Frobenius-csoportok

Szakdolgozat

Guld Attila

III. éves matematika BSc hallgató

Témavezető:
Dr. Pelikán József, egyetemi adjunktus

Eötvös Loránd Tudományegyetem Természettudományi Kar
Algebra és Számelmélet Tanszék

Budapest, 2011.

Tartalomjegyzék

Bevezetés **4**

1. Csoportelméleti előkészületek **5**

1.1. Koprím hatások 5

1.2. Nilpotencia, p-feloldhatóság 9

1.3. Normál p-komplementum tételek 13

2. Frobenius-csoportok **15**

2.1. Definíció, alaptulajdonságok 15

2.2. Példák 19

2.3. A Frobenius-csoportok szerkezete 24

3. Frobenius-csoportok karakterei **30**

3.1. Frobenius tétele 30

3.2. Frobenius-csoportok karakterei 32

4. A Frobenius-mag nilpotenciája **38**

4.1. Néhány szó mátrixcsoportokról 38

4.2. A Thompson-részcsoport 42

4.3. Thompson normál p-komplementum tétele 47

4.4. A Frobenius-mag nilpotenciája 50

5. Perfekt Frobenius-komplementumok **53**

5.1. Perfekt Frobenius-komplementumok 53

Irodalomjegyzék **69**

Bevezetés

A Frobenius-csoportok olyan véges csoportok, melyeknek létezik olyan nemtriviális valódi részcsoportja -a Frobenius-komplementum-, melynek normalizátora saját maga, és tetszőleges két különböző konjugáltja csak az egységelemben metszi egymást. Tehát a komplementumnak maximálisan sok konjugáltja van (az adott rendek mellett), és ezek „annyira diszjunktak”, amennyire ez részcsoportok esetén lehetséges.
A definíció igen erős korlátozásokat hordoz magában. Megmutatható, hogy a komplementum konjugáltjain kívül eső elemek normálosztót alkotnak, a Frobenius-magot. Az előbbi állítás bizonyítása a karakterelmélet egyik első diadala (Frobenius, 1901).
Ennél azonban több is mondható: a mag nilpotens. Ezt a hosszú évtizedekig nyitott problémát Thompsonnak sikerült megoldania 1959-ben. Hasonló kérdés tehető fel a komplementummal kapcsolatban is. Feloldható-e minden Frobenius-komplementum? A válasz nemleges. A feladat nehézségét mutatja, hogy Burnside tévesen bizonyította ennek ellenkezőjét. „Lényegében” csupán egyetlen ellenpélda létezik: ha a komplementum perfekt is, akkor izomorf $\mathrm{SL}(2,5)$-tel (Zassenhaus, 1936).
A dolgozatban a fentiekben vázolt kérdések megoldásait fogjuk nyomon követni. Az első fejezetben a kapcsolódó fogalmakat, tételeket vesszük sorra. A második fejezetben a Frobenius-csoportok szerkezetét vizsgáljuk részletesen. Adunk egy saját bizonyítást a Frobenius-mag egyértelműségére. A harmadik fejezetben belátjuk Frobenius tételét és más karakterelméleti állításokat. Az itt található bizonyítások számottevő része önálló munka eredménye. A negyedik fejezetben Thompson a mag nilpotenciáját igazoló gondolatmenetét mutatjuk be. Végül az ötödik fejezetben a perfekt komplementumokkal kapcsolatos tételt igazoljuk.
Itt szeretnék köszönetet mondani témavezetőmnek, Pelikán Józsefnek útmutatásáért, és a dolgozathoz tett hasznos észrevételeiért.

1. fejezet

Csoportelméleti előkészületek

Ebben a fejezetben összefoglaljuk azon definíciókat, tételeket, melyeket fontosnak vélünk a későbbiek megértése céljából, és nem feltétlenül tartalmazza őket egy bevezető csoportelméleti kurzus. Nem törekszünk teljességre, de ahol az állítás kellőképp fontos, vagy annak bizonyítása kellőképp rövid, közöljük azt is.

1.1. Koprím hatások

Későbbi vizsgálódásaink egyik legfontosabb eszköze a koprím csoporthatások lesznek. Az alábbi részt nekik szenteljük. Az alfejezet tételei, gondolatmenete Huppert Character Theory of Finite Groups [3] 14. fejezetén alapulnak. Kivételt képez ez alól az 1.1.8 Tétel, mely Isaacs Finite Group Theory című könyvében [6] található.

1.1.1 Tétel: (Schur-Zassenhaus)
Legyen G véges csoport és $N \trianglelefteq G$. Tegyük fel, hogy $(|G : N|, |N|) = 1$. Ekkor létezik K komplementum, vagyis olyan $K \leq G$, hogy $G = N \rtimes K$. Ha N vagy G/N feloldható, akkor bármely két N-hez tartozó komplementum konjugált egy N-beli elem által.

1.1.2 Megjegyzés:
A feloldhatóságról tett feltevés nem szükséges, ugyanis a Feit-Thompson tétel értelmében a relatív prím rendű N és G/N csoportok közül legalább az egyik páratlan rendű, tehát feloldható. Dolgozatunkban azonban nem kívánunk hivatkozni erre az igen mély eredményre.

1.1.3 Tétel:
Legyenek A és G véges csoportok, és közülük legalább az egyik feloldható. Hasson A G-n automorfizmusokon keresztül. Legyen $H \leq G$ olyan részcsoport, és $g \in G$ olyan elem, hogy $(|A|, |H|) = 1, \quad H^a = H, \quad Hg = Hg^a \quad (\forall a \in A)$. Ekkor $\exists g_0 \in G$, hogy $Hg = Hg_0$ és ${g_0}^a = g_0 \quad (\forall a \in A)$, azaz $g_0 \in \mathrm{C}_G(A)$.
Bizonyítás:(Glauberman)
Ha g_0 létezik, akkor felírható hg alakban, ahol $h \in H$. Így olyan $h \in H$ elemet kell találnunk, melyre $(hg)^a = hg$, azaz $h^{-1}h^a = g(g^{-1})^a = (g^a g^{-1})^{-1} \quad (\forall a \in A)$.
Tekintsük az $S = G \rtimes A$ szorzatcsoportot, legyen $f(a) = g^a g^{-1}$. A feltételekből könnyű látni, hogy $f(a) \in H$. Vizsgáljuk a $K = \{af(a) | a \in A\}$ komplexust, megmutatjuk, hogy $K \leq S$. Ehhez elegendő látnunk, hogy bármely két K-beli elem szorzata is K-beli. Felhasználva, hogy $f(a_1a_2) = g^{a_1a_2}(g^{a_2})^{-1}g^{a_2}g^{-1} = (g^{a_1}g^{-1})^{a_2}g^{a_2}g^{-1} = f(a_1)^{a_2}f(a_2)$, adódik a kívánt állítás, $a_1f(a_1)a_2f(a_2) = a_1a_2f(a_1)^{a_2}f(a_2) = a_1a_2f(a_1a_2)$.
Mivel $H^a = H$, így $AH \leq S$ és $H \trianglelefteq AH$. $KH = AH$, ugyanis $KH \subseteq AH$, $f(a) \in H \quad (a \in A)$ miatt, míg $AH \subseteq KH$, $ah = af(a)(f(a)^{-1}h) \quad (a \in A, h \in H)$ miatt. $(|AH : H|, |H|) = 1$, H vagy A feloldható, így alkalmazhatjuk a Schur-Zassenhaus tétel második állítását, azaz létezik $h \in H$, melyre $A^h = K$. Tehát $a^h = h^{-1}ah = aa^{-1}h^{-1}ah = a(h^{-1})^a h \in aH \cap K$. Így szükségképpen $a^h = af(a)$.
Eszerint $h^{-1}ah = af(a) \Leftrightarrow a^{-1}h^{-1}a = f(a)h^{-1} \Leftrightarrow (h^{-1})^a = f(a)h^{-1} \Leftrightarrow h^a = hf(a)^{-1} \Leftrightarrow h^{-1}h^a = (g^a g^{-1})^{-1}$, és épp ezt akartuk. ■

1.1.4 Tétel:
Legyen $S = G \rtimes A$ véges permutációcsoport Ω-n, G tranzitív Ω-n, $(|G|, |A|) = 1$ és G vagy A feloldható.
(i) $\exists \omega \in \Omega$, hogy A stabilizálja ω-t.
(ii) Azon $\omega \in \Omega$ elemek, melyeket A stabilizál egy $\mathrm{C}_G(A)$-orbithoz tartoznak.
Bizonyítás:
(i) Tetszőleges $\alpha \in \Omega$ esetén jelölje S_α α stabilizátorát, $G_\alpha = S_\alpha \cap G$.

Rögzítsünk egy $\omega \in \Omega$-t, mivel G -és így S is- tranzitív, ezért $|\Omega| = |S : S_\omega| = |G : G_\omega|$. Átrendezve az egyenletet $|S_\omega : G_\omega| = |S : G| = |A|$. $G_\omega \trianglelefteq S_\omega$, így az előző egyenlőség miatt teljesülnek a Schur-Zassenhaus tétel feltételei, tehát $\exists B \leq S_\omega$: $S_\omega = G_\omega \rtimes B$. A csoportok rendjei miatt $S = G \rtimes B$-nek is teljesülnie kell. Ismét csak a Schur-Zassenhaus tételt alkalmazva kapjuk, hogy $\exists g \in G : A = B^g$. Így $A = B^g \leq S_\omega^g = S_{\omega g}$, azaz A stabilizálja ωg-et.
(ii) Legyenek $\alpha, \beta \in \Omega$ olyan elemek, melyeket A stabilizál. Mivel G tranzitív, így $\beta = \alpha h$ valamely $h \in G$ esetén. $\alpha h = \alpha h a = \alpha a h^a = \alpha h^a \quad (\forall a \in A)$, ezért $G_\alpha h = G_\alpha h^a \quad (\forall a \in A)$, továbbá $G_\alpha^a = G_{\alpha a} = G_\alpha \quad (\forall a \in A)$. Mivel $(|G_\alpha|, |A|) = 1$, és G_α vagy A legalább egyike feloldható, ezért teljesülnek az 1.1.3 Tétel feltételei. Azaz $\exists g \in \mathrm{C}_G(A) : G_\alpha h = G_\alpha g$, így $\beta = \alpha h = \alpha g$. ■

1.1.5 Tétel:
Legyenek A és G véges csoportok, közülük legalább az egyik feloldható, $(|A|, |G|) = 1$, és hasson A G-n automorfizmusokon keresztül.
(i) $|G|$ összes p prímosztójára létezik A-invariáns $P \in Syl_p G$ csoport (azaz $P = P^a \quad (\forall a \in A)$), és bármely kettő ilyen p-Sylow konjugált $\mathrm{C}_G(A)$ által.
(ii) Legyen $Q \leq G$ A-invariáns p-csoport. Ekkor létezik P A-invariáns p-Sylow, hogy $Q \leq P$.
Bizonyítás:
(i) Alkalmazzuk az előző tételt az $S = G \rtimes A$ és $\Omega = Syl_p G$ esetre.
(ii) Legyen R maximális az olyan A-invariáns p-csoportok között, melyek tartalmazzák Q-t. Tegyük fel, hogy R nem p-Sylow. Ekkor $R < P$ valamely $P \in Syl_p G$-re. $R < \mathrm{N}_P(R) \leq \mathrm{N}_G(R) = \mathrm{N}_G(R^a) = \mathrm{N}_G(R)^a \quad (\forall a \in A)$, hisz p-csoportban a noramlizátor határozottan nagyobb a normalizált valódi részcsoportnál. Tehát $\mathrm{N}_G(R)$ A-invariáns, és rendjét p magasabb hatványa osztja, mint R-ét. Az (i) pont alapján $N_G(R)$-nek létezik A-invariáns p-Sylowja, legyen ez P_0. Mivel $R \triangleleft N_G(R)$ p-normálosztó, így R $N_G(R)$ minden p-Sylowjának valódi részcsoportja, speciálisan az A-invariáns P_0-nak is. Ez viszont ellentmond R maximalitásának. ■

1.1.6 Tétel:
Legyenek A és G véges csoportok, közülük legalább az egyik feloldható, és hasson A G-n automorfizmusokon keresztül.
(i) Legyen $N \trianglelefteq G$ A-invariáns, és $(|A|, |N|) = 1$. Jelöljük a G-ből G/N-be menő természetes homomorfizmus képét felülvonással. Ekkor $\mathrm{C}_{\overline{G}}(a) = \overline{\mathrm{C}_G(a)} \quad (\forall a \in A)$, és $\mathrm{C}_{\overline{G}}(A) = \overline{\mathrm{C}_G(A)}$.

