Eötvös Loránd Tudományegyetem
Matematika Intézet

LESKÓ ZOLTÁN MÁRK

SZIMMETRIKUS CSOPORTOK

BSc szakdolgozat

Témavezető: Ágoston István

ELTE Algebra és Számelméleti Tanszék

2017. Budapest

Köszönetnyilvánítás

Először szeretném megköszönni Ágoston Istvánnak a sok segítséget, a hasznos tanácsokat, a rengeteg konzultációs lehetőséget, amit biztosított a számomra. Továbbá szeretnék köszönetet mondani Schőn Tímeának, aki sokat segített nekem, hogy ez a szakdolgozat elkészülhessen, az édesanyámnak, aki egyetemi éveim alatt mindvégig mellettem állt és türelmes volt hozzám, valamint Tar Lillának.

Tartalomjegyzék

1. Bevezetés **1**

1.1. Rövid elméleti áttekintés 1

2. Szimmetrikus csoportok automorfizmusai **5**

2.1. Automorfizmuscsoportok 5

2.2. S_n automorfizmuscsoportja 6

3. Az alternáló csoport egyszerűsége **9**

3.1. Bevezetés 9

3.2. Az A_5 és A_6 egyszerűsége 10

3.3. Az A_n egyszerűségének bizonyítása konjugált elemek segítségével 12

3.4. Az A_n egyszerűségének bizonyítása A_6 egyszerűségének felhasználásával 14

3.5. Az A_n egyszerűségének bizonyítása konjugáltosztályok felhasználásával 15

3.6. Az A_n egyszerűségének bizonyítása hármas ciklusok konstruálásával 17

3.7. Az A_n egyszerűségének bizonyítása normalizátorok segítségével 19

4. Maximális elemrend a véges elemszámú szimmetrikus csoportban **23**

4.1. Bevezetés 23

4.2. Adott rendű permutációk és a prímtényezős felbontás kapcsolata 24

4.3. F(n) és G(n) közötti összefüggések 25

4.4. A maximális elemrend aszimptotikus becslése 29

4.5. G(n) kiszámítása adott n esetén 32

4.6. Érdekességek a partíciófüggvényről 35

Irodalomjegyzék **36**

1. fejezet

Bevezetés

A dolgozat a szimmetrikus csoportokat mutatja be. A Bevezetés második felében a szimmetrikus csoportok legérdekesebb tulajdonságait ismertetjük. Ezután a második fejezetben a szimmetrikus csoportok automorfizmusait vizsgáljuk. A szimmetrikus csoport részcsoportja az alternáló csoport. A harmadik fejezetben ennek egyszerűségét bizonyítjuk ötféleképpen. Végül azt vizsgáljuk, hogy mekkora lehet a maximális elemrend a véges szimmetrikus csoportokban.

1.1. Rövid elméleti áttekintés

Ebben a fejezetben [5] és [3] alapján röviden ismertetjük a szimmetrikus csoportokkal kapcsolatos legfontosabb fogalmakat, és megemlítjük néhány ismert tulajdonságukat.

1.1.1. Definíció. Egy X halmazt önmagára képező kölcsönösen egyértelmű leképezéseket az X permutációinak nevezzük, ezek halmazát S_X-szel jelöljük.

1.1.2. Definíció. Legyen X egy tetszőleges halmaz. A kompozíció műveletére nézve S_X csoportot alkot, ezt az X halmazon ható szimmetrikus csoportnak hívjuk. Az S_X egységelemét id jelöli, ez az identikus leképezés, amely minden elemet önmagába visz. Az $f \in S_X$ inverzét f^{-1}-gyel jelöljük. A kompozíció műveletét szorzásnak hívjuk majd és gyakran $f \circ g$ helyett fg-t írunk. Az fg permutációnál tehát először alkalmazzuk a g-t, utána pedig az f-et.

1.1.3. Definíció. Ha $|X| = n$, akkor az S_X csoportot n-edfokú szimmetrikus csoportnak nevezzük. Ha $X = \{1,2,\ldots,n\}$, akkor S_X helyett S_n-et írunk.

1.1.4. Definíció. Legyen X egy halmaz. Azt a permutációt, amely az $x \neq y \in X$ elemeket cseréli ki (azaz $x \mapsto y$ és $y \mapsto x$), továbbá X összes többi elemét fixen hagyja, az (x, y) szimbólummal fogjuk jelölni. Az így kapott permutációkat transzpozíciónak nevezzük.

1.1.5. Megjegyzés. *A transzpozíciók generálják S_n-t.*

1.1.6. Definíció. Legyen X halmaz és $x_1, x_2, x_3 \dots x_{k-1}, x_k \in X$ egymástól különböző elemek. Jelölje $(x_1, x_2, x_3 \dots x_{k-1}, x_k)$ azt a permutációt, amelynél az x_1 képe x_2, az x_2 képe x_3, ... ,x_{k-1} képe x_k, végül az x_k képe x_1, és X többi eleme a helyén marad. Az így kapott permutációkat ciklusnak nevezzük. A k szám ennek a ciklusnak a hossza, $x_1, \dots x_k$ pedig a ciklus elemei.

1.1.7. Definíció. Legyen $a \in S_n$. Ekkor az a permutáció páros, ha felírható páros sok csere szorzataként. Egyébként az a permutáció páratlan. A páros permutációk részcsoportot alkotnak, ezt alternáló csoportnak nevezzük. Jele: A_n.

1.1.8. Megjegyzés. *Egy ciklus paritása pontosan akkor páros, ha a hossza páratlan. Például az* (1234) *permutáció páratlan, a* (23)(45) *permutáció pedig páros.*

1.1.9. Definíció. Legyenek $a, b \in S_n$ ciklusok. Ha nincs közös eleme a-nak és b-nek, akkor azt mondjuk, hogy diszjunktak egymástól.

1.1.10. Definíció. Legyen $a \in S_n$. Ekkor a felírható diszjunkt ciklusok szorzataként

$$a = a_1 a_2 \dots a_k$$

alakban, és ebben a felbontásban az $a_1, a_2, \dots, a_k$ ciklusok a sorrendtől eltekintve egyértelműek. Ezt nevezzük az a ciklusfelbontásának.

1.1.11. Definíció. Egy G csoport rendje a csoport elemeinek száma. Jele: $|G|$.

1.1.12. Megjegyzés. *Így például* $|S_n| = n!$ *és* $|A_n| = \dfrac{n!}{2}$ *tetszőleges véges n esetén.*

1.1.13. Definíció. Legyen N részcsoport G-ben. N normálosztója G-nek, ha minden $a \in N$ és $g \in G$ esetén $gag^{-1} \in N$.

1.1.14. Megjegyzés. *Például ha $n \geq 5$, akkor S_n normálosztói* $\{1\}, A_n, S_n$

1.1.15. Definíció. Legyen $a, b \in G$. Az a és b elemek akkor konjugáltak egymással, ha létezik olyan $g \in G$ elem, melyre $gag^{-1} = b$ teljesül.

1.1.16. Megjegyzés. *Például S_5-ben az $a =$* (1345) *elem konjugált a $b =$* (1542) *elemmel $g =$* (235) *esetén.*

1.1.17. Megjegyzés. *A konjugáltság ekvivalenciareláció, osztályait a csoport konjugáltosztályainak nevezzük.*

1.1.18. Definíció. Egy G csoport centrumának azon $a \in G$ elemek halmazát nevezzük, amelyek G minden elemével fölcserélhetők. Jele $Z(G)$.

1.1.19. Megjegyzés. *Például $n \geq 3$ esetén $Z(S_n) = (1)$. Ezt az állítást bebizonyítjuk a 2.2 alfejezetben.*

1.1.20. Tétel. *(Lagrange) Legyen $H \leq G$. Ekkor H elemszáma osztója G elemszámának.*

1.1.21. Megjegyzés. *Például A_n részcsoportja S_n-nek, és $\frac{n!}{2} \mid n!$.*

1.1.22. Definíció. *Supp* $\sigma = \{i \in \{1, \ldots, n\} |\ \sigma(i) \neq i\}$ a σ által mozgatott elemek halmaza. Ezt nevezzük néha a σ tartójának.

1.1.23. Tétel. *Két elem akkor és csak akkor konjugált egymással S_n-ben, ha azonos a ciklusszerkezetük.*

Bizonyítás. Legyen $\sigma \in S_n$. Ha $\sigma = (x_1, \ldots x_k)$ egy k ciklus, akkor könnyen ellenőrizhető, hogy

$$\tau\sigma\tau^{-1} = (\tau(x_1), \ldots \tau(x_k))$$

teljesül.

Ha $y \neq \tau(x_i)$ semmilyen i-re, akkor $\tau^{-1}y \neq x_i$, és így $\sigma\tau^{-1}y = \tau^{-1}y$. Ebből

$$\tau\sigma\tau^{-1}y = \tau\tau^{-1}y = y$$

adódik.

Ha $y = \tau(x_i)$, akkor $1 \leq i \leq k-1$ esetén

$$\tau\sigma\tau^{-1}(\tau(x_i)) = \tau\sigma(x_i) = \tau(x_{i+1}).$$

teljesül.

Ha $i = k$, akkor $\tau\sigma\tau^{-1}(\tau(x_k)) = \tau(x_1)$ igaz.

Ha $\sigma = \rho_1\rho_2 \ldots \rho_k$, ahol a ρ_i-k diszjunkt ciklusok, akkor a

$$\tau\sigma\tau^{-1} = \tau\rho_1\tau^{-1}\tau\rho_2\tau^{-1} \ldots \tau\rho_k\tau^{-1}$$

felírásban szereplő ciklusok diszjunktak egymástól, amiből az következik, hogy σ és $\tau\sigma\tau^{-1}$ ciklusszerkezete ugyanaz.

Másrészt, ha σ és ρ hasonló ciklusszerkezetűek, akkor létezik olyan $x_1, \ldots x_n$ és $y_1, \ldots y_n$ sorozat, hogy

$$\sigma = (x_1, \ldots x_{k_1})(x_{k_1+1} \ldots x_{k_2}) \ldots (x_{k_2+1} \ldots x_n)$$

és

$$\rho = (y_1, \dots y_{k_1})(y_{k_1+1} \dots y_{k_2}) \dots (y_{k_2+1} \dots y_n)$$

diszjunkt ciklusfelbontás.

Ekkor legyen $\tau : x_i \to y_i$. Ilyenkor

$$\tau\sigma\tau^{-1} = \rho$$

az előzőek alapján.

Most legyenek τ és σ azonos ciklusszerkezetű permutációk, és legyenek ezen permutációk ciklusai $P_1, \dots P_s$, illetve $Q_1, \dots Q_s$ úgy, hogy $|P_i| = |Q_i|$. Vegyünk mindegyik P_i-ből egy u_i és minden Q_i-ből egy v_i elemet. Legyen

$$\rho : \rho(\sigma^k(u_i)) = \tau^k(v_i),$$

ahol $1 \leq i \leq s$, és k nemnegatív egész. Bebizonyítjuk, hogy ρ egy leképezést ad meg. Ez tényleg leképezés, hiszen a $\sigma^k(u_i) = \sigma^m(u_i)$ feltétel mellett teljesül $\tau^k(v_i) = \tau^m(v_i)$, mert $|P_i| = |Q_i|$. Hasonló módon kapjuk meg, hogy a $\tau^k(v_i) = \tau^m(v_i)$ feltételből következik a $\sigma^k(u_i) = \sigma^m(u_i)$ összefüggés. Így ρ injektív. Figyelembe véve, hogy minden 1 és n közötti egész felírható alkalmas k és i választással $\sigma^k(u_i)$ és $\tau^k(v_i)$ alakban, ezért ρ az $\{1, \dots n\}$ halmazt önmagába képezi injektíven. Így ρ ezen halmaz permutációja.

