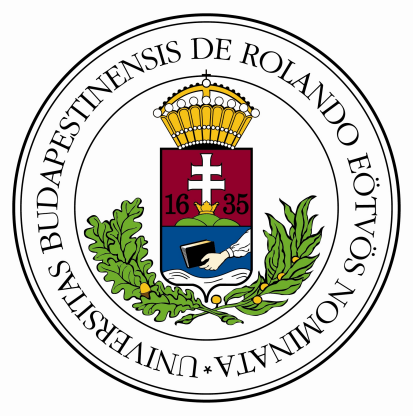


Eötvös Loránd Tudományegyetem

Természettudományi Kar

Szakdolgozat

A Kocka és ami mögötte van

Készítette:
Böszörményi Balázs

Témavezető:
Halasi Zoltán
egyetemi adjunktus

Budapest
2015

Tartalomjegyzék

Bevezetés

A szakdolgozatom témájának kiválasztásakor egyértelmű volt, hogy valamilyen csoportelmélettel kapcsolatos témával szeretnék foglalkozni, mivel az egyetemi tanulmányaim során nagyon könnyen elsajátítottam az anyagot, ugyanakkor világos volt előttem, hogy csak ízelítőt kaptam az egészből, szívesen elmélyültem volna jobban benne. A lehetséges szakdolgozati témákat végignézve azért erre esett a választásom, mert a Rubik-kocka mint játék, igen népszerű nagyon sok olyan ember körében is, aki matematikával egyáltalán nem foglalkozik, úgy gondoltam – és gondolom, hogy a későbbi tanári tevékenységem során haszonnal mutathatom be érdeklődő diákoknak a témát ebből a nézőpontból. A harmadik fő indok az volt, hogy személy szerint sosem foglalkoztam a Rubik-kockával, bár egyszer testvéri unszolásra sikerült kiraknom, de inkább csak mechanikus módon, nem próbáltam megérteni az elveket, amelyek mögötte húzodnak. A szakdolgozat megírása közelebb hozta a témát hozzám, ugyanakkor úgy érzem, még bőven van mit meggondolni, úgyhogy szeretném folytatni a vizsgálatát, a későbbiekben akár egy szakkörsorozatot is szívesen tartanék diákoknak.

Röviden ismertetném a különböző fejezetek tartalmát. Az első fejezet, ahogy a címe is mutatja, csoportelméleti témákat tartalmaz, az alapfogalmakon (csoport, részcsoport, rend, mellékosztályok, homomorfizmusok, izomorfizmusok, normálosztók, faktorcsoport) túl a permutációcsoportoknak, hatásoknak jut fontos szerep, illetve a direkt szorzattal, a szemidirekt szorzattal és a koszorúszorzattal foglalkozom. Az utolsó alfejezetben pedig azt vizsgálom meg, hogy bizonyos tulajdonsággal rendelkező ciklusokat tartalmazó generátorhalmaz mikor generálja S_n-t, illetve A_n-t. A második fejezetben a 3×3-as Rubik-kocka csoportját vizsgálom. Az első alfejezetben bevezetek egy jelölésrendszert, utána definiálom a csoport generátorelemeit. Mutatok példát elem rendjére, ennek kapcsán megvizsgálom a tranzitivitást. Ezután egy részcsoport szerkezetét vizsgálom meg. Az ezt követő alfejezetben a Rubik-kocka

csoportjának szerkezetét vizsgálom meg a kibővített csoport szerkezetének tükrében. Végül néhány, a Rubik-kockához kapcsolódó érdekességet mutatok be.

Szeretném köszönetemet kifejezni Halasi Zoltánnak, a témavezetőmnek, egyrészt mert nagyon készségesen segített bármilyen felmerülő kérdésben, másrészt mert hagyta, hogy a saját megközelítésemben dolgozzak, sokszor a tanácsai, kérdései vezettek egy új ötlethez, amellyel folytatni tudtam.

1. fejezet

Csoportok

Ebben a fejezetben különböző csoportelméleti fogalmakat definiálok, tételeket mondok ki, illetve bizonyítok be. Ezek egy részét a későbbiekben, a 3×3-as Rubik-kockáról szóló fejezetben fogom használni, egy részüket csak áttekintés céljából írtam. Egyes állításoknál nem foglalkoztam a bizonyítással, mivel nem ez a szakdolgozat lényegi része, csupán szükségem lesz rájuk a későbbiekben (a bizonyítások megtalálhatóak [1]-ben, amely nagy segítségemre volt).

1.1. Csoportelméleti alapfogalmak

1.1.1. Definíció. Legyen G egy nem üres halmaz, $*$ egy G elemein értelmezett, kétváltozós művelet[1]. A G halmazt $*$-gal együtt *csoportnak* nevezzük, ha teljesülnek a következők:

1. G zárt $*$-ra, azaz $\forall a, b \in G$-re: $a * b \in G$
2. $\exists e : \forall g \in G : e * g = g * e = g$ – neutrális vagy egységelem létezése.
3. $\forall g \in G\ \exists g^{-1} : g * g^{-1} = g^{-1} * g = e$ – inverz létezése
4. $\forall a, b, c \in G : (a * b) * c = a * (b * c)$ – asszociativitás

A fenti definíció eltér az [1]-belitől, mivel abból, hogy $*$ értelmezve van G elemein, következik, hogy G zárt, néhol ezt is beveszik a csoportaxiómák közé (így a részcsoportnál nem kell külön kitérni rá, ld. később).

[1] A műveletet a későbbiekben – egy-két kivételtől eltekintve – egybeírással vagy a $\cdot$ jellel fogom jelölni, $*$ pedig általában egy csoport hatását fogja jelölni egy halmazon, ld. később.

1.1.2. Definíció. Legyen G csoport, és $a, b \in G$. a és b *felcserélhetőek* vagy *kommutálnak*, ha $a*b = b*a$. Ha G-ben bármely két elem felcserélhető, akkor G *kommutatív* vagy *Abel-csoport*.

Az utóbbi két definíciót [1]-ben az 53. oldalon találjuk. Az itt következő részt nagyrészt [1] alapján készítettem, bár ott más sorrendben találhatóak az egyes definíciók stb. A 4. fejezet (*Csoportok*) első négy és hetedik alfejezetét vettem alapul. Az egyéb forrás alapján írt részeket külön megemlítem, illetve azt is jelzem, ha valamit önállóan vezettem le.

1.1.3. Definíció. Egy G csoport rendjén az elemei számát értjük. Jelölés: $|G|$.

1.1.4. Definíció. Legyen G csoport és $g \in G$. A g elem *rendjén* g különböző hatványainak számát értjük. Jelölés: $o(g)$. Véges csoport elemeinek rendje természetesen véges.

A rendnek további fontos tulajdonsága, hogy $g^{o(g)} = 1$, ahol 1 G egységeleme, illetve hatvány rendje $o(g^k) = \frac{o(g)}{(o(g),k)}$.

1.1.5. Definíció. Legyen G csoport. A $H \subseteq G$ halmaz G *részcsoportja*, ha a G-beli műveletre nézve H maga is csoport. Jelölés: $H \leq G$.

Két részcsoport mindig van: G részcsoportja önmagának, illetve az egyelemű, csak az egységelemet tartalmazó csoport is. Ezeket *triviális részcsoportoknak* nevezzük, a G-től különböző részcsoportokat pedig *valódi részcsoportnak*. Egy részhalmaz pontosan akkor lesz részcsoport, ha zárt a szorzásra és az inverzképzésre. Véges csoport esetén elég a szorzást vizsgálni, mivel $g^{o(g)-1} = g^{-1}$.

Mutatok néhány példát csoportokra, elsősorban azokat, amelyeket a későbbiekben használni fogok.

1.1.6. Definíció. Legyen X tetszőleges halmaz. Az X-et önmagára képező bijekciókat X *transzfomációinak*, ha X véges, X *permutációinak* nevezzük. A transzformációk halmazát S_X, illetve ha $|X| = n$, akkor S_n jelöli.

1.1.7. Állítás. S_X csoport a kompozíció műveletére.

Kétféle megközelítés létezik leképezések kompozíciójának (szorzatának) az értelmezésére, általában $(f \circ g)(x) = f(g(x))$, azaz a leképezéseket balról írjuk,

és jobbról balra haladunk (tehát a példában először g-t, aztán f-et alkalmazzuk). Csoportelmélettel foglalkozó könyvekben megszokottabb a másik konvenció, amikor a leképezéseket jobbról írjuk, és balról jobbra haladunk, ekkor $(x)(f \circ g) = ((x)f)g$. Ez olyan szempontból természetesebb, hogy olvasni is balról jobbra szoktunk. Mivel a Rubik-kocka vizsgálatánál használni fogok elég hosszú permutáció-kompozíciókat, és ezeknél sokkal egyszerűbb balról jobbra olvasni, hogy milyen forgatásokat alkalmazok, a szakdolgozatban végig a jobboldali konvenciót használom. [1]-ben a baloldali konvenció szerint szerepelnek a definíciók, tételek, ezért azzal összehasonlítva kissé máshogy festenek.

1.1.8. Definíció. Legyen X tetszőleges halmaz. Az S_X csoportot az X halmazon ható *szimmetrikus csoportnak* hívjuk.

Egyszerű példa bijekciókra az $\{1, 2, 3, \ldots, n\}$ halmaz permutációi. Ezt S_n-nel jelöljük, de természetesen az 1 és n közötti egész számok helyett bármi állhat, az ábécé első n betűje, vagy mint a Rubik-kocka esetében látni fogjuk, például a Rubik-kocka sarokkockái vagy ezek lapkái (ezekből háromszor annyi van). A permutációk azt írják le, hogy a halmaz elemei közül melyek „cserélnek helyet", ez a lényeg, nem az elemek maguk. A középiskolában tanult permutációfogalommal az kapcsolja össze, hogy az $\{1, 2, 3, \ldots, n\}$ elemek két különböző (vagy akár megegyező) sorrendjéhez egyértelműen tartozik egy permutáció, amely az elsőt a másodikba viszi. Általában persze az $123\ldots n$ alapsorrendhez viszonyítva szoktuk tekinteni a permutációkat.

A permutációkat többféleképp fel tudjuk írni. Például:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

Ez a permutáció az $1, 2, 3, 4, 5$ alapsorrendet a $2, 3, 1, 5, 4$-be viszi, tehát az 1-es a harmadik helyre, a 2-es az első helyre, a 3-as a második helyre, az 4-es az ötödik, az 5-ös pedig a negyedik helyre kerül.

A másik nagyon gyakori felírás ciklus(ok) segítségével történik. Ilyenkor az alapsorrendet nem tüntetjük fel, csak azt, hogy mi mivel cserél helyet. Az előző permutációt ciklusokkal például így tudjuk felírni:[2]

$$(123)(45)$$

[2]A példában szereplő felírást *diszjunkt ciklusok szorzataként való felírásnak* nevezzük, ebben minden elem legfeljebb egyszer szerepel, hamarosan szóba fog kerülni.

Egy ciklust persze többféleképp is fel lehet írni, mivel a benne szereplő elemek körbepermutálódnak, azaz $(123) = (231) = (312)$. Egy ciklus hosszán az elemei számát értjük.

A „legegyszerűbb" ciklusnak csak két eleme van, ezeket *transzpozíciónak* nevezzük. Minden permutáció felírható transzpozíciók szorzataként (kompozíciójaként). Egy permutáció *páros*, illetve *páratlan*, ha előáll páros, illetve páratlan sok transzpozíció szorzataként. Két páros permutáció szorzata páros, két páratlané szintén, egy páros és egy páratlan permutáció szorzata pedig páratlan. Emiatt a páros permutációk részcsoportot alkotnak, ezt *alternáló csoportnak* nevezzük, jele: A_n. Egy n hosszú ciklus felírható $n-1$ transzpozíció szorzataként, emiatt egy ciklus páros, ha hossza páratlan, illetve páratlan, ha hossza páros. A páros permutációk előjele $+1$, a páratlanoké -1 (jelölés: sg). (Az előjel pontos bevezetésétől most eltekintek.)

A ciklusfelbontásnak az igazi jelentősége abban rejlik, hogy minden permutációt fel lehet írni diszjunkt ciklusok szorzataként, és ez egyértelmű is a tényezők sorrendjétől eltekintve (két ciklus diszjunkt, ha nincs közös elemük, ilyenkor felcserélhetőek egymással). Könnyen belátható, hogy egy ciklus rendje a ciklus hosszával egyenlő, és tetszőleges permutációt diszjunkt ciklusok szorzataként felírva megkaphatjuk a permutáció rendjét is, a ciklusok rendjének legkisebb közös többszöröseként. Ezenkívül $|S_n| = n!$ (ez könnyen látszik abból, hogy az első felírási módnál az alapsorrend alá $n!$ különböző sorrendet írhatunk, és ezek mind más permutációt határoznak meg), és $|A_n| = n!/2$, mivel a páros és a páratlan permutációk száma egyenlő. Az itt összefoglaltak pontos részletei megtalálhatóak például [1]-ben.

1.1.9. Definíció. A G csoport *ciklikus*, ha létezik olyan $g \in G$, amelynek a csoport összes eleme hatványa. Ekkor g a csoport generátoreleme. A ciklikus csoportokat C_n-nel fogom jelölni, ahol n a generátorelem, egyúttal a csoport rendje.

Ciklikus csoportra példa a $\mathbb{Z}_n^+$ csoport. Ennek elemei $\{0, 1, \ldots, n-1\}$ az összeadást pedig mod n tekintjük. A Rubik-kocka esetében hasznát vesszük majd olyan csoportoknak, amelyek például egy adott alkockát forgatnak, ezek ciklikus csoportok lesznek. A generálással kapcsolatos másik fogalom, amelyre szükségem lesz még, a következő:

1.1.10. Definíció. Legyen G csoport, $X \subset G$. Az X által *generált részcsoport* ($\langle X \rangle$) a *legszűkebb* X-et tartalmazó részcsoportja G-nek, azaz, ha $X \subseteq H \leq G$, akkor $\langle X \rangle \leq H$.

$\langle X \rangle$ elemei pontosan az X elemei és inverzeik szorzataként felírható G-beli elemek. (Ha G véges, az inverzekre nincs szükség.)

A harmadik példám csoportra:

1.1.11. Definíció. Tekintsük a sík egybevágóságai közül azokat, amelyek egy adott szabályos n-szöget önmagába visznek. Ezek csoportot alkotnak a kompozícióra. Ezt a csoportot n-edfokú *diédercsoportnak* nevezzük, jele: D_n.

A diédercsoportnak $2n$ eleme van, n darab forgatás a sokszög középpontja körül (köztük az identitás), illetve n darab tükrözés (páros n esetén a szemben lévő csúcsokat összekötő átlókra, illetve a szemben lévő oldalak oldalfelező pontjait összekötő egyenesekre, páratlan n esetén egy-egy csúcs és a vele szemközti oldal felezőpontját összekötő szakaszra). Ezeket fel tudjuk írni a következőképp:

$$D_n = \{\mathrm{id} = f^n, f, f^2, \ldots, f^{n-1}, t, tf, tf^2, \ldots, tf^{n-1}\},$$

ahol f a középpont körüli $\frac{2\pi}{n}$ szögű forgatás, t pedig tetszőleges tükrözés az előbb felsoroltak közül. Ezenkívül $tft = f^{-1}$ (ez szemléletesen azt jelenti, hogy ha a sokszöget tükrözzük egy szimmetriatengelyére, elforgatjuk a középpontja körül, majd megint tükrözzük, akkor ugyanazt kapjuk, mintha az ellenkező irányba forgattuk volna).

1.1.12. Definíció. Legyen G csoport, $H \leq G$ és $g \in G$. A gH halmazt H szerinti bal, a Hg halmazt pedig jobb oldali mellékosztálynak hívjuk. Itt $gH = \{g*h, \text{ ahol } h \in H\}$, $Hg = \{h*g, \text{ ahol } h \in H\}$, és h végigfut H összes elemén.

1.1.13. Állítás. Legyen G csoport, $H \leq G$. A H szerinti jobb (bal) oldali mellékosztályok G egy partícióját adják.

1.1.14. Definíció. Legyen G csoport, $H \leq G$. A különböző H szerinti jobb oldali mellékosztályok számát H indexének nevezzük G-n belül. Jelölés: $|G : H|$.

1.1.15. Állítás. Legyen G véges csoport, $H \leq G$. Ekkor $|G| = |H| \cdot |G : H|$. Ebből következik, hogy egy véges csoport részcsoportjának rendje és indexe osztója a csoport rendjének, illetve bármely $g \in G$-re $o(g)$ osztója $|G|$-nek, mivel $\langle g \rangle = o(g)$.

1.1.16. Definíció. Legyen G csoport, $g_1, g_2 \in G$. Azt mondjuk, hogy g_1 és g_2 *konjugáltak*, ha létezik olyan $g_3 \in G$, hogy $g_3^{-1} * g_1 * g_3 = g_2$.

A konjugáltság ekvivalencia-reláció, osztályait G *konjugáltosztályainak* nevezzük.

1.1.17. Definíció. Legyen G csoport, és $g \in G$ adott elem. A $\phi_g : G \to G$, $(x)\phi_g = g^{-1}xg$ leképezést a g-vel vett *konjugálásnak* nevezzük.

1.1.18. Tétel. S_n-ben két permutáció akkor és csak akkor konjugált, ha a diszjunkt ciklusfelbontásukban ugyanannyi i hosszú ciklus található minden $i \in \{2, 3, \ldots, n\}$-re.

A tételből következik, hogy S_n-ben konjugált elemek rendje egyenlő.

1.1.19. Definíció. Legyen G_1 csoport a $*_1$ műveletre, és G_2 csoport a $*_2$ műveletre. Egy $\Psi : G_1 \to G_2$ leképezés *csoport-homomorfizmus*, ha művelettartó, azaz $\forall a, b \in G_1$-re teljesül, hogy

$$(a *_1 b)\Psi = (a)\Psi *_2 (b)\Psi.$$

Ha Ψ kölcsönösen egyértelmű G_1 és G_2 között, akkor Ψ *izomorfizmus*. Ekkor G_1 és G_2 *izomorf csoportok* (jelölés: $G_1 \cong G_2$).

1.1.20. Definíció. Egy $\phi : G \to H$ csoport-homomorfizmus *képén* az

$$\mathrm{Im}(\phi) = \{(g)\phi \,|\, g \in G\} \subseteq H$$

halmazt értjük, és ϕ *magján* a

$$\mathrm{Ker}(\phi) = \{g \in G : (g)\phi = 1_H\} \subseteq G$$

halmazt értjük, ahol 1_H H egységelemét jelöli.

1.1.21. Állítás. $\mathrm{Ker}(\phi)$ részcsoport G-ben, $\mathrm{Im}(\phi)$ részcsoport H-ban.

1.1.22. Definíció. A G csoport N részcsoportja *normálosztó*, ha létezik olyan G-n értelmezett homomorfizmus, amelynek N a magja. Jelölés: $N \lhd G$.

1.1.23. Tétel. Ha a G csoport N részcsoportja normálosztó, akkor minden $g \in G$-re $gN = Ng$.

Bizonyítás. Ha N normálosztó, akkor valamilyen $\phi : G \to H$ homomorfizmus magja. Vizsgáljuk meg, hogy mely G-beli elemek képe lesz adott $h \in \mathrm{Im}(\phi)$. Mivel $h \in \mathrm{Im}(\phi)$, létezik g, amelyre $(g)\phi = h$. Ekkor

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

Ugyanakkor:

$$(g)\phi = (g')\phi \iff 1_H = (g'g^{-1})\phi \iff g'g^{-1} \in \mathrm{Ker}(\phi) = N \iff g' \in Ng.$$

Az első egyenlet szerint h-ra a gN mellékosztály elemei, a második szerint az Ng mellékosztály elemei képződnek. Ezek tehát megegyeznek.

q. e. d.

1.1.24. Definíció. Legyen G csoport, és $N \lhd G$. G N-szerinti *faktorcsoportja* az a csoport, amelynek elemei G N szerinti mellékosztályai, a közöttük értelmezett művelet a következő:

$$g_1N * g_2N = (g_1g_2)N$$

Jelölés: G/N.

1.1.25. Állítás. Az előbb definiált faktorcsoport valóban csoport.

Bizonyítás. A csoporttulajdonságokon kívül azt is be kell látni, hogy a definiált művelet nem ellentmondásos, mivel létezhetnek olyan g_1, g_1' és $g_2, g_2' \in G$, amelyekre $g_1N = g_1'N$, illetve $g_2N = g_2'N$. Belátom, hogy a felírás módjától függetlenül ugyanazt az eredményt kapjuk, azaz a felírt művelet *jóldefiniált*. Mivel N normálosztó, az előző tétel alapján $gN = Ng\ \forall g \in G$. Ezt felhasználhatjuk a következő módon:

$$(g_1N)*(g_2N) = (g_1g_2)N = g_1Ng_2 = g_1'Ng_2 = g_1'g_2N = g_1'g_2'N = (g_1'N)*(g_2'N).$$

A zártság következik G zártságából, a faktorcsoport egységeleme N lesz, mivel ezt felírhatjuk $1N$-ként, és tetszőleges gN mellékosztály inverze $g^{-1}N$ lesz. Az asszociativitás is teljesül, mivel:

$$((g_1N) * (g_2N)) * (g_3N) = (g_1g_2N) * g_3N = g_1g_2g_3N,$$

és

$$(g_1N) * ((g_2N)) * (g_3N)) = g_1N * (g_2g_3N) = g_1g_2g_3N.$$

q. e. d.

1.1.26. Tétel. Ha $N \leq G$ és minden $g \in G$-re $gN = Ng$, akkor N normálosztó.

Bizonyítás. Vegyük észre, ahhoz, hogy az N szerinti mellékosztályok szorzása jóldefiniált legyen, nincs szükség arra, hogy N normálosztó, a bizonyításban azt használtuk ki, hogy $gN = Ng \; \forall g \in G$ (ami persze következik abból, hogy N normálosztó). Tehát a $(g)\Psi = gN$ leképezés csoport-homomorfizmus. Mi lesz Ψ magja? Azon $g \in G$-k, amelyekre igaz, hogy $gN = N$, azaz $g \in N$ (mivel N részcsoport). Tehát N egy homomorfizmus magja, azaz normálosztó.

q. e. d.

Az előző két tételt összefoglalva:

1.1.27. Tétel. A G csoport N részcsoportja akkor és csak akkor normálosztó, ha minden $g \in G$-re $gN = Ng$.

1.1.28. Tétel. A G csoport N részcsoportja akkor és csak akkor normálosztó, ha zárt a konjugálásra, azaz minden $g \in G$ esetén $g^{-1}Ng = N$ ($g^{-1}Ng = (g^{-1}ng \,|\, n$ befutja N-t)).

Bizonyítás. Ez közvetlenül adódik az előző tételből, hiszen a $gN = Ng$ egyenletet balról g^{-1}-gyel szorozva az állítást kapjuk.

q. e. d.

1.1.29. Tétel. (homomorfizmus-tétel) Ha G és H csoportok, és létezik $\phi : \; G \; \rightarrow \; H$ homomorfizmus, akkor $\mathrm{Im}(\phi) \cong G/\mathrm{Ker}(\phi)$.

1.1.30. Definíció. A G csoportot önmagába képző homomorfizmusokat *endomorfizmusnak* nevezzük. Amennyiben kölcsönösen egyértelmű is egy ilyen leképezés, akkor *automorfizmusról* beszélünk. A *belső automorfizmusok* G konjugálásai. Egy G csoport automorfizmusai csoportot alkotnak a kompozíció műveletére, ez G *automorfizmus-csoportja*, jele $\mathrm{Aut}(G)$. A belső automorfizmusok szintén csoportot alkotnak, jele $\mathrm{Inn}(G)$.