(Mivel N A-invariáns, így A hatása $\overline{G}$-n jól definiált az $(Ng)^a = Ng^a$ képlet által.)
(ii) $(|A|, |G|) = 1$ esetén $G = [G, A]\mathrm{C}_G(A)$, ahol $[G, A] = \langle g^{-1}g^a | g \in G, a \in A\rangle$.
(iii) (Fitting tétele) Ha G Abel-csoport és $(|A|, |G|) = 1$, akkor $G = \mathrm{C}_G(A) \times [G, A]$

Bizonyítás:

(i) Az 1.1.3 Tétel közvetlen következménye $N = H$ választás mellett.

(ii) Alkalmazzuk (i)-t: belátjuk, hogy $N = [G, A]$ A-invariáns normálosztó G-ben, és a faktor-csoporton A triviálisan hat. Így (i) miatt minden mellékosztályban van $\mathrm{C}_G(A)$-beli elem.

Egyszerű számolások mutatják, hogy $[g, a]^b = [g^b, a^b]$ $(\forall a, b \in A, g \in G)$ és $[g, a]^h = [gh, a][h, a]^{-1}$ $(\forall a \in A,\ h, g \in G)$. Így $[G, A]$ A-invariáns normálosztó. Válasszunk egy g G-beli elemet, $g^a = g^a g^{-1} g = (g(g^{-1})^a)^{-1} g \in [G, A]g$ tetszőleges $a \in A$-ra. Ezért $[G, A]g = [G, A]g^a \quad (\forall a \in A,\ g \in G)$, tehát A triviálisan hat a faktor-csoporton. Mivel minden mellékosztályban van $\mathrm{C}_G(A)$-beli elem, így G=$[G, A]\mathrm{C}_G(A)$.

(iii) Ismerve (ii)-t, elegendő megmutatni, hogy $[G, A] \cap \mathrm{C}_G(A) = 1$. Definiáljuk $\beta \in \mathrm{Hom}(G, G)$-t a következő képlettel: $g\beta = (\prod_{a \in A} g^a)^k$, ahol $k|A| \equiv 1 \pmod{|G|}$. $g^a\beta = g\beta$, miatt $g^{-1}g^a\beta = 1$, így $[G, A] \leq \ker\beta$. Ezzel szemben $g \in \mathrm{C}_G(A)$ esetén $g\beta = g^{|A|k} = g$. Tehát $[G, A] \cap \mathrm{C}_G(A) = 1$. ■

1.1.7 Megjegyzés:

(i) A fenti tétel (i) pontját szavakban így fogalmazhatnánk meg "faktorcsoportbeli fixpontok fixpontoktól származnak".

(ii)A fenti tételben definiált $[G, A] \leq G$ csoport épp a kommutátor által definiált csoportot adja $G \rtimes A$-ban.

1.1.8 Tétel:

Legyenek A és G véges csoportok, hasson A G-n automorfizmusokon keresztül, és legyen $(|A|, |G|) = 1$. Ekkor $[G, A, A] = [[G, A], A] = [G, A]$ (ahol az első egyenlőséggel a $[G, A, A]$ kifejezést definiáltuk).

Bizonyítás:

$[G, A, A] \leq [G, A]$ nyilvánvaló, így elegendő az ellenkező irányú tartalmazást megmutatnunk. Bizonyítjuk, hogy $\forall g \in G, a \in A$ esetén $[g, a] \in [G, A, A]$. Először tegyük fel, hogy A feloldható. Ekkor $G = [G, A]\mathrm{C}_G(A)$ miatt $g = cx$, ahol $c \in \mathrm{C}_G(A)$ és $x \in [G, A]$. $[g, a] = [cx, a] = [c, a]^x[x, a] = [x, a] \in [G, A, A]$. Az általános esetben pedig $[g, a] \in [G, \langle a\rangle] = [G, \langle a\rangle, \langle a\rangle] \leq [G, A, A]$ bizonyítja a tételt.■

1.2. Nilpotencia, p-feloldhatóság

Legfontosabb problémáink közé tartozik a Frobenius-mag nilpotenciájának és a Frobenius-komplementum feloldhatóságának kérdése. Az alfejezetben az ehhez szükséges fogalmakat vesszük górcső alá. Az állítások részletes ismertetése megtalálható Isaacs könyveiben [6], [5].

1.2.1 Megjegyzés:
A továbbiakban π-vel egy G véges csoport rendje prímosztóinak egy részhalmazát jelöljük, π' pedig a π-n kívüleső prímosztók halmaza.

1.2.2 Definíció:
Legyen G véges csoport. $\mathrm{O}_\pi(G)$ a legnagyobb π-normálosztó G-ben.

1.2.3 Megjegyzés:
(i) A fenti definícióban helyesen használtuk a legnagyobb szót. Ha $N, M \trianglelefteq G$ π-normálosztók, akkor $NM \trianglelefteq G$ is π-normálosztó. Így G összes π-normálosztójának szorzata a legnagyobb a π-normálosztók között.
(ii) Mivel $\mathrm{O}_\pi(G)$ legnagyobb, így szükségképpen karakterisztikus.

1.2.4 Állítás:
Legyen G véges csoport, $p||G|$ prím, ekkor $\mathrm{O}_p(G) = \bigcap\limits_{P \in Syl_p G} P$.
Bizonyítás:
$\bigcap\limits_{P \in Syl_p G} P$ p-csoport. A konjugálás egymás között permutálja a p-Sylowokat ezért p-normálosztó is. Elegendő belátni, hogy $\mathrm{O}_p(G) \leq \bigcap\limits_{P \in Syl_p G} P$. $\mathrm{O}_p(G)$ p-csoport, így része valamely p-Sylownak, mivel a p-Sylowok konjugáltak, így az összesnek része kell, hogy legyen.$\blacksquare$

1.2.5 Definíció:
Legyen G véges csoport. $\mathrm{O}^\pi(G)$ a legkisebb normálosztó G-ben, mely szerint vett faktor π-csoport.

1.2.6 Megjegyzés:
(i) A fenti definícióban helyesen használtuk a legkisebb szót. Ugyanis, ha $N, M \trianglelefteq G$ olyan normálosztók, hogy G/N és G/M π-csoportok, akkor N és M $\forall p \in \pi'$-re tartalmaznak egy-egy $P \in Syl_pG$-t. Így szükségképpen az összeset is tartalmazzák. Ezért $N \cap M$ is tartalmazza az összes p-Sylowot, és normálosztó. Tehát az általa vett faktor rendje nem osztható p-vel. Így G összes olyan normálosztójának metszete, mely által vett faktor π-csoport a legkisebb az őt meghatározó tulajdonságra nézve.
(ii) Mivel $\mathrm{O}^{\pi}(G)$ legkisebb, így szükségképpen karakterisztikus.

1.2.7 Állítás:
Legyen G véges csoport, ekkor $\mathrm{O}^{\pi}(G) = \langle P | \exists p \in \pi' : P \in Syl_pG \rangle$.
Bizonyítás:
$\langle P | \exists p \in \pi' : P \in Syl_pG \rangle$-ben a generáló elemek zártak a konjugálásra nézve, ezért a generált csoport normálosztó. Továbbá $\forall p \in \pi'$-re tartalmaz egy p-Sylowot, így az általa vett faktor π-csoport. Elegendő belátni, hogy $O^{\pi}(G) \geq \langle P | \exists p \in \pi' : P \in Syl_pG \rangle$. Mivel az O^{π} által vett faktor π-csoport, így O^{π} tartalmaz egy, és így az összes, p-Sylowot $\forall p \in \pi'$-re. Tehát $O^{\pi}(G) \geq \langle P | \exists p \in \pi' : P \in Syl_pG \rangle$.■

1.2.8 Definíció:
G π-szeparábilis, ha létezik olyan invariáns lánca, hogy minden faktor π- vagy π'-csoport. Azaz

$$1 = N_0 \leq N_1 \leq ... \leq N_r = G$$

olyan, hogy $\forall i : N_i/N_{i-1}$ π- vagy π'-csoport, és $\forall i : N_i \trianglelefteq G$.

1.2.9 Állítás:
Legyen G véges csoport. Az alábbi állítások ekvivalensek.
(i) G π-szeparábilis
(ii) G-nek létezik karakterisztikus részcsoportokból álló invariáns lánca, hogy a faktorok π- vagy π'-csoportok
(iii) G-nek létezik normállánca, hogy a faktorok π- vagy π'-csoportok. (A normálláncban szereplő csoportok csak a rákövetkező csoportban kell, hogy normálosztók legyenek, nem pedig

az egész G-ben.)

1.2.10 Megjegyzés:
Ha G π-szeparábilis csoport, akkor minden részcsoportja és faktora is π-szeparábilis. Ez az izomorfizmus-tételek egyszerű következménye.

1.2.11 Definíció:
A G véges csoport π-feloldható, ha létezik invariáns lánca, hogy minden faktor vagy feloldható π-csoport, vagy π'-csoport.

1.2.12 Megjegyzés:
A p-feloldhatóság és a p-szeparabilitás ugyanazt jelenti, hisz minden p-csoport feloldható.

1.2.13 Állítás:
A G véges csoport pontosan akkor feloldható, ha minden p prímre p-feloldható.

1.2.14 Tétel: (Hall-Higman Lemma)
Legyen G egy π-szeparábilis csoport, $\mathrm{O}_{\pi'}(G) = 1$. Ekkor $\mathrm{C}_G(\mathrm{O}_\pi(G)) \leq \mathrm{O}_\pi(G)$.
Bizonyítás:
Használjuk a következő jelöléseket, $C = \mathrm{C}_G(\mathrm{O}_\pi(G))$, $B = C \cap \mathrm{O}_\pi(G)$. Megmutatjuk, ha $B < C$, akkor C egy részcsoportjában, amely normális G-ben, tudunk találni nemtriviális π'-normálosztót. Így a karakterisztikus legnagyobb π'-normálosztó sem lesz triviális az adott részcsoportban. Ez által G-ben is találunk nemtriviális π'-normálosztót, ami ellentmondáshoz vezet, hisz $\mathrm{O}_{\pi'}(G)$ triviális.
B és C karakterisztikus G-ben. Tegyük fel, hogy $B < C$. C/B π-szeparábilis, így benne a legnagyobb π- vagy a legnagyobb π'-normálosztó legalább egyike nem triviális. Jelölje az előbb bevezetett nemtriviális normálosztó természetes homomorfizmusnál vett ősét K. K definíciójából adódóan $K/B \operatorname{char} C/B$, és K/B π- vagy π'-csoport. $K/B \operatorname{char} C/B \trianglelefteq G/B$ miatt $K \trianglelefteq G$. Mivel $\mathrm{O}_\pi(G)$ nem tartalmazza K-t, ezért K/B csak π'-csoport lehet.
Ekkor azonban a K-beli B normálosztóra alkalmazható a Schur-Zassenhaus tétel, azaz létezik $H \leq K$ komplementum, hogy $K = B \rtimes H$, ahol H π'-csoport. Tehát $K = BH$, és $K < C$

centralizálja B-t. Ezért tetszőleges $k \in K$ felírható $k = bh$ alakban, ahol $b \in B$, $h \in H$, és $H^k = H^{bh} = H$, azaz $H \trianglelefteq K$ π'-normálosztó. Így $1 < H \leq \mathrm{O}_{\pi'}(K) \operatorname{char} K \trianglelefteq G$ és $1 < \mathrm{O}_{\pi'}(K) \leq \mathrm{O}_{\pi'}(G)$, ami ellentmond a feltevéseinknek.■

1.2.15 Definíció:
Legyen G csoport, $G^0 = G$, $G^i = [G, G^{i-1}]$ $\forall i > 0$ egész számra. G nilpotens, ha $G^i = 1$ valamely i-re.

