Eötvös Loránd Tudományegyetem
Természettudományi Kar

Wolosz János
Matematikus MSc

Vizsgálatok a csoportreprezentációk külső hatványai témájában

Szakdolgozat

Témavezető: Pálfy Péter Pál egyetemi tanár

Budapest, 2014

Köszönetnyilvánítás

Ezúton szeretném megköszönni témavezetőmnek, Pálfy Péter Pálnak a kiváló témaajánlást, a szakmai segítségnyújtást és a jó hangulatú konzultációkat.

Tartalomjegyzék

Bevezetés

Ez a szakdolgozat egy új reprezentációelméleti fogalmat vizsgál, az ESQ reprezentációk fogalmát. Egy modulus akkor ESQ modulus, ha van a külső négyzetének a modulussal izomorf faktora. Ezt a fogalmat a [3] cikkben vezették be először. A szakdolgozatban két természetes irányból vizsgáljuk az ESQ reprezentációkat. Az első irány a kis dimenziós hű irreducibilis ESQ reprezentációk leírása. A másik irány annak megvizsgálása, hogy bizonyos nevezetes csoportosztályoknak van-e irreducibilis ESQ reprezentációja. Mindkét megközelítés további érdekes kérdéseket vet fel. A szakdolgozat második és harmadik fejezetének eredményei megtalálhatók a [3] cikkben, a negyedik és ötödik fejezetek a szerző önálló munkáját tartalmazzák. A szakdolgozat felépítése a következő:

- Az első fejezetben bevezetjük az ESQ reprezentáció fogalmát, tisztázzuk a jelölésbeli konvenciókat, és néhány közvetlenül a definícióból adódó észrevételt teszünk ESQ reprezentációkkal kapcsolatban.
- A második fejezetben egy tisztán csoportelméleti kérdésen keresztül motiváljuk az ESQ reprezentációk vizsgálatát.
- A harmadik fejezetben leírjuk a 4 dimenziós hű irreducibilis ESQ reprezentációkat, illetve az 5 dimenziós hű irreducibilisek közül a minimálisakat.
- A negyedik fejezetben bebizonyítjuk, hogy az S_n ($n \geq 4$) szimmetrikus csoportnak van egy $\binom{n-1}{2}$ dimenziós irreducibilis ESQ reprezentációja. Ezt az eredményt felhasználva az A_n egyszerű alternáló csoportnak is megmutatjuk egy irreducibilis ESQ reprezentációját.
- Az ötödik fejezetben egyes metaciklikus csoportok esetén bebizonyítjuk, hogy egy irreducibilis ESQ reprezentáció létezése ekvivalens egy Fermat-tétel szerű egyenlet nem triviális megoldhatóságával $\mathbb{F}_p$-ben. Ezt felhasználva megoldunk két természetesen felmerülő aszimptotikus kérdést.

1. fejezet

Jelölések és definíciók, valamint az ESQ reprezentációk néhány alaptulajdonsága

Ebben a fejezetben bevezetjük azokat a definíciókat, amelyeket a szakdolgozat későbbi fejezeteiben már ismertnek tekintünk, és tisztázzuk a jelölésbeli konvenciókat is. Egy V vektortér külső négyzetét $\widehat{V}$-vel fogjuk jelölni. Ennek megfelelően, ha egy M modulus karaktere χ, akkor a modulus külső négyzetét $\widehat{M}$-mel, az ehhez tartozó karaktert $\widehat{\chi}$-vel jelöljük.

Most definiáljuk az ESQ reprezentáció fogalmát.

1.1. Definíció. *Egy V $\mathbb{F}G$-modulus akkor ESQ (exterior self-quotient) modulus, ha létezik olyan $U \leq \widehat{V}$ $\mathbb{F}G$-részmodulus, hogy $\widehat{V}/U \cong V$ mint $\mathbb{F}G$-modulusok. Ha a G hatása hű a V vektortéren, akkor azt mondjuk, hogy G ESQ részcsoportja $GL(V)$-nek, vagy egyszerűen azt, hogy G ESQ csoport.*

Néha a könnyebb megfogalmazás kedvéért egy reprezentációt és a hozzá tartozó karaktert azonosítjuk, így beszélhetünk ESQ karakterekről. Mivel 0 karakterisztika esetén a reprezentációk és karaktereik kölcsönösen meghatározzák egymást, ez nem okozhat félreértést. A következő tétel az ESQ reprezentációk néhány rögtön adódó tulajdonságát mondja ki.

1.2. Tétel. *Legyen V egy ESQ $\mathbb{F}G$-modulus.*

(i) Ha $G \leq GL(V)$ egy ESQ részcsoport, és $H \leq G$, akkor a H is egy ESQ részcsoportja $GL(V)$-nek.

(ii) A $V \otimes_{\mathbb{F}} \mathbb{E}$ egy ESQ $\mathbb{E}G$-modulus tetszőleges $\mathbb{F} \leq \mathbb{E}$ testbővítés esetén.

(iii) G-ben nincs más skalármátrix, mint az identitás, és $\dim(V) \geq 3$.

Az 1.2 tétel (i) pontja szerint az ESQ tulajdonság öröklődik a részcsoportokra, a (ii) szerint pedig egy ESQ reprezentáció tetszőleges testbővítés esetén ESQ marad.

Ismert, hogy egy adott test feletti irreducibilis reprezentáció egy nagyobb test felett már nem feltétlenül irreducibilis. Ez az észrevétel indokolja a következő definíciót.

1.3. Definíció. *Egy $\mathbb{F}$ test feletti reprezentáció abszolút irreducibilis, ha tetszőleges $\mathbb{F} \leq \mathbb{E}$ véges testbővítés esetén $\mathbb{E}$ felett is irreducibilis.*

2. fejezet

Az ESQ reprezentációk vizsgálatának motivációja

Az ESQ reprezentáció fogalma a [3] cikkben jelent meg először. Ebben a cikkben a szerzők egy tisztán csoportelméleti kérdést vizsgálva jutottak el ehhez az új reprezentációelméleti fogalomhoz. E fejezetben ezt az utat mutatjuk be.

UCS-csoportnak (unique proper non-trivial characteristic subgroup) akkor nevezünk egy csoportot, ha egyetlen nemtriviális karakterisztikus részcsoportja van. Ezt a fogalmat Taunt vezette be a [7] cikkben. A [3] cikk az UCS p-csoportokat vizsgálja. Nézzük meg az UCS p-csoportok pár rögtön adódó tulajdonságát. Egy UCS p-csoport ha Abel csoport, akkor csak $(C_{p^2})^r$ lehet. Egy nem Abel UCS p-csoport nilpotencia osztálya csak 2 lehet, hiszen az alsó centrális láncbeli részcsoportok karakterisztikusak. Egy UCS p-csoport exponense csak p vagy p^2 lehet, hiszen a G^{p^i} részcsoportok karakterisztikusak, a nemtriviálisak pedig különbözők. Az ESQ fogalom motivációjához elegendő lesz a $p > 2$ UCS p-csoportok vizsgálata, ezért mostantól feltesszük, hogy $p > 2$. (A $p = 2$ esetben ugyanis a csoport struktúrája bonyolultabb, mivel ezekre nem teljesül, hogy $(xy)^p = x^p y^p$.)

Legyen $H_{p,r}$ a szabad r elemmel generált csoport p^2 exponenssel, 2 nilpotenciaosztállyal, úgy, hogy $(H_{p,r})^p \leq Z(H)$. Ismert, hogy páratlan p esetén $\Phi(H_{p,r}) = = (H_{p,r})^p \oplus (H_{p,r})'$. Legyenek a $H_{p,r}$ csoport generátorai $x_1, x_2, \ldots, x_r$. Ekkor a $(H_{p,r})'$ csoportot minimálisan generálják az $[x_i, x_j]$ kommutátorok, ahol $1 \leq i < j \leq r$. A $(H_{p,r})^p$ csoportot pedig az x_i^p hatványok generálják minimálisan, ahol $1 \leq i \leq r$.

Tetszőleges G p-csoport esetén jelöljük a $G/\Phi(G)$ elemi Abel csoportot $\overline{G}$-vel. Világos, hogy a $\overline{H_{p,r}}$ elemi Abel csoporton $GL(\overline{H_{p,r}})$ természetesen hat. Az $x \to x^p$ leképezés segítségével a $(H_{p,r})^p$ csoportra is tekinthetünk úgy, mint $GL(\overline{H_{p,r}})$-modulusra. Ehhez hasonlóan a kommutátorképzés segítségével a $(H_{p,r})'$ csoport is tekinthető

$GL(\overline{H_{p,r}})$-modulusnak, ekkor a kapott modulus éppen a $\overline{H_{p,r}}$ modulus külső négyzete. Így $\Phi(H_{p,r})$ is $GL(\overline{H_{p,r}})$-modulus. Ennek a modulusnak a szerkezetéről szól a következő lemma.

2.1. Lemma. *Legyen $H = H_{p,r}$. Ekkor H' egy $GL(\overline{H})$-részmodulusa $\Phi(H)$-nak, és $\Phi(H)/H' \cong \overline{H}$ mint $GL(\overline{H})$-modulus. Ha p páratlan, akkor $\Phi(H) = H^p \oplus H'$, tehát $\overline{H} \cong H^p$ mint $GL(\overline{H})$-modulus.*

A jobb átláthatóság érdekében a továbbiakban a következő jelöléseket használjuk. A $H_{p,r}$ csoportot röviden csak H-nak írjuk. Ha az L csoport hat a V vektortéren, akkor L^V-vel jelöljük az L elemeinek megfelelő $GL(V)$ részcsoportot. L_X-szel jelöljük L-nek azt a maximális részcsoportját, amely egy adott X objektumot (mint halmazt) stabilizál.

Az r elemmel generálható UCS-csoportokat kereshetjük H/N alakban, ahol $N \leq \leq \Phi(H)$. Bármely r elemmel generált G UCS p-csoportban a $\overline{H}$ és $\overline{G}$ r dimenziós vektorterek megfeleltethetők egymásnak. Ebből a megfigyelésből következik az alábbi lemma.