A ψ_g leképezés (a g elemmel vett konjugálás) automorfizmusa G-nek, továbbá a $\psi : G \rightarrow \mathrm{Aut}(G)$, $(g)\psi = \psi_g$ leképezés homomorfizmus. Ennek képe $\mathrm{Inn}(G)$, magja pedig a $Z(G) := \{g \in G \,|\, g^{-1}xg = x$ minden $x \in G$-re$\}$ részcsoport, ezt G *centrumának* nevezzük. Könnyen látszik, hogy a centrum elemei minden G-beli elemmel felcserélhetőek. 1.1.29 szerint $G/Z(G) \cong \mathrm{Inn}(G)$. Ezenkívül $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

1.2. Permutációcsoportok

Az itt következő csoportelméleti fogalmakat fogom elsősorban a Rubik-kocka vizsgálatánál felhasználni, az itt következő részt nagyrészt [1] alapján írtam, konkrétan a 4. fejezet ötödik és tizenkettedik alfejezete alapján. A más forrásokat és az önálló részeket külön megemlítem.

1.2.1. Definíció. Az S_X szimmetrikus csoport részcsoportjait *transzformációcsoportoknak*, véges $|X|$ esetén *permutációcsoportoknak* nevezzük.

Mivel a Rubik-kocka esetében mindig véges halmazokat vizsgálunk, ezért csak a permutációcsoportokkal foglalkozom érdemben. A következő definíciót [2] alapján mondom ki (90. oldal, 70. definíció).

1.2.2. Definíció. $g_1, g_2, \ldots, g_n$ legyenek a véges X halmaz permutációi (tehát minden i-re $g_i \in S_X$). Tekintsük a következő véges hosszúságú „szavakat":

$$g = x_1 x_2 \ldots x_m, \quad m > 0,$$

ahol minden $x_i \in \{g_1, \ldots, g_n\}$. Ezeknek a „szavaknak" a halmazát jelölje G. Ekkor azt mondjuk, hogy a G permutációcsoportot *generálja* $g_1, g_2, \ldots, g_n$. Jelölés: $G = \langle g_1, g_2, \ldots, g_n \rangle \subset S_X$.

Ez a definíció összhangban van az általánosabb 1.1.10 definícióval (ld. az 1.1.10 utáni megjegyzés).

A szimmetrikus csoport definíciójában használtam azt a kifejezést, hogy egy csoport hat egy halmazon. Ennek pontos definíciója a következő:

1.2.3. Definíció. Egy G csoport *hat* az X halmazon, ha bármely $g \in G$-re és $x \in X$-re $x * g \in X$ (ebbe természetesen beleértem, hogy a művelet értelmezve van az összes megfelelő elem között), illetve minden $g_1, g_2 \in G$-re és $x \in X$-re teljesül, hogy

$$(x * g_1) * g_2 = x * (g_1 g_2).$$

Ezenkívül G egységeleme identikusan hat X-en.

Könnyű belátni, hogy teljesül a következő állítás:

$$x * g = y \iff y * g^{-1} = x$$

A bal oldali egyenlőséget szorozzuk meg jobbról g inverzével. A hatás definíciója szerint azt kapjuk:

$$(x * g) * g^{-1} = x * (g^{-1}g) = x * 1 = x = y * g^{-1}.$$

A másik irány hasonlóan adódik, csak a jobb oldali egyenlőséget kell jobbról g-vel szorozni.

Példa. S_n konjugálásai kapcsán is definiálhatunk egy hatást, a mi céljainknak megfelel, ha olyan permutációkra tesszük meg, amelyek ciklusok, legyen $g, h \in S_n$, és $h = (h_1, h_2, \ldots, h_k)$ (minden $h_i \in \{1, 2, \ldots, n\}$). Ekkor

$$g^{-1}hg = (h_1 * g, h_2 * g, \ldots, h_k * g),$$

ahol $h_1 * g = (h_1)g$. Ha egy permutáció több diszjunkt ciklus szorzata, akkor is hasonlóan kell eljárni külön-külön minden ciklussal.

1.2.4. Definíció. G legyen csoport, hasson X-en. Ha minden $g \in G$ elemhez vesszük a $(g)\Psi = X * g$ leképezést, képként egy X-en ható permutációcsoportot kapunk. Ekkor $\Psi : G \to S_X$ homomorfizmus. Magját a *hatás magjának* nevezzük. A hatás *hű*, ha magja csak az egységelemből áll, ekkor Ψ injektív.

Valóban homomorfizmust kaptunk, mivel $(g_1g_2)\Psi = X * (g_1g_2) = (X * g_1) * g_2 = (g_1)\Psi(g_2)\Psi$. A hatás magja (N) azon G-beli elemekből áll, amelyekre minden $x \in X$ esetén $x * g = x$, vagyis az összes X-beli elem stabilizátorának metszete. Ekkor $G/N \cong \mathrm{Im}(\Psi)$.

1.2.5. Definíció. Legyen G csoport, és hasson X-en. Az $x \in X$ elem *orbitja* vagy *pályája* azon X-beli elemekből áll, amelyekbe G-beli elemekkel x átvihető. Jelölése: $G(x)$. Az orbit *hosszán* $G(x)$ elemeinek számát értjük. Jelölése: $|G(x)|$.

G hatása X-en *tranzitív*, ha X bármely két elemét egymásba lehet vinni alkalmas G-beli elemmel. Ilyenkor X-nek egyetlen orbitja van, azaz $G(x) = X$.

1.2.6. Definíció. Legyen G csoport, és hasson X-en. Egy $x \in X$ elem G-beli *stabilizátorán* azon $g \in G$ elemek összességét értjük, amelyekre $x * g = x$ (azaz *fixen hagyják* x-et). Jelölése: G_x. Ilyenkor x *fixpontja* g-nek. $G_x \leq G$, mivel ha g_1 és g_2 fixen hagyja x-et, akkor a kompozíciójuk is. Az egységelem – mivel mindent fixen hagy – szintén eleme a stabilizátornak. Az asszociativitás természetesen ugyanúgy érvényes, mint G-ben. Az is könnyedén látszik, hogy ha $g \in G_x$, akkor $g^{-1} \in G_x$.

1.2.7. Tétel. (Orbit-stabilizátor tétel) Legyen G csoport, és hasson X-en. X elemeinek orbitjai X egy partícióját alkotják. Igaz továbbá a következő egyenlet bármely $x \in X$ esetén:

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

Ha $|X|$ véges, akkor ebből, illetve a $|G| = |G_x| \cdot |G : G_x|$ egyenletből következik, hogy

$$|G| = |G(x)| \cdot |G_x|.$$

Bizonyítás. Tekintsük a következő ekvivalencia-relációt: $x \sim y \iff \exists g \in G : x * g = y$. Ennek osztályai maguk az orbitok.

Az egyenlet azt fejezi ki, hogy az x pont pályájának hossza megegyezik az x stabilizátora szerint vett jobb oldali mellékosztályok számával. Tegyük fel, hogy $g_1, g_2 \in G$ hatása megegyezik az $x \in X$ ponton:

$$x * g_1 = x * g_2 \iff x * (g_2 g_1^{-1}) = x \iff g_2 g_1^{-1} \in G_x \iff g_2 \in G_x g_1.$$

Tehát egy adott mellékosztály minden eleme ugyanoda viszi x-et, különböző mellékosztályok elemei különböző helyekre. Mivel a mellékosztályok G egy partícióját adják, x orbitjának minden eleme előáll, így x orbitjának elemei kölcsönösen egyértelműen megfeleltethetőek az x stabilizátora szerinti mellékosztályokkal, tehát az orbit hossza valóban egyenlő a stabilizátor indexével.

q. e. d.

1.2.8. Definíció. Legyen G csoport, és hasson X-en. Egy X elemei között értelmezett ekvivalencia-relációt *kongruenciának* nevezünk, ha minden $x, y \in X$ és minden $g \in G$ esetén $x \sim y \iff x * g \sim y * g$.

Két kongruencia mindig létezik, ha G vagy X nem egyelemű (de ezek nem túl érdekes esetek). Ezeket *triviális kongruenciáknak* nevezzük. Az egyik triviális kongruencia, mikor minden X-beli elem önmagában egy osztály, ezt 0_X-szel jelölöm, a másik, mikor minden X-beli elem egy osztályba tartozik, ezt pedig 1_X-szel. Mivel minden kongruencia ekvivalencia-reláció, ezért a kongruencia-osztályok (*blokkok*) X egy partícióját alkotják, és ennek a partíciónak olyan tulajdonsága is van, hogy minden $g \in G$ permutálja ezeket az osztályokat. Algebrai formában: $X = \Delta_1 \cup \ldots \cup \Delta_k$, és minden $g \in G$ és minden $i \in \{1, 2, \ldots, k\}$ esetén létezik $j \in \{1, 2, \ldots, k\}$, hogy $(\Delta_i)g = \Delta_j$. Másrészt ha van egy ilyen tulajdonságú partíciója X-nek, akkor $x \sim y \iff \exists i : x, y \in \Delta_i$ kongruenciája a csoporthatásnak.

1.2.9. Definíció. Legyen G csoport, és hasson X-en. Ha X-nek pontosan két kongruenciája van G szerint, és G tranzitíven hat X-en, akkor G hatását X-en *primitívnek* nevezzük. Ha egy hatás nem primitív, akkor *imprimitív*. Amennyiben egy G csoport hatását adott X halmazon tekintjük, ezt úgy is mondhatjuk, hogy G primitív/imprimitív.

Ha $|X| > 2$ ($|X| = 2$ esetén értelemszerűen csak a két triviális kongruencia lehetséges) és $|G| > 1$, akkor a tranzitivitás feltétele felesleges, mivel abból, hogy G primitív, következik a tranzitivitás. Ugyanis X orbitjai egy kongruenciát határoznak meg, és ez nem lehet 0_X, tehát 1_X.

1.3. Direkt szorzat, szemidirekt szorzat, koszorúszorzat

Ezt a fejezetet [1] *Csoportok A direkt szorzat* című alfejezete alapján dolgoztam ki, kivéve a koszorúszorzatos részt, azt témavezetői segítséggel.

1.3.1. Definíció. Legyenek $G_1, \ldots, G_n$ csoportok. Tekintsük a $(g_1, \ldots, g_n)$ sorozatokat, ahol $g_i \in G_i \ \forall\ 1 \leq i \leq n$-re. Ezek a sorozatok a $G_1 \times \ldots \times G_n$ halmaz elemei. Két elem szorzatát tagonként vesszük, azaz:

$$(g_1, \ldots, g_n) * (h_1, \ldots, h_n) = (g_1 *_1 h_1, \ldots, g_n *_n h_n),$$

ahol $*_i$ a G_i csoport művelete. Csoportot kaptunk, és a $G_1 \times \ldots \times G_n$ csoport a $G_1, \ldots, G_n$ csoportok *direkt szorzata*. Adott G csoport esetén a $G \times \ldots \times G$ n-tényezős direkt szorzatot G n-edik *direkt hatványának* nevezzük.

Ellenőrizzük gyorsan a csoport-tulajdonságokat! Mivel minden G_i zárt a maga műveletére, ha tagonként végezzük el őket, a zártság megőrződik. A direkt szorzat egységeleme $(1_1, 1_2, \ldots, 1_j, \ldots, 1_n)$, ahol 1_i a G_i csoport egységelemét jelöli. Az inverz képzése a következő módon történik:

$$(g_1, g_2, \ldots, g_j, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_j^{-1}, \ldots, g_n^{-1}).$$

Az egyenlőség jobb oldalán a zárójelen belül adott g_i elem G_i-beli inverze szerepel. Hasonlóan belátható, hogy az asszociativitás is megmarad tagonként. A következő tétel megmutatja, milyen feltételek mellett lehet egy csoportot két részcsoportjának direkt szorzataként felírni:

1.3.2. Tétel. Ha a G csoport két normálosztójára, N_1-re és N_2-re teljesül, hogy $N_1 \cap N_2 = \{1\}$, és $G = N_1N_2 = \{n_1n_2 \,|\, n_1 \in N_1,\ n_2 \in N_2\}$, akkor $G \cong N_1 \times N_2$.

Most a direkt szorzat egy általánosabb verziója következik:

1.3.3. Definíció. N, H legyen csoport, és $\Psi : H \to \mathrm{Aut}(N)$ tetszőleges homomorfizmus. Tekintsük az (n, h) rendezett párok halmazát (ahol $n \in N$, $h \in H$), és legyen a $*$ művelet a következő:

$$(n_1, h_1) * (n_2, h_2) = ((n_1)((h_2)\Psi)\, n_2, h_1h_2).$$

Csoportot kapunk, amelyet N és H *szemidirekt szorzatának* nevezünk. Jelölés: $N \rtimes_\Psi H$.

Ellenőrizzük most is a csoport-tulajdonságokat! A képletben szereplő $(h_2)\Psi$ függvény N automorfizmusa, tehát $(n_1)((h_2)\Psi) \in N$. Emiatt a felírt $*$ műveletre zárt a szemidirekt szorzat. Az egységelem az $(1_N, 1_H)$. Tetszőleges (n, h) elem inverze:

$$(n, h)^{-1} = ((n^{-1})((h^{-1})\Psi), h^{-1}).$$

Végül az asszociativitás:

$$\begin{aligned}(n_1, h_1) * ((n_2,h_2) * (n_3, h_3)) &= (n_1, h_1) * ((n_2)((h_3)\Psi)\, n_3, h_2h_3) = \\ &= ((n_1)((h_2h_3)\Psi)\, (n_2)((h_3)\Psi)\, n_3, h_1h_2h_3)\end{aligned}$$

és

$$\begin{aligned}((n_1, h_1) * (n_2,h_2)) * (n_3, h_3)) &= ((n_1)((h_2)\Psi)\, n_2, h_1h_2) * (n_3, h_3) = \\ &= (((n_1)((h_2)\Psi)\, n_2)((h_3)\Psi)\, n_3, h_1h_2h_3) = \\ &= ((n_1)((h_2h_3)\Psi)\, (n_2)((h_3)\Psi)\, n_3, h_1h_2h_3).\end{aligned}$$

(A második számításnál a harmadik sor azért igaz, mert Ψ homomorfizmus, tehát művelettartó.)

1.3.4. Tétel. Ha $G = N \rtimes_\Psi H$, és $N_1 = \{(n, 1_H) \,|\, n \in N\}$, $H_1 = \{(1_N, h) \,|\, h \in H\}$, akkor $N_1 \lhd G$, $H_1 \leq G$, $N_1 \cap H_1 = (1_N, 1_H)$, $N_1H_1 = G$, illetve $N_1 \cong N$ és $H_1 \cong H$ teljesül. Ezenkívül H_1 úgy hat konjugálással N_1-en, ahogy azt a Ψ homomorfizmus megadja:

$$(1, h)^{-1}(n, 1)(1, h) = (1, h^{-1})((n)((h)\Psi), h) = ((n)((h)\Psi), 1)$$

Amit a későbbiek szempontjából fontos még megjegyezni, hogy a szemidirekt szorzat definíciójában szereplő Ψ homomorfizmus tulajdonképpen egy hatást definiál, a H csoport hatását N-en mint halmazon. Illetve példaként megemlítem, hogy adott G csoport k-adik direkt hatványának automorfizmusa a koordináták tetszőleges permutációja, azaz S_k beleágyazódik $\mathrm{Aut}(G^k)$-ba. Így képezhetjük a $G^k \rtimes S_k$ szemidirekt szorzatot, amely jó példa a következő (számunkra fontos) koszorúszorzatra is.

1.3.5. Definíció. Legyen H és K csoport, K hasson Δ-n. $\Delta = (\delta_1, \delta_2, \ldots, \delta_l)$. H^Δ jelölje H l-edik direkt hatványát, a koordináták legyenek $(\delta_1, \delta_2, \ldots, \delta_l)$, azaz H^Δ elemei $(h_{\delta_1}, h_{\delta_2}, \ldots, h_{\delta_l})$ alakúak, ahol minden $h_{\delta_i} \in H$ minden $\delta_i \in \Delta$-ra.

Ekkor H és K *koszorúszorzata* a következő:

$$H \text{ wr } K = H^\Delta \rtimes K$$

A szemidirekt szorzatban az előző definíció szerinti Ψ homomorfizmust K hatásából kapjuk, ugyanis K hasson úgy H^Δ koordinátáin, mint Δ-n.

Részletezve:

$$\begin{aligned}&((h_{\delta_1}, h_{\delta_2}, \ldots, h_{\delta_l}), k) \cdot ((h'_{\delta_1}, h'_{\delta_2}, \ldots, h'_{\delta_l}), k') = \\ &= ((h_{\delta_1}, h_{\delta_2}, \ldots, h_{\delta_l}) * k' (h'_{\delta_1}, h'_{\delta_2}, \ldots, h'_{\delta_l}), kk'),\end{aligned}$$

ahol $\cdot$ a koszorúszorzatbeli műveletet, $*$ pedig K hatását jelöli.

A direkt szorzat és a szemidirekt szorzat definíciójából adódik, hogy a koszorúszorzat valóban csoport. Megjegyzem még, hogy $|H \text{ wr } K| = |H|^{|\Delta|} \cdot |K|$. Az előző definíció a koszorúszorzatot mint absztrakt csoportot határozza meg. Ha nemcsak K, hanem H is hat egy véges halmazon, akkor a koszorúszorzat (imprimitív) hatását a következőképpen értelmezhetjük:

1.3.6. Definíció. Legyen H és K csoport, H hasson Γ-n (illetve $H \leq S_\Gamma$), K hasson Δ-n (illetve $K \leq S_\Delta$). Legyenek $\Gamma = (\gamma_1, \gamma_2, \ldots, \gamma_k), \Delta = (\delta_1, \delta_2, \ldots, \delta_l)$. Ekkor $G = H$ wr K hat $\Gamma \times \Delta$-n, illetve $G \leq S_{\Gamma \times \Delta}$, ahol $\Gamma \times \Delta = \{(\gamma, \delta) | \gamma \in \Gamma, \delta \in \Delta\}$, és G hatása a következő:

$$((h_1, h_2, \ldots, h_l), k)(\gamma, \delta_i) = (h_i(\gamma), k(\delta_i))$$

Példa. A négyzet szimmetriacsoportja, D_4 előáll mint két csoport koszorúszorzata, ugyanis $D_4 = H$ wr K, ahol $H \cong C_2$, $K \cong C_2$. H az egyik átlóra

vett tükrözés által generált csoport, K pedig egy oldalfelezőre vett tükrözés által generált csoport.
Ha $\Delta > 1$ és $\Gamma > 1$, akkor $\Gamma \times \Delta$-nak létezik nemtriviális kongruenciája. Vegyük ugyanis a $\Delta_1 = \{(\gamma_i, \delta_1) \,|\, 1 \leq i \leq k\}, \Delta_2 = \{(\gamma_i, \delta_2) \,|\, 1 \leq i \leq k\}, \ldots, \Delta_l = \{(\gamma_i, \delta_l) \,|\, 1 \leq i \leq k\}$ halmazokat. A $(\gamma_i, \delta_j) \sim (\gamma'_i, \delta'_j) \iff \delta_j = \delta'_j$ reláció ekvivalenciareláció, osztályai az előbb megadott halmazok, és G szerint kongruenciát alkotnak, mivel tetszőleges $g \in G$ elemre $g(\gamma_i, \delta) \sim g(\gamma'_i, \delta)$.

1.3.7. Tétel. Ha a $G \leq S_X$ permutációcsoport imprimitíven és tranzitívan hat a véges X halmazon, akkor léteznek Y, Z halmazok, egy $X = Y \times Z$ megfeleltetés, továbbá $H \leq S_Y$ és $K \leq S_Z$ csoportok, amelyekre igaz, hogy $G \leq H$ wr K, ahol H wr K hat $X = Y \times Z$-n.

Még a bizonyítás előtt belátok egy állítást, amelyet felhasználok a bizonyításban.

1.3.8. Állítás. Ha $G \leq S_X$ tranzitív permutációcsoport, és $\sim$ X G szerinti kongruenciája, akkor $\sim$ minden osztálya ugyanannyi elemből áll.

Bizonyítás. Legyen X_1, $X_2 \sim$ két tetszőleges osztálya, és $x_1 \in X_1$, $x_2 \in X_2$. Mivel G tranzitív, létezik olyan $g \in G$, amelyre $(x_1)g = x_2$. Mivel $\sim$ kongruencia, $(X_1)g \subseteq (X_2)$, és tudjuk még, hogy $|(X_1)g| = |X_1|$, mivel g permutáció. Tehát $|X_1| \leq |X_2|$. Ugyanakkor $(x_2)g^{-1} = x_1$, és így $(X_2)g^{-1} \subseteq (X_1)$, $|(X_2)g^{-1}| = |X_2|$ tehát $|X_2| \leq |X_1|$. A két egyenlőtlenségből adódik, hogy $|X_1| = |X_2|$.

q. e. d.

Az állítás bizonyításából az is látszik, hogy ha G nem tranzitív permutációcsoport, X két kongruencia-osztálya akkor feleltethető meg egyértelműen egymásnak, ha van egy-egy elemük, amelyek ugyanahhoz az orbithoz tartoznak.

Most rátérek a tétel bizonyítására:

Bizonyítás. Az X halmazból konstruktívan származtatjuk a H és K csoportokat. Mivel G imprimitíven hat X-en, X-nek létezik nemtriviális kongruenciája. Legyen X-nek ezen kongruencia szerinti osztályokra bontása:

$$X = X_1 \cup X_2 \cup \ldots \cup X_l,$$

ahol minden $1 \leq i \leq l$ esetén $1 < |X_i| < |X|$, illetve minden $1 \leq i, j \leq l$ és $i \neq j$ esetén $X_i \cap X_j = \emptyset$. Az X-beli tranzitivitás miatt G tranzitívan hat

a $\Delta := \{X_1, X_2, \ldots, X_l\}$ halmazon, pontosabban tranzitívan permutálja Δ elemeit, illetve az előző állítás miatt minden $1 \leq i, j \leq l$ esetén $|X_i| = |X_j|$. Minden X_i halmazra tekintsük a következő részcsoportokat G-n belül:

$$M_i = \{g \mid (X_i)g = X_i\}$$
$$N_i = \{g \mid (x_i)g = x_i \ \forall x_i \in X_i\}.$$

M_i tehát X_i mint halmaz stabilizátora, N_i pedig X_i pontonkénti stabilizátora. Világos, hogy $N_i \leq M_i$. Ha M_i hatását csak X_i-n vizsgáljuk, ezen hatás magja N_i, így $N_i \lhd M_i$. Definiáljuk ezek segítségével az X_i-n ható H_i csoportot:

$$H_i := M_i/N_i \leq S_{X_i}$$

Itt tulajdonképpen arról van szó, hogy minden M_i hat X_i-n, tehát M_i összes eleméhez hozzárendelhetjük az $(m)\Phi = X_i * m$ permutációt, és N_i-vel faktorizálva X_i egy permutációcsoportját kapjuk. Most tekintsük a következő részcsoportját G-nek: $M := M_1 \cap M_2 \ldots \cap M_l$, amely Δ-n hat. Ez részcsoportja $H_1 \times H_2 \times \ldots \times H_l$-nek. Mivel G tranzitívan permutálja egymás között az X_i-ket, $(X_i)g = X_j$ esetén $g^{-1}H_i g = H_j$ teljesül, tehát a H_i-k mind konjugált részcsoportok G-ben, így izomorfak. M minden X_i halmazt önmagába képez, tehát az összes $X_i \in \Delta$ elem stabilizátorainak metszete, így normálosztó G-n belül. Innen kapjuk K-t:

$$K := G/M \leq S_\Delta$$

Most is hasonló okokból faktorizáltam, mint az előbb. Tehát $G \leq H$ wr $K \leq S_{X_1}$ wr $S_\Delta \cong S_{|X_1|}$ wr $S_{|\Delta|}$.

q. e. d.

