Eötvös Loránd Tudományegyetem
Természettudományi Kar

Elemrendek véges csoportokban

Szőnyi Laura

Matematika MSc

Témavezető:

Halasi Zoltán
Algebra és Számelmélet Tanszék
Eötvös Loránd Tudományegyetem, Természettudományi Kar

Budapest, 2023

Köszönöm témavezetőmnek, Halasi Zoltánnak a szakdolgozat megírásában nyújtott sok segítséget és türelmet.

Tartalomjegyzék

1. Bevezetés

A véges csoportok elemrendjeinek összegét és szorzatát már többen vizsgálták, ezen eredményekre támaszkodik jelen írás is, azokat részben bemutatva, részben további vizsgálatoknak vetve alá.

Az első fejezetben elsőként a Ψ függvény definíciója és az azzal kapcsolatos legalapvetőbb korábbi eredmények szerepelnek, melyekre a dolgozat egészében szükség lesz. Ezután a prímnégyzet-indexű ciklikus részcsoporttal rendelkező prímhatvány rendű csoportok elemrendösszegét hasonlítjuk össze a ciklikus csoportéval. Ezt követően először a $\frac{\Psi(C_n)}{n\varphi(n)}$ függvényre adunk felső becslést, majd korábbi hasonló függvényekhez hasonlóan bizonyos tulajdonsággal nem rendelkező csoportokra (mint ciklikus, Abel, nilpotens) javított felső becslést. Végül a Ψ függvény egy általánosítását tekintjük, és egy korábbi tétellel kapcsolatos sejtés cáfolataként ismertetünk egy ellenpéldát.

A második fejezetben az elsőben említett $\frac{\Psi(G)}{n\varphi(n)}$ függvényt egy aritmetikai középnek tekintve vesszük a hozzá tartozó egyéb nevezetes közepeket. Elsőként a harmonikus középre adunk felső becslést, majd a négyzetes középről látjuk be, hogy felülről nem korlátozható, végül a mértani közepet becsüljük felülről.

A harmadik fejezetben véges csoportokban vizsgáljuk az elemrendek szórását. Ezzel kapcsolatban a szakirodalomban nem szerepeltek ismert eredmények. Először prímhatvány rendű Abel csoportok esetén látjuk be, hogy legnagyobb szórása a ciklikus csoport elemrendjeinek van, elsőként 3-nál nagyobb prímekre, majd a becslést élesítve kiterjesztve $p = 3$-ra, végül a $p = 2$ esetet külön vizsgálva. Ezt követően az állítást kiterjesztjük az összes Abel csoportra, később a p-csoportokra, legvégül pedig a nilpotens csoportokra.

A negyedik fejezet célja egy, a véges csoportok elemrendjeinek átlagával kapcsolatos már ismert tétel és annak bizonyításának ismertetése. Itt elsőként az adott rendű elemek darabszámára adunk különböző becsléseket, majd ismertetünk néhány, a későbbiekben használandó állítást a csoportok elemrend-átlagával kapcsolatban. Ezek után a fejezet fő tételének bizonyításához látunk hozzá a bizonyítás rövid vázlatának és néhány korábbi eredmény ismertetése után. A bizonyítás két legfontosabb lemmáját egy-egy újabb alfejezetben tárgyaljuk, majd, használva a véges egyszerű csoportok klasszifikációját, ellenőrizzük a tétel állítását egyszerű csoportokra, végül általánosan is belátjuk a tételt.

2. Az elemrendek összege véges csoportokban

2.1. A Ψ függvény

Az alábbiakban azon legalapvetőbb eredmények ismertetése található, melyeken a későbbiek alapulni fognak.

Jelölje C_n az n elemű ciklikus csoportot, $\Psi(G) = \sum_{g \in G} o(g)$ a G csoport elemrendjeinek összegét, n a G véges csoport rendjét.

Nem nehéz belátni, hogy $\Psi(G) < \Psi(C_n)$, amennyiben nem izomorf vele, de ennél többet igazolt Herzog, Longobardi és Maj [1]-ben.

2.1. Tétel. *[1, Theorem 1.] Ha G nem ciklikus, n rendű csoport, akkor $\Psi(G) \leq \frac{7}{11}\Psi(C_n)$.*

Az állítás éles, ugyanis páratlan k-ra $n = 4k$ esetén $\Psi(C_{2k} \times C_2) = \frac{7}{11}\Psi(C_n)$ [1, Proposition 2] alapján.

Egyes esetekben ugyanakkor lehet még javítani a becslést.

2.2. Tétel. *[1, Theorem 3] Ha G nem ciklikus, n rendű csoport, q az n legkisebb prímosztója, akkor $\Psi(G) \leq \frac{1}{q-1}\Psi(C_n)$.*

Látható, hogy páratlan rendű csoportoknál ez többet mond, mint az előző tétel, ugyanis ekkor $\Psi(G) \leq \frac{1}{2}\Psi(C_n)$ biztosan teljesül [1, Corollary 4], páros rendűekre viszont nem állít semmi újat.

Hasznos tudni az alábbi, egyszerű számolás után adódó képletet.

2.3. Tétel. *Ha $n = p^r$, azaz prímhatvány, akkor $\Psi(C_n) = \frac{p^{2r+1}+1}{p+1}$.*

Az Euler-féle φ-függvénnyel való kapcsolatáról a következőt állíthatjuk.

2.4. Tétel. *[1, Theorem 11] Legyen q az n legkisebb prímosztója. Ekkor $\Psi(G) \geq \frac{n}{q}\varphi(n)$.*

Továbbá H. Amiri, S.M. Jafarian Amiri, I.M. Isaacs [2] cikke alapján igaz a következő állítás is.

2.5. Tétel. *[2, Corollary B] Ha p prímre $P \in Syl_p(G)$, ahol P ciklikus normálosztója G-nek, akkor $\Psi(G) \leq \Psi(P)\Psi(G/P)$, egyenlőség pedig pontosan akkor áll fenn, ha P benne van a G centrumában.*

2.6. Következmény. *Ha $n = \prod_{p|n} p^{r_p}$ az n kanonikus alakja, akkor $\Psi(C_n) = \prod_{p|n} \Psi(C_{p^{p_r}})$.*

2.2. Az elemrendek összegének felső becslése

Könnyen látható, hogy a $\frac{\Psi(C_n)}{n\varphi(n)}$ kifejezés $n > 1$ esetén mindig nagyobb, mint 1, hiszen az n-nel relatív prím elemek mind n-edrendűek, továbbá $o(1) = 1$ miatt szigorú az egyenlőtlenség. Felvetődik a kérdés, hogy lehet-e felső korlátot mondani.

2.7. Tétel. $\frac{\Psi(C_n)}{n\varphi(n)} < 2,1666$

Bizonyítás. Legyen $n = \prod_{p|n} p^{r_p}$ az n kanonikus alakja. Rövid számolással adódik az alábbi becslés.

$$\frac{\Psi(C_n)}{n\varphi(n)} = \prod_{p|n} \frac{\Psi(C_{p^{r_p}})}{p^{r_p}\varphi(p^{r_p})} = \prod_{p|n} \frac{p^{2r_p+1}+1}{(p^2-1)p^{2r_p-1}} \leq \prod_{p|n} \frac{p^3+1}{p^3-p} = \prod_{p|n} \left(1 + \frac{p+1}{p^3-p}\right) \leq e^{\sum_{p|n} \frac{p+1}{p^3-p}}$$

Ekkor a $\sum_{p\ prím} \frac{p+1}{p^3-p}$ kifejezést lehet tovább vizsgálni.

$$\sum_{p\ prím} \frac{p+1}{p^3-p} = \sum_{p\ prím} \frac{1}{p^2-1} + \sum_{p\ prím} \frac{1}{p^3-p}$$

Tudjuk a mértani sor összegképletéből, hogy teljesül az következő.

$$\frac{1}{p^2-1} = \frac{1}{p^2} + \frac{1}{p^4} + \frac{1}{p^6} + \dots$$

Jelölje $P(s) = \sum_{p\ prím} \frac{1}{p^s}$ a prím zeta-függvényt, ez minden $s > 1$-re konvergens. Ennek használatával adódik az alábbi.

$$\sum_{p\ prím} \frac{1}{p^2-1} = P(2) + P(4) + P(6) + \dots$$

Hasonlóan

$$\frac{1}{p^3-p} = \frac{1}{p^3} + \frac{1}{p^5} + \frac{1}{p^7} + \dots$$

így

$$\sum_{p\ prím} \frac{1}{p^3-p} = P(3) + P(5) + P(7) + \dots$$

Ebből következik, hogy

$$\sum_{p\ prím} \frac{p+1}{p^3-p} = P(2) + P(3) + P(4) + P(5) + P(6) + P(7) + \ldots \approx 0,773156669$$

Így

$$\frac{\Psi(C_n)}{n\varphi(n)} \le e^{\sum_{p|n} \frac{p+1}{p^3-p}} < e^{\sum_{p\ prím} \frac{p+1}{p^3-p}} \approx 2,1665947$$

$\square$

Ugyanakkor ennél több is igaz, ez látható az alábbiakban.

2.8. Tétel. $\frac{\Psi(C_n)}{n\varphi(n)} < 1,9436$

Bizonyítás. Az iménti számolás elejét is felhasználva adódik az alábbi.

$$\frac{\Psi(C_n)}{n\varphi(n)} \le \prod_{p\ prím} \frac{p^3+1}{p^3-p} = \prod_{p\ prím} \frac{p^6-1}{(p^3-1)(p^2-1)p} = \prod_{p\ prím} \frac{1-\frac{1}{p^6}}{(1-\frac{1}{p^3})(1-\frac{1}{p^2})} =$$

$$= \frac{\prod(1-\frac{1}{p^6})}{\prod(1-\frac{1}{p^3})\prod(1-\frac{1}{p^2})}$$

A mértani sor összegképletéből adódik az alábbi számítás.

$$\prod \frac{1}{1-\frac{1}{p^k}} = \prod \left(1 + \frac{1}{p^k} + \frac{1}{p^{2k}} + \ldots\right) = \sum_{n=1}^{\infty} \frac{1}{n^k} = \zeta(k)$$

Tehát az eredeti kifejezés az alábbi alakra hozható.

$$\frac{\Psi(C_n)}{n\varphi(n)} \le \frac{\prod(1-\frac{1}{p^6})}{\prod(1-\frac{1}{p^3})\prod(1-\frac{1}{p^2})} = \frac{\zeta(3)\zeta(2)}{\zeta(6)} = \gamma \approx 1,94359643682076$$

$\square$

A becsült értékek Wolframalfával való kalkulációkból adódtak.

Látható, hogy ez az eredmény tovább már nem javítható, mert az $n_i = p_1 \cdot p_2 \cdot \ldots \cdot p_i$ sorozattal, ahol p_i az i. prím, $\frac{\Psi(C_{n_i})}{n_i\varphi(n_i)}$ pont ezen számhoz konvergál, n_{1229}-re már $1,943577\ldots$ a tört értéke.

Összevetve az eredményt a 2.1 és 2.2. Tételekkel adódik, hogy nem ciklikus, páratlan elemrendű csoport esetén $\Psi(G) < n\varphi(n)$, páros elemrendű csoport esetén pedig $\Psi(G) < 1,24n\varphi(n)$.

Alsó becslést tekintve a $n = 2^k$ esetből látható, hogy $\Psi(C_2^k) = 2n - 1$, ennél jobbat nem lehet mondani, mert egy elem rendje 1, az összes többi elem rendje pedig legalább 2, tehát $\Psi(G) \geq 2n - 1$.

2.3. Az elemrendek összegének alsó becslése

Legyen $\Psi_1(G) = \frac{\Psi(G)}{|G|^2}$. Könnyen látható, hogy $0 \leq \Psi_1(G) \leq 1$. Ennek bizonyos tulajdonságait Marius Tărnăuceanu [4] cikkében vizsgálta, amelyben felső korlátot adott bizonyos tulajdonságokkal nem rendelkező csoportokon vett értékére.

2.9. Tétel. *[4, Theorem 1.1] Legyen G véges csoport, ekkor teljesülnek a következő állítások:*

- *Ha* $\Psi_1(G) > \frac{7}{16} = \Psi_1(C_2^2) = 0,4375$*, akkor G ciklikus.*
- *Ha* $\Psi_1(G) > \frac{27}{64} = \Psi_1(Q_8) \approx 0,4218$*, akkor G Abel.*
- *Ha* $\Psi_1(G) > \frac{13}{36} = \Psi_1(S_3) \approx 0,3611$*, akkor G nilpotens.*
- *Ha* $\Psi_1(G) > \frac{31}{144} = \Psi_1(A_4) \approx 0,2153$*, akkor G szuperfeloldható.*
- *Ha* $\Psi_1(G) > \frac{211}{3600} = \Psi_1(A_5) \approx 0,0586$*, akkor G feloldható.*

A $\Psi_1(G)$ és a $A(G) = \frac{\Psi(G)}{\varphi(G)\cdot|G|}$ közti látszólagos hasonlóság miatt felvetődik annak a lehetősége, hogy hasonló tételt próbáljunk $A(G)$-re kimondani. Számítógépes kalkulációk alapján azonban sejthető, hogy ez esetben nem lesz olyan felső határ, amit egy adott csoport (a fenti tétel analogonjaként) fel is vesz, ugyanakkor konnyen látható, hogy adható korlát, amit nem lép át nem-ciklikus csoport. A számolásokhoz szükség lesz az alábbi tételekre.

Tudjuk, hogy adott n-re $\Psi(G)$ akkor maximális, ha G ciklikus. Felvetül a kérdés, hogy a második legnagyobb értéket mikor veszi fel a Ψ függvény, ezt vizsgálta Marcel Herzog, Patrizia Longobardi és Mercede Maj [5] és [6] cikkeikben.

Általánosan az alábbi tétel mondható ki:

2.10. Tétel. *[5, Theorem 4] Ha* $G \ncong C_n$*, q az n legkisebb prímosztója, akkor*

$$\Psi(G) \leq \frac{((q^2-1)q+1)(q+1)}{q^5+1}\Psi(C_n)$$

és egyenlőség pontosan akkor áll fenn, ha $G = C_q^2 \times C_k$ *ahol* $n = q^2k$, $(q,k) = 1$.

A $q = 2$ esetre a korábban látott $\frac{7}{11}$ értéket adja a tört. Ha a csoport rendje osztható 4-gyel, de 8-cal nem, akkor van olyan csoport, ami felveszi ezt az értéket.

Ha a csoport rendje páros, de nem osztható 4-gyel, akkor igaz a következő állítás.

2.11. Tétel. *[6] Ha $n = 2m$, ahol $m = \prod_{i=1}^{t} p_i^{\alpha_i}$ páratlan, $G \ncong C_n$, $l = min\{p_i^{\alpha_i}\}$, akkor*

$$\Psi(G) \leq \left(\frac{1}{3} + \frac{2 \cdot l}{3 \cdot \Psi(C_l)}\right) \cdot \Psi(C_n)$$

és egyenlőség pontosan akkor áll fenn, ha $G \cong D_{2l} \times C_{\frac{n}{2l}}$.

Mivel a tételbeli $\frac{1}{3} + \frac{2 \cdot l}{3 \cdot \Psi(C_l)}$ a maximumát $l = 3$-ra veszi fel, így a következő tétel az előbbinek speciális esete, ahol n osztható 3-mal, de 9-cel nem.