2.2. Lemma. *Legyen $G = H/N$, ahol $N \leq \Phi(H)$. Ekkor a $\overline{H}$ és $\overline{G}$ vektortereket megfeleltetve egymásnak a következőket kapjuk:*

$$Aut(G)^{\overline{G}} = GL(\overline{H})_N, \quad Aut(G)^{\Phi(G)} = (GL(\overline{H})_N)^{\Phi(H)/N}.$$

A következő tétel már reprezentációelméleti feltételt ad az UCS p-csoport tulajdonságra.

2.3. Tétel. *Legyen $G = H/N$, $N \leq \Phi(H)$. Ekkor a következő állítások ekvivalensek:*

(i) G UCS p-csoport.

(ii) $Aut(G)^{\overline{G}}$ és $Aut(G)^{\Phi(G)}$ is irreducibilisek.

(iii) $GL(\overline{H})_N$ és $(GL(\overline{H})_N)^{\Phi(H)/N}$ is irreducibilisek.

Bizonyítás. A 2.2 lemma szerint (ii) és (iii) ekvivalensek. Most bebizonyítjuk (i) és (ii) ekvivalenciáját. $Aut(G)^{\overline{G}}$ részmodulusai pontosan megfelelnek a G csoport azon karakterisztikus részcsoportjainak, amelyek tartalmazzák a $\Phi(G)$ részcsoportot. Ehhez hasonlóan az $Aut(G)^{\Phi(G)}$ részmodulusai pontosan megfelelnek a G csoport azon karakterisztikus részcsoportjainak, amelyek a $\Phi(G)$-nek részcsoportjai. Ezzel $(i) \Rightarrow (ii)$-t beláttuk. A megfordításhoz legyen L egy tetszőleges karakterisztikus

részcsoportja G-nek. Ekkor az $L\Phi(G)$ is karakterisztikus részcsoport, és tartalmazza $\Phi(G)$-t. Az $Aut(G)^{\overline{G}}$ modulus részmodulusaira tett megfigyelésünk szerint $L\Phi(G) = = G$, vagy $L\Phi(G) = \Phi(G)$. Az első esetben $L = G$, hiszen $\Phi(G)$ a nemgeneráló elemek részcsoportja. A második esetben $L \leq \Phi(G)$. Ekkor azonban az $Aut(G)^{\Phi(G)}$ modulus részmodulusaira tett megfigyelésünk szerint az L vagy a triviális részcsoport, vagy $\Phi(G)$. Minden esetet megvizsgáltunk és azt kaptuk, hogy L vagy 1, vagy $\Phi(G)$, vagy G. Ezzel $(ii) \Rightarrow (i)$-t beláttuk. □

2.4. Tétel. *Legyen $G = H/N$ UCS p-csoport, ahol $N \leq \Phi(H)$. Ekkor a következő három állítás közül pontosan egy áll fenn:*

(i) $H' = N$ *és* G *Abel csoport.*

(ii) $H^p \leq N$ *és* G p *exponensű nem Abel csoport.*

(iii) $H^p \cap N = 1$, $\overline{H}$ *és* $H'/(H' \cap N)$ *izomorfak mint* $GL(\overline{H})_N$ *modulusok, és* G p^2 *exponensű nem Abel csoport.*

Bizonyítás. Tegyük fel, hogy a G Abel csoport. Ekkor $H' \leq N$, így G a $H/H' = = (C_{p^2})^r$ csoport faktora. Tudjuk, hogy minden Abel UCS p-csoport $(C_{p^2})^{r'}$ alakú. Mivel a G r elemmel generált, ezért $G = (C_{p^2})^r$, azaz $H' = N$, tehát az (i) eset áll fenn.

Tegyük fel, hogy a G nem Abel csoport. A 2.1 lemma szerint a $H^p \leq \Phi(H)$ egy $GL(\overline{H})$-részmodulus, így a $H^p \cap N \leq \Phi(H)$ egy $GL(\overline{H})_N$-részmodulus. Ugyanakkor újra csak a 2.1 lemma szerint $\overline{H} \cong H^p$, és azt is tudjuk, hogy a $GL(\overline{H})_N$ irreducibilis $\overline{H}$-n. Így $N \cap H^p = 1$, vagy $H^p \leq N$. Ha $H^p \leq N$, akkor éppen a (ii) eset áll fenn.

Még azt az esetet kell megvizsgálnunk, amikor $N \cap H^p = 1$. A 2.1 lemma szerint $H'N$ részmodulusa a $\Phi(H)$ $GL(\overline{H})_N$-modulusnak. Ekkor $H'N/N$ részmodulusa a $\Phi(H)/N$ $GL(\overline{H})_N$-modulusnak, és a 2.2 lemma szerint azt is tudjuk, hogy $Aut(G)^{\Phi(G)} = (GL(\overline{H})_N)^{\Phi(H)/N}$. Mivel a G egy UCS-csoport, a 2.3 tétel szerint $Aut(G)^{\Phi(G)}$ irreducibilis. Így $H'N/N = \Phi(G)$ vagy $H'N/N = 1$, ezért $H'N = \Phi(H)$ vagy $H'N = N$. Mivel G nem Abel csoport, ezért a két lehetőség közül csak a $H'N = = \Phi(H)$ állhat fenn. A fenti gondolatmenetet a H^pN részmodulusra megismételve azt kapjuk, hogy $H^pN = \Phi(H)$ vagy $H^pN = N$. $N \cap H^p = 1$ miatt itt csak az előbbi állhat fenn, így $H^pN = \Phi(H)$. Innen megkapjuk a kívánt $GL(\overline{H})_N$-modulus izomorfiát a következőképpen:

$$\overline{H} \cong H^p \cong \frac{H^p}{N \cap H^p} \cong \frac{H^pN}{N} = \frac{\Phi(H)}{N} = \frac{H'N}{N} \cong \frac{H'}{N \cap H'}.$$

Tehát az utolsó esetben valóban (iii) áll fenn. □

A 2.4 tétel (*iii*) pontjában szereplő H' éppen a $\overline{H}$ modulus külső négyzete, tehát azt kaptuk, hogy minden p^2 exponensű UCS p-csoport meghatároz egy egyszerű ESQ modulust. Ez a modulus az $Aut(G)$ természetes hatása a $\overline{G}$ vektortéren. A 4 dimenziós irreducibilis ESQ reprezentációkkal a 3.1 tételben foglalkozunk. E tételből rögtön következik, hogy például nincs 25 exponensű 4 elemmel generált UCS 5-csoport.

A fenti eredmények egy csoportelméleti motivációt adnak az irreducibilis ESQ reprezentációk vizsgálatára, és rávilágítanak arra, miképp született meg ez a fogalom a [3] cikkben.

3. fejezet

A 4 és 5 dimenziós irreducibilis ESQ csoportok vizsgálata

A 4 és 5 dimenziós irreducibilis ESQ csoportokat fogjuk ebben a fejezetben vizsgálni. Természetes lenne a 3 dimenziós ESQ csoportok vizsgálatával kezdenünk, ezekről azonban nem tudunk olyan erős állításokat bizonyítani, mint a 4 és 5 dimenziós esetekben. Rögzítve a v_1, v_2, v_3, valamint a $v_2 \wedge v_3, v_3 \wedge v_1, v_1 \wedge v_2$ bázisokat látszik, hogy tetszőleges $g \in SO(3)$ esetén $g = g \wedge g$, tehát maga az $SO(3)$ csoport is ESQ csoport. Így $SO(3)$ egy tetszőleges részcsoportja megad egy 3 dimenziós ESQ csoportot, ezek száma tehát túl nagy.

A fejezetben közölt eredmények megtalálhatók a [3] cikkben. A 4 dimenziós véges irreducibilis ESQ csoportokat a 3.1 tétel, az 5 dimenziós irreducibilis ESQ csoportok közül a minimálisakat a 3.3 tétel klasszifikálja. A következőkben ezeket az eredményeket mutatjuk be.

Legyen $\mathbb{F}$ egy nem 2 karakterisztikájú test. Legyen $L = AGL_1(5)$, az 5-elemű test feletti 1 dimenziós vektortér holomorfja (ezt a csoportot az 5. fejezetben $F_{5,4}$-gyel jelöljük). Ekkor $|L| = 20$, és az L mint $GL_5(\mathbb{F})$ részcsoport természetesen hat az $\mathbb{F}^5$ vektortéren. Feltéve, hogy char $\mathbb{F} \neq 5$, ez a modulus felbomlik az $\mathbb{F}^5 = V \oplus V_1$ nem triviális modulus direktösszegre, ahol $V = \{(x_0, x_1, \ldots, x_4) | x_0 + x_1 + \ldots + x_4 = 0\}$, és $V_1 = \{(x, x, \ldots, x) | x \in \mathbb{F}\}$. A most bevezetett L csoportot a következő tétel kimondása, illetve bizonyítása során használni fogjuk.

3.1. Tétel. *Legyen $\mathbb{F}$ egy nem 2 karakterisztikájú test, és legyen $K \leq GL_4(\mathbb{F})$ egy véges irreducibilis ESQ részcsoport. Ekkor char $\mathbb{F} \neq 5$ és K izomorf L egyik részcsoportjával. Továbbá, ha az 5 négyzetelem $\mathbb{F}$-ben, akkor $K \cong L$.*

Bizonyítás. A bizonyítás során felhasználjuk azt a tényt, hogy ha char $\mathbb{F} \neq 2$, akkor

egy nem Abel véges egyszerű csoportnak nincs kétdimenziós nem-triviális reprezentációja. Ez az állítás az [5] könyv 5.5.10-es állítása. Legyen M a K minimális normálosztója. Ekkor M izomorf egyszerű csoportok direkt szorzata, hiszen karakterisztikusan egyszerű. Először megmutatjuk, hogy M egy Abel csoport. Indirekten tegyük fel, hogy M nem Abel. Legyen S az M egyik egyszerű nem Abel faktora. Ekkor a Clifford-tételt az $S \lhd M \lhd K$ láncra alkalmazva azt kapjuk, hogy az S is irreducibilis. Legyen $V = \mathbb{F}^4$. A V irreducibilis ESQ S-modulus $S \leq K$ miatt, ezért létezik olyan $U \leq \widehat{V}$ S-modulus, amire $\widehat{V}/U \cong V$. Így az U dimenziója $6 - 4 = 2$, azaz az első megjegyzésünk szerint U-n az S hatása triviális.

