Konjugálás és hatványozás véges csoportokban

HEGEDŰS PÁL
V. matematikus

Témavezető
PÁLFY PÉTER PÁL egyetemi docens

ELTE, 1997. Budapest

Tartalomjegyzék

1 Bevezető 2

2 Definíciók és alaptulajdonságok 3

3 Reprezentáció-elméleti segédeszközök 6

4 A fő eredmények 10

5 Egyéb eredmények 24

6 Weyl-csoportok 25

7 Megjegyzések 35

Irodalomjegyzék 36

1 Bevezető

Ez a szakdolgozat azzal a kérdéskörrel foglalkozik, hogy mit jelent egy csoport struktúrájára nézve egy olyan kikötés, hogy minden elem konjugált egy rögzített kitevőjű hatványával.

Az egész egy általam megoldatlan zárthelyi feladat nyomán vetődött fel, amely azt állította, hogy véges esetben csak a triviális csoportban konjugált minden elem a négyzetével. Később ezt a feladatot mégis megoldva ötlött fel a kérdés: Milyen véges csoportokban konjugált minden elem a köbével? A válasz nem ad strukturális feleletet, de mégis elég jól "korlátozza" a csoportot. Kettő, illetve három helyett tetszőleges n-nel nem sikerült a feloldható esetben sem hasonló választ adni, csupán még $n = 4$ esetén.

Az általános kérdésre is sikerült azonban jó választ adni azzal az erősebb kikötéssel, hogy a csoport legyen feloldható és valós, azaz minden elem konjugált legyen az inverzével.

A szakdolgozat fejezetei:

Alaptulajdonságok Itt néhány alapvető definíció és tény szerepel.

Reprezentáció-elmélet Mivel a kérdéskör fő megközelítési iránya a reprezentáció-elmélet, így számos segédállításra és bizonyításra van szükség. Ezeket tartalmazza ez a fejezet.

Fő eredmények Ez magáért beszél.

Egyéb eredmények Itt a témakörrel szorosan összefüggő, de bizonyítás nélküli tételek szerepelnek.

Weyl-csoportok Itt a Weyl-csoportok karakter-táblájának egész voltáról, és ennek okairól esik szó.

Megjegyzések Ez a kérdéskör "történelmét", illetve a felmerült kérdéseket tartalmazza.

Ezúton szeretnék köszönetet mondani a Lehrstuhl D für Mathematik RWTH-Aachen munkatársainak, és a TEMPUS Computer Algebra Projektjének, amiért lehetővé tették, hogy Aachenban töltsek 5 hónapot, és e szakdolgozat egy részét ott elkészíthessem.

Ezenkívül köszönetet mondok Pálfy Péter Pál témavezetőmnek ezen szakdolgozat elkészítéséhez nyújtott sok segítségéért, és a kitűnő egyetemi előadásaiért; valamint Pelikán Józsefnek, aki a csoportelméletet megszerettette velem az első két egyetemi évem során tartott, szintén kitűnő előadásokkal.

2 Definíciók és alaptulajdonságok

Definíció 1 *Legyen G véges csoport! A csoport konjugációs hatványszámának nevezzük, és $\mathrm{cp}(G)$-vel jelöljük a $\min\{1 < n \mid \forall g \in G$-re $g \sim g^n\}$ kitevőt. (Itt, és a továbbiakban is $\sim$ a konjugáltságot jelenti.)*

A definíció értelmes végtelen csoportra is, de mivel ezen szakdolgozatban minden csoport véges lesz, így felesleges lenne az általánosítás. Véges csoportra a minimum véges, $\mathrm{cp}(G) \leq |G| + 1$.

Definíció 2 *Legyen G véges csoport, $\mathcal{H} \subseteq \mathbb{Z}$ tetszőleges halmaz! Ekkor G egy $\mathcal{H} - \mathrm{cp}$-csoport, ha $\forall g \in G$-re, és $\forall n \in \mathcal{H}$-ra $g \sim g^n$. Ha $\mathcal{H} = \{n\}$, akkor $\{n\} - \mathrm{cp}$-csoport helyett $n - \mathrm{cp}$-csoportot írok.*

Világos, hogy speciálisan G egy $\mathrm{cp}(G) - \mathrm{cp}$-csoport. Egy G véges csoportra $2 \leq \mathrm{cp}(G) \leq |G| + 1$. A két extrémumot karakterizálja az alábbi két tétel.

Tétel 3 $\mathrm{cp}(G) = 2 \Leftrightarrow |G| = 1$.

Bizonyítás 1. A jobbról balra irány triviális, a másikat látom be. Ha $\mathrm{cp}(G) = 2$, akkor $|G|$ páratlan. Másrészt $\forall g \exists x : g^2 = x^{-1}gx$, azaz $g = [g, x] \in G'$, így $G = G'$, és a Feit-Thompson tétel szerint $|G|$ páros, vagy $G = 1$, és ezzel kész. $\checkmark$

Miután nagyágyúval lelőttem a verebet, jöjjön egy kellemesebb bizonyítás is:

Bizonyítás 2. Legyen p a G rendjének legkisebb prímosztója! Ha $|G| > 1$, akkor $p > 2$. Legyen továbbá $g \in G$ p-edrendű elem! Erre triviálisan $1 < |\{h \in \langle g \rangle | h \sim g\}| < p$, hiszen $g \neq g^2$ benne vannak a halmazban. Másrészt $|\{h \in \langle g \rangle | h \sim g\}| = |N_G(\langle g \rangle) : C_G(\langle g \rangle)|$, ami osztja G rendjét, és ez ellentmondás. $\checkmark$

A bizonyításból általánosan kijött az is, hogy ha $p \mid |G|$ minimális, akkor $\mathrm{cp}(G) \equiv 1 \pmod{p}$.

Tétel 4 $\mathrm{cp}(G) = |G| + 1 \Leftrightarrow G$ *ciklikus.*

Bizonyítás A jobbról balra irány magától értetődő, a másikat mutatom meg. Mivel $|G| + 1 = \mathrm{cp}(G) \leq \exp(G) + 1$, így G exponense egyenlő a rendjével, vagyis G minden Sylowja ciklikus. Ekkor Zassenhaus jól ismert tétele szerint $G \cong Z_a \rtimes Z_b$, a ciklikus generátorok: x, y, $o(x) = a$, $o(y) = b$, $(a, b) = 1$, $x^y = x^r$ olyan r-rel, melyre $a|r^b - 1$, de $(a, r-1) = 1$. (Az $a = 1$ a ciklikus csoport esete.) Legyen n a legkisebb pozitív egész, melyre $n \equiv 1 \pmod b$, $\quad n \equiv r \pmod a$! Belátom, hogy minden csoportelem konjugált az n-edik hatványával. Ezzel a bizonyítás be is fog fejeződni, hiszen $n = |G| + 1$ csak a ciklikus esetben lehet. Legyen $g = y^\beta x^\alpha$ egy tetszőleges csoportelem! Bontsuk fel x-et a ciklikus p_i-Sylowokból adódó szorzótényezőkre:

$$g = y^\beta x_1^{\alpha_1} \cdots x_k^{\alpha_k},$$

valamint

$$g^n = y^{n\beta} x^{(1+r^\beta+r^{2\beta}+\cdots+r^{(n-1)\beta})\alpha} = y^\beta x_1^{(1+\cdots+r^{(n-1)\beta})\alpha_1} \cdots x_k^{(1+\cdots+r^{(n-1)\beta})\alpha_k}.$$

Azt állítom, hogy van olyan γ egész, melyre $g^{yx^\gamma} = g^n$. Ehhez az kellene, hogy

$$g^n = (y^\beta x^{r\alpha})^{x^\gamma} = y^\beta x^{r\alpha+(1-r^\beta)\gamma} = y^\beta x_1^{r\alpha_1+(1-r^\beta)\gamma_1} \cdots x_k^{r\alpha_k+(1-r^\beta)\gamma_k},$$

ahol $x^\gamma = x_1^{\gamma_1} \cdots x_k^{\gamma_k}$ definiálja γ_i-ket. Vagyis az kellene, hogy minden i-re

$$x_i^{(1+\cdots+r^{(n-1)\beta})\alpha_i} = x_i^{r\alpha_i+(1-r^\beta)\gamma_i},$$

azaz

$$p_i^{a_i} | (1 + \cdots + r^{(n-1)\beta})\alpha_i - r\alpha_i - (1 - r^\beta)\gamma_i.$$

Ha itt p_i nem osztja $1 - r^\beta$-t, akkor triviálisan találhatok jó γ_i-t. Ha pedig osztja, akkor y^β centralizálja $x_i^{p_i^{a_i-1}}$-et, így ennek mind a $p_i^{a_i-1}$ darab $p_i^{a_i-1}$-edik gyökét is fixálnia kell $(p_i, o(y)) = 1$ miatt, vagyis azt kapom, hogy $p_i^{a_i} | 1 - r^\beta$. Ekkor viszont minden m-re $r^{m\beta} \equiv 1 \pmod{p_i^{a_i}}$, s végül

$$(1 + \cdots + r^{(n-1)\beta})\alpha_i - r\alpha_i - (1 - r^\beta)\gamma_i \equiv n\alpha_i - r\alpha_i \equiv 0 \pmod{p_i^{a_i}},$$

ahogyan kellett. $\surd\!\!/$

Látható (a bizonyításból kiderül), hogy az állítás többé-kevésbé csalás, hiszen $\mathrm{cp}(G) \leq \exp(G)+1$ is mindig jó korlát; azokat a csoportokat kellene klasszifikálni, amelyekre itt teljesül egyenlőség. Ez a kérdés azonban összehasonlíthatatlanul nehezebbnek tűnik. **Tétel 3** úgy lenne élesíthető, hogy mik azok a csoportok, amelyekben $\mathrm{cp}(G) = \min\{p | \!\!/ \exp(G) \text{ prím}\}$. (Nyilván ennél nem lehet kisebb.) Ez is sokkal nehezebb kérdés, hiszen magában foglalja az úgynevezett "racionális" csoportok klasszifikációját is, amelyről később lesz még szó.

A bizonyítás kis módosítása mutatja, hogy Z-csoportokra, vagyis ahol a Sylowok ciklikusak $\mathrm{cp}(G) = \min\{n > 1 | n \equiv 1 \,(\mathrm{mod}\ b),\, n \equiv r^i \,(\mathrm{mod}\ a) \text{ valamely } i\text{-re}\}$. E formula segítségével válasz adható olyan kérdésekre is, hogy milyen csoportokban lesz $\mathrm{cp}(G) = |G| - k$ valamilyen rögzített k-ra. Ugyanis, ha az exponens kisebb a rendnél, akkor legfeljebb a fele, így véges sok kivételtől eltekintve csak Z-csoportokat kell vizsgálnunk, amelyekre van formula. A válasz se teljes, se szép nem lesz, ezért ki sem térek rá. (A $k = 1$ esetben a Klein-csoport tartozik a kivételek közé, a páratlanfokú diédercsoportok pedig a Z-csoportok közé.)

Most jöjjön még néhány egyszerű tulajdonság!

Állítás 5 *Ha $N \triangleleft G$, akkor $\mathrm{cp}(G/N) \leq \mathrm{cp}(G)$; sőt, ha G egy $\mathcal{H}-\mathrm{cp}$-csoport, akkor G/N is az.*

Állítás 6 *Ha $N \triangleleft G$, akkor $\mathrm{cp}(G)^{|G:N|} \geq \mathrm{cp}(N)$. $H \leq G$-re $\mathrm{cp}(G)^{|G:H|!} \geq \mathrm{cp}(H)$.*

Bizonyítás Ha $h \in H$, és $g \in G$ olyan, hogy $h^g = h^n$, akkor $h^{g^k} = h^{n^k}$. Az állítás most következik abból, hogy ha $N \triangleleft G$, akkor minden elem $|G:N|$-edik hatványa N-ben van, illetve ha $H \leq G$, akkor minden elem $|G:H|!$-adik hatványa H-ban van. $\surd$

Ennél több nem állítható normálosztóra. Ugyanis tekintsük például a $G = \langle x, y | x^{(k+1)^k-1} = y^k = 1,\, x^{k+1} = y^{-1}xy\rangle \cong Z_{(k+1)^k-1} \rtimes Z_k$ csoportot! Itt $\mathrm{cp}(G) = k+1$ triviális, hiszen kisebb nem lehet y miatt, de ez jó is. (Direkt kalkuláció helyett emlékezhetünk **Tétel 4** bizonyítására is.) Másrészről viszont $N = \langle x\rangle \triangleleft G$ ciklikus, $\mathrm{cp}(N) = (k+1)^k$, ezt összehasonlítva $|G:N| = k$-val látható, hogy az állítás tényleg pontos. (Megjegyzem, hogy $k = 2$ esetén $|G| = 16$ egy olyan csoport, amelynek konjugációs hatványszáma 3, és megvan az a különleges tulajdonsága, hogy a maximális részcsoportjai páronként nem izomorfak. Ilyen tulajdonságú p-csoportot ezen kívül csak a ciklikusakat ismerem.) Részcsoportra nem tudom, hogy mennyire éles a fenti korlát.

Bővítésről az alábbi szól:

Állítás 7 *Két csoport direkt szorzata akkor és csak akkor $\mathcal{H}-$ cp-csoport, ha mindkét tényező az.*

Itt sem állítható több; a direkt szorzat még szubdirektre sem cserélhető. $G = \langle x, y | x^4 = y^4 = 1, y^{-1}xy = x^{-1} \rangle$-ben $N_1 = \langle x^2 \rangle$, és $N_2 = \langle x^2 y^2 \rangle$ két diszjunkt normálosztó, a szerintük vett faktorcsoportok Q, illetve D_4. Mindkettő konjugációs hatványszáma 3, míg G-é 5.

3 Reprezentáció-elméleti segédeszközök

Ebben a fejezetben néhány kevésbé ismert tény mellett sok ismert szerepel, ha az olvasó jártas ezekben, átugorhatja a bizonyításaikat.