2.12. Tétel. *Ha $n = 2m$, ahol m páratlan, $G \ncong C_n$, akkor $\Psi(G) \leq \frac{13}{21} \cdot \Psi(C_n)$, és egyenlőség pontosan akkor áll fenn, ha $G \cong S_3 \times C_k$, ahol $(k, 6) = 1$.*

Ezek segítségével már bebizonyítható a következő állítás.

2.13. Tétel. *Ha $A(G) > 1,2032$, akkor G ciklikus.*

Bizonyítás. Mint azt az előző fejezetben láttuk teljesül az alábbi:

$$\frac{\Psi(C_n)}{n\varphi(n)} = \prod_{p|n} \frac{\Psi(C_{p^{r_p}})}{p^{r_p}\varphi(p^{r_p})} = \prod_{p|n} \frac{p^{2r_p+1}+1}{(p^2-1)p^{2r_p-1}} \leq \prod_{p|n} \frac{p^3+1}{p^3-p} < \gamma$$

Ha n osztható 4-gyel, akkor igaz az alábbi:

$$\frac{\Psi(C_n)}{n\varphi(n)} = \frac{2^{2r_2+1}+1}{3 \cdot 2^{2r_2-1}} \cdot \prod_{p|n, p>2} \frac{p^{2r_p+1}+1}{(p^2-1)p^{2r_p-1}} \leq \frac{11}{8} \cdot \prod_{p|n, p>2} \frac{p^3+1}{p^3-p} < \frac{\frac{11}{8}}{\frac{3}{2}} \cdot \gamma = \frac{11}{12} \cdot \gamma$$

Ha n páratlan, akkor teljesül a következő becslés:

$$\frac{\Psi(C_n)}{n\varphi(n)} = \prod_{p|n, p>2} \frac{p^{2r_p+1}+1}{(p^2-1)p^{2r_p-1}} \leq \prod_{p|n, p>2} \frac{p^3+1}{p^3-p} < \frac{1}{\frac{3}{2}} \cdot \gamma = \frac{2}{3} \cdot \gamma \approx 1,94$$

Most tekintsük, hogy az egyes esetekben mekkora lehet adott n-re a második legnagyobb elemrend-összegű csoportra a $\Psi(G)$ értéke. Mivel adott n-re $n \cdot \varphi(n)$ állandó, így az $A(G)$ értéke is ezekben az esetekben lesz második legnagyobb. Legyen a továbbiakban G nem ciklikus n rendű csoport.

Ha n páratlan, akkor ugyan nem tudjuk, hogy pontosan mekkora a második érték, viszont tudunk rá felső becslést adni, így adódik az alábbi:

$$\frac{\Psi(G)}{n\varphi(n)} \leq \frac{7}{11} \cdot \frac{\Psi(C_n)}{n\varphi(n)} < \frac{7}{11} \cdot \frac{2}{3} \cdot \gamma = \frac{14}{33} \cdot \gamma \approx 0,8246$$

Ha n páros, de nem osztható 4-gyel, akkor teljesül a következő:

$$\frac{\Psi(G)}{n\varphi(n)} \leq \frac{13}{21} \cdot \frac{\Psi(C_n)}{n\varphi(n)} < \frac{13}{21} \cdot \gamma \approx 1,2032$$

Könnyen meggondolható, hogy a fenti esetben az egyenlőtlenség éles, ugyanis van olyan sorozata a csoportoknak, amelyre az $A(G)$ értéke az adott felső korláthoz konvergál, nevezetesen $G \cong S_3 \times C_k$, ahol $k = \frac{n}{6}$, és n az első l darab prímszám szorzata.

Ha n osztható 4-gyel, akkor ismét tudunk egy felső becslést adni:

$$\frac{\Psi(G)}{n\varphi(n)} \leq \frac{7}{11} \cdot \frac{\Psi(C_n)}{n\varphi(n)} < \frac{7}{11} \cdot \frac{11}{12} \cdot \gamma = \frac{7}{12} \cdot \gamma \approx 1,1338$$

A fenti három eset lefedi az összes lehetőséget, így megállapítható, hogy $A(G) > \frac{13}{21} \cdot \gamma$ esetében G bizonyosan ciklikus. □

A bizonyításból látható, hogy mivel S_3 nem Abel és nem is nilpotens, ezért ezekre az esetekre is ugyanez a korlát mondható.

A szuperfeloldható és feloldható esetekre a számítógépes számítások alapján hasonló módon adható korlát, várhatóan egy olyan csoport-sorozatra, amely rendje az első l prímszám szorzatának kétszerese.

Megjegyzendő, hogy egy hasonló tétel az elemrendek szorzatáról [7] alapján bizonyítást nyert. Jelölje $\varrho(G) = \prod_{g \in G} o(g)$ az elemrendek szorzatát, $l(G) = \frac{\varrho(G)^{\frac{1}{n}}}{n}$.

2.14. Tétel. *[7, Theorem 1.1, Theorem 1.2] Legyen G véges csoport, ekkor teljesülnek a következő állítások:*

- *Ha* $l(G) > l(C_2^2) \approx 0,4204$*, akkor G ciklikus.*
- *Ha* $l(G) > \frac{27}{64} = l(Q_8) \approx 0,3856$*, akkor G Abel.*
- *Ha* $l(G) > \frac{13}{36} = l(S_3) \approx 0,3399$*, akkor G nilpotens.*
- *Ha* $l(G) > \frac{31}{144} = l(A_4) \approx 0,2061$*, akkor G szuperfeloldható.*
- *Ha* $l(G) > \frac{211}{3600} = l(A_5) \approx 0,0544$*, akkor G feloldható.*

Ezek a határok pontosan ugyanazok, melyek $\Psi_1(G)$ esetén is szerepeltek, és a körülbelüli értékük is hasonló (a számtani-mértani egyenlőtlenségnek megfelelően $l(G)$ kisebb valamivel).

2.4. A Ψ_H függvény

Jelölje G egy H részcsoportjára $\Psi_H(G) = \sum_{g\in G} o_H(g)$-t, ahol $o_H(g)$ az a legkisebb m szám, amire $g^m \in H$. Látható, hogy ez $H = 1$-re az elemrendek összegét adja. Ennek bizonyos tulajdonságait vizsgálta Marius Tărnăuceanu [8] cikkében, a fő állítása a következő.

2.15. Tétel. *[8, Theorem 1.2.] Ha G egy n rendű nilpotens csoport, $H \le G$, $|H| = m$, H_m az C_n m-rendű részcsoportja, akkor $\Psi_H(G) \le \Psi_{H_m}(C_n)$.*

Könnyen látható, hogy $N \triangleleft G$, $|N| = k$ esetén $o_N(g) = o(gN)$ a G/N csoportban, így $\Psi_N(G) = |N| \cdot \Psi(G/N) \le k \cdot \Psi(C_{\frac{n}{k}}) = \Psi_{C_k}(C_{\frac{n}{k}})$.

A cikkben szerepeltek továbbá az alábbi, számolást segítő állítások is.

2.16. Tétel. *[8, Lemma 2.1. a)] Ha a $G_1, \ldots, G_k$ csoportoknak páronként relatív prím rendűek és $H_i \le G_i$, akkor $\Psi_{H_1\times\ldots\times H_k}(G_1 \times \ldots \times G_k) = \prod\limits_{i=1}^{k} \Psi_{H_i}(G_i)$.*

2.17. Következmény. *[8, Lemma 2.1. a)] Ha G véges nilpotens csoport, G_i a G-nek p_i-Sylow részcsoportjai, $H_i \le G_i$ és $H = H_1 \times \ldots \times H_k \le G$, akkor $\Psi_H(G) = \prod\limits_{i=1}^{k} \Psi_{H_i}(G_i)$.*

2.18. Tétel. *[8, Lemma 2.1. b)] Ha G véges csoport és $H \triangleleft K \le G$, akkor $\Psi_H(G) \le |K : H| \cdot \Psi_K(G) - |K| + |H|$.*

2.19. Következmény. *[8, Lemma 2.1. b)] Ha G véges p-csoport, $H \le K \le G$, $|H| = p^m$, $|K| = p^{m+1}$, akkor $\Psi_H(G) \le p \cdot \Psi_K(G) - p^m \cdot (p-1)$.*

2.20. Tétel. *[8, Lemma 2.2.)] Ha G rendje p^n, ahol p prím, H ennek p^m rendű részcsoportja, akkor $\Psi_H(G) \le \Psi_{C_{p^m}}(C_{p^n})$.*

Mindezek alapján a következőképpen bizonyíthatjuk a 2.15 tételt.

Bizonyítás. Ha az n pramtényezős felbontása $p_1^{n_1} \cdot \ldots \cdot_k^{n_k}$, akkor a G csoport nilpotens volta miatt egyenlő a Sylowjainak direkt szorzatával, azaz ha G_i a G csoport p_i-Sylowja, akkor $G \simeq G_1 \times \ldots \times G_k$. Ugyanez mondható el a G csoport H részcsoportjáról, azaz $H \simeq H_1 \times \ldots \times H_k$, ahol $H_i \le G_i$, továbbá $|H_i| = p_i^{m_i}$. Ekkor teljesül az alábbi.

$$\Psi_H(G) = \prod_{i=1}^{k} \Psi_{H_i}(G_i) \le \prod_{i=1}^{k} \Psi_{C_{p_i^{m_i}}}(C_{p_i^{n_i}}) = \Psi_H(G) \le \Psi_{H_m}(C_n)$$

Tehát a tétel állítása valóban teljesül. $\square$

Felmerül a kérdés, hogy az 2.15 tételben valóban szükséges-e megkövetelni, hogy G nilpotens legyen. A szerző sejtése szerint nem, és minden véges csoportra igaz a tétel. Az alábbiakban látható, hogy ez nem igaz.

2.21. Tétel. *Van olyan n rendű G csoport és annak m elemű H részcsoportja, melyekre $\Psi_H(G) > \Psi_{H_m}(C_n)$.*

Bizonyítás. Legyen $p = 2^k - 1$ alakú Mersenne-prím, K a 2^k elemű test, ekkor ennek multiplikatív csoportja ciklikus, méghozzá $K^\times \simeq C_p$. Tekintsük a $G = \{ax + b | a \in K^\times, b \in K\}$, a K-ból K-ba menő invertálható affin függvények csoportját. Ennek normálosztója az eltolások alkotta $N = \{x + b | b \in K\}$ csoport, részcsoportja a $H = \{ax | a \in K^\times\}$, azaz az invertálható lineáris függvények csoportja, és $G \simeq N \rtimes H$.

Ekkor G Frobenius csoport, mert tranzitív, nem reguláris és az egységelemen kívül minden permutációnak legfeljebb egy fixpontja van, így felírható $G = \{N \setminus 1\} \cup \bigcup_{g\in G} (H^g \setminus 1) \cup 1$ alakban, ahol ezek mind diszjunktak egymástól.

Egy $n \in N \setminus 1$ elem rendje $o(n) = 2$, így $o_H(n) = 2$, egy $g \notin N$ elem rendje $o(g) = p$, így ha $g \notin H \cup N$, akkor $o_H(g) = p$, tehát teljesül a következő.

$$\Psi_H(G) = \sum_{h\in H} 1 + \sum_{n\in N\setminus 1} o_H(n) + \sum_{g\notin H\cup N} o_H(g) = p \cdot 1 + p \cdot 2 + (p^2 - p) \cdot p = p^3 - p^2 + 3 \cdot p$$

Ugyanakkor az $n = p \cdot 2^k$ rendű ciklikus csoport p rendű részcsoportját tekintve a következő teljesül:

$$\Psi_{C_p}(C_n) = p \cdot \Psi(C_{2^k}) = p \cdot \frac{2^{2k+1} + 1}{2 + 1} = p \cdot \frac{2 \cdot (p + 1)^2 + 1}{3} = \frac{2}{3} \cdot p^3 + \frac{4}{3} \cdot p^2 + p$$

$p > 6$ esetén $p^3 - p^2 + 3 \cdot p > \frac{2}{3} \cdot p^3 + \frac{4}{3} \cdot p^2 + p$, azaz $\Psi_H(G) > \Psi_{C_p}(C_n)$ a 3 kivételével az összes Mersenne-prímre. □

3. Közepek

Legyen G véges csoport, $n > 1$ a csoport rendje, $\Psi(G)$ a csoport elemrendjeinek összege. Jelölje $a(g)$ az $\frac{o(g)}{\varphi(n)}$ hányadost. Ekkor $A(G) = \frac{\sum_{g\in G} a(g)}{n} = \frac{\Psi(G)}{n\cdot\varphi(n)}$ az $a(g)$ számok számtani közepe, erről láttuk korábban, hogy ciklikus csoport esetén 1 és γ közt van, ahol $\gamma = 1,9435\ldots$. Tudjuk, hogy ha rendre $H(G), M(G), A(G), N(G)$ jelölik egy adott G csoportra az $a(g)$ számok harmonikus, mértani, számtani és négyzetes közepét, akkor $H(G) \leq M(G) \leq A(G) \leq N(G)$ (sőt $n > 1$ miatt és mert pontosan egy elem rendje 1, ezért itt mindenhol szigorú egyenlőtlenség áll).

3.1. Harmonikus közép

Tekintsük a harmonikus közepet:

$$H(G) = \frac{n}{\sum_{g\in G} \frac{1}{a(g)}} = \frac{n}{\sum_{g\in G} \frac{\varphi(n)}{o(g)}} = \frac{n}{\varphi(n)} \cdot \frac{1}{\sum_{g\in G} \frac{1}{o(g)}}$$

3.1. Tétel. *G véges csoport esetén $H(G) \leq \frac{4}{3}$, és egyenlőség pontosan $G \simeq C_2$ esetén van.*

Bizonyítás. Tudjuk, hogy $1 < \frac{n}{\varphi(n)} \leq 2$, és pontosan akkor 2, ha $n = 2^k$, tehát $H(G) \leq 2 \cdot \frac{1}{\sum_{g\in G} \frac{1}{o(g)}}$.

Ha $p \mid n$, ahol p prím, akkor

$$\sum_{g\in G} \frac{1}{o(g)} \geq 1 + \frac{p-1}{p},$$

mert ekkor van egy p rendű g elem, és a g által kifeszített p rendű részcsoport elemrendjeit véve ez adódik. Ekkor

$$\frac{1}{\sum_{g\in G} \frac{1}{o(g)}} \leq \frac{1}{1 + \frac{p-1}{p}} = \frac{p}{2\cdot p - 1} \leq \frac{2}{3},$$

és $\frac{p}{2\cdot p-1}$ monoton fogyó sorozat, ami a $\frac{2}{3}$-ot $p = n = 2$ esetén veszi fel.

A fentieket egybevetve látszik az alábbi:

$$H(G) \leq \frac{n}{\varphi(n)} \cdot \frac{1}{\sum_{g\in G} \frac{1}{o(g)}} \leq 2 \cdot \frac{2}{3} = \frac{4}{3},$$

és egyenlőség pontosan $n = 2$ esetben teljesül. $\square$

Amennyiben az $a(g)$-k helyett az $o(g)$-k harmonikus közepét vettük volna, úgy $n = p$-re

$$\frac{n}{\sum_{g\in G}\frac{1}{o(g)}} = p \cdot \frac{p}{2\cdot p - 1} = \frac{p^2}{2\cdot p - 1},$$

tehát ez bármilyen nagy lehet.