Jelöljük a V duálisát V^*-gal. A $\phi : Hom(V, V^*) \to V \otimes V$ leképezést a következőképpen definiáljuk. Rögzítsük V egy $x_1, \ldots, x_4$ bázisát, valamint az ehhez tartozó $x_1^*, \ldots, x_4^*$ duális bázist. Tetszőleges $f \in Hom(V, V^*)$-nak megfelel egy $(\alpha_{i,j})$ 4×4-es mátrix. Ekkor legyen $\phi(f) = \sum_{i,j} \alpha_{i,j}(x_i \otimes x_j)$. Világos, hogy a ϕ leképezés lineáris izomorfizmus. A $Hom(V, V^*)$ vektortéren definiálható egy S-hatás a következőképpen: $S \leq GL(V)$ miatt egy tetszőleges $s \in S$-re tekinthetünk 4×4-es mátrixként, így ha f mátrixa $(\alpha_{i,j})$, akkor $s \cdot f = s^T(\alpha_{i,j})s$ egy S-hatást definiál $Hom(V, V^*)$-n. A $V \otimes V$ vektortéren is definiálható a tenzorokon szokásos S-hatás. Számolással ellenőrizhető, hogy a fent definiált ϕ leképezés egy S-modulus izomorfizmus. A $V \otimes \otimes V$ tér S által fixált pontjainak megfelelő pontok a $Hom(V, V^*)$-ban éppen a V és V^* S-modulusok közötti S-modulus homomorfizmusok. Mivel $U \leq \widehat{V} \leq V \otimes V$, így a fixpontok dimenziója legalább 2. Így a V S-modulus centralizáló algebrájának dimenziója legalább 2. A Schur-lemma szerint a centralizáló algebra az $\mathbb{F}$ egy másodfokú testbővítése, jelöljük ezt $\mathbb{E}$-vel. Tehát a V 4 dimenziós nem triviális $\mathbb{F}S$-modulus tekinthető 2 dimenziós $\mathbb{E}S$-modulusnak, ami ellentmond az első megjegyzésünknek. Így M egy elemi Abel csoport és r-csoport valamilyen r prímre, ahol r nem egyezik meg $\mathbb{F}$ karakterisztikájával.

Vegyük $\mathbb{F}$ olyan $\mathbb{E}$ testbővítését, amely tartalmazza az r-edik egységgyököket. Ekkor az $M \leq GL_4(\mathbb{E})$ egy ESQ csoport. Mivel az $\mathbb{E}$ az M felbontási teste és M Abel csoport, ezért rögzíthető egy e_1, e_2, e_3, e_4 bázis az $\mathbb{E}^4$-ben, amely minden $m \in \in M \leq GL_4(\mathbb{E})$ lineáris leképezésnek sajátbázisa.

Tegyük fel, hogy létezik egy $g \in M$, amelynek egyik sajátértéke sem 1. Legyenek g sajátértékei λ_i, ahol $1 \leq i \leq 4$. Ekkor $g \wedge g$ sajátértékei a $\lambda_i\lambda_j$ értékek, ahol $1 \leq \leq i < j \leq 4$. Mivel az M ESQ csoport, ezért létezik egy olyan $\varphi : [4] \to \binom{4}{2}$ injekció, hogy $i \notin \varphi(i)$, és $\lambda_i = \lambda_j\lambda_k$, ahol $\varphi(i) = \{j, k\}$. Tehát kaptunk egy 4 egyenletből álló egyenletrendszert. Az indexek permutálásának erejéig két lényegesen különböző

típusú egyenletrendszert kaphatunk, ezek a következők:

$$\lambda_1 = \lambda_2\lambda_3, \quad \lambda_2 = \lambda_3\lambda_4, \quad \lambda_3 = \lambda_4\lambda_1, \quad \lambda_4 = \lambda_1\lambda_2, \tag{3.1}$$

és

$$\lambda_1 = \lambda_2\lambda_3, \quad \lambda_2 = \lambda_1\lambda_4, \quad \lambda_3 = \lambda_1\lambda_2, \quad \lambda_4 = \lambda_1\lambda_3. \tag{3.2}$$

Oldjuk meg a (3.1) egyenletrendszert. A $\lambda_1 = \lambda_2\lambda_3$ összefüggést a későbbi egyenletekbe beírva $1 = \lambda_2\lambda_4$, valamint $\lambda_4 = \lambda_2^2\lambda_3$ következik. Most ezekbe írjuk be a $\lambda_2 = \lambda_3\lambda_4$ összefüggést, és ekkor azt kapjuk, hogy $1 = \lambda_3\lambda_4^2$ és $1 = \lambda_3^3\lambda_4$. Ebből az utolsó két összefüggésből $\lambda_3^5 = 1$, tehát $r = 5$, és ha ε egy primitív ötödik egységgyök, akkor

$$\lambda_1 = \varepsilon^4, \quad \lambda_2 = \varepsilon^3, \quad \lambda_3 = \varepsilon, \quad \lambda_4 = \varepsilon^2.$$

A (3.2) egyenletrendszert a fentihez hasonlóan megoldhatjuk, ekkor azt kapjuk, hogy

$$\lambda_1 = \varepsilon^4, \quad \lambda_2 = \varepsilon^3, \quad \lambda_3 = \varepsilon, \quad \lambda_4 = \varepsilon^5,$$

ahol $\varepsilon^6 = 1$. Megmutatjuk, hogy ez a második eset nem fordulhat elő. Az M csoport minden eleme prímrendű, ezért $\lambda_3 = \varepsilon$ és $\varepsilon^6 = 1$ miatt $\varepsilon^2 = 1$ vagy $\varepsilon^3 = 1$. Ha $\varepsilon^2 = 1$, akkor $\lambda_1 = 1$, ha $\varepsilon^3 = 1$, akkor $\lambda_2 = 1$. Ez ellentmond annak a feltevésünknek, hogy az 1 nem sajátérték.

Most megmutatjuk, miért nem lehetséges, hogy minden $g \in M$ esetén az 1 a g-nek sajátértéke legyen. Mivel $M \lhd K$ és K irreducibilis, ezért $\{v \in \mathbb{F}^4 |\ \forall g \in \in M : vg = g\} = 0$. Így a triviális modulus nem faktora az $\mathbb{F}^4$ M-modulusnak. Tehát a triviális modulus nem faktora a $\mathbb{E}^4$ M-modulusnak sem, azaz $\{v \in \mathbb{E}^4 |\ \forall g \in \in M : vg = g\} = 0$. Emiatt egy tetszőleges $e_i, 1 \leq i \leq 4$ bázisvektort legfeljebb $|M|/r$ darab M-beli elem fixál. Feltettük, hogy minden $g \in M$-beli elemnek van nemtriviális fixpontja, ezért bármelyik $g \in M$ fixálja legalább az egyik bázisvektort. A skatulyaelv szerint $4 \cdot |M|/r < |M|$. Emiatt az r vagy 2 vagy 3. Az M nem ciklikus, ezért $SL_4(\mathbb{F})$-et nem triviálisan metszi. Az M minimalitása miatt így $M \leq SL_4(\mathbb{F})$.

Legyen $r = 2$. Tekintsük azokat a 4 dimenziós diagonális mátrixokat, melyek főátlójában csak ± 1 szerepel és a determinánsuk 1. Ezt a nyolc elemű csoportot jelöljük D-vel. Most $M \leq D$, és tudjuk, hogy $-I \notin M$, hiszen $-I$-nek az 1 nem sajátértéke. Könnyű ellenőrizni, hogy a D egy maximális részcsoportjában vagy szerepel a $-I$, vagy a részcsoport valamelyik bázisvektornak a stabilizátora. Tudjuk, hogy ezek egyike sem állhat fenn, ezért $r \neq 2$.

Legyen $r = 3$, és legyen az $\omega \in \mathbb{E}$ egy primitív harmadik egységgyök. Vegyünk egy

$g \in M \leq SL_4(\mathbb{E})$ elemet, úgy, hogy $g \neq 1$. Az 1 sajátértéke g-nek. Ha az 1 egyszeres sajátérték, akkor g spektruma csak $1, \omega, \omega, \omega$, vagy $1, \omega^2, \omega^2, \omega^2$ lehet. Ekkor azonban a $g \wedge g$ egyik sajátértéke sem 1. Ez ellentmond annak, hogy az M egy ESQ csoport. Emiatt az 1 legalább kétszeres sajátértéke g-nek, így g spektruma csak $1, 1, \omega, \omega^2$ lehet. Ahogy az $r = 2$ esetben, az M most is valódi részcsoportja a megfelelő D diagonális mátrixok 3^3 rendű csoportjának, így M két elemmel generálható. A két generátor nem fixálhatja ugyanazt a vektort az e_1, e_2, e_3, e_4 vektorok közül. Emiatt csak az lehetséges, hogy azt a két bázisvektort, amelyet az első generátor fixál, a második ω, illetve ω^2-szeresére nyújtja. Így azonban a két generátor szorzatának az 1 nem sajátértéke. Most is ellentmondást kaptunk, tehát $r \neq 3$.

Összefoglalva azt kaptuk, hogy az $M \lhd K$ minimális normálosztó elemi Abel csoport, 5-csoport, és az e_1, e_2, e_3, e_4 bázisban létezik olyan g eleme, melyre $g = = diag(\varepsilon^4, \varepsilon^3, \varepsilon^1, \varepsilon^2)$, ahol az ε egy primitív ötödik egységgyök. Rögzítsük a $\widehat{\mathbb{E}^4}$ egy bázisát. A bázisvektorok legyenek rendre:

$$e_2 \wedge e_3, \quad e_3 \wedge e_4, \quad e_4 \wedge e_1, \quad e_1 \wedge e_2, \quad e_1 \wedge e_3, \quad e_2 \wedge e_4.$$

Ebben a bázisban $g \wedge g = diag(\varepsilon^4, \varepsilon^3, \varepsilon^1, \varepsilon^2, 1, 1)$, tehát az ESQ feltétel miatt létező $\mathbb{E}^4 \to \widehat{\mathbb{E}^4}$ injektív $\mathbb{E}K$-modulus homomorfizmusnál az e_i képe az $e_{i+1} \wedge e_{i+2}$ vektor i-től nem függő konstansszorosa.

