Középiskolai versenyfeladatok csoportelméleti háttere

Szakdolgozat

Írta: Szegedi Gábor

Matematika BSc, tanári szakirány

Témavezető:

Károlyi Gyula, egyetemi tanár
Algebra és Számelmélet Tanszék
Eötvös Loránd Tudományegyetem, Természettudományi Kar

Eötvös Loránd Tudományegyetem
Természettudományi Kar
2016

Tartalomjegyzék

Ábrák jegyzéke

Bevezetés

Matematika–fizika szakos tanárnak készülök, ezért igyekeztem olyan témát választani, ami valamilyen módon kapcsolatot teremt a középiskolás és az egyetemi matematika között. Szakdolgozatomban olyan, többségében igen nehéz versenyfeladatok szerepelnek, amelyeket csoportelméleti törvényszerűségek, észrevételek ihlettek. Ennek megfelelően fő célkitűzésem az ihlet forrásának minél alaposabb feltárása volt. Ez legizgalmasabban az utolsó példában nyilvánult meg, ahol egészen a feladat alapjául szolgáló kutatási területig, ezzel együtt egy máig bizonyítatlan sejtésig sikerült eljutnom.

Munkám során egyfelől összegyűlt néhány érdekes csoportelméleti alkalmazás, másfelől nagyban sikerült általánosítanom a tárgyalt feladatok megoldását. Mindezeknél azonban fontosabbnak gondolom azt a tartalmat, hogy az itt szereplő feladatok mindegyike felsőfokú ismeretek révén született, és gyakran mélyebb megértésük is csak azok segítségével lehetséges. Ezért külön-külön is választ adnak arra a klasszikus, gyakran hallható kérdésre, hogy miért érdemes egy általános- vagy középiskolai tanárnak felsőfokú matematikát tanulnia.

De egyszerűen úgy is tekinthetünk a dolgozatra, mint egy sokszínű csoportelméleti búvárkodásra, amely során a legkülönfélébb problémákkal találkozunk: a tárgyalt feladatok többek között a számelmélet, a geometria és az analízis területéről származnak. Talán Károlyi Gyula tanár úr is erre a búvárkodásra gondolt, amikor a téma kitűzésekor rövid ismertetőjét azzal zárta: „csoportelmélet nem marad szárazon".

A dolgozat felépítése

A szakdolgozat három nagyobb egységre tagolódik. Az elsőben középiskolai megoldásokon keresztül ismertetem a feladatokat. Ezek kidolgozása során gyakran merítettem a www.komal.hu weblapon olvasható megoldásokból. A leírásokban nem pusztán rövid megoldások felsorolása volt a célom, ehelyett igyekeztem minél részletesebben megmutatni a megoldásokhoz vezető utat. Ennek ellenére gyakran találkozunk „kalapból nyuszi" típusú gondolatokkal.

A második részben a szakdolgozathoz felhasznált, az alapképzés tananyagán túlmutató ismereteket foglaltam össze. Itt külön kiemelném a $\mathbb{Z}_p^\times$ ciklikusságára vonatkozó bizonyítást, amelyben Károlyi tanár úr javaslatára $\mathbb{Z}_p^\times$ elemeit a $(p-1)$-edik egységgyökökkel állítottam párhuzamba.

Ezt követi a dolgozat utolsó, egyben legfontosabb része. A feladatok csoportelméleti hátterének bemutatásán keresztül részben igyekeztem eloszlatni a ködöt a korábban „isteni szikrát" igénylő ötletekről, emellett a problémák minél általánosabb szinten történő vizsgálatára is törekedtem. Egy-két helyen úgy éreztem, hogy az eredmény a feladat keretein kívül is hasznos lehet. Ezek tartalmát „Állítások"-ba foglalva külön kiemeltem.

Röviden a feladatok csoportelméleti hátteréről

Az első feladatban egy h függvényről kell megmutatnunk, hogy nem áll elő adott f és g függvények kompozíciójaként. Ezt kétféleképpen is belátjuk. Kiderül, hogy f és g kompozíciói egy D_3-mal izomorf csoportot alkotnak. Emiatt az nem tartalmazhatja a végtelen rendű h-t. Másfelől azt is tudjuk, hogy a csoportelemek a csoport pályáit önmagukra képezik, ez h-ra azonban nem teljesül.

A másodikban az a kérdés, hogy adott lépések mellett eljuthatunk-e egy konstrukció A állapotából annak B állapotába. Meglepő módon kiderül, hogy a konstrukcióhoz éppen D_3 konjugáltosztályai szolgáltatnak teljes invariáns rendszert.

A harmadik feladatban megmutatjuk, hogy a térparkettázásban hogyan lehet segítségünkre a homomorfizmustétel, illetve egy megfelelő Abel-csoport.

A negyedikben ötödrendű törtlineáris leképezést kell konstruálnunk. Ehhez azt használjuk fel, hogy a törtlineáris leképezések csoportja homomorf képe a 2×2-es invertálható mátrixok csoportjának, amelyben könnyen találhatunk megfelelő rendű elemet.

Végül egy pozitív egészeken értelmezett, bonyolult színezési problémával foglalkozunk. Az első megoldásban azt $\mathbb{Z}_p^\times$ ciklikusságára, a másodikban pedig a $\pi(n)$-dimenziós tér rácspontjainak parkettázására vezetjük vissza.

Technikai tudnivalók

A dolgozatban – a hagyományostól eltérő módon – a függvénykompozíciót balról jobbra értelmezem, és többnyire a $\circ$-jelet elhagyva, egymás mellé írással jelölöm. Tehát $fg(x) = (f \circ g)(x) = g(f(x))$. Ez alól egyedül a Törtlineáris leképezések csoportja c. részben teszek kivételt, hogy ne kelljen megváltoztatnom a mátrixszorzás megszokott irányát. Itt tehát $(f \circ g)(x) = f(g(x))$.

(Ennek a furcsaságnak az az oka, hogy eredetileg az Algebra 3 kurzusnak megfelelően a kitevős (pl. x^f) írásmódot alkalmaztam, hosszú távon azonban a hagyományos jelölés (pl. $f(x)$) szerencsésebbnek bizonyult. Felmerült ezzel együtt a sorrend visszafordítása is, ehhez viszont számos korábbi eredményt kellett volna újraszámolni. Mivel a dolgozat keretein belül ebből az „összvér" jelölésből különösebb nehézség nem származott, erre végül nem került sor.)

Köszönetnyilvánítás

Szeretnék nagy-nagy köszönetet mondani témavezetőmnek, Károlyi Gyula tanár úrnak a téma kijelöléséért, a feladatok összegyűjtéséért, a rengeteg hasznos tanácsért és útmutatásért, nem utolsó sorban pedig végtelen türelméért. Köszönöm továbbá Pach Péter Pál tanár úrnak, hogy igen alaposan beavatott kutatási eredményeibe, emellett bármikor azonnal válaszolt felmerülő kérdéseimre. Nélkülük ez a szakdolgozat nem jöhetett volna létre.

1. fejezet

A feladatok megoldása középiskolai eszközökkel

1.1. Függvények kompozíciója

(B. 3851.) Tekintsük az $f : x \to \frac{1}{x}$, $g : x \to 1 - \frac{1}{x}$ függvények véges sok példányának kompozíciójaként előállítható függvényeket; például

$$fgf : x \to \frac{1}{x} \to 1 - \frac{1}{\frac{1}{x}} = 1 - x \to \frac{1}{1-x}.$$

Előállítható-e így az $x \to x+1$ függvény (az értelmezési tartományából esetleg véges sok helyet elhagyva)? [7]

1. megoldás: Nevezzük az a és b függvényeket *„lényegében egyenlőnek”*, ha néhány (véges sok) ponttól eltekintve értelmezve vannak a teljes számegyenesen, továbbá értelmezési tartományuk metszetén egyenlő értékeket vesznek fel. Jelölje ezt $a \approx b$.[1]

Kezdjünk el kísérletezni, milyen függvényeket tudunk előállítani f és g kompozíciójaként. Először gyűjtsük össze a kéttényezős függvényeket:

$$f^2 : x \to \frac{1}{x} \to x, \quad fg : x \to \frac{1}{x} \to 1 - x, \quad g^2 : x \to 1 - \frac{1}{x} \to \frac{1}{1-x}, \quad gf : x \to 1 - \frac{1}{x} \to \frac{x}{x-1},$$

majd nézzük meg a háromtényezősöket. Elméletileg nyolc eset lehetséges, $f^2 \approx \mathrm{id}$ miatt azonban csak öt kompozíció esetében számíthatunk a korábbiaktól *lényegében különböző* függvényre:

$$g^2 f : x \to \frac{1}{1-x} \to 1 - x, \quad g^3 : x \to \frac{1}{1-x} \to x, \quad fgf : x \to 1 - x \to \frac{1}{1-x},$$

$$fg^2 : x \to 1 - x \to \frac{x}{x-1}, \quad gfg : x \to \frac{x}{x-1} \to \frac{1}{x}.$$

Vegyük észre, hogy

$$g^2 f \approx fg, \quad g^3 \approx f^2 \approx \mathrm{id}, \quad fgf \approx g^2, \quad fg^2 \approx gf, \quad gfg \approx f.$$

Azaz egyetlen új esetet sem kaptunk, minden háromtényezős kompozíció *lényegében egyenlő* valamelyik korábbival. Ebből következően pedig minden tetszőlegesen hosszú kompozíció is, hiszen az első három tényezőt (a függvénykompozíció asszociativitása miatt) mindig kicserélhetjük egy vagy

[1] Ez nyilván ekvivalenciareláció.

két függvényre, így véges sok lépésben eljuthatunk az első hat eset (f, g, f^2, fg, g^2, gf) valamelyikéhez.

Ha $h : x \to x + 1$ előállítható lenne, akkor $h^2 : x \to x + 2$, $h^3 : x \to x + 3$ stb. is. Ez azonban végtelen sok *lényegében különböző* függvény, ezért h nem állítható elő.

2. megoldás: Tekintsük a $\left\{-1, \frac{1}{2}, 2\right\}$ halmazt. Ezt f és g egyaránt önmagára képezi, így ezek összes kompozíciói is. Mivel h-ra ez nem teljesül, ezért az nem is állítható elő.

Ezt az igen frappáns megoldást sajnos azonban elrontja, hogy h értelmezési tartományából néhány elem elhagyható, akár éppen ez a három is.

A probléma megoldásához vegyük most az $\left\{a, 1 - \frac{1}{a}, \frac{1}{1-a}, \frac{1}{a}, \frac{a}{a-1}, 1 - a\right\}$ halmazt, ahol $a \neq 0, 1$. Erre is teljesül, hogy mind f, mind g, mind ezek kompozíciói önmagára képezik. Mivel h értelmezési tartományából csak véges sok elem hagyható el, mindig lesz olyan a szám, melyre h értelmezési tartománya tartalmazni fogja ezt a halmazt és nem képezi önmagára.

1.2. Játék színes pontokkal

Egy körvonal mentén néhány kék és piros pontot helyeztünk el. Ezekkel az alábbi műveleteket végezhetjük:

(a) valahova beillesztünk egy új piros pontot, és a két szomszédját ellentétes színűre változtatjuk,

(b) ha legalább három pont van, és ezek közül legalább az egyik piros, akkor egy piros pontot törlünk, a két szomszédját pedig ellentétes színűre változtatjuk.

Kezdetben két pont van a kör kerületén, mindkettő kék. Elérhetjük-e a lépések többszöri alkalmazásával, hogy újra két pontunk legyen, de azok pirosak legyenek? [12]

Némi próbálkozás után arra juthatunk, hogy a két kék pontból valószínűleg nem lehet eljutni a két piroshoz. Ennek bizonyítására jó lenne találni valamiféle invariánst, ami a két állapotban különböző.

Foglaljuk össze a lehetséges lépéseket:

1. KK $\leftrightarrow$ PPP
2. KP $\leftrightarrow$ PPK
3. PK $\leftrightarrow$ KPP
4. PP $\leftrightarrow$ KPK

Vegyük észre, hogy ezek során a kék pontok száma mindig 0-val vagy ± 2-vel változik. Mivel két darab kékről indulunk, ezek száma mindig páros marad, így páros sok részre osztják a kört. Az invariáns megtalálásához az adhat ihletet, ha megvizsgáljuk a kék osztópontok két oldalán a piros pontok számának változását.

Osszák a kék pontok n ívre a kört, ezekbe jusson pozitív körüljárás szerint rendre a_1, $a_2, \ldots,$ a_n darab piros. Képezzük az alábbi összeget:

$$S := \pm a_1 \mp a_2 \pm a_3 \mp \cdots \mp a_n \pmod 3.$$

Ennek előjele persze az első ív megválasztásán múlik, így S az objektum egy adott állapotához 0-t vagy ± 1-et rendel.