1.2.16 Megjegyzés:
(i) $G^i \operatorname{char} G$ és $G^i \geq G^{i+1}$ minden i esetén.
(ii) Ha a G véges csoport nem nilpotens, akkor létezik egy legkisebb i, hogy $G^i = G^j \quad \forall j \geqq i$. Jelöljük ezt a G^i-t a továbbiakban G^∞-nel.

1.2.17 Tétel:
A G csoport pontosan akkor nilpotens, ha létezik invariáns lánca, hogy

$$1 = N_0 \leq N_1 \leq ... \leq N_r = G$$

és $N_{i+1}/N_i \leq \mathrm{Z}(G/N_i) \quad (0 \leqq i < r)$.

1.2.18 Tétel:
A G véges csoport pontosan akkor nilpotens, ha p-Sylowjainak direkt szorzata.
Bizonyítás:
Legyen G a p-Sylowjainak direkt szorzata. Ahhoz, hogy belássuk, G nilpotens, elegendő p-csoportok nilpotenciáját megmutatni. Hiszen nilpotens csoportok direkt szorzata is nilpotens. (A műveleteket koordinátánként végezhetjük.)
Legyen $|P| = p^n$ (p prím). n szerinti indukcióval bebizonyítjuk, hogy P nilpotens. $n = 1$ esetén az állítás nyilvánvaló. Mivel P p-csoport, így centruma nem triviális. Az indukciós feltevés szerint a $P/\mathrm{Z}(P)$ faktorcsoport nilpotens. Tehát létezik i egész szám, hogy $(P/\mathrm{Z}(P))^i = 1$. Mivel a mellékosztályok lefedik a csoportot, és $g, h \in P$, $z_1, z_2 \in \mathrm{Z}(P)$ esetén $[gz_1, hz_2] = [g, h]$, így $P^i \leq \mathrm{Z}(P)$, tehát $P^{i+1} = 1$.
Tegyük fel, hogy G nilpotens, belátjuk, hogy ekkor p-Sylowjai direkt szorzata.
Ehhez elegendő megmutatni, hogy G összes p-Sylowja normálosztó. Ugyanis legyen

$|G| = p_1^{\alpha_1}...p_k^{\alpha_k}$, és $P_i \lhd G$ p_i-Sylow ($1 \leqq i \leqq k$). Ekkor $P_i^* = P_1...P_{i-1}P_{i+1}...P_k < G$, és indukcióval bizonyítható, hogy $|P_i^*| = \frac{|G|}{p_i^{\alpha_i}}$. Emiatt $P_i^* \cap P_i = 1$, és $P_1P_2...P_k = G$, tehát G a p-Sylowok direkt szorzata.

Megmutatjuk, hogy, ha létezik egy p-Sylow G-ben, amely nem normálosztó, akkor G nem lehet nilpotens. Tegyük fel, hogy P egy ilyen p-Sylow. Jelölje N $\mathrm{N}_G(P)$-t. A feltételek szerint $N < G$. $\mathrm{N}_G(N) = N$, ugyanis, ha létezne $g \in G \setminus N$, hogy $N^g = N$, akkor, mivel $P \operatorname{char} N$, így $P^g = P$ teljesülne, ami ellentmondás.

Indukcióval belátjuk, hogy minden i-re G^i-nek van N-en kívüli eleme, így egyik sem lehet a triviális csoport. G^0-ra teljesül az állítás. Tegyük fel, hogy $g \in G^i \setminus N$. Mivel $\mathrm{N}_G(N) = N$, és $g \in G \setminus N$, így létezik $n \in N$, hogy $n^g \in G \setminus N$. $[n, g] \in G^{i+1}$ és $P^{[n,g]} = P^{n^{-1}n^g} = P^{n^g} \neq P$ miatt $[n, g] \in G \setminus N$. Így G nem lehet nilpotens, ami ellentmondás.■

1.3. Normál p-komplementum tételek

Igen sokszor hasznos szolgálatot tesznek a különböző normál p-komplemetum tételek. Ebben a fejezetben ezeket ismertetjük. A részletes bizonyítások megtalálhatóak [6]-ban.

1.3.1 Definíció:

Legyen G véges csoport, p prím. $N \trianglelefteq G$ normál p-komplementum, ha $p \nmid |N|$, és $P \in Syl_pG$ esetén $G = N \rtimes P$.

1.3.2 Megjegyzés:

(i) A normál p-komplementum karakterisztikus részcsoport. Ha N és M normális, akkor az NM csoport tartalmazza mind N-et, mind M-et, továbbá $|NM| = \frac{|N||M|}{|N\cap M|}$ nem osztható p-vel. Tehát $|N| = |M| = |NM|$. Ezért $N = M$.

(ii) Az izomorfizmus-tételek egyszerű alkalmazásaként adódik: ha egy csoportnak van normál p-komplementuma, akkor minden részcsoportjának, és minden faktorcsoportjának is van normál p-komplementuma.

1.3.3 Tétel: (Burnside normál p-komplementum tétele)
Legyen G véges csoport, $P \in Syl_p(G)$ olyan p-Sylow, hogy $\mathrm{N}_G(P) = \mathrm{C}_G(P)$. Ekkor létezik G-nek normál p-komplementuma.

1.3.4 Állítás:
$\mathrm{Aut}(\mathrm{Z}_n) \cong U_n$, ahol U_n a modulo n redukált maradékosztályok multiplikatív csoportja.

1.3.5 Következmény:
Legyen G véges csoport.
(i) Legyen p G rendjének legkisebb prímosztója. Tegyük fel, hogy $P \in Syl_pG$ ciklikus, ekkor G-nek létezik normál p-komplementuma.
(ii) Legyen G összes Sylow-részcsoportja ciklikus, ekkor G feloldható.
Bizonyítás:
(i) Legyen $|P| = p^k$. Mivel P ciklikus, így $P \leq \mathrm{C}_G(P)$. $\mathrm{N}_G(P)/\mathrm{C}_G(P)$ izomorf a $\varphi(p^k) = p^{k-1}(p-1)$ rendű $\mathrm{Aut}(P)$ valamely részcsoportjával, és p $|G|$ legkisebb prímosztója, ezért $\mathrm{N}_G(P)/\mathrm{C}_G(P)$ p-csoport. Összevetve ezt az előző megállapításunkkal kapjuk, hogy $\mathrm{N}_G(P)/\mathrm{C}_G(P)$ triviális. Alkalmazhatjuk tehát Burnside tételét, amiből a kívánt állítást is megkapjuk.
(ii) Végezzünk $|G|$ prímosztóinak száma szerinti indukciót. Egy prímosztó esetén az állítás nyilvánvalóan igaz. Tegyük fel, hogy n-ig igaz, belátjuk, hogy $n+1$-re is igaz. Az (i) pont alapján $G = N \rtimes P$, ahol p $|G|$ legkisebb prímosztója, N p-komplementum, $P \in Syl_pG$. N-re alkalmazhatjuk az indukciós feltevést, $G/N \cong P$ pedig p-csoport, így feloldható, ezért G is feloldható.$\blacksquare$

1.3.6 Tétel: (Frobenius normál p-komplemetum tétele)
Legyen G véges csoport, ekkor ekvivalensek a következő állítások.
(i) G-nek létezik normál p-komplementuma.
(ii) Minden $1 < P \leq G$ p-csoport esetén $\mathrm{N}_G(P)$-nek létezik normál p-komplementuma.
(iii) Minden $1 < P \leq G$ p-csoport esetén $\mathrm{N}_G(P)/\mathrm{C}_G(P)$ p-csoport.

2. fejezet

Frobenius-csoportok

A fejezetben bevezetésre kerül szakdolgozatunk tárgya, a Frobenius-csoportok. Látni fogjuk, hogy a definíció igen erős megkötést ad a csoportok szerkezetére. A továbbiakban ezt kívánjuk mélyebben elemezni.

2.1. Definíció, alaptulajdonságok

A következő részben a Frobenius-csoportokkal kapcsolatos ismertebb eredményeket tárgyaljuk. A nehezebb gondolatokat igénylő 2.1.4 Tételt [3] és a 2.1.10 Tételt [6] megfelelő része alapján írtuk.

2.1.1 Definíció:
A G véges csoport Frobenius-csoport, ha létezik olyan $1 < A < G$ részcsoportja, amelyre $A \cap A^g = 1 \quad \forall g \in G \setminus A$. Ekkor A-t Frobenius-komplementumnak nevezzük.

2.1.2 Állítás:
(i) Legyen G tranzitív permutációcsoport az Ω véges halmazon ($|\Omega| > 1$). Ha $G \setminus \{1\}$ minden elemének legfeljebb egy fixpontja van, és van olyan elem, melynek van fixpontja, akkor G Frobenius-csoport.
(ii) Legyen G Frobenius-csoport A Frobenius-komplementummal. G reprezentációja A

mellékosztályain hűséges, így képét azonosíthatjuk G-vel. Ekkor G tranzitív, $G \setminus \{1\}$ elemeinek, mint permutációknak A mellékosztályain, legfeljebb egy fixpontjuk van, és van olyan elem, melynek van fixpontja.

Bizonyítás:

(i) Tetszőleges $\alpha \in \Omega$ esetén jelölje G_α α stabilizátorát.

Rögzítsünk egy $\omega \in \Omega$ elemet. $1 < G_\omega < G$. Mivel G tranzitív, így a stabilizátor részcsoportok G valódi részcsoportjai, továbbá páronként konjugáltak egymással. Van elem, amelynek van fixpontja, így nemtriviálisak. $G_\omega \cap G_\omega^g = G_\omega \cap G_{\omega g} = 1 \quad (\forall g \in G \setminus G_\omega)$, ugyanis csak $1 \in G$-nek van 1-nél több fixpontja. Tehát G Frobenius-csoport, G_ω pedig Frobenius-komplementum.

(ii) A reprezentáció hűséges, hisz a magja triviális, $\bigcap\limits_{g \in G} A^g = 1$. Nyilvánvalóan tranzitív. A tetszőleges elemének A fixpontja. $h \in G$ pontosan akkor stabilizálja az Ag mellékosztályt, ha $h \in A^g$. Így, ha $1 \neq h \in H$ stabilizálja az Ag_1, Ag_2 mellékosztályokat, akkor $A^{g_1} \cap A^{g_2} > 1$. Az $A^g \cap A = 1 \quad (\forall g \in G \setminus A)$ feltétel miatt, ez csak $Ag_1 = Ag_2$ esetben teljesülhet. Ezzel az állítást bizonyítottuk. ■

2.1.3 Tétel:(Frobenius-tétel)

Legyen G Frobenius-csoport A Frobenius-komplementummal. Ekkor $N = (G \setminus \bigcup\limits_{g \in G} A^g) \cup \{1\}$ normálosztó, melyet Frobenius-magnak nevezünk.

2.1.4 Megjegyzés:

(i) Az előbbi tételt teljes egészében a 3. fejezetben fogjuk bizonyítani. Itt két speciális esetre adunk bizonyítást, melyek valójában az összes esetet kimerítik, ám ennek megmutatásához a Feit-Thompson-tételre kellene hivatkoznunk.

(ii) Ha N csoport, akkor a konstrukció folytán nyilvánvalóan normálosztó. Mivel $A = \mathrm{N}_G(A)$, ezért A-nak $|G : A|$ különböző konjugáltja van. Ezek az egységelemtől eltekintve páronként diszjunktak, így $|N| = |G| - |G : A|(|A| - 1) = |G : A|$.

(iii) A 2.1.2 Állításban szereplő permutációcsoportokra a következőképp fogalmazhatjuk meg Frobenius tételét: a fixpontmentes elemek és az identitás normálosztót alkotnak.

2.1.4 Tétel:

(i) (Shaw, Grün) Legyen G Frobenius-csoport A feloldható Frobenius-komplementummal. Ekkor $N = (G \setminus \bigcup\limits_{g \in G} A^g) \cup \{1\}$ normálosztó.