Vegyünk egy tetszőleges h elemet a g K-beli centralizátorából. Mivel a g sajátértékei különbözők, ezért a h is diagonális az e_i bázisban. Így $h = diag(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$. Ekkor a fenti injektív modulus homomorfizmus miatt a λ_i koordináták kielégítik a (3.1) egyenletrendszert. Emiatt a h a g egy hatványa. Tehát a g által generált részcsoport saját magát centralizálja a K-ban. Ebből következik, hogy az M csoport ez a centralizátor, így $M \cong Z_5$. Mivel az $M \lhd K$ saját magát centralizálja, ezért a K izomorf a $Hol(M) = L$ egy részcsoportjával. Mivel az M nem triviális elemeinek a karakterisztikus polinomja éppen $x^4+x^3+x^2+x+1 = 0$, ezért az $M \leq GL_4(\mathbb{F})$ részcsoport egyértelmű konjugálás erejéig. Így az $L \leq GL_4(\mathbb{F})$, és K valóban ennek egy részcsoportja. Az L-nek három M-et tartalmazó részcsoportja van, az M, a D_5, és az L. Ha az 5 négyzetszám, akkor a D_5 és az M irreducibilis reprezentációi legfeljebb kétdimenziósak, így ekkor valóban $K \cong L$. Ezzel a tétel bizonyítása kész. □

A prím dimenziós minimális irreducibilis ESQ csoportokról a [3] cikkben a következő tétel található. Ezt a tételt bizonyítás nélkül közöljük.

3.2. Tétel. *Legyen a p prím, és a q egy prímhatvány (nem feltétlenül p-hatvány), valamint legyen K egy minimális ESQ csoport, úgy, hogy $K \leq GL_p(q)$. Ekkor pon-*

tosan az egyik áll fenn a következő három állítás közül:

(i) A K nem abszolút irreducibilis, $|K| = r$ prím, és $q^p = 1 \pmod r$. Továbbá léteznek olyan különböző $\alpha, \beta \in \langle q \rangle \leq \mathbb{F}_r^\times$ maradékok, melyekre igaz az $\alpha + \beta = 1 \pmod r$ összefüggés.

(ii) A K abszolút irreducibilis, nem Abel egyszerű csoport.

(iii) A K abszolút irreducibilis, $|K| = pr^s$, ahol az $r \neq p$ prím, $r \mid q - 1$, és $s = ord_p(r)$. Továbbá K' elemi Abel csoport, $|K'| = r^s$, és K/K' irreducibilisen hat K'-n.

A $p = 5$ dimenziós esetben többet is állíthatunk a K csoportról, mint a 3.2 tétel. Erről szól az alábbi tétel.

3.3. Tétel. *Legyen q egy prímhatvány, és legyen $K \leq GL_5(q)$ minimális ESQ csoport. Ekkor pontosan az egyik áll fenn a következő két állítás közül:*

(i') A K nem abszolút irreducibilis, $|K| = 11$ és $q^5 = 1 \pmod{11}$.

(ii') A K abszolút irreducibilis, $|K| = 55$ és $11 \mid q - 1$.

Igaz továbbá, hogy mindkét eset előfordulhat.

Bizonyítás. Tegyük fel, hogy K az (i) esetet teljesíti a 3.2 tételben. A 3.2 tétel szerint $|K| = r$ prím, $q^5 = 1 \pmod r$, és léteznek az $\alpha = q^i$ és $\beta = q^j$ maradékok amikre igaz az $\alpha + \beta = 1 \pmod r$ összefüggés. Legyen $C \in GL_5(r)$ az (1,2,3,4,5) 5 hosszú ciklusnak megfelelő mátrix. Ekkor C-nek a q sajátértékhez tartozó sajátvektora a $v = (q^4, q^3, q^2, q^1, 1)$. Így $v(I - C^i - C^j) = 0$, tehát $\det(I - C^i - C^j) = 0$. Konkrét számolás mutatja $\mathbb{C}$ fölött, hogy $i + j = 0 \pmod 5$ esetén $\det(I - C^i - C^j) = -1$, így $i + j \neq 0 \pmod 5$. Ekkor azonban újra csak számolással $\det(I - C^i - C^j) = -11$, tehát $r = 11$, azaz az (i') eset valóban fennáll.

A $\langle q \rangle = \{1, 3, 4, 5, 9\} = (\mathbb{F}_{11}^\times)^2$ részcsoportban valóban megoldható az $\alpha + \beta = 1 \pmod{11}$ egyenlet az $\alpha = 3$ és $\beta = 9$ választással. A $q^5 = 1 \pmod{11}$ kongruencia miatt a tizenegyedik körosztási polinom két ötödfokú irreducibilis polinom szorzata $\mathbb{F}_q$ fölött. Vegyünk egy olyan $M \in GL_5(q)$ mátrixot amelynek a minimálpolinomja az egyik előbb említett ötödfokú irreducibilis polinomok egyike. Ekkor $K = \langle M \rangle$ éppen egy olyan minimális irreducibilis ESQ csoport, amelyre az (i') eset fennáll.

Tegyük fel, hogy a K az (iii) esetet teljesíti a 3.2 tételben. Az előbbiekhez hasonlóan most is $r = 11$ következik. Mivel $s = ord_5(11) = 1$, így $|K| = 55$, tehát

$K \cong \langle g, n \mid g^5 = n^{11} = 1, g^{-1}ng = n^t \rangle$, ahol $ord_{11}(t) = 5$ (ezt a csoportot az 5. fejezetben $F_{11,5}$-tel jelöljük). Azt, hogy (ii') fennállhat tetszőleges $11 \mid q-1$ esetén most nem mutatjuk meg, csak hivatkozzuk. Egy bizonyítás megtalálható itt: [3] cikk 18. tétel. ($\mathbb{C}$ feletti reprezentációk esetén nincs szükségünk a fenti hivatkozásra, az, hogy van ilyen 55-elemű ESQ csoport rögtön következik az 5.3 lemmából.)

A tétel bizonyításához már csak azt kell megmutatnunk, hogy 5 dimenzióban a 3.2 tétel (ii) esete nem állhat fenn. Indirekten tegyük fel, hogy a K csoportra teljesülnek a 3.2 tétel (ii) esetében megállapított tulajdonságok. Legyen a q elemű test karakterisztikája c. Mivel K nem Abel és egyszerű, ezért $K \leq SL_5(q)$, és $K \cap$ $\cap\, Z(SL_5(q)) = 1$. Így a K izomorf a $PSL_5(q)$ csoport egyik részcsoportjával.

Először tekintsük a $c = 2$ esetet. A $PSL_5(2^k)$ irreducibilis csoportjait Wagner már klasszifikálta a [8] cikkben. Ezen eredmény szerint bármely irreducibilis részcsoport izomorf a $PSL_2(11)$, $PSL_5(2^l)$ (ahol $l \mid k$) vagy $PSU_5(4^l)$ (ahol $2l \mid k$) csoportok valamelyikével. Mivel a $PSL_5(2) \leq PSL_5(2^l)$, és a $PSL_2(11) \leq PSU_5(4^l)$, ezért a K minimalitása miatt $K = PSL_5(2)$ vagy $K = PSL_2(11)$. Ennek a két csoportnak az 5 dimenziós irreducibilis reprezentációi 2 karakterisztikában ismertek, 4 darab van belőlük, és mind a négy külső négyzete irreducibilis. Így a K nem lehet ESQ csoport.

Azt az esetet kell még megnéznünk, amikor $c > 2$. A $PSL_5(c^k)$ csoportok irreducibilis részcsoportjait a [2] cikkben klasszifikálták. Ezekről a részcsoportokról belátható, hogy mindegyikük tartalmazza az A_4-et részcsoportként.

Bebizonyítjuk, hogy nincs 5 dimenziós hű ESQ A_4-modulus. Indirekten tegyük fel, hogy az M 5 dimenziós vektortéren van ilyen A_4 hatás. Ekkor a $V_4 \leq A_4$ Klein-csoport is hűen hat M-en, és ez a reprezentáció is ESQ. Mivel $c \neq 2$, ezért a V_4-nek a triviálison kívül még három nem triviális 1 dimenziós reprezentációja van. A V_4 Abel csoport, ezért rögzíthetjük a V_4 elemeinek egy sajátbázisát M-ben. Legyen az egyik sajátbázis vektor v. Egyszerű számolás mutatja, hogy ha a $\langle v \rangle$ téren a V_4 csoport nem triviálisan hat, és $p \in A_4$ egy harmadrendű elem, akkor a $\langle v \rangle$, $\langle vp \rangle$, $\langle vp^2 \rangle$ tereken a V_4 hatás a három irreducibilis reprezentációnak felel meg. Tehát a kapott 5 dimenziós V_4-modulusban a nem triviális reprezentációk ugyanannyiszor szerepelnek. Ugyanakkor 0-szor nem szerepelhetnek, mert akkor V_4 triviálisan hat M-en, és ez ellentmond a hűségnek. Így a kapott V_4-modulus két triviális és a három nem triviális reprezentáció direkt összege. Azonban ekkor a külső négyzetben a triviális reprezentáció csak egyszer szerepel. Ez ellentmond az ESQ tulajdonságnak. $\square$

4. fejezet

A szimmetrikus csoport egy ESQ reprezentációja

Ebben a fejezetben megmutatjuk az S_n szimmetrikus csoport egy ESQ reprezentációját, ha $n \geq 4$. Kisebb n-ekre S_n-nek ESQ reprezentációja nincsen, hiszen minden irreducibilis reprezentációjának dimenziója maximum 2. S_n standard irreducibilis reprezentációját jelöljük χ_1-gyel. Ez $n-1$ dimenziós és $\chi_1(g)$ nem más mint g fixpontjainak száma -1. A következőkben két állítást bizonyítunk be.