Végezetül meghatározzuk a $H(G)$ illetve az $A(G)$ értékeket abban az esetben, amikor G prímhatványrendű ciklikus csoport.

$$H(C_{p^k}) = \frac{p^k}{p^k - p^{k-1}} \cdot \frac{1}{1 + \frac{p-1}{p} + \frac{p^2-p}{p^2} + \ldots + \frac{p^k-p^{k-1}}{p^k}} = \frac{p}{p-1} \cdot \frac{p}{k\cdot(p-1)+p}$$

$$A(C_{p^k}) = \frac{p^{2k+1}+1}{(p^2-1)\cdot p^{2k-1}}$$

Vagyis az értékek $p = 2$ esetén a következőképpen alakulnak.

$$H(C_{2^k}) = 2 \cdot \frac{1}{1 + k\cdot\frac{1}{2}} = \frac{4}{k+2} \leq \frac{4}{3}$$

$$A(C_{2^k}) = \frac{2^{2k+1}+1}{3\cdot 2^{2k-1}} > \frac{1}{3}\cdot\frac{2^{2k+1}}{2^{2k-1}} = \frac{4}{3}$$

3.2. Négyzetes közép

Tekintsük egy véges G csoport elemeinek négyzetes közepét:

$$N(G) = \sqrt{\sum_{g\in G} \frac{a(g)^2}{n}} = \sqrt{\frac{\sum_{g\in G} o(g)^2}{n \cdot \varphi(n)^2}}$$

3.2. Tétel. *G véges csoport esetén $N(G)$ bármilyen nagy lehet, nem adható rá felső korlát.*

Bizonyítás. A négyzetes közepet tekintve tudjuk, hogy $A(G) \leq N(G)$, és a ciklikus csoportokra $n > 1$ esetén $1 < A(C_n) \leq N(C_n)$.

Subhrajyoti Saha [9] cikke alapján tudjuk, hogy az $R_l(G) = \sum_{g\in G} o(g)^l$ jelöléssel, ahol $l \in \mathbb{Z}$

$$R_l(C_{p^k}) = 1 + \frac{p-1}{p} \cdot \sum_{r=1}^{k} p^{r\cdot(l+1)}$$

ahol p prím ([9, Lemma 5]), illetve általában egy ciklikus csoportra

$$R_l(C_n) = \prod_{i=1}^{k} R_l(C_{p_i^{r_i}})$$

ahol $n = \prod_{i=1}^{k} p_i^{r_i}$ az n prímtényezős felbontása ([9, Lemma 6]). Ezt alkalmazva $l = 2$ esetre kapjuk, hogy

$$N(C_n) = \sqrt{\sum_{g\in G} \frac{a(g)^2}{n}} = \sqrt{\frac{\sum_{g\in G} o(g)^2}{n \cdot \varphi(n)^2}} = \sqrt{\frac{R_2(C_n)}{n \cdot \varphi(n)^2}} = \prod_{i=1}^{k} \sqrt{\frac{1 + p_i^2 \cdot (p_i - 1) \cdot \frac{p_i^{3\cdot r_i}-1}{p_i^3-1}}{p_i^{r_i} \cdot (p_i^{r_i} - p_i^{r_i-1})^2}}$$

Ha $n = p^k$ prímhatvány, akkor a következőt kapjuk.

$$N(C_{p^k})^2 = \frac{1 + p^2 \cdot (p-1) \cdot \frac{p^{3\cdot k}-1}{p^3-1}}{p^k \cdot (p^k - p^{k-1})^2} = \frac{p^{3\cdot k+2} - p^2 + 1}{(p^2+p+1) \cdot p^k \cdot (p^k - p^{k-1})^2} =$$

$$= \frac{p^{3\cdot k+2} - p^2 + 1}{p^{3\cdot k+2} - p^{3\cdot k+1} - p^{3\cdot k-1} + p^{3\cdot k-2}} = 1 + \frac{p^{3\cdot k+1} + p^{3\cdot k-1} - p^{3\cdot k-2} - p^2 + 1}{p^{3\cdot k+2} - p^{3\cdot k+1} - p^{3\cdot k-1} + p^{3\cdot k-2}}$$

Rögzített p-re ez a szám k növelésével egyre nagyobb lesz, így 1-nél mindig nagyobb marad. Tehát ha $N(C_n)$ felső becslésére vagyunk kíváncsiak, akkor elég minden prímre ahatárértéket venni, ahogy növeljük a kitevőt.

$$L(p) = lim_{k\to\infty} N(C_{p^k})^2 = 1 + \frac{1}{p}$$

Látható, hogy a prímek növelésével az érték csökken. Az első néhány prímre az alábbi értékeket kapjuk.

$$L(2) = 1,2247\ldots, L(3) = 1,1547\ldots, L(5) = 1,0954\ldots, L(7) = 1,0690\ldots$$

Tekintsük $n_i = p_1 \cdot p_2 \cdot \ldots \cdot p_i$ esetét, ahol p_i az i. prím.

$$L(n) = lim_{k\to\infty} N\left(C_{n_i^k}\right)^2 = \prod_{j=1}^{i}\left(1 + \frac{1}{p_j}\right) > \sum_{j=1}^{i}\frac{1}{p_j}$$

ugyanis egy kivételével a szorzat összes tagjából az 1-et, egy tagjából pedig $\frac{1}{p_j}$-t veszünk, és ezeket összeadjuk, akkor megkapjuk az első i prím reciprokösszegét, ami i növelésével a végtelenbe tart, így $N(C_n)$ bármilyen nagy lehet.

□

Megjegyzendő, hogy $G \simeq C_2^k$ esetén teljesül a következő:

$$N(G) = \sqrt{\frac{1 + 4 \cdot (2^k - 1)}{2^k \cdot 2^{2k-2}}} < \sqrt{\frac{2^{k+2}}{2^{3k-2}}} = 2^{-k+2}$$

Ez utóbbi k növelésével 0-hoz tart, így alsó korlát nem adható $N(G)$-re, és $H(G) \leq M(G) \leq A(G) \leq N(G)$ miatt a többi nevezetes középre sem.

3.3. Mértani közép

Jelölje $\varrho(G) = \prod_{g\in G} o(g)$ az elemrendek szorzatát.

3.3. Tétel. *G véges csoport esetén $M(G) < 1,48$, maximális értékét $G \simeq C_6$ esetén veszi fel.*

Bizonyítás. Elena Di Domenico, Carmine Monetta és Marialaura Noce közös [10] cikke, Garinzi és Patassini [11] cikke és Marius Tărnăuceanu [12] cikke alapján tudjuk, hogy adott n rendű csoportra $\varrho(G) \le \varrho(C_n)$, és egyenlőség pontosan akkor van, ha $G \simeq C_n$. Azt is tudjuk, hogy $G = A \times B$, $(a, b) = 1$ esetén, ahol a az A csoport rendje, b a B csoport rendje $\varrho(G) = \varrho(A)^b \cdot \varrho(B)^a$ ([12, Proposition 1.1.]), tehát egy adott $n = \prod p_i^{k_i}$ esetén

$$M\left(C_n\right) = \left(\prod_{g\in C_n} a(g)\right)^{\frac{1}{n}} = \left(\prod_{g\in C_n} \frac{o(g)}{\varphi(n)}\right)^{\frac{1}{n}} = \frac{\left(\prod_{g\in C_n} o(g)\right)^{\frac{1}{n}}}{\varphi(n)} = \prod \frac{\left(\prod_{g\in C_{p_i^{k_i}}} o(g)\right)^{\frac{1}{p_i^{k_i}}}}{\varphi(p_i^{k_i})} =$$

$$= \prod M\left(C_{p_i^{k_i}}\right)$$

Tekintsük $n = p^k$-t. Ekkor

$$\varrho(C_{p^k}) = p^{p-1} \cdot (p^2)^{p^2-p} \cdot \ldots \cdot (p^k)^{p^k-p^{k-1}} = p^{-(1+p+\ldots+p^{k-1})+k\cdot p^k} = p^{k\cdot p^k - \frac{p^k-1}{p-1}}$$

azaz

$$M(C_{p^k}) = \frac{(\varrho(C_{p^k}))^{\frac{1}{p^k}}}{\varphi(p^k)} = \frac{p^{k-\frac{p^k-1}{p^{k+1}-p^k}}}{p^k - p^{k-1}} = \frac{1}{p^{\frac{p^k-1}{p^{k+1}-p^k}}} \cdot \frac{p}{p-1}$$

Rögzített p esetén ez az érték akkor a legnagyobb, ha $\frac{p^k-1}{p^{k+1}-p^k} = \frac{1-\frac{1}{p^k}}{p-1}$ kicsi, azaz $k = 1$ esetén, mikor is $M(C_p) = \frac{p^{1-\frac{1}{p}}}{p-1}$. Megjegyzendő, hogy ha k tart a végtelenbe, akkor $M(C_{p^k})$ értéke tart $\frac{p}{p-1}$-hez. Ha a legnagyobb $M(C_n)$ értéket akarjuk megkapni, akkor tudnunk kell, hogy $M(C_p)$ mikor nagyobb 1-nél, ami pontosan akkor teljesül, ha $p^{p-1} > (p-1)^p$, azaz $p \in \{2, 3\}$ esetén, azaz $M(C_6) = 1,4708\ldots$ a maximuma $M(C_n)$-nek.

Tehát a ciklikus csoportok közül a C_6-ra a legnagyobb az $M(G)$ értéke. Ha volna egy n-rendű nem-ciklikus G csoport, amire $M(G) \ge M(C_6)$, akkor $M(C_n) > M(G) \ge M(C_6)$ állna fönn, ami nem lehetséges, tehát az összes csoport közül az $M(C_6)$ a legnagyobb.

□

4. Elemrendek szórása

Az előzőek felhasználásával vizsgálhatjuk egy csoport elemrendjeinek szórását. Legyen X egy egyenletes eloszlás szerint véletlenszerűen választott csoportelem rendje.

$$\mathbb{D}^2_G(X) = \mathbb{E}_G(X^2) - \mathbb{E}^2_G(X) = \frac{\sum_{g\in G} o^2(g)}{n} - \left(\frac{\sum_{g\in G} o(g)}{n}\right)^2 = \frac{R_2(G)}{n} - \frac{\Psi(G)^2}{n^2}$$

4.1. Prímhatvány rendű Abel csoportok szórása

Legyen G egy Abel csoport, $|G| = n = p^k$, és $G = C_{p^{r_1}} \times \ldots \times C_{p^{r_l}}$, ahol a kitevők közül $r = r_1$ szigorúan a legnagyobb, azaz $r_1 > r_i$ minden $i \geq 2$-re, r_l esetleg lehet 0, a többi $r_i > 0$. Legyen $H = C_{p^{q_1}} \times \ldots \times C_{p^{q_l}}$, ahol $q_1 = r_1 - 1$, valamelyik $i > 1$-re $q_i = r_i + 1$ úgy, hogy $q_i < r$, a többi $q_j = r_j$ így H rendje is n. A cél annak belátása, hogy G elemrendjeinek szórása nagyobb H elemrendjeinek szórásánál:

$$\mathbb{D}^2_G(X) = \frac{R_2(G)}{n} - \frac{\Psi(G)^2}{n^2} > \mathbb{D}^2_H(X) = \frac{R_2(H)}{n} - \frac{\Psi(H)^2}{n^2}$$

Ez ekvivalens a következővel:

$$n \cdot R_2(G) - \Psi(G)^2 > n \cdot R_2(H) - \Psi(H)^2$$

Illetve átrendezve:

$$n \cdot R_2(G) - \Psi(G)^2 - n \cdot R_2(H) + \Psi(H)^2 > 0$$

Jelölje a G csoportbeli p^i rendű elemek számát $db_G(i)$. Mivel r szigorúan nagyobb az összes többi kitevőnél, C_{p^r}-ben $p^r - p^{r-1}$ db p^r rendű elem van, ezek mellé a többiből bármit választva G-ben is p^r rendű elemet kapunk, máshogy pedig ilyet nem kaphatunk, ezért $db_G(r) = p^k - p^{k-1} = p^k \cdot \left(1 - \frac{1}{p}\right)$. Ebből következik, hogy az összes többi elemre $\sum_{i=0}^{r-1} db_G(i) = p^{k-1}$, így kapjuk a következő becsléseket:

$$n \cdot R_2(G) = n \cdot \sum_{i=0}^{r} p^{2i} \cdot db_G(i) \geq n \cdot p^{2r} \cdot p^k \cdot \left(1 - \frac{1}{p}\right) = p^{2k+2r} \cdot \left(1 - \frac{1}{p}\right)$$

Mivel a nem p^r rendű elemek maximális rendje p^{r-1}, adódik az alábbi:

$$\Psi(G) = \sum_{i=0}^{r} p^i \cdot db_G(i) \leq p^r \cdot p^k \cdot \left(1 - \frac{1}{p}\right) + p^{r-1} \cdot p^{k-1} = p^{k+r} \cdot \left(1 - \frac{1}{p}\right) + p^{k+r-2}$$

Ezt négyzetre emelve kapjuk:

$$\Psi(G)^2 \leq p^{2k+2r} \cdot \left(1 - \frac{1}{p}\right)^2 + 2 \cdot p^{2k+2r-2} \cdot \left(1 - \frac{1}{p}\right) + p^{2k+2r-4}$$

Így a következő alsó becslést kapjuk $n^2\mathbb{D}_G(X)$-re:

$$n \cdot R_2(G) - \Psi(G)^2 \geq p^{2k+2r} \cdot \left(1 - \frac{1}{p}\right) - p^{2k+2r} \cdot \left(1 - \frac{1}{p}\right)^2 - 2 \cdot p^{2k+2r-2} \cdot \left(1 - \frac{1}{p}\right) - p^{2k+2r-4} =$$

$$= p^{2k+2r} \cdot \left(\frac{1}{p} - \frac{1}{p^2}\right) - 2 \cdot p^{2k+2r-2} \cdot \left(1 - \frac{1}{p}\right) - p^{2k+2r-4} = p^{2k+2r-1} - 3 \cdot p^{2k+2r-2} + 2 \cdot p^{2k+2r-3} - p^{2k+2r-4}$$

Hasonlóan becsülhetjük a H csoportra vonatkozó adatokat, azzal a különbséggel, hogy ott már nem biztos, hogy van szigorúan legnagyobb kitevő, ezért $p^k - p^{k-1} \leq db_H(r-1) \leq p^k - 1 < p^k$. Ennek felhasználásával kapjuk a következő becslést:

$$n \cdot R_2(H) = n \cdot \sum_{i=0}^{r-1} p^{2i} \cdot db_H(i) \leq n \cdot p^{2r-2} \cdot p^k = p^{2k+2r-2}$$

Az elemrendösszegre az alábbi adódik:

$$\Psi(H) = \sum_{i=0}^{r-1} p^i \cdot db_H(i) \geq p^{r-1} \cdot p^k \cdot \left(1 - \frac{1}{p}\right) = p^{k+r-1} \cdot \left(1 - \frac{1}{p}\right)$$

Ezt négyzetre emelve kapjuk:

$$\Psi(H)^2 \geq p^{2k+2r-2} \cdot \left(1 - \frac{1}{p}\right)^2$$

Ekkor a következő felső becslést kapjuk $n^2\mathbb{D}_H^2(X)$-ra:

$$n \cdot R_2(H) - \Psi(H)^2 \leq p^{2k+2r-2} - p^{2k+2r-2} \cdot \left(1 - \frac{1}{p}\right)^2 = 2 \cdot p^{2k+2r-3} - p^{2k+2r-4}$$

Ezek alapján rátérhetünk a szórásnégyzetek összehasonlítására:

$$n^2\mathbb{D}_G^2(X) - n^2\mathbb{D}_H^2(X) = n \cdot R_2(G) - \Psi(G)^2 - n \cdot R_2(H) + \Psi(H)^2 \geq$$

$$\geq p^{2k+2r-1} - 3 \cdot p^{2k+2r-2} + 2 \cdot p^{2k+2r-3} - p^{2k+2r-4} - 2 \cdot p^{2k+2r-3} - p^{2k+2r-4} =$$

$$= p^{2k+2r-1} - 3 \cdot p^{2k+2r-2} - 2 \cdot p^{2k+2r-4} > 0$$

amennyiben $p > 3$ teljesül. Ebből következik, hogy p^k rendű Abel csoportok esetén ($p > 3$) a legnagyobb szórása a ciklikus csoportnak van.