Állítás 8 *Ha χ karaktere G-nek, $K \leq \mathbb{C}$ a G-nek egy felbontási teste, és $\sigma \in Gal(K : \mathbb{Q})$, akkor χ^σ is karakter. Sőt σ permutálja az irreducibilis karaktereket.*

Speciálisan $K = \mathbb{Q}(\zeta)$ is vehető, ahol $\zeta = e^{\frac{2\pi i}{|G|}}$ (Brauer tétele). Itt minden relatív automorfizmus egy $|G|$-hez relatív prím kitevőjű hatványozás, így minden automorfizmus hathat a konjugáltosztályokon is. Ha $\zeta^\sigma = \zeta^k$, akkor legyen $[g]^\sigma = [g^k]$. (Itt $[g]$ jelöli g konjugáltosztályát.) E két hatás kapcsolatárol szól Brauer Permutációs Lemmája:

Állítás 9 *Ha van két permutáció, amely hat egy csoport irreducibilis karakterein, illetve konjugáltosztályain, és a két hatás a karaktertáblán ugyanaz, akkor a fixpontok száma is ugyanaz.*

Bizonyítás Legyen X a karaktertábla, mint mátrix, A a sorpermutációk mátrixa, B az oszloppermutációk mátrixa! Ekkor a feltételünk szerint $AX = XB$, s X invertálható volta miatt $A = XBX^{-1}$, speciálisan A és B nyoma egyenlő. De egy permutáció-mátrix nyoma egyenlő a permutáció fixpontszámával, így éppen a belátandó állítást kaptuk. $\surd$

Például az invertálás a konjugáltosztályokon, és a konjugálás a karaktereken ugyanazt implikálja a karaktertáblán (a komplex konjugálást), így a valós irreducibilis karakterek száma és a valós konjugáltosztályok száma ugyanaz. (Egy konjugáltosztály valós, ha $x \sim x^{-1}$ minden elemére.) Általában legyen $(k, |G|) = 1$! Most a $\zeta^\sigma = \zeta^k$ automorfizmussal $\chi^\sigma(g) = \chi(g^k)$ jelenti azt, hogy σ hatása az irreducibilis karaktereken, és a "k-adikra emelés" a konjugáltosztályokon ugyanazt indukálják a karaktertáblán. Így a k-adik hatványozásra zárt konjugáltosztályok száma és a σ-invariáns irreducibilis karakterek száma megegyezik. Ezt a gondolatmenetet sokszor fogom alkalmazni, főleg olyan környezetben, hogy az egyik permutáció az identitás, s ekkor a másik is az.

A moduláris karakterekkel egy kicsit más típusú leírást lehet adni:

Állítás 10 *Legyen p prím, q egy p-hatvány! Ekkor a következő állítások ekvivalensek:*

(i) $\mathbb{F}_q$ felbontási teste G-nek modulo p;

(ii) G-ben minden p-reguláris elem konjugált a q-adik hatványával.

Bizonyítás G-nek létezik véges felbontási teste modulo p, ami bővebb $\mathbb{F}_q$-nál, mondjuk $\mathbb{F}_{q^n}$. Legyenek $\varphi_1, \ldots, \varphi_l$ az irreducibilis p-moduláris karakterek ($\mathbb{F}_{q^n}$-beli értékekkel), valamint a p-reguláris osztályok egy teljes reprezentáns-rendszere $x_1, \ldots, x_l$! (Ezek száma, mint ismeretes, szintén l.) Miután $\det(\varphi_i(x_j)) \neq 0$, így Brauer Permutációs Lemmájának (**Állítás 9**) bizonyítása erre az esetre is alkalmazható a $\sigma : \alpha \mapsto \alpha^q$ testautomorfizmusra és a konjugáltosztályok q-adik hatványozására. Vagyis azt kapom, hogy ha minden irreducibilis p-moduláris karakter σ-invariáns, akkor minden p-reguláris elem konjugált a q-adik hatványával, és viszont. Egy karakter pontosan akkor σ-invariáns, ha értékei $\mathbb{F}_q$-ba esnek, és közismert tény, hogy ebben az esetben a reprezentáció is megvalósítható $\mathbb{F}_q$ fölött. Ez adja a bizonyítás végét. $\surd$

Definíció 11 *Legyen G olyan csoport, melynek minden karakterértéke valós, illetve racionális! Ekkor G-t valós, illetve racionális csoportnak hívjuk.*

Látszik a fenti jellemzésekből, hogy egy csoport pontosan akkor valós, ha minden eleme konjugált az inverzével. Illetve racionális, ha minden eleme konjugált minden, a rendjéhez relatív prím hatványához. Ami pontosan akkor teljesül, ha minden p prímre $\mathbb{F}_p$ felbontási teste G-nek.

A felbontási test kérdése jóval nehezebb 0-karakterisztikában, és nem is tartozik a tárgyhoz, csak megjegyzem, hogy a Brauer-Speiser tétel szerint egy valós karakter kétszerese már előáll valós reprezentáció karaktereként. Q nemlineáris karaktere mutatja, hogy ez nem javítható racionális karakter esetén sem.

Definíció 12 *Legyen K egy test, Ψ egy K fölötti G-reprezentáció! Ekkor a $\Psi^*(g) = \Psi(g^{-1})^T$ reprezentációt Ψ kontragrediens reprezentációjának hívjuk.*

Állítás 13 *Legyen K egy test, Ψ egy K-beli irreducibilis G-reprezentáció, amely ekvivalens a kontragredienssével! Ekkor Ψ megőriz egy nemelfajuló szimmetrikus vagy antiszimmetrikus bilineáris formát.*

Bizonyítás Legyen $W = \{A \in M_n(K) | A\Psi(g) = \Psi^*(g)A, \forall g \in G\} \leq M_n(K)$ altér. A Schur lemma szerint W minden nemnulla eleme invertálható (ez a nemelfajuláshoz kell majd). Ha $A \in W$, akkor nyilván $A^T \in W$ is, így $A + A^T$ jó lenne szimmetrikus bilineáris formának, amelyet megőriz Ψ, de lehet, hogy 0. Ha viszont minden $A \in W$-re $A + A^T = 0$, akkor Ψ antiszimmetrikusat tart meg. $\surd$

Ez az állítás tovább erősíthető egy fontos speciális esetben:

Állítás 14 ([9]) *Tegyük fel, hogy G minden komplex (irreducibilis) reprezentációja megvalósítható a valós test felett is! Ekkor G minden páratlan karakterisztikájú test feletti abszolút irreducibilis Ψ reprezentációja megtart egy nemelfajuló szimmetrikus bilineáris formát.*

Bizonyítás A feltételből azonnal következik, hogy minden karakter valós, vagyis minden Brauer-karakter is valós (a karakterek egész kombinációi a p'-osztályokon), s ezért minden modulo p reprezentáció ekvivalens a kontragredienssével. (Ugyanis ugyanaz a Brauer-karakterük.) Tehát az előző állítás (**Állítás 13**) miatt Ψ megtart egy szimmetrikusat, vagy egy antiszimmetrikusat. Belátom, hogy szimmetrikusat tart meg. (Valójában mindig csak egyik félét tarthat meg.)

Legyen ψ a Brauer-karaktere Ψ-nek, és legyenek $d_{\chi,\psi}$ a hozzá tartozó felbontási számok! Ekkor léteznek olyan $a_1, \ldots, a_k$ egész számok, melyekkel $\psi = \sum a_i\chi_i$ a p'-osztályokon, speciálisan $1 = \sum a_i d_{\chi_i,\psi}$, így van olyan χ, melyre $d_{\chi,\psi}$ páratlan. Rögzítsük ezt!

Legyen $K = \mathbb{Q}(\zeta)$, ahol ζ primitív $|G|$-edik egységgyök, valamint S a K-beli egészek gyűrűje, P egy itteni, p-t tartalmazó maximális ideál! K-nak a P-adikus értékelésre nézve egész elemeit A-val, ennek a gyűrűnek a maximális ideálját πA-val jelölve, $k = A/\pi A$ egy p karakteriszikájú test. Ismert, hogy ez G-nek felbontási teste modulo p. (A bizonyítása ennek a ténynek megtalálható például [5]-ben.)

Legyen tehát V egy χ karakterű irreducibilis KG-modulus! Ekkor, mivel a valós test felett megvalósítható, így megtart egy nemelfajuló szimmetrikus bilineáris formát. (Például vehetjük a következőt: Ha a Φ valós reprezentáció karaktere χ, akkor $A = \sum_{g\in G}\Phi(g)\Phi(g)^T$ szimmetrikus, azaz diagonalizálható ortogonális transzformációval. $B = T^TAT = \sum_{g\in G}T^{-1}\Phi(g)T^{-1}T\Phi(g)^TT$, ami nemelfajuló, szimmetrikus, és $T^{-1}\Phi(G)T$-invariáns.) Most találhatunk egy G-invariáns rácsot V-ben (maximális rangú szabad A-modulus), melynek πA szerinti faktora, L egy kG-modulus a következő tulajdonságokkal:

(i) L-ben $d_{\chi,\psi}$-szer fordul elő ψ-nek megfelelő egyszerű modulus kompozíciófaktorként,

(ii) van egy U kG-részmodulusa, hogy U-n és L/U-n is van egy-egy nemelfajuló, szimmetrikus, G-invariáns bilineáris forma.

Az első automatikusan teljesül, a másodikhoz tekintsünk először egy tetszőleges G-invariáns rácsot, M-et! Ha $B(u,v)$ jelöli a bilineáris formát, akkor legyen $M^+ = \{v \in V | B(M,v) \subseteq A\}$! Világos, hogy van egy elég nagy n egész, hogy $\pi^n M^+ \subseteq M \subseteq M^+$. $j = \lceil n/2 \rceil$ jelöléssel:

$$(M + \pi^j M^+)^+ = M^+ \cap \pi^{-j} M \supseteq M + \pi^j M^+$$

$$\pi^j (M + \pi^j M^+)^+ = \pi^j M^+ \cap M \subseteq M + \pi^j M^+$$

mutatják, hogy M helyett $M + \pi^j M$ is írható, n helyett j-vel. És ezt egészen $n = j = 1$-ig folytathatom.

Ez pedig azt mutatja, hogy

$$v, v' \mapsto B(v,v') \,(\mathrm{mod}\ \pi) \text{ nemelfajuló } M/\pi M^+\text{-on,}$$

$$v, v' \mapsto \pi^{-1}B(v,v') \,(\mathrm{mod}\ \pi) \text{ nemelfajuló } M^+/M \cong \pi M^+/\pi M\text{-en.}$$

Vagyis $L = M$ modulo π, $U = \pi M^+$ modulo π jó választás.

(Ez a része a bizonyításnak Quillentől származik.[15])

A bizonyítás befejezéséhez most már elegendő a következőt igazolni: Ha W olyan irreducibilis kG-modulus, amely nem tart meg nemelfajuló szimmetrikus bilineáris formát, de izomorf a kontragrediensével, akkor egy nemelfajuló szimmetrikusat megtartó végesen generált modulus kompozícióláncában páros sokszor szerepel. Ez ugyanis alkalmazható L/U-ra és U-ra is, ellentmondva $d_{\chi,\psi}$ páratlan voltának.

Legyen tehát U egy végesen generált kG-modulus, amelyen van egy G-invariáns szimmetrikus bilineáris forma, $X \leq U$ egy irreducibilis kG-részmodulus! X-re megszorítva a forma csak nemelfajuló, vagy teljesen izotróp lehet az irreducibilitás miatt. Ha X-en a forma nemelfajuló, akkor persze $X \ncong W$, és $U \cong X \oplus X^\perp$ miatt áttérve $X^\perp$-re folytatható a felbontogatás. Vagyis feltehető, hogy X-re megszorítva a forma teljesen izotróp.

Ekkor $X^\perp \geq X$, és a forma indukál egy nemelfajuló formát $X^\perp/X$-en is. Másrészről pedig $U/X^\perp$ kontragrediense X-nek, vagyis W vagy ugyanannyiszor van meg $X^\perp/X$-ben, mint U-ban, vagy 2-vel többször, de mindkét esetben lehet indukciót alkalmazni. Ezzel az állítást beláttam. $\surd$

Szükség lesz a későbbiekben a következő állítás módosított változatára:

Állítás 15 *Legyen G Frobenius-csoport N Frobenius-maggal. Ekkor minden nemtriviális irreducibilis komplex N-karakternek az indukáltja is irreducibilis, és így előáll minden N-et nem tartalmazó magú irreducibilis komplex G-karakter.*

Bizonyítás Legyen $\varphi \in \mathrm{Irr}(N)$ nemtriviális! φ^G irreducibilis voltához elegendő, hogy φ inercia-részcsoportja N. Legyen $g \in G \setminus N$ tetszőleges, ha valamely $x \in N$-re $x^g \sim x$ N-ben, akkor $x^g = x^n$, s így $gn^{-1} \in C_G(x) \setminus N$, vagyis $x = 1$. Tehát g hatása fixpontmentes a nemtriviális konjugáltosztályokon, így Brauer Permutációs Lemmája (**Állítás 9**) miatt a nemtriviális karaktereken is, hiszen $\theta^g(n) = \theta(n^{g^{-1}})$.

Ha $\chi \in \mathrm{Irr}(G)$ magja nem tartalmazza N-et, akkor legyen φ nemtriviális irreducibilis összetevője χ_N-nek. Erre $(\chi, \varphi^G) = (\chi_N, \varphi) > 0$, és φ^G irreducibilis, azaz $\chi = \varphi^G$. $\surd$

4 A fő eredmények

Először jöjjön egy tétel, amelynek a bizonyítása jó illusztrációja a továbbiaknak is:

Tétel 16 ([9]) *Ha G minden komplex reprezentációja a valósak felett is megvalósítható, és G racionális csoport, akkor ciklikus kompozíció-faktora csak Z_2, Z_3 lehet.*

Bizonyítás Legyen $L \triangleleft G$, $M/L \triangleleft G/L$ minimális úgy, hogy M/L elemi Abel p-csoport! G helyett most tekinthetem G/L-et, erre is teljesülnek ugyanis a feltételek, vagyis feltehető, hogy $L = 1$, M elemi Abel p-normálosztó.