4.1. Tétel. *$\widehat{\chi_1}$ irreducibilis reprezentáció.*

4.2. Tétel. *$\widehat{\chi_1}$ ESQ reprezentáció.*

Jelöljük X_t-vel azt az $S_n \to \mathbb{N}$ függvényt, mely n elem egy permutációjához hozzárendeli a t-ciklusok számát. Ezzel a jelöléssel kifejezhetők a χ_1, illetve $\widehat{\chi_1}$ karakterek, hiszen $\chi_1(g) = X_1(g) - 1$ és $\chi_1(g^2) = X_1(g) + 2X_2(g) - 1$. A következő lemmából már könnyen következnek a 4.1 és 4.2 tételek.

4.3. Lemma. *Legyen $a, b, k, l \in \mathbb{N}$, $k \neq l$. Ekkor létezik olyan $c \in \mathbb{Q}$, hogy minden $n \geq ka + lb$ esetén*

$$\sum_{g \in S_n} \binom{X_k(g)}{a} \binom{X_l(g)}{b} = n! \cdot c. \tag{4.1}$$

Bizonyítás. Kettős leszámlálással pontosan meghatározható a (4.1) bal oldala. Nézzük meg, hogy hányszor számolunk meg egy adott k hosszú ciklusokból álló a-ast és egy adott l hosszú ciklusokból álló b-est. Vegyük észre, hogy így $a+b$ darab ciklust rögzítettünk, hiszen $k \neq l$ miatt egyik ciklus sem szerepel kétszer.

Mivel az imént említett $a+b$ darab ciklus adott, ezért még $n - ka - lb$ darab elemnek nincs képe egy lehetséges permutációban, így egy ilyen rögzített helyzetet

$(n-ka-lb)$!-szor számolunk a (4.1) bal oldalán. Most számoljuk meg, hányféleképpen rögzíthetjük az a darab k hosszú és a b darab l hosszú ciklust. Egymás után választva ki először az a darab k hosszú ciklust, majd a b darab l hosszú ciklust, a következőt kapjuk:

$$\prod_{i=0}^{a-1}\binom{n-ik}{k}\cdot\prod_{j=0}^{b-1}\binom{n-ka-jl}{l}\cdot\big((k-1)!\,\big)^a\cdot\big((l-1)!\,\big)^b \tag{4.2}$$

Ha a produktumokba beírjuk a binomiális együtthatókat faktoriálisokkal kifejezve, akkor a szorzat teleszkopikus lesz, így a lehetséges egyszerűsítések után azt kapjuk, hogy (4.2) éppen:

$$\frac{n!}{k^a\cdot l^b\cdot(n-ka-lb)!}$$

Tehát a (4.1) bal oldalán álló összeg éppen $\frac{n!}{k^a\cdot l^b}$, ezzel a lemmát beláttuk. □

4.4. Lemma. *Legyen $a,b,k,l\in\mathbb{N}$. Ekkor létezik olyan $d\in\mathbb{Q}$, hogy minden $n\geq$ $\geq ka+lb$ esetén*

$$\sum_{g\in S_n}X_k(g)^a\cdot X_l(g)^b=n!\cdot d.$$

Bizonyítás. $a+b$-re vonatkozó indukcióval bizonyítjuk a lemma állítását. Ha $a=$ $=b=0$, akkor az állítás triviálisan igaz $d=1$-gyel. Most legyen $a+b>0$. Írjuk fel a 4.3 lemmát. A (4.1) egyenlet bal oldalán a binomiális együtthatókra $X_k(g)$-ben illetve $X_l(g)$-ben mint polinomokra tekinthetünk. A szorzás elvégzése után éppen $\sum_{g\in S_n}X_k(g)^{a'}\cdot X_l(g)^{b'}$ típusú kifejezések jelennek meg n-től független együtthatókkal, ahol $a'+b'\leq a+b$. Világos, hogy a $\sum_{g\in S_n}X_k(g)^a\cdot X_l(g)^b$ kifejezés együtthatója nem 0. Tehát a 4.3 lemmából és az indukciós feltevésből következik a 4.4 lemma állítása. □

Vegyük észre, hogy a 4.3 lemma állítása igaz marad, ha az egyenlet bal oldalán az összegben több $\binom{X_k(g)}{a}$ típusú kifejezést szorzunk össze. A bizonyítás ekkor is teljesen hasonló a már bemutatottal. Ennek a megfigyelésnek megfelelően a 4.4 lemma is általánosítható. Most bebizonyítjuk a 4.1 és 4.2 tételeket.

Bizonyítás. A már bevezetett jelölésekkel

$$\widehat{\chi_1}(g)=\frac{(X_1(g)-1)^2-(X_1(g)+2X_2(g)-1)}{2}.$$

Így

$$\langle\widehat{\chi_1},\widehat{\chi_1}\rangle=\frac{1}{n!}\sum_{g\in S_n}\Big(\frac{(X_1(g)-1)^2-(X_1(g)+2X_2(g)-1)}{2}\Big)^2.$$

A 4.4 lemma szerint a fenti egyenlet jobb oldala $n \geq 4$ esetén nem függ n-től. Így elegendő S_4-ben kiszámolni $\langle \widehat{\chi_1}, \widehat{\chi_1} \rangle$-t, ami éppen 1. Ezzel a 4.1 tételt bebizonyítottuk.

A 4.2 tétel bebizonyításához elegendő megmutatnunk, hogy $\langle \widehat{\chi_1}, \widehat{\widehat{\chi_1}} \rangle \neq 0$. Kifejezzük a $\widehat{\widehat{\chi_1}}(g)$ értéket $X_1(g)$, $X_2(g)$, $X_4(g)$ segítségével. Mivel

$$\widehat{\chi_1}(g^2) = \frac{(\chi_1(g^2))^2 - \chi_1(g^4)}{2} = \frac{(X_1(g^2)-1)^2 - (X_1(g^4)-1)}{2} = \frac{(X_1(g)+2X_2(g)-1)^2 - (X_1(g)+2X_2(g)+4X_4(g)-1)}{2},$$

ezért

$$\widehat{\widehat{\chi_1}}(g) = \frac{(\widehat{\chi_1}(g))^2 - \widehat{\chi_1}(g^2)}{2} = \frac{\left(\frac{(X_1(g)-1)^2-(X_1(g)+2X_2(g)-1)}{2}\right)^2 - \frac{(X_1(g)+2X_2(g)-1)^2-(X_1(g)+2X_2(g)+4X_4(g)-1)}{2}}{2}.$$

Összegként felírva a $\langle \widehat{\chi_1}, \widehat{\widehat{\chi_1}} \rangle$ skaláris szorzást, a következőt kapjuk:

$$\langle \widehat{\chi_1}, \widehat{\widehat{\chi_1}} \rangle = \frac{1}{n!} \sum_{g \in S_n} \frac{(X_1(g)-1)^2 - (X_1(g)+2X_2(g)-1)}{2} \cdot \frac{\left(\frac{(X_1(g)-1)^2-(X_1(g)+2X_2(g)-1)}{2}\right)^2 - \frac{(X_1(g)+2X_2(g)-1)^2-(X_1(g)+2X_2(g)+4X_4(g)-1)}{2}}{2}.$$

A 4.4 lemma szerint ez $n \geq 6$ esetén nem függ n-től. S_6-ra kiszámolva azt kapjuk, hogy $\langle \widehat{\chi_1}, \widehat{\widehat{\chi_1}} \rangle = 1$. Így $n \geq 6$ esetén a $\widehat{\chi_1}$ irreducibilis karakterhez tartozó reprezentáció valóban ESQ. Az $n = 4$ és $n = 5$ esetekben külön-külön ellenőrizhető a $\langle \widehat{\chi_1}, \widehat{\widehat{\chi_1}} \rangle = 1$ azonosság. Ezeket a számolásokat könnyen elvégezhetjük a következő karaktertáblázatok segítségével. Ezzel a 4.2 tételt is bebizonyítottuk. □

g_i	1	(2)	(3)	(2,2)	(4)
$\lvert C_{S_4}(g_i)\rvert$	24	4	3	8	4
χ_1	3	1	0	-1	-1
$\widehat{\chi_1}$	3	-1	0	-1	1
$\widehat{\widehat{\chi_1}}$	3	-1	0	-1	1

g_i	1	(2)	(3)	(2,2)	(4)	(3,2)	(5)
$\lvert C_{S_5}(g_i)\rvert$	120	12	6	8	4	6	5
χ_1	4	2	1	0	0	-1	-1
$\widehat{\chi_1}$	6	0	0	-2	0	0	1
$\widehat{\widehat{\chi_1}}$	15	-3	0	-1	1	0	0

g_i	1	(2)	(3)	(2,2)	(4)	(3,2)	(5)	(2,2,2)	(3,3)	(4,2)	(6)
$\lvert C_{S_6}(g_i)\rvert$	720	48	18	16	8	6	5	48	18	8	6
χ_1	5	3	2	1	1	0	0	-1	-1	-1	-1
$\widehat{\chi_1}$	10	2	1	-2	0	-1	0	-2	1	0	1
$\widehat{\widehat{\chi_1}}$	45	-3	0	-3	1	0	0	-3	0	1	0

Megjegyezzük, hogy a χ_1 reprezentáció soha sem ESQ, éppen a 4.1 tétel miatt. Most megvizsgáljuk, hogyan viselkedik a $\widehat{\chi_1}$ reprezentáció megszorítva az $A_n \leq S_n$ alternáló részcsoportra.