Mutassuk meg, hogy egy piros pont hozzáadása vagy elvétele – rögzített előjelezés esetén – az összeg ± 3-mal való változását eredményezi, azaz S invariáns a lépések során! A táblázatban az alsó indexek az ívek sorszámát jelölik.

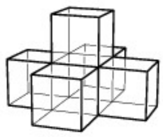
Lépés	Összeg változása
${}_i\mathrm{K}_{i+1}\mathrm{K}_{i+2} \leftrightarrow {}_i\mathrm{PPP}_{i+2}$	$\pm a_i \mp 0 \pm a_{i+2} \leftrightarrow \pm a_i + 3 \pm a_{i+2}$
${}_i\mathrm{KP}_{i+1} \leftrightarrow {}_i\mathrm{PPK}_{i+1}$	$\pm a_i \mp a_{i+1} \leftrightarrow \pm(a_i + 2) \mp (a_{i+1} - 1) = \pm a_i \mp a_{i+1} \pm 3$
${}_i\mathrm{PK}_{i+1} \leftrightarrow {}_i\mathrm{KPP}_{i+1}$	$\pm a_i \mp a_{i+1} \leftrightarrow \pm(a_i - 1) \mp (a_{i+1} + 2) = \pm a_i \mp a_{i+1} \mp 3$
${}_i\mathrm{PP}_{i+2} \leftrightarrow {}_i\mathrm{KP}_{i+1}\mathrm{K}_{i+2}$	$\pm a_i \pm a_{i+2} \leftrightarrow \pm(a_i - 1) \mp 1 \pm (a_{i+2} - 1) = \pm a_i \pm a_{i+2} \mp 3$

1.1. táblázat.

Tehát S valóban invariáns a lépésekre. Mivel $S(KK) = 0$, viszont $S(PP) = \pm 1$, ezért az egyik állapotból nem lehet eljutni a másikba.

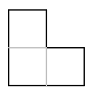
1.3. Parkettázás

(B. 4190.) Hat egybevágó kockából az ábrán látható testet ragasztottuk össze. Kitölthető-e a tér hézagmentesen és átfedések nélkül ennek a testnek egybevágó példányaival? [8]



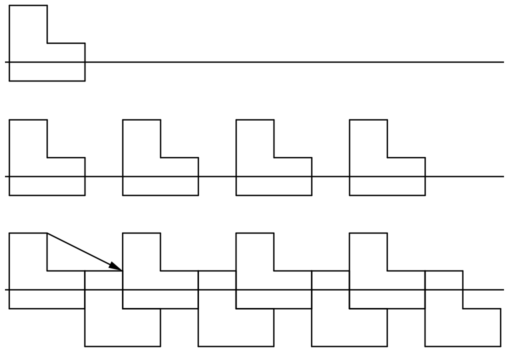
Az átfedés- és hézagmentes kitöltést röviden parkettázásnak is szokás nevezni. Ha a kitöltéshez csak eltolást alkalmazhatunk, akkor E-parkettázásról beszélünk. [3]

1. megoldás: Oldjunk meg először egy egyszerűbb problémát: kiparkettázható-e a sík az alábbi, három egybevágó négyzetből álló síkidommal, ha csak eltolást alkalmazhatunk?



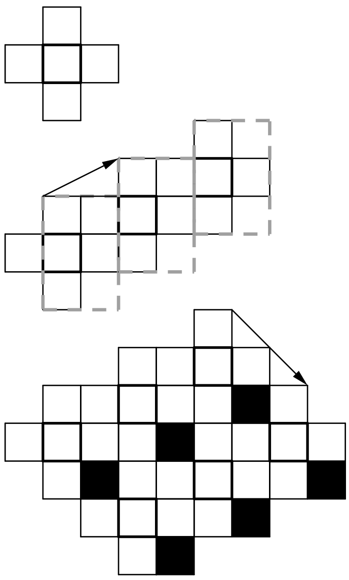
Helyezzük el ezt valahol a síkon, majd illesszünk egy egyenest az alsó két négyzetére az 1.1. ábrán látható módon. Természetesen adódik a gondolat, hogy egy egyenletes parkettázás esetében a síkidom eltolt példányainak alsó négyzetei az egyenes „kétharmad részét” töltik ki. Ezt úgy valósíthatjuk meg, ha kihagyunk ezek között egy-egy négyzetet. Látható, hogy ekkor a szomszédos lyukak éppen olyan messze vannak egymástól, mint a felső sorban lévő négyzetek, ezért ha erre az egy egyenesbe eső síkidom-sokaságra a(z egyik) megfelelő eltolást alkalmazzuk, akkor az egész egyenes kitölthető. Ily módon egyenesről-egyenesre a teljes síkot ki tudjuk parkettázni.

Térjünk vissza az eredeti feladathoz. Helyezzük el a térben ezt a testet, majd illeszünk egy síkot az alsó sorában lévő kockákra. A korábbiak alapján arra számítunk, hogy az eltolt példányok „alsó emeletei” a sík „öthatod részét” töltik ki. Nézzünk rá fölülről erre a síkra, és rajzoljunk egy kétszer hármas téglalapot a test köré úgy, hogy az egyik ága kilógjon belőle (ld. 1.2. ábra). Ekkor ennek négy négyzetét lefedtük, kettő üresen maradt. Most toljuk el a testet (a köré rajzolt téglalappal együtt) úgy, hogy a kilógó kocka eltoltja az egyik üres négyzetbe kerüljön, majd vegyük



1.1. ábra. Egyszerű síkbeli parkettázás

ezen eltolás többszöröseit. Ezután az összes eddigi példányt toljuk el úgy, hogy a téglalapok üres négyzetei továbbra is üresek maradjanak, a sík többi része viszont legyen kitöltve. Az 1.2. ábrán látható, hogy felülnézetben a lyukrendszer éppen a felső kockák rendszerének egy eltoltja, ezért az eddigi kitöltést el tudjuk tolni egy emelettel lejjebb úgy, hogy a felső kockák pont a lyukakba kerüljenek. Ennek többszöri ismétlésével az egész tér kiparkettázható.



1.2. ábra. Nehezebb térbeli parkettázás

2. megoldás: A kockák élei legyenek egységnyi hosszúságúak és helyezzük el ezt a testet egy térbeli derékszögű koordinátarendszerben úgy, hogy a kockák középpontjai az alábbi koordinátájú pontok legyenek:

$$A_0(0,0,0); A_1(1,0,0); A_2(0,1,0); A_3(0,0,1); A_4(0,-1,0); A_5(-1,0,0).$$

Jelöljük ezek halmazát A-val és nevezzük ezt őshalmaznak, elemeit pedig őspontoknak. A továbbiakban a kockákat azonosítsuk azok középpontjával, így a feladat a rácspontok lefedésére egyszerűsödik (hiszen ha a rácspontokat lefedtük, akkor a hozzájuk, mint középpontokhoz tartozó kockák nyilván átfedés- és hézagmentesen kitöltik a teret).

Tekintsük az alábbi függvényt:

$$f: \quad \mathbb{Z}^3 \to \mathbb{Z}_6, \quad (x,y,z) \to x+2y+3z \pmod 6.$$

Azokat a P pontokat (ill. vektorokat), amelyekre $f(P)=i$ (i=0,...,5), nevezzük i-maradékú pontoknak (ill. vektoroknak). Vegyük az A halmaznak a 0-maradékú $\underline{v}$ vektorokkal való eltoltjait:

$$A_{\underline{v}} = \{A_0+\underline{v}, A_1+\underline{v}, A_2+\underline{v}, A_3+\underline{v}, A_4+\underline{v}, A_5+\underline{v}\}.$$

A továbbiakban belátjuk, hogy az így kapott halmazsokasággal éppen a keresett „parkettázást" adtuk meg.

Világos, hogy ezek az őshalmazzal mind egybevágó ponthalmazok. Az átfedés- és hézagmentességhez azt kell megmutatnunk, hogy a tér minden pontját ezek közül pontosan egy tartalmazza.

Az őspontok mindegyikére teljesül, hogy $f(A_i)=i^2$. Most vizsgáljuk meg ezek eltoltjait. $A_i(x,y,z)$, $\underline{v}(x',y',z')$ esetén $f(A_i+\underline{v}) = x+x'+2(y+y')+3(z+z') = (x+2y+3z)+(x'+2y'+3z') \equiv i+0=i$. Tehát az i-maradékú őspontok képe is i-maradékú. Ezek szerint egy tetszőleges i-maradékú $P(x'',y'',z'')$ ponthoz tartozó $\underline{v}$-ra egyetlen jelöltünk van: $\overrightarrow{A_iP}$. Ennek a koordinátái nyilván egészek, emellett a 0-maradékúság is teljesül: $f(\overrightarrow{A_iP}) = f(P-A_i) = x''-x+2(y''-y)+3(z''-z) = (x''+2y''+3z'')-(x+2y+3z) \equiv i-i=0$. Ily módon minden P pontnak egyértelműen megfeleltettünk egy $\underline{v}$ vektort, ezzel együtt pedig a P-t tartalmazó $A_{\underline{v}}$-t.

Az őshalmaz 0-maradékú vektorokkol való eltoltjaival tehát tényleg „kiparkettáztuk" a teret.

1.4. Törtlineáris leképezések

(B. 4650.) Létezik-e olyan $f(x)=\frac{ax+b}{cx+d}$ alakú függvény, melyre alkalmas páronként különböző $x_1,\dots,x_5$ valós számokkal

$$f(x_1)=x_2, \quad f(x_2)=x_3, \quad f(x_3)=x_4, \quad f(x_4)=x_5, \quad f(x_5)=x_1$$

teljesül? [11]

Tehát $x_1 \xrightarrow{f} x_2 \xrightarrow{f} x_3 \xrightarrow{f} x_4 \xrightarrow{f} x_5 \xrightarrow{f} x_1$. A megoldás kulcsgondolata, hogy jó lenne találni egy olyan p periódusú g függvényt, amelyre f külső függvényként oly módon hat, hogy $f(g(x)) = g(x+\frac{p}{5})$. Ekkor ugyanis $f^2(g(x)) = g(x+\frac{2p}{5})$, hasonlóan $f^5(g(x)) = g(x+\frac{5p}{5}) = g(x+p) = g(x)$.

Kézenfekvő gondolat, hogy valamiféle szögfüggvénnyel lenne érdemes próbálkoznunk. Az ezekre vonatkozó összefüggéseket böngészve találhatunk is alkalmasat, ilyen például a $\mathrm{tg}(x)$. Ennek periódusa $p=180°$, tehát $\frac{p}{5}=36°$. A megfelelő addíciós képlet a külső függvényt is a kezünkbe adja:

$$\mathrm{tg}(x+36°) = \frac{\mathrm{tg}(x)+\mathrm{tg}(36°)}{-\mathrm{tg}(36°)\,\mathrm{tg}(x)+1},$$

azaz a jelöltjeink

$$g(x)=\mathrm{tg}(x), \quad f(x) = \frac{x+\mathrm{tg}(36°)}{-\mathrm{tg}(36°)x+1},$$

hiszen ekkor $f(\mathrm{tg}(x)) = \mathrm{tg}(x+36°)$. (A feladat paramétereit használva $a=d=1$, $b=\mathrm{tg}(36°)$, $c=-\mathrm{tg}(36°)$.)

Legyen $x_1=\mathrm{tg}(0°)$. Ekkor

$$\mathrm{tg}(0°) \xrightarrow{f} \mathrm{tg}(36°) \xrightarrow{f} \mathrm{tg}(72°) \xrightarrow{f} \mathrm{tg}(108°) \xrightarrow{f} \mathrm{tg}(144°) \xrightarrow{f} \mathrm{tg}(180°) = \mathrm{tg}(0°).$$

[2] Persze nekünk az is elegendő lenne, ha az értékek különbözőek lennének. Ekkor azonban az indexeket érdemes lenne ezekkel utólag egyenlővé tenni.

Mivel $\mathrm{tg}(x)$ egy periódusára nézve bijektív és ezek a szögek mind $\mathrm{tg}(x)$ ugyanazon periódusában szerepelnek, valóban különböző $x_1, \ldots, x_5$ értékeket kaptunk. Tehát létezik ilyen függvény.