1.4. Permutációcsoportok, generátorok

A következő pár tétel arról szól, hogy milyen elemekkel tudjuk generálni S_n-t vagy A_n-t, illetve hogy legaláb hány generátorelemre van szükség. Ezt a részt részben témavezetői javaslatra, részben saját ötlet miatt önállóan dolgoztam ki. Elsőnek egy segédtétel és néhány ahhoz kapcsolódó definíció. Legyen c_1 és c_2 két tetszőleges ciklus. Ekkor $c_1 \cup c_2$ és $c_1 \cap c_2$ a ciklusokon mint halmazokon értelmezett műveletek. Ezenkívül értelmezzük a $\sim_\cap$ relációt a következő módon:

$$c_1 \sim_\cap c_2 \iff c_1\text{-nek és } c_2\text{-nek van közös eleme.}$$

Világos, hogy $\sim_\cap$ nem ekvivalencia-reláció, mivel nem teljesül a tranzitivitás. Adott $C = \{c_1, c_2, \ldots, c_k\}$ halmaz esetén, amelynek minden eleme S_n-beli ciklus, legyen $G(C)$ az az egyszerű gráf, amelyben a csúcsok C elemei, és c_i és c_j között akkor megy él, ha $c_i \sim_\cap c_j$, és $i \neq j$.

1.4.1. Lemma. Adott a $C = \{c_1, c_2, \ldots, c_k\}$ halmaz, amelyben minden $c_i \in S_n$ ciklus. A $\langle C \rangle$ csoport tranzitíven hat az $\{1, 2, \ldots, n\}$ halmazon akkor és csak akkor, ha

$$(1)\ \bigcup_{i=1}^{k} c_i = \{1, 2, \ldots, n\},$$

és (2) $G(C)$ összefüggő.

Bizonyítás. Tegyük fel, hogy $\langle C \rangle$ tranzitív, de (1) vagy (2) nem teljesül. Ha (1) nem teljesül, az azt jelenti, hogy létezik $i \in \{1, 2, \ldots, n\}$, amely minden c_i-nek fixpontja, de ekkor $\langle C \rangle$ nem lehet tranzitív. Ha (1) teljesül, de (2) nem, az azt jelenti, hogy vannak olyan $i \neq j$ számok, amelyek nem vihetők egymásba. Most tegyük fel, hogy (1) és (2) teljesül. Ekkor X legyen egy orbitja $\langle C \rangle$-nek. Jelöljük A-val azon c_i ciklusok halmazát, amelyeknek van közös elemük X-szel. Ha valamely $c_i \in A$, akkor c_i minden eleme X-beli, mivel c_i alkalmas hatványával X-beli elembe vihető. Ez viszont azt jelenti, hogy az A-nak megfelelő csúcshalmazból nem megy ki él $G(C)$-ben. (2) miatt $A = C$, (1) miatt pedig $X = \{1, 2, \ldots, n\}$.

q. e. d.

A lemma kapcsán feltehető a kérdés, hogy legalább hány l hosszúságú ciklusra van szükség, hogy az általuk generált csoport tranzitív legyen. Adott $c_1, \ldots, c_k$ esetén a ciklusok indexét írjuk át úgy, hogy minden $1 < j \leq k$ esetén a $c_1, \ldots, c_j$ ciklusoknak megfelelő csúcsokra összefüggő részgráf illeszkedik $G(C)$-ben. Ebben az esetben c_1 l elemet tartalmaz $\{1, \ldots, n\}$-ből, minden további elem pedig legfeljebb $l - 1$ új elemet ad hozzá $c_1 \cup \ldots \cup c_{j-1}$-hez. Ezek szerint annak, hogy $c_1, \ldots, c_k$ tranzitív legyen, szükséges feltétele, hogy $k \geq \lceil \frac{n-l}{l-1} + 1 \rceil = \lceil \frac{n-1}{l-1} \rceil$, és az érvelés alapján látszik, hogy mindig meg tudunk adni $\lceil \frac{n-1}{l-1} \rceil$ darab olyan l hosszúságú ciklust, amelyek tranzitívan hatnak $\{1, 2, \ldots, n\}$-en.

1.4.2. Tétel. Ha az adott $T = \{t_1, t_2, \ldots, t_k\} \subset S_n$ halmaz minden eleme transzpozíció, és a T által generált csoport tranzitívan hat az $\{1, 2, \ldots, n\}$ halmazon, akkor $\langle T \rangle = S_n$.

Bizonyítás. Tudjuk, hogy minden permutáció előáll transzpozíciók szorzataként, tehát ha sikerül belátni, hogy $t_1, \ldots, t_k$ generál minden transzpozíciót, kész vagyunk. Mivel $\langle T \rangle$ tranzitíven hat az $\{1, 2, \ldots, n\}$ halmazon, teljesül az 1.4.1-ben szereplő (1) és (2). Vegyünk két generátorelemet, amelyeknek van közös elemük: (ab) és (ac). Teljesül a következő egyensőség:

$$(ab)(ac)(ab) = (bc).$$

Tehát konjugálással megkapjuk az $\{a, b, c\}$ halmaz összes transzpozícióját, és 1.4.1 alapján minden $\{1, 2, \ldots, n\}$-beli számhoz létezik olyan generátorelem, amely tartalmazza. Mivel $G(T)$ összefüggő, bármely két generátorelem között vezet út, és ha a szomszédos csúcsokként reprezentált transzpozíciókat konjugáljuk egymással, akkor „bárkihez eljuthatunk". Így megkapjuk az összes transzpozíciót.

q. e. d.

1.4.3. Tétel. Ha az adott $H = \{h_1, h_2, \ldots, h_k\} \subset S_n$ halmaz minden eleme hármasciklus, és a H által generált csoport tranzitívan hat az $\{1, 2, \ldots, n\}$ halmazon, akkor $\langle H \rangle = A_n$.

Bizonyítás. Elsőnek belátom, hogy a hármasciklusok generálják A_n-t. Minden A_n-beli permutáció felírható páros sok transzpozíció szorzataként, így elég megmutatni, hogy két transzpozíció szorzatát meg tudjuk adni hármasciklusok szorzataként. Ha diszjunkt transzpozíciókról van szó, akkor a következő egyenlet szerint kell eljárni:

$$(abc)(abd) = (ad)(bc).$$

Ha pedig két transzpozíciónak van közös eleme, akkor $(ab)(ac) = (abc)$, és kész vagyunk.

Most már csak azt kell belátni, hogy $\langle H \rangle$ generálja az összes hármasciklust. Vegyünk két generátorelemet, amelyeknek van közös elemük: $h_1 = (abc)$, $h_2 = (cde)$. Megmutatom, hogy e két generátorelemből generálni tudjuk az $\{a, b, c, d, e\}$ halmaz összes hármasciklusát (előfordulhat, hogy két elem is megegyezik, de ez a lényegen nem változtat). A konjugálás jelenti a kulcsot:

$$(ced)(abc)(cde) = (dab)$$

Az inverzzel vett konjugálás kiadja (eab)-t, és további konjugálásokkal valóban megkapjuk $\{a, b, c, d, e\}$ összes hármasciklusát. 1.4.1 alapján minden

$\{1, 2, \ldots, n\}$-beli számhoz létezik olyan generátorelem, amely tartalmazza. Mivel $G(H)$ összefüggő, bármely két generátorelem között vezet út, és ha a szomszédos csúcsokként reprezentált hármasciklusokat konjugáljuk egymással, akkor „bárkihez eljuthatunk". Így megkapjuk az összes hármasciklust, ezekről pedig már beláttam, hogy generálják A_n-t.

q. e. d.

Példa. A 15-ös puzzle néven ismert játék bizonyára mindenkinek ismerős, de azért röviden összefoglalnám a lényegét: adott 15 kis kocka egy táblán belül, rajtuk az egész számok 1 és 15 között. A táblába 16 kis kocka fér, de az egyik helye üres. A játék lényege, hogy a kis kockákat a rájuk írt számok szerint növekvő sorrendbe állítsuk, és csak a kockák tologatásával változtathatunk a helyzetükön, a táblából nem vehetjük ki őket. Egy kép a megoldott pozícióról:

Tekintsük azokat a helyzeteket, amikor a lyuk a jobb alsó sarokban található. Az olyan tologatások, amelyek ilyen helyzetből indulnak, és ilyenbe helyzetbe jutnak, csoportot alkotnak, ez a 15-ös puzzle csoportja, jelöljük G_{15}-tel. Világos, hogy egy-egy ilyen tologatássorozat egy permutációnak felel meg, a kockákra írt számok permutálódnak egymás között. Tehát $G_{15} \leq S_{15}$. Milyen elemek generálhatják G_{15}-öt? Vegyük a megoldott helyzetet, és jelöljük a lyukat 16-ossal! Ha csak egy „kört teszünk" a lyukkal az óramutató járásával megegyező irányban, azt a $(16, 15)(15, 11)(11, 12)(12, 16) = (11, 15, 12)$ permutáció írja le. Ha bármely másik három L alakban elhelyezkedő kockát szeretnénk körbepermutálni, megtehetjük úgy, hogy az L-et négyzetté kiegészítő helyre visszük a lyukat, ott hasonlóan járunk el, majd ugyanazon útvonalon visszavisszük a lyukat. Mivel az L kockáinak cseréje független az odaút és a visszaút cseréitől, és ezek egymás inverzei, így az eredmény az

L elemeinek egy hármasciklusa lesz. Az így kapott hármasciklusok teljesítik 1.4.3 feltételeit, azaz generálják A_{15}-öt, emiatt $A_{15} \leq G_{15}$. Ugyanakkor bármely G_{15}-beli elem páros kell, hogy legyen, mivel a lyuk útját fel tudjuk írni jobbra, balra, felfelé és lefelé történő tologatások (tulajdonképpen transzpozíciók) szorzataként, és ahhoz, hogy a lyuk visszajuthasson a kezdeti helyére, szükséges feltétel, hogy a jobbra és a balra, illetve a felfelé és lefelé történő tologatások száma megegyezzen, tehát páros sok transzpozíciót találunk minden G_{15}-beli elem felírásában, így nem lehet páratlan köztük. Emiatt $G_{15} \cong A_{15}$.

A következő két tétel bizonyításában használni fogom a következő állítást:

1.4.4. Állítás. Ha a c_1 és $c_2 \in S_n$ ciklusok tranzitívan hatnak az $\{1, 2, \ldots, n\}$ halmazon, és $|c_1 \cap c_2| = 1$, akkor $A_n \leq \langle c_1, c_2 \rangle$.

Bizonyítás. Tegyük fel, hogy $|c_1| = k$, $|c_2| = l$. A 1.4.1-es lemma alapján $k + l - 1 = n$. Az általánosság megszorítása nélkül feltehetjük, hogy $c_1 = (1, 2, \ldots, k)$ és $c_2 = (k, k+1, \ldots, n)$. Ekkor

$$\begin{aligned} c_2^{-i} c_1 c_2^i &= ((1)c_2^i, (2)c_2^i, \ldots, (k)c_2^i) = (1, 2, \ldots, k-1, k+i) \\ c_2^{-i} c_1 c_2^i c_1^{-1} &= (k, k-1, k+i) =: x_i \\ c_1^{-j} x_i c_1^j &= (j, j-1, k+i), \end{aligned}$$

ahol $1 \leq i \leq l-1$ és $1 \leq j \leq k-1$. Ezek alapján fel tudunk írni minden $\{1, 2, \ldots, n\}$-beli számhoz olyan hármasciklust, amely tartalmazza, és ezen hármasciklusok gráfja összefüggő lesz. Ekkor 1.4.3 alapján az állítást kapjuk.

q. e. d.

Az is világos, hogy ha k vagy l páros (azaz c_1 vagy c_2 páratlan), akkor a generált csoport S_n lesz.

Még a tétel kimondása előtt definiálok egy kissé szokatlan fogalmat (legalábbis csoportelméletben), ami a lineáris algebra bázisához hasonlít. Ha a $C = \{c_1, c_2, \ldots, c_k\}$ halmaz elemei ciklusok, $\langle C \rangle = G$, és minden $X \subset C$ esetén $\langle X \rangle \cap (C \backslash X) = \emptyset$, akkor C *minimális generátorhalmaza* G-nek. Ez a definíció nem állítja, hogy nincs ennél kisebb elemszámú generátorhalmaz, csak azt, hogy ha C bármelyik elemét elhagynánk, akkor nem kapnánk meg G-t. Világos, hogy bármely generátorrhalmazból készíthetünk minimális generátorhalmazt, akár többfélét is! Ami nekünk fontos lesz, hogy hány eleme van ezeknek, mivel az elemszámuk meg kell egyezzen. Adott $\{c_1, c_2, \ldots, c_k\}$ generátorhalmaz esetén k' jelölje a minimális generátorhalmaz elemszámát.

1.4.5. Tétel. Ha az adott $N = \{n_1, n_2, \ldots, n_k\} \subset S_n$ halmaz minden eleme négyesciklus, az N által generált csoport tranzitívan hat az $\{1, 2, \ldots, n\}$ halmazon, és $n \geq 7$, akkor $\langle N \rangle = S_n$, kivéve ha $\langle n_1^2, \ldots, n_k^2 \rangle \cong C_2^{k'}$.

Bizonyítás. A bizonyítás során használni fogom több ízben is a következő állítást:

1.4.6. Állítás. A $c_1, c_2, \ldots, c_k \in S_n$ négyesciklusok tranzitívan hatnak az $\{1, 2, \ldots, n\}$ halmazon. Ha létezik $h \in \langle c_1, \ldots, c_k \rangle$, amelyre $|h| = 3$, akkor $\langle c_1, \ldots, c_k \rangle = S_n$.

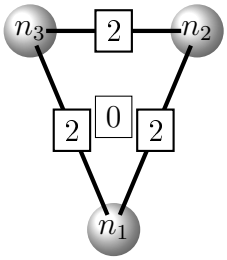
Bizonyítás. Vizsgáljuk meg a $k = 1$ esetet! Ha $|h \cap c_1| = 1$, akkor 1.4.4 miatt kész vagyunk. Ha $|h \cap c_1| = 2$, akkor $|h \cup c_1| = 5$, azaz h és $c_1 \in S_5$. A $G = \langle h, c_1 \rangle$ csoport elemszáma biztos osztható 3-mal, illetve 4-gyel, mivel van ilyen rendű eleme, és tudjuk még, hogy G tranzitívan hat $\{1, 2, \ldots, 5\}$-ön, így 1.2.7 miatt 5 is osztója $|G|$-nek. Ezek szerint 60 osztója $|G|$-nek, így $A_5 \leq G$, mivel ez az egyetlen 2 indexű részcsoportja S_5-nek. Ugyanakkor $c_1 \notin A_5$, tehát $G = S_5$. Ha $|h \cap c_1| = 3$, akkor $h, c_1 \in S_4$, és 12 osztója a $\langle h, c_1 \rangle$ csoportnak, így $A_4 \leq \langle h, c_1 \rangle$, ugyanakkor $c_1 \notin A_4$, tehát $\langle h, c_1 \rangle = S_4$.

Mostantól legyen $k > 1$ és $X \subseteq \{1, 2, \ldots, n\}$ maximális olyan értelemben, hogy $S_X \leq S_n$, és S_X a szokásos módon hat X-en, $\{1, 2, \ldots, n\} \backslash X$-en pedig identikusan. Be szeretnénk látni, hogy $|X| = n$. Tegyük fel, hogy $|X| < n$, ekkor léteznie kell c_i-nek, amelyre $0 < |X \cap c_i| < 4$, és olyan $h \in \langle c_1, \ldots, c_k \rangle$ hármasciklusnak is, amelyre $|c_i \cap h| \neq 0$. Ekkor viszont $\langle c_i, h \rangle = S_{|c_i \cup h|}$, és ebből következik, hogy $S_{|X \cup c_i|} \leq \langle c_1, c_2, \ldots, c_k \rangle$. De ez ellentmond X maximalitásának.

q. e. d.

Hogy minél egyszerűbbé tegyem a bizonyítás következő részét, bevezetek egy plusz jelölésrendszert. A $G(N)$ gráf minden élére írjuk rá azt a számot, ahány közös eleme van a két ciklusnak, amelyeket összeköt, illetve ha három ciklus egy három hosszú kör csúcsai, akkor a körbe írjuk be azon elemek számát, amelyek mindhárom ciklusban szerepelnek. Ha például $n_1 = (1, 2, 3, 4)$, $n_2 = (3, 4, 5, 6)$ és $n_3 = (1, 2, 5, 6)$, akkor a következő gráfot kapjuk:[3]

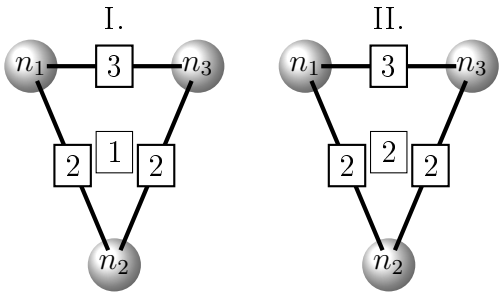
[3] A különböző eseteket reprezentáló gráfok ábráit külön-külön mellékelni fogom a későbbiekben, de hogy a gráfok és a ciklusok felírása könnyen összevethető legyen, külön lapokon mellékelem a szakdolgozathoz, a következő tétel kapcsán is így járok el.

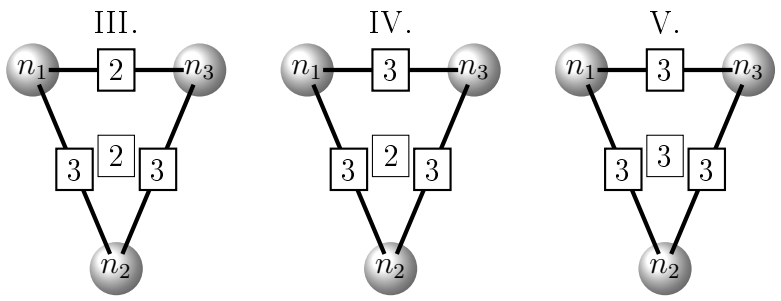


Ha három csúcsra illeszkedik egy kör, akkor a következő módon kapjuk, hogy hány elemet permutálnak a csúcsoknak megfelelő ciklusok: 12-ből kivonjuk az élekre írt számok összegét és hozzáadjuk a körbe írt számot (szita-formula). Ezenkívül a generálás szempontjából fontos, hogy a $G(N)$ gráfot kiegészíthetjük új csúcsokkal és élekkel: például a generátorelemek által generált ciklusokat bevehetjük a generátorelemek közé, a generált részcsoport értelemszerűen ugyanaz lesz (a generátorelemek közé bármely általuk generált permutációt is bevehetünk, azért írtam ciklust, mivel a $G(N)$ gráfot ciklusokra definiáltam, és ilyen lépésekkel fogok operálni a bizonyításokban).

A bizonyítás első lépéseként belátom, hogy ha két négyesciklusnak egy közös eleme van, akkor $\langle n_1, \ldots, n_k \rangle = S_n$. Ez adódik az 1.4.4-es és az 1.4.6-os állításokból.

Ezek után tegyük fel, hogy $G(N)$-ben nincs olyan él, amelyre 1-est vagy 4-est írtunk. (Ha egy élre 4-es kerül, az nem változtat az elemek számán, így a következő részgráfok egyikét biztosan megtalálhatjuk $G(N)$-ben.) Ez azt jelenti, hogy legalább három csúcsa van. Most tekintsük azokat az eseteket, amikor van olyan él, amelyre 3-as kerül. A következő gráfokat kapjuk:





Ezenkívül bevezetek egy új jelölést is: $(\overline{abcd})$ jelöljön egy tetszőleges négyesciklust, amelynek elemei a, b, c és d, de nem tudjuk, milyen sorrendben követik egymást. Hasznos lesz még egy másik jelölés is: ha c_1, c_2 ciklusok, akkor c_1Qc_2 jelölje azt a halmazt, amelynek elemei c_2-nek c_1 különböző hatványaival vett konjugáltjai, azaz

$$c_1Qc_2 = \{c_1^{-i}c_2c_1^i \mid 0 \leq i \leq o(c_1) - 1\}.$$

Először tekintsük azt az esetet, amikor minden élre 3-ast írunk. Ekkor $n_1 = (\overline{abcd})$, $n_2 = (\overline{abce})$, $n_3 = (\overline{abcf})$. Mivel ezekben a ciklusokban csak 6 elem szerepel, még lennie kell egy negyedik ciklusnak is, amely kapcsolódik hozzájuk, $n_4 = (\overline{abcg})$. (Azt könnyű belátni, hogy ha nem az V. gráfból indulunk ki, hanem a IV.-ből, akkor is szükség van egy negyedik ciklusra, és ennek valamelyik korábbi ciklussal háromnál kevesebb közös eleme lesz – emiatt a IV. gráfot vissza lehet vezetni az I., II. és III. gráfokra, vagy lesz benne 1-es él –, illetve ha n_4 nem ilyen alakú, akkor is lesz olyan él, amelyre 3-nál kisebb szám kerül.) Nézzük meg, mi történik, ha adott két négyesciklus, amelyeknek 3 közös elemük van, és konjugáljuk az egyiket a másik hatványaival! A két ciklus legyen (1234) és (1235).

$$\begin{aligned}(1432)(1235)(1234) &= (2345)\\ (1234)(1235)(1432) &= (1254)\\ (13)(24)(1235)(13)(24) &= (1534)\end{aligned}$$

Két dolgot fontos megjegyezni: a közös elemek közül pontosan kettő szerepel, és az nem szerepel, amelybe a konjugáló ciklusban a nem közös elem megy.

Ennél általánosabb tulajdonság, hogy ha egy permutációt konjugálunk egy másikkal, akkor azon elemek, amelyekbe nem közös elem megy a konjugáló tagban, nem fognak szerepelni a konjugálás eredményében. Mivel egy ciklus tranzitívan hat az elemein, ha konjugáljuk n_2-t n_1 hatványaival, a következő ciklusokhoz jutunk: $(\overline{abed})$, $(\overline{aced})$, $(\overline{bced})$. Illetve tudjuk, hogy n_3-nak van olyan hatványa, amelyben $c \to f$, emiatt $(\overline{abcf})Q(\overline{abcg}) \ni (\overline{abgf})$, és ennek egy közös eleme van $(\overline{aced})$-vel, így az 1.4.4 állítás alapján kész vagyunk.

Most tekintsük azokat az eseteket, amikor van olyan él, amelyen 3-as áll, és olyan is, amelyen 2-es. A II. gráfban $n_1 = (\overline{abcd})$, $n_2 = (\overline{abfg})$, $n_3 = (\overline{abce})$. Ekkor $n_1Qn_3 \ni (\overline{acde})$, és ennek egy közös eleme van n_2-vel.

A III. gráfban $n_1 = (\overline{abcd})$, $n_2 = (\overline{abce})$, $n_3 = (\overline{abef})$. Mivel csak 6 elem szerepel, kell lennie még egy ciklusnak, amelyben legalább egy új elem szerepel. Ha három új elem szerepel benne, akkor találtunk egy 1-es élt. Ha kettő, akkor $n_4 = (\overline{abgh})$, különben megint lenne 1-es él. Ekkor $n_1Qn_2 \ni (\overline{acde})$, és ennek megint egy közös eleme van n_4-gyel. Végül ha egy új elem szerepel n_4-ben, akkor lehet $(\overline{abcg})$, $(\overline{abdg})$, $(\overline{bceg})$, $(\overline{bcfg})$ és $(\overline{bdeg})$ (ezeket úgy kaptam, hogy vettem n_1 és n_4 lehetséges közös elemeit (kettő vagy három lehet) úgy, hogy n_4-nek n_2-vel és n_3-mal is legalább két közös eleme legyen, és kihasználtam a és b, illetve a generátorelemek szimmetriáját (n_1 és n_3 felcserélhetőek)). Ha $n_4 = (\overline{abcg})$, akkor $n_1Qn_4 \ni (\overline{acdg})$, amelynek egy közös eleme van n_3-mal. A többi esetben is tudunk generálni 1-es élt, mivel majdnem mindegyikhez találunk olyan i-t, hogy $n_iQn_4 \ni (\overline{abcg})$ (csak gyorsan felsorolom: $(\overline{abdg})$ – n_1, $(\overline{bceg})$ – n_2). Végül ha $n_4 = (\overline{bcfg})$, akkor $n_1Qn_2 \ni (\overline{abed})$-nek egy közös eleme van n_4-gyel, ha $n_4 = (\overline{bdeg})$, akkor hasonlóan $n_2Qn_3 \ni (\overline{abcf})$-nek van egy közös eleme n_4-gyel

Az I. gráfban $n_1 = (\overline{abcd})$, $n_2 = (\overline{adef})$, $n_3 = (\overline{abce})$. Ekkor $n_1Qn_3 \ni (\overline{abde}) = n_4$, és n_1, n_2 és n_4 a III. gráfot valósítja meg, erről pedig már beláttam, hogy generál 1-es élt.