4.2. A becslés élesítése

Az előző fejezet alapján $\mathbb{D}_G^2(X) - \mathbb{D}_H^2(X) > p^{2r-4} \cdot (p^3 - 3 \cdot p^2 - 2)$, de ez utóbbi $p = 2, 3$ esetén negatív ($-6 \cdot 2^{2r-4}$ illetve $-2 \cdot 3^{2r-4}$), így cél a becslés javítása.

Vegyük észre, hogy $n \cdot R_2(G)$ alsó becslésében csak a legnagyobb (p^r) rendű elemeket számoltuk, ám ha az egyes csoportelemek C_{p^r}-beli részét tekintjük, akkor magának a csoportelemnek a rendje legalább a C_{p^r}-beli részének a C_{p^r}-beli rendje, azaz felírható az alábbi becslés:

$$n \cdot R_2(G) \geq n \cdot R_2(C_{p^r}) \cdot p^{k-r} \geq p^{2k-r} \cdot \sum_{i=0}^{r} \left(p^{2i} \cdot \left(p^i - p^{i-1}\right)\right) = p^{2k-r} \cdot \left(\frac{p^{3r+3} - 1}{p^3 - 1} - \frac{p^{3r+2} - p^2}{p^3 - 1}\right) =$$

$$= p^{2k-r} \cdot \frac{p^{3r+3} - p^{3r+2} + p^2 - 1}{p^3 - 1} > p^{2k-r} \cdot \frac{p^{3r+3} - p^{3r+2}}{p^3 - 1}$$

Ha ezt összehasonlítjuk a korábbi ($n \cdot R_2(G) \geq p^{2k+2r} - p^{2k+2r-1}$) becsléssel, akkor különbséget hozzáadhatjuk az eddigi becsléssel a szórásnégyzetek különbségéhez:

$$n^2 \mathbb{D}_G^2(X) - n^2 \mathbb{D}_H^2(X) = n \cdot R_2(G) - \Psi(G)^2 - n \cdot R_2(H) + \Psi(H)^2 \geq$$

$$\geq \left(p^{2k+2r-1} - 3 \cdot p^{2k+2r-2} - 2 \cdot p^{2k+2r-4}\right) + \frac{1}{p^3 - 1} \cdot \left(p^{2k+2r} - p^{2k+2r-1}\right) =$$

$$= p^{2k+2r-4} \cdot \left(\left(p^3 - 3 \cdot p^2 - 2\right) + \frac{1}{p^3 - 1} \cdot \left(p^4 - p^3\right)\right)$$

Ez utóbbi, most hozzáadott érték $p = 3$ esetében $\frac{1}{3^3-1} \cdot (3^4 - 3^3) = \frac{1}{26} \cdot (81 - 27) = \frac{54}{26} > 2,07$, vagyis ez több, mint az eredeti becslésbeli érték abszolútértéke, azaz így $p = 3$ esetben is bizonyítást nyert, hogy a különbség nagyobb mint nulla, azaz $\mathbb{D}_G(X) > \mathbb{D}_H(X)$.

Érdemes megjegyezni, hogy sem az előző, sem a mostani becslésben nem használtuk fel azt a tényt, hogy H szinte ugyan úgy néz ki, mint G, csupán hogy a maximális elemrend eggyel csökkent, illetve hogy a G csoport ciklikusokra való felbontásában csak egy legnagyobb rendű csoport van. Így kimondhatjuk az alábbi tételt:

4.1. Tétel. *Ha G és H azonos, $p > 2$ esetén p^k rendű csoportok, G maximális elemrendje p^r, amely rendű elemből pontosan $p^k - p^{r-1}$ darab van, H maximális elemrendje p^{k-1}, akkor a G csoport elemrendjeinek szórása nagyobb, mint H elemrendjeinek szórása, azaz $\mathbb{D}_G(X) > \mathbb{D}_H(X)$.*

4.3. A $p = 2$ eset

Hátra van még azon eset vizsgálata, ahol a csoportok rendje 2-hatvány. Itt a következőképpen fogunk eljárni: először a G csoport szórását hasonlítjuk össze a H csoport szórásával, ahol r legalább 2-vel nagyobb, mint az utána következő legnagyobb r_i, H pedig két lépésben kapható meg G-ből: mindkét lépésben a maximális r-et csökkentjük 1-gyel, és egy másik r_i-t növelünk (ekkor eredetileg akár két r_i is lehet nulla), tehát H maximális elemrendje p^{r-2} lesz. Második lépésben C_{p^k} szórását hasonlítjuk össze $C_{p^{k-1}} \times C_p$ szórásával.

Az előző fejezetbeli élesítést felhasználva és alkalmazva $p = 2$-re kapjuk az alábbi becslést:

$$n \cdot R_2(G) \geq p^{2k-r} \cdot \frac{p^{3r+3} - p^{3r+2}}{p^3 - 1} = p^{2k+2r-4} \cdot \frac{p^7 - p^6}{p^3 - 1} = 2^{2k+2r-4} \cdot \frac{64}{7}$$

Mivel tudjuk, hogy p^{r-1} rendű elem is csak egyféleképpen adódhat, illetve $2^l - 2^{l-1} = 2^{l-1}$ felhasználásával pontosíthatjuk a $\Psi(G)$-re adott becslést is:

$$\Psi(G) \leq 2^r \cdot 2^{k-1} + 2^{r-1} \cdot 2^{k-2} + 2^{r-2} \cdot 2^{k-2} = 2^{k+r-2} \cdot \left(2 + \frac{1}{2} + \frac{1}{4}\right) = 2^{k+r-2} \cdot \frac{11}{4}$$

Ezt négyzetre emelve kapjuk a következőt:

$$\Psi(G)^2 \leq 2^{2k+2r-4} \cdot \frac{121}{16}$$

Így a szórásnégyzetre az alábbi becslést kapjuk:

$$n^2 \mathbb{D}_G^2(X) = n \cdot R_2(G) - \Psi(G)^2 \geq 2^{2k+2r-4} \cdot \frac{177}{112}$$

Az $n \cdot R_2(H)$ értékét az eddigiekhez hasonlóan becsülhetjük, figyelembe véve a maximális elemrend csökkenését:

$$n \cdot R_2(H) \leq p^k \cdot p^{2r-4} \cdot p^k = 2^{2k+2r-4}$$

A bizonyításhoz ennyi elég is lenne, hiszen ez kivonva az előbbi $n^2 \mathbb{D}_G^2(X)$-ből még mindig pozitív lesz, és ehhez egy négyzetszámot hozzáadva az összeg is nagyobb lesz, mint nulla, de a $\Psi(H)$-ra is tudjuk még élesíteni hasonlóan, mint ahogy az előző fejezetben tettük $n \cdot R_2(G)$-vel:

$$\Psi(H) \geq p^{k-(r-2)} \cdot \Psi(C_{p^{r-2}}) = p^{k-r+2} \cdot \frac{p^{2r-3} + 1}{p + 1} > p^{k+r-2} \cdot \frac{p}{p + 1} = 2^{k+r-2} \cdot \frac{2}{3}$$

Ezt négyzetre emelve kapjuk a következőt:

$$\Psi(H)^2 > 2^{2k+2r-4} \cdot \frac{4}{9}$$

Tehát a fentieket összegezve és leosztve n^2-tel a szórásnégyzetek különbségére a következő becslés adódik:

$$\mathbb{D}^2_G(X) - \mathbb{D}^2_H(X) = \frac{R_2(G)}{n} - \frac{\Psi(G)^2}{n^2} - \frac{R_2(H)}{n} + \frac{\Psi(H)^2}{n^2} >$$

$$> 2^{2r-4} \cdot (\frac{177}{112} + \frac{4}{9} - 1) = 2^{2r-4} \cdot \frac{1033}{1008} > 2^{2r-4} > 0$$

Most tekintsük a $G \simeq C_{p^k}$, $H \simeq C_{p^{k-1}} \times C_p$ esetet. Ekkor tudjuk becsülni G szórását, $k = r$ figyelembevételével a korábbiakat alkalmazva:

$$n \cdot R_2(G) \geq p^k \cdot \frac{p^{3k+3} - p^{3k+2}}{p^3 - 1} = p^{4k} \cdot \frac{p^3 - p^2}{p^3 - 1} = 2^{4k} \cdot \frac{4}{7}$$

$\Psi(G)$-re a szokásos képletet alkalmazhatjuk:

$$\Psi(G) = \frac{p^{2k+1} + 1}{p + 1} = \frac{2^{2k+1}}{3} + \frac{1}{3}$$

Ezt négyzetre emelve kapjuk a következőt:

$$\Psi(G)^2 = \frac{1}{9} \cdot (2^{4k+2} + 2^{2k+2} + 1)$$

Így a szórásnégyzetre az alábbi becslést kapjuk, mely valóban pozitív $k \geq 2$ esetén:

$$n^2\mathbb{D}^2_G(X) = \frac{8}{63} \cdot 2^{4k} - \frac{1}{9} \cdot 2^{2k+2} - \frac{1}{9} = \frac{8}{63} \cdot 2^{4k} - \frac{4}{9} \cdot 2^{2k} - \frac{1}{9}$$

H elemrendjeit tekintve csak a p rendűekből lehet több, mint amennyit $C_{p^{k-1}}$ arányosan meghatározna.

$$n \cdot R_2(H) < n \cdot (R_2(C_{p^{k-1}}) + p \cdot (p-1)) \cdot p = p^{k+1} \cdot \left(\frac{p^{3k} - p^{3k-1} + p^2 - 1}{p^3 - 1} + p^2 - p \right) = \frac{1}{7} \cdot 2^{4k} + \frac{30}{7} \cdot 2^k$$

Hasonlóan becsülhetjük az elemrendek összegét:

$$\Psi(H) > \Psi(C_{p^{k-1}}) \cdot p = \frac{p^{2k-1}+1}{p+1} \cdot p > \frac{p^{2k}+p}{p+1}$$

Ezt négyzetre emelve kapjuk a következőt:

$$\Psi(H)^2 > \frac{p^{4k} + 2 \cdot p^{2k+1} + p^2}{(p+1)^2} = \frac{1}{9} \cdot 2^{4k} + \frac{1}{9} \cdot 2^{2k+2} + \frac{1}{9} \cdot 4$$

Így felírhatjuk $n^2\mathbb{D}^2_H(X)$-ra is az felső becslést:

$$n^2\mathbb{D}^2_H(X) < \frac{2}{63} \cdot 2^{4k} - \frac{4}{9} \cdot 2^{2k} + \frac{30}{7} \cdot 2^k - \frac{4}{9}$$

Ezek alapján rátérhetünk a szórásnégyzetek összehasonlítására:

$$n^2\mathbb{D}^2_G(X) - n^2\mathbb{D}^2_H(X) = n \cdot R_2(G) - \Psi(G)^2 - n \cdot R_2(H) + \Psi(H)^2 >$$

$$> \frac{6}{63} \cdot 2^{4k} - 4 \cdot 2^k + \frac{3}{9} = \frac{2}{21} \cdot 2^{4k} - \frac{30}{7} \cdot 2^k + \frac{1}{3}$$

Ez utóbbi $k > 1,82$ esetén mindig pozitív, azaz az azonos, 2-hatvány rendű csoportok közül a ciklikus csoport szórása nagyobb $C_{2^{k-1}} \times C_2$ szórásánál, illetve a legnagyobb rendű elem rendjét kettővel csökkentve mindig kisebb szórású csoportot kapunk, következésképpen a ciklikus csoport szórása a legnagyobb az Abel csoportok körében. Az előző fejezetekkel összevetve kimondhatjuk, hogy bármely prímhatvány rendet tekintve az Abel csoportok közül a ciklikus csoport szórása a legnagyobb.

4.4. Abel csoportok szórása

Subhrajyoti Saha már korábban is hivatkozott [9] cikkében szerepelt a következő állítás ($R_l(G) = \sum_{g\in G} o(g)^l$ jelöléssel, ahol $l \in \mathbb{Z}$, $l \neq 0$):

4.2. Tétel. *[9, Theorem 3]*

$$R_l(G \times H) \leq R_l(G) \cdot R_l(H)$$

ahol G, H véges csoportok, és egyenlőség pontosan abban az esetben áll fenn, ha a két csoport rendje relatív prím.

Ezt a tételt alkalmazzuk $l = 1, 2$-re.

Legyen G tetszőleges n rendű véges Aben csoport, azaz felírható a következő alakban: $G \simeq G_{p_1} \times \ldots \times G_{p_r}$, ahol p_i mind különböző prímek, G_{p_i} pedig p_i-hatvány Abel csoport, azaz alkalmazhatók rá az előző fejezetekben tárgyaltak.

Az $l = 2$ esetet alkalmazva az alábbi becslést kapjuk:

$$n \cdot R_2(G) = n \cdot \prod_{i=0}^{r} R_2(G_{p_i})$$

Hasonlóan, $l = 1$ alkalmazásával adódik az alábbi:

$$\Psi(G) = \prod_{i=0}^{r} \Psi(G_{p_i})$$

Ezt négyzetre emelve kapjuk:

$$\Psi(G)^2 = \left(\prod_{i=0}^{r} \Psi(G_{p_i})\right)^2 = \prod_{i=0}^{r} \Psi(G_{p_i})^2$$

Ekkor felírhatjuk $n^2\mathbb{D}_G^2(X)$-t is:

$$n^2\mathbb{D}_G^2(X) = n \cdot R_2(G) - \Psi(G)^2 = n \cdot \prod_{i=0}^{r} R_2(G_{p_i}) - \prod_{i=0}^{r} \Psi(G_{p_i})^2$$

Most már össze tudjuk hasonlítani két azonosrendű Abel csoport szórásnégyzeteinek különbségét, mely által bebizonyítható a következő tétel.