Tetszőleges $\sigma^k(u_i)$ esetén:

$$\rho\sigma\sigma^k(u_i) = \rho\sigma^{k+1}(u_i) = \tau^{k+1}(v_i) = \tau(\tau^k(v_i)) = \tau\rho(\sigma^k(u_i)),$$

amiből $\rho\sigma = \tau\rho$ következik, amely ugyanaz, mint $\tau = \rho\sigma\rho^{-1}$. $\square$

2. fejezet

Szimmetrikus csoportok automorfizmusai

Ebben a fejezetben [5] és [4] alapján bemutatjuk a csoportok automorfizmusait és azok legfontosabb jellemzőit. Lezárásként [6] alapján megfogalmazunk és bizonyítunk egy tételt S_n automorfizmusaival kapcsolatban.

2.1. Automorfizmuscsoportok

2.1.1. Definíció. Egy G csoportot önmagába képező kölcsönösen egyértelmű homomorfizmust automorfizmusnak nevezzük. Ilyenek pl. a G elemeivel való konjugálások: $g \in G$-re a g elemmel való konjugálás az a ϕ_g automorfizmus, melynél $\phi_g(x) = x^g := gxg^{-1}$. Egy G csoport automorfizmusai a kompozíció műveletére nézve csoportot alkotnak. Ezt nevezzük a G automorfizmuscsoportjának és $Aut(G)$-vel jelöljük. A belső automorfizmusok részcsoportot alkotnak, ennek jele $Inn(G)$.

2.1.2. Állítás. $Inn(G) \triangleleft Aut(G)$.

Bizonyítás. Tegyük fel, hogy $\psi \in Aut(G)$ és $\phi_g \in Inn(G)$. Ekkor a konjugálás definícióját használva kapjuk, hogy

$$\psi\phi_g\psi^{-1}(x) = \psi(g\psi^{-1}(x)g^{-1}) = \psi(g)x\psi(g^{-1}) = \phi_{\psi(g)}(x)$$

így $\psi\phi_g\psi^{-1} = \phi_{\psi(g)}(x)$. □

2.1.3. Definíció. Az $Aut(G)/Inn(G)$ faktorcsoportot a G külső automorfizmuscsoportjának nevezzük, jele $Out(G)$.

2.1.4. Megjegyzés. $Inn(G) \cong G/Z(G)$.
Bizonyítás. *Legyen $\phi : g \to \phi_g$ homomorfizmus, melyre $Ker\phi = Z(G)$ és $Im\phi = Inn(G)$. Így a homomorfizmus tétel miatt $Inn(G) \cong G/Z(G)$.* □

2.2. S_n automorfizmuscsoportja

Ebben az alfejezetben [4]-t követve bebizonyítjuk a 2.2.3 lemmát, továbbá a [6]-t felhasználva fogjuk bizonyítani, hogy egy kivételes esettől eltekintve S_n minden automorfizmusa belső.

2.2.1. Állítás. *Ha $n \geq 3$, akkor $Z(S_n) = 1$.*

Bizonyítás. Legyen x egységelemtől különböző eleme S_n-nek. Ekkor $x = (\alpha\beta\ldots)$ teljesül valamely $\alpha \neq \beta$ elemre. Ha γ egy α-tól és β-tól különböző elem S_n-ben, akkor $g = (\beta\gamma)$ esetén

$$gxg^{-1} = (\beta\gamma)(\alpha\beta\ldots)(\beta\gamma) = (\alpha\gamma\ldots),$$

így $gxg^{-1} \neq x$, amiből már következik, hogy x nem cserélhető fel minden S_n-beli elemmel, tehát $x \notin Z(S_n)$. □

2.2.2. Következmény. *A 2.1.4 megjegyzés alapján ha $n \geq 3$, akkor $Inn(S_n) \cong S_n$, tehát $S_n \leq Aut(S_n)$.*

2.2.3. Lemma. *S_n automorfizmusa akkor és csak akkor belső, ha transzpozíciót transzpozícióba képez.*

Bizonyítás. A belső automorfizmusok megőrzik a ciklusszerkezetet, így a transzpozíciókat is megőrzik.

Az ellenkező irányhoz tegyük fel, hogy $\phi \in Aut(S_n)$ megőrzi a transzpozíciókat. Legyen

$$(12), (23), (34), \ldots, (n-1, n)$$

transzpozíciók sorozata. Ebben a sorozatban minden transzpozíció felcserélhető a többi transzpozícióval, kivéve a mellette lévőkkel. A feltevés szerint $\phi(12) = (ab), \phi(23) = (cd)$. Mivel ezek nem cserélhetők fel egymással, ezért $b = d$. Így az adódik, hogy $\phi(12) = (ab), \phi(23) = (bc)$. Így a $\phi(34)$ transzpozíció szükségszerűen felcserélhető (ab)-vel, de nem cserélhető fel (bc)-vel, így ez tartalmazza c-t és egy új elemet, például d-t. Hasonlóan $\phi(45) = (de)$ valamely e-re. Legyen $\sigma \in S_n$ adott úgy, hogy $\sigma(1) = a, \sigma(2) = b, \sigma(3) = c$, és így tovább. Ekkor ϕ ugyanaz, mint ϕ_σ a fenti transzpozíciókon. Mivel a transzpozíciók generálják S_n-t, ezért $\phi = \phi_\sigma$. □

2.2.4. Tétel. *Ha $n \geq 3$ és $n \neq 6$, akkor S_n automorfizmuscsoportja a belső automorfizmusok csoportja, és ez a csoport S_n-nel izomorf.*

Bizonyítás. A 2.2.1 állítás miatt $Z(S_n) = 1$, így $Aut(S_n) = Inn(S_n) \cong S_n$.

Legyen $n \geq 3$. Az automorfizmusok konjugáltosztályt konjugáltosztályba képeznek, tehát a másodrendű elemek konjugáltosztályait is egymás közt permutálják. Szeretnénk igazolni, hogy a

transzpozíciók osztálya önmagába megy minden automorfizmusnál. Most megnézzük a másodrendű elemek konjugáltosztályainak elemszámát. Jelölje K_1 az egy, és K_k a k darab diszjunkt transzpozíció által meghatározott konjugáltosztályt. Könnyen látható, hogy

$$|K_1| = \binom{n}{2}$$

és

$$|K_k| = \frac{1}{k!}\binom{n}{2}\binom{n-2}{2}\dots\binom{n-2k+2}{2}.$$

Azt vizsgáljuk, hogy milyen esetekben lehet ugyanannyi eleme K_1-nek és K_k-nak, ha $k > 1$.

$$\binom{n}{2} = \frac{1}{k!}\cdot\binom{n}{2}\cdot\binom{n-2}{2}\cdot\dots$$
$$k!\cdot 2^{k-1} = (n-2)\cdot\dots(n-2k+1)$$

Ha $k = 2$, akkor az alábbi egyenlethez jutunk:

$$4 = (n-2)(n-3)$$

Tehát, ha n pozitív egész, akkor nincs megoldása az egyenletnek.

Ha $k = 3$, akkor a

$$24 = (n-2)(n-3)(n-4)(n-5)$$

egyenlethez jutunk. Könnyen ellenőrizhető, hogy $n = 6$ adja az egyenletnek a gyökét.

Ha $k \geq 4$, akkor azt szeretnénk igazolni, hogy

$$k!\cdot 2^{k-1} < (n-2)\cdot\dots(n-2k+1)$$

Ezt k-ra vonatkozó teljes indukcióval bizonyítjuk. A bal oldal független n-től. Vegyük a jobb oldal n-ben vett minimumát, amikor még pozitív az értéke. Ezt akkor kapjuk meg, ha n helyébe $2k$-t írunk. Ekkor az előbbiek alapján:

$$k!\cdot 2^{k-1} < (2k-2)\dots 1$$

Ez ekvivalens a

$$2\cdot 4\cdot\dots\cdot(2k-2)\cdot k < (2k-2)\cdot\dots\cdot 1$$

egyenlőtlenséggel. Ha mindkét oldalt elosztjuk $2\cdot\dots\cdot(2k-2)$-vel, akkor a

$$k < 1\cdot 3\cdot\dots\cdot(2k-3)$$

egyenlőtlenséghez jutunk.

Mivel $k \geq 4$, ezért a

$$k < 2k - 3$$

egyenlőtlenség fennáll, amiből a

$$k < 1 \cdot 3 \cdot \ldots \cdot (2k - 3)$$

egyenlőtlenség is igaz, valamint

$$k > 3$$

is teljesül.

Tehát azt kaptuk, hogy $n \neq 6$ esetén minden automorfizmusra a K_1 konjugáltosztály önmagába képződik, így

$$Aut(S_n) = Inn(S_n) \cong S_n.$$

□

3. fejezet

Az alternáló csoport egyszerűsége

3.1. Bevezetés

Ebben a fejezetben az alternáló csoport egyszerűségét mutatjuk meg ötféleképpen. A fejezet az [1] cikk felépítését követi. Először kimondunk három lemmát. Az első Fried Ervin könyvében [3] szerepel. Ezután [5] alapján kimondjuk az Első izomorfizmustételt. Ezeket majd több bizonyításnál is felhasználjuk. Végül belátjuk, hogy A_5 és A_6, sőt $n \geq 5$ esetén az A_n is egyszerű.

3.1.1. Definíció. Egy véges elemszámú G csoportot egyszerűnek nevezünk, ha csak a triviális normálosztói vannak.

3.1.2. Lemma. *Ha $n \geq 3$, akkor A_n-t generálják a hármas ciklusok.*

Bizonyítás. Először bebizonyítjuk, hogy két transzpozíció szorzatát elő tudjuk állítani ily módon.

1. eset:

Ha a permutáció $(ab)(ab)$ alakban írható fel, ahol a és b különbözők, akkor ez az egységelem.

2. eset:

Ha a permutáció $(ab)(bc)$ alakú, ahol a, b, c különbözők akkor (abc)-vel egyezik meg, amely hármas ciklus.

3. eset:

Ha a permutáció $(ab)(cd)$ alakú, ahol a, b, c, d különböznek egymástól, akkor:

$$(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)$$

Tehát beláttuk, hogy a két transzpozíció szorzataként felírható permutációkat generálják a hármas ciklusok.