Így beláttam, hogy ha a generátorelemek között van két olyan négyesciklus, amelyeknek 1 vagy 3 közös eleme van, akkor generálják S_n-t. Már csak az az eset van hátra, amikor bármely két generátorelemnek 2 (esetleg 0) közös eleme van. Nézzük meg, mi történik, ha adott két négyesciklus, amelyeknek 2 közös elemük van, és konjugáljuk az egyiket a másik hatványaival! Most annyival bonyolultabb a helyzet, ahhoz képest, amikor 3 közös elemük volt, hogy a közös elemek lehetnek szomszédosak és nem szomszédosak is. Emiatt előfordulhat, hogy mindkét közös elem nem közös elembe megy, és így nem lesz eleme a konjugálás eredményének. Ha a közös elemek mindkét ciklusban szomszédosak, akkor legyenek (1234) és (1256) (az, hogy a sorrendjük

megegyezik-e, nem lényeges, az inverzben megfordul).

$$\begin{aligned}(1432)(1256)(1234) &= (2356)\\ (1234)(1256)(1432) &= (1564)\\ (13)(24)(1256)(13)(24) &= (3456)\end{aligned} \tag{1.1}$$

Látszik, hogy a közös elemek közül bármelyiket, vagy akár mindkettőt eltüntethetjük, illetve tudunk generálni olyan elemet, amelynek három közös eleme van valamelyik korábbival. Ha a közös elemek az egyik ciklusban szomszédosak, a másikban pedig nem, akkor legyenek (1234) és (1526). Ekkor:

$$\begin{aligned}(1432)(1526)(1234) &= (2536)\\ (1234)(1526)(1432) &= (1645)\\ (13)(24)(1526)(13)(24) &= (3546),\end{aligned} \tag{1.2}$$

illetve

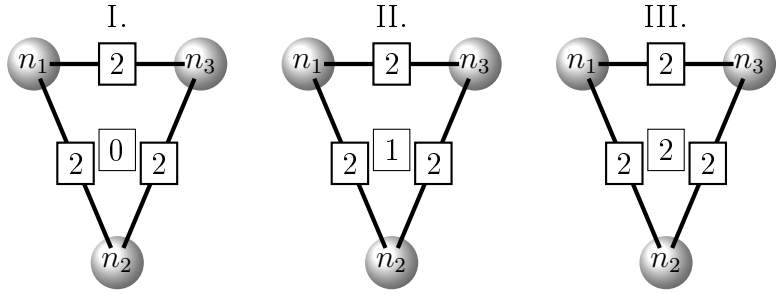
$$\begin{aligned}(1625)(1234)(1526) &= (3456)\\ (1526)(1234)(1625) &= (3465)\\ (12)(56)(1234)(12)(56) &= (1342).\end{aligned} \tag{1.3}$$

Hasonlót tapasztalunk, mint az előbb. Ha a közös elemek egyik ciklusban sem szomszédosak, akkor legyenek (1324) és (1526).

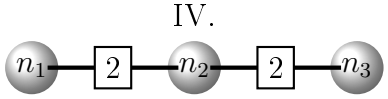
$$\begin{aligned}(1625)(1324)(1526) &= (3645)\\ (1526)(1324)(1625) &= (3546)\\ (12)(56)(1324)(12)(56) &= (1423).\end{aligned}$$

Itt a bökkenő! Ha ilyen elemeket konjugálunk egymással, a közös elemek eltűnnek, a nem közös elemek (amelyek szintén nem szomszédos helyzetben vannak egymással) ugyanakkor nem szomszédos helyzetbe mennek. Ha ilyen tulajdonságú négyesciklusokból szeretnénk olyan négyesciklust generálni, amelyben nem szomszédos elemek szomszédos elemekbe mennek (vagy fordítva), nem fogunk sikerrel járni. Vegyük észre, ez az eset csak akkor fordulhat elő, ha $n = 2m$ valamely m természetes számra. Feltehető, hogy minden n_i $(a, b, a+1, b+1)$ alakú, ahol a és b páratlan számok. Ekkor $\langle n_1, \ldots, n_k\rangle$ imprimitíven hat $\{1, 2, \ldots, n\}$-en, ugyanis $\Delta_1 = \{1, 2\}$, $\Delta_2 = \{3, 4\}$, …, $\Delta_m = \{n-1, n\}$ egy olyan partíció, amelynek elemeit az $n_1, \ldots, n_k$ generátorok mindegyike permutálja. Így $x \sim y \iff \exists i : x, y \in \Delta_i$ nemtriviális kongruenciája $\{1, 2, \ldots, n = 2m\}$-nek $\langle n_1, \ldots, n_k\rangle$ szerint. Tetszőleges $a \neq b \in \{1, 2, \ldots, n\}$ páratlan számokra az $(a, b, a+1, b+1)$ ciklus a

Δ_1, Δ_2, …, Δ_m halmazok közül kettőt felcserél, a többit fixen hagyja. Így összesen $\binom{m}{2}$ ilyen négyesciklust lehet felírni, tehát ennél több négyesciklus biztosan generálja S_n-t. Ezek a négyesciklusok szerepelnek a tételben kivételként, mivel a négyzetükben a nem szomszédos elemek páronként egy-egy transzpozíciót alkotnak, és a szorzatuk szintén valahány diszjunkt transzpozícióból áll. Így az általuk generált csoportban minden elem rendje 2. Ha például az 1-es és a 2-es nem szomszédos elemek, mint fentebb, és olyan négyesciklusokat veszünk be a generátorok közé, amelyekben szintén nem szomszédosak, akkor a négyzeteikben az 1-es és a 2-es csak az (12) transzpozícióként jelenhet meg. Hasonló elmondható tetszőleges a, b elemekről is: ha valamelyik generátorelem négyzetében szerepel az (ab) transzpozíció, akkor bármely más generátorelem négyzetében is csak ilyen formában jelenhet meg a és b. Emiatt bármely két n_i^2 bármely két transzpozíciója vagy diszjunkt, vagy egyenlő. Így a csoportunk kommutatív, tehát izomorf C_2^m-mel, valamely m egész számra. Milyen gráfot alkothat három tetszőleges generátorelem, amelyekre $n_1 \sim_\cap n_2 \sim_\cap n_3$, ebben az esetben? Először tekintsük azokat, amelyekben van 3 hosszú kör! A lehetséges részgráfok:



Ha nincs kör:



Az, hogy a két közös elem nem szomszédos egymással, előfordulhat az I., a III. és a IV. gráfban is, a II.-ban viszont nem, mivel ott egy olyan elem van, amely mindhárom négyesciklusban szerepel, tehát a „párja” különbözik két generátorelemben. Ha nincs minden cikluselemnek egy párja, amelynek a helyzete minden négyesciklusban rögzített hozzá képest (mégpedig nem

szomszédos helyen), akkor mind a négy gráfot vissza tudjuk vezetni egy korábbi esetre, mivel tudunk 3-as élt generálni a korábbi (1.1), (1.2), illetve (1.3) egyenletek alapján. Nézzük meg, mi történik az egyes gráfokon belül, ha nem generálják S_n-t! Az I. gráfban bármely két generátorelem generálja a harmadikat, így ez az eset visszavezethető a többire. A III. és a IV. gráfnak megfelelő négyesciklusok 8 elemet permutálnak. Kérdés, hogy hány különböző diszjunkt transzpozícióra bomlik tetszőleges gráf csúcsainak négyzete, ha bármely három generátorelemre a III. vagy a IV. gráf illeszkedik. Ha van három generátorelem, amelyekre az I. gráf illeszkedik, az egyik csúcsát és a hozzá tartozó éleket töröljük ki – a gráf így is összefüggő marad, és ugyanazt generálja. Ha minden ilyen részgráfot megszüntetünk, azzal tulajdonképpen egy minimális generátorrendszert készítünk, tehát k' darab csúcs marad. Ezután tekintsük $\langle n_1^2, n_2^2, \dots n_{k'}^2 \rangle$ csoport gráfjának egy feszítőfáját. k' darab generátorelem esetén $k'-1$ él vezet köztük, ami azt jelenti, hogy összesen $2+(k'-1) = k'+1$ diszjunkt transzpozíciót kapunk, mivel minden él egy új transzpozíciót jelent. Ezek segítségével $2^{k'+1}$ db permutáció készíthető. Ugyanakkor minden n_i^2 két transzpozíciót tartalmaz, emiatt a szorzatuk is páros sokat fog (ha van közös transzpozíciójuk, akkor az eltűnik, ha nincs, akkor páros sokkal nő), tehát ezekből $2^{k'}$ darab permutációt variálhatunk ki. Így $\langle n_1^2, n_2^2, \dots, n_k^2 \rangle \cong C_2^{k'}$.

q. e. d.

1.4.7. Tétel. Ha az adott $O = \{o_1, o_2, \dots, o_k\} \subset S_n$ halmaz minden eleme ötösciklus, és az O által generált csoport tranzitívan hat az $\{1, 2, \dots, n\}$ halmazon, és $n \geq 7$, akkor $\langle O \rangle = A_n$.

A tétel bizonyításában fel fogok használni két másik tételt, először ezek következnek:

1.4.8. Tétel. Az előző tételben szereplő $\langle O \rangle$ csoport primitív.

Bizonyítás. Tudjuk, hogy $\langle O \rangle$ hat az $\{1, 2, \dots, n\}$ halmazon. Ha $\sim$ egy kongruenciája $\{1, 2, \dots, n\}$-nek G szerint, és $\sim$-szerinti kongruencia-osztályai $\Delta_1, \Delta_2, \dots, \Delta_l$ ($\Delta_1 \cup \dots \cup \Delta_l = \{1, 2, \dots, n\}$), akkor $\langle O \rangle$ elemei permutálják a $\{\Delta_1, \dots, \Delta_l\}$ halmaz elemeit. Ha $l = 1$, akkor $\sim$ triviális kongruencia. Ha $l > 1$, akkor a tranzitivitás miatt van olyan $o_i \in O$, amely nem hagyja fixen az összes Δ_i-t. Ezenkívül o_i hatása a $\{\Delta_1, \dots, \Delta_l\}$ halmazon szintén ötösciklus. Mivel összesen öt elemet mozgat, ezért ha nem hagyja fixen Δ_i-t,

akkor egy elemet mozgat ki belőle, és ebből a kongruencia definíciója alapján következik, hogy $|\Delta_i| = 1$ minden i-re. Ez megintcsak triviális kongruencia, tehát $\langle O \rangle$ valóban primitív.

q. e. d.

Ezt a tételt általánosíthatjuk, mivel bármely p prímszámra átvihető az érvelés, sőt, ha a ciklusok hossza mind különböző prím, akkor is működik.

1.4.9. Tétel. Ha a G primitív permutációcsoport tartalmaz hármasciklust, akkor $A_n \leq G$.

Bizonyítás. Először defniálok egy ekvivalencia-relációt $\{1, 2, \ldots, n\}$-en:

$$x \sim y \iff x = y \text{ vagy van olyan } z \notin \{x, y\}, \text{ hogy } (xyz) \in G$$

Hogy $\sim$ reflexív, az könnyen látszik. A szimmetrikus tulajdonság az egyenlőség esetében triviális, a másik esetben az inverzzel látszik. Végül ha $x \sim y$ és $y \sim z$, akkor léteznek (xya) és $(yzb) \in G$ hármasciklusok. Ha $z = a$ vagy $x = b$, akkor $(xyz) \in G$, tehát $x \sim z$. Ha egyik sem teljesül, akkor $(ybz)(xya)(yzb) = (xza) \in G$, így megintcsak $x \sim z$, tehát $\sim$ tranzitív.

Valójában ennél több is mondható: $\sim$ kongruenciája G-nek. Ha $x \sim y$ és g tetszőleges G-beli elem, akkor $g^{-1}(xyz)g = ((x)g, (y)g, (z)g)$, tehát $(x)g \sim (y)g$. Mivel G tartalmaz hármasciklust, $\sim$ nemcsak az egyenlőség, és mivel G primitív, $x \sim y$-nak teljesülnie kell minden $x, y \in \{1, 2, \ldots, n\}$ esetén. Ezek szerint a G-beli hármasciklusok tranzitív részcsoportot generálnak, és 1.4.3 alapján $A_n \leq G$.

q. e. d.

Az utóbbi két tétel alapján 1.4.7 igazolásához elég azt belátnunk, hogy $\langle O \rangle$ generál hármasciklust. Most rátérek 1.4.7 bizonyítására.

Bizonyítás. Három esetet elég gyorsan el lehet intézni: ha van két generátorelem, amelyekenek 1, 2 vagy 3 közös elemük van, akkor $\langle O \rangle = A_n$. Ha van két ötösciklus, amelyeknek 1 közös elemük van, akkor 1.4.4 alapján generálják A_n-t. Ha két közös elemük van, akkor hatványozással elérhető, hogy a közös elemek szomszédosak legyenek mindkét permutációban, így feltehetjük, hogy $o_1 = (12345)$, $o_2 = (45678)$. Megmutatom, hogy o_1 és o_2 generál

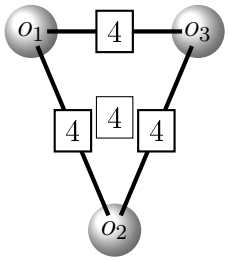
hármasciklust.

$$\begin{aligned}(12345)(45678)(15432) &= (34678)\\ (14253)(45678)(13524) &= (12678)\\ (12678)(38764) &= (12438)\\ (61728)(34678)(82716) &= (12348)\\ (12438)(13824)(12438) &= (134)\end{aligned} \tag{1.4}$$

(1.4) első két egyenletében generáltam két olyan hármasciklust, amelyekben a közös elemek szomszédosak, és ugyanabban a sorrendben követik egymást, és onnantól minden mást ezekből generáltam, tehát ezt az esetet is kipipálhatjuk. Világos, hogy a három közös elemet hatványozással mindig egymás mellé tudjuk vinni, viszont a sorrendjük nem feltétlenül fog megegyezni. Azt kell észrevenni, hogy az számít igazából, hogy a három közös elem közül melyik áll „középen", mivel ha ugyanaz, akkor a közös elemek sorrendje megegyezik, vagy ellentétes, de ekkor az inverzben egyezik meg. Azt az esetet kell csak megnézni tehát, amelyben más elem szerepel a három közös elem közül „középen". Feltehetjük, hogy $o_1 = (12345)$ és $o_2 = (13267)$.

$$\begin{aligned}(12345)(13267) &= (167)(345)\\ (13267)(12345) &= (145)(267)\\ (167)(345)(145)(267) &= (174)(26)(35)\end{aligned}$$

Az utolsó egyenlet eredményének négyzete pedig (147). Beláttam tehát, hogy ha van két olyan ötösciklus, amelyeknek 1, 2 vagy 3 közös elemük van, akkor $\langle O \rangle = A_n$. Hátra van még az az eset, amikor minden generátorelemnek 4 közös eleme van (most sem foglalkozom azokkal az esetekkel, amikor 5 közös eleme van két ötösciklusnak, mivel ez nem növeli az elemek számát, tehát a generátorelemek gráfjában valamelyik másik eset gráfjának is meg kell jelennie). A következő gráfot kapjuk:



Ez csak úgy fordulhat elő, ha minden ötösciklusban ugyanaz a négy közös elem, tehát mindegyikben van egy olyan elem, amely csak benne szerepel. E szerint $o_1 = (\overline{abcde})$, $o_2 = (\overline{abcdf})$, $o_3 = (\overline{abcdg})$. Ekkor o_1-nek van olyan hatványa, amelyben $d \to e$, emiatt $o_4 := (\overline{abcef}) \in o_1 Q o_2$, és ekkor o_4-nek és o_3-nak 3 közös eleme van.

q. e. d.

Az előző négy tétel alapján megfogalmazok egy sejtést:

1.4.10. Sejtés. Legyenek $g_1, g_2, \ldots, g_k \in S_n$ $l > 4$ hosszúságú ciklusok, $n \geq 2l - 1$, és $\langle g_1, \ldots, g_k \rangle$ hasson tranzitívan az $\{1, 2, \ldots, n\}$ halmazon. Ha l prímszám, akkor $\langle g_1, \ldots, g_k \rangle = A_n$. Ha $l = 2p$, ahol $p > 2$ prím, akkor $\langle g_1, \ldots, g_k \rangle = S_n$, kivéve ha $\langle g_1^2, \ldots, g_k^2 \rangle \cong C_p^{k'}$ vagy $\langle g_1^p, \ldots, g_k^p \rangle \cong C_2^{k'}$, és ha $l = p^2$, akkor $\langle g_1, \ldots, g_k \rangle = A_n$, kivéve ha $\langle g_1^p, \ldots, g_k^p \rangle \cong C_p^{k'}$.

Olyan összetett számokra, amelyek egy prím magasabb hatványai, biztos bonyolultabb a dolog, a GAP segítségével megnéztem néhány nyolcasciklus által generált csoport rendjét, és különböző fokozatokat találtam, attól, hogy egy elemet „elrontottam" az egyik generátorban, nem jött ki az egész S_n. Hasonlóképpen kérdés, hogy ha l-nek legalább két prímosztója van, és a prímfelbontásában a prímek kitevőinek összege nagyobb, mint 2, akkor milyen plusz feltételekre lehet szükség (tizenkét és tizenöt hosszú ciklusok esetén is hasonlót tapasztaltam, mint a nyolcasciklusoknál) – és persze a sejtés állítása sem magától értetődő, hatos-, kilences-, tizes- és tizennégyesciklusokra jónak tűnik.

Utólagos hozzáfűznivaló: az utóbbi két tétellel egyértelműen a Rubik-kocka vizsgálata miatt kezdtem el foglalkozni, egyébként nem lett volna indokolt. A sejtéssel kapcsolatban jutott eszembe, hogy tulajdonképpen arról van szó, hogy ha vesszük az $\mathrm{Aut}(S_n)$ csoportot, akkor ez hat az l hosszú ciklusok halmazán. Az a kérdés, hogy ha vesszük a generátorelemekhez tartozó $\mathrm{Aut}(S_n)$-beli (pontosabban $\mathrm{Inn}(S_n)$-beli) leképezéseket (tulajdonképp a konjugálásokat), akkor az ezek által generált részcsoport hatása tranzitív-e, vagy van olyan részhalmaza az l hosszú ciklusok halmazának, amelynek orbitja diszjunkt a többiek orbitjától. Ha ugyanis az összes l hosszú ciklus előáll, akkor biztosan tudunk hármasciklust generálni. Másrészt 1.4.5 bizonyítása alapján, ha $\{1, 2, \ldots, n\}$-nek van olyan partíciója, amelynek osztályait a generátorelemek permutálják, akkor a generált csoport imprimitív, tehát nem tartalmazhatja A_n-t. Sajnos, már nincs időm a kérdés vizsgálatára, de

jó támpont lehet a sejtés igazolásához, cáfolásához, módosításához vagy bővítéséhez is. Ettől függetlenül hasznosnak tartom az előző két relatíve elemi bizonyítást is.

2. fejezet

A Rubik-kocka

Ebben a fejezetben nagyrészt [2]-ben szereplő témákat vizsgálok, sokszor más megközelítéssel, más módszerrel, mint ami abban szerepel.

2.1. Jelölések

Elsőként bevezetek egy jelölésrendszert a 3×3-as Rubik-kocka lapkáira. A tárgyalás során végig úgy fogok a Rubik-kocka egyes lapjairól beszélni, hogy felteszem, végig ugyanabban a helyzetben tartom a Rubik-kockát, tehát magát a kockát nem forgatom, csak a lapjait. Így a szemben lévő lapot f-fel, a hátsót b-vel, a jobb oldalit r-rel, a bal oldalit l-lel, a felsőt u-val, az alsót pedig d-vel jelölöm. A lapkákat meg tudjuk számozni, a Rubik-kocka hálója így néz ki (ezt a jelölést [2]-ből vettem át (67. oldal)):

			1	2	3						
			4	u	5						
			6	7	8						
9	10	11	17	18	19	25	26	27	33	34	35
12	l	13	20	f	21	28	r	29	36	b	37
14	15	16	22	23	24	30	31	32	38	39	40
			41	42	43						
			44	d	45						
			46	47	48						

Minden lap kilenc lapkából áll, és kilenc alkocka tartozik hozzá. A sarokban elhelyezkedő alkockákat sarokkockáknak, ezek lapkáit csúcslapkáknak fogom

nevezni (minden sarokkockának három csúcslapkája van). Összesen 8 sarokkocka, így 24 csúcslapka van. Azokat az alkockákat, amelyeket két sarokkocka fog közre, élkockáknak, ezek lapkáit éllapkáknak fogom hívni (minden élkockának két éllapkája van). Összesen 12 élkocka, így 24 éllapka van. Azokat az alkockákat, amelyeknek csak egy lapkájuk van, középkockáknak, lapkájukat középlapkának nevezem. Az egyes lapkákat megadhatjuk azokkal a lapokkal, amelyekkel van közös lapkája az alkockának, amelyhez tartoznak. Az első karakter mindig azt a lapot adja meg, amelyen az adott lapka található.

- f lap: f, fru, fr, frd, fd, fld, fl, flu, fu
- b lap: b, blu, bl, bld, bd, brd, br, bru, bu
- r lap: r, rbu, rb rbd, rd, rfd, rf, rfu, ru
- l lap: l, lfu, lf, lfd, ld, lbd, lb, lbu, lu
- u lap: u, urb, ur, urf, uf, ulf, ul, ulb, ub
- d lap: d, drf, dr, drb, db, dlb, dl, dlf, df

Ezt a jelölésrenszert szintén [2]-ből vettem át – igaz, a középlapkákat ott nem betűzték meg külön –, ott [3]-ra hivatkoznak ennek kapcsán. Az alkockákat is megjelölhetjük hasonlóan, például az fru, ruf, urf lapkák sarokkockáját k_{FRU}-val fogom jelölni, az fr és rf lapkák élkockáját pedig k_{FR}-rel (világos, hogy itt a sorrend nem számít).