(ii) (Bender) Legyen G Frobenius-csoport A Frobenius-komplementummal, és $2 \mid |A|$. Ekkor $N = (G \setminus \bigcup_{g \in G} A^g) \cup \{1\}$ normálosztó.

Bizonyítás:

(i) Mivel $A' < A$, így az A-ba menő transzfer magja egy kisebb (esetleg „elfajuló") Frobenius-csoportot fog adni, amelyen indukció segítségével már bizonyítottnak tekinthetjük az állítást (A feloldhatósága miatt $1 < B \leq A$ esetén $B' < B$). Kiderül, hogy a kisebb csoportban talált mag megfelelő lesz a nagyobban is.

Tetszőleges $g \in G$-re a g által az A mellékosztályain megvalósított permutáció felírható diszjunkt ciklusok szorzataként. Közülük a j-edik legyen: $(As_j, As_jg, ..., As_jg^{f_j-1})$ $(j = 1, 2, ..., t(g))$. A transzfer ekkor a következő alakot ölti: $v(g) = \prod_{j=1}^{t(g)} s_jg^{f_j}s_j^{-1}A'$. Feltehető, hogy $s_1 = 1$.

Indukciót alkalmazunk G rendje szerint. Az első néhány kisebb rendű csoportra az állítás nyilvánvalóan igaz.

Belátjuk, hogy $G = \ker v \cdot A$. Tetszőleges $a \in A$ esetén $v(a) = aA'$, ugyanis a szorzatban szereplő első tag az $s_1 = 1$ választás miatt aA'-tal egyenlő, míg $j \geq 2$ esetén $s_ja^{f_j}s_j^{-1} \in A \cap A^{s_j^{-1}} = 1$ $(s_j \in G \setminus A)$. Tehát $\ker v \cap A = A'$. Tetszőleges $g \in G$-re pedig $v(g) = aA' = v(a)$ valamely $a \in A$-val, így $ga^{-1} \in \ker v$, ebből pedig $G = \ker v \cdot A$ adódik.

Jelölje K $\ker v$-t, és tegyük fel, hogy $1 < A'$, ekkor K Frobenius-csoport A' komplementummal. $K \setminus A' \subseteq G \setminus A$, ezért $A' \cap (A')^y \leq A \cap A^y = 1 \quad \forall y \in K \setminus A'$. $|K| < |G|$, így alkalmazhatjuk az indukciós feltevést, azaz $M = (K \setminus \bigcup_{k \in K} A'^k) \cup \{1\}$ normálosztó K-ban, valamint $K = MA'$, és $M \cap A' = 1$. Az utóbbi két egyenlőség $A' = 1$ esetben is teljesül. 2.1.4 Megjegyzésünk szerint $|M| = |K : A'| = |K : K \cap A| = |KA : A| = |G : A| = |N|$. A bizonyítás befejezéséhez elegendő tehát megmutatnuk, hogy $M \subseteq N$. Mivel tetszőleges $g \in G$-hez található $a \in A, k \in K$, hogy $g = ak$, emiatt $M \cap A^g = M \cap A^k = M^k \cap A^k = (M \cap A)^k = (K \cap M \cap A)^k = (M \cap (K \cap A))^k = (M \cap A')^k = 1$. Tehát $N = M$ normálosztó.

(ii) Jelölje $|G : A|$-t n. A 2.1.4 Megjegyzés szerint A-nak n darab különböző konjugáltja van. Indexeljük meg a konjugáltakat j-vel, és válasszunk mindegyikből egy i_j involúciót $(j = 1, 2, ..., n)$. $i_ji_k \in N$ $(j \neq k$ és $j, k = 1, 2, ..., n)$, ugyanis ha nem így lenne, akkor $i_ji_k \in A_l$ valamely l-re. $1 \neq (i_ji_k)^{i_j} = (i_ki_j) = (i_ji_k)^{-1} \in A_l \cap (A_l)^{i_j}$, így $i_j \in A_l$, és hasonlóan bizonyítható, hogy $i_k \in A_l$ is teljesül. Ekkor viszont $i_j = i_k$, ami ellentmondás. Tehát tetszőleges rögzített $j \in \{1, 2, ..., n\}$ esetén $\{i_ki_j \mid k = 1, ..., n\} = \{i_ji_k \mid k = 1, 2, ..., n\} = N$, ahol egyenlőséget a számosságok egyenlősége miatt írhatunk (ismét csak a 2.1.4 Megjegyzésre hivatkozva). Legyen n, m N két tetszőleges eleme, ekkor $nm \in N$ is teljesül, így N csoport. Válasszunk egy rögzített $j \in \{1, 2, ..., n\}$ elemet, ekkor léteznek $k, l \in \{1, 2, ..., n\}$ elemek, hogy

$n = i_k i_j$, $m = i_j i_l$, így $nm = i_k i_l \in N$. Ezzel a tételt bizonyítottuk.■

2.1.5 Állítás:

Legyen $G = N \rtimes A$ véges csoport, $1 < A < G$. Ekkor a következő állítások ekvivalensek.
(i) A Frobenius-komplementum.
(ii) Az A elemeivel való konjugálás fixpontmentes hatást valósít meg N-en. (Azaz $n \in N, a \in A$ esetén $n^a = n \Leftrightarrow n = 1$ vagy $a = 1$)

Bizonyítás:

(i)⇒(ii) Tegyük fel, hogy $\exists 1 \neq n \in N, 1 \neq a \in A : n^a = n$, ekkor $a^n = a$, így $A \cap A^n > 1$, ami ellentmondás.
(ii)⇒(i) $G = N \rtimes A$ miatt $g \in G \setminus A$ felírható $g = an \quad (a \in A, 1 \neq n \in N)$ alakban. $A^g \cap A > 1$ pontosan akkor teljesül, ha $A^n \cap A > 1$. Ekkor léteznek $1 \neq a, b \in A$ elemek, hogy $a^n = b$. $b = n^{-1}an = a(n^{-1})^a n \Leftrightarrow (n^{-1})^a n = a^{-1}b$, mivel $N \cap A = 1$, így $(n^{-1})^a n = 1$, azaz $n^a = n$, ami ellentmondás.■

2.1.6 Definíció:

Legyenek A, N véges csoportok, hasson A N-en automorfizmusokon keresztül. Ha A hatása fixpontmentes N-en, akkor Frobenius-hatásnak nevezzük.

2.1.7 Állítás:

Legyen $G = N \rtimes A$ Frobenius-csoport A komplemetummal. Ekkor az A által megvalósított Frobenius-hatás koprím hatás.

Bizonyítás:

A fixpontmentesség miatt A egységelemet nem tartalmazó orbitjai $|A|$ számosságúak, így $|N| \equiv 1 \pmod{|A|}$.■

2.1.8 Állítás:

Valósítson meg A N-en egy Frobenius-hatást. Legyen $M \trianglelefteq N$ A-invariáns normálosztó. Ekkor A Frobenius-hatást valósít meg N/M-en is.

Bizonyítás:

Az 1.1.6 Tétel (i) pontjának és a 2.1.7 Állításnak a következménye.■

2.1.9 Állítás:
Legyen $G = N \rtimes A$ Frobenius csoport A komplementummal, ekkor aN elemei egy konjugált osztályhoz tartoznak tetszőleges $a \in A$ esetén.
Bizonyítás:
Legyen $a \in A$ tetszőleges elem. Vegyük észre, hogy $|aN| = |a^N|$, így az állítás belátásához elegendő megmutatnunk, hogy $a^N \subseteq aN$. $a^n = n^{-1}an = aa^{-1}n^{-1}an = a(n^{-1})^a n$ ■

2.1.10 Tétel:
A G véges csoport pontosan akkor Frobenius-csoport, ha létezik olyan $N \lhd G$ normálosztó, hogy $\mathrm{C}_G(n) \leq N \quad \forall\, 1 \neq n \in N$ esetén.
Bizonyítás:
Ha G Frobenius-csoport, akkor az állítás a 2.1.5 Tétel alapján nyilvánvaló.
Legyen N a feltételekben szereplő normálosztó. Belátjuk, hogy $(|G:N|, |N|) = 1$. Tegyük fel, hogy létezik p prím, hogy $p \mid (|G:N|, |N|)$. Legyen $P \in Syl_p N$ és $Q \in Syl_p G$ olyan, hogy $P < Q$. $C = \mathrm{Z}(Q) \cap N > 1$, ugyanis $\mathrm{Z}(Q)$ p-csoport, N pedig normálosztó (ez a konjugált osztályok p-vel való oszthatóságára tett egyszerű meggondolásokból adódik). Mivel Q centralizálja C-t, $1 < C \leq N$, és $Q \nsubseteq N$, így ellentmondásra jutunk.
Tehát $(|G:N|, |N|) = 1$, így alkalmazhatjuk a Schur-Zassenhaus-tételt. Legyen A egy N-hez tartozó komplementum. Feltételeink szerint az A elemeivel való konjugálásnak nem lehet fixpontja N-ben, így G Frobenius-csoport.■

2.2. Példák

A következő alfejezetben példákat mutatunk Frobenius-csoportokra. Közülük az első három ismertebbnek tekinthető, míg a második hármat [3]-ből kölcsönözzük. A velük kapcsolatos nem bizonyított állítások Huppert Endliche Gruppen I. című könyvében [2] találhatóak. A 2.2.7 Példa megtalálásában kulcsszerep jut az 5-ödfokú alternáló csoportnak. A példa igen fontos, hisz bizonyítja, hogy létezik nemfeloldható Frobenius-komplementum. A_5 definiáló relációkkal való megadására, egy a szokásostól eltérő, saját bizonyítást adunk.

2.2.1 Példa:
Legyen H páratlan rendű Abel-csoport, hasson rajta a Z_2 csoport az invertálás segítségével. Ekkor a $H \rtimes \mathrm{Z}_2$ csoport Frobenius, ugyanis H-ban nincs másodrendű elem, így Z_2 hatása fixpontmenetes. Ennek speciális esete a $\mathrm{D}_{2k+1} = \langle f,\, t \mid f^{2k+1} = 1,\, t^2 = 1,\, tft = f^{-1} \rangle \quad (k \geqq 1)$ diédercsoport.
A Példa "megfordítása" is igaz, ezt a 4.4.1 Tételben bizonyítjuk.

2.2.2 Példa:
Legyenek $p < q$ prímek és $q \equiv 1 \pmod{p}$. Tekintsük a pq rendű nem ciklikus csoportot, $\mathrm{Z}_q \rtimes \mathrm{Z}_p$-t, ez Frobenius. Z_q, Z_p minden egységelemtől különböző eleme generálja a megfelelő részcsoportot. Ha Z_p valamely egységelemtől különböző elemével való konjugálás fixen hagyja Z_q egy egységelemtől különböző elemét, akkor a csoport Abel. Ezért ciklikus is. Z_p hatása tehát fixpontmentes.

2.2.3 Példa:
Legyen $K = \mathrm{GF}(p^f)$ a p^f rendű test. Az $\mathrm{Aff}(p^f) = \{x \mapsto ax + b \mid 0 \neq a, b \in K\}$ csoport Frobenius. Ha $\mathrm{Aff}(p^f)$-re mint K feletti permutációcsoportra gondolunk, akkor egyértelmű, hogy minden egységelemtől különböző elemnek legfeljebb 1 fixpontja van, és van elem, amelynek van fixpontja.