Mivel a páros permutációk páros sok transzpozíció szorzataként állnak elő, ezért a páros permutációkat generálják a hármas ciklusok . □

3.1.3. Lemma. *Ha $n \geq 5$, akkor A_n-t az $(ab)(cd)$ alakban felírható permutációk generálják, ahol a, b, c, d különbözők.*

Bizonyítás. Amint az előbb láttuk, A_n-t hármas ciklusok generálják $n \geq 5$ esetén. Azt kell megmutatnunk, hogy egy tetszőleges (abc) hármas ciklus felírható a fenti alakban. Válasszuk úgy d-t és e-t, hogy azok a-tól, b-től és c-től különbözzenek. Ekkor

$$(abc) = (ab)(de)(de)(bc).$$

Ez azt jelenti, hogy bármely hármas ciklus felírható $(ab)(cd)$ alakú permutációk szorzataként. □

3.1.4. Lemma. *Ha $n \geq 5$, akkor A_n-ben bármely két hármas ciklus egymás konjugáltja.*

Bizonyítás. Megmutatjuk, hogy A_n-ben minden hármas ciklusnak konjugáltja az (123). Legyen σ hármas ciklus A_n-ben. Ekkor létezik $\pi \in S_n$, hogy:

$$(123) = \pi\sigma\pi^{-1}$$

Ha $\pi \in A_n$, akkor nincs mit bizonyítanunk. Egyébként legyen $\pi' = (45)\pi$, így $\pi' \in A_n$ és

$$\pi'\sigma\pi'^{-1} = (45)\pi\sigma\pi^{-1}(45) = (45)(123)(45) = (123).$$

□

3.1.5. Tétel. *(Első izomorfizmustétel) Legyen $N \triangleleft G$, és $K \leq G$. Ekkor NK részcsoport G-ben, $K \cap N$ normálosztó K-ban, és*

$$KN/N \cong K/(K \cap N).$$

3.2. Az A_5 és A_6 egyszerűsége

A későbbiekben többször is hivatkozni fogunk a következő tételre.

3.2.1. Tétel. *Az A_5 csoport egyszerű.*

Bizonyítás. Ehhez azt kell bizonyítanunk, hogy az A_5 normálosztói az $\{1\}$ és az A_5. Ezt kétféleképpen tehetjük meg. Most például meghatározzuk a konjugáltosztályok elemszámát és megmutatjuk, hogy a 60 valódi osztói között nincs olyan, amelyet elő tudunk állítani ezeknek az elemszámoknak az összegeként. Az A_5-ben 5 konjugáltosztály van összesen, a reprezentánsokat és az elemszámokat a következő táblázat tartalmazza:

Reprezentáns	(1)	(12345)	(21345)	(12)(34)	(123)
Elemszám	1	12	12	15	20

Ha az A_5-nek van egy N normálosztója, akkor N konjugáltosztályok uniójaként áll elő, amelyek közül az egyik az egységelemet tartalmazó konjugáltosztály. Mivel N normálosztó, ezért az elemszáma osztója a 60-nak. Ha N nemtriviális normálosztó, akkor az 2, 3, 4, 5, 6, 10, 12, 15, 20, vagy 30 elemű lehet. Ezek egyike sem lehet a fenti módon előálló konjugáltosztályok uniójának elemszáma, kivéve az 1-et és a 60-at. Ez azt jelenti, hogy N triviális részcsoport. Tehát A_5 valóban egyszerű csoport. □

Az előző tétel A_5 ciklusszerkezeteinek vizsgálatával is bizonyítható.

Bizonyítás. Legyen $N \triangleleft A_5$ nemtriviális normálosztó. Megmutatjuk, hogy N tartalmaz hármas ciklust. Legyen σ egységelemtől különböző elem N-ben. Ekkor σ ciklusszerkezete (abc), $(ab)(cd)$ vagy $(abcde)$ lehet, ahol a, b, c, d, e különböznek egymástól. Esetszétválasztással megmutatjuk, hogy N tartalmaz hármas ciklust.

1. eset: Ha σ ciklusszerkezete (abc), akkor N tartalmaz hármas ciklust.

2. eset: Ha σ ciklusszerkezete $(ab)(cd)$, akkor N tartalmaz hármas ciklust, mert

$$((abe)(ab)(cd)(abe)^{-1})(ab)(cd) = (be)(cd)(ab)(cd) = (aeb).$$

3. eset: Ha σ $(abcde)$ alakú, akkor N tartalmazza az alábbi ciklust:

$$((abc)(abcde)(abc)^{-1})(abcde)^{-1} = (adebc)(aedcb) = (abd).$$

Tehát N tartalmaz hármas ciklust, így a 3.1.2 lemma miatt $N = A_5$. □

Most megmutatjuk, hogy az A_6 egyszerű csoport. Ezt a 3.4 alfejezetben használjuk fel.

3.2.2. Tétel. *Az A_6 egyszerű csoport.*

Bizonyítás. Ismét konjugáltosztályok segítségével bizonyítunk, ugyanúgy, mint A_5 csoport esetén. A következő táblázat tartalmazza a konjugáltosztályok elemszámát és a reprezentáns elemeket:

Reprezentáns	(1)	(123)	(123)(456)	(12)(34)	(12345)	(23456)	(1234)(56)
Elemszám	1	40	40	45	72	72	90

Ha N nemtriviális normálosztója A_6-nak, akkor az elemszáma osztója a 360-nak. Belátjuk, hogy a konjugáltosztályoknak nem létezik olyan uniója, melynek elemszáma osztja a 360-at. Ez alól csak A_6 és az (1) kivétel. Ezt úgy állapítjuk meg, hogy vesszük 360-nak a 40-nél nem kisebb osztóit. Ezek a 40, 45, 60, 72, 90, 120, 180. Ezek a számok nem állíthatók elő összegként

a konjugáltosztályok elemszámaiból úgy, hogy az egységelemet tartalmazó konjugáltosztályt is használjuk. Beláttuk tehát, hogy A_6 egyszerű csoport. □

A 3.2.2 tétel A_6 ciklusszerkezeteinek elemzése alapján is bizonyítható.

Bizonyítás. Legyen $N \triangleleft A_6$ nemtriviális normálosztó, és legyen $\sigma \in N$ egységelemtől különböző elem. Megmutatjuk, hogy N tartalmaz hármas ciklust. Ekkor σ lehetséges ciklusszerkezetei $(abc), (abcde), (abcd)(ef), (ab)(cd), (abc)(def)$ alakúak lehetnek, ahol a, b, c, d, e, f különbözők. A lehetséges ciklusszerkezetek alapján végezzük el az esetszétválasztást.

1. eset: Ha σ (abc) alakú, akkor N tartalmaz hármas ciklust.

2. eset: Ha σ $(abcde)$ alakú, akkor az A_5 esetnél láttuk, hogy N tartalmaz hármas ciklust.

3. eset:

Ha $\sigma = (abc)(def)$, akkor σ két diszjunkt hármas ciklus szorzata, így N-ben található hármas ciklus.

4. eset:

Ha $\sigma = (ab)(cd)$, akkor az A_5 esetben látottak alapján N tartalmaz hármas ciklust.

5. eset:

Ha $\sigma = (abcd)(ef)$, akkor

$$((abc)(abcd)(ef)(abc)^{-1})((ef)^{-1}(abcd)^{-1}) = (abd),$$

így ebben az esetben is van hármas ciklus N-ben.

Mivel minden esetben van hármas ciklus N-ben, ezért $N = A_6$ a 3.1.2 lemma miatt. Tehát A_6 egyszerű.

□

Az $n \geq 5$ feltétel szükséges, ugyanis A_4 nem egyszerű csoport. Az A_4-nek van 4 elemből álló normálosztója, mégpedig $\{(1), (12)(34), (13)(24), (14)(23)\}$. Ez a Klein-csoporttal izomorf. Az A_3 csoport egyszerű, mivel 3 eleme van és három elemű csoportnak csak 2 részcsoportja van. Az A_1 és A_2 csoportok triviálisak.

3.3. Az A_n egyszerűségének bizonyítása konjugált elemek segítségével

Ehhez a bizonyításához fel fogjuk használni a következő lemmát.

3.3.1. Lemma. *Ha $n \geq 5$, akkor bármely identitástól különböző σ elemnek létezik olyan σ' konjugáltja A_n-ben, melyre $\sigma' \neq \sigma$, továbbá az $\{1,2,\ldots,n\}$ halmaznak létezik olyan eleme, amelynek σ-nál és σ'-nél vett képe megegyezik.*

Bizonyítás. Legyen σ az A_n csoport egységelemtől különböző eleme. Jelölje r a σ-ban lévő leghosszabb diszjunkt ciklus hosszát. Ekkor feltehető, hogy

$$\sigma = (12 \dots r)\pi,$$

ahol $(12 \dots r)$ és π diszjunktak. Csoportosítsuk az eseteket a lehetséges r értékek szerint.

1. eset: Ha $r \geq 3$, akkor legyen $\tau = (345)$ és $\sigma' = \tau\sigma\tau^{-1}$. Ekkor

$$\sigma' = (1246 \dots r),$$

így $\sigma' \neq \sigma$ továbbá σ és σ' képe az 1-ben megegyezik.

2. eset: Ha $r = 2$, akkor σ egymástól diszjunkt transzpozíciók szorzata. Legalább 3 diszjunkt transzpozíció esetén feltehető, hogy $\sigma = (12)(34)(56)(\dots)$. Legyen $\tau = (12)(35)$ és $\sigma' = \tau\sigma\tau^{-1}$. Ekkor

$$\sigma' = (12)(36)(45)(78) \dots (n-1, n),$$

azaz $\sigma' \neq \sigma$ és ezek képe megegyezik 1-ben.

3. eset: Ha $r = 2$ és σ pontosan 2 diszjunkt transzpozíció szorzatát tartalmazza, akkor feltehető, hogy $\sigma = (12)(34)$. Legyen $\tau = (132)$. Ekkor

$$\sigma' = (13)(24),$$

következésképpen $\sigma' \neq \sigma$, továbbá mindkét kifejezésben az 5 fixpont. □

3.3.2. Tétel. *Ha $n \geq 5$, akkor A_n egyszerű.*

Bizonyítás. Az A_5 egyszerűségét beláttuk, ezért feltehetjük, hogy $n \geq 6$. Legyen $H_i \subset A_n$ olyan részcsoport, amely stabilizálja i-t, így $H_i \cong A_{n-1}$, mert H_i az

$$\{1,2, \dots, (i-1), (i+1), \dots n\}$$

halmaz páros permutációiból álló csoport. Teljes indukcióval bizonyítjuk, így feltehető, hogy minden H_i egyszerű. Először megmutatjuk, hogy H_i tartalmaz hármas ciklust.

Legyen $N \triangleleft A_n$ egy nemtriviális normálosztó. Azt szeretnénk megmutatni, hogy $N = A_n$. Legyen σ egységelemtől különböző eleme N-nek. A 3.3.1 lemma miatt van olyan σ' konjugáltja σ-nak, amelyre $\sigma' \neq \sigma$ és az $\{1,2, \dots, n\}$ valamely i eleménél vett képük megegyezik. Mivel $\sigma \in N$, ezért $\sigma' \in N$ is fennáll. Ekkor $\sigma^{-1}\sigma'$ egy nemtriviális eleme N-nek, amely helybenhagyja i-t, így $N \cap H_i$ nemtriviális. A 3.1.5 tétel miatt $N \cap H_i$ normálosztója H_i-nek. Mivel $N \cap H_i$ nemtriviális, és H_i egyszerű, ezért $N \cap H_i = H_i$, amiből már következik, hogy $H_i \subset N$. Mivel H_i tartalmaz hármas ciklust, így N is tartalmaz hármas ciklust, tehát $N = A_n$ a 3.1.2 lemma miatt. □

3.4. Az A_n egyszerűségének bizonyítása A_6 egyszerűségének felhasználásával

A 3.2.2 tételben beláttuk A_6 egyszerűségét, most ezt felhasználva fogjuk belátni a következő tételt.