2.2. Elemi forgatások

A Rubik-kockán a lapkák elhelyezkedését a lapok hat elemi forgatásának sorozataival lehet megváltoztatni. Ezeket az elemi forgatásokat jelölje rendre F, B, R, L, U, D. Ahol pl. F az f lap 90°-os elforgatása az óramutató járásával megegyező irányba, vagy a lapkákkal leírva: ha X $\in$ {F, B, R, L, U, D} az x lapot forgatja, és x $\neq$ y $\neq$ z $\neq$ x $\in$ {f, b, r, l, u, d} akkor az X forgatás az xyz lapkát az xy'z lapkába viszi, ahol y'-t y-ból a következő egyszerű megfeleltetéssel kapjuk: f' = b, b' = f, r' = l, l' = r, u' = d, d' = u. Ha a számozott hálót tekintjük, az F, B, R, L, U, D elemi forgatásokat felírhatjuk

S_{48} elemeinek szorzataként:

$$\mathrm{F} = (17, 19, 24, 22)\,(18, 21, 23, 20)\,(6, 25, 43, 16)\,(7, 28, 42, 13)\,(8, 30, 41, 11)$$
$$\mathrm{B} = (33, 35, 40, 38)\,(34, 37, 39, 36)\,(1, 14, 48, 27)\,(2, 12, 47, 29),(3, 9, 46, 32)$$
$$\mathrm{R} = (25, 27, 32, 30)\,(26, 29, 31, 28)\,(3, 38, 43, 19)\,(5, 36, 45, 21)\,(8, 33, 48, 24)$$
$$\mathrm{L} = (9, 11, 16, 14)\,(10, 13, 15, 12)\,(1, 17, 41, 40)\,(4, 20, 44, 37)\,(6, 22, 46, 35)$$
$$\mathrm{U} = (1, 3, 8, 6)\,(2, 5, 7, 4)\,(17, 9, 33, 25)\,(18, 10, 34, 26)\,(19, 11, 35, 27)$$
$$\mathrm{D} = (41, 43, 48, 46)\,(42, 45, 47, 44)\,(22, 30, 38, 14)\,(23, 31, 39, 15)\,(24, 32, 40, 16)$$

A Rubik-kocka csoportját G-vel fogom jelölni. G elemeit generálják az elemi forgatások, tehát minden $g \in G$ felírható $X_1X_2 \dots X_n$ alakban, ahol minden $X_i \in \{\mathrm{F}, \mathrm{B}, \mathrm{R}, \mathrm{L}, \mathrm{U}, \mathrm{D}\}$, vagy másképp: $G = \langle \mathrm{F}, \mathrm{B}, \mathrm{R}, \mathrm{L}, \mathrm{U}, \mathrm{D} \rangle$. G valóban csoport, mert zárt a kompozícióra, létezik egységelem (amikor egyik lapot sem forgatjuk vagy pl. $\mathrm{F}^4 = \mathrm{id}$). A generátorelemek inverzeit jelölje F^{-1}, B^{-1}, R^{-1}, L^{-1}, U^{-1}, D^{-1}. (Ezeket is fel tudjuk írni a generátorelemek segítségével: $\mathrm{F}^3 = \mathrm{F}^{-1}$ stb.) Így tetszőleges elem inverze:

$$(X_1X_2 \dots X_n)^{-1} = X_n^{-1} \dots X_2^{-1}X_1^{-1}.$$

Végül az asszociativitás is teljesül, mivel minden $g \in G$ egy bijekció a Rubik-kocka lapkái között, és a függvények kompozíciója asszociatív. (Apropó függvények, a csoportelméleti fejezethez hasonlóan most is balról jobbra olvassuk a kompozíciót, tehát pl. az FR forgatás azt jelöli, hogy először F-et, majd R-et hajtjuk végre).

2.3. Példa elem rendjére

G rendjére még visszatérünk a későbbiekben, most vizsgáljuk meg néhány G-beli elem rendjét. Könnyen látszik, hogy a generátorelemek rendje 4, és az is, hogy például FB rendje is 4, mivel F és B diszjunkt lapkákat mozgatnak. Mennyi lesz FU rendje? Vegyük F és U S_{48}-beli ciklusfelbontását, és szorozzuk őket össze, majd alakítsuk át úgy, hogy előálljanak diszjunkt ciklusok szorzataként. A könnyebb átláthatóság kedvéért F ciklusfelbontásában az első elem legyen f_1, a második elem f_2 stb, hasonlóan U ciklusfelbontásában az első elem u_1 stb. (Tehát épp abban a sorrendben, ahogy fentebb

szerepel.)

$$\mathrm{FU} = f_1 f_2 f_3 f_4 f_5 u_1 u_2 u_3 u_4 u_5 =$$
$$= (f_2 u_4)(f_4 u_2)(f_1 f_3 f_5 u_1 u_3 u_5) =$$
$$= (f_2 u_4)(f_4 u_2)(f_3 f_5 u_1 f_1 u_3 u_5)$$

$$f_2 u_4 = (18,\ 21,\ 23,\ 20)(18,\ 10,\ 34,\ 26) = (18,\ 21,\ 23,\ 20,\ 10,\ 34,\ 26)$$

$$f_4 u_2 = (7,\ 28,\ 42,\ 13)(2,\ 5,\ 7,\ 4) = (7,\ 28,\ 42,\ 13,\ 4,\ 2,\ 5)$$

$$f_3 f_5 u_1 = (6,\ 25,\ 43,\ 16)(8,\ 30,\ 41,\ 11)(1,\ 3,\ 8,\ 6) =$$
$$= (6,\ 25,\ 43,\ 16)(8,\ 30,\ 41,\ 11,\ 6,\ 1,\ 3) = (6,\ 25,\ 43,\ 16,\ 1,\ 3,\ 8,\ 30,\ 41,\ 11)$$

$$f_1 u_3 u_5 = (17,\ 19,\ 24,\ 22)(17,\ 9,\ 33,\ 25)(19,\ 11,\ 35,\ 27) =$$
$$= (17,\ 19,\ 24,\ 22,\ 9,\ 33,\ 25)(19,\ 11,\ 35,\ 27) = (17,\ 11,\ 35,\ 27,\ 19,\ 24,\ 22,\ 9,\ 33,\ 25)$$

$$f_3 f_5 u_1 f_1 u_3 u_5 = (6,\ 25,\ 43,\ 16,\ 1,\ 3,\ 8,\ 30,\ 41,\ 11)$$
$$(17,\ 11,\ 35,\ 27,\ 19,\ 24,\ 22,\ 9,\ 33,\ 25) =$$
$$= (6,\ 17,\ 11)(25,\ 43,\ 16,\ 1,\ 3,\ 8,\ 30,\ 41,\ 35,\ 27,\ 19,\ 24,\ 22,\ 9,\ 33)$$

Tehát négy darab diszjunkt ciklussal fel lehet írni FU-t, ahol az egyes ciklusok rendjei: 7, 7, 3, 15. FU rendje ezek legkisebb közös többszöröse, azaz $7 \cdot 15 = 105$. Mivel F-et és U-t valahol önkényesen választottuk ki (bármely lap bármely helyzetbe hozható), ezért világos, hogy hasonlóan FD, LB^{-1}, illetve bármely két nem diszjunkt elemi forgatás szorzatának rendje is 105.

2.4. Hatás, tranzitivitás

Világos, hogy G hat a Rubik-kocka lapkáin és az alkockákon is, mivel az elemi forgatások lapkát lapkába, alkockát alkockába képeznek, tehát ugyanez igaz az elemi forgatások egymásutánjaira, azaz G elemeire is. Értelemszerűen G neutrális eleme minden lapkát helyben hagy.

Vizsgáljuk meg G, pontosabban FU hatását a Rubik-kocka alkockáin/lapkáin. Két egyszerű megállapítással kezdünk: a középkockák – így a középlapkák –

minden G-beli elem fixpontjai, és G bármely eleme élkockát élkockába, sarokkockát sarokkockába visz, tehát az éllapkák orbitja(i) diszjunkt(ak) a csúcslapkák orbitjá(i)tól. (Később belátjuk, hogy az éllapkák, illetve a csúcslapkák egy orbiton belül vannak.)

Ha megvizsgáljuk a fenti permutációkat, és összehasonlítjuk a Rubik-kocka hálójával, könnyen meghatározhatjuk az alkockák pályáit. Látszik, hogy van egy „kitüntetett" alkocka, az RFU sarokkocka, amelyet FU mindig önmagába visz, és 120°-ot forgat rajta (emiatt a lapkái egymás között permutálódnak). Ezen kívül a maradék öt sarokkocka egymás között permutálódik, és mivel ezek is forognak, ezek adják a 15 hosszú ciklus lapkáit. A hét élkocka egymás között permutálódik, sőt, a megfelelő lapkáik is egymástól függetlenül (azaz két diszjunkt hetescikluson belül változnak).

Tehát láttuk, hogy a nyolc sarokkocka közül ötöt át tudunk vinni egymásba FU-val, a maradék hármat is „csatlakoztathatjuk" például BU-val, így könnyen látszik, hogy a sarokkockák halmazán tranzitívan hat G. Mi a helyzet a csúcslapkákkal? Az FU elem vizsgálatánál leírtak alapján könnyen látszik, hogy tetszőleges k_{ABC} sarokkockát ($\mathrm{A} \neq \mathrm{B} \neq \mathrm{C} \neq \mathrm{A} \in \{\mathrm{F}, \mathrm{B}, \mathrm{R}, \mathrm{L}, \mathrm{U}, \mathrm{D}\}$) helyben hagy és a lapkáit egymás között forgatja például BC. Tehát bármely csúcslapkát el tudunk vinni bármely másik csúcslapkába például úgy, hogy először a megfelelő sarokkockát elvisszük a másik sarokkockába (ha ugyanazon sarokkocka lapkáiról van szó, akkor ezt természetesen kihagyjuk), majd az adott sarokkockát átforgatjuk a megfelelő pozícióba. Tehát a csúcslapkák egy orbiton belül helyezkednek el, azaz G tranzitívan hat a csúcslapkák halmazán.

A 12 élkocka közül 7-et egymásba tudtunk vinni már FU „segítségével". A maradék öt élkockát például BD-vel „csatlakoztathatjuk", tehát az élkockák halmazán is tranzitívan hat G. Ahhoz, hogy az éllapkákra is kiterjesszük a tranzitivitást, elég egy olyan $g \in G$ elemet találni, amely egy tetszőleges élkocka lapkáit felcseréli. A k_{AB} élkocka esetében ilyen g az AXB alakú elemek egyike, ahol $\mathrm{A}, \mathrm{B} \in \{\mathrm{R}, \mathrm{L}, \mathrm{U}, \mathrm{D}, \mathrm{F}, \mathrm{B}\}$ és $\mathrm{X} \in \{\mathrm{R}, \mathrm{L}, \mathrm{U}, \mathrm{D}, \mathrm{F}, \mathrm{B}\} \backslash \{\mathrm{A}, \mathrm{A}^*, \mathrm{B}, \mathrm{B}^*\}$ (itt a * művelet az átellenes lapokat felelteti meg egymásnak, pl. $\mathrm{R}^* = \mathrm{L}$). Tehát G az éllapkákon is tranzitívan hat.

2.5. Példa részcsoportra

A Rubik-kocka csoportjának rengeteg részcsoportja létezik, most nézzünk erre példát. Legyen $H = \langle \mathrm{U}^2, \mathrm{R}^2 \rangle$. Milyen elemei vannak H-nak? Mivel U^2

és R^2 generálja H-t, minden eleme felírható

$$h = \mathrm{X}_1\mathrm{X}_2 \dots \mathrm{X}_n$$

alakban, ahol minden $\mathrm{X}_i \in \{\mathrm{U}^2, \mathrm{R}^2\}$. Mivel mindkét generátorelem rendje 2, ezért adott h elem legrövidebb felírásában $\mathrm{X}_i \neq \mathrm{X}_{i+1}$ minden i-re (különben az adott „párral" egyszerűsíthetnénk). Ez alapján H minden elemét fel lehet írni a következő alakban:

$$h = (\mathrm{U}^2)^l(\mathrm{R}^2\mathrm{U}^2)^n(\mathrm{R}^2)^m, \tag{2.1}$$

ahol $l, m \in \{0, 1\}$. Vizsgáljuk meg, mennyi $\mathrm{R}^2\mathrm{U}^2$ (egyúttal az inverze, $\mathrm{U}^2\mathrm{R}^2$) rendje. Permutációk segítségével felírva (x_i most is X i-edik permutációját jelöli az adott sorrenden belül):

$$\mathrm{R}^2 = (25,27,32,30)^2\,(26,29,31,28)^2\,(3,38,43,19)^2\,(5,36,45,21)^2\,(8,33,48,24)^2$$
$$\mathrm{U}^2 = (1,3,8,6)^2\,(2,5,7,4)^2\,(17,9,33,25)^2\,(18,10,34,26)^2\,(19,11,35,27)^2$$
$$\mathrm{R}^2\,\mathrm{U}^2 = r_1^2\,r_2^2\,r_3^2\,r_4^2\,r_5^2\,u_1^2\,u_2^2\,u_3^2\,u_4^2\,u_5^2 = (r_2^2\,u_4^2)\,(r_4^2\,u_2^2)\,(r_1^2\,r_3^2\,u_5^2\,r_5^2\,u_1^2\,u_3^2)$$
$$r_2^2\,u_4^2 = (26,31)\,(29,28)\,(18,34)\,(10,26) = (29,28)\,(18,34)\,(26,31,10)$$
$$r_4^2\,u_2^2 = (5,45)\,(36,21)\,(2,7)\,(5,4) = (36,21)\,(2,7)\,(5,45,4)$$
$$r_1^2\,r_3^2\,u_5^2 = (25,32)\,(27,30)\,(3,43)\,(38,19)\,(19,35)\,(11,27) =$$
$$= (25,32)\,(27,30,11)\,(3,43)\,(19,38,35)$$
$$r_5^2\,u_1^2\,u_3^2 = (8,48)\,(33,24)\,(1,8)\,(3,6)\,(17,33)\,(9,25) =$$
$$= (8,48,1)\,(33,24,17)\,(3,6)\,(9,25)$$
$$r_1^2r_3^2u_5^2r_5^2u_1^2u_3^2 = (8,48,1)\,(33,24,17)\,(27,30,11)\;(38,19,35)\,(25,32,9)\,(3,43,6)$$

A felírt permutációk alapján látható, hogy $\mathrm{R}^2\mathrm{U}^2$ diszjunkt ciklusfelbontásában szereplő ciklusok rendje 2 vagy 3. Ez alapján $\mathrm{R}^2\mathrm{U}^2$ rendje 6.

Visszatérve a H részcsoport elemszámához: mivel $\mathrm{R}^2\mathrm{U}^2$-nek 6 különböző egész kitevős hatványa van, összességében 24-féle elemet tudunk felírni (2.1) alapján. Előfordulhat-e, hogy ugyanazt az elemet többféleképp írtuk fel? Mivel $\mathrm{U}^2\mathrm{U}^2 = \mathrm{id} = (\mathrm{R}^2\mathrm{U}^2)^6$, ezért $\mathrm{U}^2 = (\mathrm{R}^2\mathrm{U}^2)^5\mathrm{R}^2$. Tehát azon $h \in H$, amelyekre $l = 1$, tovább alakíthatóak:

$$h = \mathrm{U}^2(\mathrm{R}^2\mathrm{U}^2)^n(\mathrm{R}^2)^m = (\mathrm{R}^2\mathrm{U}^2)^5\mathrm{R}^2(\mathrm{R}^2\mathrm{U}^2)^n(\mathrm{R}^2)^m =$$
$$= (\mathrm{R}^2\mathrm{U}^2)^5(\mathrm{U}^2\mathrm{R}^2)^n(\mathrm{R}^2)^{m+1} = (\mathrm{R}^2\mathrm{U}^2)^{5-n}(\mathrm{R}^2)^{m+1},$$

ahol $(5-n)$-t mod 6, $(m+1)$-et mod 2 kapjuk.

Emiatt tetszőleges $h \in H$ elemet kétféleképp is fel tudunk írni (2.1) szerint, mivel az $l = 1$ és az $l = 0$ esetek megfeleltethetők egymásnak. Ebből következik, hogy $|H| \leq 12$. Tudjuk még, hogy H-nak 6-nál több eleme van, mivel nem ciklikus, tehát $|H| = 12$.

A H részcsoportot W. D. Joyner is vizsgálja [2]-ben (97. oldal), bár az eddig leírtakat nem viszi végig ilyen részletesen. A következő részt a könyv alapján, érdekességként említem meg.

Milyen 12-edrendű csoportokat ismer(het)ünk? Mivel C_n rendje n, ezért 12-edrendű csoport például C_{12}. S_n rendje $n!$, emiatt nincs 12-edrendű szimmetrikus csoport, viszont $|A_4| = 12$, mivel $|A_n| = \frac{n!}{2}$. Végül láttuk, hogy $|D_n| = 2n$, tehát D_6 rendje is 12.

H nem lehet izomorf C_{12}-vel, mivel H-nak legalább két másodrendű eleme van, C_{12}-nek pedig csak egy. A_4 sem jó, mert A_4-ben nincs hatodrendű elem.

D_6 forgatásait felírhatjuk, mint a 60°-os forgatás (f) hatványait, tükrözéseit pedig f hatványainak és egy tetszőleges t tükrözésnek a szorzataként. Így $D_6 = \{\mathrm{id} = f^6, f, f^2, \ldots, f^5, t, ft, f^2t, \ldots, f^5t\}$. Látszik, hogy az $\mathrm{R}^2\mathrm{U}^2 \leftrightarrow f, \mathrm{R}^2 \leftrightarrow t$ megfeleltetés H elemeit D_6 elemeibe képezi.

Két tetszőleges H-beli elem szorzata:

$$\begin{gathered}(\mathrm{R}^2\mathrm{U}^2)^{n_1}(\mathrm{R}^2)^{m_1}(\mathrm{R}^2\mathrm{U}^2)^{n_2}(\mathrm{R}^2)^{m_2} = \\ = (\mathrm{R}^2\mathrm{U}^2)^{n_1}(\mathrm{R}^2)^{m_1}\mathrm{R}^2(\mathrm{U}^2\mathrm{R}^2)^{n_2}(\mathrm{R}^2)^{m_2-1} = \\ = (\mathrm{R}^2\mathrm{U}^2)^{(n_1+(-1)^{m_1}\cdot n_2)}(\mathrm{R}^2)^{m_2-m_1}\end{gathered}$$

Két D_6-beli elem szorzata:

$$f^{n_1}t^{m_1}f^{n_2}t^{m_2} = f^{n_1}f^{(-1)^{m_1}\cdot n_2}t^{m_2-m_1} = f^{n_1+(-1)^{m_1}\cdot n_2}t^{m_2-m_1}$$

Ebben az egyenletben azt használtam fel, hogy $tf^nt = f^{-n}$. A művelettartás miatt $H \cong D_6$.

2.6. A kibővített csoport

Ezt az alfejezetet [2] 10. fejezete alapján írtam (185-195. oldal), bár ott más megközelítésben dolgozik a szerző.

Korábban láttuk, hogy G elemei hatnak a saroklapkák és az éllapkák halmazán is (ezeket V-vel, illetve E-vel jelölöm mostantól), ugyanakkor ez a két hatás nem feltétlen független egymástól (a későbbiekben belátom, hogy nem az). Mindazonáltal vizsgáljuk meg ezt a két hatást külön. Tekintsük V,

illetve E pontonkénti stabilizátorát G-n belül (tehát azon G-beli elemeket, amelyek identikusan hatnak V-n, illetve E-n), jelöljük őket N_V-vel, illetve N_E-vel. N_V és N_E normálosztók G-ben, mivel azon homomorfizmusok magjai, amelyek G hatását V-re, illetve E-re szűkítik. Vegyük a G/N_V és a G/N_E faktorcsoportokat, és G/N_V, illetve G/N_E hasson úgy V-n, illetve E-n, mint G.

Korábban beláttam, hogy G tranzitívan hat V-n, illetve E-n is, ez igaz tehát G/N_V-re, illetve G/N_E-re. G szerint (s így G/N_V szerint is) V-nek van nemtriviális kongruenciája, mivel egy tetszőleges, adott sarokkocka három lapkáját bármely G-beli elem három olyan lapkába viszi, amelyek szintén egy sarokkockához tartoznak. Hasonlóan E-nek is van nemtriviális kongruenciája G (s így G/N_E) szerint, ennek osztályai az adott élkockához tartozó lapkakettesek. Felsorolva V osztályai:

$$\begin{pmatrix} \text{fru} \\ \text{ruf} \\ \text{ufr} \end{pmatrix}; \begin{pmatrix} \text{flu} \\ \text{luf} \\ \text{ufl} \end{pmatrix}; \begin{pmatrix} \text{frd} \\ \text{rdf} \\ \text{dfr} \end{pmatrix}; \begin{pmatrix} \text{fld} \\ \text{ldf} \\ \text{dfl} \end{pmatrix};$$
$$\begin{pmatrix} \text{bru} \\ \text{rub} \\ \text{ubr} \end{pmatrix}; \begin{pmatrix} \text{blu} \\ \text{lub} \\ \text{ubl} \end{pmatrix}; \begin{pmatrix} \text{brd} \\ \text{rdb} \\ \text{dbr} \end{pmatrix}; \begin{pmatrix} \text{bld} \\ \text{ldb} \\ \text{dbl} \end{pmatrix}.$$

E osztályai:

$$\begin{pmatrix} \text{fr} \\ \text{rf} \end{pmatrix}; \begin{pmatrix} \text{fl} \\ \text{lf} \end{pmatrix}; \begin{pmatrix} \text{fd} \\ \text{df} \end{pmatrix}; \begin{pmatrix} \text{fu} \\ \text{uf} \end{pmatrix};$$
$$\begin{pmatrix} \text{br} \\ \text{rb} \end{pmatrix}; \begin{pmatrix} \text{bl} \\ \text{lb} \end{pmatrix}; \begin{pmatrix} \text{bd} \\ \text{db} \end{pmatrix}; \begin{pmatrix} \text{bu} \\ \text{ub} \end{pmatrix};$$
$$\begin{pmatrix} \text{lu} \\ \text{ul} \end{pmatrix}; \begin{pmatrix} \text{ld} \\ \text{dl} \end{pmatrix}; \begin{pmatrix} \text{ru} \\ \text{ur} \end{pmatrix}; \begin{pmatrix} \text{rd} \\ \text{dr} \end{pmatrix}.$$

Mivel G/N_V, illetve G/N_E tranzitívan és imprimitíven hat V-n, illetve E-n, 1.3.7 és a bizonyítása alapján léteznek H_1, H_2, K_1, K_2 csoportok, hogy $G/N_V \leq H_1$ wr $K_1 \leq S_3$ wr S_8 és $G/N_E \leq H_2$ wr $K_2 \leq S_2$ wr S_{12}. Fontos észrevenni, hogy egy adott alkocka lapkái nem permutálódhatnak egymás között akárhogy, mivel egymáshoz képest rögzített a helyzetük, nem fordulhat elő például, hogy az egyik lapka a helyén marad, a másik kettő pedig helyet cserél, ezért az alkockák lapkái $A_3 \cong C_3$ szerint változhatnak egymás között. A másik észrevétel csupán annyi, hogy $S_2 \cong C_2$. Ha ezeket figyelembe

vesszük, kapjuk, hogy $G/N_V \leq C_3$ wr S_8 és $G/N_E \leq C_2$ wr S_{12}. Innen kapjuk, hogy $G \leq G/N_V \times G/N_E \leq (C_3 \text{ wr } S_8) \times (C_2 \text{ wr } S_{12})$ (Teljesen pontosan G egy G/N_V-vel izomorf csoport és egy G/N_E-vel izomorf csoport direkt szorzatának részcsoportja). A „részcsoport-egyenlőtlenség" jobb oldalán álló csoportot a Rubik-kocka kibővített csoportjának fogom nevezni,

$$G_0 = (C_3 \text{ wr } S_8) \times (C_2 \text{ wr } S_{12}).$$

G_0-t úgy lehet szemléltetni, hogy ha szétszedjük a Rubik-kockát, és akárhogy össze lehet rakni, akkor minden egyes összerakáshoz találunk pontosan egy $g \in G_0$ elemet, amely azt valósítja meg. (Néhány megkötés azért van: a középkockákat fixen hagyjuk, így a különböző összerakások nem vihetők egymásba a kocka szimmetriáival, illetve sarokkocka helyére csak sarokkockát, élkocka helyére csak élkockát tehetünk, és minden alkocka minden lapkájának a nagy kocka felszínéhez kell tartoznia.)

Határozzuk meg G indexét G_0-on belül! G_0 és G elemeit fel tudjuk írni a következő alakban:

$$g = (o_V^{k_1}, \ldots, o_V^{k_8}, p_V, o_E^{l_1}, \ldots, o_E^{l_{12}}, p_E) = (\vec{o}_V, p_V, \vec{o}_E, p_E), \tag{2.2}$$

ahol $o_V = (123) \in S_3$, minden i-re $k_i \in \{0, 1, 2\}$, $p_V \in S_8$, $o_E = (12) \in S_2$, minden i-re $l_i \in \{0, 1\}$, $p_E \in S_{12}$. Meg kell vizsgálni, hogy milyen feltételek mellett lesz egy G_0-beli elem G-nek is eleme. A következő alfejezetekben megnézem, hogy a sarokkockák és az élkockák permutációi, a sarokkockák orientációi, illetve az élkockák orientációi milyen alakot vehetnek fel ebben az esetben.