2.2.4 Példa: (N. Ito)
Válasszunk p, q prímeket, és f, n természetes számokat, hogy $q > n$ és $q | p^f - 1$. Jelölje K $\mathrm{GF}(p^f)$-et. Tekintsük az $N = \{(k_{ij}) | i, j = 1, 2, ..., n;\, k_{ij} \in K;\, k_{ii} = 1;\, k_{ij} = 0 \quad i > j \,\text{esetén}\}$ csoportot, azaz azokat az $n \times n$-es felső háromszög mátrixokat, melyeknek a főátlójukban egyesek állnak. $q \mid p^f - 1$, így vegyük K multiplikatív csoportjának, a K^* ciklikus csoportnak, az egyetlen q-adrendű részcsoportját, és legyen benne b egy generáló elem. Legyen $a = \mathrm{diag}(b, b^2, ..., b^n)$, $A = \langle a \rangle$. Egyszerű számolás mutatja, hogy $N = N^a$ (mind A, mind N részcsoportja $\mathrm{GL}(n, p^f)$-nek), így nézhetjük a $G = N \rtimes A$ csoportot. Ez Frobenius, ugyanis A hatása fixpontmentes. Ha $a^m \quad (1 \leqq m < q)$ fixen hagyja $(k_{ij}) \in K$-t, akkor $(k_{ij}) = a^{-m}(k_{ij})a^m = (b^{-im}k_{ij}b^{jm}) = (b^{m(j-i)}k_{ij})$. Mivel $(m, q) = 1$, így $b^{m(i-j)} \neq 1 \quad i \neq j$ esetén, ezért $k_{ij} = 0 \quad i \neq j$. Eszerint $(k_{ij}) = I$.
A későbbiekben belátjuk Thompson híres tételét, hogy a Frobenius-mag nilpotens. Mivel N nilpotenciaosztálya $n - 1$, így a példa mutatja, hogy ez tetszőlegesen nagy lehet.

2.2.5 Példa:

Válasszunk most p prímet és m természetes számot, hogy $2m \mid p-1$. Az előzőekhez hasonlóan legyen $K = \mathrm{GF}(2,p)$, ε pedig K^* $2m$ rendű csoportjának egy generáló eleme. Legyen $A = \langle a,b \rangle$, ahol $a = \begin{pmatrix} \varepsilon & \\ & \varepsilon^{-1} \end{pmatrix}$ és $b = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$. Könnyen meggondolható, hogy $a^{2m}=1$, $b^4=1$, $b^2=a^m$, $a^b=a^{-1}$, és így $A = \langle a \rangle \cup \langle a \rangle b$. Legyen $V=K^2$, K feletti 2 dimenziós vektortér. A hatása V-n fixpontmentes, ezért $G = V \rtimes A$ Frobenius. Az $a^j \quad (1 \leqq j < 2m)$ alakú elemek esetén $(x_1,x_2) = (x_1,x_2)a^j = (\varepsilon^j x_1, \varepsilon^{-j}x_2)$ csak $(x_1,x_2)=0$ választással teljesülhet. Az $a^j b \quad (0 \leqq j < 2m)$ alakú elemek esetén $(x_1,x_2) = (x_1,x_2)a^j b = (-\varepsilon^{-j}x_2, \varepsilon^j x_1)$-t is csak az $(x_1,x_2)=0$ vektor elégíti ki.
Észrevehető, ha m 2-hatvány, akkor az általánosított kvaterniócsoportot kapjuk A-ként.

2.2.6 Állítás:

$\mathrm{A}_5 \cong \langle a,b | a^5=1,\ b^2=1,\ (ab)^3=1 \rangle$

Bizonyítás:

$a=(12345)$ és $b=(12)(34)$ választással az állításban szereplő relációk teljesülnek A_5-ben, így a Dyck-tétel szerint $G = \langle a,b | a^5=1,\ b^2=1,\ (ab)^3=1 \rangle$-nek homomorf képe A_5. Elég tehát belátni, hogy G-nek legfeljebb 60 eleme van.
Jelölje A $\langle a \rangle$-t. Megmutatjuk, hogy a következő 12 mellékosztály egymás között permutálódik a generálóelemekkel (a,b) való szorzásra, így $|G|=60$:

$$A, Ab, Aba, Aba^2, Aba^3, Aba^4, Aba^2b, Aba^3b, Aba^3ba, Aba^3ba^2, Aba^3ba^3, Aba^3ba^2b.$$

1.A
$Aa = A,\ Ab = Ab$

2.Ab
$Aba = Aba,\ Abb = A$

3.Aba
$Abaa = Aba^2,\ Abab = Aba^4$

$abab = b(bababa)a^4 = ba^4$
$Abab = Aabab = Aba^4$

$4.Aba^2$
$Aba^2a = Aba^3$, $Aba^2b = Aba^2b$

$5.Aba^3$
$Aba^3a = Aba^4$, $Aba^3b = Aba^3b$

$6.Aba^4$
$Aba^4a = Ab$, $Aba^4b = Aba$

$Aba^4b = A(abab)b = Aba$

$7.Aba^2b$
$Aba^2ba = Aba^3b$, $Aba^2bb = Aba^2$

$aba^2ba = ababbaba = (abab)(baba) = ba^4a^4b = ba^3b$
$Aba^2ba = Aaba^2ba = Aba^3b$

$8.Aba^3b$
$Aba^3ba = aba^3ba$, $Aba^3bb = Aba^3$

$9.Aba^3ba$
$Aba^3baa = Aba^3ba^2$, $Aba^3bab = Aba^3ba^3$

$aba^3bab = (abab)(ba^2bab) = ba^4ba^2bab = (ba^4ba)(abab) = ba^4baba^4 = (ba^3)(abab)(a^4) = ba^3ba^4a^4 = ba^3ba^3$
$Aba^3bab = Aaba^3bab = Aba^3ba^3$

$10.Aba^3ba^2$
$Aba^3ba^2a = Aba^3ba^3$, $Aba^3ba^2b = Aba^3ba^2b$

$11.Aba^3ba^3$
$Aba^3ba^3a = Aba^2b$, $Aba^3ba^3b = Aba^3ba$

$Aba^3ba^3a = Aba^3ba^4 = A(ba^3b)a^4 = A(aba^2ba)a^4 = Aba^2b$
$Aba^3ba^3b = (Aba^3b)a^3b = (Aba^2ba)(a^3b) = (Aba^2b)(a^4b) = (Aba^2b)(baba) = Aba^3ba$

12.Aba^3ba^2b
$Aba^3ba^2ba = Aba^3ba^2b$, $Aba^3ba^2bb = Aba^3ba^2$

$Aba^3ba^2ba = (Aba^2)(aba^2ba) = (Aba^2)(ba^3b) = Aba^2ba^3b = A(aba^2ba)a^2b = A(aba^2ba)(a^2b) = Aba^3ba^2b$ ■

2.2.7 Példa:
Tekintsük a $\mathrm{PSL}(2,11)$ csoportot. Legyenek $a = \begin{pmatrix} 3 & \\ & 4 \end{pmatrix}$ és $b = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}$, ahol a mátrixelemekre, mint a $K = \mathrm{GF}(11)$ elemeire gondolunk. Jelölje $\overline{a}$ és $\overline{b}$ a megfelelő $\mathrm{PSL}(2,11)$-beli elemeket. Könnyen ellenőrizhető, hogy $\overline{a}^5 = 1$, $\overline{b}^2 = 1$ és $(\overline{a}\overline{b})^3 = 1$, tehát a 2.2.6 Állítás és a Dyck-tétel szerint $\overline{A} = \langle \overline{a}, \overline{b} \rangle$ A_5 homomorf képe. Mivel A_5 egyszerű és $\overline{A}$ nem a triviális csoport, így $\overline{A} \cong \mathrm{A}_5$.
A fentiek alapján $\mathrm{SL}(2,11)$-nek létezik A részcsoportja, hogy $A/\langle -I \rangle = \overline{A} \cong \mathrm{A}_5$. Legyen $V = K^2$ K feletti 2 dimenziós vektortér. Megmutatjuk, hogy A fixpontmentesen hat V-n (a hatást a vektortéren értelmezett lineáris transzformáció szolgáltatja), így $G = V \rtimes A$ Frobenius-csoport. Tegyük fel, hogy valamely $a \in A$-nak van nemtriviális fixpontja. Egészítsük ki a fixponthoz tartozó vektort bázissá, és írjuk fel a mátrixát ebben a bázisban. Mivel $\det a = 1$, így ez a következő alakot ölti: $a = \begin{pmatrix} 1 & \\ k & 1 \end{pmatrix}$. Mivel $\mathrm{char} K = 11$, így $a^{11} = 1$, de $11 \nmid |A| = 120$, tehát $a = 1$.
A példa mutatja, hogy létezik nem feloldható Frobenius-komplementum.

2.2.8 Megjegyzés:
A 2.2.7 Példa általánosítható. Ha p olyan prím, hogy $5 \mid p^2 - 1$, akkor létezik $\mathrm{PSL}(2,p)$-nek $\mathrm{SL}(2,5)$-tel izomorf részcsoportja, és ez fixpontmentesen hat a megfelelő 2-dimenziós vektortéren.

2.3. A Frobenius-csoportok szerkezete

Korábban említettük, hogy a Frobenius-csoportok szerkezete igen kötött. Ennek részletes vizsgálatát tartalmazza az alábbi rész. Gondolatmenetünk Isaacs könyve [6] 6.fejezetének felépítését követi.
Adunk egy egyszerű saját bizonyítást a Frobenius-mag egyértelműségére, és a Frobenius-komplementum konjugáltság erejéig való egyértelműségére.

2.3.1 Definíció:
P-t a G csoport egy partíciójának nevezzük, ha P G nemtriviális valódi csoportjainak egy halmaza, ahol P bármely két elemének metszete csak az egységelemet tartalmazza, és P elemeinek uniója lefedi G-t.

2.3.2 Lemma:
Legyen P az A véges csoport egy partíciója. A hasson automorfizmusokon keresztül, az U Abel-csoporton, és tegyük fel, hogy $u \in U$ rendje nem osztja $|\mathrm{P}| - 1$-et. Ekkor létezik $B \in \mathrm{P}$, hogy $\mathrm{C}_U(B) > 1$.
Bizonyítás:
Tetszőleges $H \leq A$-hoz konstruáljunk egy H-invariáns U-beli elemet a következő módon: valamely $v \in U$-ra készítsük el a $v_H = \prod_{h \in H} v^h$ szorzatot. Mivel $h \in H$ csak a tényezők sorrendjét permutálja v_H előállításában, így valóban H-invariáns elemet kapunk.
Tegyük fel, hogy $\mathrm{C}_U(B) = 1$ $(\forall B \in \mathrm{P})$. Ekkor $v_B = 1$ $(\forall v \in U, B \in \mathrm{P})$. Tehát $1 = \prod_{B \in \mathrm{P}} u_B = u^{|\mathrm{P}|-1} u_A$. Mivel u rendje nem osztja $|\mathrm{P}| - 1$-et, így $1 \neq u_A$. Tehát találtunk egy az egységelemtől különböző elemet $\mathrm{C}_U(A)$-ban, ami ellentmond a feltevésünknek.■

2.3.3 Állítás:
Frobenius-csoportnak létezik feloldható Frobenius-féle részcsoportja.
Bizonyítás:
Legyen $G = N \rtimes A$ Frobenius-csoport N maggal és A komplementummal. Legyen $a \in A$ egy prímrendű elem, és jelölje A_1 $\langle a \rangle$-t $(o(a) = q)$. A_1 továbbra is fixpontmentesen hat N-en, így $N \rtimes A_1$ Frobenius. Legyen $|N| = p^k m$, valamely p prímre, $m \geq 1$, $k \geq 1$ egész számokra, ahol m nem osztható p-vel és q-val sem (mivel a komplementum rendje relatív prím a magéhoz).