Felmerülhet bennünk a kérdés: f^5 vajon maga az identitás vagy csak van néhány fixpontja, amelyek közül $\mathrm{tg}(0°)$ az egyik? A válasz az, hogy f^5 „majdnem az identitás", ugyanis a fenti gondolatmenetet tetszőleges $\mathrm{tg}(\alpha)$-ra megismételhetjük, arra azonban ügyelnünk kell, hogy a sorozatban sem $\mathrm{tg}(90°)$, sem $\mathrm{tg}(270°)$ nem jelenhet meg. Tehát f^5 értelmezési tartományából ki kell zárnunk a következőket: $\mathrm{tg}(-54°)$, $\mathrm{tg}(-18°)$, $\mathrm{tg}(18°)$, $\mathrm{tg}(54°)$, $\mathrm{tg}(126°)$, $\mathrm{tg}(162°)$, $\mathrm{tg}(198°)$, $\mathrm{tg}(234°)$. (Valójában ez persze csak négy különböző számot jelent.) Ezek kivételével azonban minden valós szám fixpont lesz, tehát az első feladatban bevezetett fogalommal élve: f^5 és id lényegében egyenlőek.

1.5. Számok színezése

(B. 4265.) Színezzük ki a pozitív egész számokat 7 színnel úgy, hogy minden a pozitív egész számra az $\{a, 2a, 3a, 4a, 5a, 6a, 7a\}$ halmaz elemeinek színe páronként különböző legyen. [9]

Tehát keressük azt az $f : \mathbb{Z}^+ \to \mathbb{Z}_7$ függvényt, ami az $\{a, 2a, 3a, 4a, 5a, 6a, 7a\}$ alakú halmazok elemeihez különböző értékeket rendel ($a \in \mathbb{Z}^+$). Az alábbi megoldás azon az észrevételen alapul, hogy egy ilyen halmazban a 2, 3, 5, 7 prímtényezők száma páronként különböző.

A számelmélet alaptétele szerint minden $a \in \mathbb{Z}^+$ egyértelműen felírható $a = 2^\alpha 3^\beta 5^\gamma 7^\delta q$ alakban, ahol $\alpha, \beta, \gamma, \delta$ nemnegatív egészek, q pedig a többi prímhatvány szorzata (esetleg 1). Vizsgáljuk meg az α, β, γ és δ kitevők változását a halmazban:

a	α	β	γ	δ
$2a$	$\alpha+1$	β	γ	δ
$3a$	α	$\beta+1$	γ	δ
$4a$	$\alpha+2$	β	γ	δ
$5a$	α	β	$\gamma+1$	δ
$6a$	$\alpha+1$	$\beta+1$	γ	δ
$7a$	α	β	γ	$\delta+1$

1.2. táblázat.

A fenti f függvényt a legegyszerűbb $f = k\alpha + l\beta + m\gamma + n\delta \pmod 7$ alakban keresni, ahol $k, l, m, n \in \mathbb{Z}^+$. Tehát a kitevők megfelelő súlyozásával szeretnénk elérni, hogy a szóban forgó prímtényezők darabszámának különbsége különböző függvényértékeket eredményezzen. Legyen $f(a) = s$, ekkor egy ilyen függvény az egyes halmazelemekhez a következő értékeket rendeli:

a	a	$2a$	$3a$	$4a$	$5a$	$6a$	$7a$
$f(a)$	s	$s+k$	$s+l$	$s+2k$	$s+m$	$s+k+l$	$s+n$
Például	s	$s+1$	$s+3$	$s+2$	$s+5$	$s+4$	$s+6$

1.3. táblázat.

Innen már könnyen találhatunk megfelelő súlyozást, ami minden elemhez különböző értéket rendel. Több jó megoldás is van, a táblázat alsó sorában megadtuk az egyiket. Tehát egy megfelelő színezés például a következő:

$$f(x = 2^\alpha 3^\beta 5^\gamma 7^\delta q) = \alpha + 3\beta + 5\gamma + 6\delta \pmod 7.$$

2. fejezet

Elméleti áttekintés

2.1. Centralizátor, konjugáltosztályok

Ebben a részben a konjugálással ismerkedünk. Ennek során konjugáltosztályokat fedezünk fel, majd ezek elemszámának vizsgálata közben eljutunk a centralizátor fogalmához. Végül felismerjük, hogy a konjugáltosztály elemszáma osztója a csoport rendjének.

2.1.1. Definíció. *Legyen G csoport. Azt mondjuk, hogy $b \in G$ konjugáltja $a \in G$-nek, ha létezik olyan $g \in G$, melyre $b = g^{-1}ag$. Jelölés: $b \sim a$.*

A definícióban a g-vel való konjugálás azt jelenti, hogy jobbról szorzunk g-vel, balról pedig annak inverzével. Ennek a sorrendnek azonban nincs jelentősége, hiszen ha létezik megfelelő g csoportelem, akkor a $h = g^{-1}$ választással a $b = hah^{-1}$ is teljesül.

Szorozzuk meg ezt a kifejezést balról h inverzével, jobbról h-val. Így azt kapjuk, hogy $h^{-1}bh = a$, azaz $a \sim b$, tehát ez egy szimmetrikus reláció. Reflexív is, ennek bizonyítására megfelelő pl. az egységelem, de maga az a is: $a = 1^{-1}a1$, vagy $a = a^{-1}aa$. Sőt, a tranzitivitás is teljesül. Legyen $b \sim a$ és $c \sim b$. Ekkor létezik olyan g és h, melyekre $b = g^{-1}ag$, $c = h^{-1}bh$, így $c = h^{-1}g^{-1}agh$. A $h^{-1}g^{-1} = (gh)^{-1}$ helyettesítést elvégezve $c = (gh)^{-1}a(gh)$, tehát $c \sim a$.

2.1.2. Definíció. *A fenti ekvivalenciareláció osztályait konjugáltosztályoknak nevezzük, az a elemet tartalmazó osztály jele: $K(a)$.*

Felmerülhet bennünk, vajon hány elemet tartalmaz egy konjugáltosztály. $|K(a)|$ elemszámának megállapításához konjugáljuk a-t G minden elemével és vizsgáljuk meg, hogy mikor kapjuk ugyanazt:

$$g^{-1}ag = h^{-1}ah$$
$$hg^{-1}a = ahg^{-1}.$$

Tehát pontosan akkor, ha a és hg^{-1} felcserélhető.

2.1.3. Definíció. *Egy G csoportban az a elemmel felcserélhető elemek halmazát a centralizátorának nevezzük. Jele: $C(a)$.*

2.1.4. Állítás. $C(a)$ *részcsoport G-ben.*

Bizonyítás.

(i) Az 1 tartalmazása nyilvánvaló.

(ii) Zárt a szorzásra: $g, h \in C(a)$ esetén $ga = ag$, $ha = ah$. Szorozzuk előbbit jobbról h-val: $gah = agh$. Utóbbi alapján $(gh)a = a(gh)$. Tehát $gh \in C(a)$.

(iii) Zárt az inverzképzésre: $g \in C(a)$ esetén a $ga = ag$. Ezt jobbról, majd balról g inverzével szorozva adódik, hogy $ag^{-1} = g^{-1}a$, tehát $g^{-1} \in C(a)$.

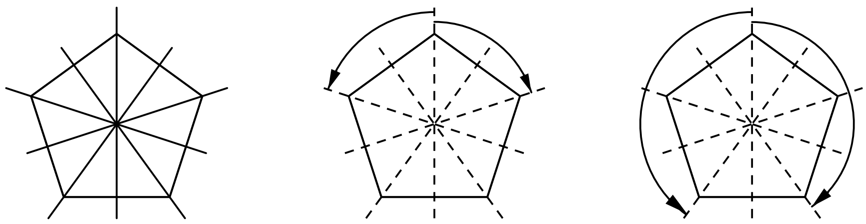
Ezt akartuk megmutatni. □

A $hg^{-1} \in C(a)$ feltétel ekvivalens azzal, hogy $h \in C(a)g$, tehát a konjugáltjai pontosan akkor egyenlőek, ha centralizátorának ugyanazon jobboldali mellékosztályából választjuk a konjugáló elemeket. Más szóval pontosan akkor nem egyenlőek, ha különböző mellékosztályokból vett elemmel konjugálunk. Ezzel beláttuk az alábbi tételt.

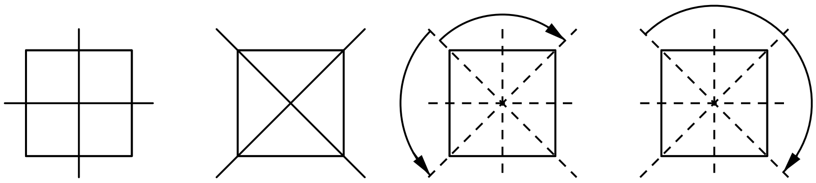
2.1.5. Tétel. *Legyen G csoport. Az $a \in G$-t tartalmazó konjugáltosztály elemszáma egyenlő az a elem centralizátorának G-beli indexével. Képlettel:* $|K(a)| = |G : C(a)|$.

2.1.6. Következmény. *Ha G véges, akkor* $|K(a)| = \frac{|G|}{|C(a)|}$, *így* $|K(a)|\,\big|\,|G|$.

2.2. D_n konjugáltosztályai



2.1. ábra. D_5 identitástól különböző konjugáltosztályai



2.2. ábra. D_4 identitástól különböző konjugáltosztályai

2.2.1. Definíció. *A szabályos n-szög szimmetriacsoportját n-edfokú diédercsoportnak nevezzük és D_n-nel jelöljük.*

A középpont körüli $\frac{2\pi}{n}$ szögű forgatást f-fel, egy tetszőleges szimmetriatengelyre való tükrözést t-vel jelölve, ezzel legtöbbször az alábbi alakban találkozhatunk:

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

ahol teljesül, hogy

$$\mathrm{id} = t^2 = f^n, \qquad tf^i = f^{n-i}t.$$

A csoport láthatóan $2n$ darab elemet tartalmaz és azt is érdemes észrevennünk, hogy a forgatásokból álló részhalmaza (az identitást is beleértve) ciklikus részcsoportot alkot.

Hogy megkönnyítsük további számításainkat, illetve megspóroljunk számos esetszétválasztást, most írjuk fel D_n-et egy ennél általánosabban kezelhető alakban:

$$D_n = \left\{ t^\alpha f^\beta |\ 0 \leq \alpha \leq 1,\ 0 \leq \beta \leq n-1 \right\},$$

és a korábbi összefüggések alapján adjuk meg az erre a felírásra vonatkozó szorzási szabályt is:

$$t^\alpha f^\beta t^\gamma f^\delta = \begin{cases} t^\alpha f^{\beta+\delta} & \text{ha } \gamma = 0 \\ t^{\alpha+\gamma} f^{n-\beta+\delta} & \text{ha } \gamma = 1 \end{cases}$$

A felső sorban t kitevőjébe egy $+\gamma$-t csempészve, az alsó sorból pedig f kitevőjéből n-et elhagyva (ezt megtehetjük, hiszen a forgatások kitevőjét modulo n értelmezzük), az alábbi egyszerűbb alakot kapjuk:

$$t^\alpha f^\beta t^\gamma f^\delta = t^{\alpha+\gamma} f^{\delta+(-1)^\gamma \beta}.$$

A konjugálás elvégzéséhez az inverzszámolás szabályára is szükségünk lesz:

$$\left(t^\alpha f^\beta\right)^{-1} = f^{-\beta} t^{-\alpha} = f^{-\beta} t^\alpha = \begin{cases} f^{-\beta} & \text{ha } \alpha = 0 \\ t^\alpha f^\beta & \text{ha } \alpha = 1 \end{cases}$$

Amit egyszerűbben úgy is írhatunk, hogy

$$\left(t^\alpha f^\beta\right)^{-1} = t^\alpha f^{(-1)^{\alpha+1}\beta}.$$

Most, hogy minden eszközt előkészítettünk, számoljuk ki a konjugáltosztályokat. Rögzítsünk egy $a = t^\alpha f^\beta$ csoportelemet és konjugáljuk egy általános $g = t^x f^y$ elemmel:

$$g^{-1}ag = \left(t^x f^y\right)^{-1} t^\alpha f^\beta t^x f^y = t^\alpha f^{(-1)^x \beta + [(-1)^{\alpha+1}+1]y}.$$

Ha ezen most végrehajtanánk egy esetszétválasztást, egyes konjugáltosztályokban a valódinál sokkal több elemet kapnánk, persze csak formálisan. Nagy segítséget nyújtana, ha ismernénk az egyes osztályok elemszámát, hiszen ekkor csak annyi lenne a dolgunk, hogy találjunk megfelelő számú, egymástól biztosan különböző elemet. Ebben az esetben ugyanis a további, az eddigiektől különböző alakban felírt elemek szükségképpen egyenlőek lennének valamelyik korábbival.