4.5. Tétel. *A $\widehat{\chi_1} \downarrow A_n$ egy irreducibilis ESQ reprezentációja az A_n csoportnak, ha $n \geq 4$ és $n \neq 5$. Ha $n = 5$, akkor a $\widehat{\chi_1} \downarrow A_5$ két irreducibilis reprezentáció összege, és ez a két reprezentáció ESQ.*

Bizonyítás. Tudjuk, hogy a $\widehat{\chi_1} \downarrow A_n$ egy ESQ reprezentáció, hiszen általánosan igaz, hogy ha a χ G-nek egy ESQ reprezentációja és $H \leq G$, akkor a $\chi \downarrow H$ a H-nak egy ESQ reprezentációja $\widehat{\chi} \downarrow H = \widehat{\chi \downarrow H}$ miatt. Így elegendő a $\widehat{\chi_1} \downarrow A_n$ irreducibilitását bebizonyítanunk. Az $n \geq 4$ esetben $\widehat{\chi_1}$ egy irreducibilis S_n reprezentáció. Az A_n kettő indexű részcsoport, ezért $\widehat{\chi_1} \downarrow A_n$ vagy irreducibilis, vagy két irreducibilis reprezentáció összege. A második eset pontosan akkor következik be, ha a $\widehat{\chi_1}$ minden értéke 0 az A_n komplementerén, azaz a páratlan permutációkon. Számoljuk ki a $\widehat{\chi_1}$ értékét az (12) transzpozíción! A korábbi jelöléseket használva:

$$\widehat{\chi_1}((12)) = \frac{(X_1((12)) - 1)^2 - (X_1((12)) + 2X_2((12)) - 1)}{2} = \frac{(n-3)^2 - (n-1)}{2}.$$

A fenti számláló csak $n = 2$ vagy $n = 5$ esetén 0, így a tétel első állítását bebizonyítottuk. Az $n = 5$ esetben az A_5 csoport két 3 dimenziós irreducibilis reprezentációjára tekinthetünk úgy, mint az ikozaéder szimmetriacsoportjának két részcsoportjára, így

ezek $SO(3)$-ban is részcsoportot alkotnak. A harmadik fejezet elején tett megfigyelésünk szerint ezek tehát valóban ESQ reprezentációk. □

Legyen az n egy tetszőleges háromnál nagyobb egész. Tekintsünk egy n dimenziós V vektorteret, és ezen hasson S_n a koordináták permutálásával. Így kaptunk egy $\mathbb{C}S_n$-modulust, jelöljük ezt M'-vel. Az $M < M'$ részmodulus az a $\mathbb{C}S_n$-modulus, amely a 0 koordináta összegű vektorokból áll. Ekkor az M éppen a χ_1 karakterhez tartozó $\mathbb{C}S_n$-modulus. Vezessük be az $\widehat{M}$ és $\widehat{\widehat{M}}$ jelöléseket az M $\mathbb{C}S_n$-modulus külső négyzetére, illetve a külső négyzet külső négyzetére. A 4.2 tétel szerint létezik egy $\phi : \widehat{M} \to \widehat{\widehat{M}}$ injektív modulus-homomorfizmus. A következőkben célunk a ϕ homomorfizmus meghatározása lesz.

Legyen adott az M egy bázisa. Az M bázisvektorainak ékszorzata megadja az $\widehat{M}$ egy generátorrendszerét, és az így kapott $\widehat{M}$-beli generátorok ékszorzata megadja az $\widehat{\widehat{M}}$ egy generátorrendszerét. Az M-re célszerű mint az M' részmodulusára tekintenünk. Legyen M' egy bázisa v_i, ahol $i = 1, 2, \ldots, n$, és M bázisa $e_i = v_i - v_n$, ahol $i = 1, 2, \ldots, n-1$. Az $\widehat{M}$-et generálják az $r_{ij} = e_i \wedge e_j$ vektorok, ahol $1 \leq \leq i, j \leq n-1$, és $i \neq j$. Ez a generátorrendszer csak "majdnem" bázis az $r_{ij} = -r_{ji}$ összefüggés miatt. Végül $\widehat{\widehat{M}}$-et generálják az $R_{ij,kl} = r_{ij} \wedge r_{kl}$ vektorok, ahol az $\{i, j\}$ és $\{k, l\}$ kételemű halmazok végigfutják az $\{1, 2, \ldots, n-1\}$ halmaz kételemű részhalmazait, és $\{i, j\} \neq \{k, l\}$. A következő tétel explicite megadja ϕ-t a fenti $\widehat{M}$ generátorrendszeren. Ezt lineárisan kiterjesztve megkapjuk a megfelelő $\phi : \widehat{M} \to \widehat{\widehat{M}}$ injektív modulus-homomorfizmust.

4.6. Tétel. *Legyen*

$$\phi(r_{ab}) = (n-1) \sum_{\substack{1 \leq x \leq n-1 \\ x \notin \{a,b\}}} R_{ax,bx} - \sum_{\substack{1 \leq x,y \leq n-1 \\ x,y \notin \{a,b\} \\ x \neq y}} R_{ax,by} - \sum_{\substack{1 \leq x \leq n-1 \\ x \notin \{a,b\}}} R_{ab,ax} - \sum_{\substack{1 \leq x \leq n-1 \\ x \notin \{a,b\}}} R_{ab,bx},$$

ahol $1 \leq a, b \leq n-1$, és $a \neq b$. Ekkor ϕ lineárisan kiterjeszthető az $\widehat{M}$ modulusra, és az így kapott $\overline{\phi}$ injektív modulus-homomorfizmus lesz.

Bizonyítás. A lineáris kiterjeszthetőséghez elég, hogy egy általános r_{ab} esetén $\phi(r_{ab}) = = -\phi(r_{ba})$. Ez triviálisan teljesül a fenti leképezésre, hiszen az általános $R_{ij,kl}$ generátort egy ékszorzatként definiáltuk, ami antiszimmetrikus. A $\overline{\phi}$ leképezés injektivitása világos lesz miután megmutattuk, hogy $\overline{\phi}$ modulus-homomorfizmus, hiszen $\widehat{M}$ irreducibilis. Rögzítsünk egy általános r_{ab} generátort. Megmutatjuk, hogy tetszőleges

$(ij) \in S_n$ transzpozíció esetén

$$(ij)\phi(r_{ab}) = \phi((ij)r_{ab}). \tag{4.3}$$

Ebből már következik, hogy a $\overline{\phi}$ modulus-homomorfizmus, tehát a tétel bizonyítása kész lesz.

Eseteket vizsgálunk attól függően, hogy az (ij) transzpozíció mely két elemet cseréli fel.

Ha az (ij) transzpozíció fixálja n-et, akkor az M modulus egy tetszőleges báziselemén (ij) a koordinátákon hat, azaz $(ij)e_x = e_{(ij)x}$. Azonban így (ij) az r_{xy} és az $R_{xy,zw}$ generátorokon is koordinátánként hat. Ebből azonnal következik, hogy a (4.3) egyenlőség fennáll.

Ha (ij) nem fixálja az n-et, akkor feltehető, hogy $j = n$. Vizsgáljuk először azt az esetet, amikor $i = a$. Először ismét az M modulus bázisán nézzük meg, hogyan hat (an). A következőkben x, y mindig 1 és $n-1$ közötti, a-tól és egymástól különböző számokat jelöl. Világos, hogy $(an)e_a = -e_a$, és $(an)e_x = e_x - e_a$. Így $(an)r_{ax} = -e_a \wedge (e_x - e_a) = -r_{ax}$, és $(an)r_{xy} = r_{xy} - r_{xa} - r_{ay}$. Végül $(an)R_{ax,ay} = R_{ax,ay}$, $(an)R_{ax,bx} = -R_{ax,bx} + R_{ab,ax}$, és $(an)R_{ax,by} = (-r_{ax}) \wedge (r_{by} - r_{ba} - r_{ay}) = -R_{ax,by} + + R_{ab,ax} + R_{ax,ay}$. A (4.3) egyenlőséget szeretnénk ellenőrizni. Ennek jobb oldalán $\phi((an)r_{ab}) = \phi(-r_{ab}) = -\phi(r_{ab})$ áll. Most vizsgáljuk meg $(ij)\phi(r_{ab})$-t. A korábbiak szerint

$$(n-1) \sum_{\substack{1 \le x \le n-1 \\ x \notin \{a,b\}}} (an)R_{ax,bx} = (n-1) \sum_{\substack{1 \le x \le n-1 \\ x \notin \{a,b\}}} (-R_{ax,bx} + R_{ab,ax}).$$

A második szumma a következők szerint alakul:

$$- \sum_{\substack{1 \le x,y \le n-1 \\ x,y \notin \{a,b\} \\ x \ne y}} (an)R_{ax,by} = - \sum_{\substack{1 \le x,y \le n-1 \\ x,y \notin \{a,b\} \\ x \ne y}} (-R_{ax,by} + R_{ab,ax} + R_{ax,ay}) =$$

$$= - \sum_{\substack{1 \le x,y \le n-1 \\ x,y \notin \{a,b\} \\ x \ne y}} (-R_{ax,by} + R_{ab,ax}) = - \sum_{\substack{1 \le x,y \le n-1 \\ x,y \notin \{a,b\} \\ x \ne y}} (-R_{ax,by}) - (n-4) \sum_{\substack{1 \le x \le n-1 \\ x \notin \{a,b\}}} R_{ab,ax}.$$

A fenti levezetés második egyenlősége azért igaz, mert a szummában tetszőleges x, y esetén megjelenik az $R_{ax,ay}$ és az $R_{ay,ax}$ tag is, és ezek összege 0. A harmadik

szummát (an) fixálja. Végül a negyedik szumma képe (an)-nél:

$$-\sum_{\substack{1\le x\le n-1\\ x\notin\{a,b\}}}(an)R_{ab,bx}=-\sum_{\substack{1\le x\le n-1\\ x\notin\{a,b\}}}(-R_{ab,bx}+R_{ab,ax}).$$

Most számoljuk meg, melyik szumma hányszor szerepel $(ij)\phi(r_{ab})$-ben. Mivel az általános tagok megkülönböztetik az egyes szummákat, a pontos határokat ettől kezdve nem írjuk ki. A $\sum R_{ax,bx}$ $-(n-1)$-szer szerepel. A $\sum R_{ax,by}$ és a $\sum R_{ab,bx}$ egyszer szerepelnek. Végül a $\sum R_{ab,ax}$ is $n-1-(n-4)-1-1=1$-szer szerepel $(ij)\phi(r_{ab})$-ben. Így a (4.3) az (an) transzpozíció esetén is valóban fennáll.