A Sylow-tételek következményeként $|Syl_pN| \mid m$. Mivel a egy identikus vagy q-adrendű permutációt valósít meg N p-Sylowjain, így szükségképpen van fixpontja. Legyen $P \in Syl_pN$ egy A_1-invariáns p-Sylow. $P \rtimes A_1$ Frobenius, és feloldható, hisz P és a P-vel vett faktor is feloldható. ■

2.3.4 Tétel:
Legyen A Frobenius-komplementum, azaz olyan véges csoport, mely fixpontmentesen hat egy N véges csoporton. Ekkor A-nak nem létezik olyan részcsoportja, mely Frobenius-csoport, vagy olyan elemi Abel-p-csoport, melynek rendje p-nél nagyobb.
Bizonyítás:
Tegyük fel, hogy a tétel állítása nem igaz, és az A, N csoportok ellenpéldát szolgáltatnak. Ha A Frobenius-hatást valósít meg N-en, akkor minden részcsoportja is, így $A_1 \rtimes N$ Frobenius-csoport, ahol A_1 p^2 rendű elemi Abel-csoport vagy feloldható Frobenius-csoport. Mivel mindkét esetben A_1 feloldható és koprím módon hat N-en, így létezik N-nek A_1-invariáns Sylow-részcsoportja, Q. $U = \mathrm{Z}(Q)$ karakterisztikus Q-ban, ezért A_1-invariáns is. Tehát $U \rtimes A_1$ Frobenius-csoport, ahol U (nemtriviális) Abel-csoport.
Ha A_1 p^2 rendű elemi Abel-csoport, akkor a p rendű részcsoportjai A_1 egy partícióját adják, ahol a partíció számossága $p + 1$. Ha A_1 Frobenius-csoport, akkor egy komplementumának a konjugáltjai és a komplementumhoz tartozó mag A_1 egy partícióját adják. Ennek számossága $m + 1$, ahol m a megfelelő mag rendjét jelöli. Mindkét esetben A_1-nek van egy partíciója, melynek számossága $a + 1$ alakú, ahol $a \mid |A_1|$.
Mivel A_1 és U rendje relatív prím, így a 2.3.2 Lemmát alkalmazva kapjuk, hogy U egy egységelemtől különböző elemét A_1 partíciójának valamely tagja centralizálja. Ez ellentmond a Frobenius-hatás fixpontmentességének.■

2.3.5 Következmény:
(i) Legyen A Frobenius-komplementum, p és q nem feltétlen különböző prímek. Ekkor A összes pq rendű részcsoportja ciklikus.
(ii) Legyen A Frobenius-komplementum, és $P \in Syl_pA$ (p A rendjének prímosztója). Ekkor P-nek pontosan egy p-edrendű részcsoportja van.
Bizonyítás:
(i) Ha egy pq rendű csoport nem ciklikus, akkor vagy elemi Abel és $p = q$, vagy Frobenius.
(ii) Tekintsük P centrumát, válasszunk benne egy z p-edrendű elemet. Ha lenne P-nek z-től

különböző p-edrendű eleme, akkor ők ketten elemi Abel-csoportot generálnának. ■

2.3.6 Tétel:
A Frobenius-mag egyértelmű.
Bizonyítás:
Legyen G Frobenius-csoport, N és M pedig különböző G-beli Frobenius-magok.
Tegyük fel, hogy mind N-nek van M-en kívül eső eleme, mind M-nek van N-en kívül eső eleme. Legyen $n \in N \setminus M$. Mivel M Frobenius-mag, n pedig rajta kívül eső elem, így $|M| = |n^M|$. N normálosztó, így tartalmazza $1 \neq n$ összes konjugáltját és az egységelemet is, emiatt $|M| < |N|$. Hasonlóképpen belátható, hogy $|N| < |M|$, ami ellentmondás. Tehát, ha N és M Frobenius-magok, akkor az egyik tartalmazza a másikat.
Jelölje a továbbiakban N a G Frobenius-csoport legnagyobb Frobenius-magját, egy hozzátartozó komplementum legyen A. Tegyük fel, hogy létezik egy N-től különböző M mag ($M < N$) B komplementummal. Mivel B konjugáltjai partícionálják $G \setminus M$-et, így $\exists g \in G : B^g \cap A > 1$. Legyen $B_0 = B^g$, tudjuk, hogy B_0 is megfelelő Frobenius-komplementum M-hez. Vegyük észre, hogy $A \cap B_0$ is egy Frobenius-komplementum, hisz $(A \cap B_0) \cap (A \cap B_0)^g = (A \cap A^g) \cap (B_0 \cap B_0^g) = 1 \quad \forall g \in G \setminus (A \cap B_0)$ esetén, ugyanis $G \setminus (A \cap B_0) = (G \setminus A) \cup (G \setminus B_0)$. Mivel $M < N$, így $A \cap B_0 < B_0$, hisz $B_0 \nsubseteq A$. Természetesen $A \cap B_0$ B_0-ban is rendelkezik a komplementumot definiáló tulajdonsággal, így B_0 Frobenius-csoport. Mivel B_0 komplementum is, ellentmondásra jutottunk. Tehát N az egyetlen Frobenius-mag.■

2.3.7 Következmény:
A Frobenius-komplementum konjugáltság erejéig egyértelmű.
Bizonyítás:
Legyen G Frobenius-csoport, és N az egyértelmű mag. Ha A és B különböző komplementumok, melyek nem konjugáltak, akkor, akárcsak az előző bizonyításban $1 < A \cap B^g < A$ valamely $g \in G$-re, és $A \cap B^g$ Frobenius-komplementum G-ben. Ekkor $A \cap B^g$ Frobenius-komplementum A-ban, ez pedig ellentmondás.■

2.3.8 Tétel:
Legyen P olyan p-csoport (p prím), amely pontosan egy p-edrendű részcsoportot tartalmaz. Ekkor vagy $p > 2$ és P ciklikus, vagy $p = 2$ és P ciklikus vagy általánosított kvaterniócsoport.

2.3.9 Következmény:
Egy A Frobenius-komplementum Sylow-részcsoportjai ciklikusak vagy általánosított kvaterniócsoportok.
Bizonyítás:
A 2.3.5 Következményből és a 2.3.8 Tételből világos az állítás.■

2.3.10 Megjegyzés:
(i) Ha egy Abel-csoport összes Sylow-részcsoportja ciklikus, akkor a csoport ciklikus, hisz a Sylowok generáló elemeinek szorzata generálja a csoportot.
(ii) Ha egy Frobenius-komplemetum Abel-csoport, akkor ciklikus.
(iii) Ha egy Frobenius-komplementum páratlan rendű vagy 2-Sylowjai ciklikusak, akkor feloldható.

2.3.11 Tétel:
Legyen G véges csoport, P pedig egy ciklikus p-Sylowja (p G rendjének prímosztója). Ekkor p $|G'|$ és $|G : G'|$ közül pontosan az egyiket osztja.
Bizonyítás:
A Fitting-tételben (1.1.6 Tétel (iii) pontja) szereplő direkt szorzat felbontás egyik tagja a kommutátor-részcsoporthoz, míg másik tagja Burnside tételén (1.3.3 Tétel) keresztül a G egy faktorához kötődik. Ezt az észrevételt fogjuk kihasználni a következőkben.
Legyen $N = \mathrm{N}_G(P)$. A Schur-Zassenhaus-tétel a P N-beli normálosztóra alkalmazva garantálja, hogy N-nek legyen K normál p-komplementuma. Fitting tétele miatt $P = \mathrm{C}_P(K) \times [P, K]$, hisz K a konjugálás által hat P-n. Mivel P-nek pontosan egy p-edrendű részcsoportja van, és ezt a direkt szorzatban szereplő tényezők közül csak az egyik tartalmazhatja, így a másik csak a triviális csoport lehet.
Ha $P = \mathrm{C}_P(K)$, akkor $N = P \times K$, így $\mathrm{C}_G(P) = \mathrm{N}_G(P)$, tehát alkalmazhatjuk Burnside normál p-komplementum tételét. Létezik egy $M \lhd G$ normálosztó, hogy $G/M \cong P$. Mivel P ciklikus, ezért $G' \leq M$, ekkor azonban p nem oszthatja G' rendjét.
Ha $P = [P, K]$, akkor $P \leq G'$, ezért p nem osztja $|G : G'|$-t.■

2.3.12 Tétel:
Ha egy G véges csoport összes Sylow-részcsoportja ciklikus, akkor G/G' és G' is ciklikus, és a rendjeik relatív prímek.
Bizonyítás:
Az előző tétel miatt világos, hogy G/G' és G' rendjeik relatív prímek.
Mivel G-Sylow részcsoportjai ciklikusak, így a G/G' Abel-csoport Sylow-részcsoportjai is ciklikusak, ezért G/G' ciklikus.
G' ciklikusságának bizonyításához indukciót alkalmazunk G rendje szerint. A legkisebb néhány rendre nyilvánvalóan teljesül az állítás. Az 1.3.5 Következmény szerint G feloldható, így $G' < G$. A tétel első fele alapján G'/G'' ciklikus, ezért elég megmutatni, hogy $G'' \leq \mathrm{Z}(G')$. Ugyanis, ha egy csoportnak a centruma egy részcsoportjával vett faktora ciklikus, akkor a csoport Abel. Olyan Abel-csoport, melynek minden Sylow-részcsoportja ciklikus maga is ciklikus.
Az indukciós feltevés szerint G'' ciklikus, így az 1.3.4 Állítás szerint $\mathrm{Aut}(G'')$ Abel-csoport. Mivel $G/\mathrm{C}_G(G'')$ izomorfikusan be van ágyazva $\mathrm{Aut}(G'')$-be, így Abel-csoport. Ekkor azonban $G' \leq \mathrm{C}_G(G'')$. G'' elemei kommutálnak minden G'-beli elemmel, így $G'' \leq \mathrm{Z}(G')$, és épp ezt akartuk.■

2.3.13 Következmény:
Ha egy A Frobenius-komplementum páratlan rendű, vagy páros rendű és a 2-Sylowja ciklikus, akkor A' és A/A' ciklikusak és relatív prím rendűek.
Bizonyítás:
A 2.3.9 Következményből és a 2.3.12 Tételből adódik.■

2.3.14 Tétel:
Ha egy A Frobenius-komplementum páratlan rendű, vagy páros rendű és a 2-Sylowja ciklikus, akkor A rendjének minden p prímosztójára A pontosan egy p-edrendű részcsoportot tartalmaz.
Bizonyítás:
Legyen r A rendjének olyan prímosztója, amely osztja A' rendjét is. A 2.3.13 Következmény szerint, ekkor r nem osztja A/A' rendjét. Így A' tartalmaz egy r-Sylowot, ezért minden r-edrendű csoport A'-ben fekszik. Mivel A' ciklikus, ezért egyetlen egy r-edrendű csoport van A'-ben, így A-ban is. Az egyetlen r-rendű csoport természetesen normálosztó.
Legyen q A rendjének olyan prímosztója, amely nem osztja A' rendjét. A 2.3.13 Következmény

szerint A/A' ciklikus, így pontosan egy q-adrendű részcsoportja van. Vegyük ennek természetes homomorfizmus általi ősét, B-t. A minden q-adrendű részcsoportja része B-nek (hisz a természetes homomorfizmusnál vett képe része B képének). Választva közülük egy tetszőleges Q részcsoportot kapjuk, hogy $B = A'Q$. Minden q-adrendű részcsoport $A'Q$-ban fekszik, és a csoportrendek miatt $Q \in Syl_q(A'Q)$. Elegendő megmutatnuk, hogy $Q \lhd A'Q$.
A 2.3.13 Következmény miatt A' ciklikus, így Fitting-tétele (1.1.6 Tétel (iii) pontja) miatt $A' = \mathrm{C}_{A'}(Q) \times [A', Q]$. Belátjuk, hogy $|A'|$ minden r prímosztójára, az egyetlen R r-edrendű részcsoport centralizálja Q-t, ezért $[A', Q] = 1$. Ebből már következik, hogy $Q \lhd A'Q$.
Mivel $R \lhd A$, így RQ rq-adrendű csoport. Ez a 2.3.5 Következmény értelmében ciklikus, így $R \leq \mathrm{C}_{A'}(Q)$. Ezzel a bizonyítást befejeztük.■

3. fejezet

Frobenius-csoportok karakterei

A karakterelmélet születésétől fogva szorosan kötődik a Frobenius-csoportok elméletéhez. Egyik első alkalmazásaként maga Frobenius bizonyította, hogy a komplementum konjugáltjain kívül eső elemek normálosztót alkotnak, a Frobenius-magot. Ennek a tételnek ma sem ismert a karakterelméletet nélkülöző elemi bizonyítása.
Egy csoport Frobenius volta a karakterekre is erős korlátozásokat hordoz magában. Ezt vizsgáljuk a fejezet második felében.

3.1. Frobenius tétele

Ebben a részben a témánk szempontjából kiemelkedő jelentőségű Frobenius-tételt bizonyítjuk. A bizonyítást Isaacs Character Theory of Finite Groups című könyve [4] alapján végezzük.

3.1.1 Tétel: (Frobenius reciprocitás)
Legyen G véges csoport, $H \leq G$, φ osztályfüggvény H-n, θ osztályfüggvény G-n. Ekkor $[\varphi^G, \theta]_G = [\varphi, \theta \mid_H]_H$.