4.3. Tétel. *Ha G ciklikus csoport, H pedig vele azonos rendű nemciklikus Abel csoport, akkor a G csoport elemrendjeinek szórása nagyobb a H csoport elemrendjeinek szórásánál.*

Bizonyítás. Tekintsük a G_{p_i}, H_{p_i} csoportokból adódó adatokat a következőképpen: a p_1-hez tartozó csoportokra mindenképp igaz lesz az állítás (feltehetjük, hogy H_{p_1} nem ciklikus), a továbbiakban pedig indukciót alkalmazva egyesével vegyük hozzá a következő prímekhez tartozó adatokat, míg végül eljutunk a teljes csoportokig. Legyen $A \simeq G_{p_1} \times \ldots \times G_{p_i}, B \simeq H_{p_1} \times \ldots \times H_{p_i}$. Az indukciós feltevés miatt tudjuk, hogy teljesül $k \cdot R_2(A) - \Psi(A)^2 - k \cdot R_2(B) + \Psi(B)^2 > 0$, ahol $k = p_1 \cdot \ldots \cdot p_i$. Szeretnénk belátni, hogy $k \cdot R_2(A) \cdot p_{i+1}^{s_{i+1}} \cdot R_2(G_{p_{i+1}}) - \Psi(A)^2 \cdot \Psi(G_{p_{i+1}})^2 - k \cdot R_2(B) \cdot p_{i+1}^{s_{i+1}} \cdot R_2(H_{p_{i+1}}) + \Psi(B)^2 \cdot \Psi(H_{p_{i+1}})^2 > 0$

1. Első lépésként lássuk be, hogy teljesül a következő egyenlőtlegség:

$$k \cdot R_2(A) \cdot p_{i+1}^{s_{i+1}} \cdot R_2(G_{p_{i+1}}) - \Psi(A)^2 \cdot \Psi(G_{p_{i+1}})^2 - k \cdot R_2(B) \cdot p_{i+1}^{s_{i+1}} \cdot R_2(H_{p_{i+1}}) + \Psi(B)^2 \cdot \Psi(H_{p_{i+1}})^2 >$$

$$> k \cdot R_2(A) \cdot p_{i+1}^{s_{i+1}} \cdot R_2(G_{p_{i+1}}) - \Psi(A)^2 \cdot \Psi(G_{p_{i+1}})^2 - k \cdot R_2(A) \cdot p_{i+1}^{s_{i+1}} \cdot R_2(H_{p_{i+1}}) + \Psi(A)^2 \cdot \Psi(H_{p_{i+1}})^2$$

Ez ekvivalens az alábbival:

$$k \cdot R_2(B) \cdot p_{i+1}^{s_{i+1}} \cdot R_2(H_{p_{i+1}}) - \Psi(B)^2 \cdot \Psi(H_{p_{i+1}})^2 < k \cdot R_2(A) \cdot p_{i+1}^{s_{i+1}} \cdot R_2(H_{p_{i+1}}) - \Psi(A)^2 \cdot \Psi(H_{p_{i+1}})^2$$

Ezt átrendezve kapjuk:

$$\left(\Psi(A)^2 - \Psi(B)^2\right) \cdot \Psi(H_{p_{i+1}})^2 < (k \cdot R_2(A) - k \cdot R_2(B)) \cdot p_{i+1}^{s_{i+1}} \cdot R_2(H_{p_{i+1}})$$

Ez utóbbi pedig igaz, ugyanis az indukciós feltevés miatt $0 < \Psi(A)^2 - \Psi(B)^2 < k \cdot R_2(A) - k \cdot R_2(B)$, illetve $0 < \Psi(H_{p_{i+1}})^2 < p_{i+1}^{s_{i+1}} \cdot R_2(H_{p_{i+1}})$ minden esetben.

2. Második lépésként lássuk be az alábbi egyenlőtlenséget:

$$k \cdot R_2(A) \cdot p_{i+1}^{s_{i+1}} \cdot R_2(G_{p_{i+1}}) - \Psi(A)^2 \cdot \Psi(G_{p_{i+1}})^2 - k \cdot R_2(A) \cdot p_{i+1}^{s_{i+1}} \cdot R_2(H_{p_{i+1}}) + \Psi(A)^2 \cdot \Psi(H_{p_{i+1}})^2 =$$

$$= k \cdot R_2(A) \cdot \left(p_{i+1}^{s_{i+1}} \cdot R_2(G_{p_{i+1}}) - p_{i+1}^{s_{i+1}} \cdot R_2(H_{p_{i+1}})\right) - \Psi(A)^2 \cdot \left(\Psi(G_{p_{i+1}})^2 - \Psi(H_{p_{i+1}})^2\right) \geq$$

$$\geq k \cdot R_2(A) \cdot \left(\Psi(G_{p_{i+1}})^2 - \Psi(H_{p_{i+1}})^2\right) - \Psi(A)^2 \cdot \left(\Psi(G_{p_{i+1}})^2 - \Psi(H_{p_{i+1}})^2\right)$$

Ez azért teljesül, mert $G_{p_{i+1}} \simeq C_{p_{i+1}}$, és prímhatvány csoportokra már korábban beláttuk, hogy $p_{i+1}^{s_{i+1}} \cdot R_2(C_{p_{i+1}}) - \Psi(C_{p_{i+1}})^2 - p_{i+1}^{s_{i+1}} \cdot R_2(H_{p_{i+1}})) + \Psi(H_{p_{i+1}})^2 \geq 0$, azaz igaz az alábbi egyenlőtlenség:

$$p_{i+1}^{s_{i+1}} \cdot R_2(G_{p_{i+1}}) - \Psi(G_{p_{i+1}})^2 \geq p_{i+1}^{s_{i+1}} \cdot R_2(H_{p_{i+1}}) - \Psi(H_{p_{i+1}})^2$$

3. Végül ennek nemnegatív voltát már nem nehéz belátni:

$$k \cdot R_2(A) \cdot \left(\Psi(G_{p_{i+1}})^2 - \Psi(H_{p_{i+1}})^2\right) - \Psi(A)^2 \cdot \left(\Psi(G_{p_{i+1}})^2 - \Psi(H_{p_{i+1}})^2\right) =$$

$$= \left(\Psi(G_{p_{i+1}})^2 - \Psi(H_{p_{i+1}})^2\right) \cdot (k \cdot R_2(A) - k \cdot R_2(B)) \geq 0$$

Ugyanis a szorzat mindkét tagja egyesével nemnegatív, hiszen azonos rendű csoportok esetén mind az elemrendek összege, mind az elemrendek négyzetösszege a ciklikus csoport esetén maximális.

Most összeolvasva az egyenlőtlenségek elejét és végét kapjuk az alábbit:

$$k \cdot R_2(A) \cdot p_{i+1}^{s_{i+1}} \cdot R_2(G_{p_{i+1}}) - \Psi(A)^2 \cdot \Psi(G_{p_{i+1}})^2 - k \cdot R_2(B) \cdot p_{i+1}^{s_{i+1}} \cdot R_2(H_{p_{i+1}}) + \Psi(B)^2 \cdot \Psi(H_{p_{i+1}})^2 > 0$$

Ez pont az, amit bizonyítani akartunk.

□

A bizonyításból látható, hogy nem csupán akkor nagyobb az egyik csoport szórásnégyzete egy másikénál, ha az előbbi ciklikus, hanem ha egyesével az egyes prímekhez tartozó szórásnégyzetek mind az előbbi csoportban nagyobbak (illetve nem kisebbek). Így például az előző fejezet alapján ez teljesül, ha $p > 2$ esetén a G_p-hez tartozó maximális elemrend nagyobb, mint a H_p-hez tartozó maximális elemrend, $p = 2$ esetén a G_2-höz tartozó maximális elemrend páros sokkal több, mint H_2-höz tartozó maximális elemrend, vagy G_2 ciklikus.

4.5. p-csoportok szórása

Ha nem várjuk el a H csoport kommutativitását, akkor is tudunk a szórására becslést adni, még ha gyengébbet is, mint kommutatív esetben. A $p = 2$ esethez hasonlóan általános p-re is tudjuk becsülni a ciklikus csoport szórását.

$$n \cdot R_2(G) \geq p^k \cdot \frac{p^{3k+3} - p^{3k+2}}{p^3 - 1} = p^{4k} \cdot \frac{p^3 - p^2}{p^3 - 1}$$

$\Psi(G)$-re a szokásos képletet alkalmazhatjuk:

$$\Psi(G) = \frac{p^{2k+1} + 1}{p + 1}$$

Ezt négyzetre emelve kapjuk a következőt:

$$\Psi(G)^2 = \frac{p^{4k+2} + 2 \cdot p^{2k+1} + 1}{(p + 1)^2}$$

Így a szórásnégyzetre az alábbi becslést kapjuk:

$$n^2 \mathbb{D}_G^2(X) \geq \frac{p^{4k+4} - p^{4k+3} - 2 \cdot p^{2k+4} + 2 \cdot p^{2k+1} - p^3 + 1}{(p^3 - 1) \cdot (p + 1)^2}$$

Legyen H nem ciklikus csoport, ekkor a maximális elemrendje legfeljebb p^{k-1}. Az $R_2(H)$ értékét felülről becsülhetjük azt feltételezve, hogy minden elem rendje maximális:

$$n \cdot R_2(H) < p^k \cdot p^k \cdot (p^{k-1})^2 = p^{4k-2}$$

Ekkor becsülhetjük a szórásnégyzetek különbségét, felhasználva, hogy $\Psi(H)^2 > 0$.

$$n^2 \mathbb{D}_G^2(X) - n^2 \mathbb{D}_H^2(X) > n \cdot R_2(G) - \Psi(G)^2 - n \cdot R_2(H) >$$

$$> \frac{p^{4k+4} - 2 \cdot p^{4k+3} - 2 \cdot p^{4k+2} - p^{4k+1} + p^{4k} + 2 \cdot p^{4k-1} + p^{4k-2} - 2 \cdot p^{2k+4} + 2 \cdot p^{2k+1} - p^3 + 1}{(p^3 - 1) \cdot (p + 1)^2}$$

Ez $p > 2$ esetén pozitív, azaz ekkor a ciklikus csoport szórása a legnagyobb.

A $p = 2$ esetben már bebizonyítottuk, hogy ha a p^k elemű H csoportban a maximális elemrend legfeljebb p^{k-2}, akkor H elemrendjeinek szórása kisebb, mint C_{p^k} elemrendjeinek a szórása, így már csak az az eset van hátra, amikor $\exists m \in H : o(m) = 2^{k-1}$. Ekkor $\langle m \rangle = M \simeq C_{p^{k-1}} < H$, $|H : M| = 2$, azaz M normálosztó H-ban, így egy $h \in (H \setminus M)$ elemmel konjugálva m-et az m-nek egy hatványát kapjuk. Ekkor a H csoport esetekre bontással meghatározható, ezen csoportok felhasznált tulajdonságait vizsgálta Herendi Zsolt: *Elemrendek összege csoportokban* című szakdolgozatában, amelyre támaszkodni fogunk. Az első esetben $h^{-1}mh = m$, ekkor a csoport kommutatív, ezt az esetet már megvizsgáltuk az előző fejezetekben.

A második esetben $h^{-1}mh = m^{-1}$ (ezek az adott rendhez tartozó diédercsoportok és az általánosított kvaterniócsoportok), a negyedik esetben $h^{-1}mh = m^{2^{k-2}-1}$, mindkét esetben az következik, hogy $o(h) \leq 4$. Ekkor könnyen becsülhetjük $R_2(H)$ értékét:

$$n \cdot R_2(H) \leq n \cdot R_2(M) + n \cdot 2^{k-1} \cdot 2^4 = \frac{1}{14} \cdot 2^{4k} + 2^{2k+3}$$

Innen ismét $\Psi(H)^2 > 0$ tudatában becsülhetjük a szórásnégyzetek különbségét:

$$n^2\mathbb{D}^2_G(X) - n^2\mathbb{D}^2_H(X) > n \cdot R_2(G) - \Psi(G)^2 - n \cdot R_2(H) >$$

$$> \frac{1}{18} \cdot 2^{4k} - \frac{76}{9} \cdot 2^{2k} - \frac{1}{9}$$

Ez $k > 3$ esetén pozitív, $k = 3$ esetén a diéder- és kvaterniócsoport szórását könnyen ellenőrizhetjük, hogy kisebbek C_8 szórásánál.

Utolsóként a harmadik esetet vizsgáljuk, mikor is $k \geq 4$ esetén $h^{-1}mh = m^{2^{k-2}+1}$ (ekkor $H \simeq M_n(2)$). Ekkor az alábbi módon számítható ki:

$$n \cdot R_2(H) = n \cdot R_2(M) + n \cdot 4 \cdot R_2(C_{2^{k-2}}) = \frac{1}{14} \cdot 2^{4k} + \frac{1}{224} \cdot 2^{4k}$$

Vagyis a különbség a következőképpen becsülhető:

$$n^2\mathbb{D}^2_G(X) - n^2\mathbb{D}^2_H(X) > n \cdot R_2(G) - \Psi(G)^2 - n \cdot R_2(H) >$$

$$> \frac{103}{2016} \cdot 2^{4k} - \frac{76}{9} \cdot 2^{2k} - \frac{1}{9}$$

Ez szintén pozitív, így kimondható, hogy bármely p-csoport szórása legfeljebb az azonos rendű ciklikus csoport szórása lehet.

4.6. Nilpotens csoportok szórása

Mint az már korábban szerepelt, $R_l(G \times H) \leq R_l(G) \cdot R_l(H)$, ahol G, H véges csoportok, és egyenlőség pontosan abban az esetben áll fenn, ha a két csoport rendje relatív prím. Ugyanakkor azt is tudjuk, hogy nilpotens csoport felírható a p-Sylowjainak direkt szorzataként, és mivel minden p-csoportról tudjuk, hogy szórása legfeljebb az azonos rendű ciklikus csoport szórása, így az Abel-csoportok szórásánál kimondott tétel bizonyítását az azt követő megjegyzés alapján felhasználva kimondhatjuk a következő állítást.

4.4. Tétel. *Ha G ciklikus csoport, H pedig vele azonos rendű nemciklikus nilpotens csoport, akkor a G csoport elemrendjeinek szórása nagyobb a H csoport elemrendjeinek szórásánál.*

5. Az elemrendek átlaga véges csoportokban

A dolgozat témájához kapcsolatosan felmerülő kérdések megválaszolásában hasznos lehet tudni, hogy adott rendű elemből hány darab van a csoportban. Ebben a fejezetben először erre vonatkozó becsléseket ismertetünk, majd a továbbiakban a 5.12. Tétel bizonyításában való alkalmazását nézzük meg. Legyen G egy véges, n rendű csoport.

5.1. Becslések az adott rendű elemek darabszámára

Jelölje $i_j(G)$ a j rendű elemek darabszámát a G csoportban, ekkor $\Psi(G) = 1 \cdot 1 + 2 \cdot i_2(G) + 3 \cdot i_3(G) + \ldots$.

Thompson azt sejtette, hogy ha egy H véges csoportra és egy G véges feloldható csoportra minden j-re $i_j(H) = i_j(G)$, akkor H is feloldható, ám egyelőre még nincs bizonyítva.

T. C. Burness és S. D. Scott [13] cikke alapján igazak a következő tételek:

5.1. Tétel. *[13, Corollary 1.2.] G véges csoportra ha $i_2(G) \geq \frac{3}{4} \cdot n$, akkor G elemi Abel 2-csoport.*

5.2. Tétel. *[13, Lemma 2.9., Lemma 2.16.] Ha G véges, nem feloldható csoport, akkor $i_2(G) \leq \frac{4}{15} \cdot n - 1$, illetve $i_3(G) \leq \frac{7}{20} \cdot n - 1$.*

Belátható az alábbi tétel is:

5.3. Tétel. *$i_2(G) + 1 \leq \sum_{\chi \in Irr(G)} \chi(1)$, ahol $Irr(G)$ a G csoport irreducibilis reprezentációinak halmaza.*

Bizonyítás. Jelölje $\nu(\chi) = \frac{1}{n} \sum_{g \in G} \chi(g^2)$ a $\chi \in Irr(G)$ Frobenius-Schur indikátorát. Erről tudjuk, hogy az értéke $-1, 0$ vagy 1 lehet.

Jelölje $\gamma(g) = |\{x \in G : x^2 = g\}|$ azon elemek számát, melyek négyzete g.