Már csak az (xn) transzpozíció esetét kell végigszámolnunk, ahol $x\neq a,b,n$. Ekkor $\phi((xn)r_{ab})=\phi(r_{ab}-r_{ax}-r_{xb})$. Az $(xn)\phi(r_{ab})$-t hasonlóan számíthatjuk ki, mint az (an) transzpozíció esetén — igaz, most az x index is kitüntetett, ezért még többet kell számolnunk. Ezt a hosszú számítást itt nem végezzük el, hasonló módon működik minden, mint az (an) transzpozíció esetén, elég az adott típusú szummákat megszámolni. □

Megjegyezzük, hogy a 4.6 tételben a $\phi(r_{ab})$-re a következő egyszerűbb kifejezést is adhatjuk (bár azt, hogy a ϕ modulus-homomorfizmus, ekkor sem tűnik egyszerűbbnek ellenőrizni):

$$\phi(r_{ab})=n\sum_{1\le x\le n-1}R_{ax,bx}-\sum_{1\le x,y\le n-1}R_{ax,by}.$$

A fenti képletben $R_{ij,kl}=0$, ha $i=j$, vagy $k=l$, vagy $\{i,j\}=\{k,l\}$.

Végül kiszámoljuk a $\widehat{\chi_1}$ irreducibilis ESQ reprezentáció Young-diagramját a Murnaghan-Nakayama tétel segítségével. Ezt a tételt röviden ismertetjük.

Legyen adott a χ irreducibilis S_n karakter, és a hozzá tartózó T Young-diagram. Egy Young-diagram élszomszédos mezőinek egy délnyugat-északkelti irányú monoton láncát horognak nevezzük, ha a lánc elhagyása után a maradék mezők rész Young-diagramot alkotnak az eredeti Young-diagramban. A Murnaghan-Nakayama tétel szerint tetszőleges $g\in S_n$ esetén a $\chi(g)$ érték rekurzívan kiszámítható a következő módon. Vegyük g egy tetszőleges ciklusát, ennek hosszát jelöljük l-el. Hagyjuk el g-ből az l-hosszú ciklust, ekkor egy új $g'\in S_{n-l}$ permutációt kapunk. A $\chi(g)$ érték kiszámításához hagyjuk el az összes lehetséges l méretű horgot T-ből és a maradék $n-l$ méretű Young-diagramokhoz tartozó karaktereken számoljuk ki g' értékét, majd ezeket előjelesen adjuk össze. Az előjelet az elhagyott horog által érintett sorok paritása határozza meg, ha ez páratlan, akkor az előjel pozitív, különben negatív.

Az üres Young-diagram az üres permutáción az 1 értéket veszi fel, ha pedig T-ből nem lehet l hosszú horgot elhagyni, akkor $\chi(g) = 0$.

4.7. Tétel. *A $\widehat{\chi_1}$ irreducibilis ESQ reprezentáció Young-diagramja $(n-2,1,1)$.*

Bizonyítás. Jelöljük az $(n-2,1,1)$ Young-diagramhoz tartozó irreducibilis karaktert χ-vel. Megmutatjuk, hogy $\forall g \in S_n$ esetén $\chi(g) = \widehat{\chi_1}(g)$. Tudjuk, hogy $\widehat{\chi_1}(g)$ értéke csak a g permutáció 1- illetve 2-ciklusainak számától függ, hiszen

$$\widehat{\chi_1}(g) = \frac{(X_1(g)-1)^2 - (X_1(g) + 2X_2(g) - 1)}{2}. \tag{4.4}$$

Bebizonyítjuk n-re vonatkozó indukcióval, hogy a (4.4) összefüggés igaz $\chi(g)$-re is. Az $n = 3$ esetben χ az előjel karakter, így könnyen ellenőrizhető rá a (4.4). Az $n = = 4$ esetben is könnyen ellenőrizhető a (4.4) összefüggés, hiszen ekkor χ a standard irreducibilis karakter és az előjel karakter szorzata (vö. táblázat a 19. oldalon). Most legyen $n > 4$. Legyen $g \in S_n$ tetszőleges permutáció, és jelöljük a g permutáció leghosszabb ciklusának a méretét l-el. Eseteket fogunk vizsgálni l értéke szerint.

Ha $l = n$, akkor $\widehat{\chi_1}(g) = 1$. A $\chi(g) = 1$ abból látszik, hogy egy n hosszú horgot pontosan egyféleképpen tehetünk be az $(n-2,1,1)$ Young-diagramba, és ennek a magassága páratlan.

Ha $l = n-1$, akkor egyszerű számolás mutatja, hogy $\widehat{\chi_1}(g) = 0$. Mivel egy $n-1$ hosszú horgot nem tudunk az $(n-2,1,1)$ Young-diagramba betenni, ezért $\chi(g) = 0$ is igaz.

Ha $l = n-2$, akkor a maradék két elemet g akár felcseréli, akár fixálja, $\widehat{\chi_1}(g) = 0$ lesz. Mivel egy $n-2$ hosszú horgot sem tudunk az $(n-2,1,1)$ Young-diagramba betenni, ezért $\chi(g) = 0$ is igaz.

Az $3 \leq l \leq n-3$ esetben az l hosszú horgot csak a Young-diagram első sorából hagyhatjuk el. Ekkor egy 1, azaz páratlan magasságú horgot hagytunk el. Jelöljük g'-vel azt a permutációt $n-l$ elemen, melyet úgy kapunk, hogy g-ből elhagyjuk az l hosszú ciklust. A megmaradt Young-diagram az $(n-2-l,1,1)$ diagram, ezen kell kiszámolnunk a g' permutáció értékét. Az indukciós feltevés miatt g'-re igaz a (4.4) összefüggés. Mivel az l legalább három, ezért a g és g' permutációk 1 illetve 2 hosszú ciklusainak a száma egyenlő, tehát g-re is igaz a (4.4) összefüggés.

Az $l = 2$ esetben jelöljük a g permutáció fixpontjainak a számát x_1-gyel, a 2 ciklusok számát x_2-vel. Jelöljük g'-vel azt a permutációt $n-2$ elemen, melyet úgy kapunk, hogy g-ből elhagyunk egy 2 ciklust. Egy 2 hosszú horgot kétféleképpen hagyhatunk el az $(n-2,1,1)$ Young-diagramból. Ha az első oszlop utolsó két eleme

alkotja az elhagyott horgot, akkor egy 2, azaz páros magasságú horgot hagytunk el. A maradék Young-diagram a triviális karakterhez tartozik, így az a g'-n az 1 értéket veszi fel. A másik lehetséges horog elhagyás után a maradék Young-diagram az $(n-4,1,1)$ lesz. Legyen az ehhez tartozó karakter χ'. Mivel a g' fixpontjainak a száma x_1, a 2 ciklusainak a száma x_2-1, ezért az indukciós feltevés szerint $\chi'(g') = \\ = \frac{(x_1-1)^2-(x_1+2(x_2-1)-1)}{2}$. Így

$$\chi(g) = \chi'(g') - 1 = \frac{(x_1-1)^2 - (x_1+2(x_2-1)-1)}{2} - 1,$$

tehát a (4.4) összefüggés most is igaz.

Végül az $l=1$ esetben már elég a sorortogonalitásra hivatkoznunk, hogy lássuk a $\chi(g) = \widehat{\chi_1}(g)$ egyenlőséget. Ezzel a tétel bizonyítása kész.

□

5. fejezet

Egyes metaciklikus csoportok vizsgálata

Ebben a fejezetben p prím, $q > 1$ egész és $q \mid p-1$. Továbbá vezessük be az $r = \frac{p-1}{q}$ jelölést. $F_{p,q}$ csoporton a következőt értjük:

$$F_{p,q} = \langle a, b : a^p = b^q = 1, b^{-1}ab = a^u \rangle,$$

ahol u rögzített és rendje q $Z_p^\times$-ben. Az $F_{p,q}$ csoportokra tekinthetünk úgy, mint $Z_p \rtimes_\phi Z_q$ szemidirekt szorzatra, ahol $\phi : Z_q \to Z_p^\times$ injektív homomorfizmus. A következőkben azt szeretnénk megvizsgálni, mely p, q értékekre van az $F_{p,q}$ csoportnak irreducibilis ESQ reprezentációja. A két legtermészetesebben felmerülő aszimptotikus kérdést tisztázzák az 5.1 és 5.2 tételek.

5.1. Tétel. *Ha q rögzített, és $6 \nmid q$ akkor $\exists C$, hogy ha $p > C$, akkor $F_{p,q}$-nak nincs irreducibilis ESQ reprezentációja. Ha $6 \mid q$, akkor minden szóba jövő p-re van $F_{p,q}$-nak irreducibilis ESQ reprezentációja.*

5.2. Tétel. *Ha r rögzített, akkor $\exists C$, hogy ha $p > C$, akkor $F_{p,q}$-nak van irreducibilis ESQ reprezentációja.*

Az $F_{p,q}$ csoportok irreducibilis karakterei jól ismertek. Egy teljes leírás megtalálható például a [4] könyv 25.10-es tételében. A nemlineáris karakterek száma r, dimenziójuk q és a következő értékeket veszik fel. Ha $y \neq 0$, akkor $\phi_j(a^x b^y) = 0$. Továbbá legyen $\varepsilon = e^{2\pi i/p}$ és legyenek $v_1, v_2, \ldots, v_r$ az $\langle u \rangle \leq Z_p^\times$ részcsoport mellékosztály reprezentánsai. Ekkor

$$\phi_t(a^x) = \sum_{i=0}^{q-1} \varepsilon^{v_t u^i x}, \tag{5.1}$$

ahol $t = 1, 2, \ldots, r$. Világos, hogy a fenti formula jól definiált, tehát nem függ a reprezentánsoktól és u tetszőleges q-ad rendű u'-vel helyettesíthető. Rögzítsünk egy tetszőleges ϕ_t irreducibilis reprezentációt. Egy hasznos ekvivalens átfogalmazását adjuk annak, hogy ϕ_t ESQ reprezentáció.