3.1.2 Következmény:
Legyen G véges csoport, $H \leq G$. Ekkor, ha φ karaktere H-nak, akkor φ^G karaktere G-nek.

3.1.3 Lemma:

Legyen G Frobenius-csoport A komplementummal. θ legyen osztályfüggvény A-n, és $\theta(1)=0$. Ekkor $\theta^G\mid_A=\theta$.

Bizonyítás:

Mivel $\theta(1)=0$, így $\theta^G(1)=0$ nyilvánvaló. Legyen $1\neq a\in A$, ekkor $\theta^G(a)=\frac{1}{|A|}\sum\limits_{x\in G}\theta^0(xax^{-1})=\frac{1}{|A|}\sum\limits_{x\in A}\theta^0(xax^{-1})=\frac{1}{|A|}\sum\limits_{x\in A}\theta(a)=\theta(a)$.■

2.1.3 Tétel:(Frobenius-tétel)

Legyen G Frobenius-csoport A Frobenius-komplementummal. Ekkor $N=(G\setminus\bigcup\limits_{g\in G}A^g)\cup\{1\}$ normálosztó, melyet Frobenius-magnak nevezünk.

Bizonyítás:

A Frobenius-komplementumról kiindukált karakterek magjainak metszeteként előállítjuk a Frobenius-magot.

Legyen $\varphi\in\mathrm{Irr}A$ A egy nemtriviális irreducibilis karaktere, és $\theta=\varphi-\varphi(1)1_A$. θ-ra teljesülnek a 3.1.3 Lemma feltételei, ezért $[\theta^G,\theta^G]_G=[\theta,\theta^G\mid_A]_A=[\theta,\theta]_A=1+\varphi(1)^2$. Mivel $[\theta^G,1_G]_G=[\theta,1_A]_A=-\varphi(1)$, így $\theta^G=\varphi^*-\varphi(1)1_G$, ahol vagy φ^* vagy $-\varphi^*$ irreducibilis karaktere G-nek. Legyen a tetszőleges A-beli elem, ekkor $\varphi^*(a)=\theta^G(a)+\varphi(1)=\theta(a)+\varphi(1)=\varphi(a)$. Ezért $\varphi^*(1)=\varphi(1)$, így $\varphi^*\in\mathrm{Irr}G$.

Legyen $M=\bigcap\limits_{\substack{\varphi\in\mathrm{Irr}A\\ \varphi\neq 1_A}}\ker\varphi^*$. Belátjuk, hogy $M=N$.

Ha $x\in M\cap A$, akkor $\varphi(x)=\varphi^*(x)=\varphi^*(1)=\varphi(1)$, ahol az első és utolsó egyenlőség $\varphi^*(a)=\varphi(a)\quad(\forall a\in A)$ miatt, míg a középső $x\in M\subseteq\ker\varphi^*$ miatt áll fenn. Tehát $x\in\bigcap\limits_{\varphi\in\mathrm{Irr}A}\ker\varphi=1$, azaz $M\cap A=1$. Mivel M normálosztó, így A összes konjugáltjával is csak az egységelemben metszik egymást, ami mutatja, hogy $M\subseteq N$.

Ha $n\in N$, akkor $0=\theta^G(n)=\varphi^*(n)-\varphi(1)\quad(1_A\neq\varphi\in\mathrm{Irr}A)$, ahol az első egyenlőség igaz, mert N elemei nem konjugáltak A elemeivel. Tehát $\varphi^*(n)=\varphi(1)=\varphi^*(1)$, ezért $n\in\ker\varphi^*\quad(\forall\, 1_A\neq\varphi\in\mathrm{Irr}A)$, $N\subseteq M$.

Ezek szerint $N=M\lhd G$.■

3.2. Frobenius-csoportok karakterei

Megmutatjuk, miként konstruálhatóak meg Frobenius-csoportok karakterei a mag és a komplementum karaktereinek ismeretében. Az ehhez kapcsolódó tételt először Frobenius bizonyította. Ezt követően egy új, karakterelméleten alapuló jellemzését adjuk Frobenius-csoportoknak. A megfelelő tétel először Kuisch és van der Wall cikkében szerepel [7].
Az alfejezetben található bizonyítások önálló munkán alapulnak. Kivételt képez ez alól a 3.2.4 Tétel, ez megtalálható [4]-ben (a 3.2.5 Lemma pedig ekvivalens egy jól ismert állítással).

3.2.1 Definíció:
Legyen G véges csoport, $N \trianglelefteq G$, θ osztályfüggvény N-en. A $\theta^g : N \mapsto \mathbb{C}$, $\theta^g(h) = \theta(ghg^{-1})$ osztályfüggvényt θ konjugáltjának nevezzük. Ha $\varphi \in \mathrm{Irr}N$, akkor a $\{\varphi^g \mid g \in G\} \subseteq \mathrm{Irr}N$ halmazt φ konjugált osztályának nevezzük.

3.2.2 Megjegyzés:
Ha G véges csoport, $N \trianglelefteq G$, akkor a konjugáltság ekvivalencia reláció $\mathrm{Irr}N$-en.

3.2.3 Tétel:
Frobenius-csoportok irreducibilis karaktereit megkapjuk a magról kiindukált (nemtriviális) irreducibilis karakterek, és a komplementum irreducibilis karaktereinek megfelelő karakterek összességeként. (Utóbbi alatt olyan karaktereket értünk, melyek magja tartalmazza a Frobenius-magot, a komplementumra való megszorítása pedig annak egy irreducibilis karakterét adja.)
Bizonyítás:
Legyen $G = N \rtimes A$ Frobenius-csoport, ahol N a Frobenius-mag, A pedig a komplementum. Jelölje k_N, k_A N és A, mint absztrakt csoportok, konjugált osztályainak számát.
$1 \neq a \in A$ esetén aN elemei egy konjugált osztályba tartoznak (2.1.9 Állítás). Mivel $G \setminus N$ minden eleme an alakú ($1 \neq a \in A, n \in N$), így $G \setminus N \cup \{1\}$ k_A G-beli konjugált osztályt tartalmaz. Épp ennyien vannak a komplementum irreducibilis karaktereinek megfelelő karakterek.
G $N \setminus \{1\}$-beli konjugált osztályai $\bigcup\limits_{a \in A} \mathcal{C}_N^a$ alakúak, ahol $\mathcal{C}_N$ a megfelelő N-beli konjugált osztályt jelöli. Mivel $a_1 \neq a_2$ esetén $n^{a_1} \neq n^{a_2}$ ($a_1, a_2 \in A, 1 \neq n \in N$), ezért $|A|$ darab N-beli konjugált osztály olvad össze egy G-belivé. Így $N \setminus \{1\}$ $\frac{k_N - 1}{|A|}$ darab G-beli konjugált osztályt tartalmaz. Megmutatjuk, hogy $\mathrm{Irr}N$ nemtriviális karaktereinek kiindukáltjai épp ennyien vannak.

Tekintsük φ^G-t ($\varphi \in \mathrm{Irr}N \setminus \{1_N\}$). $x \in N$ esetén

$$\varphi^G(x) = |C_G(x)| \sum \frac{\varphi(x_i)}{|C_N(x_i)|} = \sum \varphi(x_i) = \sum_{a \in A} \varphi(a^{-1}xa) = \sum_{\psi \epsilon \mathcal{C}_\varphi} n_\psi \psi(x)$$

x G-beli konjugált osztálya N-ben felbomlik, x_i ezeknek egy-egy reprezentánsa; $\mathcal{C}_\varphi$ jelöli φ konjugált osztályát; n_ψ pedig a megfelelő konjugált osztálybeli elem együtthatója. $|C_G(x)| = |C_G(x_i)| = |C_N(x_i)|$, mivel a csoport Frobenius (2.1.10 Tétel). Ha pedig $x \in G \setminus N$, akkor $\varphi^G(x) = 0$.

Látható, hogy minden konjugált osztályhoz tartozik (legalább) egy indukált karakter. A különböző konjugált osztályhoz tartozóak merőlegesek egymásra, és az A irreducibilis karaktereiből származó karakterekre is.

$$[\varphi^G, \psi^G]_G = \frac{1}{|G|} \sum_{x \in G} \varphi^G(x) \overline{\psi^G(x)} = \frac{1}{|G|} \sum_{x \in N} \varphi^G(x) \overline{\psi^G(x)} = \frac{1}{|G|} \sum_{x \in N} (\sum_{\widetilde{\varphi} \in \mathcal{C}_\varphi} n_{\widetilde{\varphi}} \widetilde{\varphi}(x)) \overline{(\sum_{\widetilde{\psi} \in \mathcal{C}_\psi} n_{\widetilde{\psi}} \widetilde{\psi}(x))} =$$

$$\frac{|N|}{|G|} \sum_{\widetilde{\varphi} \in \mathcal{C}_\varphi} \sum_{\widetilde{\psi} \in \mathcal{C}_\psi} n_{\widetilde{\varphi}} n_{\widetilde{\psi}} [\widetilde{\varphi}, \widetilde{\psi}]_N = 0$$

$$[\varphi^G, \chi]_G = [\varphi, \chi|_N]_N = \chi(1)[\varphi, 1_N]_N = 0$$

ahol φ, ψ $\mathrm{Irr}N$ nemtriviális elemei (melyekhez különböző konjugált osztály tartozik), χ pedig egy $\mathrm{Irr}A$-beli elemnek megfelelő karakter. Az indukált karakterek merőlegessége miatt legfeljebb $\frac{k_N - 1}{|A|}$ lehet belőlük. Ez csak úgy lehetséges, ha minden konjugált osztályban $|A|$ darab karakter van, és így mindegyik $n_\varphi = 1$. Hiszen $\mathrm{Irr}N \setminus \{1_N\}$-nek $k_N - 1$ eleme van, és $G = N \rtimes A$ miatt egy konjugált osztályban legfeljebb $|A|$ elem lehet. Ekkor:

$$[\varphi^G, \varphi^G]_G = \frac{1}{|G|} \sum_{x \in G} \varphi^G(x) \overline{\varphi^G(x)} = \frac{1}{|G|} \sum_{x \in N} \varphi^G(x) \overline{\varphi^G(x)} = \frac{1}{|G|} \sum_{x \in N} (\sum_{\psi \in \mathcal{C}_\varphi} \psi(x)) \overline{(\sum_{\chi \in \mathcal{C}_\varphi} \chi(x))} =$$

$$\frac{1}{|G|} \sum_{\psi \in \mathcal{C}_\varphi} \sum_{\chi \in \mathcal{C}_\varphi} (\sum_{x \in N} \psi(x) \overline{\chi(x)}) = \frac{1}{|G|} \sum_{\psi \in \mathcal{C}_\varphi} |N| [\psi, \psi]_N = \frac{|A||N|}{|G|} = 1$$

Tehát a Frobenius-magról kiindukált nemtriviális irreducibilis karakterek épp a hiányzó $\frac{k_N - 1}{|A|}$ irreducibilis karaktert adják. Ezzel a bizonyítást befejeztük.■

3.2.4 Tétel: (Clifford)

Legyen G véges csoport, $N \trianglelefteq G$, $\chi \in \mathrm{Irr}G$. Legyen θ $\chi\mid_N$ $\mathrm{Irr}N$-beli elemekkel való felírásának egy nemnulla együtthatós tagja (azaz θ irreducibilis konstituense $\chi\mid_N$-nek), és $\theta = \theta_1, \theta_2, ..., \theta_t$ θ konjugált osztályának összes eleme. Ekkor $\chi\mid_N = e \sum_{i=1}^{t} \theta_i$, ahol $e = [\chi\mid_N, \theta]_N$.