3.4.1. Tétel. *Ha $n \geq 5$, akkor A_n egyszerű.*

Bizonyítás. Mivel tudjuk, hogy A_5 és A_6 egyszerű, ezért a tételt $n \geq 7$ esetén szeretnénk bizonyítani. Legyen $N \triangleleft A_n$ egy nem triviális normálosztó. Megmutatjuk, hogy N tartalmaz hármas ciklust.

Legyen $\sigma \neq (1) \in N$. Ekkor feltehetjük, hogy $\sigma(1) \neq 1$. Legyen $\tau = (ijk)$, ahol i, j, k egyike sem 1, és $\sigma(1) \in \{i, j, k\}$. Ekkor

$$\tau\sigma\tau^{-1}(1) = \tau(\sigma(1)) \neq \sigma(1),$$

így $\tau\sigma\tau^{-1} \neq \sigma$. Legyen

$$\varphi = \tau\sigma\tau^{-1}\sigma^{-1},$$

így $\varphi \neq (1)$. Ekkor felírhatjuk φ-t a következő alakban:

$$\varphi = (\tau\sigma\tau^{-1})\sigma^{-1},$$

Nyilvánvaló, hogy $\varphi \in N$. Az asszociativitás miatt:

$$\varphi = \tau(\sigma\tau^{-1}\sigma^{-1}).$$

Mivel τ^{-1} hármas ciklus, $\sigma\tau^{-1}\sigma^{-1}$ is hármas ciklus az 1.1.23 tétel alapján. Tehát φ 2 darab hármas ciklus szorzata, így φ legfeljebb 6 számot permutál az $\{1,2,\ldots,n\}$ halmazon. Feltehető, hogy ezek az 1,2,3,4,5,6. Legyen

$$H = \{\sigma \in A_n \mid Supp\ \sigma \subseteq \{1,2,3,4,5,6\}\}$$

ezen 6 szám páros permutációinak a halmaza az A_n-en belül. Ez részcsoportot alkot A_n-ben. Ekkor $N \cap H$ nemtriviális, mert tartalmazza φ-t, továbbá H-nak a normálosztója a 3.1.5 tétel miatt. Mivel $H \cong A_6$, amelyről tudjuk, hogy egyszerű, ezért $N \cap H = H$. Tehát $H \subset N$, így N tartalmaz hármas ciklust. Következésképpen $N = A_n$ a 3.1.2 lemma miatt. $\square$

3.5. Az A_n egyszerűségének bizonyítása konjugáltosztályok felhasználásával

A bizonyításhoz a következő lemmát fogjuk felhasználni.

3.5.1. Lemma. *Ha $n \geq 6$, akkor a nemtriviális konjugáltosztályok S_n-ben és A_n-ben legalább n eleműek.*

Bizonyítás. Legyen $n \geq 6$, és $\sigma \in S_n$, ahol $\sigma \neq (1)$. Megvizsgáljuk σ konjugáltosztályát S_n-ben, illetve A_n-ben, hogy legalább n különböző konjugáltat találjunk. Bontsuk fel σ-t diszjunkt ciklusok szorzatára.

Ekkor 3 eset lehetséges:

1. eset: A σ diszjunkt ciklusfelbontása tartalmaz 2-nél hosszabb ciklust. Az általánosság megszorítása nélkül legyen $\sigma = (123\ldots)\ldots$.

Ha $3 \leq k \leq n$, akkor rögzítsünk egy l-et, ahol $l \notin \{1,2,3,k\}$, és legyen $\alpha_k = (2kl)$, valamint $\beta_k = (3kl)$. Ha $k = 3$, akkor $\beta_k = (1)$.

Ekkor az $\alpha_k \sigma \alpha_k^{-1}$ szorzat

$$(1k\ldots).$$

Ha $k = 3$, akkor $\beta_k \sigma \beta_k^{-1}$:

$$(123\ldots).$$

Ha $k > 3$, akkor $\beta_k \sigma \beta_k^{-1}$ értéke pedig

$$(12k\ldots).$$

Tehát a konjugáltak különböznek egymástól, mert az $\alpha_k \sigma \alpha_k^{-1}$ konjugáltak képe az 1-ben nem egyezik meg, a $\beta_k \sigma \beta_k^{-1}$ konjugáltak képe pedig nem azonos a 2-ben, és $\alpha_k \sigma \alpha_k^{-1} \neq \beta_k \sigma \beta_k^{-1}$ is teljesül, mert 1-ben a képük különböző. Mivel a fentebb kapott konjugáltak különbözők, ezért a konjugáltak száma legalább $2(n-2)$, amely n-nél nagyobb, ha $n \geq 6$. Ha $\sigma \in A_n$, akkor ezek a konjugáltak a σ A_n-beli konjugáltosztályában vannak benne.

2. eset: σ diszjunkt ciklusfelbontása csak 1 vagy 2 hosszú ciklust tartalmaz. Tehát az általánosság megszorítása nélkül σ transzpozíció vagy legalább 2 diszjunkt transzpozíció szorzata. Ha σ egy transzpozíció, akkor az S_n konjugáltosztályának a halmaza az összes (ij) transzpozícióból áll, ahol $1 \leq i < j \leq n$ és ezeknek a permutációknak a száma $\binom{n}{2} = \frac{n(n-1)}{2}$, amely nagyobb, mint n, ha $n \geq 6$.

3. eset: Ha σ legalább 2 diszjunkt transzpozíció szorzata, akkor $\sigma = (12)(34)\ldots$.

Ha $5 \leq k \leq n$, akkor legyen $\alpha_k = (12)(3k)$, $\beta_k = (13)(2k)$ és $\gamma_k = (1k)(23)$.

Ekkor

$\alpha_k\sigma\alpha_k^{-1}$ értéke

$$(12)(k4),$$

a $\beta_k\sigma\beta_k^{-1}$ szorzat

$$(14)(3k)$$

és a $\gamma_k\sigma\gamma_k^{-1}$ szorzás után

$$(24)(3k)$$

adódik.

Az $\alpha_k\sigma\alpha_k^{-1}$ konjugáltak mind különböznek egymástól, mert különböző elemeket képeznek 4-be. A $\beta_k\sigma\beta_k^{-1}$ konjugáltjak mindegyike különbözik egymástól, mert különböző elemeket rendelnek 3-hoz. A $\gamma_k\sigma\gamma_k^{-1}$ tagok különbözők, mert különböző elemeket rendelnek 3-hoz.

Az $\alpha_k\sigma\alpha_k^{-1} \neq \beta_k\sigma\beta_k^{-1}$ feltétel azért teljesül, mert az 1-et különböző helyekre viszik. Az $\alpha_k\sigma\alpha_k^{-1} \neq \gamma_k\sigma\gamma_k^{-1}$ is igaz, mert a 2 képe különböző ezen konjugáltak esetén. Végül a $\beta_k\sigma\beta_k^{-1}$ és a $\gamma_k\sigma\gamma_k^{-1}$ konjugáltak sem egyeznek meg egymással, mert a 4 képe különböző ezeknek a konjugáltaknak. Így megkaptuk σ mindegyik konjugáltját, melyeknek száma $3(n-4)$, és $3(n-4) \geq n$ igaz $n \geq 6$ esetén. □

3.5.2. Tétel. *Ha $n \geq 5$, akkor A_n egyszerű.*

Bizonyítás. Korábban láttuk, hogy $n = 5$ esetén A_n egyszerű, ezért indukcióval bizonyítjuk $n \geq 6$-ra. Legyen N nemtriviális normálosztó A_n-ben. Ekkor N tartalmaz egységelemtől különböző konjugáltosztályokat A_n-ben. A 3.5.1 lemma alapján bármely nem az egységelemet tartalmazó konjugáltosztály A_n-ben legalább n elemű, ha $n \geq 6$. Tehát a triviális konjugáltosztály és a nemtriviális konjugáltosztály uniójának elemszáma legalább $n+1$. Ugyanakkor meg fogjuk mutatni, hogy ha $N \neq A_n$, akkor $|N| \leq n$.

Legyen $1 \leq i \leq n$, és legyen $H_i \subset A_n$ az i-t stabilizáló elemek részcsoportja, így $H_i \cong A_{n-1}$. H_i egyszerű csoport az indukciós feltevés miatt. Az $N \cap H_i$ normálosztója H_i-nek a 3.1.5 tétel alapján, így H_i egyszerűsége miatt $N \cap H_i$ vagy $\{(1)\}$, vagy H_i lehet. Ha $N \cap H_i = H_i$ valamely i-re, akkor $H_i \subset N$. Mivel H_i tartalmaz hármas ciklust, ezért N is tartalmaz, így $N = A_n$ a 3.1.2 lemma miatt.

Legyen $N \neq A_n$. Ekkor $N \cap H_i = \{(1)\}$ minden i-re. Ekkor minden egységelemtől különböző N-beli σ elemre teljesül, hogy a $\{1,2,\ldots n\}$ halmazon nincsen fixpontja. Legyen $\tau \in N$ és $\tau \neq (1)$, továbbá tegyük fel, hogy $\sigma(1) = \tau(1)$. Ekkor $\sigma^{-1}\tau(1) = (1)$, amiből az következik, hogy $\sigma^{-1}\tau(1) \in H_1 \cap N$, tehát $\sigma^{-1}\tau$ az egységelem, így $\sigma = \tau$.

A $\sigma(1)$-nek $n-1$ lehetséges értéke van: $\sigma(1) \in \{2,3,\ldots,n\}$, így az előzőek szerint, $N - \{(1)\}$ elemszáma legfeljebb $n-1$. Mivel 1 képe maximum n-féle lehet, ezért $|N| \leq n$. Mivel korábban beláttuk, hogy $|N| \geq n+1$, ezért ellentmondást kaptunk. Tehát $N = A_n$, azaz A_n egyszerű. □

3.6. Az A_n egyszerűségének bizonyítása hármas ciklusok konstruálásával

Ebben az alfejezetben megmutatjuk, hogy az A_n normálosztója tartalmaz hármas ciklust, így a 3.1.2 lemma miatt megegyezik A_n-nel.

3.6.1. Tétel. *Ha $n \geq 5$, akkor A_n egyszerű.*

Bizonyítás. Legyen $N \triangleleft A_n$ egy nemtriviális normálosztó. Megmutatjuk, hogy N tartalmaz hármas ciklust. Legyen σ egységelemtől különböző eleme N-nek.

Írjuk fel σ-t diszjunkt ciklusok szorzataként a következőképpen:

$$\sigma = \pi_1 \pi_2 \dots \pi_k,$$

A fenti felírásban a π_i-k felcserélhetők, hiszen diszjunktak, továbbá az 1 hosszú ciklusok elhagyhatóak anélkül, hogy a permutáció megváltozna. A továbbiakban aszerint csoportosítjuk az eseteket, hogy az ezután megmaradt ciklusok milyen hosszúak lehetnek.