Ha γ-t felbontjuk irreducibilis karakterek lineáris kombinációjaként, akkor $\chi \in Irr(G)$ együtthatója $\langle \gamma, \chi \rangle = \frac{1}{n} \sum_{g \in G} \gamma(g)\chi(g) = \frac{1}{n} \sum_{g \in G} \chi(g^2) = \nu(\chi)$, azaz $\gamma = \sum_{\chi \in Irr(G)} \nu(\chi) \cdot \chi$.

$i_2(G) + 1 = \gamma(1) = \sum_{\chi \in Irr(G)} \nu(\chi) \cdot \chi(1) \leq \sum_{\chi \in Irr(G)} \chi(1)$ □

A továbbiakban jelölje ezt az összeget $T(G) = \sum_{\chi \in Irr(G)} \chi(1)$.

5.2. Az elemrendek átlaga

Jelölje $o(G)$ az elemrendek átlagát, azaz $o(G) = \frac{\Psi(G)}{n}$, ahol G egy n rendű véges csoport. Erről könnyen belátható, hogy $n > 1$ esetén $o(G) \geq \frac{3}{2}$ (hiszen $\Psi(G) \geq 1+2\cdot(n-1)$), és látható, hogy elemi Abel 2-csoportokra $o(G) = 2 - \frac{1}{n}$, minden egyéb esetben pedig $o(G) \geq 2 + \frac{1}{n}$ (egy 2-nél nagyobb rendű elem inverzének rendje is nagyobb, mint 2, így $\Psi(G) \geq 1 + o(g) + o(g^{-1}) + 2 \cdot (n-3) \geq 2n+1$). Páratlan n esetén $o(G) \geq 3 - \frac{2}{n} \geq \frac{7}{3}$. 4.2 alapján adódik, hogy ha $G = A \times B$, ahol a és b rendre A és B rendjei, $(a, b) = 1$, akkor $o(G) = o(A) \cdot o(B)$.

Marcel Herzog, Patrizia Longobardi és Mercede Maj [17] cikke alapján a következő tételt is állíthatjuk.

5.4. Tétel. *[17, Lemma 3.1] Legyen G véges csoport, N nemtriviális normálosztó. Ekkor $o(G/N) < o(G)$.*

Bizonyítás. Írjuk fel a G csoportot az N normálosztó baloldali mellékosztályainak uniójaként: $G = N \cup x_1N \cup \ldots \cup x_sN$, és $\Psi(G) = \Psi(N) + \Psi(x_1N) + \ldots + \Psi(x_sN)$.

Ekkor bármely $x \in G$-re $\Psi(x_iN) \geq |N| o_{G/N}(xN)$, ugyanis $h \in N$, $o(xh) = k$ esetén $(xh)^k = 1$, és $(xN)^k = (xhN)^k = N$, így $o_{G/N}(xN)|k$, azaz $o(xh) \geq o_{G/N}(xN)$.

Ennek alapján teljesül a következő:

$$\Psi(G) \geq \Psi(N) - |N| + |N| \cdot \left(1 + o_{G/N}(x_1N) + \ldots + o_{G/N}(x_sN)\right) = \psi(N) - |N| + |N|\Psi(G/N)$$

Ezt leosztva G rendjével és $\Psi(H) > |H|$ felhasználásával adódik:

$$o(G) > \frac{\Psi(N) - |N|}{|G|} + \frac{|N|}{|G|}\Psi(G/N)$$

□

Mihai-Silviu Lazorec, Marius Tărnăuceanu [14] cikke alapján pontosabban be tudjuk szorítani $o(G)$ lehetséges értékét.

5.5. Tétel. *[14, Theorem 1.5.] Legyen G véges csoport.*

Ha $o(G) < o(S_3) = \frac{13}{6}$, akkor G elemi Abel 2-csoport.

Ha $o(G) < o(C_4) = \frac{11}{4}$, akkor G feloldható.

Ezen bizonyításhoz is felhasználták $i_j(G)$ becsléseit, a tételből pedig levonhatjuk az alábbi következtetést:

5.6. Következmény. *G véges csoport esetén $o(G) \notin [2, \frac{13}{6})$.*

A. Jaikin-Zapirain [15] cikke alapján a G csoport konjugáltosztályainak számát $k(G)$-vel jelölve teljesül az alábbi:

5.7. Tétel. *[15, Lemma 2.7., Corolllary 2.10.] G véges csoportra $k(G) \geq o(G) \geq o(Z(G))$.*

Bizonyítás. Legyen $x \in G$, $m = min\{o(y) : y \in xZ(G)\}$, és legyen y az az elem, amelyre a minimum adódik, azaz $y \in xZ(G)$, $o(y) = m$. Legyen továbbá $Z = Z(G)$.

Legyen $a \in Z$, ekkor $(ya)^m = a^m \in Z^(m) := \{z^m | z \in Z\}$, azaz $l = o_{G/Z^m}(ya)$-ra $l|m$, továbbá van egy $z \in Z$, amire $(ya)^l = z^m$. Ekkor $\left(yaz^{-\frac{m}{l}}\right)^l = 1$, tehát $l \geq m$ az m minimalitása miatt, így $l = m$.

Az $o(G)$ mintájára a G csoport tetszőleges X részhalmazára is definiáljuk $o(X)$-et, mint az elemeinek rendjeinek átlagát. Mivel $o_{G/Z^m}(ya)|o(ya) = o_G(ya)$, így kapjuk az alábbit:

$$o(ya) = m \cdot o((ya)^m) = m \cdot o(a^m) = m \cdot \frac{o(a)}{lnko(m, o(a))} \geq o(a)$$

Ekkor $o(xZ(G))$-t felírva kapjuk:

$$o(xZ) = \frac{1}{|Z(G)|} \sum_{g \in xZ} o(g) = \frac{1}{|Z(G)|} \sum_{a \in Z} o(ya) \geq \frac{1}{|Z(G)|} \sum_{a \in Z} o(a) = o(Z(G))$$

Tehát ebből adódik $o(G) \geq o(Z(G))$.

A tétel másik feléhez a Burnside lemmát használjuk, melynek speciális esete az alábbi:

$$k_G = \frac{1}{|G|} \sum_{x \in G} |C_G(x)|$$

Ebből következik $k(G) \geq o(G)$, ugyanis $|C_G(x)| \geq \langle x \rangle$ így $|C_G(x)| \geq |C_G(x)N/N| \geq |\langle x \rangle| = o(x)$ minden $x \in G$-re. □

5.3. Kapcsolat az elemrendek átlaga és a feloldhatóság közt

Korábban már láttunk több tételt, ami az elemrendek összegére, szorzatára, vagy ezekből képzett függvényekről jelentette ki, hogy ha az érték egy adott határ fölé esik, akkor a csoportra teljesülnek bizonyos tulajdonságok (például ciklikus, nilpotens, feloldható, stb). Az alább E. I. Khukhro, A. Moretó és M. Zarrin [16] cikkbeli sejtését Marcel Herzog, Patrizia Longobardi és Mercede Maj által [17] alapján bizonyítandó tétel ezekhez hasonló, ám itt felső korlátot fogunk adni. A bizonyításnak két fontos lemmája van, először azokat fogjuk több lépésben bebizonyítani, majd magát a 5.12. Tételt.

Jelölje $\Pi(G)$ a G véges csoport rendjének prímosztóinak halmazát, azaz $\Pi(G) = \{p \text{ prím} : p||G|\}$.

Egy csoportot p-feloldhatónak mondunk, ha van olyan normállánca, melynek faktorai vagy p-csoportok, vagy a rendjük relatív prím p-hez. Véges csoport pontosan akkor feloldható, ha p-feloldható minden $p \in \Pi(G)$-re.

Szükség lesz az alábbi, Hongfei Pan és Xianhua Li által [19] alapján bizonyított tételre.

5.8. Tétel. *Legyen $p \geq 7$ prím, G véges nem p-feloldható csoport, és $p \equiv 3$ mod 4 esetén $g_1(p) = p-1$, $p \equiv 1$ mod 4 esetén $g_1 = \frac{p(p^2-1)}{p^2+p+2}$, valamint $g_2 = \frac{p(p-2)}{p-1}$. Ekkor vagy $T(G) = \frac{|G|}{g_1(p)}$, vagy $T(G) = \frac{|G|}{g_2(p)}$, vagy $T(G) \leq \frac{|G|}{p-1}$.*

Ezt fel fogjuk használni az első lemma bizonyításához.

5.9. Lemma. *Ha p prím, G véges nem-feloldható csoport, $p \geq 17$ és $o(G) \leq o(A_5)$, akkor G p-feloldható.*

W. M. Potter bizonyította [20] cikkében a következő tételt.

5.10. Tétel. *Legyen G véges csoport, $\varphi \in Aut(G)$.*

Ha φ több, mint $\frac{4}{15}|G|$ elemet invertál, akkor G feloldható.

Ha φ több, mint $\frac{3}{4}|G|$ elemet invertál, akkor G Abel csoport.

Ennek segítségével bizonyítható a következő lemma.

5.11. Lemma. *Legyen G nem feloldható véges csoport, $\varphi \in Aut(G)$. Ha φ legalább $\frac{2}{9}|G|$ elemet invertál, akkor vagy $G \simeq A_5$, vagy G-nek van egy nemtriviális feloldható normálosztója.*

Ezek alapján fog bizonyítást nyerni az alábbi tétel.

5.12. Tétel. *[17, Theorem B] Ha G véges csoportra $o(G) \leq o(A_5) = \frac{211}{60} \approx 3,5167$, akkor vagy $G \simeq A_5$, vagy G feloldható.*

5.4. Az első lemma bizonyítása

Ebben a fejezetben az 5.9. Lemmát fogjuk bebizonyítani.

5.13. Tétel. *[17, Corollary 2.2.] Legyen p prím, G nem p-feloldható véges csoport. Ekkor teljesülnek az alábbi állítások.*

1. *Ha $p \geq 11$, akkor $i_2 < \frac{10}{99}|G|$.*
2. *Ha $p \geq 17$, akkor $i_2 < \frac{1}{15}|G|$.*
3. *Ha $p \geq 23$, akkor $i_2 < \frac{1}{20}|G|$.*

Bizonyítás. Tudjuk, hogy $i_2(G) < T(G)$, illetve $g_i(p) > p-2$, $i = 1, 2$-re, így $p \geq 11$ miatt $i_2(G) < T(G) < \frac{1}{p-2}|G|$.

$p = 11$-re $g_1(11) = 10$, $g_2(11) = \frac{99}{10}$, így $T(G) \leq \frac{10}{99}|G|$, vagyis $i_2(G) < \frac{10}{99}|G|$. Ha $p \geq 13$, akkor $i_2(G) < \frac{1}{11}|G| < \frac{10}{99}|G|$, azaz minden $p \geq 11$-re teljesül az első állítás.

$p \geq 17$-re $i_2(G) < \frac{1}{17-2}|G| = \frac{1}{15}|G|$, illetve $p \geq 23$ esetén $i_2(G) < \frac{1}{23-2}|G| = \frac{1}{21}|G| < \frac{1}{20}|G|$. □

Amint azt a 5.2 tétel kimondta, G véges nem feloldható csoport esetén $i_2(G) \leq \frac{4}{15} \cdot n - 1$, illetve $i_3(G) \leq \frac{7}{20} \cdot n - 1$, ezt fel fogjuk használni a következő állításban.

5.14. Tétel. *[17, Lemma 3.2.] Legyen G véges nem feloldható csoport.*

1. *$o(G) > \frac{187}{60} > 3,11$*
2. *Ha $i_2(G) \leq \frac{1}{20}|G|$, akkor $o(G) \geq \frac{71}{20} > 3,55$.*
3. *Ha $i_2(G) \leq \frac{10}{99}|G|$, akkor $o(G) \geq \frac{6827}{1980} > 3,4479$.*
4. *Ha $i_2(G) \leq \frac{1}{15}|G|$, akkor $o(G) > \frac{211}{60} = o(A_5)$.*
5. *Ha $i_2(G) \leq \frac{1}{16}|G|$ és $i_3(G) + 1 \leq \frac{1}{14}|G|$, akkor $o(G) \geq \frac{213}{56} > 3,8$.*

Bizonyítás. Legyen R a G-beli, 3-nál nagyobb rendű elemek halmaza, ennek számossága pedig r, azaz $R = \{x \in G : o(x) \geq 4\}$, $r = |R|$. Ekkor felírható

$$|G| = 1 + i_2(G) + i_3(G) + r$$

azaz átrendezve

$$r - i_2 = |G| - 2 \cdot i_2 - i_3 - 1$$

Továbbá az elemrendekre adható a következő becslés G nem-feloldható voltának figyelembevételével, ami miatt van egy legalább 5 rendű y eleme, amelynek inverzének rendje sem lehet 5-nél kisebb.

$$\Psi(G) \geq 1 + 2 \cdot i_2 + 3 \cdot i_3 + 4 \cdot r + 2 = 3 + 3 \cdot i_2 + 3 \cdot i_3 + 3 \cdot r + (r - i_2) = 3 \cdot |G| + (r - i_2)$$

1. Általános esetben az alábbi lesz igaz:

$$r - i_2 = |G| - 2 \cdot i_2 - (i_3 + 1) > |G| - \frac{8}{15}|G| - \frac{7}{20}|G| = \frac{7}{60}|G|$$

Azaz az elemrendek összegére adódik

$$\Psi(G) \geq 3 \cdot |G| + (r - i_2) > \frac{187}{60}|G|$$

Ezt leosztva G rendjével adódik az állítás.

2. $i_2(G) \leq \frac{1}{20}|G|$ esetén az előbbi számolás a következőképpen módosul:

$$r - i_2 = |G| - 2 \cdot i_2 - (i_3 + 1) \geq |G| - \frac{2}{20}|G| - \frac{7}{20}|G| = \frac{11}{20}|G|$$

Azaz az elemrendösszeg a következőképpen alakul:

$$\Psi(G) \geq 3 \cdot |G| + (r - i_2) \geq \frac{71}{20}|G|$$

3. $i_2(G) \leq \frac{10}{99}|G|$ esetén

$$r - i_2 = |G| - 2 \cdot i_2 - (i_3 + 1) \geq |G| - \frac{20}{99}|G| - \frac{7}{20}|G| = \frac{887}{1980}|G|$$

Azaz

$$\Psi(G) \geq 3 \cdot |G| + (r - i_2) \geq \frac{6827}{1980}|G|$$

4. $i_2(G) < \frac{1}{15}|G|$ esetén

$$r - i_2 = |G| - 2 \cdot i_2 - (i_3 + 1) > |G| - \frac{2}{15}|G| - \frac{7}{20}|G| = \frac{31}{60}|G|$$

Azaz

$$\Psi(G) \geq 3 \cdot |G| + (r - i_2) > \frac{211}{60}|G| = o(A_5)|G|$$

5. $i_2(G) \le \frac{1}{16}|G|$ és $i_3(G) + 1 \le \frac{1}{14}|G|$ esetén

$$r - i_2 = |G| - 2 \cdot i_2 - (i_3 + 1) \ge |G| - \frac{1}{8}|G| - \frac{1}{14}|G| = \frac{45}{56}|G|$$

Azaz

$$\Psi(G) \ge 3 \cdot |G| + (r - i_2) \ge \frac{213}{56}|G|$$

□

Most rátérhetünk a 5.9. Lemma bizonyítására.

5.15. Tétel. *[17, Lemma 3.3.] Legyen G véges nem feloldható csoport, p prím mely osztja G rendjét.*

1. *Ha $p \ge 11$ és $o(G) \le 3,4479$, akkor a G csoport p-feloldható.*
2. *Ha $p \ge 17$ és $o(G) \le o(A_5)$, akkor a G csoport p-feloldható.*
3. *Ha $p \ge 23$ és $o(G) \le 3,55$, akkor a G csoport p-feloldható.*

Bizonyítás. Az eseteket egyesével fogjuk vizsgálni.