Határozzuk meg a konjugáltosztályok elemszámát a 2.1.6. Tétel segítségével. Ehhez először ki kell számolnunk az egyes elemek centralizátorát. Ismét rögzítsünk le egy $a = t^\alpha f^\beta$ elemet, és keressük meg azokat a $g = t^x f^y$ elemeket, amelyekkel felcserélhető.

$$\begin{aligned} ag &= ga \\ t^\alpha f^\beta t^x f^y &= t^x f^y t^\alpha f^\beta \\ t^{\alpha+x} f^{y+(-1)^x \beta} &= t^{x+\alpha} f^{\beta+(-1)^\alpha y} \end{aligned}$$

A két oldal pontosan akkor egyenlő, ha a forgatások kitevői egyenlők modulo n.

$$y + (-1)^x \beta \equiv \beta + (-1)^\alpha y \pmod{n}$$

Ezt a kongruenciát megoldhatjuk például egy egyszerű esetszétválasztással, felhasználva, hogy $x, \alpha \in \{0, 1\}$. Érdekes módon azt tapasztaljuk, hogy páros, illetve páratlan n-ek esetén különböző konjugáltosztályokat kapunk. Eredményeinket a 2.1.-2.4. táblázatokba gyűjtöttük össze.

Röviden összefoglalva a következőkre jutottunk. Páratlan n-ek esetén van egy egyelemű, néhány kételemű és egy n-elemű konjugáltosztályunk. Ezek elemei az identitás, a forgatások párosával az inverzeikkel és a tükrözések. Páros n-ek esetén azonban a 180°-os forgatás, más szóval a középpontos tükrözés is eleme a csoportnak, ami egyenlő az inverzével, így az egyik $\{f^{-\beta}, f^{\beta}\}$-alakú osztály egyeleművé esik össze. További, ennél sokkal meglepőbb változás, hogy a tükrözések két $\frac{n}{2}$-elemű osztályra esnek szét. Könnyen utánagondolhatunk, hogy az egyikben éppen a csúcsokon, a másikban pedig éppen az oldalakon átmenő tengelyekre való tükrözések szerepelnek. A 2.5. Táblázatban két konkrét példát is mutatunk.

2.3. S_n konjugáltosztályai

2.3.1. Definíció. *Az $X = \{1, 2, \ldots, n\}$ véges halmaz összes permutációinak halmazát n-edfokú szimmetrikus csoportnak nevezzük és S_n-nel jelöljük.*

S_n elemeit az egyszerű táblázatos felírás mellett ciklusok szorzataként is fel tudjuk írni, sőt már az alábbi tételt is bebizonyítottuk.

2.3.2. Tétel. *S_n minden eleme felírható páronként diszjunkt ciklusok szorzataként, a sorrendtől, az egyelemű ciklusoktól és a ciklusok kezdőelemének megválasztásától eltekintve egyértelmű módon.*

Ez a megállapítás rendkívül egyszerűvé teszi a konjugáltosztályok feltárását, ehhez ugyanis elegendő belátnunk a következő állítást.

2.3.3. Állítás. *S_n-ben b akkor és csak akkor konjugáltja a-nak, ha ciklusfelbontásuk azonos szerkezetű, azaz ha ugyanannyi azonos hosszússágú ciklust tartalmaznak.*

Bizonyítás. Először lássuk be, hogy ha $b \sim a$, akkor ciklusszerkezetük azonos. Rörgzített $a \in S_n$ felbontása legyen $a = (x_1, x_2, \ldots, x_k)(y_1, y_2, \ldots, y_l) \ldots (z_1, z_2, ..., z_m)$, ahol $x_i, y_i, \ldots, z_i \in X$. Konjugáljuk a-t egy általános $g \in S_n$ elemmel. Vizsgáljuk meg, hogy „hova viszi" $g^{-1}ag$ $g(x)$-et: $g(x) \xrightarrow{g^{-1}} x \xrightarrow{a} a(x) \xrightarrow{g} g(a(x))$. Ennek segítségével építsük fel $g^{-1}ag$ ciklusfelbontását. Kezdjük azzal a ciklussal, amelynek első eleme $g(x_1)$, ennek képe az előbbiek szerint $g(a(x_1)) = g(x_2)$ lesz. Hasonlóan folytatva a további elemek $g(x_3)$, $g(x_4)$, végül $g(x_k)$ lesz, amit a permutáció visszavisz $g(x_1)$-be, így megkaptuk az első diszjunkt ciklust. Mivel g bijekció, ezek mind különböző elemek, tehát a kapott ciklus valóban k hosszúságú. Ezt az eljárást a további diszjunkt ciklusaira megismételve látható, hogy ez szó szerint lemásolja annak ciklusszerkezetét. Ha pedig olyan ponthoz érünk, amely a-nak fixpontja, az nyilván $g^{-1}ag$-nek is fixpontja lesz.

A tétel megfordításának bizonyításához azt kell belátnunk, hogy ha a és b azonos ciklusszerkezetű, akkor létezik olyan g, hogy $g^{-1}ag = b$. Legyen

$$a = (x_1, x_2, \ldots, x_k)(y_1, y_2, \ldots, y_l) \ldots (z_1, z_2, ..., z_m),$$
$$b = (\alpha_1, \alpha_2, \ldots, \alpha_k)(\beta_1, \beta_2, \ldots, \beta_l) \ldots (\gamma_1, \gamma_2, ..., \gamma_m).$$

Válasszuk g-nek azt a permutációt, melyre $g(x_1) = \alpha_1$, $g(x_2) = \alpha_2$, $\ldots$, $g(x_k) = \alpha_k$, $g(y_1) = \beta_1$, $g(y_2) = \beta_2$, $\ldots$, $g(y_l) = \beta_l$, $\ldots$, $g(z_1) = \gamma_1$, $g(z_2) = \gamma_2$, $\ldots$, $g(z_m) = \gamma_m$. Mivel mind a g argumentumában lévő, mind az egyenlőségek jobb oldalán álló számok különbözők és S_n az összes permutációt tartalmazza, az így megadott permutáció valóban létezik. A bizonyítás első felének alapján pedig nyilvánvalóan megfelelő. □

α	β	$a = t^\alpha f^\beta$	$C(a)$	$\lvert K(a)\rvert = \frac{\lvert G\rvert}{\lvert C(a)\rvert}$
0	0	id	G	$\frac{2n}{2n} = 1$
0	$\beta \neq 0$	f^β	$\{\mathrm{id}, f^1, \ldots, f^{n-1}\}$	$\frac{2n}{n} = 2$
1	β	tf^β	$\{\mathrm{id}, tf^\beta\}$	$\frac{2n}{2} = n$

2.1. táblázat. Konjugáltosztályok elemszáma páratlan n-ek esetén

α	β	$a = t^\alpha f^\beta$	$g^{-1}ag$	$K(a)$
0	0	id	id	$\{\mathrm{id}\}$
0	$\beta \neq 0$	f^β	$f^{(-1)^x\beta}$	$\{f^{-\beta}, f^\beta\}$
1	β	tf^β	$tf^{(-1)^x\beta+2y}$	$\{t, tf, \ldots, tf^{n-1}\}$

2.2. táblázat. Konjugáltosztályok meghatározása páratlan n-ek esetén

α	β	$a = t^\alpha f^\beta$	$C(a)$	$\lvert K(a)\rvert = \frac{\lvert G\rvert}{\lvert C(a)\rvert}$
0	0	id	G	$\frac{2n}{2n} = 1$
0	$\frac{n}{2}$	$f^{\frac{n}{2}}$	G	$\frac{2n}{2n} = 1$
0	$\beta \neq 0, \beta \neq \frac{n}{2}$	f^β	$\{\mathrm{id}, f^1, \ldots, f^{n-1}\}$	$\frac{2n}{n} = 2$
1	β	tf^β	$\{\mathrm{id}, f^{\frac{n}{2}}, tf^\beta, tf^{\beta+\frac{n}{2}}\}$	$\frac{2n}{4} = \frac{n}{2}$

2.3. táblázat. Konjugáltosztályok elemszáma páros n-ek esetén

α	β	$a = t^\alpha f^\beta$	$g^{-1}ag$	$K(a)$
0	0	id	id	$\{\mathrm{id}\}$
0	$\frac{n}{2}$	$f^{\frac{n}{2}}$	$f^{(-1)^x\frac{n}{2}}$	$\{f^{\frac{n}{2}}\}$
0	$\beta \neq 0, \beta \neq \frac{n}{2}$	f^β	$f^{(-1)^x\beta}$	$\{f^{-\beta}, f^\beta\}$
1	0	t	tf^{2y}	$\{t, tf^2, \ldots, tf^{n-2}\}$
1	1	tf	$tf^{(-1)^x+2y}$	$\{tf, tf^3, \ldots, tf^{n-1}\}$

2.4. táblázat. Konjugáltosztályok meghatározása páros n-ek esetén

D_5	D_4
$\{\mathrm{id}\}$	$\{\mathrm{id}\}$
$\{f, f^4\}$	$\{f, f^3\}$
$\{f^2, f^3\}$	$\{f^2\}$
$\{t, tf, tf^2, tf^3, tf^4\}$	$\{t, tf^2\}$
	$\{tf, tf^3\}$

2.5. táblázat. D_5 és D_4 konjugáltosztályai

Tehát minden lehetséges ciklusszerkezethez tartozik egy konjugáltosztály. Ez azt jelenti, hogy S_n konjugáltosztályainak száma egyenlő az n pozitív egész partícióinak számával. Konkrét n esetében ezek elemszámának meghatározása egyszerű kombinatorika feladat. Például S_5 konjugáltosztályai az alábbiak:

Ciklusszerkezet	Elemszám
$(abcde)$	24
$(abcd)$	30
(abc)	20
$(abc)(de)$	20
(ab)	10
$(ab)(cd)$	15
id	1

2.6. táblázat.

2.4. Törtlineáris leképezések csoportja

Ebben a fejezetben megismerkedünk a törtlineáris leképezések csoportjával, majd megmutatjuk, hogy ez homomorf képe a 2×2-es invertálható mátrixok csoportjának. Ezt követően a homomorfizmustétel segítségével belátjuk, hogy az ugyanazon leképezésnek megfelelő mátrixok a homomorfizmus magja szerinti mellékosztályokba sorolódnak, a vizsgált csoport pedig az így kapott faktorcsoporttal izomorf.

A dolgozat többi részével ellentétben a függvények kompozícióját itt jobbról balra értelmezzük (tehát $f \circ g = f(g(x))$), hogy a mátrixokkal való homomorfizmus igazolásához ne kelljen eltérnünk a mátrixszorzás megszokott irányától.

2.4.1. Definíció. *Az $f:\ \mathbb{R} \setminus \{-\frac{d}{c}\} \to \mathbb{R},\ f(x) = \frac{ax+b}{cx+d}$ alakú függvényeket törtlineáris leképezéseknek nevezzük, ahol $a, b, c, d \in \mathbb{R}$, és $ad - bc \neq 0$.*

2.4.2. Állítás. *A törtlineáris leképezések csoportot alkotnak a kompozíció műveletére. A továbbiakban ezt a csoportot* TL*-lel fogjuk jelölni.*

Bizonyítás.

(i) Először mutassuk meg a kompozícióra való zártságot. Legyen $f(x) = \frac{ax+b}{cx+d}$, $g(x) = \frac{ex+f}{gx+h}$ két tetszőleges csoportelem. Ekkor

$$(f \circ g)(x) = f(g(x)) = \frac{a\frac{ex+f}{gx+h} + b}{c\frac{ex+f}{gx+h} + d} = \frac{(ae+gb)x + (af+bh)}{(ce+gd)x + (cf+dh)}.$$

Ennek az alakja megfelelő, de még azt is be kell látnunk, hogy $(ae+gb)(cf+dh) - (af+bh)(ce+gd) \neq 0$. Rendezzük át ezt a kifejezést: $(ae+gb)(cf+dh) - (af+bh)(ce+gd) = aecf + aedh + gbcf + gbdh - afce - afgd - bhce - bhgd = ad(eh-fg) - bc(eh-fg) = (eh-fg)(ad-bc)$. Ennek a szorzatnak egyik tényezője sem 0, ezért a szorzat sem 0.

(ii) A kompozícióról már tudjuk, hogy asszociatív.

(iii) Az egységelem nyilván az identitás: $\mathrm{id} = \frac{1x+0}{0x+1} = x$.