Legyen $K = C_G(M) \triangleleft G$, $H = G/K$! A korábbi **Állítás 10** szerint $\mathbb{F}_p$ felbontási teste H-nak, így M-en H hatása abszolút irreducibilis. Jelölje ezt a reprezentációt Ψ! Minden $x \in M$-re, minden $(r,p) = 1$-et kielégítő r-re van olyan $g \in H$, hogy $x^r = x^g$. M-et $\mathbb{F}_p$-vektortérnek tekintve ezt úgy fejezhető ki, hogy minden $x \in M$-re, és $\lambda \in \mathbb{F}_p^*$-ra van olyan $g \in H$, hogy $\lambda x = x\Psi(g)$.

A szintén korábbi **Állítás 14** szerint M-en van egy $\Psi(H)$-invariáns szimmetrikus forma $(-,-)$. Legyen $\mathbb{F}_p^* = \langle\lambda\rangle$! Ekkor minden $x \in M$-re van $g \in H$, hogy $x\Psi(g) = \lambda x$, ahonnan $(x,x) = (x\Psi(g), x\Psi(g)) = \lambda^2(x,x)$. Miután (x,x) nem lehet minden x-re 0, vagyis $\lambda^2 = 1 \Rightarrow p-1|2$, így $p \leq 3$ adódik, amivel a bizonyításnak vége. $\surd\!\!/$

S_n példája mutatja, hogy az alternáló csoportok mindig előfordulhatnak racionális csoportban kompozíció-faktorként. Az E_6, E_7, E_8 gyökrendszerek Weyl-csoportjai három újabb egyszerű csoportot hoznak be a képbe, így látszik, hogy az állítás tetszőleges racionális csoportra való továbberősítéséhez már komolyabb eszközök szükségesek.

Most következik néhány, a későbbiekben többször használt állítás, amelyek egymásutánja előrevetíti alkalmazásukat is. A feltételek között az antiszimmetrikusság fog szerepelni, mivel a szimmetrikus eset az állítások jelentős részében elő sem fordulhat. Másrészt a szimmetrikus esetben a fent látható módon $o_q(h)|2$ következik. (Jelölést lásd lent.)

A gondolatmenet Gowtól[9], a Brauer-karakteres állításokra vonatkozó részek jórészt Soarestól[6] származnak. Tudtommal korábban nem voltak ismertek **Tétel 25**, **Tétel 27** és **Tétel 29**.

Először egy definíció:

Definíció 17 *Legyen $\mathcal{H} \subseteq K$ tetszőleges halmaz! Egy G csoport egy ${}_KV$ vektortéren vett hatása kielégíti a $\mathcal{H}$-sajátérték feltételt, ha minden $v \in V$-hez, $\lambda \in \mathcal{H}$-hoz létezik olyan $g \in G$, melyre $vg = \lambda g$. A precízség kis mellőzésével az egész számokat is fogom az $\mathbb{F}_p$ testek elemeinek tekinteni.*

Állítás 18 *Legyen $\mathbb{F}_q$ egy p-karakterisztikájú véges test, $\mathcal{H} \subseteq \mathbb{F}_q$ tetszőleges halmaz! G egy p'-csoport, amely hat egy ${}_{\mathbb{F}_q}V$ vektortéren, teljesíti a $\mathcal{H}$-sajátérték feltételt, valamint vagy*

(i) megőriz egy nemelfajuló antiszimmetrikus bilineáris formát, vagy

(ii) a hatás Brauer-karaktere, φ σ-invariáns, ahol $\sigma \in Gal(\mathbb{Q}(e^{\frac{2\pi i}{|G|}}) : \mathbb{Q})$ egy testautomorfizmus.

Ekkor van ugyanezeket a feltételeket kielégítő G_0 csoport egy ${}_{\mathbb{F}_q}V_0$-on vett hatással, amely ráadásul még fixpontmentes is.

Bizonyítás Legyen adott $v \in V$ esetén $C_G(v)$ a v stabilizátora, és legyen K egy maximális ilyen! $N = N_G(K)$, $V_0 = C_V(K) = \{v \in V | vk = v \ \forall k \in K\text{-ra}\}$ jelöléssel $G_0 = N/K$ hatása fixpontmentes V_0-on a maximalitás miatt. Ha $v \in V_0$, $\lambda \in \mathcal{H}$ tetszőleges, akkor van $g \in G$, hogy $vg = \lambda v$. Ezzel a g-vel $g^{-1}C_G(v)g = C_G(v)$, de K maximalitása folytán $K = C_G(v)$, így $g \in N$, tehát G_0 is teljesíti a $\mathcal{H}$-sajátérték feltételt.

Most szétválik a bizonyítás a két lehetőség szerint.

(i) Legyen $W = \{v \in V_0 | (v, u) = 0 \ \forall u \in V_0\}$, $W^0 = W$-nek V-beli annullátora! Így $W^0 \geq V_0$, és N-invariáns, vagyis a Maschke-tétel miatt van N-invariáns direkt kiegészítője: $V = W^0 \oplus U$. Itt $\dim U = \dim W$, és U izomorf W duális terével, s N skalárszorzattartása miatt ezek, mint N-modulusok egymás kontragrediensei. De K fixálja W-t, így fixálja U-t is, amiből $U \cap V_0 = 0$ miatt $U = W = 0$ következik, tehát a forma nemelfajuló.

(ii) Maschke tétele miatt most is létezik egy $V = V_0 \oplus U$ N-invariáns felbontás. Ennek megfelelően adódik a $\varphi_N = \varphi_1 + \varphi_2$ Brauer-karakter felbomlása is. Ha ψ tetszőleges irreducibilis Brauer-karakter, akkor triviális, hogy $\mathrm{Ker}\psi = \mathrm{Ker}\psi^\sigma$. És $(\varphi_1, \psi) > 0 \Rightarrow \mathrm{Ker}\psi \geq K$, $(\varphi_2, \psi) > 0 \Rightarrow \mathrm{Ker}\psi \not\geq K$, azaz σ permutálja φ_1 irreducibilis komponenseit, vagyis maga φ_1 is σ-invariáns.

Mindkét esetet, s ezzel a bizonyítást is lezártam. $\surd$

Állítás 19 *Legyen $\mathbb{F}_q$ egy p-karakterisztikájú véges test, $\mathcal{H} \subseteq \mathbb{F}_q$ tetszőleges halmaz! G egy p'-csoport, amely fixpontmentesen hat egy ${}_{\mathbb{F}_q}V$ vektortéren, teljesíti a $\mathcal{H}$-sajátérték feltételt, $2 \neq r | o_q(h)$ prím valamilyen $h \in \mathcal{H}$-ra. Ekkor a következőket állítom:*

(*i*) *Ha G megőriz egy nemelfajuló antiszimmetrikus bilineáris formát, akkor $O_r(G)=1$.*

(*ii*) *Ha a hatás Brauer-karaktere, φ σ-invariáns, ahol $\sigma: e^{\frac{2\pi i}{|G|}}=\zeta\mapsto\zeta^k$ egy testautomorfizmus, akkor vagy $r|k-1$, vagy $O_r(G)=1$.*

Bizonyítás Mivel r páratlan, G r-Sylowja ciklikus, (hiszen G most Frobenius-komplementum,) s ha $O_r(G)>1$, akkor pontosan egy r-edrendű R részcsoportja van G-nek. Legyen mondjuk $R=\langle x\rangle$! Ha most $v\in V$ tetszőleges, akkor van olyan $g\in G$, hogy $vg=hv$. Legyen $o_q(h)=rt$, $\mu=h^t$ egy $\mathbb{F}_q^*$-beli r-edrendű elem. Nyilván $vg^t=\mu v$, így $o(g^t)=r$, hiszen g^t még nem fixálja v-t, de az r-edik hatványa már igen, és fixálni csak az egységelem tud. Vagyis $g^t\in R$, amiből következik, hogy v x-nek is sajátvektora. Beláttuk, hogy x-nek minden vektor sajátvektora, vagyis $x=\mu_0\mathrm{id}_V$, ahol μ_0 is r-edrendű $\mathbb{F}_q^*$-ban.

Most válik szét a bizonyítás.

(i) Ekkor minden u,v vektorra $(u,v)=(ux,vx)=\mu_0^2(u,v)$, vagyis $\mu_0^2=1$, de ez lehetetlen. Azaz az $O_r(G)>1$ feltevésünk jogtalan volt.

(ii) Ekkor $\mu_0\varphi(1)=\varphi(x)=\varphi(x^k)=\mu_0^k\varphi(1)$, vagyis $\mu_0^{k-1}=1$, ahonnan $r|k-1$ adódik.

A bizonyításnak mindkét esetben vége. $\surd$

A következő állítás bizonyításában fontos szerepe van a feloldhatóságnak.

Állítás 20 *Legyen $\mathbb{F}_q$ egy p-karakterisztikájú véges test, $\mathcal{H}\subseteq\mathbb{F}_q$ tetszőleges halmaz! G egy feloldható p'-csoport, amely fixpontmentesen hat egy ${}_{\mathbb{F}_q}V$ vektortéren, teljesíti a $\mathcal{H}$-sajátérték feltételt, $2\neq r|o_q(h)$ prím valamilyen $h\in\mathcal{H}$-ra. Ha $O_r(G)=1$, akkor csak $r=3$ lehet, de ebben az esetben is igaz, hogy $|G|\not\equiv 0\,(mod\ 9)$.*

Bizonyítás Legyen F a Fitting-részcsoportja G-nek! Ekkor $C_G(F)\leq F$. Ha most $g\in G$ r-edrendű elem, akkor g nemtriviális automorfizmust indukál F-en, hiszen $g\notin F$. Így g nemtriviálisan hat F egy S s-Sylowján is valamilyen s-re, hiszen F nilpotens. Ha $s>2$, akkor S ciklikus. Legyen $u\in S$ s-edrendű! Most $u^g=u$ esetén $g\in C_G(S)$, amit kizártunk, de $u^g\neq u$ esetén $\langle u,g\rangle$ egy nemciklikus sr-rendű részcsoportja egy Frobenius-komplementumnak, ami lehetetlen.

Maradt az az eset, amikor $s = 2$. Ilyenkor S általánosított kvaternió, vagy ciklikus, amelyeknek az automorfizmuscsoportja 2-csoport, kivéve az $S = Q_8$ esetet, melyre $\mathrm{Aut}(S) \cong S_4$. Így csak $r = 3$ lehet. De 9-edrendű automorfizmus egyáltalán nem fordulhat elő, mint ezt már eddig beláttam. Ezzel az állítást igazoltam. $\surd$

A következő részek az "$r = 3$; $r = 2$, kvaternió Sylow; $r = 2$, ciklikus Sylow" esetszétválasztást írják le.

Állítás 21 *Legyen $\mathbb{F}_q$ egy p-karakterisztikájú véges test, $\mathcal{H} \subseteq \mathbb{F}_q$ tetszőleges halmaz! G egy feloldható p'-csoport, $O_3(G) = 1$, fixpontmentesen hat egy ${}_{\mathbb{F}_q}V$ vektortéren, teljesíti a $\mathcal{H}$-sajátérték feltételt, $o_q(h) = 2^b 3$ valamilyen $h \in \mathcal{H}$-ra. Ekkor $o_q(h) = 6$, vagy $o_q(h) = 3$.*

Bizonyítás Az előző állítás (**Állítás 20**) bizonyítása mutatta, hogy ebben az esetben $O_2(G)$ a (8-adrendű) kvaterniócsoport, és így G 2-Sylowja is általánosított kvaternió. De egy általánosított kvaterniócsoportnak minden nemciklikus valódi normálosztója 2 indexű, vagyis a Sylow rendje legfeljebb 16. Mivel G-ben van 2^b-edrendű elem, így $b \leq 3$. A $b \leq 1$ eseten kívül az alábbiak lehetnek:

$b = 3$ Ekkor G-ben van 24-edrendű elem g, és G-nek a $\{2, 3\}$-Hall-részcsoportja 48-adrendű. Így G 3-Sylowja, $\langle g^8 \rangle$ normális a Hall-részcsoportban. Másrészt $O_2(G)$ is normális ott, ami ellentmond annak, hogy g^8 nemtriviálisan hat rajta.

$b = 2$ Ekkor G-ben van 12-edrendű elem g, és G-nek a $\{2, 3\}$-Hall-részcsoportja 24-ed-, vagy 48-adrendű. Így G 3-Sylowja, $\langle g^4 \rangle$ vagy normális a Hall-részcsoportban, és az előző ellentmondást kapom, vagy a Hall-részcsoport 48-adrendű, és $\langle g^4 \rangle$ normalizátora a Hall-részcsoportban $\langle g \rangle$. Ekkor viszont alkalmazható Burnside Transzfer Tétele, ami mutatja, hogy $\langle g^4 \rangle$-nek van normál-komplementuma a Hall-részcsoportban. Ez azonban 16-odrendű általánosított kvaterniócsoport, amelyen nincs harmadrendű hatás. Vagyis ez az eset sem fordulhat elő.

Más eset nincs, a bizonyításnak vége. $\surd$

Állítás 22 *Legyen $\mathbb{F}_q$ egy p-karakterisztikájú véges test, $\mathcal{H} \subseteq \mathbb{F}_q$ tetszőleges halmaz! G egy feloldható p'-csoport, amely fixpontmentesen hat egy ${}_{\mathbb{F}_q}V$ vektortéren, teljesíti a $\mathcal{H}$-sajátérték feltételt, $o_q(h) = 2^t$ valamilyen $h \in \mathcal{H}$-ra, és G 2-Sylowja általánosított kvaterniócsoport.*

(i) Ha G megőriz egy nemelfajuló antiszimmetrikus bilineáris formát, akkor $o_q(h) = 4$.