1. eset: Létezik olyan π_i, amelynek a hossza legalább 4. Legyen ez π_1. Jelöljük ennek a hosszát r-rel. Nyilván feltehető, hogy:

$$\pi_1 = (12 \dots r)$$

Legyen $\varphi = (123)$. Ekkor $\varphi\sigma\varphi^{-1} \in N$, mert N zárt a konjugálásra, így

$$\varphi\sigma\varphi^{-1} = \varphi\pi_1\varphi^{-1}\varphi\pi_2\varphi^{-1} \dots \varphi\pi_k\varphi^{-1}$$

A fenti felírásban φ^{-1} felcserélhető a $\pi_2, \dots \pi_k$ elemekkel, mert diszjunkt tőlük. Így azt kapjuk, hogy

$$\varphi\sigma\varphi^{-1} = \varphi\pi_1\varphi^{-1}\pi_2 \dots \pi_k.$$

Mivel $\pi_2 \dots \pi_k = \pi_1^{-1}\sigma$, ezért

$$\varphi\sigma\varphi^{-1} = \varphi\pi_1\varphi^{-1}\pi_1^{-1}\sigma.$$

Behelyettesítés után adódik a következő felírás:

$$(123)(123 \dots r)(132)(r \dots 321)\sigma.$$

A korábbiak alapján:

$$\varphi\sigma\varphi^{-1} = (124)\sigma,$$

tehát $\varphi\sigma\varphi^{-1}\sigma^{-1} = (124)$. Mivel $\sigma \in N$, így $\varphi\sigma\varphi^{-1}\sigma^{-1} \in N$, tehát $(124) \in N$, ami azt jelenti, hogy N tartalmaz hármas ciklust.

2. eset: Minden π_i hossza legfeljebb 3 és legalább 2-nek a hossza pontosan 3. Az általánosság megszorítása nélkül választhatjuk π_1-et és π_2-t a következőképpen: $\pi_1 = (123)$ és $\pi_2 = (456)$.

Legyen $\varphi = (124)$. Ekkor:

$$\varphi\sigma\varphi^{-1} = \varphi\pi_1\varphi^{-1}\varphi\pi_2\varphi^{-1}\varphi\pi_3\varphi^{-1}\dots\varphi\pi_k\varphi^{-1}$$

Ebben a felírásban φ^{-1} felcserélhető a $\pi_3, \dots \pi_k$ elemekkel, mert ezek mindegyikétől diszjunkt. Ekkor

$$\varphi\sigma\varphi^{-1} = \varphi\pi_1\varphi^{-1}\varphi\pi_2\varphi^{-1}\pi_3\dots\pi_k = \varphi\pi_1\pi_2\varphi^{-1}\pi_3\dots\pi_k$$

Mivel $\pi_3\dots\pi_k = \pi_2^{-1}\pi_1^{-1}\sigma$, így

$$\varphi\sigma\varphi^{-1} = \varphi\pi_1\pi_2\varphi^{-1}\pi_2^{-1}\pi_1^{-1}\sigma.$$

Ha ebbe behelyettesítünk, akkor

$$\varphi\sigma\varphi^{-1} = (124)(123)(456)(142)(654)(132)\sigma$$

adódik. A műveletek elvégzése után kapjuk, hogy:

$$\varphi\sigma\varphi^{-1}\sigma^{-1} = (12534).$$

Mivel $\varphi\sigma\varphi^{-1}\sigma^{-1} \in N$, így $(12534) \in N$ adódik. Erre az első esetet alkalmazva azt kapjuk, hogy:

$$\varphi\sigma\varphi^{-1}\sigma^{-1} = (124)(12534)(421)(43521) = (154).$$

Tehát ebben az esetben is tartalmaz N hármas ciklust.

3. eset: Pontosan egy π_i létezik, amelynek a hossza 3, és a többi hossza legfeljebb 2. Az általánosság megszorítása nélkül legyen $\pi_1 = (123)$ és a többi π_i 2-es ciklus. Ha a

$$\sigma = (123) \cdot \pi_2 \cdot \dots \cdot \pi_k$$

kifejezést négyzetre emeljük, akkor a másodrendű elemek négyzete 1, és $\sigma^2 = \pi_1^2 = (132) \in N$ adódik, tehát N-ben van hármas ciklus.

4. eset: Minden π_i 2-ciklus. Legyen $\pi_1 = (12)$ és $\pi_2 = (34)$, valamint legyen $\varphi = (123)$. Ekkor

$$\varphi\sigma\varphi^{-1} = \varphi\pi_1\pi_2\varphi^{-1}\pi_3\dots\pi_k$$

mert φ^{-1} felcserélhető $\pi_3, \dots \pi_k$ mindegyikével. Így kapjuk a

$$\varphi\sigma\varphi^{-1} = (123)(12)(34)(132)(34)(12)\sigma$$

eredményt. Ebből:

$$\varphi\sigma\varphi^{-1}\sigma^{-1} = (13)(24),$$

tehát $(13)(24) \in N$ teljesül.

Most erre a következőt alkalmazzuk:

Legyen $\Psi = (135)$.

Ekkor

$$(13)(24)\Psi(13)(24)\Psi^{-1} = (13)(24)(135)(13)(24)(153),$$

amely ugyanaz, mint

$$(13)(24)\Psi(13)(24)\Psi^{-1} = (13)(135)(13)(153).$$

Ekkor

$$(13)(24)\Psi(13)(24)\Psi^{-1} = (135),$$

így N tartalmaz hármas ciklust.

Tehát azt kaptuk mind a négy esetben, hogy N tartalmaz hármas ciklust, így a 3.1.2 lemma alapján $N = A_n$. □

3.7. Az A_n egyszerűségének bizonyítása normalizátorok segítségével

A következő lemmát az 5. bizonyításban alkalmazzuk.

3.7.1. Lemma. *Ha $n \geq 5$, akkor S_n egyetlen nemtriviális normálosztója az A_n, és ez az egyetlen 2 indexű részcsoportja S_n-nek.*

Bizonyítás. Legyen N nemtriviális normálosztója S_n-nek. Megmutatjuk, hogy $A_n \subset N$, így $N = A_n$, vagy $N = S_n$. Legyen σ egységelemtől különböző elem N-ben. Ekkor létezik olyan $i \in \{1,2 \dots, n\}$, amelyre $\sigma(i) \neq i$. Válasszunk egy j elemet az $\{1,2, \dots, n\}$ halmazból úgy, hogy $j \neq i$ és $j \neq \sigma(i)$. Legyen $\tau = (ij)$. Ekkor

$$\sigma\tau\sigma^{-1}\tau^{-1} = (\sigma(i)\sigma(j)(ij)$$

Itt $\sigma(i) \neq \sigma(j)$, mert $i \neq j$. A $\sigma\tau\sigma^{-1}\tau^{-1}$ nem egységelem, ezért σ és τ egymással nem fölcserélhetők. A $\sigma\tau\sigma^{-1}\tau^{-1}$ elem N-beli, mert σ és σ^{-1} konjugáltja is benne van. Ha $\sigma(i)$ és $\sigma(j)$ egyike sem egyenlő i-vel és j-vel, akkor a két ciklus diszjunkt és így $(ab)(cd)$ szerkezetű. Különben a két ciklusnak van egy darab közös eleme és így szorzatuk egy hármas ciklus. N normálosztó, így teljes konjugáltosztályokat tartalmaz. Ha kettő permutációnak megegyezik a ciklusszerkezete, akkor azok konjugáltak S_n-ben. Ekkor a 3.1.2 lemma miatt A_n-t az ilyen típusú permutációk kigenerálják, tehát N tartalmazza az alternáló csoportot.

Mivel a 2 indexű részcsoportok normálosztók, és mert beláttuk, hogy S_n egyetlen nemtriviális normálosztója A_n, így A_n az egyetlen 2 indexű részcsoport is. □

Most definiáljuk a normalizátor fogalmát, melynek segítségével újabb bizonyítást kaphatunk A_n egyszerűségére.

3.7.2. Definíció. Legyen H részcsoportja a G csoportnak. Ekkor azoknak a $g \in G$ elemek halmazát, melyekre $gH = Hg$, a H részcsoport G-beli normalizátorának nevezzük.

3.7.3. Tétel. *Ha $n \geq 5$, akkor A_n egyszerű.*

Bizonyítás. Legyen N nemtriviális normálosztó A_n-ben. A 3.7.1 lemma miatt N nem normálosztó S_n-ben. Mivel N részcsoportja A_n-nek, és A_n részcsoport S_n-ben, így N részcsoport S_n-ben igaz, mert a részcsoportnak lenni tulajdonság tranzitív. Tehát a normalizátor definíciója alapján, és mivel a normalizátor a legnagyobb olyan részcsoport, amiben N normálosztó, így az

$$A_n = N_{S_n}(N)$$

eredményhez jutunk.

Legyen τ tetszőleges transzpozíció. Ekkor $\tau \notin N_{S_n}(N)$, így $\tau N\tau^{-1} \neq N$. A $\tau N\tau^{-1}$ részcsoportja A_n-nek, mert tetszőleges elemmel való konjugálás automorfizmust eredményez. A 3.1.5 tétel miatt teljesül, hogy $N \cdot \tau N\tau^{-1}$ részcsoportja A_n-nek. Az előzőek alapján a következők teljesülnek:

$$N \cap \tau N\tau^{-1} \subset N \subset N \cdot \tau N\tau^{-1} \subset A_n.$$

Szeretnénk igazolni, hogy bármely S_n-beli τ transzpozíció esetén:

$$N \cap \tau N\tau^{-1} \lhd S_n, \;\; N \cdot \tau N\tau^{-1} \lhd S_n. \tag{3.1}$$

Ha ugyanis ezt beláttuk, akkor a tétel könnyen adódik, ugyanis a 3.1-ből a 3.7.1 alapján:

$$N \cap \tau N\tau^{-1} = \{(1)\}, \;\; N \cdot \tau N\tau^{-1} = A_n \tag{3.2}$$

bármely $\tau \in S_n$ transzpozíció esetén. Az A_n elemszáma:

$$|A_n| = \left|N\tau N\tau^{-1}\right| = |N|^2 .$$

Tudjuk, hogy $|S_n| = 2 \cdot |A_n|$, és $|S_n| = n!$, tehát

$$n! = 2\,|N|^2$$

Ha $n \geq 5$, akkor az $n!$ értéke 8-cal osztható. Ez pedig azt jelenti, hogy N elemszáma páros, azaz N-nek létezik olyan σ eleme, amely másodrendű. Ekkor σ diszjunkt kettes ciklusok szorzata.

Legyen ρ olyan transzpozíció, amely σ diszjunkt ciklusfelbontásában szerepel. Ekkor

$$\sigma = \rho\sigma\rho^{-1} \in N \cap \rho N\rho^{-1}.$$

Tehát $N \cap \rho N\rho^{-1}$ legalább kételemű, de $N \cap \rho N\rho^{-1}$ triviális a 3.2 miatt, így ellentmondást kaptunk. Ez tehát igazolja a tétel állítását.