(iv) Végül megmutatjuk, hogy a halmaz minden eleme invertálható. Rögzített $f(x) = \frac{ax+b}{cx+d}$ csoportelemhez keressük azt a $g(x) = \frac{ex+f}{gx+h}$ elemet, melyre $(f \circ g)(x) = \frac{(ae+gb)x+(af+bh)}{(ce+gd)x+(cf+dh)} = x$. Ez az alábbi lineáris egyenletrendszerre vezet:

$$\begin{aligned} ae + gb &= 1 \\ af + bh &= 0 \\ ce + gd &= 0 \\ cf + dh &= 1. \end{aligned}$$

Ezt például Gauss-eliminációval megoldva azt kapjuk, hogy ha $a \neq 0$, akkor

$$\begin{aligned} e &= \frac{1}{a} + \frac{bc}{a(ad-bc)} \\ f &= -\frac{b}{ad-bc} \\ g &= -\frac{c}{ad-bc} \\ h &= \frac{a}{ad-bc}, \end{aligned}$$

ha viszont $a = 0$, akkor

$$\begin{aligned} e &= -\frac{d}{bc} \\ f &= \frac{1}{c} \\ g &= \frac{1}{b} \\ h &= 0. \end{aligned}$$

Ezek a törtek valóban értelmesek, hiszen már a definícióban kikötöttük, hogy $ad - bc \neq 0$.

TL tehát valóban csoport. □

2.4.3. Állítás. *A valós elemű, $n \times n$-es, invertálható mátrixok csoportot alkotnak a szorzásra. Ezt általános lineáris csoportnak nevezzük, jele:* $\mathrm{GL}(n, \mathbb{R})$.[1]

Ezt már korábbi tanulmányainkból tudjuk. Mivel egy mátrix pontosan akkor invertálható, ha a determinánsa nem 0, ezért $\mathrm{GL}(2, \mathbb{R})$ elemei azok az $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ alakú mátrixok, melyekre $ad - bc \neq 0$. Természetesen adódik az alábbi φ megfeleltetés $\mathrm{GL}(2, \mathbb{R})$ és TL között:

$$\varphi : \quad \mathrm{GL}(2, \mathbb{R}) \to \mathrm{TL}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \frac{ax+b}{cx+d}.$$

2.4.4. Állítás. *φ homomorfizmus.*

Bizonyítás. Legyen $\mathrm{GL}(2, \mathbb{R})$ két tetszőleges eleme $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ és $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$.

Ekkor egyfelől

$$AB = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix},$$

[1] A jelölés az angol general linear group elnevezésből származik.

másfelől már az előző bizonyításban kiszámoltuk, hogy

$$\left(\frac{ax+b}{cx+d}\right) \circ \left(\frac{ex+f}{gx+h}\right) = \frac{(ae+gb)x+(af+bh)}{(ce+dg)x+(cf+dh)}.$$

Tehát $\varphi(AB) = \varphi(A) \circ \varphi(B)$. $\square$

Világos, hogy ez a homomorfizmus szürjektív, hiszen minden $\frac{ax+b}{cx+d}$ alakú leképezés előáll a megfelelő $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mátrix képeként. Ezért a homomorfizmustétel alapján $\mathrm{TL} = \mathrm{Im}(\varphi)$ izomorf $\mathrm{GL}(2,\mathbb{R})$ φ magja szerinti faktorcsoportjával. Határozzuk meg $\mathrm{Ker}(\varphi)$-t:

$$\mathrm{Ker}(\varphi) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \frac{ax+b}{cx+d} = x \right\}.$$

A feltétellel ekvivalens, hogy $b = c = 0$, továbbá $a = d \neq 0$. Így

$$\mathrm{Ker}(\varphi) = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \;\middle|\; \lambda \neq 0 \right\}.$$

Tehát TL izomorf $\mathrm{GL}(2,\mathbb{R})$ e szerinti faktorcsoportjával. Használjuk az $N := \mathrm{Ker}(\varphi)$ jelölést. Tudjuk, hogy ilyenkor a bijekciót az

$$N\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \frac{ax+b}{cx+d}$$

függvény szolgáltatja, emellett egy adott mellékosztály az alábbi elemeket tartalmazza:

$$N\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \lambda \neq 0 \right\} = \left\{ \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix} \;\middle|\; \lambda \neq 0 \right\}.$$

Nézzük meg ezek képeit:

$$\varphi\left(\begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}\right) = \frac{\lambda a x + \lambda b}{\lambda c x + \lambda d}.$$

Az egyes mellékosztályokban tehát azok a mátrixok szerepelnek, amelyek képei ugyanazon törtlineáris leképezés egyszerűsített-bővített alakjának felelnek meg.

2.5. $\mathbb{Z}_p$ multiplikatív csoportja

Az alábbiakban megmutatjuk, hogy a $\mathbb{Z}_p^\times$ csoport minden p prímszám esetén ciklikus, azaz modulo p létezik primitív gyök. Károlyi tanár úr javaslatára ennek során $\mathbb{Z}_p^\times$ elemeit a $(p-1)$-edik komplex egységgyökökkel állítjuk párhuzamba; a bizonyítást ezekhez kötődő ismereteinkre vezetjük vissza.

2.5.1. Tétel. *Ha p prím, akkor a $\mathbb{Z}_p^\times$ csoport ciklikus, azaz minden eleme előáll egy alkalmas g elemének egész kitevős hatványaiként. Ekkor g-t primitív gyöknek nevezzük.*

Bizonyítás. A komplex számok teste fölött már tudjuk, hogy

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

ahol $\Phi_d(x)$ a d-edik körosztási polinom, vagyis az a normált polinom, melynek gyökei pontosan a primitív d-edik egységgyökök (mindegyik egyszeres). [5] Ennek együtthatói egészek (emiatt $\mathbb{Z}[x]$-beli polinomként is tekinthetünk rá), foka $\varphi(d)$ (ahol φ az Euler-függvény), továbbá irreducibilis $\mathbb{Z}$ és $\mathbb{Q}$ felett.

Rendeljük hozzá a $\mathbb{Z}$ fölötti polinomokhoz a $\mathbb{Z}_p[x]$-beli polinomokat a következőképpen:

$$\mathbb{Z}[x] \to \mathbb{Z}_p[x], \quad f(x) \to f(x) \pmod p,$$

vagyis vegyük az együtthatókat modulo p. Jelöljük $f \in \mathbb{Z}[x]$ képét $\tilde{f}$-mal. Ez nyilván összeg- és szorzattartó, emellett speciálisan Φ_d-re megőrzi a fokot, mivel annak főegyütthatója 1, tehát $\deg \Phi_d = \deg \widetilde{\Phi_d}$.

A „kis" Fermat-tétel alapján ha $p \nmid a$, akkor $a^{p-1} \equiv 1 \pmod p$, emiatt $\mathbb{Z}_p$-ben az $1, 2, \ldots, p-1$ számok mindegyike gyöke lesz az $x^{p-1} - 1$ polinomnak. Mivel a fokszám egyenlő a gyökök számával, ez gyöktényezőkre bontható:

$$x^{p-1} - 1 = (x-1)(x-2)\ldots(x-(p-1)).$$

Világos, hogy $p-1$ minden csoportelemnek *jó kitevője*, emiatt a csoportban csak olyan elemek fordulhatnak elő, amelyek d rendjére teljesül, hogy $d \mid p-1$. Mivel ezek mind $x^d - 1$ gyökei között szerepelnek, azt kell megmutatnunk, hogy létezik olyan elem, amelyik nem gyöke semelyik $x^d - 1$-nek, ahol $d \mid p-1$, $d \neq p-1$. Egy ilyen szám rendje, ezzel együtt különböző hatványainak száma csak $p-1$ lehet, tehát valóban primitív gyök.

$\mathbb{C}[x]$-ben, ezzel együtt $\mathbb{Z}[x]$-ben teljesül, hogy $x^{p-1} - 1 = \prod_{d \mid p-1} \Phi_d$. Emiatt $\mathbb{Z}_p[x]$-ben:

$$(x-1)(x-2)\ldots(x-(p-1)) = \widetilde{x^{p-1} - 1} = \prod_{d \mid p-1} \widetilde{\Phi_d}(x).$$

Hasonlóan, ha $d \mid p-1$, $d \neq p-1$:

$$\widetilde{x^d - 1} = \prod_{e \mid d} \widetilde{\Phi_e}(x).$$

Vegyük észre, hogy egyfelől ezek a körosztási polinomok az előző felbontásban is szerepelnek, hiszen $e \mid p-1$, másfelől ezek gyökei között az összes d rendű elem szerepel, mivel azok mindegyike gyöke $x^d - 1$-nek. Tehát a $p-1$-nél kisebb rendű elemek

$$\prod_{d \mid p-1, d \neq p-1} \widetilde{\Phi_e}(x)$$

gyökei között vannak. Emiatt a $p-1$ rendűek pontosan $\widetilde{\Phi_{p-1}}(x)$ gyökei, ugyanígy a d rendű elemek pontosan $\widetilde{\Phi_d}(x)$ gyökei lesznek. Mivel a leképezés foktartó és $x^{p-1} - 1$ $\mathbb{Z}_p[x]$-ben páronként különböző gyöktényezőkre esik szét, ezért a d rendű elemek száma $\deg \widetilde{\Phi_d} = \varphi(d)$. Speciálisan a $p-1$ rendűek száma $\varphi(p-1)$, tehát létezik ilyen elem. $\square$

3. fejezet

A csoportelméleti háttér vizsgálata

3.1. Függvények kompozíciója

(B. 3851.) Tekintsük az $f : x \to \frac{1}{x}$, $g : x \to 1 - \frac{1}{x}$ függvények véges sok példányának kompozíciójaként előállítható függvényeket; például

$$fgf : x \to \frac{1}{x} \to 1 - \frac{1}{\frac{1}{x}} = 1 - x \to \frac{1}{1-x}.$$

Előállítható-e így az $x \to x + 1$ függvény (az értelmezési tartományából esetleg véges sok helyet elhagyva)? [7]

A megoldás során először belátjuk, hogy a korábban kapott hat függvény egy D_3-mal izomorf csoportot alkot, majd megmutatjuk, hogy a villámmegoldásban szereplő, a függvények által önmagukra képezett halmazok valójában e csoport két különböző hosszúságú pályáját adják.

Elevenítsük fel a középiskolai megoldásban kapott *lényegében különböző* függvényeket és összefüggéseket, előbbieket foglaljuk egy H halmazba:

$$H := \left\{f, g, f^2, fg, g^2, gf\right\},$$

$$g^2 f \approx fg, \quad g^3 \approx f^2 \approx \mathrm{id}, \quad fgf \approx g^2, \quad fg^2 \approx gf, \quad gfg \approx f.$$

Könnyen látható, hogy H csoportot alkot a kompozíció műveletére: a műveleti zártságot már beláttuk, az egységelem f^2 és az inverzek léte is egyszerűen leellenőrizhető.[1] A korábbi 1. megoldás csoportelméleti megfelelőjét a következőképen fogalmazhatjuk meg: H nem tartalmazhatja a $h : x \to x + 1$ függvényt, mivel egy véges csoportban nem szerepelhet a csoport rendjénél nagyobb rendű elem, h rendje azonban végtelen.

Érdekesebb volt ennél a 2. megoldás, annak megértéséhez vessünk egy pillantást az összefüggésekre! Ha jobban megnézzük, valójában csak az első és a második független egymástól, a többi ezekből levezethető.

Vegyük észre, hogy H egy olyan 6-elemű csoport, amelyet f és g generál, továbbá teljesül, hogy $g^3 \approx f^2 \approx \mathrm{id}$, illetve $fgf \approx g^2$, emiatt izomorf a szabályos háromszög szimmetriacsoportjával, D_3-mal! [6]

Próbáljuk meg a háromszög csúcsait valós számokkal reprezentálni. Ehhez szükségünk lenne egy olyan számra, amelynek H-beli stabilizátora kételemű, hiszen ekkor pályájának hossza 3 lenne,

[1] Itt hallgatólagosan egyenlőnek tekintettük az egymással csak lényegében egyenlő függvényeket, ez azonban nem okoz gondot, hiszen ez ugyanúgy ekvivalenciareláció.

hasonlóan a háromszög csúcsaihoz. Megfelelő választás pl. a -1:

$$H_{-1} = \{\mathrm{id}, f\} \Rightarrow |H_{-1}| = 2 \Rightarrow |H(-1)| = \frac{|H|}{|H_{-1}|} = \frac{6}{2} = 3.$$

A középiskolás megoldásban mutatott két halmazról ugyan be tudtuk látni, hogy minden függvénykompozíció önmagára képezi, ezek előállítása azonban egyáltalán nem magától értetődő. Most már világos, hogy ennek hátterében egy valós számokon ható csoport pályái állnak. Az első önmagára képeződő halmaz éppen -1 pályája:

$$H(-1) = \left\{-1, 2, \frac{1}{2}\right\},$$

az értelmezési tartománnyal kapcsolatos problémára pedig egy általános $a \neq 0, 1$ elem pályája nyújtott megoldást:

$$H(a) = \left\{a, 1 - \frac{1}{a}, \frac{1}{1-a}, \frac{1}{a}, \frac{a}{a-1}, 1 - a\right\}.$$

3.2. Játék színes pontokkal

Egy körvonal mentén néhány kék és piros pontot helyeztünk el. Ezekkel az alábbi műveleteket végezhetjük:

(a) valahova beillesztünk egy új piros pontot, és a két szomszédját ellentétes színűre változtatjuk,

(b) ha legalább három pont van, és ezek közül legalább az egyik piros, akkor egy piros pontot törlünk, a két szomszédját pedig ellentétes színűre változtatjuk.