1. $p \ge 11$ esetben ha G nem volna p-feloldható, akkor $i_2(G) < \frac{10}{99}|G|$ következne a 5.13. Tétel alapján, azaz az előző állítás miatt $o(G) > 3,4479$ volna, ami ellentmondás.
2. $p \ge 17$ esetben ha G nem volna p-feloldható, akkor $i_2(G) < \frac{1}{15}|G|$ következne a 5.13. Tétel alapján, azaz az előző állítás miatt $o(G) > o(A_5)$ volna, ami ellentmondás.
3. $p \ge 23$ esetben ha G nem volna p-feloldható, akkor $i_2(G) < \frac{1}{20}|G|$ következne a 5.13. Tétel alapján, azaz az előző állítás miatt $o(G) > 3,55$ volna, ami ellentmondás.

□

5.5. A második lemma bizonyítása

Ebben a fejezetben a 5.11. Lemmát fogjuk bizonyítani. Ehhez legyen $\varphi \in Aut(G)$ esetén

$$S(\varphi) = \{g \in G : g^{\varphi} = g^{-1}\}$$

azaz azon csoportelemek halmaza, melyeket az adott automorfizmus az inverzébe visz, illetve

$$r(G, \varphi) = \frac{|S(\varphi)|}{|G|}$$

mely ezen elemek csoportbéli arányát mutatja. Jelölje továbbá egy $x \in G$ elemre $x\varphi$ azt az automorfizmust, amelyre teljesül

$$g^{x\varphi} = (x^{-1} \cdot g \cdot x)^{\varphi}$$

Az alábbi, W. M. Potter által [20] alapján bizonyított állításokat fogjuk felhasználni.

5.16. Tétel. *[20, Lemma 2.1.] Legyen G véges csoport, $H \leq G$, $\varphi \in Aut(G)$.*

1. *Ha $x \in S(\varphi)$, akkor $S(x\varphi) = S(\varphi)x^{-1}$.*
2. *Van olyan $x \in S(\varphi)$, amire teljesül*

$$|Hx \cap S(\varphi)| = |H \cap S(x\varphi)| \geq r(G, \varphi) \cdot |H|$$

Legyen a G egy φ-invariáns normálosztója N (azaz $N^{\varphi} = N$), ekkor legyen $\overline{\varphi} \in Aut(G/N)$, melyre

$$(Ng)^{\overline{\varphi}} = Ng^{\varphi}$$

5.17. Tétel. *[20, Lemma 2.2.] Ha van egy olyan $t \in (0; 1]$, amelyre minden $S(\varphi)$-beli g csoportelemre teljesül*

$$|Ng \cap S(\varphi)| \leq t|N|$$

akkor

$$t^{-1} \cdot r(G, \varphi) \leq r(G/N, \overline{\varphi})$$

Legyen a G egy H részcsoportjára p a részcsoport rendjének legkisebb prímosztója.

5.18. Tétel. *[20, Lemma 2.3.] Ha $\varphi \in Aut(G)$ a H-t pontonként invertálja, azaz $H \subset S(\varphi)$, és $r(G,\varphi) > \frac{1}{p}$, akkor*

$$|G : C_G(H)| \leq \frac{p-1}{p \cdot r(G,\varphi) - 1}$$

p-Sylow részcsoportokról a következőt állíthatjuk.

5.19. Tétel. *[20, Lemma 2.4.] Legyen G véges csoport, $\varphi \in Aut(G)$, $P \in Syl_p(G)$. Ekkor ha teljesül, hogy*

$$r(G,\varphi) > \frac{2}{p+1}$$

akkor P a G-nek normálosztója.

Mindezekre támaszkodva rátérhetünk a 5.11. Lemma bizonyítására.

5.20. Tétel. *[17, Theorem 5.5.] Legyen G véges, nem feloldható csoport, amelynek nincs nemtriviális feloldható normálosztója, illetve legyen $\varphi \in Aut(G)$. Ekkor ha φ a G elemei közül legalább $\frac{2}{9}|G|$ elemet invertál, akkor $G \simeq A_5$.*

Bizonyítás. A bizonyításnak két fő esete lesz.

1. Legyen először G egyszerű, továbbá legyen $p \in \Pi(G)$, $P \in Syl_p(G)$. Mivel G egyszerű, így P nem lehet neki normálosztója, így adódik

$$\frac{2}{p+1} \geq r(G,\varphi) \geq \frac{2}{9}$$

   tehát $p+1 < 9$, azaz $p \in \{2,3,5,7\}$. Mivel G feloldható, így Burnside tétele miatt $|\Pi(G)| \geq 3$, tehát G-nek biztosan van $p = 5$ vagy $p = 7$ esetén nemtriviális p-Sylow részcsoportja. Ekkor $p \geq 5$ miatt

$$r(G,\varphi)|P| > \frac{2}{9}|P| > \frac{|P|}{p}$$

   illetve a 5.16. Tétel alapján választható φ úgy, hogy

$$|P \cap S(\varphi)| \geq r(G,\varphi) \cdot |P|$$

ezeket összevetve adódik

$$|P \cap S(\varphi)| > \frac{|P|}{p}$$

azaz $\langle P \cap S(\varphi)\rangle = P$. Ekkor $P^{\varphi} = P$ és φ-nek P-re való megszorítása 2 rendű. [21, Lemma 4.1, Chapter 10] alapján mivel p páratlan ($p \geq 5$), így $P = C_P(\varphi)(S(\varphi) \cap P)$, azaz $|C_P(\varphi)| = \frac{|P|}{|S(\varphi)\cap P|} < p$, tehát $S(\varphi) \cap P = P$. Ennek alapján φ pontonként invertálja P-t, vagyis P Abel csoport. Ekkor a 5.18. Tétel alapján és $r(G, \varphi) > \frac{2}{9} > \frac{1}{p}$ figyelembevételével állítható, hogy

$$|G : C_G(P)| \leq \frac{p-1}{p \cdot r(G,\varphi) - 1} < \frac{p-1}{p \cdot \frac{2}{9} - 1} = \frac{9(p-1)}{2p-9}.$$

Ez $p = 7$ esetén azt jelenti, hogy $|G : C_G(P)| < \frac{54}{5} < 11$. Mivel P Abel csoport, továbbá G nem p-nilpotens, így a Burnside lemma miatt $P \leq C_G(P) < N_G(P)$. Tehát $|G : N_G(P)| \geq 8$, és $|G : C_G(P)| \geq 16$, ami ellentmondás. Tehát $p = 5$, $\Pi(G) = \{2, 3, 5\}$. Továbbá $|G : C_G(P)| < \frac{9(p-1)}{2p-9} = 36$.

Használva a következő fejezetben kimondott 5.21. Tételt $\Pi(G) = \{2, 3, 5\}$ miatt G izomorf a következő csoportok egyikével: $A_5, A_6, S_4(3)$. Ezen csoprtok mindegyikére $|P| = |C_G(P)| = 5$ (ez A_5 és A_6 esetén nyilvánvaló, $S_4(3)$-ra levonható az Atlasbeli ([22]) információk alapján). $G \simeq A_6$ vagy $G \simeq S_4(3)$ esetén $|G : C_G(P)| > 36$, ami ellentmondás, tehát csak $G \simeq A_5$ lehet.

2. Tekintsük most a G nem egyszerű esetet és legyen N egy minimális normálosztója G-nek. Ekkor N izomorf egyszerű csoportok direkt szorzata, mert karakterisztikusan egyszerű a minimalitás miatt. Ekkor a 5.18. Tétel alapján választható olyan φ, amelyre

$$|N \cap S(\varphi)| \geq r(G, \varphi) \cdot |N| \geq \frac{2}{9}|N| > \frac{1}{5}|N|$$

és mivel ha N nem feloldható, akkor van benne perfekt részcsoport, egyébként pedig ő maga perfekt, aminek nem lehet 5-nél kisebb indexű részcsoportja, így $N = \langle N \cap S(\varphi)\rangle$, illetve $N^{\varphi} = N$. Legyen X az N egyik egyszerű faktora. A 5.18. Tételt ismét használva, a φ módosításával az is elérhető, hogy $|X \cap S(\varphi)| > \frac{2}{9}|X|$ és $X^{\varphi} = X$, tehát az előző pont alapján $X \simeq A_5$.

Mivel X nem feloldható, a 5.10. Tétel szerint egy tetszőleges automorfizmusa legfeljebb az elemeinek $\frac{4}{15}$ részét invertálja, így bármely $y \in S(\varphi) \cap N$ esetén teljesül

$$|X \cap S(y\varphi)| = |Xy \cap S(\varphi)| \leq \frac{4}{15}|X|$$

A 5.17. Tétel szerint $t = \frac{4}{15}$-re teljesül

$$t^{-1} \cdot r(N, \varphi) \leq r(N/X, \overline{\varphi})$$

amit az előzőekkel összevetve kapjuk

$$r(N/X, \overline{\varphi}) > \frac{15}{4} \cdot \frac{2}{9} = \frac{5}{6} > \frac{4}{15}$$

tehát N/X feloldható, azaz $N = X \simeq A_5$. Mivel így $X \lhd G$, így hasonlóan G/X is feloldható, és $X \cap C_G(X) = 1$ is teljesül X egyszerű volta miatt, tehát $C_G(X) \lhd G$ ami $C_G(X)$ feloldhatsága miatt azt jelenti, hogy $C_G(X) = \{1\}$, vagyis G izomorf $Aut(A_5) \simeq S_5$ egy részhalmazával. Ugyanakkor S_5 belső automorfizmusai legföljebb az elemek $\frac{1}{6}$ részét invertálják, és $\frac{1}{6} < \frac{2}{9}$ miatt $|G| < |S_5|$, vagyis $G \simeq A_5$, ami ellentmondás, mert G nem egyszerű.

$\square$

5.6. Egyszerű csoportok adott $\Pi(G)$-vel

Szükségünk lesz - illetve korábban már hivatkoztunk is - a következő tételre . H. Convey, R. T. Curtis, S. P. Norton, R. A. Parker és R. A. Wilson [22] könyve, valamint Y. Bugeaud, Z. Cao és M. Mignotte [23], C. Burness és S. D. Scott [13], M. Herzog [24], Jafarzadeh és A. Iranmanesh [25] továbbá Jafarzadeh és A. Iranmanesh [26] cikkei alapján. Jelölje $\pi(n)$ egy adott természetes szám prímosztóinak halmazát.

5.21. Tétel. *[17, Proposition 2.5.] Legyen G véges egyszerű csoport,* $\Pi(G) \subset \{2, 3, 5, 7, 11, 13\}$.

1. *Ha* $|\Pi(G)| = 3$*, akkor G a következő csoportok egyikével izomorf:*
   - $A_5, A_6, S_4(3) \simeq U_4(2), L_2(7), L_2(8), L_3(3), U_3(3)$
2. *Ha* $|\Pi(G)| = 4$*, akkor G a következő csoportok egyikével izomorf:*
   - $L_2(q)$*, q prím,* $|\pi(q^2 - 1)| = 3$
   - $L_2(2^m)$*,* $2^m - 1 = u$*,* $2^m + 1 = 3t$*,* u, t *prímek,* $t > 3$
   - $L_2(3^m)$*,* $3^m - 1 = 2u$*,* $3^m + 1 = 4t$*,* u, t *prímek*
   - $L_2(25), L_2(49), L_3(4), L_4(3), U_3(4), U_3(5), U_4(3), U_5(2), S_4(5), S_4(7) S_6(2), O_8^+(2), G_2(3), ^3D_4(2), ^2F_4(2)', Sz(8), A_7, A_8, A_9, A_10, M_{11}, M_{12}, J_2$
3. *Ha* $|\Pi(G)| = 5$*, akkor G a következő csoportok egyikével izomorf:*
   - $L_2(q)$*, q prímhatvány,* $|\pi(q^2 - 1)| = 4$
   - $L_3(q)$*, q prímhatvány,* $|\pi((q^2 - 1)(q^3 - 1))| = 4$
   - $U_3(q)$*, q prímhatvány,* $|\pi((q^2 - 1)(q^3 + 1))| = 4$
   - $O_5(q) \simeq S_4(q)$*, q prímhatvány,* $|\pi(q^4 - 1)| = 4$
   - $Sz(2^{2m+1}) \simeq^2 B_2(2^{2m+1}$*,* $|\pi((2^{2m+1} - 1)(2^{4m+2} + 1))| = 4$
   - $R(q)$*,* $q = 3^{2m+1}$*,* $|\pi(q^2 - 1)| = 3$*,* $|\pi(q^2 - q + 1)| = 1$
   - $L_5(3), S_6(3), U_4(5), U_6(2), O_7(3), O_8^+(3), G_2(4), A_{11}, A_{12}, M_{22}, HS, McL$
4. *Ha* $|\Pi(G)| = 6$*, akkor G a következő csoportok egyikével izomorf:*
   - $L_2(q)$*, q prímhatvány,* $|\pi(q^2 - 1)| = 5$
   - $L_3(q)$*, q prímhatvány,* $|\pi((q^2 - 1)(q^3 - 1))| = 5$
   - $L_4(q)$*, q prímhatvány,* $|\pi((q^2 - 1)(q^3 - 1)(q^4 - 1))| = 5$
   - $U_3(q)$*, q prímhatvány,* $|\pi((q^2 - 1)(q^3 + 1))| = 5$
   - $U_4(q)$*, q prímhatvány,* $|\pi((q^2 - 1)(q^3 + 1)(q^4 - 1))| = 5$

- $O_5(q) \simeq S_4(q)$, *q prímhatvány*, $|\pi(q^4-1)| = 5$
- $G_2(q)$, *q prímhatvány*, $|\pi(q^6-1)| = 5$
- $Sz(2^{2m+1}) \simeq^2 B_2(2^{2m+1})$, $|\pi((2^{2m+1}-1)(2^{4m+2}+1))| = 5$
- $R(3^{2m+1})$, $|\pi((3^{2m+1}-1)(3^{6m+3}+1))| = 5$
- $L_6(3), A_{13}, A_{14}, A_{15}, A_{16}, Suz, Fi_{22}$

A továbbiakban is feltételezzük, hogy G véges egyszerű csoport, erről szeretnénk belátni, hogy $\Pi(G) \subset \{2,3,5,7,11,13\}$ esetén vagy $G \simeq A_5$, vagy $o(G) > o(A_5)$.

5.22. Tétel. *[17, Lemma 4.1.] Legyen* $G \simeq A_n$, $n \geq 5$. *Ekkor vagy* $G \simeq A_5$, *vagy* $o(G) > o(A_5)$.

Bizonyítás. Tekintsük először az $n = 6$ esetet, ekkor könnyen ellenőrizhető, hogy $|A_6| = 360$, $\Psi(A_6) = 1411$, $o(A_6) = \frac{1411}{360} = 3,9194\ldots$.

Most legyen $n \geq 7$, ekkor teljesül [13] miatt

$$\frac{i_2(A_n)}{|A_n|} \leq \frac{2}{8\cdot(n-4)!} + \frac{2}{2^4\cdot 23} = \frac{1}{4}\left(\frac{1}{(n-4)!} + \frac{1}{46}\right)$$

Ez egy csökkeő sorozat, és az első tagjára

$$\frac{i_2(A_7)}{|A_7|} \leq \frac{1}{4}\left(\frac{1}{6} + \frac{1}{46}\right) = \frac{13}{276} = 0,0471\ldots$$

Azaz a sorozat minden tagja kisebb $\frac{1}{20}$-nál, tehát $i_2(G) \leq \frac{1}{20}|G|$ miatt $o(G) \geq \frac{71}{20} > 3,55$. □

A 5.21 tétel és a 5.9 lemma segítségével bizonyíthatóak az alábbiak.