2.6.1. A sarokkockák és az élkockák permutációi

Minden elemi forgatás 4 sarok- és 4 élkockát mozgat, tehát a hatásuk a sarokkockák halmazán és az élkockák halmazán is egy 4 hosszú ciklusnak, tehát páratlan permutációnak felel meg. Minden G-beli elem felírható ezek szorzataként, így kapjuk, hogy ha egy $g \in G$ elem hatása a sarokkockákon egy páratlan (páros) permutációnak felel meg, akkor g hatása az élkockákon szintén egy páratlan (páros) permutációnak felel meg. Tehát ha $g \in G$, akkor a (2.2)-ban szereplő p_V és p_E permutációk előjele megegyezik.

2.6.2. A sarokkockák orientációja

A sarokkockák orientációját úgy érdemes vizsgálni, hogy az egyes sarokkockák lapkáira képzeletben ráírjuk az 1, 2, 3 számokat, majd megnézzük, hogy az elemi forgatások hatására hogy permutálódnak a számok az egyes alkockákon. A sarokkockák számozása a következő legyen: $k_{\mathrm{FUL}} = 1$, $k_{\mathrm{FUR}} = 2$, $k_{\mathrm{FDR}} = 3$, $k_{\mathrm{FDL}} = 4$, illetve $k_{\mathrm{BUR}} = 5$, $k_{\mathrm{BUL}} = 6$, $k_{\mathrm{BDL}} = 7$, $k_{\mathrm{BDR}} = 8$. A következő felírást *referenciafelírásnak* nevezem, ehhez fogjuk viszonyítani az egyes elemek hatását (az egyértelműség kedvéért feltüntettem a sarokkockák számát is). Értelemszerűen most csak a sarokkockákat ábrázolom (ez tulajdonképpen a 2×2-es Rubik-kocka).

1.	1	2	2.
2	3	3	1
1	3	3	2
4.	2	1	3.

5.	1	2	6.
2	3	3	1
1	3	3	2
8.	2	1	7.

A sarokkockák számozásából látszik, hogy a bal oldali lapkaháló az f lap sarokkockáié, a jobb oldali pedig a b lap sarokkockáié, így megadtam az összes sarokkocka helyzetét, a többi lap hálóját ezek alapján könnyen el lehet készíteni.

Hogyan hat egy $g \in G$ elem az orientációra? Az elemi forgatások hatása könnyen megadható:

$$\begin{aligned}
\vec{o_V}(\mathrm{F}) &= \vec{o_V}(\mathrm{B}) = \mathrm{id} \in S_3^8 \\
\vec{o_V}(\mathrm{R}) &= (\mathrm{id}, (123), (132), \mathrm{id}, (132), \mathrm{id}, \mathrm{id}, (123)) \\
\vec{o_V}(\mathrm{L}) &= ((132), \mathrm{id}, \mathrm{id}, (123), \mathrm{id}, (123), (132), \mathrm{id}) \\
\vec{o_V}(\mathrm{U}) &= ((123), (132), \mathrm{id}, \mathrm{id}, (123), (132), \mathrm{id}, \mathrm{id}) \\
\vec{o_V}(\mathrm{D}) &= (\mathrm{id}, \mathrm{id}, (123), (132), \mathrm{id}, \mathrm{id}, (123), (132))
\end{aligned} \tag{2.3}$$

S_n^k azon elemeit, amelyeknek koordinátáinak szorzata az S_n-beli egységelem, *egységvektornak* fogom nevezni (bár a mi esetünkben ez nem lesz lényeges, a

koordináták sorrendjét a szorzás során $(1, 2, \ldots, k)$-nak veszem, hogy a definíciónak minden esetben legyen értelme). Egyből látszik, hogy az összes elemi forgatás orientációvektora egységvektor. Észre lehet venni, hogy az elemi forgatások orientációvektoraiban csak páros permutációk szerepelnek, ezekről tudjuk, hogy felcserélhetőek (legalábbis S_3-ban!).

Tudjuk, hogy minden $g \in G$ felírható az elemi forgatások szorzataként, úgyhogy érdemes meghatározni a szorzat orientációját, és akkor minden $g \in G$ elem orientációját ki lehet számítani. Ehhez egyrészt a megfelelő orientációvektorok megfelelő elemeinek szorzatát kell venni, másrészt meg kell vizsgálni, hogy az egyes sarokkockák hogy permutálódnak egymás között, mivel az orientációjuk is permutálódik. (Ez nem a legpontosabb megfogalmazás, de kockával a kézben érdemes átgondolni.) Jelöljük tetszőleges $g \in G_0$ (2.2) szerinti felírásában szereplő p_V-t $p_V(g)$-vel, az orientációt hasonlóan $\vec{o_V}(g)$-vel. Ekkor minden $g, h \in G_0$-ra teljesül, hogy:

$$\vec{o_V}(g \cdot h) = (\vec{o_V}(g) * p_V(h)) \cdot \vec{o_V}(h),$$

ahol $* \; p_V(h)$ hatását jelenti az orientációvektor koordinátáin. Ha minden $g \in G_0$ elem esetén vesszük az $(\vec{o_V}, p_V)$ rendezett párokat, akkor tulajdonképpen a C_3 wr S_8 csoportról van szó, a fenti képlet a C_3^8-beli elemet adja meg, a permutációkra pedig természetesen $p_V(g \cdot h) = p_V(g)p_V(h)$ teljesül. Ez alapján pedig tetszőleges $g = X_1 \ldots X_n \in G$-re (minden $X_i \in \{$F, B, R, L, U, D$\}$):

$$\vec{o_V}(X_1 \ldots X_n) = (\vec{o_V}(X_1 \ldots X_{n-1}) * p_V(X_n)) \cdot \vec{o_V}(X_n).$$

Észre lehet venni, hogy az egységvektorok részcsoportot alkotnak C_3^8-ban, ennek automorfizmusa minden S_8-beli permutáció (a koordinátákon), így C_3 wr S_8-ban részcsoport az egységvektorokból és tetszőleges S_8-beli permutációból képzett rendezett párok halmaza. Mivel az elemi forgatásokhoz tartozó $(\vec{o_V}, p_V)$ párok mind elemei ennek a csoportnak, az általuk generált csoport részcsoport, tehát minden G-beli elem orientációvektora egységvektor. Ezenkívül az egységvektorok alkotják a

$$\Psi : S_3^8 \to S_3, \; \Psi((s_1, s_2, \ldots, s_8)) = s_1 \cdot s_2 \cdot \ldots \cdot s_8$$

homomorfizmus magját, s így az egységvektorok csoportja normálosztó S_3^8-ban.

Még nem tértem ki arra, hogy a kibővített csoportban hogyan adjuk meg a sarokkockáknak tetszőleges g elemhez tartozó helyzetét (lényegében az orientációt, a permutáció elég egyértelmű a számozás függvényében). Első lépésként a Rubik-kocka kirakott helyzetében írjuk fel a referenciafelírást az egyes saroklapkákra, ezután szedjük szét a Rubik-kockát, permutáljuk a sarokkockákat egymás között p_V szerint, rakjuk össze a kockát úgy, hogy a kirakott helyzetnél felírt számozás most is a referenciafelírást valósítsa meg, majd minden kockát forgassunk meg a rá ható $o_V^{k_i}$ elem szerint. Ahhoz, hogy ezt megtehessük, szükséges és elégséges feltétel, hogy a felírás az összes sarokkockán az óramutató járása szerint ugyanabban az irányban történjen.

Mi történik, ha G_0 egy $g = (\vec{o_V}, p_V, \vec{o_E}, p_E)$ eleme megváltoztatja egy sarokkocka orientációját? Egy hármasciklus hat az adott alkockára írt számokon, az (123) vagy az (132). Tegyük fel, hogy $o_V = (123)$. Ahhoz, hogy $g \in G$ teljesülhessen (ami ekvivalens azzal, hogy a kockát az elemi forgatások segítségével eljuttathatjuk a g-nek megfelelő helyzetbe), szükséges, hogy $\vec{o_V}(g)$ egységvektor legyen, azaz $\sum_{i=1}^{8} k_i \equiv 0 \mod 3$.

Mindaz, amit az orientációkról levezettem, erősen támaszkodik a referenciafelírásra. Természetesen nem csak az általam megadott módon írhatjuk fel a számokat a lapkákra, de azt várjuk, hogy bármilyen megfelelő felírásnál ezt az eredményt kapjuk. Mit értek megfelelő felíráson? Az előző bekezdésben már volt szó erről, minden saroklapkán ugyanolyan körüljárás szerint kell szerepelnie az 1, 2, 3 számoknak. A referenciafelírás teljesíti ezt a feltételt. Minden más megfelelő felírást pedig megkaphatunk a referenciafelírásból, ha minden $i \in \{1, 2, \ldots, 8\}$ esetén hatunk az i-edik sarokkockán szereplő számokon az $f_i \in S_3$ permutációval. Az előbb kimondott feltétel az f_i-kre lefordítva azt jelenti, hogy minden $i, j \in \{1, \ldots, 8\}$ esetén $\mathrm{sg}(f_i) = \mathrm{sg}(f_j)$. Ekkor a következő referenciafelírást kapjuk:

1.	$f_1(1)$	$f_2(2)$	2.
$f_1(2)$	$f_1(3)$	$f_2(3)$	$f_2(1)$
$f_4(1)$	$f_4(3)$	$f_3(3)$	$f_3(2)$
4.	$f_4(2)$	$f_3(1)$	3.

5.	$f_5(1)$	$f_6(2)$	6.
$f_5(2)$	$f_5(3)$	$f_6(3)$	$f_6(1)$
$f_8(1)$	$f_8(3)$	$f_7(3)$	$f_7(2)$
8.	$f_8(2)$	$f_7(1)$	7.

Írjuk fel az elemi forgatások $\vec{o_V}$-ait, ha azok egységvektorok, minden más is stimmel.

$$\vec{o_V}(\mathrm{F}) = (f_1^{-1}f_4, f_2^{-1}f_1, f_3^{-1}f_2, f_4^{-1}f_3, \mathrm{id}, \mathrm{id}, \mathrm{id}, \mathrm{id})$$

$$\vec{o_V}(\mathrm{B}) = (\mathrm{id}, \mathrm{id}, \mathrm{id}, \mathrm{id}, f_5^{-1}f_8, f_6^{-1}f_5, f_7^{-1}f_6, f_8^{-1}f_7)$$

$$\vec{o_V}(\mathrm{R}) = \big(\mathrm{id}, f_2^{-1}(123)f_3, f_3^{-1}(132)f_8, \mathrm{id}, f_5^{-1}(132)f_2, \mathrm{id}, \mathrm{id}, f_8^{-1}(123)f_5\big)$$

$$\vec{o_V}(\mathrm{L}) = \big(f_1^{-1}(132)f_6, \mathrm{id}, \mathrm{id}, f_4^{-1}(123)f_1, \mathrm{id}, f_6^{-1}(123)f_7, f_7^{-1}(132)f_4, \mathrm{id}\big)$$

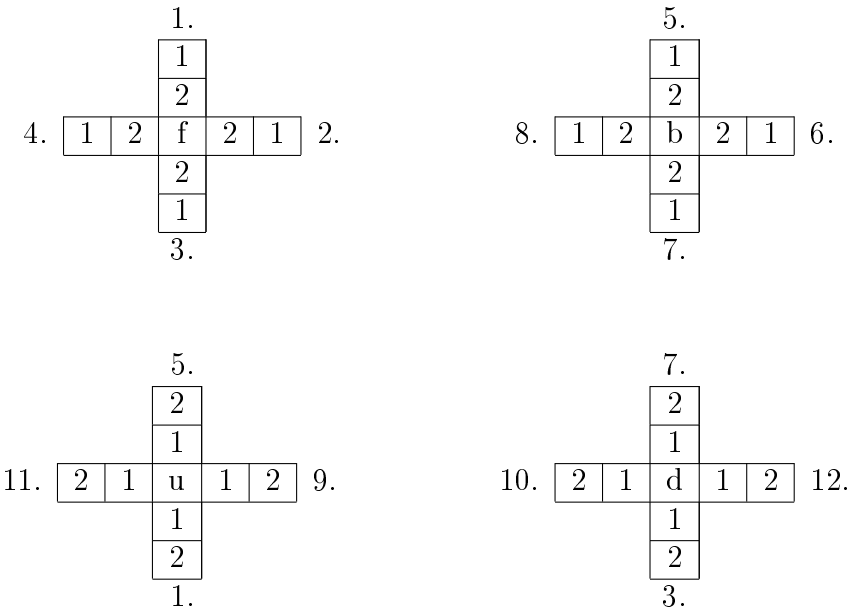
$$\vec{o_V}(\mathrm{U}) = \big(f_1^{-1}(132)f_2, f_2^{-1}(123)f_5, \mathrm{id}, \mathrm{id}, f_5^{-1}(132)f_6, f_6^{-1}(123)f_1, \mathrm{id}, \mathrm{id}\big)$$

$$\vec{o_V}(\mathrm{D}) = \big(\mathrm{id}, \mathrm{id}, f_3^{-1}(123)f_4, f_4^{-1}(132)f_7, \mathrm{id}, \mathrm{id}, f_7^{-1}(132)f_8, f_8^{-1}(123)f_3\big)$$

Mivel feltettük, hogy az összes f_i-nek azonos az előjele, ezért minden $i, j \in \{1, \ldots, 8\}$ esetén $f_i^{-1}(123)^k f_j$ $(k = 0, 1, 2)$ páros permutáció S_3-ban, így felcserélhetőek, s emiatt minden elemi forgatás orientációvektora egységvektor.

2.6.3. Az élkockák orientációja

Az élkockák orientációját a sarokkockákéhoz hasonlóan tudjuk vizsgálni. Minden élkocka lapkáira felírunk egy 1-est, illetve egy 2-est, és megnézzük, hogy milyen permutáció hat az egyes élkockákra írt számokon tetszőleges $g \in G_0$, illetve $g \in G$ esetén. Számozzuk meg az élkockákat a következő módon: $k_{\mathrm{FU}} = 1$, $k_{\mathrm{FR}} = 2$, $k_{\mathrm{FD}} = 3$, $k_{\mathrm{FL}} = 4$, $k_{\mathrm{BU}} = 5$, $k_{\mathrm{BL}} = 6$, $k_{\mathrm{BD}} = 7$, $k_{\mathrm{BR}} = 8$, $k_{\mathrm{RU}} = 9$, $k_{\mathrm{RD}} = 10$, $k_{\mathrm{LU}} = 11$, $k_{\mathrm{LD}} = 12$. A referenciafelírást tördelési okokból nem általános alakban írom fel, de az i-edik élkockán hat az $f_i \in S_2$ tetszőleges permutáció, az f_i-kre ebben az esetben semmilyen kikötést nem kell tenni.



Az r és l lapok élkockáinak hálóját ezekből már el lehet készíteni. Az elemi forgatásokhoz tartozó $\vec{o_E}$ vektorok a következők:

$$\begin{aligned}
\vec{o_E}(\mathrm{F}) &= (f_1^{-1}f_4, f_2^{-1}f_1, f_3^{-1}f_2, f_4^{-1}f_3, \mathrm{id}, \mathrm{id}, \mathrm{id}, \mathrm{id}, \mathrm{id}, \mathrm{id}, \mathrm{id}, \mathrm{id});\\
\vec{o_E}(\mathrm{B}) &= (\mathrm{id}, \mathrm{id}, \mathrm{id}, \mathrm{id}, f_5^{-1}f_8, f_6^{-1}f_5, f_7^{-1}f_6, f_8^{-1}f_7, \mathrm{id}, \mathrm{id}, \mathrm{id}, \mathrm{id});\\
\vec{o_E}(\mathrm{U}) &= (f_1^{-1}f_9, \mathrm{id}, \mathrm{id}, \mathrm{id}, f_5^{-1}f_{11}, \mathrm{id}, \mathrm{id}, \mathrm{id}, f_9^{-1}f_5, \mathrm{id}, f_{11}^{-1}f_1, \mathrm{id});\\
\vec{o_E}(\mathrm{D}) &= (\mathrm{id}, \mathrm{id}, f_3^{-1}f_{12}, \mathrm{id}, \mathrm{id}, \mathrm{id}, f_7^{-1}f_{10}, \mathrm{id}, \mathrm{id}, f_{10}^{-1}f_3, \mathrm{id}, f_{12}^{-1}f_7);\\
\vec{o_E}(\mathrm{R}) &= (\mathrm{id}, f_2^{-1}(12)f_{10}, \mathrm{id}, \mathrm{id}, \mathrm{id}, \mathrm{id}, \mathrm{id}, f_8^{-1}(12)f_9, f_9^{-1}(12)f_2, f_{10}^{-1}(12)f_8, \mathrm{id}, \mathrm{id});\\
\vec{o_E}(\mathrm{L}) &= (\mathrm{id}, \mathrm{id}, \mathrm{id}, f_4^{-1}(12)f_{11}, \mathrm{id}, f_6^{-1}(12)f_{12}, \mathrm{id}, \mathrm{id}, \mathrm{id}, \mathrm{id}, f_{11}^{-1}(12)f_6, f_{12}^{-1}(12)f_4).
\end{aligned} \tag{2.4}$$

Az összes elemi forgatásnak az élkockákhoz tartozó orientációvektora is egységvektor. A sarokkockák orientációjához hasonlóan szorzat orientációja:

$$\vec{o_E}(g \cdot h) = ((\vec{o_E}(g) * p_E(h)) \cdot \vec{o_E}(h).$$

Mivel minden G-beli elemet fel tudunk írni az elemi forgatások szorzataként, a sarokkockák orientációjának vizsgálatánál alkalmazott következtetések szinte szó szerint átvehetőek, és belátható, hogy a G-beli elemeknek az

élkockákhoz tartozó orientációvektora is egység minden esetben, illetve hogy a $\Phi : S_2^{12} \to S_2$ $\Phi(s_1, \ldots, s_{12}) = s_1 \cdot \ldots \cdot s_{12}$ homomorfizmus magja az egységvektorok csoportja. Ami a későbbiek szempontjából fontos, hogy ha $g \in G$, akkor (2.2)-ben $o_E = (12)$, és $\sum_{i=1}^{12} l_i \equiv 0 \mod 2$.

2.6.4. Előállítások

Azt látjuk tehát, hogy $|G_0 : G|$ legalább 12, mivel a sarokkockák és az élkockák nem helyezkedhetnek el egymáshoz képest bárhogy, a lehetséges esetek felét lehet megvalósítani az elemi forgatások segítségével, a sarok- és élkockák egy adott sorrendje mellett a sarokkockák lehetséges orientációinak harmada, az élkockák lehetséges orientációinak fele valósulhat meg. Megmutatom, hogy ezeket a helyzeteket el lehet érni a lapok forgatásával. Elsőként nézzük az alkockák permutációit. Az előző részben nem írtam fel, hogy az elemi forgatások hogyan permutálják a sarok-, illetve az élkockákat egymás között, mivel nem volt rá szükség, most tegyük meg:

X	$p_V(X)$	$p_E(X)$
F	$(1,2,3,4)$	$(1,2,3,4)$
B	$(5,6,7,8)$	$(5,6,7,8)$
R	$(2,5,8,3)$	$(2,9,8,10)$
L	$(1,4,7,6)$	$(4,12,6,11)$
U	$(1,6,5,2)$	$(1,11,5,9)$
D	$(3,8,7,4)$	$(7,12,3,10)$

A 1.4.1-as lemma feltételei teljesülnek az elemi forgatások sarok- és élkockapermutációira is, emiatt 1.4.5 alapján[1]

$$\langle p_V(\mathrm{F}), p_V(\mathrm{B}), p_V(\mathrm{R}), p_V(\mathrm{L}), p_V(\mathrm{U}), p_V(\mathrm{D})\rangle = S_8$$
$$\langle p_E(\mathrm{F}), p_E(\mathrm{B}), p_E(\mathrm{R}), p_E(\mathrm{L}), p_E(\mathrm{U}), p_E(\mathrm{D})\rangle = S_{12}.$$

Ugyanakkor ebből még nem következik, hogy V és E összes azonos előjelű permutációjának kombinációját is elő tudjuk állítani az elemi forgatások segítségével. Az egyik út, hogy ezt bebizonyítsuk, az lenne, hogy keresünk egy olyan G-beli elemet, amely minden sarok- vagy élkockát helyben hagy, és néhány él- vagy sarokkockát egymás között permutál – ennek és konjugáltjainak

[1] 1.4.5 kivétele nem teljesül, mivel a 2.5-ös fejezetben láttuk, hogy $\mathrm{R}^2\mathrm{U}^2$ permutációiban van hármasciklus mind a csúcs-, mind az élkockákon, de bármely két négyesciklusnak a négyzetét véve is azonnal látszik, hogy nem felcserélhetőek.

többszöri alkalmazásával minden sorrendet megkapnánk. Próbáljunk meg ennél elegánsabb bizonyítást találni! Mivel az élkockák száma nagyobb, mint a sarokkockáké, egyszerűbb azt megvizsgálni, hogy a sarokkockák egy tetszőleges, adott p_V sorrendjét megvalósító különböző G-beli elemek az élkockák összes olyan p_E permutációját megvalósítják, amelynek előjele megegyezik p_V előjelével, vagy ami ezzel ekvivalens:

$$\langle p(\mathrm{F}), p(\mathrm{B}), p(\mathrm{R}), p(\mathrm{L}), p(\mathrm{U}), p(\mathrm{D})\rangle = \mathrm{sg}(S_8 \times S_{12}),$$

ahol $p(\mathrm{X}) = (p_V(\mathrm{X}), p_E(\mathrm{X}))$ minden $\mathrm{X} \in \{\mathrm{F},\ \mathrm{B},\ \mathrm{R},\ \mathrm{L}\ \mathrm{U},\ \mathrm{D}\}$ esetén, és $\mathrm{sg}(S_8 \times S_{12})$ $S_8 \times S_{12}$ azon részcsoportját jelöli, amelynek minden (z_1, z_2) $(z_1 \in S_8,\ z_2 \in S_{12})$ elemére $(z_1)\mathrm{sg} = (z_2)\mathrm{sg}$. Ez alapján észre lehet venni, hogy $\mathrm{sg}(S_8 \times S_{12})$ a $\Phi : S_8 \times S_{12} \to \{-1, 1\}, \Phi((z_1, z_2)) = (z_1)\mathrm{sg} \cdot (z_2)\mathrm{sg}$ homomorfizmus magja (az, hogy normálosztó, már abból következett, hogy az indexe 2). Mindenesetre $\mathrm{sg}(S_8 \times S_{12})$ zárt a konjugálásra $S_8 \times S_{12}$-n belül. Nézzük meg az elemi forgatások permutációinak egymással vett konjugáltjait, hátha kapunk egy ötletet. Ami lényeges különbség az elemi forgatások p_V-je és p_E-je között, hogy bármely két nem diszjunkt elemi forgatásnak két közös sarokkockája van, ugyanakkor csak egy közös élkockája, ezért sejthetően könnyebb két olyan G-beli elemet találni, amelyek különbözőek, de a sarokkockákat ugyanúgy permutálják. Emiatt először ezeket vizsgálom. Az alábbi táblázat számolásait nem írom le, a GAP nevű programban mindenki könnyen leellenőrizheti.[2]

	F	B	R	L	U	D
F	(1234)	(5678)	(3584)	(1762)	(2653)	(1487)
B	(1234)	(5678)	(2653)	(1487)	(1762)	(3584)
R	(1524)	(3867)	(2583)	(1476)	(1685)	(2374)
L	(2374)	(1685)	(2583)	(1476)	(1524)	(3867)
U	(1346)	(2578)	(1283)	(4756)	(1652)	(3874)
D	(1283)	(4756)	(2578)	(1346)	(1652)	(3874)

(2.5)

A táblázat alapján meg tudunk adni 12 olyan elemet, amelyek nem permutálják a sarokkockákat, de nem azonosak G identitásával (a rövidség kedvéért

[2]A táblázat értelmezéséhez: az oszlopban szereplő elemi forgatáshoz tartozó permutációt konjugáljuk a sorban szereplő elemi forgatáshoz tartozó permutációval.