Kezdetben két pont van a kör kerületén, mindkettő kék. Elérhetjük-e a lépések többszöri alkalmazásával, hogy újra két pontunk legyen, de azok pirosak legyenek? [12]

A lépések szabályai és a középiskolai megoldásban talált invariáns kísérteties hasonlóságot mutat a szabályos háromszög szimmetriacsoportjának, D_3-nak bizonyos tulajdonságaival. Vizsgáljuk meg ezt a kapcsolatot közelebbről!

A kék pontokhoz rendeljük hozzá a szabályos háromszög egy szimmetriatengelyére való tükrözését, a pirosakhoz pedig a középpontjára való 120°-os forgatását:

$$K \mapsto t, \qquad P \mapsto f.$$

Az objektum egy adott állapotában vágjuk el valahol a kört és pozitív körüljárás szerint olvassuk össze, immár a t és f betűket. Ekkor egy D_3-beli szót kapunk, ami nyilván függ az elvágás helyétől. Az első betűt jelöljük x-szel, a maradék betűkből álló szót pedig jelöljük s-sel. A kapott szó tehát xs. Nézzük meg mi történik, ha „eggyel arrébb” helyezzük a vágást, azaz ha nem x előtt, hanem x után vágunk: ekkor sx-et kapunk. De hiszen ez éppen az előbbi elvágás x-szel vett konjugáltja! Tehát habár a transzformáció még függ, a konjugáltosztály már független az elvágás helyétől, így minden elrendezéshez egyértelműen hozzárendeltük D_3 valamely konjugáltosztályát. Ezeket már jól ismerjük:

$$\{\mathrm{id}\}, \{f, f^2\}, \{t, tf, tf^2\}.$$

A lépésekre való invarianciát hasonló módon is beláthatnánk, azonban a feladat és D_3 tulajdonságainak analógiáját jobban megvilágítja, ha megnézzük, mit jelentenek az egyes lépések D_3-ban (3.1. Táblázat).

Színes pontok	D_3
KK ↔ PPP	$t^2 \leftrightarrow f^3$
KP ↔ PPK	$tf \leftrightarrow f^2t$
PK ↔ KPP	$ft \leftrightarrow tf^2$
PP ↔ KPK	$f^2 \leftrightarrow tft$

3.1. táblázat.

Vegyük észre, hogy a lépési lehetőségek a transzformációk nyelvén kivétel nélkül ekvivalens átalakításokat jelentenek. Na de mit jelent az, hogy ekvivalens, ha még az elrendezéshez tartozó transzformáció sem egyértelmű? Ezt persze úgy kell értenünk, hogy a kör egy megfelelő elvágására vonatkozóan ekvivalens. Tehát ha a kört „kinyitjuk” és elvégzünk rajta egy lépést, akkor a transzformáció változatlan marad, amikor pedig „visszacsukjuk”, akkor ugyanabba a konjugáltosztályba kerülünk vissza.[2] A konjugáltosztály tehát invariáns az egyes lépések során.

Mivel a starthoz az identitás, a célhoz pedig a forgatások konjugáltosztálya tartozik, ezért egyikből nem lehet eljutni a másikba.

Valójában a középiskolai megoldásban kapott 0 és ± 1 invariánsok is e két konjugáltosztály analogonjai. A páros sok kék pont páros sok tükrözést jelent, ezért a transzformáció mindenképpen irányítástartó. Ez az oka annak, hogy a tükrözések konjugáltosztálya nem jelent meg a megoldás során. A t-k és f-k sorozata a $tf^it = f^{-i}$ szabály alapján $f^{a_1-a_2+a_3-a_4+\cdots-a_{n-1}+a_n}$ alakra hozható. A kitevőt persze modulo 3 értelmezzük, aminek előjele változhat az elvágás helyétől függően. Ennek értéke az identitás esetében 0, forgatások esetében ± 1. Innen a bűvös invariáns.

További megfontolásokkal általánosabb érvényű megoldáshoz juthatunk. Jelen állapotban a módszerünk csak arra alkalmas, hogy ha két konstrukcióhoz különböző konjugáltosztály tartozik, akkor ezekről biztosan kijelenthetjük, hogy nincs közöttük átjárás. Vajon ha két elrendezéshez ugyanaz a konjugáltosztály tartozik, akkor el lehet jutni egyikből a másikba?

Készítsünk egy olyan algoritmust, ami az egyes elrendezéseket annyira leegyszerűsíti, amennyire csak lehet. Mivel egyedül azzal tudjuk csökkenteni a pontok számát, ha elveszünk egy pirosat, ezért arra kell törekednünk, hogy az egyes lépések után mindig maradjon piros pont a konstrukcióban.

1. lépés: Ha az elrendezés már csak két pontot tartalmaz, kész vagyunk. Különben tovább.

2. lépés: Ha az elrendezés K-t és P-t is tartalmaz, akkor vegyünk el olyan P-t, aminek van K szomszédja. Különben tovább.

3. lépés: Ha az elrendezés csak P-t tartalmaz, akkor vegyük el az egyiket. Különben tovább.

4. lépés: Ha az elrendezés csak K-t tartalmaz, tegyünk le valahová egy P-t. Különben tovább.

5. lépés: Vissza az 1. lépéshez.

A 2. lépés után vagy mindegyik pont piros lesz, vagy lesznek kékek és pirosak is. A 3. lépést követően, ha háromnál több pontból indultunk, akkor szintén lesznek kék és piros pontok is. Ha viszont már csak három pontunk volt, akkor a lépés után két kékünk lesz és kész vagyunk. Ezek az egyszerűsítő lépések. A 4. lépés növeli a pontok számát, az eddigiek alapján azonban világos, hogy az algoritmus nem fog kettőnél hosszabb, csupa kék állapothoz eljutni, ilyen tehát csak a start

[2] Ehhez persze olyan helyen kell elvágnunk a kört, hogy az elvett, vagy hozzátett f ne szélső, hanem belső betű legyen. Ez legalább három betűből álló szavak esetében mindig kivitelezhető.

állapot lehet, amit egyszeri bővítő lépést követően az eljárás a továbbiakban csak egyszerűsíteni fog.

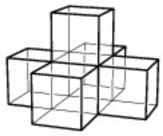
Algoritmusunkkal minden elrendezéshez megadtunk egy olyan lépéssorozatot, amely visszavezeti azokat az alábbi két pontból álló konstrukció valamelyikéhez: KK, PP, KP. Ezekhez mind különböző konjugáltosztályok tartoznak, rendre az $\{\mathrm{id}\}$, az $\{f, f^2\}$ és a $\{t, tf, tf^2\}$. Az azonos konjugáltosztályban lévő elrendezésekhez tartozó lépéssorozatok tehát összeérnek e három legegyszerűbb állapot valamelyikében. Ezzel beláttuk, hogy *két elrendezéshez akkor és csak akkor tartozik ugyanaz a konjugáltosztály, ha egyikből el lehet jutni a másikba.*

E megállapításnak a birtokában már tetszőleges két állapotról könnyedén el tudjuk dönteni, hogy létezik-e közöttük átjárás.

A felismert analógiát egyébként a teljes középiskolai megoldásra kiterjeszthetjük. Már felfedeztük, hogy a kék pontok számának paritása invariáns a lépésekre, így el tudtuk különíteni a *páros* és a *páratlan* lépéssorozatokat. A párosakon belül a piros pontok vizsgálatával további kategóriákat találtunk: meg tudtuk különböztetni a *0-s* és a *±1-es* sorozatokat. A három konjugáltosztály analogonja tehát a 0, a ±1 és a *páratlan*. A fenti algoritmust egy az egyben felhasználhatjuk. KK 0-s, PP ±1-es, KP *páratlan* elrendezés. Az adott címkéjű lépéssorozatok tehát ugyanúgy összeérnek valamelyik legegyszerűbb állapotban, így két elrendezés pontosan akkor átjárható, ha ugyanabba a kategóriába tartoznak.

3.3. Parkettázás

(B. 4190.) Hat egybevágó kockából az ábrán látható testet ragasztottuk össze. Kitölthető-e a tér hézagmentesen és átfedések nélkül ennek a testnek egybevágó példányaival? [8]



1. megoldás: Korábban már megvizsgáltuk, hogy a feladat egyenértékű a tér rácspontjainak az alábbi A halmaz eltoltjaival való egyrétegű lefedésével:

$$A = \{A_0(0,0,0); A_1(1,0,0); A_2(0,1,0); A_3(0,0,1); A_4(0,-1,0); A_5(-1,0,0)\}.$$

Az alábbiakban azt mutatjuk meg, hogy a középiskolai megoldásban bevezetett f függvény azért volt megfelelő választás, mert egy olyan szürjektív homomorfizmust létesít $\mathbb{Z}^3$ és $\mathbb{Z}_6$ között, amely az őshalmaz pontjaihoz különböző értékeket rendel.

Tudjuk, hogy $\mathbb{Z}^3$ és $\mathbb{Z}_6$ csoportot alkotnak az összeadásra, illetve a modulo 6 összeadásra, legyen ezek jele G és H. Tekintsük az alábbi függvényt:

$$f: \quad G \to H, \quad (x, y, z) \to x + 2y + 3z \pmod 6.$$

Mutassuk meg, hogy ez egy homomorfizmus. $P_1(x_1, y_1, z_1), P_2(x_2, y_2, z_2) \in G$ esetén $f(P_1 + P_2) = f(x_1+x_2, y_1+y_2, z_1+z_2) = x_1+x_2+2y_1+2y_2+3z_1+3z_2 \pmod 6 = (x_1+2y_1+3z_1)+(x_2+2y_2+3z_2) \pmod 6 = f(P_1) + f(P_2) \pmod 6$.

Mivel $f(A_i) = i$, ezért $\mathrm{Im}(f) = H$. Tehát teljesül az őspontok értékeinek különbözősége, amiből a szürjektivitás is következik. A homomorfizmustétel szerint $G/\operatorname{Ker}(f) \cong \mathrm{Im}(f)$, így $|\mathrm{Im}(f)| =$

$|G/\operatorname{Ker}(f)| = 6$. Ez azt jelenti, hogy ha a faktorcsoport 6 különböző elemét megtaláltuk, akkor az egészet sikerült előállítanunk. A továbbiakban használjuk az $N := \operatorname{Ker}(f)$ jelölést.

Tudjuk, hogy $i \neq j$ esetén $f(A_i) \neq f(A_j)$, ezért A_i és A_j N különböző mellékosztályaiba tartoznak, így G N szerinti faktorcsoportja a következő:

$$G/N = \{N + A_0, N + A_1, N + A_2, N + A_3, N + A_4, N + A_5\}.$$

Mivel ez a faktorcsoport G-nek egy partícióját szolgáltatja, ezzel megadtuk a térnek egy egyrétegű lefedését, amelyből most már egy lépéssel előállíthatjuk a keresett parkettázást. Tudjuk, hogy a $\beta_i : N \to N + A_i,\ n \to n + A_i$ függvények bijekciókat létesítenek a mellékosztályok között[3]. Származtassuk ennek segítségével G/N-ből a térnek egy másik partícióját oly módon, hogy most a bijekcióban álló ponthatosokat rendezzük halmazokba. n helyett használjuk az annak megfelelő $\underline{n}$ helyvektort:

$$A_{\underline{n}} = \{\underline{n} + A_0, \underline{n} + A_1, \underline{n} + A_2, \underline{n} + A_3, \underline{n} + A_4, \underline{n} + A_5\},$$

ahol $\underline{n} \in \operatorname{Ker}(f)$. Ezek persze egybevágók A-val, hiszen annak $\underline{n}$-ral eltolt példányai.