5.23. Tétel. *[17, Lemma 4.2. - Lemma 4.18.] Legyen G véges egyszerű csoport,* $\Pi(G) \subset \{2,3,5,7,11,13\}$.

1. *Ha* $|\Pi(G)| = 3$, *akkor vagy* $G \simeq A_5$, *vagy* $o(G) > o(A_5)$.
    - *Ha* $G \simeq L_2(q)$, $q \geq 4$ *és* $\Pi(G) \subset \{2,3,5,7,11,13\}$, *akkor vagy* $G \simeq A_5$, *vagy* $o(G) > o(A_5)$.
    - *Ha* $G \simeq L_3(q)$, $q = 3,4$ *vagy* $q \geq 8$, *akkor* $o(G) > o(A_5)$.
    - *Ha* $G \simeq U_3(q)$, $q = 3,4,5$ *vagy* $q \geq 8$, *akkor* $o(G) > o(A_5)$.
2. *Ha* $|\Pi(G)| = 4$, *akkor* $o(G) > o(A_5)$.
    - *Ha* $G \simeq L_4(q)$ *vagy* $G \simeq U_4(q)$, $q \geq 3$, *akkor* $o(G) > o(A_5)$.

- *Ha* $G \simeq L_5(q)$ *vagy* $G \simeq U_5(q)$, $q \geq 2$, *akkor* $o(G) > o(A_5)$.
- *Ha* $G \simeq R(q) \simeq^2 G_2(q)$, $q = 3^{2m+1}$, *akkor* $o(G) > o(A_5)$.
- *Ha* $G \simeq G_2(q)$, $q \geq 3$, *akkor* $o(G) > o(A_5)$.
- *Ha* $G \simeq S_4(q)$, $q \geq 5$, *akkor* $o(G) > o(A_5)$.
- *Ha* $G \simeq Sz(2^{2m+1}) \simeq^2 B_2(2^{2m+1})$, $m \geq 1$ *akkor* $o(G) > o(A_5)$.
- *Ha* $G \simeq S_6(q)$, $q \geq 2$, *akkor* $o(G) > o(A_5)$.
- *Ha* $G \simeq O_8^+(q)$, $q \geq 2$, *akkor* $o(G) > o(A_5)$.
- *Ha* $G \simeq^3 D_4(2)$, *akkor* $o(G) > o(A_5)$.
- *Ha* $G \simeq^2 F_4(2)'$, *akkor* $o(G) > o(A_5)$.

3. *Ha* $|\Pi(G)| = 5$, *akkor* $o(G) > o(A_5)$.

4. *Ha* $|\Pi(G)| = 3$, *akkor* $o(G) > o(A_5)$.

5.7. A tétel bizonyítása

Most már bebizonyíthatjuk 5.12 Tételt, mely úgy szólt, hogy ha G véges csoportra $o(G) \leq o(A_5) = \frac{211}{60} \approx 3,5167$, akkor vagy $G \simeq A_5$, vagy G feloldható.

Bizonyítás. Tegyük fel indirekt, hogy G véges, $o(G) \leq o(A_5)$, $G \not\simeq A_5$ és nem feloldható, ezek közül pedig legyen G a legkisebb rendű.

1. Először vizsgáljuk azt az esetet, amikor G egyszerű csoport. Ekkor G nem p-feloldható $p|n$-re. Az első lemmából következőleg tudjuk, hogy $\Pi(G) \subset \{2, 3, 5, 7, 11, 13\}$, azon egyszerű csoportok pedig ismertek, ahol $|\Pi(G)| \leq 6$ (melyek az előző fejezetben megtalálhatóak). Ezekre ellenőrizve látható, hogy ha $o(G) \leq o(A_5)$, akkor $G \simeq A_5$.

2. Most nézzük meg azt az esetet, amikor G nem egyszerű. Ekkor definíció szerint van neki egy nemtriviális M normálosztója. Erre mint azt már korábban láttuk teljesül a következő:

$$o(G/M) < o(G) \leq o(A_5)$$

$|G|$ minimalitása miatt tudjuk, hogy G/M feloldható.

Most vegyük azt az N normálosztót, amire teljesül, hogy $|G/N| = p$ prím. Ekkor $o(G/N) = \frac{1+(p-1)\cdot p}{p} = p - \frac{p-1}{p} < o(A_5)$, tehát N nem feloldható.

a) Először tegyük fel, hogy $p = 2$. Ekkor feltehetjük, hogy egy $x \in G \setminus N$ elemre $o_{G/N}(xN) = 2$ és $G = N \cup xN$, így $\Psi(G) = \Psi(N) + \Psi(xN)$. Ekkor $2|o_{G/N}(xn)$, és ha nem volna 2 rendű elem, akkor $o(xg) \geq 4$, vagyis $\Psi(xN) \geq 4|N|$ és $\Psi(G) \geq \psi(N) + 4|N|$ volna, következésképpen $o(G) = \frac{\Psi(G)}{|G|} \geq \frac{\Psi(N)}{|G|} + 2 = \frac{1}{2}o(N) + 2$ illetve $o(N) \leq 2(o(G) - 2) < 3,04$, ami ellentmondás, mert N nem feloldható. Tehát feltehetjük, hogy $o_G(x) = 2$.

Definiáljuk X-et a következőképpen:

$$X = \{xn : n \in N, o(xn) = 2\}$$

Azaz X az xN-beli involúciók halmaza. Látható, hogy egy xn alakú elem rendje pontosan akkor 2, ha $xnx = n^{-1}$, tehát

$$|X| = |\{n \in N : xnx = n^{-1}\}|$$

illetve látható

$$\Psi(xN) \geq 2|X| + 4|xN \setminus X|$$

Most beláthatjuk, hogy N-nek nincs nemtriviális feloldható normálosztója, ugyanis ha volna egy ilyen K, akkor $L = KK^x$ a G-nek volna nemtriviális feloldható normálosztója, vagyis $o(G/L) < o(G) \leq o(A_5)$ teljesülne, viszont mivel G/L nem feloldható, így $G/L \simeq A_5$ a G minimalitása folytán, ami ellentmondás. Tehát nincs az N-nek nemtriviális feloldható normálosztója, és $N \cap C_G(N) = 1$.

Jelölje φ az x-szel való konjugálást, ekkor a második lemmából következik, hogy vagy $|X| \leq \frac{2}{9}|N|$, vagy $N \simeq A_5$.

Ha $N \simeq A_5$, akkor $N \cap C_G(N) = 1$ miatt két eset lehetséges. Ha $C_G(N) \neq 1$, akkor $|C_G(N)| = 2$ és $G = N \times C_G(N)$ is teljesül, ugyanakkor tudjuk, hogy $o(N) = o(G/C_G(N)) < o(G) \leq o(A_5)$, ami ellentmondás. Másrészről ha $C_G(N) = 1$, akkor $G = G/C_G(N) \leq Aut(A_5) = S_5$, és $|G| = 2|N| = |S_5|$ miatt $G \simeq S_5$, ám $o(S_5) = \frac{157}{40} > o(A_5)$, így ez is ellentmondás, tehát $N \not\simeq A_5$.

Így $|X| \leq \frac{2}{9}|N|$, tehát teljesül az alábbi:

$$|xN \setminus X| \geq |xN| - |X| \geq |xN| - \frac{2}{9}|N| = \frac{7}{2}|N|$$

Tudjuk továbbá:

$$\Psi(G) = \Psi(N) + \Psi(xN) \geq 2|N| + 2|X| + 4|xN \setminus X| = \Psi(N) + 2|N| + 2|xN \setminus X|$$

Az előbbieket összevetve pedig adódik:

$$\Psi(G) \geq \Psi(N) + 2|N| + 2 \cdot \frac{7}{9}|N| = \Psi(N) + \frac{32}{9}|N|$$

Így ha leosztunk n-nel kapjuk az alábbit:

$$o(G) \geq \frac{1}{2}o(N) + \frac{16}{9}$$

Azaz átrendezve, és $2 \cdot \frac{16}{9} > \frac{211}{60}$ miatt:

$$o(N) \leq 2\left(o(G) - \frac{16}{9}\right) < o(A_5)$$

Mivel $|G|$ minimális volt az adott tulajdonságokkal, így N-nek feloldhatónak kell lennie, így viszont G is feloldható, ami ismét ellentmondás.

b) Most tegyük fel, hogy $p = 3$, azaz $|G/N| = 3$. Legyen $Y = G \setminus N$, ekkor minden elemére $y \in Y : y^3 \in N$, amire persze $y \notin N$, így $o_{G/N}(yN) = 3$, így $o(y) = 3h$ egy $h \in (Z)$-ra.

Legyen T az Y 3 rendű elemeiből álló halmaz, V pedig a maradék, azaz $T = \{y \in Y : o(y) = 3\}$, illetve $V = Y \setminus T$. Ekkor $\Psi(Y) \geq 3|T| + 6|V|$, illetve a korábbiak miatt teljesül $i_3(G) \geq |T|$ mellett $i_3(G) < \frac{7}{20}|G|$ is.

Tegyük fel, hogy $|T| > \frac{2}{3}|Y|$, ekkor az előbbiek összefésülésével adódik

$$\frac{7}{20}|G| > i_3(G) \geq |T| > \frac{2}{3}|Y| = \frac{4}{3}|G|$$

Ez viszont $\frac{7}{20} < \frac{4}{9}$ miatt ellentmondás, így $|T| \leq \frac{2}{3}|Y|$. Ekkor

$$|V| = |Y| - |T| \geq |Y| - \frac{2}{3}|Y| = \frac{1}{3}|Y|$$

Ebbő következik

$$\Psi(G) - \Psi(N) = \Psi(Y) \geq 3|T| + 6|V| = 3(|T| + |V|) + 3|V| \geq 4|Y| = \frac{8}{3}|G|$$

Amit átrendezve kapjuk

$$o(G) = \frac{\Psi(G)}{|G|} \geq \frac{\Psi(N)}{|G|} + \frac{8}{3} > \frac{1}{3}o(N) + \frac{8}{3}$$

Vagyis $o(N) < 3(o(G) - \frac{8}{3})$. Mivel a feltevés miatt N nem feloldható, így $o(N) > \frac{187}{60}$, így $o(G) > \frac{667}{180} = 3,7055\ldots > \frac{211}{60}$, ami ismét ellentmondás.

c) Végül legyen $p > 3$, ekkor

$$o(G/N) = o(C_p) = p - 1 + \frac{1}{p} > 4 > o(A_5)$$

tehát ismét ellentmondásra jutottunk, így a tételt beláttuk.

□

Hivatkozások

[1] Marcel Herzog, Patrizia Longobardi, Mercede Maj. *An exact upper bound for sums of element orders in non-cyclic finite groups*. https://arxiv.org/pdf/1610.03669.pdf, J. Pure Appl. Algebra, 222 n.7 (2018) , 1628-1642.

[2] H. Amiri, S.M. Jafarian Amiri, I.M. Isaacs. *Sums of element orders in finite groups*. Comm. Algebra 37 (2009) 2978–2980.

[3] Herendi Zsolt. *Elemrendek összege csoportokban*. https://web.cs.elte.hu/blobs/diplomamunkak/msc_mat/2021/herendi_zsolt.pdf

[4] Marius Tărnăuceanu. *Detecting Structural Properties of Finite Groups by the Sum of Element Orders*. Israel Journal of Mathematics 238 (2020), 629–637.

[5] Marcel Herzog, Patrizia Longobardi, Mercede Maj. *The second maximal groups with respect to the sum of element orders*. Journal of Pure and Applied Algebra 225 (2021) 106531.

[6] Marcel Herzog, Patrizia Longobardi, Mercede Maj. *Sums of element orders in groups of order* $2m$ *with* m *odd*. Communications in Algebra, 47:5, 2035-2048.

[7] Morteza Baniasad Azad, Behrooz Khosravi. *Properties of Finite Groups Determined by the Product of their Element Orders*. Bull. Aust. Math. Soc. 103 (2021), 88–95.

[8] Marius Tărnăuceanu. *A Generalization of a Result on the Sum of Element Orders of a Finite Group*. Math. Slovaca 71 (2021), No. 3, 627–630.

[9] Subhrajyoti Saha. *Sum of the Powers of the Orders of Elements in Finite Abelian Groups*. Advances in Group Theory and Applications, 13. 1 - 11.

[10] Elena Di Domenico, Carmine Monetta, Marialaura Noce: *Upper bounds for the product of element orders of finite groups*. Journal of Algebraic Combinatorics (2022)

[11] M. Garonzi, M. Patassini. *inequalities detecting structural properties of a finite group*. Comm. Algebra 45 (2016), 677-687.

[12] Marius Tărnăuceanu. *A note on the product of element orders of finite abelian groups*. Bull. Malays. Math. Sci. Soc. (2) 36 (2013), pp. 1123–1126.

[13] T. C. Burness, S. D. Scott. *On the number of prime order subgroups of finite groups*. J. Australian Math. Soc. 87 (2009), 329-357.

[14] Mihai-Silviu Lazorec, Marius Tărnăuceanu. *On the average order of a finite group*. Journal of Pure and Applied Algebra Volume 227, Issue 4, April 2023, 107276.

[15] A. Jaikin-Zapirain. *On the number of conjugacy classes of finite nilpotent groups*. Adv. Math. 227 (2011), 1129-1143.

[16] E. I. Khukhro, A. Moretó, M. Zarrin. *The average element order and the number of conjugacy classes of finite groups*. Journal of Algebra, Volume 569, 1 March 2021, Pages 1-11

[17] Marcel Herzog, Patrizia Longobardi, Mercede Maj. *Another criterion for solvability of finite groups*. Journal of Algebra, Volume 597, 1 May 2022, Pages 1-23

[18] Marcel Herzog, Patrizia Longobardi, Mercede Maj. *On a criterion for solvability of a finite group*. J. Algebra 597 (2022), 1-23.

[19] Hongfei Pan, Xianhua Li. *On the character degree sums*. Comm. Algebra 45 (3) (2017), 1211-1217.

[20] W. M. Potter. *Nonsolvable groups with an automorphism inverting many elements*. Arch. Math. 50 (1988), 292-299.

[21] D. Gorenstein. *Finite groups*. AMS Chelsea Publishing, New York, 1968.

[22] J. H. Convey, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson. *ATLAS of Finite Groups, Maximal Subgroups and Ordinary Characters for Simple Groups*. Clarendon Press, Oxford, 2003, ISSN 978-0-19-853299-9.

[23] Y. Bugeaud, Z. Cao, M. Mignotte. *On simple K_4-groups*. J. Algebra 241 (2) (2001), 658-668.

[24] M. Herzog. *On finite simple groups of order divisible by three primes only*. J. Algebra 10 (1968), 383-388.

[25] A. Jafarzadeh, A. Iranmanesh. *On simple K_n-groups for $n = 5, 6$*. Group St. Andrews 2005, Volume 2, London Mathematical Society Lecture Note Series, Cambridge University Press 340 (2007), 517-526.

[26] D. Yu, J. Li, G. Chen, L. Zhang, W. Shi. *A new characterization of simple K_5-groups of type $L_3(p)$*. Bull. Iran. Math. Soc. 45 (2019), 771-781.