Az maradt hátra, hogy megmutassuk, a 3.1-ben szereplő mindkét részcsoport normálosztó S_n-ben. Ha a 3.1-ben szereplő részcsoportokról meg tudjuk mutatni, hogy a normalizátoruk S_n, akkor abból már következik, hogy normálosztók is S_n-ben.

Először vizsgáljuk meg a $N \cap \tau N\tau^{-1}$ részcsoportot. Ezt τ normalizálja, mert

$$\tau(N \cap \tau N\tau^{-1})\tau^{-1} = \tau N\tau^{-1} \cap \tau^2 N\tau^{-2} = \tau N\tau^{-1} \cap N.$$

Utóbbi egyenlőség azért teljesül, mert τ transzpozíció, és transzpozíciók négyzete 1. Így:

$$N \cap \tau N\tau^{-1} = \tau N\tau^{-1} \cap N.$$

Most legyen $\pi \in A_n$ tetszőleges elem. Ekkor $\pi N\pi^{-1} = N$ teljesül. Most $\tau N\tau^{-1}$-t konjugáljuk π-vel, és $\tau\tau^{-1}$-gyel szorozzuk balról és jobbról. Ekkor

$$\pi(\tau N\tau^{-1})\pi^{-1} = \tau(\tau^{-1}\pi\tau)N(\tau^{-1}\pi^{-1}\tau)\tau^{-1} = \tau N\tau^{-1} \tag{3.3}$$

adódik. Ekkor az utolsó egyenlőség igaz, mert a $\tau^{-1}\pi\tau$ és a $\tau^{-1}\pi^{-1}\tau$ elemek egymás inverzei. Következésképpen

$$\pi(N \cap \tau N\tau^{-1})\pi^{-1} = \pi N\pi^{-1} \cap \pi\tau N\tau^{-1}\pi^{-1} = N \cap \tau N\tau^{-1},$$

tehát A_n normalizálja $N \cap \tau N\tau^{-1}$-t. Tehát a normalizátor tartalmazza S_n-t az 1.1.20 tétel miatt.

Most nézzük meg az $N \cdot \tau N\tau^{-1}$ részcsoportot. Vegyünk ebből a csoportból egy elemet, például a

$$\sigma = \sigma_1\tau\sigma_2\tau^{-1}$$

elemet, ahol $\sigma_1, \sigma_2 \in N$. Mivel $N \lhd A_n$, így

$$\tau\sigma\tau^{-1} = \tau\sigma_1\tau\sigma_2\tau^{-2} = \tau\sigma_1\tau\sigma_2 \in \tau N\tau^{-1} \cdot N.$$

Ha $N \cdot \tau N\tau^{-1}$-t konjugáljuk τ-val, akkor

$$\tau(N \cdot \tau N\tau^{-1})\tau^{-1} = \tau N\tau^{-1} \cdot N$$

adódik.

Mivel

$$N \cdot \tau N\tau^{-1} = \tau N\tau^{-1} \cdot N$$

nyilván teljesül, ezért τ normalizálja a $N \cdot \tau N\tau^{-1}$ részcsoportot.

Most vegyünk egy $\pi \in A_n$ elemet. Annak megmutatására, hogy π normalizálja $N \cdot \tau N\tau^{-1}$-t, vegyük σ-t úgy, mint az előbb. Ekkor

$$\pi\sigma\pi^{-1} = \pi\sigma_1\pi^{-1} \cdot \pi(\tau\sigma_2\tau^{-1})\pi^{-1}.$$

Az első tényező N-beli, mert $\sigma_1 \in N$. A második tényező eleme a $\pi\tau N\tau^{-1}\pi^{-1}$ halmaznak, amelyről láttuk, hogy megegyezik $\tau N\tau^{-1}$-gyel a 3.3 miatt. Így ennek a részcsoportnak is S_n a normalizátora a 1.1.20 tétel alapján. □

4. fejezet

Maximális elemrend a véges elemszámú szimmetrikus csoportban

Ebben a fejezetben azt vizsgáljuk a [7] cikket feldolgozva, hogy mekkora lehet S_n-ben a permutáció maximális elemrendje.

4.1. Bevezetés

4.1.1. Definíció. Legyen G tetszőleges csoport. Egy $g \in G$ elem rendje a g különböző hatványainak a száma.

4.1.2. Megjegyzés. *Egy permutáció rendje S_n-ben a diszjunkt ciklushosszak legkisebb közös többszöröse.*

4.1.3. Definíció. Legyenek f és g tetszőleges függvények, ahol $g \neq 0$. Azt mondjuk, hogy f aszimptotikusan egyenlő g-vel, azaz $f \sim g$, ha $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

Jelöljük az S_n-beli permutációk maximális rendjét $G(n)$-nel. A fejezet célja annak megmutatása, hogy

$$\ln G(n) \sim \sqrt{n \cdot \ln n}. \tag{4.1}$$

A 4.1 bizonyításához felhasználjuk a prímszámtételt:

4.1.4. Tétel. *Legyen x pozitív egész szám. Jelölje $\pi(x)$ az x-ig terjedő prímszámok számát. Ekkor*

$$\pi(x) \sim \frac{x}{\ln(x)}.$$

4.2. Adott rendű permutációk és a prímtényezős felbontás kapcsolata

Vizsgáljunk egy S_n-beli m-rendű permutációt. Legyen az m prímfelbontása $\prod_{j=1}^{s} q_j^{e_j}$.

A 4.1.2 megjegyzésben szerepelt, hogy egy S_n-beli permutáció rendje a diszjunkt ciklushosszak legkisebb közös többszöröse, amely jelen esetben $\prod_{j=1}^{s} q_j^{e_j} = m$.

Most definiálunk egy S függvényt, amit még később használni fogunk.

4.2.1. Definíció. Legyen az S pozitív egész számokon értelmezett függvény, amelyre $S(1) = 1$ és $m > 1$ esetén $S(m) = \sum_{j=1}^{s} q_j^{e_j}$, ahol $\prod_{j=1}^{s} q_j^{e_j}$ az m szám prímfelbontása.

Az $S(m)$ definíciója miatt szükséges, hogy legyen legalább $S(m)$ darab különböző elem, amelyet felhasználhatunk egy permutáció megkonstruálásához. Azt szeretnénk tehát megmutatni, hogy nem tudunk m-edrendű elemet létrehozni $S(m)$-nél kevesebb különböző elem felhasználásával. Ebben a következő lemma segít nekünk.

4.2.2. Lemma. *Legyenek $a_1, \dots a_k$ pozitív egész számok, és legyen m a legkisebb közös többszörösük. Ekkor $S(m) \leq \sum_{i=1}^{k} a_i$.*

Bizonyítás. Indirekt módon tegyük fel, hogy $[a_1, \dots a_k] = m$ és $S(m) > \sum_{i=1}^{k} a_i$. Vegyünk minimális ellenpéldát, azaz legyen $\sum_{i=1}^{k} a_i$ minimális.

A bizonyítást több lépésben végezzük el.

1. lépés: Az $a_1, \dots a_k$ kifejezések egyike sem 1. Ha az a_i-k között szerepelne az 1, akkor azokat az a_i kifejezés(ek)et elhagyhatjuk, így kapunk egy olyan $a_1, \dots a_k$ sorozatot, amelynek az összege kisebb, mint $\sum_{i=1}^{k} a_i$, de továbbra is m az $a_1, \dots a_k$ számok legkisebb közös többszöröse. Ez ellentmond a minimalitásnak.

2. lépés: Minden $a_1 \dots a_k$ kifejezés prímhatvány. Ha ez nem teljesül, akkor létezik olyan a_i kifejezés, például a_1, amelyet felírhatunk két relatív prím, s és t szorzataként, ahol $s, t > 1$. Feltehetjük, hogy $t > s$. Ekkor:

$$s + t < 2 \cdot t \leq s \cdot t$$

Tehát a_1 törlésével, valamint t és s beszúrásával kapnánk egy új sorozatot kisebb összeggel, viszont a legkisebb közös többszörös továbbra is m, amely ugyanaz, mint $a_1 \dots a_k$ legkisebb közös többszöröse. Ez is ellentmond a minimalitásnak.

3. lépés: Végül megmutatjuk, hogy az $a_1 \dots a_k$ kifejezések különböző prímhatványok. Ha a_i és a_j azonos prímnek a hatványa, akkor a kisebb elhagyásával kapunk egy új sorozatot,

amelynek az összege kisebb, de a legkisebb közös többszörös mégis megegyezik $a_1 \dots a_k$ legkisebb közös többszörösével. Ebből az következik, hogy $\sum_{i=1}^{k} a_i = S(m)$. Tehát ebben az esetben sem találtunk ellenpéldát. □

4.2.3. Állítás. *S_n-ben létezik m-edrendű elem, ha $S(m) \leq n$.*

Bizonyítás. Világos, hogy $S_{S(m)}$-ben van m-rendű elem, és ekkor $S(n)$-ben is van ilyen elem minden $n \geq S(m)$-re.

Ha S_n-ben van m-rendű elem, és ennek a ciklusfelbontása $(a_1, \dots a_k)$, akkor egyrészt $\sum_{i=1}^{n} a_i \leq n$, másrészt $[a_1, \dots a_n] = m$ miatt a 4.2.2 lemma alapján:

$$n \geq \sum_{i=1}^{n} a_i \geq S(m).$$

□

4.3. F(n) és G(n) közötti összefüggések

Az alábbiakban bevezetjük a P-t, és az $F(n)$ függvényt, amelyeket később használni fogunk. Az $F(n)$ olyan függvény, amely könnyebben kezelhető a $G(n)$ függvénynél, valamint igazolni tudjuk, hogy

$$\ln G(n) \sim \ln F(n).$$

4.3.1. Definíció. Legyenek $p_1, \dots p_n$ különböző prímek. Ekkor legyen P olyan, hogy

$$\sum_{i=1}^{n} p_i \leq n,$$

és a

$$p_1 + \ldots + p_n + P > n$$

feltételek teljesülnek, ahol P különbözik $p_1, \dots, p_n$ mindegyikétől.

4.3.2. Definíció. Legyen $F(n)$ pozitív egész számokon értelmezett függvény, amelyre $F(1) = 1$, és $n > 1$ esetén

$$F(n) = \prod_{p<P} p.$$

A következő két lemma a 4.3.5 tétel bizonyítása során kerül felhasználásra.