Érdemes megfigyelni, hogy $\operatorname{Ker}(f)$ éppen az eltolásvektorokat tartalmazza, a faktorcsoportjának egy-egy mellékosztályában pedig az eredeti test ugyanazon darabjának eltolt példányai szerepelnek. Például a „felső kockák” N_{A_3}-ban, az „alsó-középső kockák” pedig N_{A_0}-ban találhatók.

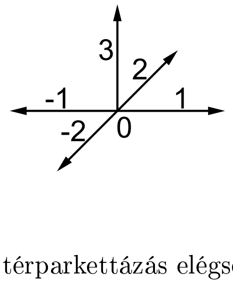
Megoldásunk általánosításával a következő állítás bizonyítását kapjuk.

3.3.1. Állítás. *Legyen $A = \{A_0, \ldots, A_k\}$ a tér (véges sok) k db rácspontját tartalmazó halmaz. A tér kiparkettázható ennek eltolt példányaival, ha létezik olyan $f : \mathbb{Z}^3 \to \mathbb{Z}_k$ szürjektív homomorfizmus, melyre $i \neq j$ esetén $f(A_i) \neq f(A_j)$. Ekkor a keresett eltolásvektorok éppen* $\operatorname{Ker}(f)$ *elemei.*

2. megoldás: Károlyi tanár úr 1986-ban írt TDK dolgozatában [3] elégséges feltételt bizonyított be $\mathbb{R}^n$ egy k (akár végtelen) elemű ponthalmazzal való E-parkettázhatóságára, ami tulajdonképpen a 3.3.1. Állítás általánosítása. A tér rácspontjaira, illetve véges ponthalmazokra vonatkozóan ezt az alábbi módon fogalmazhatjuk meg.

3.3.2. Állítás. *Legyen $A = \{P_0, P_1, \ldots, P_k\}$ véges ponthalmaz, ahol $P_i \in \mathbb{Z}^n$. Képezzük ebből az alábbi vektorhalmazt: $\tilde{A} = \{\overrightarrow{P_0P_i} | i = 0, 1, \ldots, k\}$. $\mathbb{Z}^n$ kiparkettázható A eltoltjaival, ha létezik egy olyan $G = \{g_0 = 0, \ldots, g_k\}$ Abel-csoport, melynek elemeit $\tilde{A}$ elemeinek megfeleltetve teljesül, hogy $\sum_{\alpha \in I} a_\alpha g_\alpha = 0$, valahányszor $\sum_{\alpha \in I} a_\alpha \overrightarrow{P_0P_\alpha} = 0$, ahol I legfeljebb k elemű indexhalmaz, a_α egész.*

Az első megoldásban definiált A halmazból származtatott $\tilde{A}$-hoz létezik ilyen Abel-csoport: $\mathbb{Z}_6^+$. A 3.1. ábrán mutatunk egy megfelelő hozzárendelést. A kérdéses térkitöltés tehát lehetséges.



3.1. ábra. A térparkettázás elégséges feltétele

[3] Ez a bijekció szerepel például annak az állításnak bizonyításában, amely szerint egy részcsoport szerinti mellékosztályok azonos elemszámúak.

Könnyen látható, hogy nyilvánvaló szimmetriáktól eltekintve ez az egyetlen megoldás, ami a 3.3.2. Állítás alkalmazásával nyerhető, tehát az eredeti középiskolás 2. megoldás mögött ténylegesen ez áll.

3.4. Törtlineáris leképezések

(B. 4650.) Létezik-e olyan $f(x) = \frac{ax+b}{cx+d}$ alakú függvény, melyre alkalmas páronként különböző $x_1, \ldots, x_5$ valós számokkal

$$f(x_1) = x_2, \quad f(x_2) = x_3, \quad f(x_3) = x_4, \quad f(x_4) = x_5, \quad f(x_5) = x_1$$

teljesül? [11]

A csoportelmélet eszközeivel felvértezve feladatunk egy ötödrendű törtlineáris leképezés keresése. Most nagy hasznát vesszük az elméleti részben leírt $\varphi : \mathrm{GL}(2, \mathbb{R}) \to \mathrm{TL}$ homomorfizmusnak, hiszen TL-lel korábban nemigen találkoztunk, ellenben $\mathrm{GL}(2, \mathbb{R})$-ben már egész otthonosan mozgunk.

Vizsgáljuk meg, hogy egy tetszőleges $\psi : G \to H$ homomorfizmusban hogyan „öröklődik” a G-beli rend H-ba. Tegyük fel, hogy $g \in G$ rendje k, azaz $g^k = 1$. Ekkor felhasználva, hogy a homomorfizmus művelettartó, illetve hogy az egységelemet egységelembe viszi, $\psi(1) = \psi(g^k) = \psi(g)^k = 1$. Ebből azonban sajnos csak annyi következik, hogy k a H-ban *jó kitevő*, azaz $o(\psi(g))|k$.

Ez azt jelenti, hogy ha találunk $\mathrm{GL}(2, \mathbb{R})$-ben egy ötödrendű mátrixot, akkor a képe vagy elsőrendű, vagy ötödrendű lesz. De csak az identitás elsőrendű, ami a $\mathrm{Ker}(\varphi)$-ben lévő mátrixok képe, amelyek rendje 1, 2 vagy végtelen. Tehát az ötödrendűség mindenképpen átöröklődik. (Ugyanezt a gondolatmenetet persze bármelyik 2-nél nagyobb prímszámra megismételhetnénk, tehát általában is igaz, hogy ha $o(g) = k$ ($g \in \mathrm{GL}(2, \mathbb{R})$) 2-nél nagyobb prím, akkor $o(\varphi(g)) = k$.)

A legegyszerűbb ötödrendű mátrix a 72°-os forgatás mátrixa:

$$A = \begin{pmatrix} \cos(72^\circ) & -\sin(72^\circ) \\ \sin(72^\circ) & \cos(72^\circ) \end{pmatrix}.$$

Ekkor

$$\varphi(A) = f(x) = \frac{\cos(72^\circ)x - \sin(72^\circ)}{\sin(72^\circ)x + \cos(72^\circ)},$$

amit $\cos(72^\circ)$-kal egyszerűsítve azt kapjuk, hogy

$$\varphi(A) = f(x) = \frac{x - \mathrm{tg}(72^\circ)}{\mathrm{tg}(72^\circ)x + 1}.$$

Ez hasonlít a középiskolás megoldásban felírt függvényhez, de nem pontosan az:

$$f(x) = \frac{x + \mathrm{tg}(36^\circ)}{-\mathrm{tg}(36^\circ)x + 1}.$$

Könnyen levezethető, hogy ennek a -36°-os forgatás mátrixa felel meg. Ez azt jelenti, hogy a homomorfizmus a rendet áltában tényleg nem örökíti át, hiszen ennek a mátrixnak a rendje 10, a képéről viszont már tudjuk, hogy ötödrendű.

Vajon min múlik, hogy a homomorfizmus hányad részére csökkenti a rendet? Azt kell észrevennünk, hogy az identitásnak nem csak az egységmátrix, hanem pontosan $\mathrm{Ker}(\varphi)$ elemei felelnek meg. Tehát ha az A mátrixra teljesül, hogy $A^k \in \mathrm{Ker}(\varphi)$ és k a legkisebb ilyen pozitív egész kitevő, akkor $o(\varphi(A)) = k$. A forgatások mátrixaira vonatkozóan:

$$A^k = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}^k = \begin{pmatrix} \cos(k\alpha) & -\sin(k\alpha) \\ \sin(k\alpha) & \cos(k\alpha) \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}.$$

A $sin(k\alpha) = 0$ egyenlőség két esetben teljesül: ha $k\alpha = 0°$, vagy ha $k\alpha = 180°$ (a szögeket persze modulo 360° értelmezzük). Előbbi esetben A^k az egységmátrix, utóbbiban viszont

$$A^k = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ez a középpontos tükrözés, más szóval a 180°-os forgatás mátrixa. Tehát a forgatások mátrixai közül pontosan kettő felel meg az identitásnak: a 0°-os és a 180°-os forgatásé.

Ez azt jelenti, hogy $\frac{360°}{k}$-val való forgatás esetén (k pozitív egész) a törtlineáris leképezés rendje vagy $\frac{k}{2}$, vagy k lesz aszerint, hogy k páros vagy páratlan. Ez az oka annak, hogy mind $72° = \frac{360°}{5}$, mind $36° = \frac{360°}{10}$ esetében ötödrendű törtlineáris leképezést kaptunk.

Vegyük észre, hogy eddigi megoldásunkat arra a sejtésre alapoztuk, hogy egy k-adrendű törtlineáris leképezés minden esetben tartalmazni fog k hosszúságú ciklusokat. A rend és a ciklusok kapcsolata azonban nem magától értetődő. Hiszen miért ne tartalmazhatna például egy tizedrendű függvény ötödrendű ciklusokat, vagy miért ne állhatna például egy hatodrendű függvény kizárólag 2 és 3 hosszú ciklusokból?

Az 5 rendű leképezésekkel könnyű dolgunk van. Ezek az ötös ciklusokon kívül csak egy hosszúakat, azaz fixpontokat tartalmazhatnak. Számoljuk is ki ezeket:

$$f(x) = \frac{ax+b}{cx+d} = x.$$

Ez nem lehet azonosság, hiszen tudjuk, hogy f nem az identitás (mivel ötödrendű), ezért vagy első, vagy másodfokú egyenletre vezet, így a fixpontok száma legfeljebb kettő. Ezektől eltekintve a függvény kizárólag öt hosszúságú ciklusokat tartalmaz. Ugyanígy tetszőleges (pozitív) p prímre belátható, hogy egy p rendű törtlineáris leképezés egy-két fixpontot leszámítva csak p hosszú ciklusokból áll.

Az összetett számú rendek esetén valamivel nehezebb dolgunk van. Például ha f rendje 6, akkor fixpontok és 6 hosszú ciklusok mellett – ahogyan azt már említettük – 2 és 3 hosszú ciklusok létezése is lehetséges. A kettes ciklusok elemeit f^2 fixpontjaiként kaphatjuk meg:

$$f^2(x) = \frac{a\frac{ax+b}{cx+d} + b}{c\frac{ax+b}{cx+d} + d} = \frac{(a^2+bc)x + (ab+bd)}{(ac+cd)x + (bc+d^2)} = x.$$

Ez most sem lehet azonosság, emellett ismét legfeljebb másodfokú egyenletre vezet, emiatt egynél több kettes ciklus biztosan nem fordul elő. Ugyanígy f^3-nek is legfeljebb két fixpontja van, de ez lehetetlen, hiszen egy hármas ciklus pontosan 3 számot mozgat! Ugyanígy 2-nél hosszabb, a rendnél rövidebb ciklusok általában sem lesznek lehetségesek.

Foglaljuk össze eredményeinket:

3.4.1. Állítás. *Minden k pozitív egészhez létezik olyan $f(x) = \frac{ax+b}{cx+d}$ törtlineáris leképezés, melynek rendje k. Ekkor f legfeljebb két fixponttól és legfeljebb egy kettes ciklustól eltekintve kizárólag k-hosszú ciklusokat tartalmaz.*

Általános képletet is könnyen adhatunk f-re. A $\frac{360°}{2k}$-val történő forgatás mátrixa $2k$ rendű, ezért képének rendje k:

$$f(x) = \frac{\cos\left(\frac{360°}{2k}\right)x - \sin\left(\frac{360°}{2k}\right)}{\sin\left(\frac{360°}{2k}\right)x + \cos\left(\frac{360°}{2k}\right)} = \frac{\cos\left(\frac{180°}{k}\right)x - \sin\left(\frac{180°}{k}\right)}{\sin\left(\frac{180°}{k}\right)x + \cos\left(\frac{180°}{k}\right)},$$

amit $k \neq 2$ esetén tovább egyszerűsíthetünk:

$$f(x) = \frac{x - \operatorname{tg}\left(\frac{180°}{k}\right)}{\operatorname{tg}\left(\frac{180°}{k}\right) x + 1}.$$

3.5. Számok színezése

(B. 4265.) Színezzük ki a pozitív egész számokat 7 színnel úgy, hogy minden a pozitív egész számra az $\{a, 2a, 3a, 4a, 5a, 6a, 7a\}$ halmaz elemeinek színe páronként különböző legyen. [9]

A feladat szerzője, Pach Péter Pál tanár úr szerint 7 helyett vélhetően minden pozitív egészre létezik ilyen színezés. Sejtése azonban egyelőre még nem nyert bizonyítást.