$h^{-1}gh$-t g^h-val fogom jelölni):

$$p_V(\mathrm{R}^{\mathrm{F}}(\mathrm{D}^{-1})^{\mathrm{B}}) = p_V(\mathrm{L}^{\mathrm{F}}(\mathrm{U}^{-1})^{\mathrm{B}}) = p_V(\mathrm{U}^{\mathrm{F}}(\mathrm{R}^{-1})^{\mathrm{B}}) = p_V(\mathrm{D}^{\mathrm{F}}(\mathrm{L}^{-1})^{\mathrm{B}}) =$$
$$= p_V(\mathrm{F}^{\mathrm{R}}(\mathrm{U}^{-1})^{\mathrm{L}}) = p_V(\mathrm{B}^{\mathrm{R}}(\mathrm{D}^{-1})^{\mathrm{L}}) = p_V(\mathrm{U}^{\mathrm{R}}(\mathrm{B}^{-1})^{\mathrm{L}}) = p_V(\mathrm{D}^{\mathrm{R}}(\mathrm{F}^{-1})^{\mathrm{L}}) =$$
$$= p_V(\mathrm{F}^{\mathrm{U}}(\mathrm{L}^{-1})^{\mathrm{D}}) = p_V(\mathrm{B}^{\mathrm{U}}(\mathrm{R}^{-1})^{\mathrm{D}}) = p_V(\mathrm{R}^{\mathrm{U}}(\mathrm{F}^{-1})^{\mathrm{D}}) = p_V(\mathrm{L}^{\mathrm{U}}(\mathrm{B}^{-1})^{\mathrm{D}})$$

Nézzük meg, hogy ezek az elemek milyen permutációkat eredményeznek az élkockákon! Ezeket a számításokat is a GAP-ben végeztem el.

$$p_E(\mathrm{R}^{\mathrm{F}}(\mathrm{D}^{-1})^{\mathrm{B}}) = (3,9,10,12,8); \qquad p_E(\mathrm{L}^{\mathrm{F}}(\mathrm{U}^{-1})^{\mathrm{B}}) = (1,12,11,9,6);$$
$$p_E(\mathrm{U}^{\mathrm{F}}(\mathrm{R}^{-1})^{\mathrm{B}}) = (2,11,9,10,5); \qquad p_E(\mathrm{D}^{\mathrm{F}}(\mathrm{L}^{-1})^{\mathrm{B}}) = (4,10,12,11,7);$$
$$p_E(\mathrm{F}^{\mathrm{R}}(\mathrm{U}^{-1})^{\mathrm{L}}) = (1,5,4,9,3); \qquad p_E(\mathrm{B}^{\mathrm{R}}(\mathrm{D}^{-1})^{\mathrm{L}}) = (3,6,10,5,7);$$
$$p_E(\mathrm{U}^{\mathrm{R}}(\mathrm{B}^{-1})^{\mathrm{L}}) = (1,5,7,11,8); \qquad p_E(\mathrm{D}^{\mathrm{R}}(\mathrm{F}^{-1})^{\mathrm{L}}) = (1,12,2,7,3);$$
$$p_E(\mathrm{F}^{\mathrm{U}}(\mathrm{L}^{-1})^{\mathrm{D}}) = (2,4,6,3,11); \qquad p_E(\mathrm{B}^{\mathrm{U}}(\mathrm{R}^{-1})^{\mathrm{D}}) = (2,7,9,6,8);$$
$$p_E(\mathrm{R}^{\mathrm{U}}(\mathrm{F}^{-1})^{\mathrm{D}}) = (1,8,2,4,10); \qquad p_E(\mathrm{L}^{\mathrm{U}}(\mathrm{B}^{-1})^{\mathrm{D}}) = (4,6,8,12,5)$$

Azt kaptuk, hogy míg a sarokkockákat mind helyben hagyják, az élkockákat mind különböző módokon permutálják! Ez azt jelenti, hogy a sarok- és az élkockák minden olyan permutációját meg lehet valósítani, amelyeknek az előjele megegyezik. Először ugyanis állítsuk be a sarokkockákat a megfelelő sorrendbe – ezt meg tudjuk tenni, hiszen az elemi forgatások p_V-i generálják S_8-at. Ezután pedig a sarokkockákon (a permutációikat tekintve csak) identikusan ható 12 elem segítségével be lehet állítani az élkockák tetszőleges sorrendjét, hiszen ezen elemek permutációi által generált csoport A_{12} (valójában már a két oszlop első két-két eleme is generálja), mivel eleget tesznek 1.4.1 feltételeinek, s így érvényes rájuk 1.4.7. Az is egyértelműen kijött, hogy az így kirakott helyzetekben $(p_V(g))\mathrm{sg} = (p_E(g))\mathrm{sg}$, ahogy vártuk.

Most ugyan nem volt rá szükségem, de a későbbiekben még használni fogom, hogy az elemi forgatások egymással vett konjugáltjai hogyan permutálják az élkockákat egymás között, az előző táblázat párja:

	F	B	R	L	U	D
F	$(1,2,3,4)$	$(5,6,7,8)$	$(3,9,8,10)$	$(1,12,6,11)$	$(2,11,5,9)$	$(4,10,7,12)$
B	$(1,2,3,4)$	$(5,6,7,8)$	$(2,9,5,10)$	$(4,12,7,11)$	$(1,11,6,9)$	$(3,10,8,12)$
R	$(1,9,3,4)$	$(5,6,7,10)$	$(2,9,8,10)$	$(4,12,6,11)$	$(1,11,5,8)$	$(2,7,12,3)$
L	$(1,2,3,12)$	$(5,11,7,8)$	$(2,9,8,10)$	$(4,12,6,11)$	$(1,4,5,9)$	$(3,10,7,6)$
U	$(2,3,4,11)$	$(6,7,8,9)$	$(1,8,10,2)$	$(4,12,6,5)$	$(1,11,5,9)$	$(3,10,7,12)$
D	$(1,2,10,4)$	$(5,6,12,8)$	$(2,9,8,7)$	$(3,6,11,4)$	$(1,11,5,9)$	$(3,10,7,12)$

(2.6)

Hátra van még annak bizonyítása, hogy az alkockák tetszőleges, adott sorrendje mellett az alkockák összes lehetséges orientációját meg tudjuk valósítani a Rubik-kocka forgatásaival. Mielőtt ezt belátnám, kicsit jobban megvizsgálom a sarok- és az élkockák orientációvektorait, hátha találok olyan tulajdonságokat, amelyeket fel tudok használni. Mivel az orientációvektorokat teljesen analóg módon definiáltam, a legtöbb egyenletet általánosságban vezetem le (értsd: V vagy E index nélkül) mindkét esetre, majd megvizsgálom, hogy miben különböznek a végeredmény szempontjából. Először azt szeretném megvizsgálni, hogy tetszőleges elemi forgatás esetén milyen kapcsolat van $\vec{o}(X)$ és $\vec{o}(X^n)$ között, itt $X \in \{\mathrm{F}, \mathrm{B}, \mathrm{R}, \mathrm{L}, \mathrm{U}, \mathrm{D}\}, n \in \{2,3\}$. Az egyszerűség kedvéért a sarok- és az élkockák felírása is legyen a lehető legegyszerűbb, tehát az általános alakból úgy kapjuk mindkettőt, hogy minden $f_i = \mathrm{id}$. (Emlékszünk: f_i az i-edik sarok-, illetve élkocka felírásán ható permutáció.)

$$\vec{o}(X^2) = (\vec{o}(X) * p(X)) \cdot \vec{o}(X)$$

2.3 alapján (vagy ha ránézünk a sarokkockák referenciafelírására) kapjuk, hogy az elemi forgatások négyzetének esetében a sarokkockák orientációja az identitás, az élkockák orientációja pedig 2.4 alapján szintén az identitás. Ebből következik, hogy

$$\vec{o}(X^3) = (\vec{o}(X^2) * p(X)) \cdot \vec{o}(X) = \vec{o}(X) = \vec{o}(X^{-1}).$$

1.1.18 alapján tudjuk, hogy X és $Y^{-1}XY$ rendje megegyezik, illetve igaz a következő két egyenlőség:

$$\begin{aligned} Y^{-1}X^2Y &= Y^{-1}XYY^{-1}XY = (Y^{-1}XY)^2 \\ Y^{-1}X^3Y &= Y^{-1}X^2YY^{-1}XY = (Y^{-1}XY)^3, \end{aligned} \tag{2.7}$$

és egyenlő elemek p_V-je és p_E-je is egyenlő. Érdemes meggondolni még a következőket: ahogy már korábban is definiáltam, legyen $N_E = \{g \in G : p_E(g) = \mathrm{id}\}$, $N_V = \{g \in G : p_V(g) = \mathrm{id}\}$, és tetszőleges $g \in N_E$ esetén $\vec{o_E}(g^2) = (p_E(g) * \vec{o_E}(g)) \cdot \vec{o_E}(g) = (\vec{o_E}(g))^2 = \mathrm{id}$, illetve tetszőleges $g \in N_V$ esetén $\vec{o_V}(g^3) = (p_V * \vec{o_V}(g)) \cdot \vec{o_V}(g^2) = (p_V * \vec{o_V}(g))^2 \cdot \vec{o_V}(g) = (\vec{o_V}(g))^3 = \mathrm{id}$. Az egyenletek alapján az az ötletünk támadhat, hogy keressünk olyan $g_1, g_2 \in G$ elemeket, amelyekre $p_V(g_i)$ és $p_E(g_i)$ rendje l (i =1, 2 esetén), g_1 és g_2 nem egymás inverzei, a közös sarok- és élkockákat g_2g_1 nem permutálja, és van olyan sarok- vagy élkocka, amely nem közös. Ha g_2g_1-et a

$k = (o(p_V(g_2g_1)), o(p_E(g_2g_1)))$-edik[3] hatványra emeljük, $(N_E \cap N_V)$-beli elemet kapunk, amely azonban nem feltétlen az identitás (ha minden sarok- vagy élkocka közös lenne, vagy ha nem lenne közös sarok- vagy élkocka, akkor biztosan az identitást kapnánk vissza, és nem ez a célunk). Ennek négyzete identikusan hat az élkockák orientációján, a sarokkockákén viszont csak akkor, ha az eredeti k-hatvány is identikusan hatott, a köbük pedig identikusan hat a sarokkockák orientációján, az élkockákén viszont csak akkor, ha az eredeti k-hatvány is identikusan hatott. Emiatt olyan elemeket érdemes vizsgálni, amelyeknek van közös sarok-, illetve élkockájuk. Így elvileg találhatunk olyan $g \in G$ elemet, amely identikusan permutál minden alkockát, az élkockák orientációján nem változtat, a sarokkockák közül néhányén viszont igen, vagy fordítva. Elsőnek vizsgáljuk meg az $l = 2$ esetet. Tudjuk, hogy $o(\mathrm{F}^2) = o(\mathrm{B}^2) = o(\mathrm{R}^2) = o(\mathrm{L}^2) = o(\mathrm{U}^2) = o(\mathrm{D}^2) = 2$, tehát a konjugáltjaik rendje is 2. (2.5) és (2.6) alapján (2.7) segítségével könnyen találhatunk az előbbi fejtegetés feltételeinek megfelelő elemeket. Ilyen elemek: $g_1 = (\mathrm{L}^2)^{\mathrm{F}}$ és $g_2 = (\mathrm{R}^2)^{\mathrm{D}}$; $g_3 = (\mathrm{U}^2)^{\mathrm{F}}$ és $g_4 = (\mathrm{D}^2)^{\mathrm{L}}$ stb. g_1 és g_2 esetén $k = 2$. Számítsuk ki $(g_2g_1)^2$ orientációvektorát a sarokkockákon!

$$\begin{aligned} \vec{o_V}((g_2g_1)^2) &= (\vec{o_V}(g_2g_1) * p_V(g_2g_1)) \cdot \vec{o_V}(g_2g_1) \\ \vec{o_V}(g_2g_1) &= (\vec{o_V}(g_2) * p_V(g_1)) \cdot \vec{o_V}(g_1) \end{aligned}$$

A részletszámításokat az olvashatóság kedvéért külön írom:

$$\begin{aligned} \vec{o_V}(g_1) &= (\vec{o_V}(\mathrm{F}^{-1}) * p_V(\mathrm{L}^2\mathrm{F})) \cdot \vec{o_V}(\mathrm{L}^2\mathrm{F}) = \\ &= (\vec{o_V}(\mathrm{F}^{-1}) * p_V(\mathrm{L}^2\mathrm{F})) \cdot (\vec{o_V}(\mathrm{L}^2) * p_V(\mathrm{F})) \cdot \vec{o_V}(\mathrm{F}). \end{aligned}$$

Mivel $\vec{o_V}(\mathrm{F}) = \vec{o_V}(\mathrm{F}^{-1}) = \vec{o_V}(\mathrm{L}^2) = \mathrm{id}$, ezért $\vec{o_V}(g_1) = \mathrm{id}$.

$$\begin{aligned} \vec{o_V}(g_2) &= (\vec{o_V}(\mathrm{D}^{-1}) * p_V(\mathrm{R}^2\mathrm{D})) \cdot \vec{o_V}(\mathrm{R}^2\mathrm{D}) = \\ &= (\vec{o_V}(\mathrm{D}^{-1}) * p_V(\mathrm{R}^2\mathrm{D})) \cdot (\vec{o_V}(\mathrm{R}^2) * p_V(\mathrm{D})) \cdot \vec{o_V}(\mathrm{D}). \\ p_V(\mathrm{R}^2\mathrm{D}) &= (28)(35)(3874) = (274358) \\ \vec{o_V}(\mathrm{D}^{-1}) &= \vec{o_V}(\mathrm{D}) = (\mathrm{id}, \mathrm{id}, (123), (132), \mathrm{id}, \mathrm{id}, (123), (132)) \\ \vec{o_V}(\mathrm{R}^2) * p_V(\mathrm{D}) &= \mathrm{id} * p_V(\mathrm{D}) = \mathrm{id} \\ \vec{o_V}(\mathrm{D}^{-1}) * p_V(\mathrm{R}^2\mathrm{D}) &= (\mathrm{id}, (132), (132), (123), (123), \mathrm{id}, \mathrm{id}, \mathrm{id}) \\ \vec{o_V}(g_2) &= (\mathrm{id}, (132), \mathrm{id}, \mathrm{id}, (123), \mathrm{id}, (123), (132)) \end{aligned}$$

[3] tehát $p_V(g_2g_1)$ rendjének és $p_E(g_2g_1)$ rendjének legkisebb közös többszöröse

A szorzat orientációja:

$$p_V(g_1) = (16)(72)$$
$$\vec{o_V}(g_2g_1) = \vec{o_V}(g_2) * p_V(g_1) = (\mathrm{id}, (123), \mathrm{id}, \mathrm{id}, (123), \mathrm{id}, (132), (132)).$$

Végül a keresett orientációvektor:

$$p_V(g_2g_1) = (27)(58)(16)(72) = (58)(16)$$
$$\vec{o_V}((g_2g_1)^2) = (\vec{o_V}(g_2g_1) * (16)(58)) \cdot \vec{o_V}(g_2g_1) =$$
$$= (\mathrm{id}, (123), \mathrm{id}, \mathrm{id}, (132), \mathrm{id}, (132), (123)) \cdot (\mathrm{id}, (123), \mathrm{id}, \mathrm{id}, (123), \mathrm{id}, (132), (132)) =$$
$$= (\mathrm{id}, (132), \mathrm{id}, \mathrm{id}, \mathrm{id}, \mathrm{id}, (123), \mathrm{id})$$

Most vizsgáljuk meg $(g_2g_1)^2$ orientációvektorát az élkockákon! A felírt képletek érvényesek maradnak, csupán az $\vec{o_V}$-k helyébe $\vec{o_E}$-ket, a p_V-k helyébe p_E-ket kell írni.

$$\vec{o_E}((g_2g_1)^2) = (\vec{o_E}(g_2g_1) * p_E(g_2g_1)) \cdot \vec{o_E}(g_2g_1)$$
$$\vec{o_E}(g_2g_1) = (\vec{o_E}(g_2) * p_E(g_1)) \cdot \vec{o_E}(g_1)$$

A részletszámítások:

$$\vec{o_E}(g_1) = (\vec{o_E}(\mathrm{F}^{-1}) * p_E(\mathrm{L}^2\mathrm{F})) \cdot \vec{o_E}(\mathrm{L}^2\mathrm{F}) =$$
$$= (\vec{o_E}(\mathrm{F}^{-1}) * p_E(\mathrm{L}^2\mathrm{F})) \cdot (\vec{o_E}(\mathrm{L}^2) * p_E(\mathrm{F})) \cdot \vec{o_E}(\mathrm{F}).$$

Mivel $\vec{o_E}(\mathrm{F}) = \vec{o_E}(\mathrm{F}^{-1}) = \vec{o_E}(\mathrm{L}^2) = \mathrm{id}$, ezért $\vec{o_E}(g_1) = \mathrm{id}$.

$$\vec{o_E}(g_2) = (\vec{o_E}(\mathrm{D}^{-1}) * p_E(\mathrm{R}^2\mathrm{D})) \cdot \vec{o_E}(\mathrm{R}^2\mathrm{D}) =$$
$$= (\vec{o_E}(\mathrm{D}^{-1}) * p_E(\mathrm{R}^2\mathrm{D})) \cdot (\vec{o_E}(\mathrm{R}^2) * p_E(\mathrm{D})) \cdot \vec{o_E}(\mathrm{D}).$$

Mivel $\vec{o_E}(\mathrm{D}) = \vec{o_E}(\mathrm{D}^{-1}) = \vec{o_E}(\mathrm{R}^2) = \mathrm{id}$, ezért $\vec{o_E}(g_2) = \mathrm{id}$, ebből következik, hogy $\vec{o_E}(g_1g_2) = \mathrm{id}$, emiatt pedig $\vec{o_E}((g_1g_2)^2) = \mathrm{id}$.

A számolás alapján nem is kell $(g_2g_1)^2$-et négyzetre emelni, mivel már ő sem változtatja meg az élkockák orientációját, viszont $(N_V \cap N_E)$-beli elem. Igaz, így a harmadik hatványa is identikusan hat az élkockák orientációján, úgyhogy még keresni kell olyan $(N_V \cap N_E)$-beli elemet, amellyel az élkockák tetszőleges orientáció-kiosztását meg tudjuk valósítani. Ha ez megvan, akkor $(g_2g_1)^2$-tel, illetve konjugáltjaival be lehet állítani a sarokkockák orientációját. Például ha az i-edik sarokkockának meg akarjuk változtatni az

orientációját, akkor csak át kell vinni a második vagy a hetedik sarokkocka pozíciójába (ezt meg tudjuk tenni, mivel G tranzitív), végrehajtani a megadott forgatást, majd visszavinni az eredeti helyzetébe. (Úgy gondolom, ez elég világos, nem vezetem le az orientációk szorzásából.)

Próbáljunk meg hasonlóan eljárni az élkockák orientációjánál is, mint a sarokkockák esetében! A (2.6)-os táblázatban sajnos nem találni olyan permutációkat, amelyek megfelelőek lennének, és ez nem véletlen. Tudjuk, hogy két nem diszjunkt elemi forgatásnak egy közös élkockája van, tehát ha konjugáljuk őket egymással, akkor a permutációk közös eleme megváltozik, a többi helyben marad. Emiatt nem fordulhat elő, hogy két közös és két különböző elemük van az ilyen permutációknak, miközben a közös elemeket önmagukba viszi a szorzatuk. Persze ha elég sok ilyen konjugálási táblázatot készítenénk, valószínűleg találnánk megfelelő elemeket, de nagyon hosszú lenne felírni az orientációkat. Próbáljunk meg inkább máshogy $(N_E \cap N_V)$-beli elemet generálni! Ha találunk két olyan elemet, amelyekre $p_E(g_1) = p_E(g_2)$, $p_V(g_1) = p_V(g_2)$, de $g_1 \neq g_2$, akkor $g_1^{-1}g_2$ (és persze a hatványai és ezek konjugáltjai is) $(N_E \cap N_V)$-beli lesz. Mindeközben persze célunk, hogy $\vec{o_E}(g_1^{-1}g_2)$ ne az identitás legyen. Annak a feltételnek, hogy $g_1 \neq g_2$, úgy tudunk a legkönnyebben megfelelni, ha g_1 és g_2 az elemi forgatásokkal történő felírásában vannak olyan generátorelemek, amelyek a másikában nem szerepelnek. Tegyük fel, hogy $g_1 \in \langle X_1, X_2 \rangle$, $g_2 \in \langle X_1, X_3, X_4 \rangle$. Érdemes meggondolni, hogy ahhoz, hogy $p_E(g_1) = p_E(g_2)$ teljesüljön, kell, hogy ugyanazokat az élkockákat permutálják. Ha két nem diszjunkt generátorelemmel generálunk egy forgatást, akkor biztos, hogy lesz két sarok- és öt élkocka, amelyeket minden ilyen forgatás helyben hagy. Emiatt g_2-nek legalább három különböző generátorelemmel kell rendelkeznie. Csak hogy a számításokat a lehető legegyszerűbbé tegyük, legyen $X_1 = \mathrm{F}$ (ennek az elemi forgatásnak az orientációvektora a sarokkockák és az élkockák esetében is az identitás). X_3 pedig legyen U! (Most még tetszőleges elemet választhatunk.) Vizsgáljuk meg, hogyan permutálja a sarok- és az élkockákat $g_2^* = \mathrm{U}^{-1}\mathrm{FU}$! ($g_2$ és g_2^* konjugált elemek.)

$$p_V(g_2^*) = (1,2,5,6)(1,2,3,4)(1,6,5,2) = (1,3,4,6)$$
$$p_E(g_2^*) = (1,9,5,11)(1,2,3,4)(1,11,5,9) = (11,2,3,4)$$

Vizsgáljuk meg, hogy az elemi forgatások és egymással vett konjugáltjaik közül melyek p_E-je független $p_E(g_2^*)$-tól! Ha ezekkel az elemekkel konjugáljuk g_2^*-ot, akkor az élkockák permutációja nem változik, a sarokkockáké viszont igen. (2.6) alapján ilyen elemek: B és konjugáltjai, kivéve B^{L}, és ezek hatvá-

nyai. A következő táblázatban szerepel, mi lesz $p_V(h^{-1}g_2^*h)$ h függvényében:

h	$p_V(h^{-1}g_2^*h)$
id	$(1,3,4,6)$
B	$(1,3,4,7)$
$\mathrm{R}^{-1}\mathrm{BR}$	$(1,8,4,7)$
$\mathrm{U}^{-1}\mathrm{BU}$	$(1,3,4,6)$
$\mathrm{D}^{-1}\mathrm{BD}$	$(1,3,7,4)$
B^2	$(1,3,4,8)$
$\mathrm{R}^{-1}\mathrm{B}^2\mathrm{R}$	$(1,6,4,3)$
$\mathrm{U}^{-1}\mathrm{B}^2\mathrm{U}$	$(1,3,4,6)$
$\mathrm{D}^{-1}\mathrm{B}^2\mathrm{D}$	$(1,3,5,7)$

(2.8)

Most, hogy kicsit kibővítettük a lehetséges p_V-k halmazát, nézzük, hogy tudnánk F-ből és egy még fel nem használt generátorelemből olyan g_1 forgatást generálni, amelyre $p_E(g_1) = (11,2,3,4)$! A 11-es szám két elemi forgatás p_E-jében jelenik meg, de U-t már „elhasználtuk", így X_2 legyen L. A megfelelő permutációk: $p_E(\mathrm{F}) = (1,2,3,4)$, $p_E(\mathrm{L}) = (4,12,6,11)$, tehát két négyesciklusról van szó, amelyeknek egy közös eleme van. Mi történik általános esetben, ha konjugáljuk az egyiket a másikkal?