4.3.3. Lemma. *Legyen $q_1, \ldots, q_s$ $G(n)$ összes prímosztója, valamint legyen P a legnagyobb olyan prím, melyre a P-nél kisebb prímek összege nem haladja meg n-t, továbbá legyen $F(n)$ a P-nél kisebb prímek szorzata. Ekkor*

$$\sum_{j=1}^{s} \ln q_j \leq 2 + \ln F(n) + \ln P.$$

Bizonyítás. Vegyük észre, hogy az $x/\ln(x)$ függvény növő, ha $x \geq 3$, mert a deriváltja pozitív. Ha $3 \leq a \leq b$, akkor $\frac{3}{\ln 3} \leq \frac{a}{\ln a} \leq \frac{b}{\ln b}$ is teljesül és így $(a/\ln(a)) \cdot (\ln(b)) \leq b$, és $a \leq (b/\ln(b)) \cdot (\ln(a))$ teljesülnek. Vegyük észre, hogy P legalább 3, kivéve az $n = 1$ esetet, amikor a lemma nyilvánvalóan igaz. Ilyenkor $P = 2$. Legyenek $q_1, \ldots q_{t-1}$ olyan prímek, amelyek osztói a $G(n)$-nek, továbbá nem haladják meg P-t. Legyenek $p_1, \ldots p_r$ olyan P-t meg nem haladó páratlan prímek, amelyek nem osztói $G(n)$-nek. Így a $p_1, \ldots p_r, q_1, \ldots q_{t-1}$ lista tartalmaz minden P-t meg nem haladó prímszámot pontosan egyszer, kivéve esetleg a 2-t. Mivel

$$\sum_{j=1}^{s} q_j \leq S(G(n)) \leq n < \sum_{p \leq P} p,$$

teljesül, ezért arra következtethetünk, hogy

$$\sum_{j=t}^{s} q_j \leq 2 + \sum_{i=1}^{r} p_i$$

Az esetleg hiányzó 2-est a fentebbi kifejezés jobb oldalán pótoljuk ki. Mivel $3 \leq p_i \leq P \leq q_j$, így $(P/\ln P)(\ln q_j) \leq q_j$ és $p_i \leq (P/\ln P)\ln p_i$. Így a következő becsléseket kapjuk:

$$\sum_{j=t}^{s} \ln q_j \leq \sum_{j=t}^{s} q_j \cdot \frac{\ln P}{P} \leq \frac{\ln P}{P}(2 + \sum_{i=1}^{r} p_i) \leq \frac{\ln P}{P} \cdot 2 + \sum_{i=1}^{r} \frac{\ln P}{P} \cdot \frac{P}{\ln P} \cdot \ln p_i \leq 2 + \sum_{i=1}^{r} \ln p_i$$

amiből

$$\sum_{j=t}^{s} \ln q_j \leq 2 + \sum_{i=1}^{r} \ln p_i.$$

Ha a fenti egyenlőtlenség mindkét oldalához hozzáadunk $\sum_{j=1}^{t-1} \ln q_j$-t, akkor azt kapjuk, hogy

$$\sum_{j=1}^{s} \ln q_j \leq 2 + \sum_{j=1}^{t-1} \ln q_j + \sum_{i=1}^{r} \ln p_i = 2 + \ln(p_1 \ldots p_r \cdot q_1 \ldots q_{t-1}),$$

tehát

$$\sum_{j=1}^{s} \ln q_j \leq 2 + \ln F(n) + \ln P,$$

ahogyan a lemmában állítottuk. □

4.3.4. Lemma. *Legyen q prímszám, $e > 1$ egy egész szám, és P a legnagyobb olyan prím, melyre a P-nél kisebb prímek összege nem haladja meg n-t. Ha $G(n)$ osztható q^e-vel, akkor $q^e \leq 2P$ és $q \leq \sqrt{2P}$.*

Bizonyítás. Ha tudjuk, hogy $q^e \leq 2P$, akkor a második állítás már következik, hiszen ekkor $q \leq \sqrt[e]{2P}$, és itt $e > 1$ miatt $\sqrt[e]{2P} \leq \sqrt{2P}$. Tehát elegendő bizonyítanunk az első egyenlőtlenséget. Legyen Q a legkisebb prím, amely nem osztja $G(n)$-t. Ekkor minden Q-nál kisebb prím osztja $G(n)$-t, amelyeket rendre $q_1, \ldots, q_s$-sel jelölünk. Ezeknek a prímeknek a szorzata osztja $G(n)$-t. Ebből az következik, hogy az összegük legfeljebb n. Így $Q \leq P$ a P definíciója alapján. Így elegendő azt megmutatnunk, hogy $q^e \leq 2Q$.

Indirekt tegyük fel, hogy $q^e > 2Q$, és legyen N olyan egész szám, amely teljesíti a $Q^{N-1} < q < Q^N$ feltételt. Vegyük észre, hogy ilyen N választható, mert $q \mid G(n)$, de $Q \nmid G(n)$. Így teljesül a $q < Q^N < qQ$ feltétel. Legyen $m = (Q^N/q) \cdot G(n)$. Ekkor $m > G(n)$ és

$$S(m) = S(G(n)) + (Q^N + q^{e-1} - q^e)$$

Megmutatjuk, hogy a $(Q^N + q^{e-1} - q^e)$ kifejezés értéke negatív.

Ha $q < Q$, akkor $N = 1$, továbbá a $q^e > 2\dot{Q}$ indirekt feltevés miatt:

$$-q^e + q^{e-1} \leq \frac{-q^e}{2} < \frac{-2Q}{2} < -Q$$

Ha $q > Q$, akkor

$$Q^N + q^{e-1} - q^e < qQ - q^{e-1}(q-1) \leq qQ - q(q-1) \leq qQ - qQ \leq 0$$

Összességében

$$S(m) \leq S(G(n)) \leq n,$$

és mivel $m > G(n)$, ezért $S(m) > n$. Ez ellentmondást eredményez, tehát $q^e \leq 2P$ teljesül. □

4.3.5. Tétel. *Legyen P, mint eddig is, a legnagyobb olyan prím, melyre a P-nél kisebb prímek összege nem haladja meg n-t, és legyen $F(n)$ a P-nél kisebb prímek szorzata. Ekkor $\ln F(n) \sim \ln G(n)$ teljesül.*

Bizonyítás. Tudjuk, hogy $F(n) \leq G(n)$, mert S_n-ben van $F(n)$ rendű elem, hiszen

$$p_1 + p_2 + \ldots + p_{k-1} \leq n$$

ahol p_i-k a ciklushosszakat jelölik, továbbá

$$p_1 \cdot p_2 \cdot \ldots p_{k-1} = F(n).$$

Legyen $\prod_{j=1}^{s} q_j^{e_j}$ a $G(n)$ prímfelbontása. Ekkor $\ln G(n)$ felírható a következő alakban:

$$\sum_{j=1}^{s} \ln q_j^{e_j}$$

Ezt az összeget az e_j értéke szerint csoportosítjuk úgy, hogy az egyik részösszegben $e_j = 1$, míg a másikban $e_j > 1$. A 4.3.3 lemma miatt az első részösszeg legfeljebb $2 + \ln F(n) + \ln P$, míg a 4.3.4 miatt a másik részösszeg minden tagja legfeljebb $\ln 2P$, amelyből legfeljebb $\sqrt{2P}$ darab van. Így a következő dupla egyenlőtlenséget kapjuk meg:

$$\ln F(n) \leq \ln G(n) \leq 2 + \ln F(n) + \ln P + \sqrt{2P}(\ln 2P)$$

A fentebbi dupla egyenlőtlenségben minden egyes tagot $\ln F(n)$-nel osztunk, és ezeknek a határértékét vizsgáljuk meg az $F(n)$ függvényében. Később látni fogjuk, hogy

$$P \sim \ln F(n).$$

Ekkor létezik olyan c pozitív konstans, hogy

$$\ln F(n) > c \cdot P.$$

Innen az következik, hogy

$$\ln P < \ln(\frac{1}{c} \cdot \ln F(n)).$$

Ezt felhasználva kapjuk, hogy:

$$\lim_{n\to\infty} \frac{\ln P}{\ln F(n)} \leq \lim_{n\to\infty} \frac{\ln(\frac{1}{c} \cdot \ln F(n))}{\ln F(n)} = \lim_{n\to\infty} \frac{\ln(\frac{1}{c}) + \ln\ln F(n)}{\ln F(n)}.$$

A fentebbi egyenlőtlenség jobb oldalának határértéke 0, mert a számlálóban logaritmus logaritmusa és egy konstans érték található, amelynek nagyságrendje kisebb, mint a logaritmusnak. Mivel a bal oldalon 2 pozitív érték hányadosa szerepel, így

$$\lim_{n\to\infty} \frac{\ln P}{\ln F(n)} = 0.$$

Most megvizsgáljuk a

$$\frac{\sqrt{2P}(\ln 2P)}{\ln F(n)}$$

kifejezés határértékét. A következőképpen becsülhetjük felülről ezt a határértéket:

$$\lim_{n\to\infty} \frac{\sqrt{2P}(\ln 2P)}{\ln F(n)} \leq \lim_{n\to\infty} \frac{\sqrt{\frac{2}{c}} \cdot \sqrt{\ln F(n)} \cdot \ln(\frac{2}{c}) + \sqrt{\frac{2}{c}} \cdot \sqrt{\ln F(n)} \cdot \ln\ln F(n)}{\ln F(n)}$$

Mivel

$$\ln \ln F(n) \leq \sqrt[4]{\ln F(n)}$$

teljesül, ezért

$$\lim_{n\to\infty} \frac{(\ln F(n))^{3/4}}{\ln F(n)} = 0.$$

Mivel a bal oldalon két pozitív érték hányadosa található, ezért

$$\lim_{n\to\infty} \frac{\sqrt{2P}(\ln 2P)}{\ln F(n)} = 0.$$

Nyilvánvaló, hogy

$$\lim_{n\to\infty} \frac{2}{\ln F(n)} = 0.$$

Tehát azt kapjuk, hogy

$$1 \leq \lim_{n\to\infty} \frac{\ln G(n)}{\ln F(n)} \leq 1,$$

amely azt jelenti, hogy $\ln G(n) \sim \ln F(n)$, így a bizonyítandó tételt kaptuk meg. □

4.4. A maximális elemrend aszimptotikus becslése

Ebben az alfejezetben az a célunk, hogy bebizonyítsuk a 4.1 összefüggést. Az előző alfejezetben definiáltuk az $F(n)$ függvényt és a P-t. A p szokásosan egy prímet jelöl.

Jelölje $A(x)$ azon prímek összegét, amelyek értéke legfeljebb x:

$$A(x) = \sum_{p\leq x} p,$$

Legyen

$$\theta(x) = \sum_{p\leq x} \ln p.$$

Ekkor $A(P-1) \leq n < A(P)$ és $\ln F(n) = \theta(P-1)$.

A következő becslések igazak $A(x)$-re és $\theta(x)$-re a prímszámtétel miatt:

$$A(x) \sim \frac{x^2}{2 \cdot \ln x}$$

és

$$\theta(x) \sim x$$

Lássuk a második állítást külön is, melyet a teljesség igénye nélkül bebizonyítunk.

4.4.1. Állítás. $\theta(x) \sim x$.

Bizonyítás. A $\pi(x)$, $\theta(x)$ és a Stieltjes-integrál definícióit figyelembe véve:

$$\theta(x) = \int_1^x \ln t \; d(\pi(t))$$

Erre parciális integrálást alkalmazva azt kapjuk, hogy

$$\theta(x) = \ln x \cdot \pi(x) - \int_2^x \frac{\pi(t)}{t} \; dt.$$

A prímszámtétel miatt igaz az alábbi becslés, ahol C egy konstans:

$$\int_2^x \frac{\pi(t)}{t} \; dt \leq C \cdot \int_2^x \frac{1}{\ln t} \; dt$$

Ezt felírhatjuk két darab integrál összegeként a következőképpen:

$$\int_2^x \frac{1}{\ln t} \; dt = \int_2^{\sqrt{x}} \frac{1}{\ln t} \; dt + \int_{\sqrt{x}}^x \frac{1}{\ln t} \; dt$$

Ezt az összeget felülről tudjuk becsülni az integrálközelítő összeg segítségével a következő módon:

$$\int_2^{\sqrt{x}} \frac{1}{\ln t} \; dt + \int_{\sqrt{x}}^x \frac{1}{\ln t} \; dt \leq (\sqrt{x} - 2) \cdot \frac{1}{\ln 2} + (x - \sqrt{x}) \cdot \frac{1}{\ln \sqrt{x}} \leq D \cdot \frac{x}{\ln x}$$

ahol D egy konstans érték.