(ii) Ha a hatás Brauer-karaktere, φ σ-invariáns, ahol $\sigma : e^{\frac{2\pi i}{|G|}} = \zeta \mapsto \zeta^k$ egy testautomorfizmus, akkor vagy $o_q(h)|k-1$, vagy $o_q(h) = 4$.

Bizonyítás A bizonyítás az (i) esetben indirekt lesz, ugyanis felteszem, hogy $t \geq 3$.

Legyen $L = G/O_2(G)$, $F(L)$ L Fitting-részcsoportja! Mivel ez páratlan rendű, így ciklikus. Egyébiránt $L/F(L) = L/C_L(F(L)) \leq$Aut$(L)$, ami Abel, vagyis L 2-Sylowja is Abel, de faktora egy általánosított kvaterniócsoportnak, így legfeljebb 4-edrendű. Legyen $D_1 = \langle a, b | a^{2^s} = 1, a^{2^{s-1}} = b^2, b^{-1}ab = a^{-1} \rangle$ az egyik 2-Sylow G-ben ($s \geq t$), $D = \langle c, b \rangle$ (itt $c = a^{2^{s-t}}$)! L 2-Sylowja Abel, tehát $\langle a^2 \rangle = D_1' \leq O_2(G)$.

Most $\varrho \in \mathbb{F}_q^*$ egy 2^t-edrendű elem, és $\tau = \varrho^{2^{t-2}}$. Ha $v \in V$ tetszőleges, akkor van olyan $g \in G$, melyre $vg = \varrho v$. Így $o(g) = 2^t$. De minden 2^t-edrendű elem D-be konjugálható:$g^x \in \langle c \rangle$ valamilyen x-re, mivel csak ez a 2^t-edrendű ciklikus részcsoport van D_1-ben. Ekkor $(g^{2^{t-2}})^x \in O_2(G)$, de ez normális, így $g^2 \in O_2(G)$.

Vonjuk le ebből a tanulságot: Minden vektort meg tudunk τ-szorozni egy $O_2(G)$-beli elemmel. Ha $f \in G$ tetszőleges negyedrendű elem, akkor a hatása diagonalizálható, hiszen $\mathbb{F}_q^*$-ban van negyedrendű elem. Minden sajátértéke τ, vagy τ^{-1}. Azaz vagy f, vagy f^{-1} τ-szoroz egy $v \in V$ vektort. De ezt a vektort τ-szorozza egy $O_2(G)$-beli e is, vagyis a fixpontmentes hatás miatt $f = e$, vagy $f = e^{-1}$, de mindkét esetben $O_2(G)$-beli. Mivel egy általánosított kvaterniócsoportot generálnak a negyedrendű elemei, így $O_2(G) = D_1$.

Ez azt jelenti, hogy minden vektort egy $\langle c \rangle$-belivel tudok ϱ-szorozni, vagyis $c = \varrho_0 \mathrm{id}_V$. Ha most

(i) G megőriz egy nemelfajuló antiszimmetrikus bilineáris formát, akkor minden u, v vektorpárra $(u, v) = (uc, vc) = \varrho_0^2(u, v)$, ami $\varrho_0^2 \neq 1$ miatt $(u, v) = 0$-t jelentené. Ez ellentmondás.

(ii) G hatásának Brauer-karaktere, φ σ-invariáns, akkor $\varrho_0\varphi(1) = \varphi(c) = \varphi(c^k) = \varrho_0^k\varphi(1)$ miatt $2^t|k-1$.

Mindkét esetnek vége. $\surd$

Az utolsó a legnehezebb eset, először egy egyszerűbb eredmény következik.

Állítás 23 *$\mathbb{F}_q$ egy p-karakterisztikájú véges test, $\mathcal{H} \subseteq \mathbb{F}_q$ tetszőleges halmaz, G egy feloldható p'-csoport, amely fixpontmentesen hat egy ${}_{\mathbb{F}_q}V$ vektortéren, teljesíti a $\mathcal{H}$-sajátérték feltételt, $o_q(h) = 2^t$ valamilyen $h \in \mathcal{H}$-ra, és G 2-Sylowja ciklikus. Ezenkívül vagy*

(i) G megőriz egy nemelfajuló antiszimmetrikus bilineáris formát, vagy

(ii) a hatás Brauer-karaktere, φ σ-invariáns, ahol $\sigma : e^{\frac{2\pi i}{|G|}} = \zeta \mapsto \zeta^k$ egy testautomorfizmus.

Ekkor feltehető, hogy $G \cong H \rtimes Z_{2^t}$, ahol $|H|$ páratlan rendű ciklikus csoport. (Itt az, hogy "feltehető" azt jelenti, hogy van egy esetleg kisebb $G_0 \leq G$ csoport, amely ilyen szerkezetű, és a hatása teljesíti a h-sajátérték feltételt erre a fix h-ra.)

Bizonyítás Mivel G minden Sylowja ciklikus, így G metaciklikus, és ha M jelöli az egyik 2-Sylow 2^t-rendű részcsoportját, akkor az M által generált normálosztó G-ben $H \rtimes Z_{2^t}$ alakú lesz, ahol $|H|$ páratlan rendű, ciklikus. (A metaciklikusság mutatja, hogy H-ba azok a Sylowok kerülnek be, amelyeken Z_{2^t} nemtriviálisan hat. De ezek egymáson már triviálisan hatnak.) Így H kielégíti a megkívántakat. $\surd$

Most tekintsük az antiszimmetrikus esetet konklúzióját!

Állítás 24 *$\mathbb{F}_q$ egy p-karakterisztikájú véges test, $\mathcal{H} \subseteq \mathbb{F}_q$ tetszőleges halmaz, G egy feloldható p'-csoport, amely fixpontmentesen, egy nemelfajuló antiszimmetrikus bilineáris formát megőrizve hat egy ${}_{\mathbb{F}_q}V$ vektortéren. Teljesíti a $\mathcal{H}$-sajátérték feltételt, $o_q(h) = 2^t$ valamilyen $h \in \mathcal{H}$-ra, és $G \cong H \rtimes Z_{2^t}$, ahol $|H|$ páratlan rendű ciklikus csoport. Ekkor $t \leq 2$.*

Bizonyítás Legyen $d = \dim_{\mathbb{F}_q} V$, τ egy negyedrendű elem $\mathbb{F}_q^*$-ban! Ha $x \in G$ tetszőleges negyedrendű elem, akkor legyen $V(x) = Ker(x - \tau\mathrm{id}_V)$ a τ-hoz tartozó sajátaltér! Belátom, hogy ez $d/2$ dimenziós.

Mivel x megtart egy nemelfajuló bilineáris formát, így bármely két $V(x)$-beli vektor merőleges egymásra, és bármely két $V(x^{-1})$-beli vektor merőleges egymásra. Ezért aztán a nemelfajulás miatt csak $\dim V(x) = d/2$ fordulhat elő.

Ha $x \neq y$ negyedrendűek, akkor $V(x) \cap V(y) = 0$, hiszen a hatás fixpontmentes. Másrészt $V = \cup_{o(x)=4} V(x)$. Tehát G-ben pontosan $q^{d/2}+1$ darab negyedrendű elem van. Ebből az is látszik, hogy negyedrendű elem nincs $O_2(G)$-ben, ami így csak kételemű.

G-ben a negyedrendű elemeknek két konjugáltosztálya van, a reprezentánsok mondjuk m, m^{-1}. Ezért $|G : C_G(m)| = \frac{1}{2}(q^{d/2}+1)$, ami páratlan, hiszen osztja $|H|$-t. Most [12] II.3.10. tétele miatt H irreducibilis, ciklikus. ($|H|$ nem oszthatja $(q^{d/2k}+1)$-et egy $k \geq 2$-re sem.) De mivel H szimplektikus (rész)csoport, [12] II.9.23. tétele miatt $|H|\,|q^{d/2}+1$, vagyis $|H| = \frac{1}{2}(q^{d/2}+1)$, $H \cap C_G(m) = 1$. Ez azt is jelenti, hogy $G/Z(G)$ Frobenius-csoport H-val izomorf maggal, és $Z_{2^{t-1}}$-gyel izomorf komplementummal.

Itt alkalmazható a Frobenius-csoportok reprezentációiról szóló, korábban látott **Állítás 15**. Eszerint $G/Z(G)$ minden hű irreducibilis reprezentációja $HZ(G)/Z(G)$-nek egy nemtriviális irreducibilis reprezentációjáról van indukálva. Ha most G-nek keressük egy hű irreducibilis reprezentációját, akkor azt találjuk, hogy ennek pedig $HZ(G)$ egy $Z(G)$-t nem tartalmazó magú irreducibilisáról kell indukálódnia. Mivel $HZ(G)$ egy $q^{d/2}+1$-edrendű ciklikus csoport, az irreducibilisak lineárisak. G egy p'-csoport, vagyis a modulo p abszolút irreducibilis reprezentációi ugyanígy viselkednek.

Bontsuk most fel $\mathbb{F}_{q^*} \otimes_{\mathbb{F}_q} V$-t abszolút irreducibilisak összegére! (Itt $\mathbb{F}_{q^*}$ felbontási teste G-nek modulo p.) Mivel a hatás fixpontmentes volt, az összes tag hű lesz. Mindnek a foka 2^{t-1}, így $e = 2^{1-t}d$ darab van belőlük. Ha x egy 2^t-edrendű elem az S 2-Sylowban, akkor tetszőleges $\Lambda^G(x)$-nek a h pontosan egyszeres sajátértéke, hiszen $\Lambda^G{}_S$-nek tartalmaznia kell az összes hű irreducibilis S-reprezentációt. Összeszámlálással kapom, hogy x-nek a h e-szeres sajátértéke. Ebből a korábbi stabilizátoros számolással az kapom, hogy G-ben $\frac{q^d-1}{q^e-1}$ darab 2^t-edrendű elem van.

Másképpen számolva: Mivel $C_G(x) = \langle x \rangle$, ezért G-ben $\varphi(2^t)\frac{1}{2}(q^{d/2}+1)$ darab 2^t-edrendű elem van. A két eredményt összevetve:

$$q^{d/2} - 1 = 2^{t-2}(q^e - 1).$$

Ha $e < d/2$, akkor $e \leq d/4$, s $q^{d/4}+1 \leq 2^{t-2} \leq \frac{q-1}{4}$, ami lehetetlen. (Ne feledje az olvasó, hogy $\mathbb{F}_q^*$-nak van 2^t-edrendű eleme!) Így csak $e \geq d/2$ lehet, ami $t \leq 2$-t jelenti. Ez volt a bizonyítandó. $\surd$

Az invariáns Brauer-karakter esetét hasonlóan lehet kezelni. De mivel igazán jó általános következtetés nem jön ki belőle, csak a speciális esetekben fogom leírni az eljárást.

A most következő tétel a szakdolgozatom legfőbb eredménye.

Tétel 25 *$n \geq 3$ egész, $\mathcal{H} = \{-1, n\}$, G feloldható $\mathcal{H}-$ cp-csoport. Ekkor $|G|$ minden p páratlan prímosztójára $p|(n^6 - 1)$, vagy $p|(n^4 - 1)$. Itt az első eset nem lehetséges, ha $3|n$.*

Speciálisan $n = 3$-ra $p|80 = 16 \cdot 5$, vagyis $p = 5$.

Bizonyítás Legyen G_0 minimális p-vel osztható rendű ilyen tulajdonságú csoport! Ekkor G_0-nak minimális normálosztója $N \cong Z_p^k$. $G = G_0/N$ hat N-en. A hatás $-1 \in \mathcal{H}$ miatt ekvivalens a kontragrediensével, vagyis megőriz egy nemelfajuló szimmetrikus, vagy antiszimmetrikus bilineáris formát. Ha a hatás szimmetrikusat tart meg, akkor a fejezet első tételének (**Tétel 16**) bizonyításához hasonlóan kijön, hogy $p|n^2 - 1$.

Tehát antiszimmetrikusat tart meg. A fenti állítások sorát alkalmazva látható, hogy csak $o_p(n) = 1, 2, 3, 4, 6$ képzelhető el. Az $o_p(n) = 3, 6$ lehetőségek csak az $r = 3$ esetben fordulhattak elő, amit $3|n$ kizár. Ezzel a tételt beláttam. $\surd\surd$

Kevesebb feltevéssel is igaz a speciális eset:

Tétel 26 *Ha G feloldható $3-$ cp-csoport, akkor G $\{2, 5\}$-csoport.*

Bizonyítás Legyen $p \neq 5$ egy páratlan prímszám, amelyre indirekt módon felteszem, hogy van $3-$ cp-csoport, melynek p osztja a rendjét! Legyen G_0 minimális p-vel osztható rendű ilyen tulajdonságú csoport. Ekkor G_0-nak minimális normálosztója $N \cong Z_p^k$. $G = G_0/N$ hat N-en. A hatás Brauer-karaktere, φ köb-invariáns, vagyis a fenti állításokban használt jelöléssel $k = 3$. Másrészt G-re igazak a tétel feltételei, vagyis indukcióval feltehető, hogy G egy $\{2, 5\}$-csoport. Most az **Állítás 19**-ben $r|2$ adódik, ami lehetetlen, hiszen ott r egy páratlan prímet jelölt.

A továbbiakban kiderül, hogy $o_p(3)$ 2-hatvány, ugyanis 3 nem osztja G rendjét. A kvaternió típusú Sylow esete $p|3^4 - 1$-et ad.