$$(adcb)(defg)(abcd) = (aefg)$$

Tehát a közös elemet lecseréli arra, amelybe a konjugáló elemben képeződik. Ezek szerint olyan permutációra van szükségünk, amelyben az 1-es a 11-esbe képeződik. Ilyet tudunk gyártani a fenti azonosság alapján, mivel $p_E(\mathrm{L}^{-1})$-ben a 4-es a 11-esbe képeződik, $p_E(\mathrm{F})$-ben pedig az 1-esbe. Így kapjuk:

$$p_E((\mathrm{F}^{-1}\mathrm{L}^{-1}\mathrm{F})^{-1}\mathrm{F}\mathrm{F}^{-1}\mathrm{L}^{-1}\mathrm{F}) = p_E(\mathrm{F}^{-1}\mathrm{L}\mathrm{F}\mathrm{F}\mathrm{F}^{-1}\mathrm{L}^{-1}\mathrm{F}) = p_E(\mathrm{F}^{-1}\mathrm{L}\mathrm{F}\mathrm{L}^{-1}\mathrm{F}) =$$
$$= (1,4,3,2)(4,12,6,11)(1,2,3,4)(4,11,6,12)(1,2,3,4) = (4,11,2,3)$$

Tehát találtunk olyan elemet, amely az élkockákat ugyanúgy permutálja, mint g_2^*. Vizsgáljuk meg, hogy a sarokkockákat hogyan rendezi!

$$p_V(\mathrm{F}^{-1}\mathrm{L}\mathrm{F}\mathrm{L}^{-1}\mathrm{F}) = (1,4,3,2)(1,4,7,6)(1,2,3,4)(1,6,7,4)(1,2,3,4) = (2,6,3,4)$$

Legyen $g_1' = \mathrm{F}^{-1}\mathrm{L}\mathrm{F}\mathrm{L}^{-1}\mathrm{F}$. Még egy elemre szükségünk van, hogy g_1-et generálni tudjuk F-fel és L-lel. Most egy kicsit bonyolultabb kifejezéssel indítsunk,

tekintsük az $\mathrm{LF}^{-1}\mathrm{L}^{-1}\mathrm{F}$ és az $\mathrm{L}^{-1}\mathrm{FLF}^{-1}$ elemeket!

$$p_E(\mathrm{LF}^{-1}\mathrm{L}^{-1}\mathrm{F}) = (4,12,6,11)(1,4,3,2)(4,11,6,12)(1,2,3,4) = (4,1,11)$$
$$p_E(\mathrm{L}^{-1}\mathrm{FLF}^{-1}) = (4,11,6,12)(1,2,3,4)(4,12,6,11)(1,4,3,2) = (3,12,4)$$
$$p_V(\mathrm{LF}^{-1}\mathrm{L}^{-1}\mathrm{F}) = (1,4,7,6)(1,4,3,2)(1,6,7,4)(1,2,3,4) = (1,4)(2,6)$$
$$p_V(\mathrm{L}^{-1}\mathrm{FLF}^{-1}) = (1,6,7,4)(1,2,3,4)(1,4,7,6)(1,4,3,2) = (1,4)(3,7)$$

Az első elemet szorozzuk meg balról F-fel, így minden szám megjelenik a kapott permutációban, amelyre szükségünk van (2,3,4,11):

$$(1,2,3,4)(1,11,4) = (1,2,3)(4,11)$$

Ezt a permutációt szeretnénk $(2,3,4,11)$-be vinni. Ehhez meg kell szoroznunk jobbról $(1,3,2)(4,11)(2,3,4,11) = (1,4,2)$-vel. Annyi a dolgunk tehát, hogy találjunk egy olyan forgatást, amely az élkockákat így permutálja. Itt jön kapóra a másik forgatás ($\mathrm{L}^{-1}\mathrm{FLF}^{-1}$), amelynek kiszámítottam az élkockákon vett permutációit. Ennek az inverzét szorozzuk meg balról szintén F-fel, kapjuk, hogy

$$(1,2,3,4)(3,4,12) = (1,2,4)(3,12).$$

Ennek fényében $p_E((\mathrm{F}^2\mathrm{L}^{-1}\mathrm{F}^{-1}\mathrm{L})^2) = (1,4,2)$. Találtunk tehát egy másik elemet is, amely ugyanúgy permutálja az élkockákat, mint g_2^*. Jelöljük g_1''-vel. Nézzük meg, hogyan permutálja a sarokkockákat!

$$(1,2,3,4)(1,4)(2,6)(1,2,3,4)(1,4)(3,7)(1,2,3,4)(1,4)(3,7) = (1,6,3,7)$$

Írjuk fel g_1''-t az elemi forgatások szorzataként:

$$g_1'' = \mathrm{FLF}^{-1}\mathrm{L}^{-1}\mathrm{F}(\mathrm{F}^2\mathrm{L}^{-1}\mathrm{F}^{-1}\mathrm{L})^2 = \mathrm{FLF}^{-1}\mathrm{L}^{-1}\mathrm{F}^{-1}\mathrm{L}^{-1}\mathrm{F}^{-1}\mathrm{LF}^2\mathrm{L}^{-1}\mathrm{F}^{-1}\mathrm{L}$$

Már csak egy lépés hiányzik. Láttuk, hogy g_1' a sarokkockákat $(2,6,3,4)$ szerint permutálja, az élkockákat pedig ugyanúgy, mint g_2. Mivel se $p_V(g_1')$, se $p_V(g_1'')$ nem szerepel a (2.8)-as táblázatban, próbáljunk egy ottani permutációt kihozni a segítségükkel. Szeretnénk eltüntetni a 2-est $p_V(g_1')$-ből, ezt úgy tehetjük meg, hogy konjugáljuk egy olyan hatványának inverzével $p_V(g_1'')$-t, amelyben a 2-es nem közös elembe, tehát a 4-esbe megy. Ez alapján

$$(2,4,3,6)(1,6,3,7)(2,6,3,4) = (1,3,4,7).$$

Világos, hogy $g_1'^{-1}g_1''g_1'$ pont így permutálja a sarokkockákat, az élkockákat pedig $(2,3,4,11)^{-1}(2,3,4,11)(2,3,4,11) = (2,3,4,11)$ szerint, tehát pont úgy, mint g_2^*. Ez az elem g_1. Fejezzük ki g_1-et az elemi forgatások szorzataként!

$$g_1 = \mathrm{F}^{-1}\mathrm{L}\mathrm{F}^{-1}\mathrm{L}^{-1}\mathrm{F}^2\mathrm{L}\mathrm{F}^{-1}\mathrm{L}^{-1}\mathrm{F}^{-1}\mathrm{L}^{-1}\mathrm{F}^{-1}\mathrm{L}\mathrm{F}^2\mathrm{L}^{-1}\mathrm{F}^{-1}\mathrm{L}\mathrm{F}^{-1}\mathrm{L}\mathrm{F}\mathrm{L}^{-1}\mathrm{F}$$

Mivel g_1 és $g_2 = \mathrm{B}^{-1}g_2^*\mathrm{B} = \mathrm{B}^{-1}\mathrm{U}^{-1}\mathrm{F}\mathrm{U}\mathrm{B}$ ugyanúgy permutálják a sarok- és az élkockákat is, ezért $g_2^{-1}g_1 \in (N_E \cap N_V)$. A $g_2^{-1}g_1$ forgatás orientációját meglehetősen hosszú lenne kiszámítani, ettől most eltekintek, egy kirakott Rubik-kockával a kezében (vagy a GAP-ben) bárki leellenőrizheti egyrészt, hogy valóban identikusan permutálja mind a sarok-, mind az élkockákat, másrészt hogy miként változtatja meg az orientációjukat. Pontosan két élkocka, a 2. és a 11. orientációját változtatja meg. A sarokkockák közül pedig az 1., 3., 4. és 7. orientációját. Értelemszerűen $(g_2^{-1}g_1)^3$ a sarokkockákon identikusan hat, az élkockák közül pedig továbbra is ennek a kettőnek változtatja meg az orientációját.

2.6.1. Tétel. A Rubik-kocka csoportja, G részcsoportot alkot a kibővített csoporton, G_0-on belül. Minden $g \in G_0$ elemet fel tudunk írni a következő alakban:

$$g = (\vec{o_V}, p_V, \vec{o_E}, p_E),$$

ahol $\vec{o_V} = ((123)^{k_1}, \ldots, (123)^{k_8}) \in C_3^8$, $p_V \in S_8$, $\vec{o_E} = ((12)^{l_1}, \ldots, (12)^{l_{12}}) \in C_2^{12}$, és $p_E \in S_{12}$, illetve minden $k_i \in \{0,1,2\}$ és minden $l_i \in \{0,1\}$. Egy $g \in G_0$ elem akkor és csak akkor eleme G-nek, ha

- $\mathrm{sg}(p_V) = \mathrm{sg}(p_E)$
- $\sum_{i=1}^{8} k_i \equiv 0 \mod (3)$
- $\sum_{i=1}^{12} l_i \equiv 0 \mod (2),$

vagy ami ezzel ekvivalens, a Rubik-kocka azon helyzetei valósíthatók meg G-vel, amelyekre ezek a feltételek teljesülnek.

Bizonyítás. Korábban beláttuk, hogy a sarokkockák tetszőleges permutációját be lehet állítani az elemi forgatások segítségével. Ezt követően az élkockák minden olyan permutációját meg lehet valósítani, amelynek előjele

megegyezik a sarokkockák permutációjával. Végül találtunk olyan forgatásokat, amelyek nem változtatnak az alkockák sorrendjén, de két sarok- vagy élkockának megváltoztatják az orientációját – ennek a két forgatásnak és konjugáltjaiknak a segítségével minden lehetséges orientációkiosztást megvalósíthatunk.

q. e. d.

Következmény. Ez alapján $|G_0 : G| = 12$, illetve

$$|G| = \frac{3^8 \cdot 2^{12} \cdot 8! \cdot 12!}{12} = 3^8 \cdot 2^{12} \cdot 8! \cdot 11! = 43\ 252\ 003\ 274\ 489\ 856\ 000$$

2.7. Érdekességek

A szakdolgozatom zárásaként néhány érdekességet foglalnék össze a Rubik-kockával kapcsolatban. Vajon legfeljebb hány forgatásra van szükség a 3×3-as Rubik-kocka kirakásához? Kétféle módon lehet megközelíteni a kérdést: az egyik esetben forgatásnak az általam elemi forgatásoknak nevezett forgatások hatványait tekintjük, illetve az M_F, M_R, M_U forgatások hatványait, amelyek a középső sort forgatják mindig az indexben szereplő forgatással azonos irányban (az könnyen látszik, hogy elég három ilyet venni, mivel $M_U = M_D^{-1}$ stb). Egy nem túlságosan bejáratott Rubik-kockán M_R-t egyszerűbb LR^{-1}-zel megvalósítani.[4] Ezt *fél-forgatás metrikának* (*half-turn metric*) szokás nevezni. A másik esetben forgatásnak csak az általam elemi forgatásnak nevezett forgatásokat és az inverzeiket, illetve az M_F, M_R, M_U forgatásokat és inverzeiket tekintjük, ezt *negyed-forgatás metrikának* (*quarter-turn metric*) szokás nevezni (ld. [4]). A kocka adott helyzetéhez tartozó legrövidebb kirakást *Isten algoritmusának* (*God's Algorithm*) szokták hívni, azt a legkisebb számot pedig, ahány forgatással bármely helyzetet meg lehet oldani, *Isten számának* (*God's Number*). Mennyi lehet Isten száma? Ez a kérdés a Rubik-kocka megjelenésétől (1980) folyamatosan az érdeklődés középpontjában állt. Nézzük előbb a fél-forgatás metrikát! Az első komolyabb eredménnyel Morwen Thistlethwaite jelentkezett 1981-ben: megmutatta, hogy 52 forgatással minden helyzetet ki lehet rakni. A következő eredményekre a 90-es évekig kellett

[4]Emiatt nincs ellentmondás azzal, hogy korábban feltettem, a középlapkák nem mozognak, mivel a többi lapka permutációival is ki lehet fejezni egy ilyen forgatást, most annyi a lényeg, hogy az átellenes lapok ugyanolyan irányba történő, ugyanakkora elfordulással rendelkező forgatásait egy forgatásnak vesszük.

várni, két lényeges dolog történt: 1995-ben Michael Reid bebizonyította, hogy elég 29 forgatás és hogy van olyan pozíció, amelyet 20-nál kevesebb forgatással nem lehet kirakni (a *superflip* pozíció, amikor minden alkocka a helyén van, de minden élkockának rossz az orientációja). A következő lépésre több mint tíz évet kellett várni, 2005 végén Silviu Radunak sikerült megmutatnia, hogy 28 lépés is elég, pár hónappal később pedig a 27-et is igazolta. Egy évvel később Dan Kunkle és Gene Cooperman még eggyel lejjebb tudta vinni Isten számát. A 2007-es évtől Tomas Rokicki és munkatársai (az évek során többekkel dolgozott együtt) tudtak további előrelépést produkálni a kérdésben, 2008-ra 22-re tudták szorítani, végül 2010 júliusában számítógépes elemzés segítségével bebizonyították, hogy minden esetben elég 20 forgatás.

A negyed-forgatás metrikában hasonlóan alakult a dolgok menete, kisebb időbeli csúszással. Michael Reid 1995-ben belátta, hogy 42 forgatással bármely helyzetet ki lehet rakni, 1998 augusztusában pedig talált egy pozíciót (superflip + *fourspot* - még két-két átellenes középlapkát felcserél), amelynek kirakásához 26 forgatásra van szükség. Ezt Silviu Radu 2007-ig 34-re csökkentette. A végső lépést szintén Tomas Rokicki tette meg, 2014 augusztusára bebizonyította, hogy 26 forgatással minden helyzet kirakható. Az érdeklődők további információt találhatnak [4]-ben.

A 2×2-es Rubik-kocka esetében Isten száma 11 a fél-forgatás metrika szerint, illetve 14 a negyed-forgatás metrika szerint. Nem néztem utána, hogy ezt ki bizonyította be elsőként, de az interneten rengeteg helyen lehet találni olyan programozási kódokat, amelyek megoldják a problémát. (Számítógép használata nélkül elég nehéznek tűnik kihozni a választ az esetek nagy száma miatt, de úgy gondolom, nem esélytelen vállalkozás.)

A kérdés matematikai kezeléséhez a *Cayley-gráf* ad egyszerű leírást. Legyen G véges csoport. Ha adott az $X = \{g_1, g_2, \dots g_n\}$ halmaz, amelyben minden $g_i \in G$, akkor $\langle X \rangle$ Cayley-gráfjában a csúcsok $\langle X \rangle$ elemei, és két csúcs, x_1 és x_2 között akkor megy él, ha létezik i, amelyre $x_1 g_i = x_2$ vagy $x_1 g_i^{-1} = x_2$.[5] Két csúcs távolságán az őket összekötő utak hosszának minimumát értjük (vagy a legrövidebb út hosszát, ha létezik ilyen), illetve ha nincs köztük út, akkor a távolságuk ∞. Egy gráf átmérője a távolságok maximuma. Könnyen látszik, hogy egy generált csoport Cayley-gráfja mindig összefüggő. Isten száma pedig tulajdonképpen a Rubik-kocka csoportja Cayley-gráfjának (Γ_{Rubik}) átmérője. A negyed forgatás-metrikában a generátorok közé nem vesszük be az elemi forgatások és a középső sorok forgatásainak négyzetét, a

[5]Ez a definíció az irányítatlan Cayley-gráfé, meg lehet fogalmazni irányított élekkel is.

fél forgatás-metrikában viszont igen.

Miközben az Isten számához kapcsolódó anyagokat kerestem az interneten, találtam egy másik érdekes fogalmat, amely nem annyira ismert szerintem. Ezt a részt [5] alapján írom. Fel lehet tenni a kérdést, hogy létezik-e olyan forgatássorozat, amelyet ismételgetve a kocka előbb-utóbb a kirakott helyzetbe kerül (nem feltétlenül a forgatássorozat végén!), bármilyen helyzetből is indultunk. Tegyük fel, hogy léteznek ilyen forgatássorozatok. Egy ilyen forgatássorozatot az Ördög algoritmusának (*Devil's algorithm*) nevezünk. Az Ördög száma (*Devil's number*) pedig az ilyen algoritmusok hosszának minimuma. Ezt a kérdést többnyire a negyed-forgatás metrikában szokták vizsgálni, én legalábbis nem találtam a másik metrikát használó, erre vonatkozó anyagot.

A kérdés egy kicsit általánosabb verziója az lenne, hogy a Γ_{Rubik} gráfban van-e olyan út, amely minden csúcsot legalább egyszer érint. Ezt „élesítve" megkérdezhetjük, hogy van-e benne Hamilton-út vagy kör (az út minden csúcsot pontosan egyszer érint, a kör szintén, kivéve a kezdőpontot, amely egyben a végpont is). Ez pedig kapcsolódik a Lovász-sejtés egy változatához, amely szerint minden véges, összefüggő Cayley-gráf tartalmaz Hamilton-kört ([6] alapján). A [7]-es honlapon szerepel egy leírás arról, hogy találtak Hamilton-kört Γ_{Rubik}-ban a negyed-forgatás metrika szerint (ez persze a félforgatás metrika szerint is Hamilton-kör). Mindenesetre ha van egy listánk a forgatásokról, amelyekkel minden csúcsot legalább egyszer érintünk, és szeretnénk memorizálni a listát, ez akkor a legkönnyebb, ha a lista periodikus, és a periódusa a lehető legrövidebb. Ezt fejezi ki az Ördög száma. (Korábban persze azt írtam, hogy a kirakott helyzetet kell kihozni, de azon kívül, hogy általában ennek a kirakása a cél, a kirakott helyzetet semmi sem különbözteti meg a többitől.) [2, 102. o.] alapján[6] a Rubik-kocka csoportjában az elemek rendjének maximuma 1260 (tehát van olyan elem, amelynek 1260 a rendje, de ennél nagyobb rendű nincs). Világos, hogy bármely Ördög algoritmusának legalább

$$\frac{3^8 \cdot 2^{12} \cdot 8! \cdot 11!}{1260} = 34\ 326\ 986\ 725\ 785\ 600$$

hosszú szónak kell lennie, mivel ha a rendje r, akkor nincs értelme r-nél többször megismételni, tehát az Ördög száma legalább ennyi kell legyen.

Végül még egy érdekes játékot szeretnék az Olvasó figyelmébe ajánlani, a superflip-játékot (ezt a részt [2, 69. o.] alapján írtam, de nem egészen ugyan-

[6]bár ez is csak hivatkozás [3]-ra

úgy). Ez egy kétszemélyes játék, amelyben a kirakott kockát kell eljuttatni a superflip pozícióba, vagyis amikor minden alkocka a helyén van, a sarokkockák orientációja is „stimmel", az élkockák orientációja viszont mind „rossz" (tehát az (12) permutáció hat minden élkocka felírásán). A játék elején fixálni kell a kocka térbeli helyzetét, az origó legyen a kocka egyik sarka, a három koordinátatengely essen egybe az ebből a sarokból induló egy-egy éllel. Válasszunk ki egy koordinátatengelyt, amelynek külön szerepe lesz a játék során. A következő szabályok szerint kell (lehet) játszani:

1. Pénzfeldobás dönti el, hogy ki kezd.

2. A játékosok felváltva forgatják a Rubik-kockát, egy-egy engedélyezett forgatást tehetnek.

3. Az engedélyezett forgatások a saroklapkákat önmagukba viszik, az élkockákat helyben hagyják, és páros számú élkockának változtatják meg az orientációját.

4. Azon élkockák közül, amelyeknek a kirakott pozícióbeli az orientációja, meg kell keresni azt, amely a legközelebb van az origóhoz (ha több ilyen is van, akkor azt, amelyik a legközelebb van a kiválasztott tengelyhez), és ennek mindenképp meg kell változtatni az orientációját az aktuális forgatással.

5. Az nyer, aki kirakja a superflip helyzetet.

Ezenkívül még meg kell adni, hogy hány/milyen élkocka orientációját változtathatja meg egy engedélyezett forgatás. Van olyan változat, amelyben minden körben két élkocka orientációját kell megváltoztatni, és ezeknek egy lapon kell lenniük, vagy szintén két élkocka orientációját kell megváltoztatni, de pont hogy külön lapokon lévőkét, illetve van olyan is, amelyben 2, 4 vagy 6 élkocka orientációját kell megváltoztatni.

Persze ahhoz, hogy a játékot gördülékenyen lehessen játszani, a játékosoknak ismerniük kell a megfelelő forgatásokat, amelyek csak az élkockákat forgatják. Ennek kapcsán elgondolkodtam, hogy milyen keretek között lehetne ezt a játékot akár versenyszinten űzni. 2003 óta minden második évben megrendezik a Rubik-kocka világbajnokságot (az első 1982-ben volt Budapesten), ahol különböző versenyszámokban mérhetik össze tudásukat a jelentkezők (ld. [8]). Idén Brazíliában, Sao Pauloban lesz a rendezvény, július 17-19

között. A legtöbb versenyszámban természetesen a gyorsaságot mérik különböző (3×3-as, 4×4-es stb.) Rubik-kockák és hasonló játékok esetében, (van sima gyorsasági verseny, félkezes kirakás, olyan versenyszám, ahol vakon kell kirakni a kockát, de még olyan is, ahol lábbal!) de van például olyan is, ahol a Rubik-kocka adott helyzetéhez kell megtalálni a lehető legrövidebb kirakási módszert, természetesen ezt is időre (ld. [9]). Úgy gondolom, a versenyzők nagy része érdekesnek találná a superflip-játékot. Mivel véges sok lehetséges állapota van a játéknak, az egyik játékosnak biztos van nyerő stratégiája. Ezt úgy lehet kiküszöbölni, hogy két fordulót játszanak: az elsőben a kirakott kockát el kell juttatni a superflip pozícióba, a másodikban pedig vissza, és a második fordulót nem az kezdi, aki az elsőt. Ezenkívül még fontos, hogy a játék ne kerülhessen vissza ugyanabba az állapotba legfeljebb véges sokszor, ezt például meg lehet valósítani úgy, hogy az elforgatott élkockák száma minden lépésben nőjön, véges számú kivételtől eltekintve (például mindkét játékosnak 3 lehetősége van úgy forgatni, hogy nem nő az elforgatott élkockák száma). Ugyanakkor a két forduló során mérik az egyes játékosok idejét, és döntetlen esetén az nyer, akinek összességében kevesebb időre volt szüksége (vagy a vesztett fordulóban kevesebb időre volt szüksége, ez már megegyezés kérdése). Ezenkívül nemcsak ketten játszhatják a játékot, akár két csapat is.

Irodalomjegyzék

[1] Kiss Emil. *Bevezetés az algebrába.* Typotex Kiadó, Budapest, 2007. 1, 2, 3, 4, 9, 12, 61

[2] W. D. Joyner. *Mathematics of the Rubik's cube.* `http://www.permutationpuzzles.org/rubik/webnotes/rubik.pdf` (letöltés dátuma: 2015. 04. 27.). 9, 32, 33, 38, 58, 61

[3] D. Singmaster. *Notes on Rubik's magic cube.* Enslow Publishers, New Jersey, 1981. 33, 58, 61

[4] Tomas Rokicki. `http://www.cube20.org/` (letöltés dátuma: 2015. 05. 09.). 56, 57, 61

[5] `http://anttila.ca/michael/devilsalgorithm/` (letöltés dátuma: 2015. 05.30.). 58, 61

[6] `http://hu.wikipedia.org/wiki/Lovász-sejtés` (letöltés dátuma: 2015. 05.30.). 58, 61

[7] `http://bruce.cubing.net/ham333/rubikhamiltonexplanation.html` (letöltés dátuma: 2015. 05.30.). 58, 61

[8] `http://hu.wikipedia.org/wiki/Rubik-kocka-világbajnokságok_listája` (letöltés dátuma: 2015. 05.30.). 59, 61

[9] `https://www.worldcubeassociation.org/` (letöltés dátuma: 2015. 05.30.). 60, 61