Most megnézzük a

$$\lim_{x \to \infty} \frac{\frac{\sqrt{x}}{\ln 2} - \frac{2}{\ln 2} + \frac{2 \cdot x}{\ln x} - \frac{2 \cdot \sqrt{x}}{\ln x}}{\frac{x}{\ln x}}$$

határértéket. Könnyen látható, hogy ennek a kifejezésnek a határértéke 2, amelyből azt vesszük észre, hogy

$$\int_2^x \frac{1}{\ln t} \; dt \leq 2$$

Így az

$$\int_2^x \frac{\pi(t)}{t} \; dt$$

értéke felülről korlátos.

Ha a

$$\theta(x) = \int_1^x \ln t \; d(\pi(t))$$

kifejezést osztjuk x-szel, akkor azt kapjuk, hogy

$$\frac{\theta(x)}{x} = \frac{\ln x \cdot \pi(x)}{x} - \frac{2 \cdot C}{x}.$$

Mivel $\pi(x) \sim \frac{x}{\ln x}$, ezért

$$\lim_{x\to\infty} \frac{\theta(x)}{x} = 1,$$

ami a $\theta(x) \sim x$ állítást bizonyítja. $\square$

4.4.2. Állítás.

$$\ln F(n) \sim \sqrt{n \cdot \ln n}.$$

Bizonyítás. Mivel $\ln F(n) = \theta(P-1)$ és $P \sim P-1$ teljesülnek, ezért $P \sim \ln F(n)$ is igaz.

Így elegendő annak megmutatása, hogy

$$P \sim \sqrt{n \cdot \ln n}.$$

Mivel $A(x-1) \sim A(x)$, ezért

$$\frac{P^2}{2 \cdot \ln P} \sim n.$$

Ha P nem aszimptotikusan egyenlő $\sqrt{n \cdot \ln n}$-nel, akkor az alábbi 2 egyenlőtlenség közül végtelen sokszor teljesül valamelyik egyenlőtlenség valamilyen ϵ esetén:

$$P \leq (1-\epsilon)\sqrt{n \cdot \ln n},\ P \geq (1+\epsilon)\sqrt{n \cdot \ln n}.$$

Mivel az $\frac{x^2}{\ln x}$ függvény növekvő $x > \sqrt{e}$ esetén, ezért

$$\frac{P^2}{\ln P} \leq \frac{(1-\epsilon)^2 \cdot n \cdot \ln n}{\ln(1-\epsilon) + \frac{1}{2} \cdot \ln(n \cdot \ln n)}.$$

Így azt kapjuk, hogy

$$\frac{P^2}{2n \cdot \ln P} \leq \frac{(1-\epsilon)^2 \cdot \ln n}{2 \cdot \ln(1-\epsilon) + \ln n + \ln\ln n},$$

tehát

$$\lim_{n\to\infty} \frac{P^2}{2n \cdot \ln P} = 1,$$

és

$$\lim_{n\to\infty} \frac{(1-\epsilon)^2 \cdot \ln n}{2 \cdot \ln(1-\epsilon) + \ln n + \ln\ln n} = (1-\epsilon)^2.$$

Tehát azt kaptuk, hogy

$$1 \leq (1-\epsilon)^2,$$

így ellentmondást kaptunk ebben az esetben.

Nézzük meg, hogy mit kapunk a másik egyenlőtlenség esetén.

Ekkor

$$\frac{P^2}{\ln P} \geq \frac{(1+\epsilon)^2 \cdot n \cdot \ln n}{\ln(1+\epsilon) + \frac{1}{2} \cdot \ln(n \cdot \ln n)},$$

amiből azt kapjuk, hogy

$$\frac{P^2}{2n \cdot \ln P} \geq \frac{(1+\epsilon)^2 \cdot \ln n}{2 \cdot \ln(1+\epsilon) + \ln n + \ln \ln n}.$$

A kapott eredmények:

$$\lim_{n \to \infty} \frac{P^2}{2n \cdot \ln P} = 1$$

és

$$\lim_{n \to \infty} \frac{(1+\epsilon)^2 \cdot \ln n}{2 \cdot \ln(1+\epsilon) + \ln n + \ln \ln n} = (1+\epsilon)^2,$$

amiből azt kapjuk, hogy

$$1 \geq (1+\epsilon)^2,$$

ami nem igaz, így ellentmondásra jutottunk.

Így azt kaptuk, hogy

$$P \sim \sqrt{n \cdot \ln n}$$

Mivel $P \sim \ln F(n)$, ezért $\ln F(n) \sim \sqrt{n \cdot \ln n}$ is teljesül, és így a 4.3.5 tétel miatt

$$\ln G(n) \sim \sqrt{n \cdot \ln n},$$

amely éppen a 4.1-ben szereplő állítás. □

4.5. G(n) kiszámítása adott n esetén

Kis n értékekre $G(n)$ kiszámítása egyszerű. Tudjuk, hogy minden permutáció felbontható diszjunkt ciklusok szorzatára S_n-ben és a permutáció rendje a ciklushosszak legkisebb közös többszöröse. Ezt használjuk fel, amikor kiszámoljuk a lehetséges elemrendeket S_n-ben. Felbontjuk az n-t pozitív egész számok összegére és minden egyes felbontás esetén kiszámoljuk az összegben szereplő tagok legkisebb közös többszörösét. Ezen legkisebb közös többszörösök maximumát $G(n)$-nel jelöljük. A következő táblázat azt mutatja, hogy mekkorák $G(n)$ értékei, és megadja a permutációk megfelelő ciklushosszait is. A táblázatban $p(n)$ az n partícióinak a számát jelöli.

n	$p(n)$	$G(n)$	ciklushossz
1	1	1	1
2	2	2	2
3	3	3	3
4	5	4	4
5	7	6	2,3
6	11	6	1, 2, 3 vagy 6
7	15	12	3,4
8	22	15	3,5
9	30	20	4,5
10	42	30	2,3,5
11	56	30	1,2,3,5 vagy 5,6
12	77	60	3,4,5
13	101	60	1,3,4,5
14	135	84	3,4,7
15	176	105	3,5,7
16	231	140	4,5,7
17	297	210	2,3,5,7
18	385	210	1,2,3,5,7 vagy 5,6,7
19	490	420	3,4,5,7
20	627	420	1,3,4,5,7
21	792	420	3,4,5,7
22	1002	420	3,4,5,7
23	1255	840	3,5,7,8
24	1575	840	1,3,5,7,8
25	1958	1260	4,5,7,9
26	2436	1260	1,4,5,7,9
27	3010	1540	4,5,7,11
28	3718	2310	2,3,5,7,11
29	4565	2520	5,7,8,9
30	5604	4620	3,4,5,7,11
31	6842	4620	1,3,4,5,7,11
32	8349	5460	3,4,5,7,13

n	$p(n)$	$G(n)$	ciklushossz
33	10143	5460	1,3,4,5,7,13
34	12310	9240	3,5,7,8,11
35	14883	9240	1,3,5,7,8,11
36	17977	13860	4,5,7,9,11
37	21637	13860	1,4,5,7,9,11
38	26015	16380	4,5,7,9,13
39	31185	16380	1,4,5,7,9,13
40	37338	27720	5,7,8,9,11
41	44583	30030	2,3,5,7,11,13
42	53174	32760	5,7,8,9,13
43	63261	60060	3,4,5,7,11,13
44	75175	60060	3,4,5,7,11,13
45	89134	60060	3,4,5,7,11,13
46	105558	60060	3,4,5,7,11,13
47	124754	120120	3,5,7,8,11,13
48	147273	120120	1,3,5,7,8,11,13
49	173525	180180	4,5,7,9,11,13
50	204226	180180	1,4,5,7,9,11,13
51	239943	180180	4,5,7,9,11,13
52	281589	180180	4,5,7,9,11,13
53	329931	360360	5,7,8,9,11,13
54	386155	360360	1,5,7,8,9,11,13
55	451276	360360	2,5,7,8,9,11,13
56	526823	360360	3,5,7,8,9,11,13
57	614154	471240	5,7,8,9,11,17
58	715220	510510	2,3,5,7,11,13,17
59	831820	556920	5,7,8,9,13,17
60	966467	1021020	3,4,5,7,11,13,17

A táblázatban szereplő maximális elemrendeket Maple számítógépes program segítségével számítottuk ki, amely lentebb szerepel. A maximális elemrendhez tartozó ciklushosszakat a prímfelbontások segítségével határoztuk meg:

with(combinat):

for n **from** 1 **to** 60 **do**

$l := 1$:

$p := \text{partition}(n)$:
for i **from** 1 **to** numbpart(n) **do**
if ilcm($p[i][j]$ \$ $j = 1..\text{nops}(p[i])) > l$
then $l := \text{ilcm}(p[i][j])$ \$ $j = 1..\text{nops}(p[i]))$
fi:
od:
$\text{print}([n, \text{numbpart}(n), l])$;
od:

4.6. Érdekességek a partíciófüggvényről

Befejezésül a [2] forrás alapján kimondunk egy aszimptotikát a korábban már használt partíciófüggvényre.

4.6.1. Definíció. Legyen n pozitív egész szám. Ekkor n partícióin az n pozitív egészek összegeként történő különböző előállításait értjük az egytagú összeget is beleértve.

4.6.2. Megjegyzés. *Két partíciót azonosnak tekintünk, ha csak az összeadandók sorrendjében térnek el egymástól.*

A következő tételben a partíciók számára vonatkozó aszimptotikus egyenlőséget írunk le bizonyítás nélkül.

4.6.3. Tétel. *Legyen $p(n)$ az n partícióinak száma. Ekkor*

$$p(n) \sim \frac{c \cdot e^{d\sqrt{n}}}{n},$$

ahol $c = \dfrac{1}{4\sqrt{3}}$ *és* $d = \dfrac{\pi\sqrt{6}}{3}$.

Irodalomjegyzék

[1] Conrad, Keith: *Simplicity of A_n*

http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/Ansimple.pdf

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

[3] Fried Ervin: *Algebra II. Algebrai struktúrák*, Nemzeti Tankönyvkiadó 2002

[4] Igusa, Kiyoshi: *Automorphism groups*, egyetemi előadásjegyzet, 2002

http://people.brandeis.edu/~igusa/Math101b/auto.pdf

[5] Kiss Emil: *Bevezetés az algebrába*, Typotex, 2007

[6] Lukács Erzsébet: *Permutációcsoportok*, egyetemi előadásjegyzet

http://math.bme.hu/~lukacs/bboard/csop/2016/csop_perm.pdf

[7] Miller, William: *The Maximum Order of an Element of a Finite Symmetric Group*, American Mathematical Monthly **94**, (1987), 497-506.