A ciklikus esetben tehát $G \cong Z_{5^s} \rtimes Z_{2^t}$ feltehető. De most, ha Z_{2^t} egy m negyedrendű eleme centrális lenne, akkor $m = \mu \mathrm{id}_N$ adódna, ahonnét $\mu = \mu^3$, vagyis $\mu^2 = 1$, ami lehetetlen. De így m centralizátora Z_{2^t}, hiszen ha 5-elemet is fixálna, akkor minden 5-elemet fixálna.

Ekkor G hű irreducibilis reprezentációit a fenti módon le tudom írni. Ahhoz, hogy a konklúziót is ugyanúgy le tudjam vonni, az ottani stabilizátoros számolást kell ellenőriznem.

Legyen Ψ abszolút irreducibilis reprezentáció, legyen ϱ egy 2^u-adrendű elem $\mathbb{F}_p^*$-ból, és g egy egy 2^u-adrendű elem Z_{2^t}-ből! Miután $\Psi_{Z_{2^t}}$-ben minden hű irreducibilis reprezentáció pontosan egyszer előfordul, így $\Psi(g)$-nek ϱ pontosan 2^{t-u}-szoros sajátértéke. Azaz független g-től, és ϱ-tól. A leszámlálás most azt adja, hogy G-ben a 2^u-adrendű elemek száma:

$$\frac{p^d - 1}{p^{2^{1-u}d} - 1}.$$

Vagyis a fenti becslés eredménye ugyanaz, $o_p(3)|4$. Innen $p|3^4 - 1 = 16 \cdot 5$ adódik. Ezzel a tételt beláttam. $\surd\!\!/$

A feloldhatóság is kiküszöbölhető használva Thompson Tételét: Ha egy nemkommutatív egyszerű csoport rendje nem osztható hárommal, akkor Suzuki-csoport.

Tétel 27 *Ha G $3-\mathrm{cp}$-csoport, akkor G $\{2,5\}$-csoport.*

Bizonyítás Legyen G_0 minimális nemfeloldható $3-\mathrm{cp}$-csoport! Ekkor G_0-nak minimális normálosztója, N izomorf nemkommutatív egyszerűek direkt szorzata. Thompson Tétele miatt van olyan m egész szám, hogy $N \cong Sz(2^{2m+1}) \times \cdots \times Sz(2^{2m+1}) = T_1 \times \cdots \times T_k$. Ha $h \in T_1$ tetszőleges, akkor van egy $g \in G_0$, hogy $h^g = h^3$. Mivel T_1 egyszerű, $h^3 \in T_1^g \cap T_1 \triangleleft T_1$, így $T_1^g = T_1$, vagyis a g-vel való konjugálás egy automorfizmusa a T_1 Suzuki-csoportnak. De ismert, hogy a $Sz(2^{2m+1})$ Suzuki-csoportban van olyan h elem, hogy $o(h) = 2^{2m+1} - 1$, és csak a $\pm 1, \pm 2, \pm 4, \ldots, \pm 2^{2m}$-edik hatványaiba vihető automorfizmussal. ([13]XI. 1.5.) Ez a tény mutatja, hogy ilyen eset valójában nem forduhat elő. G_0 mindenképpen feloldható. $\surd\!\!/$

A minimális példa $3-\mathrm{cp}$-csoportra, amely nem 2-csoport, 200-adrendű. Az 5-Sylowja elemi Abel normálosztó, a komplementum kvaterniócsoport. A komplementum hatása $SL(2,5)$ 2-Sylowjának hatásával egyezik meg.

Kicsit több vesződséggel kezelhető az $n = 4$ eset is. Itt a feloldhatóság általában is következne a Feit-Thompson Tételből. Szükség lesz az alábbi számelméleti lemmára.

Lemma 28 *A $p^{2a}+p^a+1 = 7^l3$ diofantoszi egyenletnek $p = 19$, és 73 esetén nincsen pozitív megoldása.*

Bizonyítás $p = 19$ esetén a bal oldal 1-gyel, a jobb oldal pedig 7^l3-mal kongruens modulo 19. De $7^3 = 343 \equiv 1 \pmod{19}$, és $3 \equiv 3 \pmod{19}$, $7 \cdot 3 \equiv 2 \pmod{19}$, $7^2 3 \equiv 14 \pmod{19}$, ami mutatja, hogy $p = 19$ tényleg lehetetlen.

$p = 73$ esetén $l = 1$ nem jó, de 73 primitív gyök modulo 49, vagyis $73^{2a} + 73^a + 1 \equiv 0 \pmod{49} \Leftrightarrow 73^{3a} \equiv 1$, $73^a \not\equiv 1 \pmod{49}$ miatt $a \equiv 14, 28 \pmod{42}$ adódik. Azaz $3 \not| a$, $14|a$. Másrészt 73 primitív gyök modulo 43 is, így ilyenkor $43|73^{2a} + 73^a + 1$, viszont $43 \not| 7^l3$ triviálisan. $\surd$

Tétel 29 *Ha G (feloldható) $4-\mathrm{cp}$-csoport, akkor G $\{3,7\}$-csoport.*

Bizonyítás Legyen p egy olyan 3-tól és 7-től különböző prímszám, amelyre indirekt módon felteszem, hogy van olyan $4-\mathrm{cp}$-csoport, melynek p osztja a rendjét! Legyen G_0 minimális p-vel osztható rendű ilyen tulajdonságú csoport. Ekkor G_0-nak minimális normálosztója $N \cong Z_p^k$, $G = G_0/N$ hat N-en. A hatás Brauer-karaktere, φ invariáns a primitív $|G|$-edik egységgyök negyedik hatványra emelésére, vagyis a fenti állításokban használt jelöléssel $k = 4$. Másrészt G-re igazak a tétel feltételei, vagyis indukcióval feltehető, hogy G egy $\{3,7\}$-csoport. Most az **Állítás 19**-ben $r|3$ adódik, vagyis figyelembe véve **Állítás 20**-at is, $o_p(4)$ egy 3-hatvány, mivel $|G|$ páratlan.

Most **Állítás 23** bizonyításával megegyező módon feltehető, hogy $G \cong Z_{7^l} \rtimes Z_{3^k}$, ahol $o_p(4) = 3^k$. Ha $Z(G) = 1$ lenne, akkor G maga is Frobenius-csoport lenne, így az abszolút irreducibilis, hű karakterei λ^G alakúak lennének, ahol $\lambda \in \mathrm{Irr}(Z_{7^l})$. De ilyen esetben ${\lambda^G}_{Z_{3^k}}$ a reguláris reprezentáció karaktere, ami nem szerepelhet fixpontmentes hatásban. Így $|Z(G)| \geq 3$.

Ha $g \in Z(G)$, akkor $g = \mu \mathrm{id}_V$ valamilyen μ-re, de a Brauer-karakter invarianciája miatt $\mu = \mu^4$, vagyis $o(g)|3$. Tehát csak $|Z(G)| = 3$ lehetséges.

Legyen most $\mu = e^{\frac{2\pi i}{3}}$ az egyik primitív harmadik egységgyök, $t \in \mathbb{F}_p$ pedig egy ottani primitív harmadik egységgyök! Mivel minden $v \in V$-hez létezik $g \in G$, hogy $vg = 4g$, így létezik $h \in G$, hogy $vh = tv$. Itt a fixpontmentesség miatt csak $o(h)=3$ lehet. Ekkor G-ben a két harmadrendű elem: h, h^2, $\varphi(h)=\mu\varphi(1)$, $\varphi(h^2)=\mu^2\varphi(1)$. Ha $\psi\in$IBr(G) egy irreducibilis komponense φ-nek, akkor $\psi_{Z_{3^k}}$ a hű irreducibilis Z_{3^k}-karakterek azon felét tartalmazza, amelyekre $\xi(h)=\mu$. (Itt megint használtam, hogy ez a ψ is λ^G alakú.)

G-ben a 3^k-adrendű elemek száma $2\frac{p^d-1}{p^e-1}$, ahol $d=\dim_{\mathbb{F}_p}(V)$, és $e=3^{1-k}d$, hiszen minden $0\neq v\in V$-re pontosan egy $g\in G$ $o(g)=3^k$ van, amellyel $vg=4v$, és ezzel a tulajdonsággal a 3^k-adrendűek fele rendelkezik. (Attól függően, hogy h-nak, vagy h^2-nek az egyik 3^{k-1}-edik gyöke az illető.)

Másrészt, ugyanígy a 9-edrendű elemek száma $2\frac{p^d-1}{p^{d/3}-1}$, vagyis a 9-edrendű részcsoportok száma $\frac{1}{3}\frac{p^d-1}{p^{d/3}-1}$. Ezek szerint a 3^k-adrendű elemek száma $3^{k-2}2\frac{p^d-1}{p^{d/3}-1}$. Ezt az előzővel összevetve:

$$3^{k-2}(p^e-1)=p^{d/3}-1.$$

Itt $3^k\leq p-1$, vagyis $e|\frac{d}{3}$, s ebből csak a $3e=d$ eset lehet. Ekkor viszont $o_p(4)=9$, $p|4^9-1=27\cdot 7\cdot 19\cdot 73$. Másrészt a kilencedrendű elemek száma 7^l6, hiszen egy kilencedrendű elem nem konjugált egyetlen hatványával sem G-ben $7\not|6=\varphi(9)$ miatt. Így aztán $p^{\frac{2d}{3}}+p^{\frac{d}{3}}+1=7^l3$ adódik, ami a Lemma miatt megoldhatatlan a $p=19,73$ esetekben. Ezzel a Tételt beláttam. $\surd\!\!/$

Itt a minimális nem 3-csoport rendje 21, a hetedrendű normálosztón a komplementum generátora négyzetre-emelésként hat.

Most azt szeretném belátni, hogy minden feloldható és racionális csoport egy $\{2,3,5,7\}$-csoport. Elsőnek egy korábbi állítás specializálása jön.

Állítás 30 ([9]) *Legyen G egy p'-csoport, amely hat egy p-karakterisztikájú véges $\mathbb{F}_q$ test feletti V vektortéren, $\langle\lambda\rangle=\mathbb{F}_q^*$. G teljesíti a λ-sajátértékfeltételt, és megőriz egy nemelfajuló antiszimmetrikus bilineáris formát. Ekkor $q=2,3,5,7,11$ lehet csak. Sőt, ha $q=11$, akkor $SL(2,5)$ benne van G-ben.*

Bizonyítás A korábbiaknak megfelelően feltehető, hogy G hatása fixpontmentes. Egyelőre azt is felteszem, hogy G feloldható.

Ezután látható, hogy ha $2 \neq r | q-1$, akkor $r = 3$, és $q = 7$, vagy $q = 4$. A 4 eset nem fordulhat elő, hiszen $|G|$ páros, mivel például $O_2(G)$ kvaterniócsoport.

Ha $q-1$ 2-hatvány, akkor az általánosított kvaternió esetben, és a ciklikus esetben is $q-1|4$ jön ki, vagyis összefoglalva: Ha G feloldható, akkor $q = 2, 3, 5, 7$ lehet.

Ha G nem feloldható, akkor a Frobenius-komplementumok struktúratételéből jön, hogy G-ben van egy G_1 legfeljebb 2-indexű részcsoport, amelyre $G_1 \cong SL(2,5) \times K$, ahol K egy $\{2,3,5\}'$-csoport. Innen látható, hogy G 2-Sylowjának az exponense legfeljebb 8. A korábbi gondolatmeneteket K-ra alkalmazva látható az is, hogy $q - 1 = 2^a 3^b 5^c$ alakú, ahol $a \leq 3$. De $|SL(2,5)| = 120$ miatt $b, c \leq 1$ adódik. q ráadásul $2, 3, 5$-tel nem osztható, vagyis $q-1 = 2 \cdot 3$, $4 \cdot 3$, $2 \cdot 5, 8 \cdot 5$, $2 \cdot 3 \cdot 5$, $4 \cdot 3 \cdot 5$, $8 \cdot 3 \cdot 5$ lehet. De $SL(2,5)$-ben nincs 15-ödrendű elem, ami az utolsó három lehetőséget kizárja. $SL(2,5)$-ben 20-adrendű elem sincs, így $q - 1 = 8 \cdot 5$ sem lehet. Maradnak a $q = 7, 11, 13$ lehetőségek. Ki kell még zárni $q = 13$-at.

$SL(2,5)$ karaktertáblája (a reprezentánsok rendjeivel indexelve a konjugáltosztályokat):

	1	2	4	6	3	5_1	5_2	10_1	10_2
1_G	1	1	1	1	1	1	1	1	1
ζ_2	2	-2	0	1	-1	$\frac{-1-\sqrt{5}}{2}$	$\frac{-1+\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
ζ_3	2	-2	0	1	-1	$\frac{-1+\sqrt{5}}{2}$	$\frac{-1-\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
ζ_4	3	3	-1	0	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
ζ_5	3	3	-1	0	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
ζ_6	4	4	0	1	1	-1	-1	-1	-1
ζ_7	4	-4	0	-1	1	-1	-1	1	1
ζ_8	5	5	1	-1	-1	0	0	0	0
ζ_9	6	-6	0	0	0	1	1	-1	-1

$\mathbb{F}_{13}$ algebrai lezártja felett pontosan ugyanezek az irreducibilis Brauer-karakterek, hiszen $(13, 120) = 1$. $\mathbb{F}_{13}$ felett ekkor két fúzió történik: ζ_2, ζ_3-é, és ζ_4, ζ_5-é. (Ugyanis a Frobenius-automorfizmus $\mathbb{C}$ feletti megfelelőjét σ-val jelölve $\zeta_2^\sigma = \zeta_3$, $\zeta_3^\sigma = \zeta_2$, $\zeta_4^\sigma = \zeta_5$, $\zeta_5^\sigma = \zeta_4$.) A kapott hét irreducibilis reprezentáció között csak egyetlen fixpontmentes van, a 4 dimenziós $\zeta_2 + \zeta_3$. Összeszámolva egy ilyen 4-dimenziós irreducibilis alteren vett hatás szerint $SL(2,5)$ harmadrendű elemeit a stabilizátoros eljárással, kapjuk, hogy

$\frac{13^4-1}{13^2-1} = 170$ van belőlük. Ez több, mint ahány eleme van $SL(2,5)$-nek, ami mutatja, hogy $q = 13$ valóban nem fordulhat elő. $\surd$

A fenti esetekben tényleg lehet megfelelő csoportokat, és hatásokat találni. A $q = 2$ eset triviális, $q = 3, 5$ esetén $SL(2,q)$ 2-Sylowja megfelelően hat $\mathbb{F}_q^2$-en. $q = 7$ esetén $SL(2,3)$ ágyazható be $SL(2,7)$-be. $q = 11$ esetén pedig $SL(2,5)$ $SL(2,11)$-be.