5.3. Lemma. *ϕ_t pontosan akkor ESQ reprezentáció, ha a $z^k = z^l + 1$, $z^q = 1$ egyenletrendszer megoldható $\mathbb{F}_p^*$-ban valamilyen $k, l \in \mathbb{N}$-re úgy, hogy $z^l \neq 1$.*

Bizonyítás. Számoljuk ki $\widehat{\phi_t}(a^x)$ értékét. Egyszerű számolás mutatja, hogy

$$\widehat{\phi_t}(a^x) = \sum_{0 \leq i < j < q} \varepsilon^{v_t(u^i + u^j)x}. \tag{5.2}$$

Vegyük az (5.2) összeg egy általános tagját $\varepsilon^{v_t(u^i+u^j)x}$-t. Ha $u^i + u^j = 0$ $\mathbb{F}_p$-ben, akkor ez a tag 1. Ha $u^i + u^j \neq 0$, akkor tekintsük a

$$\sum_{k=0}^{q-1} \varepsilon^{v_t(u^{i+k}+u^{j+k})x}$$

q tagú összeget. Ez éppen egy (5.1) típusú összeg, azaz egy irreducibilis karakter értéke az a^x csoportelemen. Ezután válasszunk egy új $\varepsilon^{v_t(u^{i'}+u^{j'})x}$ tagot, ami még nem szerepelt (még q tagú összegben sem). Ezen a módon az (5.2) összeget particionáltuk 1-esekre és q tagú összegekre, melyek irreducibilis karakter értékek a^x-en. Ez azt jelenti, hogy megtaláltuk $\widehat{\phi_t}$ irreducibilis karakterekre bontását. Így $\langle \phi_t, \widehat{\phi_t} \rangle \neq 0$ pontosan akkor, ha valamilyen $i \neq j$-re $u^i + u^j \in \langle u \rangle$. Ez éppen a lemma állítása. □

Az 5.3 lemma triviális következménye, hogy a ϕ_t reprezentációk vagy egyszerre mind ESQ-k, vagy egyik sem ESQ. Mivel $\mathbb{F}_p^*$-ban egy q-ad rendű elem által generált részcsoport éppen az r-edik hatványokból áll, az 5.3 lemmát átfogalmazhatjuk $\mathbb{F}_p$-ben Fermat-tétel szerű állítássá. Ez az 5.2 tétel bizonyítása során még hasznos lesz.

5.4. Lemma. *ϕ_t pontosan akkor ESQ reprezentáció, ha az $x^r + y^r = z^r$ egyenletnek van olyan nemtriviális megoldása $\mathbb{F}_p$-ben, ahol $x^r \neq y^r$.*

Az 5.3 lemma segítségével bebizonyítjuk az 5.1 tételt.

Bizonyítás. Először a $6 \nmid q$ esettel foglalkozunk. Megmutatjuk, hogy ekkor tetszőleges $k, l \in \mathbb{N}$ esetén a $z^k = z^l + 1$, $z^q = 1$ egyenletrendszernek nincs megoldása $\mathbb{F}_p$-ben. Rögzítsük a k és l értékeket, amelyekről nyilván feltehető, hogy kisebbek mint q. Elegendő megmutatni, hogy az $f(x) = z^k - z^l - 1$ és a $g(x) = z^q - 1$ polinomoknak nincs közös gyökük $\mathbb{F}_p$-ben. Két polinomnak akkor van közös gyöke, ha a

rezultánsuk 0, ez $\mathbb{F}_p$ felett is igaz. A rezultáns kiszámítható a polinomok együtthatóiból képzett determinánssal. Ennek a determinánsnak a dimenziója $q + \max(k, l)$. Elegendő lenne megmutatni, hogy ez a determináns nem 0 $\mathbb{F}_p$ fölött. Tekintsük most az f és g polinomokat $\mathbb{C}$ feletti polinomként. Ekkor $\mathbb{C}$ felett felírhatjuk a rezultánst kiszámító determinánst. Ha ez a determináns nem 0 értékű, akkor készen vagyunk, hiszen elég nagy prímekre, például a determinánsérték abszolútértékénél nagyobb prímekre már a megfelelő $\mathbb{F}_p$ feletti determináns sem lesz 0. Azt, hogy a $\mathbb{C}$ feletti rezultáns nem 0 úgy bizonyítjuk, hogy megmutatjuk: a $\mathbb{C}$ feletti f és g polinomoknak nincs közös gyökük.

$z^q - 1 = 0$-ból következik, hogy $|z| = 1$. Így $z^k = z^l + 1$ miatt a lehetséges z^k értékek a 0 illetve az 1 középpontú egységkörök metszéspontjai. Azonban ekkor z^k primitív hatodik egységgyök. Mivel $z^q = 1$, ebből $6 \mid q$ következik.

Így $6 \nmid q$ esetben minden k, l-re kapunk egy nem 0 determinánsértéket. Ezen véges sok determinánsérték abszolútértékének maximuma jó lesz C-nek. Ezzel a $6 \nmid q$ eset kész.

Most tegyük fel, hogy $6 \mid q$. Ekkor $q \mid p - 1$ miatt van $\mathbb{F}_p^*$-ban hatodrendű elem, melyet jelöljünk g-vel. Mivel a hatodik körosztási polinom $\Phi_6(x) = x^2 - x + 1$, azt kapjuk, hogy $g^2 - g + 1 = 0$. Az 5.3 lemmában tehát a $z = g$, $k = 1$, $l = 2$ választás jó lesz. □

Végül az 5.4 lemma segítségével bebizonyítjuk az 5.2 tételt. Ha a lemmában eltekintünk az $x^r \neq y^r$ feltételtől, akkor olyan kérdést kapunk, amelyet Schur 1916-ban megoldott [6]. Ezt a bizonyítást röviden ismertetjük.

5.5. Lemma. *Legyen $c \in \mathbb{N}$ fix. Ekkor létezik olyan $s(c)$ egész, hogy ha az $S(c) = \{1, 2, \ldots, s(c)\}$ számokat c színnel színezzük, akkor $x + y = z$ egyenletnek lesz monokromatikus megoldása. Itt x és y nem feltétlenül különbözők.*

Bizonyítás. Tetszőleges $S(c)$ színezéshez rendeljük hozzá a következő $K_{s(c)+1}$ élszínezést: az e_{ij} él színe legyen $|i - j|$ színe az $S(c)$ színezésben. Ekkor mivel a színek száma fix, a Ramsey-tétel szerint van olyan nagy $s(c)$, hogy a kapott $K_{s(c)+1}$ élszínezésben biztosan lesz monokromatikus háromszög. Ha egy ilyen háromszög három csúcsa $p < q < r$, akkor $(q - p) + (r - q) = r - p$ egy monokromatikus megoldása $x + y = z$-nek $S(c)$-ben. □

Legyen $p > s(r)$ prím. Az 5.5 lemmát fogjuk alkalmazni $\mathbb{F}_p^*$ következő r-színezésére. Legyen g primitív gyök, az egyes színosztályok pedig legyenek a $\langle g^r \rangle$ multiplikatív

részcsoport mellékosztályai. Ekkor az 5.5 lemma szerinti monokromatikus hármas megadja $x^r + y^r = z^r$ egy nemtriviális megoldását $\mathbb{F}_p$-ben.

Tehát az 5.2 tétel bizonyításához az 5.5 lemma állítását kellene csak kicsit erősíteni, hogy ott ne lehessen $x = y$. Ennek az erősebb állításnak a bizonyítása megtalálható az [1] cikkben. Ezt is röviden közöljük.

Bizonyítás. A $K_{s(c)+1}$ egy élszínezését ugyanúgy konstruáljuk, mint az 5.5 lemma bizonyításában, de most olyan konstanst választunk, hogy még monokromatikus K_4 is biztosítva legyen $K_{s(c)+1}$-ben. Legyen egy ilyen négyszög négy csúcsa $w < x < y < z$. Ha $x - w = y - x = z - y = a$, akkor $(z - y) + (y - w) = z - w$ egy jó monokromatikus megoldás $S(c)$-ben. Ha $x - w \neq y - x$, akkor $(x - w) + (y - x) = y - w$ jó monokromatikus megoldás $S(c)$-ben. Végül ha $z - y \neq y - x$, akkor $(z - y) + (y - x) = z - x$ lesz jó monokromatikus megoldás $S(c)$-ben. □

Ezzel az 5.2 tétel bizonyítása kész.

Irodalomjegyzék

[1] P. Blanchard, F. Harary, R. Reis: *Partitions into sum-free sets.* INTEGERS: The E. J. of Combinatorial Number Theory 6 (2006), A7.

[2] L. Di Martino, A. Wagner: *The irreducible subgroups of $PSL(V_5, q)$, where q is odd.* Results Math. 2 (1) (1979), 54–61.

[3] S. P. Glasby, P. P. Pálfy, Cs. Schneider: *p-groups with unique proper non-trivial characteristic subgroup.* J. Algebra 348 (2011), 85-109.

[4] G. James, M. Liebeck: *Representations and Characters of Groups (2nd ed.).* Cambridge University Press, Cambridge, (2001).

[5] P. B. Kleidman, M. Liebeck: *The Subgroup Structure of the Finite Classical Groups.* London Math. Soc. Lecture Note Ser. 129, Cambridge University Press, Cambridge, (1990).

[6] I. Schur: *Über die Kongruenz $x^m + y^m = z^m$ (mod p).* Jahresber. Deutsche Math.-Verein. 25 (1916), 114-116.

[7] D. R. Taunt: *Finite groups having unique proper characteristic subgroups I.* Proc. Cambridge Philos. Soc. 51 (1955), 25–36.

[8] A. Wagner: *The subgroups of $PSL(5, 2^a)$.* Results Math. 1 (2) (1978), 207–226.