3.5.1. Sejtés. *Minden n-re igaz, hogy a pozitív egész számokat kiszínezhetjük n színnel úgy, hogy minden a esetén az $\{a, 2a, \ldots, na\}$ halmaz elemeinek színe páronként különböző legyen, ahol a, n pozitív egészek.*

Korábban ezt $n = 7$-re bebizonyítottuk. A KöMaL ugyanezen számában kitűzésre került a probléma tetszőleges $n = p - 1$-re, ahol p prím. A sejtés tehát végtelen sok n-re teljesül. Emellett egyébként minden $n \leq 70$-re, $n = \frac{p-1}{2}$-re, továbbá $n = p^2 - p$-re is belátható. [13]

(A. 506.) Igazoljuk, hogy tetszőleges p prímszámra a pozitív egészeket ki lehet színezni $p - 1$ színnel úgy, hogy minden a pozitív egész számra az $\{a, 2a, 3a, ..., (p - 1)a\}$ halmaz elemeinek színe páronként különböző legyen. [10]

1. megoldás: Oldjuk meg először a feladatot $p - 1 = 6$-ra. A számelmélet alaptételéből következően minden a pozitív egész felírható $a = 7^k m$ alakban, ahol m a többi prímhatvány szorzata, esetleg 1 (azaz $7 \nmid m$). Tekintsük az alábbi függvényt:

$$f: \quad \{\text{pozitív egészek}\} \to \mathbb{Z}_7^\times, \quad f(a = 7^k m) = m \pmod 7.$$

Tehát minden $a = 7^k m$-hez hozzárendeljük m 7-tel vett osztási maradékát. Azt állítjuk, hogy ezzel egy megfelelő színezést kaptunk. Bizonyítsuk ezt be!

A 2.5.1. Tétel alapján a $\mathbb{Z}_7^\times$ csoport ciklikus, azaz előállítható valamelyik elemének egész kitevős hatványaiként. Ilyen elem például a 3:

	3^0	3^1	3^2	3^3	3^4	3^5	3^6
(mod 7)	1	3	2	6	4	5	1

3.2. táblázat.

Tehát

$$\mathbb{Z}_7^\times = \{1, 2, 3, 4, 5, 6\} = \{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\}.$$

Számoljuk ki a függvényértékeket az egyes halmazokon, legyen a pozitív egészre $f(a = 7^k m) = 3^l \pmod 7$ (ld. 3.3. Táblázat).

Mivel a 3-hatványok periodikusan ismétlődnek a rend szerint és ezek a függvényértékek ugyanabba a periódusba esnek (hiszen a táblázatban egy adott sorban mindig az előzőben lévő érték 3-szorosa áll), ezért f a halmazelemeket valóban különbözőre színezi.

A megoldás 7 helyett tetszőleges p prímre megismételhető.

x	$f(x)$
$1a$	$1m \equiv 3^0 m \equiv 3^{l+0}$
$3a$	$3m \equiv 3^1 m \equiv 3^{l+1}$
$2a$	$2m \equiv 3^2 m \equiv 3^{l+2}$
$6a$	$6m \equiv 3^3 m \equiv 3^{l+3}$
$4a$	$4m \equiv 3^4 m \equiv 3^{l+4}$
$5a$	$5m \equiv 3^5 m \equiv 3^{l+5}$

3.3. táblázat.

2. megoldás: A feladat visszavezethető $\mathbb{Z}^{\pi(n)}$ parkettázására, ahol $\pi(n)$ az n-nél nem nagyobb (pozitív) prímek számát jelöli. Az egyszerűség kedvéért egyelőre maradjunk a síkon és vizsgáljuk meg a feladatot $n = 4$-re.

A korábbiak alapján minden a pozitív egész egyértelműen felírható $a = 2^\alpha 3^\beta q$ alakban, ahol q pozitív egész, továbbá $q \nmid 2, 3$. Képezzük az alábbi f függvényt:

$$f : \quad \{\text{pozitív egészek}\} \to \mathbb{Z}^2, \quad f(a = 2^\alpha 3^\beta q) = (\alpha; \beta).$$

Tehát minden pozitív egészhez hozzárendeljük a 2, illetve a 3 prímtényezői kitevőiből álló síkbeli pontot, illetve kitevővektort. Ekkor

$$f(\{1, 2, 3, 4\}) = \{(0; 0), (1; 0), (0; 1), (2; 0)\}.$$

Színezzük ezt a négy pontot mondjuk pirosra, zöldre, kékre és sárgára. Azt állítjuk, hogy ha a sík kiparkettázható e halmaz eltolt példányaival, akkor az egyben a pozitív egészeknek egy megfelelő színezését eredményezi.

Könnyen tudunk megfelelő E-parkettázást mutatni (ld. 3.2. ábra). (Ennek léte persze a a 3.3.2. Állítással is egyszerűen ellenőrizhető. A fenti pontoknak feleltessük meg rendre a 0, 1, 3, 2 értékeket.) Na de miért kellett kiparkettáznunk az egész síkot, amikor a pozitív egészeknek csak az első síknegyed pontjai felelnek meg? Ráadásul önmagában az első síknegyedet nem is tudnánk ilyen módon lefedni.

Nézzük meg egy $\{a, 2a, 3a, 4a\}$ halmaz képét:

$$f(\{2^\alpha 3^\beta q, 2^{\alpha+1} 3^\beta q, 2^\alpha 3^{\beta+1} q, 2^{\alpha+2} 3^\beta q\}) = \{(\alpha; \beta), (\alpha + 1; \beta), (\alpha; \beta + 1), (\alpha + 2; \beta)\}.$$

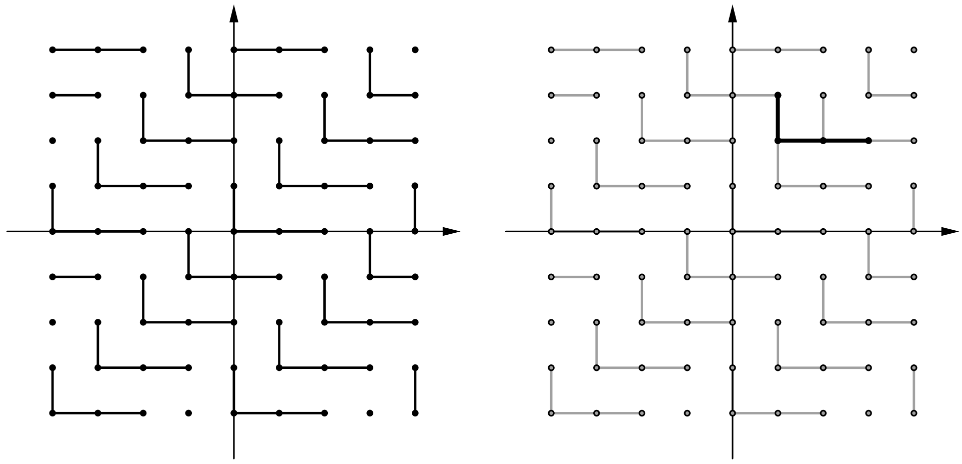
Ez éppen a $\{(0; 0), (1; 0), (0; 1), (2; 0)\}$ halmaz egy $(\alpha; \beta)$ vektorral való eltoltja, ahol α és β tetszőleges nemnegatív egészek. Vegyük észre, hogy ez nem feltétlenül esik egybe egy konkrét „parketta darabbal”, de azzal egybevágó, ezért bárhová is toljuk a fenti parkettázásban, az egyes pontjai valóban különböző színűek lesznek. A teljes sík lefedése tehát csak arra szolgál, hogy a pozitív síknegyedben tetszőleges eltolást alkalmazva különböző színű pontokat kapjunk.

Állításunk egyébként minden n-re belátható, sőt a megfordítása is igaz. [13]

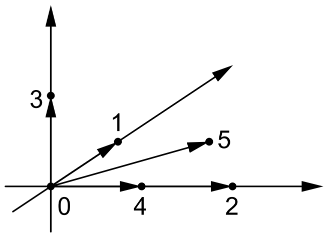
3.5.2. Állítás. *Pach tanár úr sejtése pontosan akkor igaz n-re, ha $\mathbb{Z}^{\pi(n)}$ kiparkettázható az $f(\{1, \ldots, n\})$ ponthalmaz eltolt példányaival, ahol f a pozitív egészekhez a megfelelő $\pi(n)$-dimenziós kitevővektort rendeli hozzá.*

Próbáljuk ki ezt az állítást a korábbi $n = 6$-ra. Ekkor

$$f(\{1, 2, 3, 4, 5, 6\}) = \{(0; 0; 0), (1; 0; 0), (0; 1; 0), (2; 0; 0), (0; 0; 1), (1; 1; 0)\}.$$



3.2. ábra. A pozitív egészek színezése síkparkettázással ($n = 4$)



3.3. ábra. A pozitív egészek színezése térparkettázással ($n = 6$)

A 3.3.2. Állítás alapján most is könnyen belátható, hogy ez lehetséges. E ponthalmaznak ugyanis megfeleltethetjük $\mathbb{Z}_6^+$ elemeit, például a 3.3. ábrán látható módon.

Érdekességképpen megemlítjük, hogy a tárgyalt sejtés a szerző Szabó Csaba tanár úrral írt közös cikkében szereplő, Pilztől származó 3.5.4. Sejtés vizsgálata közben született [14], amelyet minden páratlan k-ra vonatkozóan megoldana. Emellett egyébként újabb bizonyítást szolgáltatna a Graham-sejtésre [15] is. [13]

3.5.3. Sejtés (Graham-sejtés). *Bármely n különböző egész szám közül ki lehet választani a-t és b-t ($a \neq b$) úgy, hogy $\frac{a}{(a;b)} \geq n$.*

3.5.4. Sejtés. *Legyen $K = a_1, ..., a_k \subset \mathbb{N}$ véges, k elemű halmaz. Ekkor $|1K\Delta 2K\Delta \ldots \Delta nK| \geq n$, ahol Δ a szimmetrikus differenciát jelöli, n pozitív egész.*

Utóbbi kapcsolatát Pach tanár úr sejtésével könnyen beláthatjuk. Legyen k páratlan és tegyük fel, hogy létezik n-re megfelelő színezés, azaz minden a-ra az $\{a, 2a, \ldots, na\}$ halmaz elemei különböző színűek. Legyen az egyik szín mondjuk a piros. Tekintsük az alábbi halmazműveletet:

$$\{a_1, \ldots, a_k\}\Delta\{2a_1, \ldots, 2a_k\}\Delta \ldots \Delta\{na_1, \ldots, na_k\}.$$

Mivel minden $\{a_i, \ldots, na_i\}$ halmaz ($i = 1, \ldots, k$) tartalmaz pontosan egy pirosat, a fenti halmazokban összesen k darab piros elem szerepel, egy esetleg többször is. A szimmetrikus differencia páratlan sok elemet azonban nem tud kiejteni, emiatt ezek mindegyikében maradni fog legalább egy piros. Ugyanígy mind az n színből maradni fog legalább egy, ezért a fenti művelet eredménye legalább n-elemű. [13]

Irodalomjegyzék

[1] Freud Róbert: *Lineáris algebra.* ELTE Eötvös Kiadó, 2009.

[2] Freud Róbert, Gyarmati Edit: *Számelmélet.* Nemzeti Tankönyvkiadó, Budapest, 2006.

[3] Károlyi Gyula: $\mathbb{R}^n$ *parkettázása diszkrét ponthalmazokkal.* Tudományos diákköri dolgozat, ELTE, 1986.

[4] Kiss Emil: *Bevezetés az algebrába.* Typotex Kiadó, Budapest, 2007.

[5] Kiss Emil: *Bevezetés az algebrába.* Typotex Kiadó, Budapest, 2007, 131.

[6] Kiss Emil: *Bevezetés az algebrába.* Typotex Kiadó, Budapest, 2007, 227.

[7] *Középiskolai Matematikai és Fizikai Lapok*, **55** (2005), 420.

[8] *Középiskolai Matematikai és Fizikai Lapok*, **59** (2009), 292.

[9] *Középiskolai Matematikai és Fizikai Lapok*, **60** (2010), 227.

[10] *Középiskolai Matematikai és Fizikai Lapok*, **60** (2010), 228.

[11] *Középiskolai Matematikai és Fizikai Lapok*, **64** (2014), 355.

[12] *Kürschák József Matematikai Tanulóverseny*, 2004.

[13] Pach Péter Pál, *személyes kommunikáció*, 2016. május 17.

[14] Péter Pál Pach, Csaba Szabó: *On the minimal distance of a polynomial code.* Discrete Mathematics and Theoretical Computer Science **13** (2011), 33–44.

[15] R. Balasubramanian, K. Soundararajan: *On a conjecture of R. L. Graham.* Acta Arithmetica **75** (1996), 1–38.