Tétel 31 ([9]) *G feloldható racionális csoport. Ekkor G $\{2,3,5,7\}$-csoport.*

Bizonyítás Indukciót kombinálva az előző állítással azonnal kapjuk ezt az eredményt. $\surd\!\surd$

Ehhez hasonló, de lényegesen kevesebb eszközzel bizonyította Markel[14] azt a tényt, hogy szuperfeloldható racionális csoport $\{2,3\}$-csoport. (Ugyanis a minimális normálosztó prímrendű.)

A fejezetet egy érdekes eredménnyel zárom, amihez kell egy lemma.

Lemma 32 ([8]) *Legyen $N \lhd G$! Ha G-ben $o(g_1) = o(g_2) \Rightarrow g_1 \sim g_2$, akkor G/N-ben is $o(g_1) = o(g_2) \Rightarrow g_1 \sim g_2$.*

Bizonyítás Legyen $\overline{G} = G/N$, és $\overline{x}, \overline{y} \in \overline{G}$ két azonosrendű elem! Mindkét mellékosztályból választok egy minimális rendű elemet: x, y. Ha azonos rendűek, akkor konjugáltak, s így $\overline{x}$ és $\overline{y}$ is. Ha nem, akkor van egy p prím, hogy $o(x) = p^a m$, $o(y) = p^b n$, $p \nmid mn$, és $a \neq b$, mondjuk $a < b$. Jelölje $x_1 = x^{mn}$-t, és $y_1 = y^{mn}$-t! Nyilván $\overline{x_1}$ és $\overline{y_1}$ azonos rendűek $\overline{G}$-ben. De x_1, és $y_1^{p^{b-a}}$ azonos rendű, így konjugált, ami mutatja, hogy $\overline{x_1}$ és $\overline{y_1}^{p^{b-a}}$ is. De ez nem lehetséges, hiszen különböző rendűek. $\surd$

Tétel 33 ([8]) *Ha G feloldható, G-ben $o(g_1) = o(g_2) \Rightarrow g_1 \sim g_2$, akkor $G \cong S_n$, $n = 1, 2, 3$.*

Bizonyítás Indukciót alkalmazok $|G|$-re. Legyen $N \lhd G$ minimális! Ekkor G/N egy-, vagy kételemű, esetleg S_3. Mivel N elemi Abel p-csoport, így $|G/N| = 1$ esetén $|G| = 1$, vagy $|G| = 2$. Ha $|G/N| = 2$, akkor $|N| \leq 3$, hiszen $N \setminus \{1\}$-en tranzitívan hat G/N. De $|N| = 2$ nem lehet, hiszen G nem lehet negyedrendű. $|N| = 3$ pedig $G \cong S_3$-at adja.

Ha $G/K \cong S_3$, akkor $|N| - 1|6$. $|N| = 7$, nem lehet, hiszen G/N nem ciklikus. Ha $|N| = 4$, akkor G 3-Sylowja hűen hat rajta, vagyis $G \cong S_4 =$ a 3-Sylow mellékosztályain vett tranzitív permutáció-reprezentáció. De S_4-ben két involúció-osztály van.

Ha $|N| = 3$, akkor G 3-Sylowja 9-edrendű normálosztó, de Abel, és a faktor csak kettesével tudja egyesíteni az elemeket konjugáltosztályokká.

Ha $|N| = 2$, akkor G 3-Sylowja triviálisan hat N-en, vagyis normálosztó. De a szerinte vett faktor negyedrendű, ami ellentmond a Lemmának. Több eset nincs. $\surd\!\!/$

5 Egyéb eredmények

Elsőként azt kell megemlíteni, hogy Gow [9] többet bizonyított, mint ami a **Tétel 31**-ben szerepel:

Tétel 34 *Ha G feloldható racionális csoport, akkor G egy $\{2, 3, 5\}$-csoport.*

A 7-nek, mint lehetséges prímosztónak a kiküszöbölése még némi fáradtságot igényelne. A használt eszközök hasonlóak, de kicsit mélyebbek.

Szintén hasonló eszközökkel bizonyítható Soares[6] alábbi eredménye:

Tétel 35 *Minden $\varepsilon > 0$-hoz van egy olyan $A = A(\varepsilon)$ konstans, hogy ha G p-feloldható, $p| \, |G|$, G összes karakterértéke egy K testben van, melyre $|K : \mathbb{Q}| \leq n$, akkor $p \leq An^{1+\varepsilon} + 1$.*

Itt $\varepsilon = 1$ esetén $A = 4,\ 16,\ 480$ írható attól függően, hogy G szuperfeloldható, feloldható, vagy p-feloldható.

Példával megmutatható, hogy $\varepsilon = 0$ nem lehet még a szuperfeloldható esetben sem.

A nemfeloldható (nem p-feloldható) esetben Feit és Seitz[7] mutatta meg az alábbit. (A bizonyítás erősen támaszkodik a véges egyszerű csoportok klasszifikációjára!)

Tétel 36 *Van olyan $\mathcal{F}_n$ egyszerű csoportok véges halmaza, hogy ha G összes karakterértéke egy K testben van, melyre $|K : \mathbb{Q}| \leq n$, akkor G nemciklikus kompozíciófaktorai vagy alternáló csoportok, vagy $\mathcal{F}_n$-beliek.*

Speciálisan $\mathcal{F}_1 = \{PSp_4(3),\ Sp_6(2),\ O_8^+(2)',\ PSL_3(4),\ PSU_4(3)\}$.

$\mathcal{F}_1$-ben a második és a harmadik csoport már önmagában is racionális. Velük együtt az első is kompozíciófaktora egy Weyl-csoportnak. A negyedik és ötödik esetben is egy-egy automorfizmus-csoportbeli részcsoport racionális. Az S_n-beli konjugáltoszályok A_n-beli szétesése is ismert, és azonnal látszik belőle, hogy A_2 kivételével nincs racionális alternáló csoport.

A fenti tétel segítségével tovább erősíthető **Tétel 33**, amely Fitzpatrick[8] eredménye:

Tétel 37 *Ha G-ben $o(g_1) = o(g_2) \Rightarrow g_1 \sim g_2$, akkor $G \cong S_n$, $n = 1, 2, 3$.*

Bizonyítás[7] Legyen $N \triangleleft G$ minimális normálosztó! Ha N feloldható, akkor már **Tétel 33** elintézte a dolgot. Ha nem, akkor $N \cong T_1 \times \cdots \times T_k$ izomorf nemkommutatív egyszerűek direkt szorzata. De egy $a \in T_1$, és $(a, \ldots, a) \in N$ nemkonjugáltak, bár azonos rendűek. Vagyis $N = T_1$ egyszerű.

Ha $G = N$, akkor G egyszerű racionális csoport, vagyis $Sp_6(2)$, vagy $O_8^+(2)'$. De mindkettőben több konjugáltosztálynyi másodrendű elem van. Vagyis feltehető, hogy $G > N$. Ha $C_G(N) > 1$, akkor $NC_G(N) = N \times Z$, $Z \triangleleft G$, s G/Z nem feloldható, ami indukciót alkalmazva ellentmond annak, hogy a tulajdonság faktorizálásnál öröklődik. Vagyis $C_G(N) = 1$, $G \leq \mathrm{Aut}(N)$.

Ha $N \cong A_n$, akkor $\mathrm{Aut}(N) = S_n$, vagy $n = 6$, de minden szimmetrikus esetben G-nek több, mint egy involúció-osztálya van. Az $n = 6$ esetben is csak úgy lehet egy involúció-osztály, hogy cserébe 8-adrendű elemek alkotnak két osztályt.

$Sp_6(2)$ automorfizmuscsoportja önmaga, a többi esetben egy automorfizmus-részcsoportnak mindig van nembelső másodrendű eleme. $\surd\!\!/$

Ez az eredmény nem igaz végtelen csoportokra. Példa erre egy P. Hall[10] által konstruált végtelen torziócsoport.

Visszatérve a racionális csoportokoz, azt sejtik, hogy a nemfeloldható esetben sem lehet többféle ciklikus kompozíciófaktor, mint a feloldható esetben. Gow szerint Thompson megmutatta, hogy racionális csoport ciklikus kompozíciófaktora csak Z_2, Z_3, Z_5, Z_7, Z_{11} lehet, de valószínűnek látszik, hogy az utolsó kettő valójában nem fordul elő.

6 Weyl-csoportok

A szakdolgozat során többször megemlítettem azt a közismert tényt, hogy minden Weyl-csoport racionális. (Lásd például [3]-ban a reprezentációk racionalitását is.) Ennek a bizonyítása nem nehéz, ugyanis az irreducibilis gyökrendszerek Weyl-csoportjaira ellenőrizhető, a többi pedig direkt szorzata az előbbieknek. Egy kicsit bővebben:

Tétel 38 *Ha W egy A_n, B_n vagy D_n típusú gyökrendszer Weyl-csoportja, akkor W racionális.*

Bizonyítás Azt mutatom meg, hogy ezekben az esetekben minden elem minden, a rendjéhez relatív prím kitevőjű hatványával konjugált.

A_n Weyl-csoportja S_{n+1}. Legyen σ egy eleme, $(k, o(\sigma)) = 1$! Ha több orbitja is van, akkor indukcióval a ciklusokat külön-külön tudom k-adikra konjugálni, így σ-t is. Ha csak egy orbitja van, akkor alkalmas átszámozással feltehető, hogy $\sigma = (1\,2\,\cdots n)$. De ekkor $\tau = i \mapsto ik + t$ minden t esetén jó permutáció arra, hogy $\sigma^k = \sigma^\tau$ legyen. (Persze $ik+t$ csak modulo n számít.)

B_n (és C_n) Weyl-csoportja $G = Z_2 \wr S_n$. Legyen $g = (\sigma, (a_1, a_2, \ldots, a_n))$ egy eleme, $(k, o(g)) = 1$! Ha σ-nak több orbitja is van, akkor indukcióval g-nek a megfelelő részeit külön-külön tudom k-adikra hatványozni, így g-t is. Ha csak egy orbitja van, akkor átszámozással feltehető, hogy $\sigma = (1\,2\,\cdots n)$.

Ha $h = (1, (b_1, b_2, \ldots, b_n))$, akkor $g^h = (\sigma, (a_1 + b_1 + b_{1^{\sigma^{-1}}}, \ldots, a_n + b_n + b_{n^{\sigma^{-1}}})) = (\sigma, (a_1 + b_1 + b_n, \ldots, a_n + b_n + b_{n-1}))$. Így alkalmas h-val konjugálva feltehető, hogy $a_2 = a_3 = \cdots = a_n = 0$. a_1 pedig 0, vagy 1. Ha 0, akkor g és ezért g^k is benne van a komplementumban, vagyis S_n-ben, amit már néztem.

Ha $a_1 = 1$, akkor $g^n = (1, (1, 1, \ldots, 1))$, $g^{2n} = (1, (0, 0, \ldots, 0))$, s g rendje $2n$. Ha $k < n$, akkor $g^k = (\sigma^k, (1, 1, \ldots, 1, 0, 0, \ldots, 0))$, ahol k darab egyes van a vektorban, ha pedig $k > n$, akkor $g^k = (\sigma^k, (0, 0, \ldots, 0, 1, 1, \ldots, 1))$, ahol $k - n$ darab nullás van a vektorban. Ha τ olyan, hogy $\sigma^k = \sigma^\tau$, akkor legyen $h = (\tau, (b_1, \ldots, b_n)) = (\tau, (0, \ldots, 0)) \cdot (1, (b_1, \ldots, b_n))$! Ekkor $g^h = (\sigma^k, (0, \ldots, 0, 1, 0, \ldots, 0))^{(1,(b_1,\ldots,b_n))}$, ahol az egyes az 1^τ-adik pozícióban van.

Most a korábbi módszerrel meg tudjuk választani jól a b_i-ket, hisz σ^k is tranzitív, és k páratlan. (Sőt pontosan két jó vektor lesz, melyek összege $(1, \ldots, 1)$.)

D_n Weyl-csoportja egy H 2-indexű részcsoportja a fenti G-nek. Azokból az elemekből áll, amelyek páros sok egyest tartalmaznak a vektorrészükben. Legyen $g = (\sigma, (a_1, a_2, \ldots, a_n))$ egy eleme, $(k, o(g)) = 1$! Tudjuk, hogy ez G-ben konjugált g^k-hoz. H-ban is konjugáltak, ha például nem esik szét a konjugáltosztálya. De nem esik szét, ha centralizálja $G \setminus H$-beli. Ha σ-nak van páratlan hosszúságú orbitja, akkor azokon a pozíciókon eggyel, a többin nullával egyenlő vektor centralizálja, és nincs H-ban. Így elég megmutatni az állítást olyan g-kre, melyek permutációrésze nem tartalmaz páratlan ciklust. Egy ilyenről már azt sem kell feltenni, hogy nincs H-ban.

Ha σ-nak több orbitja is van, akkor indukcióval g-nek a megfelelő részeit külön-külön tudom k-adikra hatványozni, hiszen ezek párosak, így g-t is. Ha csak egy orbitja van, akkor átszámozással feltehető, hogy $\sigma = (1\,2\,\cdots n)$. A $h = (1, (b_1, b_2, \dots, b_n))$, vektort jól megválasztva, majd vele konjugálva most is feltehető, hogy $a_2 = a_3 = \cdots = a_{n-1} = 0$, és a_1, a_n közül is legalább az egyik 0. Ha mindkettő 0, akkor g benne van a komplementumban, amit már néztem.

G esetén minden jó τ-hoz volt (két) jó $(b_1, \dots, b_n)$ vektor is. Ez most csak akkor lesz jó, ha benne páros sok az egyes. Mivel n páros, így a két jó vektorban ugyanakkor lesz páros sok egyes. Azt állítom, hogy τ-t (vagyis tulajdonképpen az egyes pozícióját) alkalmasan választva a jó vektorban páros sok lesz az egyes.

Ha most rögzítettnek veszem τ-t, és felteszem, hogy $b_1 = 0$, akkor a többi b_i-t egyértelműen kapom, ugyanis $b_{1^{\sigma^k}}$-t úgy kell választanom, hogy $a_{1^{\sigma^k}} + b_{1^{\sigma^k}} + b_1$ a megfelelő értéket vegye fel. Hasonlóan meg van már kötve a kezem $b_{1^{\sigma^{2k}}}$-nál, és így tovább. Ez a "meg van kötve a kezem" azt jelenti, hogy egyértelműen jönnek az egyes-sorozatok, és a nulla-sorozatok. (Itt a sorozat persze nem az $1, 2, \dots, n$ mentén, hanem az $1, k+1, \dots, (n-1)k+1$ mentén futót jelent!) Ha az 1^τ egy egyes-sorozattal érintkezik, akkor benne eggyel elmozgatva, és azt az egyest kivéve a sorozatból a kapott vektor nem változik, de a konjugáló vektorban az egyesek számának a paritása igen. Hasonlóan, ha nulla-sorozatban van, akkor eggyel elmozgatva, és oda egy egyest berakva a kapott vektor nem változik, de a konjugálóban az egyesek számának paritása igen. Ez mutatja, hogy feltehető a konjugáló vektor H-beli volta. $\surd\!/$

A maradék csoportok: E_6, E_7, E_8, F_4 Weyl-csoportjai megtalálhatóak az irodalomban, még komplett karaktertáblákkal is. (Az első három megtalálható az ATLAS[4]-ban is, az utolsó pedig Carter könyvében[3].) G_2 esete pedig triviális, ugyanis ekkor $W \cong D_6$.

Ez a bizonyítás azonban geometriailag egyáltalán nem mutatja meg, hogy miért igaz ez az állítás. A fejezet további része arra fog szolgálni, hogy valami ebből is kiderüljön. Sajnos még ez a bizonyítás is tartalmaz olyan pontokat, amelyekben szükség van a gyökrendszerek klasszifikációjára. Tudtommal jelenleg nem ismert olyan bizonyítás, amely ne támaszkodna rá.

Az alábbi gondolatmenet Springertől[16] származik. A (későbbiekben "ismert"-ként említett) felhasznált előismeretek megtalálhatóak Bourbaki[1], illetve Humphreys[11] könyveiben. További (illetve korábbi) eredmények szerepelnek még Carternál:[2],[3].

A továbbiakban G mindig egy n dimenziós (komplex) V vektortéren ható véges tükrözés-csoportot (reflection-group) jelöl. S a koordináta-leképezések polinomjainak $\mathbb{C}$-algebrája. G hat ezeken a szokásos módon: $(g \cdot p)(v) = p(vg)$ minden $v \in V$-re. R jelöli az S-beli G-invariáns elemeket, ez is egy $\mathbb{C}$-algebra. Az alábbi lemma általánosabban, minden $G \subseteq GL(n, \mathbb{C})$ véges csoportra igaz:

Lemma 39 *$v, w \in V$-re ekvivalensek:*

(i) létezik $g \in G$, hogy $vg = w$;

(ii) minden $f \in R$-re $f(v) = f(w)$.

Bizonyítás Az $(i) \Rightarrow (ii)$ irány triviális, a másikat bizonyítom. Legyen $P = \{f \in S | f(v) = 0\}$, $Q = \{f \in S | f(w) = 0\}$! Ezek maximális ideáljai S-nek, és $P \cap R = Q \cap R$ a feltétel szerint. Belátom, hogy létezik $g \in G$, amellyel $g \cdot P \subseteq Q$, a ezzel vége is lesz a bizonyításnak, mivel $g \cdot P = \{f \in S | f(vg) = 0\}$ is maximális ideál, vagyis $g \cdot P = Q$, de így $w = vg$.

Mivel minden $f \in P$-re

$$\prod_{g \in G} (g \cdot f) \in P \cap R \subseteq Q,$$

és Q prímideál, tehát van egy $g \in G$, amelyre $g \cdot f \in Q$. Legyen $P = (f_1, f_2, \ldots, f_r)$ egy véges generátorrendszere a P ideálnak! (Ilyen létezik Hilbert bázistétele miatt.) Ekkor minden $c \in \mathbb{C}$-hez létezik $g_c \in G$, hogy $g_c \cdot (f_1 + cf_2 + \cdots + c^{r-1} f_r) \in Q$. Mivel G véges, $\mathbb{C}$ végtelen, így valamilyen $g \in G$ legalább r-szer előfordul ilyen g_c-ként. Ezzel a g-vel és a megfelelő $c_1, c_2, \ldots, c_r$-rel

$$g \cdot (f_1 + c_i f_2 + \cdots + c_i^{r-1} f_r) = \sum_{j=1}^{r} c_i^{j-1} (g \cdot f_j) \in Q \quad (i = 1, \ldots, r).$$

Vagyis minden j-re $g \cdot f_j$ előáll Q-beliek lineáris kombinációjaként, így $g \cdot f_j \in Q$. Ha $f = p_1 f_1 + \cdots + p_r f_r \in P$ tetszőleges, akkor $g \cdot f = (g \cdot p_1)(g \cdot f_1) + \cdots + (g \cdot p_r)(g \cdot f_r) \in Q$ mutatja, hogy $g \cdot P \subseteq Q$. $\surd$

V-re sokszor, mint affin algebrai halmazra lesz érdemes nézni. Ekkor a lemma azt fejezi ki, hogy V G-orbitjai affin algebrai varietásként viselkednek, a hozzájuk tartozó algebra R. Szintén G végességéből következik a most sorra kerülő, alapvető lemma.

Lemma 40 *R-et, mint $\mathbb{C}$-algebrát n darab algebrailag független homogén polinom generálja. E polinomok fokainak halmaza független a polinomok választásától, a fokok szorzata $|G|$.*

Mostantól fogva rögzítek egy $\{f_1, \dots, f_n\}$ homogén invariánsokból álló rendszert, amelyek algebrailag függetlenek, s generálják a G-invariáns koordinátafüggvények $\mathbb{C}$-algebráját, $d_i = \deg f_i$. $J(v)$ jelöli az f_i-k Jacobi-determinánsát a $v \in V$ pontban. (Ez konstans szorzó erejéig független az f_i-ktől, és pontosan akkor nulla, ha v benne van egy tükörhipersíkban.) H_i jelöli az f_i által definiált algebrai hiperfelületet V-ben: $H_i = \{v \in V | f_i(v) = 0\}$. Ha ξ egy egységgyök, akkor $V(g, \xi)$ jelöli a g csoportelem ξ-hez tartozó sajátalterét. Ez *maximális*, ha nincs nála bővebb $V(h, \xi)$, ugyanazzal a ξ-vel!

Állítás 41 *Ha ξ egy primitív d-edik egységgyök $\mathbb{C}$-ben, akkor $\cup_{g \in G} V(g, \xi) = \cap_{d \not| d_i} H_i$. Sőt, ezen algebrai halmaz irreducibilis komponensei a maximális $V(g, \xi)$-k.*

Bizonyítás Alkalmazzuk **Lemma 39**-et! Adott $v \in V$-hez pontosan akkor létezik g, mellyel $vg = \xi v$, ha $f(v) = 0$ minden d-vel nem osztható fokú $f \in R$-re. De ehhez elegendö $f_i(v) = 0$-t megkövetelni olyan i-kre, ahol d nem osztja d_i-t. Ez mutatja az első részt.

Ebből az is látszik, hogy $\cap_{d \not| d_i} H_i$ a maximális $V(g, \xi)$-k uniója. S a második rész következik abból, hogy $V(g, \xi)$ irreducibilis varietás. $\surd$

Egy következmény, ami Weyl-csoportra jól ismert:

Állítás 42 *Ha még azt is feltesszük, hogy G irreducibilisan hat, és e jelöli a fokok legnagyobb közös osztóját, akkor G centruma e-edrendű ciklikus csoport.*

Bizonyítás A Schur-lemma miatt a centrum skalárral való szorzásokból áll. Ha a ξ-vel való szorzás ilyen, akkor az előző állításban $\cap_{d \not| d_i} H_i = V$, vagyis ξ rendje oszt minden fokot. Fordítva, ha ξ rendje oszt minden fokot, akkor a második rész szerint valamely $g \in G$-re $V(g, \xi) = V$. $\surd$

Definíció 43 *Ha $d \neq 0$ tetszőleges egész, akkor a d-vel osztható fokok számát $a(d)$ jelöli.*

A most következő állítás döntő a továbbiak szempontjából.

Állítás 44 *Egy G (véges) tükrözés-csoportra az alábbiak teljesülek:*

(i) $\max_{g\in G} \dim V(g,\xi) = a(d)$, *ha ξ egy d-edik primitív egységgyök. Speciálisan pontosan akkor van olyan $g \in G$, melynek ξ sajátértéke, ha d osztja legalább az egyik fokot.*

(ii) Minden g-hez és ξ-hez létezik h, hogy $\dim V(h,\xi) = a(d)$, *és $V(g,\xi) \subseteq V(h,\xi)$.*

(iii) Ha $\dim V(g_1,\xi) = \dim V(g_2,\xi) = a(d)$, *akkor van olyan h, mellyel $V(g_1,\xi)h = V(g_2,\xi)$, vagyis G tranzitívan hat $\cap_{d \not| d_i} H_i$ irreducibilis komponensein.*

Bizonyítás Azt tudjuk, hogy $\cap_{i=1}^n H_i = \{0\}$. Ezért tetszőleges irreducibilis komponenseiket (C_i) kiválasztva $\cap_{i=1}^n C_i = \{0\}$. Ez azt jelenti, hogy a C_i-k valódi módon metszik egymást, s tetszőleges $X \subseteq \{1,2,\dots,n\}$ részhalmazra $\cap_{i\in X} C_i$ dimenziója $= n - |X|$. Vagyis a metszet minden irreducibilis komponensének is ennyi a dimenziója, aminek **Állítás 41** miatt speciális esete (i). (ii) most már szintén azonnal következik **Állítás 41**-ből.

Legyen tehát $a = a(d) = \dim V(g_1,\xi)$! Átszámozom az f_i-ket úgy, hogy az első a darab foka legyen d-vel osztható. Mindegyiket megszoríthatom $V(g_1,\xi)$-re. Azt állítom, hogy ezek a megszorítások algebrailag függetlenek.

φ jelöli a következő morfizmust a $V(g_1,\xi)$ és a $\mathbb{C}^a$ varietások között:

$$\varphi(v) = (f_1(v), \dots, f_a(v)).$$

Mivel $H_j \supseteq V(g_1,\xi)$, ha $j > a$, és $\cap_{i=1}^n H_i = \{0\}$, így a $\varphi^{-1}((0,\dots,0))$ fibrum csak a $\{0\}$-ból áll. De az egy közismert algebrai geometriai tény, hogy ezen fibrum dimenziója legalább $a - \dim \varphi(V(g_1,\xi))$, vagyis $a = \dim \varphi(V(g_1,\xi))$. De ez csak úgy lehet, ha az f_i-k megszorításai valóban algebrailag függetlenek.

$U_1 \subseteq V(g_1,\xi)$ jelöli azokat a vektorokat, amelyek egyetlenegy másik maximális $V(h,\xi)$-ben sincsenek benne. Világos, hogy U_1 nyílt halmaz a Zariski-topológiában. φ_2 és U_2 ugyanezeket jelentik $V(g_2,\xi)$ esetén.

$\varphi(U_1)$ és $\varphi_2(U_2)$ is nyílt, nemüres részhalmazai $\mathbb{C}^a$-nak, így nemüres, nyílt a metszetük. $\varphi(v_1) = \varphi_2(v_2)$ azt jelenti, hogy $f_i(v_1) = f_i(v_2)$ minden i-re. ($i > a$ esetén ugyanis mindkettő 0.) De **Lemma 39** miatt ekkor van $h \in G$, mellyel $v_1 h = v_2$. Most $v_2 \in V(g_1, \xi)h = V(hg_1h^{-1}, \xi)$, s ezért $V(g_1, \xi)h = V(g_2, \xi)$. $\surd$

Definíció 45 *Egy v vektort regulárisnak hívunk, ha nincs benne egyik tükörhipersíkban sem, azaz nem merőleges egyik gyökre sem. Egy g elemét a tükrözés-csoportnak regulárisnak mondjuk, ha van reguláris sajátvektora.*

Az alábbi állítás ismert.

Állítás 46 *Ha v egy vektor, G_v a G-beli stabilizátora, akkor*

(i) v pontosan akkor reguláris, ha $G_v = 1$;

(ii) G_v-t generálják a benne lévő tükrözések.

Állítás 47 *Ha ξ egy primitív d-edik egységgyök, g egy olyan eleme a Weyl-csoportnak, hogy $V(g, \xi)$ tartalmaz reguláris vektort, v-t, akkor*

(i) $o(g) = d$;

(ii) $\dim V(g, \xi) = a(d)$;

(iii) G (ii) tulajdonságú elemei egy konjugáltosztályt alkotnak;

(iv) g sajátértékei ξ^{1-d_i}-k.

Bizonyítás Most g^d fixálja v-t, így $g^d = 1$, másrészt kisebb kitevővel ez még nem lehet igaz. Ez mutatja (i)-t.

A korábbi **Állítás 44** szerint van olyan $h \in G$, hogy $\dim V(h, \xi) = a(d)$, és $V(g, \xi) \subseteq V(h, \xi)$, vagyis $vh^{-1}g = v$, ami mutatja, hogy $h = g$, és (ii) is megvan. Hasonló gondolatmenettel jön **Állítás 44**-ből (iii).

Az utolsó rész bizonyítása hasonló a Coxeter-elemek esetén ismerthez: V-nek legyen egy g-sajátvektorokból álló bázisa $\{v = v_1, v_2, \ldots, v_n\}$, a sajátértékek $\{\xi, \xi^{m_2}, \ldots, \xi^{m_n}\}$! Mivel v_1 nincs benne egyetlen tükörhipersíkban sem, így $J(v_1) \neq 0$. Vagyis a Jacobi-determináns kifejtése során legalább egy nemnulla tag lép fel. Alkalmas átindexelés után feltehető, hogy $\frac{\partial f_i}{\partial x_i}$ nemnulla v_1-en, $(i = 1, 2, \ldots, n)$. Ez azt jelenti, hogy ($a_i \neq 0$-val)

$$\frac{\partial f_i}{\partial x_i} = a_i x_1^{d_i - 1} + \text{ többbi koordináta-függvényt tartalmazó tagok.}$$

Vagyis deriválás előtt

$$f_i = a_i x_1^{d_i-1} x_i + \text{ maradék.}$$

Ha most mindkét oldalt g-vel szorozzuk, és f_i invarianciáját használjuk, akkor

$$f_i = a_i \xi^{1-d_i-m_i} x_1^{d_i-1} x_i + \ldots$$

mutatja, hogy $1 - d_i - m_i \equiv 0 \pmod d$, ami (iv)-t adja. $\surd$

Reguláris elemekre most már bebizonyítható a kívánt állítás:

Állítás 48 *Legyen g reguláris, d-edrendű eleme egy G Weyl-csoportnak! Ekkor minden d-hez relatív prím i egész számra $g \sim g^i$.*

Bizonyítás Mivel G Weyl-csoport, így egész mátrixokkal reprezentálhatóak az elemei, vagyis ha egy d-edik primitív egységgyök, ξ g-nek sajátértéke, akkor minden más d-edik primitív egységgyök is, és a multiplicitások megegyeznek. Azaz g^i-nek is sajátértéke ξ, ugyanazzal a multiplicitással.

Mivel g reguláris, van egy reguláris sajátvektora v, a sajátértéke ξ, és az állítás következik a korábbiakból. $\surd$

Az alábbiakban Q jelöli a gyökrendszer által kifeszített rácsot, P pedig a súlyok által kifeszítettet. (Vagyis ennek eleme egy v vektor, ha minden α gyökre: $\frac{2(v,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z}$). Ekkor P/Q egy (véges) Abel-csoport, rendjét jelölheti e.

Állítás 49 *Ha g eleme a G Weyl-csoportnak, akkor $P(g-1) \subseteq Q$. Továbbá, ha p egy prím, $v \in P$ és $v(g-1) \in pQ$, akkor g előáll olyan $t \in G$ tükrözések szorzataként, melyekre $v(t-1) \in pQ$.*

Bizonyítás Az állítás első része igaz tükrözésekre. Tetszőleges g-t előállíthatunk tükrözések szorzataként, amiből e tükrözések számára vonatkozó indukcióval $(g = g_1 t)$:

$$v(g-1) = v(g_1 - 1)t + v(t-1) \in Q.$$

A második rész belátásához használom a duális gyökrendszer affin Weyl-csoportját, amely izomorf G-nek és a Q-eltolásoknak a szemidirekt szorzatával.

Ha $v \in P$ és $v(g-1) \in pQ$, akkor legyen $w = \frac{1}{p}v$! Ekkor w-t fixálja egy h eleme az affin Weyl-csoportnak. (Hiszen wg és w különbsége Q-beli, vagyis h ráadásul g-eltolás.) De ekkor h előáll w-t fixáló tükrözések szorzataként. (Ez analóg az **Állítás 46**-hoz.) Egy általános ilyen tükrözés (α egy gyök, k egy egész):

$$t_{\alpha,k} : x \mapsto x - 2\frac{((\alpha, x) - k)}{(\alpha, \alpha)}\alpha.$$

Ezzel $wt_{\alpha,k} = w$ azt jelenti, hogy $v(t_\alpha - 1) \in pQ$. Abból, hogy h ilyenek szorzata már következik az állítás, ugyanis h-nak a szemidirekt szorzatbeli "komplementum"-része g. $\surd$

Állítás 50 *Ha g eleme a G Weyl-csoportnak, akkor* $\det(g-1)$ *egy e-vel osztható egész szám. Továbbá, ha* $\det(g-1) \neq \pm e$, *akkor G-nek egy valódi Weyl-részcsoportja is tartalmazza g-t. (A Weyl-részcsoport olyan részcsoport, amely egy rész-gyökrendszer Weyl-csoportja.)*

Bizonyítás Az állítás első része persze azonnal következik az előzőből. Ha $\det(g-1) \neq \pm e$, akkor lehet $\det(g-1) = 0$, vagyis g fixál egy nemnulla vektort, amikoris tudjuk, hogy benne van egy Weyl-részcsoportban. Hiszen a v-t fixáló csoportelemek ilyet alkotnak **Állítás 46** szerint.

Ha $\det(g-1)$ nem 0, akkor pedig van egy p prím, hogy $pe | \det(g-1)$. Így van egy $v \in P \setminus pP$ vektor, hogy $v(g-1) \in pQ$.

Jelölje R_1 azoknak az α gyököknek a halmazát, melyekre

$$2\frac{(v, \alpha)}{(\alpha, \alpha)} \equiv 0 \pmod{p}!$$

Egyszerű számolás mutatja, hogy R_1 is gyökrendszer, ráadásul valódi részrendszer, hiszen $v \notin pP$. Így a Weyl-csoportja (ami az előző állítás szerint G-nek reszcsoportja) is kisebb. $\surd$

Az alábbi redukciós tétel nagyon hasznos indukciós bizonyítások esetén. Az itt bebizonyított következményen kívül például azt is be lehet látni a segítségével, hogy egy Weyl-csoport minden eleme előáll legfeljebb két involúció szorzataként. (Ami egyébként minden véges tükrözés-csoportra is igaz.)

Tétel 51 *Legyen G egy irreducibilis gyökrendszer Weyl-csoportja, $g \in G$ tetszőleges! Ekkor az alábbiak közűl legalább egy igaz:*

(i) g G-nek egy Weyl-részcsoportjában is benne van;

(ii) g reguláris;

(iii) $-1 \in G$, és $-g$-re teljesül (i);

(iv) a gyökrendszer típusa D_n, és g-nek két orbitja van, mindkettő negatív.

A bizonyítás sajnos esetszétválasztásos, amelynek szükségességét az utolsó eset léte is indokolja. A bizonyítás helyett ezért csak leírom, hogy mit jelent az utolsó eset.

B_n gyökrendszere: $\pm e_i \pm e_j$, $(i \neq j)$, illetve $\pm e_i$. (Itt e_i-k a standard bázisvektorokat jelentik $\mathbb{R}^n$-ben.) Ha h eleme a Weyl-csoportnak, akkor $e_i^g = \varepsilon_i e_{i^\sigma}$ valamilyen $\varepsilon_i = \pm 1$ előjelekkel,és valamilyen σ permutációval. σ egy orbitját h orbitjának is hívjuk. Egy ilyen $\{i, i^\sigma, \ldots, i^{\sigma^{l-1}}\}$ h-orbitra azt mondjuk, hogy *pozitív*, ha

$$\prod_{j=0}^{l-1} \varepsilon_{i^{\sigma^j}} = +1.$$

Ellenkező esetben az orbit *negatív*.

Mivel D_n Weyl-csoportja részcsoportja B_n Weyl-csoportjának, így a definíció rá is érvényes.

Tulajdonképpen a fentihez hasonló volt a gondolatmenet **Tétel 38** bizonyításakor.

Tétel 52 *Egy G Weyl-csoport minden karakterértéke racionális.*

Bizonyítás Indukcióval bizonyítom, hogy minden eleme konjugált a hatványaival. $|G| = 2$ esetén triviális. Az indukció miatt feltehető, hogy G irreducibilis.

Legyen $g \in G$ tetszőleges! Ha rá az előző tételben az első két lehetőség egyike teljesül, akkor már tudjuk. Ha a harmadik áll fenn, akkor $o(g)$ páros, de indukcióval minden $o(g)$-hez relatív prím k-ra $g^k = -(-g)^k \sim -(-g) = g$, hiszen -1 centrális.

Az utolsó esetet már néztem korábban. $\surd\!\!/$

7 Megjegyzések

Az időrend

1973. F. M. Markel[14]: Minden szuperfeloldható racionális G csoport $\{2,3\}$-csoport. Őt főleg azok a csoportok érdekelték, amelyekben minden konjugáltosztály-méret csak egyszer fodul elő. Az ilyenek persze mind racionális csoportok.

1974. Roderick Gow[9]: Minden feloldható racionális csoport $\{2,3,5\}$-csoport. Ha a felbontási test $\mathbb{Q}$, akkor $\{2,3\}$-csoport.

1985. P. Fitzpatrick[8]: Ha G-ben minden ugyanannyiadrendű elem konjugált, akkor $G \cong S_1, S_2, S_3$ lehet csak.

1986. Elenia Farias e Soares[6]: Minden $\varepsilon > 0$-ra van $A = A(\varepsilon) > 0$, hogy minden G p-feloldható csoportra, ha karakterértékei K-ban vannak, ahol $|K : \mathbb{Q}| \leq n$, akkor $p \leq A(\varepsilon)n^{1+\varepsilon} + 1$.

1988. Walter Feit, Gary Seitz[7]: Tetszőleges véges csoportra a nemciklikus, nemalternáló kompozíciófaktorokra csak véges sok lehetőség van, ha G minden karakterértéke egy n-edfokú bővítésében van $\mathbb{Q}$-nak. Racionális csoportra ($n = 1$) ezek konkrét meghatározása.

John G. Thompson: Racionális csoportnak ciklikus kompozíciófaktora is csak $Z_2, Z_3, Z_5, Z_7, Z_{11}$ lehet.

Kérdések az alábbiak. Egy részükön már gondolkoztam, de attól még lehet, hogy triviális rájuk a válasz.

- Mit lehet mondani a beágyazásról? Igaz-e valami ilyen állítás: "Minden $\mathcal{H}_1 -$ cp-csoport beágyazható $\mathcal{H}_2 -$ cp-csoportba." (Gow megmutatta, hogy minden $\{2,3\}$-csoport beágyazható olyan $\{2,3\}$-csoportba, amelynek $\mathbb{Q}$ a felbontási teste.)

- Lehet-e javítani az **Állítás 6**-ot részcsoportra, illetve finomítható-e normálosztóra?

- Mit lehet mondani a nevezetes részcsoportokról? Az általam vizsgált esetekben például minden racionális csoport 2-Sylowja is racionális. (De általában az nem igaz, hogy ha minden elem konjugált az ötödik hatványával, akkor ez a 2-Sylowban is teljesül.) A többi Sylowról persze csak gyengébb következtetés kérhető számon.

- Persze a fő kérdés: Igaz-e, hogy n − cp-csoport rendjének prímosztói korlátosak? Részkérdések: Igaz-e feloldhatóakra? Igaz-e valósakra?
- Mi mondható egy 3−cp-csoport szerkezetéről? Az összes általam ismert esetben az 5-Sylow elemi Abel normálosztó.
- Általában mondható-e valami az n − cp-csoportok szerkezetéről, karaktereiről?
- Egyáltalán, van-e értelme a kérdésnek? Lehet-e, például más típusú kérdések megválaszolására használni?
- Mit lehet mondani végtelen csoportokról?

Irodalom

[1] N. Bourbaki. *Groupes et algèbres de Lie, IV.-VI.* Hermann, Paris, 1968.

[2] R. W. Carter. Conjugacy classes in the Weyl group. *Compositio Math.*, 25:1–59, 1972.

[3] R. W. Carter. *Finite groups of Lie type: Conjugacy classes and complex characters.* Wiley Interscience, London, 1985.

[4] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups.* Clarendon Press, Oxford, 1986.

[5] C. W. Curtis and I. Reiner. *Representation Theory of Finite Groups and Associative Algebras.* Interscience, New York, 1962.

[6] Elenia Farias e Soares. Big primes and character values for solvable groups. *J. Algebra*, 100:305–324, 1986.

[7] Walter Feit and Gary M. Seitz. On finite rational groups and related topics. *Illinois J. Math.*, 33:103–131, 1988.

[8] P. Fitzpatrick. Order conjugacy in finite groups. *Proc. Roy. Irish Acad.*, 85A:53–58, 1985.

[9] Roderick Gow. Groups whose characters are rational valued. *J. Algebra*, 40:280–299, 1976.

[10] Philip Hall. Some constructions for locally finite groups. *J. London Math. Soc.*, 34:305–319, 1959.

[11] James E. Humphreys. *Reflection Groups and Coxeter Groups*. Cambridge University Press, Cambridge, 1990.

[12] B. Huppert. *Endliche Gruppen I*. Springer-Verlag, New York, 1968.

[13] B. Huppert and N. Blackburn. *Finite Groups III*. Springer-Verlag, Berlin/Heidelberg/New-York, 1982.

[14] F. M. Markel. Groups with many conjugate elements. *J. Algebra*, 26:69–74, 1973.

[15] D. Quillen. The Adams Conjecture. *Topology*, 10:67–80, 1971.

[16] T. A. Springer. Regular elements of finite reflection groups. *Invent. Math.*, 25:159–198, 1974.