Bizonyítás:
Tekintsük θ^G-t. Legyen $n \in N$, ekkor $\theta^G(n) = \frac{1}{|N|}\sum_{x\in G}\theta^0(xnx^{-1}) = \frac{1}{|N|}\sum_{x\in G}\theta^x(n)$. Tehát $\theta^G \mid_N = \frac{1}{|N|}\sum_{x\in G}\theta^x$. Tegyük fel, hogy $\varphi \in \mathrm{Irr}N$ nincs benne θ konjugált osztályában, ekkor $0 = [\frac{1}{|N|}\sum_{x\in G}\theta^x, \varphi]_N = [\theta^G \mid_N, \varphi]_N = [\theta^G, \varphi^G]_G$. Mivel $[\chi \mid_N, \theta]_N = [\chi, \theta^G]_G$, azaz χ irreducibilis konstituense θ^G-nek, ezért $0 = [\chi, \varphi^G]_G = [\chi \mid_N, \varphi]_N$. Tehát $\chi \mid_N$ irreducibilis karakterekkel való felírásában csak θ konjugáltjai szerepelhetnek: $\chi \mid_N = \sum_{i=1}^{t}[\chi \mid_N, \theta_i]_N\theta_i$. Egyszerű számolás mutatja, hogy $[\chi \mid_N, \theta^x]_N = [(\chi \mid_N)^x, \theta^x]_N = [\chi \mid_N, \theta]_N \quad (\forall x \in G)$, ebből pedig adódik a tétel állítása.■

3.2.5 Lemma:
Legyen G véges csoport. Ekkor nem létezik olyan $H < G$ valódi részcsoport, amely G minden konjugált osztályába belemetsz.
Bizonyítás:
A lemma ekvivalens azzal az ismert állítással, hogy $H < G$ valódi részcsoport konjugáltjainak uniója nem fedheti le G-t. Tegyük fel, hogy $\bigcup_{g\in G} H^g = G$. H-nak $|G : N_G(H)|$ darab különböző konjugáltja van, és ezek nem lehetnek diszjunktak, hisz az egységelemet, mindegyikük tartalmazza. Emellett $H \leq N_G(H)$. Így $|G| = |\bigcup_{g\in G} H^g| < |H||G : N_G(H)| \leqq |H||G : H| = |G|$, ami ellentmondás.■

3.2.6 Tétel:
Legyen $N < G$ olyan nemtriviális valódi részcsoport, hogy N minden nemtriviális irreducibilis karakterét kiindukálva G irreducibilis karakterét kapjuk. Ekkor G Frobenius-csoport.
Bizonyítás:
A bizonyítást három lépésben végezzük. Először megmutatjuk, hogy G-nek az indukált karaktereken kívül van más irreducibilis karaktere is. Ezután belátjuk, hogy a kiindukált karakterektől különböző irreducibilis karakterek magjainak metszetére kiindukálva N nemtriviális irreducibilis karaktereit, továbbra is irreducibilis karaktereket kapunk. Végül bebizonyítjuk, hogy csak úgy lehet G irreducibilis karaktereinek száma egyenlő a konjugált osztályainak számával, ha G Frobenius.

Bevezetünk néhány jelölést. $\mathrm{Irr}H^\times$ legyen $H \leq G$ nemtriviális irreducibilis karaktereinek halmaza, $(\mathrm{Irr}{H_1}^\times)^{H_2}$ pedig H_2 $(H_1 \leq H_2 \leq G)$ olyan karaktereit jelölje, amiket $\mathrm{Irr}{H_1}^\times$ elemeinek indukálásával kapunk. $\mathcal{CC}_{H_2}(H_1)$ $(H_1 \trianglelefteq H_2 \leq G)$ legyen H_1 H_2-beli konjugált osztályainak a száma, $\mathcal{C}_H(x)$ $(x \in H \leq G)$ pedig x H-beli konjugált osztálya.

Ha $(\mathrm{Irr}N^\times)^G \cup \{1_G\}$ G minden irreducibilis karakterét kiadná, akkor N-nek G összes konjugált osztályába bele kellene metszenie, különben lenne egy konjugált osztály, amin minden nemtriviális irreducibilis karakter 0-át venne fel. Ez viszont a második ortogonalitási reláció miatt lehetetlen. A 3.2.5 Lemma értelmében semely csoportnak sem lehet olyan részcsoportja, ami minden konjugált osztályba belemetsz, így léteznek $(\mathrm{IrrN}^\times)^G$ elemeitől különböző nemtriviális irreducibilis karakterek.

$\chi \in \mathrm{Irr}G \setminus (IrrN^\times)^G$ esetén $\chi\mid_N = \chi(1)1_N$. Ugyanis $0 = [\chi, \varphi^G]_G = [\chi\mid_N, \varphi]_N$ $(\forall \varphi \in \mathrm{Irr}N^\times)$, mivel $\chi\mid_N$ osztályfüggvény N-en és merőleges az összes N-beli nemtriviális karakterre, így csak az 1_N skalárszorosa lehet, ebből pedig adódik az állítás. Legyen $M = \bigcap\limits_{\chi \in \mathrm{Irr}G \setminus (\mathrm{Irr}N^\times)^G} \ker\chi$, ekkor $M \lhd G$ és $N \leq M$.
Clifford tétele szerint $\varphi^G\mid_M = e\sum\limits_{i=1}^{t}\theta_i$, ahol e pozitív egész, θ_i-k különböző konjugált $\mathrm{Irr}M$-beli elemek, φ pedig N nemtriviális irreducibilis karaktere. $[\varphi^G\mid_M, \varphi^M]_M = [\varphi^G, (\varphi^M)^G]_G = [\varphi^G, \varphi^G]_G = 1$, és mivel $e \mid [\varphi^G\mid_M, \varphi^M]$, így $e = 1$ adódik. $M \lhd G$, ezért $\varphi^G = (\varphi^M)^G$ minden M-en kívül eső elemen eltűnik. $1 = [\varphi^G, \varphi^G]_G = \frac{|M|}{|G|}[\varphi^G\mid_M, \varphi^G\mid_M]_M$, tehát $[\varphi^G\mid_M, \varphi^G\mid_M]_M = |G:M|$, $t = |G:M|$ teljesül. θ-nak legfeljebb $|G:M|$ konjugáltja lehet, hisz M-nek ennyi mellékosztálya van, és azonos mellékosztálybeli elemekkel konjugálva θ-t ugyanazt a karaktert kapjuk.
Rendeljük φ^G-hez $(\varphi \in \mathrm{Irr}N^\times)$ azt a ($|G:M|$ elemű) konjugált osztályát $\mathrm{Irr}M^\times$-nek, amelynek összegeként előáll M-re vett megszűkítése. Minden $\theta \in \mathrm{Irr}M^\times$ benne van valamely φ^G-hez $(\varphi \in \mathrm{Irr}N^\times)$ rendelt konjugált osztályban. Hiszen van olyan G-beli irreducibilis karakter, amivel θ^G skalárszorzata nem 0, de $\chi \in \mathrm{Irr}G \setminus (\mathrm{Irr}N^\times)^G$-ra $[\chi, \theta^G]_G = [\chi\mid_M, \theta]_M = \chi(1)[1_M, \theta] = 0$. Így a φ^G karakterekhez $(\varphi \in \mathrm{Irr}N^\times)$ rendelt konjugált osztályok és $\{1_M\}$ partícionálják $\mathrm{Irr}M$-et.
Belátjuk, hogy φ^M $(\varphi \in \mathrm{Irr}N^\times)$ θ-ákkal $(\theta \in \mathrm{Irr}M)$ való egyértelmű felírásban a fenti partíciónak csak egy halmazából szerepelhetnek elemek, onnan is pontosan 1 darab 1 együtthatóval, így φ^M irreducibilis. Rögzítsünk egy $\varphi \in \mathrm{Irr}N^\times$ elemet. $[\varphi^M, 1_M]_M = 0$, ugyanis tetszőleges $\chi \in \mathrm{Irr}G \setminus (\mathrm{Irr}N^\times)^G$-re $0 = [\varphi^G, \chi]_G = [(\varphi^M)^G, \chi]_G = [\varphi^M, \chi\mid_M]_M = \chi(1)[\varphi^M, 1_M]$. Ha ψ^G-hez $(\psi \in \mathrm{Irr}N^\times)$ és φ^G-hez különböző $\mathrm{Irr}M$-beli konjugált osztályok tartoznak, akkor $\psi^G \neq \varphi^G$, így $0 = [\varphi^G, \psi^G]_G = [\varphi^M, \psi^G\mid_M]_M$, tehát φ^M-nek nincs ψ^G konjugált osztályából összetevője. Végül $1 = [\varphi^G\mid_M, \varphi^M]_M$ miatt $\varphi^M = \theta$ valamely φ^G konjugált osztályához tartozó θ-ra, így φ^M irreducibilis.

Mivel azonos Irr$M$-beli konjugált osztályhoz tartozó elemekről kiindukálva ugyanazt a G-beli karaktert kapjuk, így Irr$M$ elemeire is fennáll a tételben megfogalmazott feltétel. Dolgozzunk a továbbiakban velük.
$\mathcal{CC}_G(M) - 1 \geqq \frac{\mathcal{CC}_M(M)-1}{|G:M|}$, hiszen legfeljebb $|G : M|$ M-beli nemtriviális konjugált osztály olvadhat össze egy G-belivé (M azonos mellékosztályába tartozó elemekkel konjugálva ugyanazt a konjugált osztályt kapjuk). Mivel az azonos ($|G : M|$ elemű) konjugált osztályba tartozó $\theta \in \mathrm{Irr}M^{\times}$-ekről kiindukálva ugyanazt az irreducibilis karaktert kapjuk, és egy csoportnak annyi konjugált osztálya van ahány irreducibilis karaktere, így $\mathcal{CC}_G(M) - 1 \geqq |(\mathrm{IrrM}^{\times})^G|$.
$G \setminus M \cup \{1\}$-ben legalább annyi konjugált osztály van, mint G/M-ben, ugyanis a természetes homomorfizmus epimorfizmus, konjugált osztályt konjugált osztályba visz, és az egész M-et az egységbe képezi. Mivel Irr$G \setminus (\mathrm{Irr}M^{\times})^G$ elemeit egyértelműen megfeleltethetjük IrrG/M elemeinek, így előbbi legfeljebb annyi elemet tartalmaz, mint, ahány konjugált osztály van $G \setminus M \cup \{1\}$-ben, azaz $\mathcal{CC}_G(G) - \mathcal{CC}_G(M) + 1 \geqq |\mathrm{Irr}G \setminus (\mathrm{Irr}M^{\times})^G|$. Mivel G-nek annyi konjugált osztálya van ahány irreducibilis karaktere, így mindkét levezetett egyenlőtlenségben egyenlőségnek kell teljesülnie.
Az első egyenlőtlenségben csak úgy állhat fenn egyenlőség, ha minden $M \setminus \{1\}$ által tartalmazott G-beli konjugált osztály pontosan $|G : M|$ darab M-beli konjugált osztályt foglal magában (ezek a konjugált osztályok azonos méretűek kell, hogy legyenek, hisz egyik a másiknak automorfizmus általi képe). Tehát $x \in M$ esetén $|G : M| = \frac{|\mathcal{C}_G(x)|}{|\mathcal{C}_M(x)|} = |G : M|\frac{|\mathrm{C}_M(x)|}{|\mathrm{C}_G(x)|}$, azaz $|\mathrm{C}_M(x)| = |\mathrm{C}_G(x)|$. Ez pedig csak úgy teljesülhet, ha $\mathrm{C}_M(x)=\mathrm{C}_G(x)$ ($\forall x \in M$), tehát a csoport a 2.1.10 Tétel alapján Frobenius.■

3.2.7 Példa:
Példa gyanánt megadjuk két alacsony rendű Frobenius-csoport karaktertábláját. Ezeken is jól megfigyelhetőek a fejezetben megfogalmazott állítások.
(i) A D_5 karaktertáblája
$\mathrm{D}_5 = \langle t, f | f^5 = 1,\ t^2 = 1,\ f^t = f^{-1}\rangle$
$\mathcal{C}_1 = \{1\}$, $\mathcal{C}_t = \{t, tf, tf^2, tf^3, tf^4\}$, $\mathcal{C}_f = \{f, f^4\}$, $\mathcal{C}_{f^2} = \{f^2, f^3\}$.

(ii) Az Aff(5) karaktertáblája
$\mathrm{Aff}(5) = \{x \mapsto \alpha x + b | \alpha, b \in \mathrm{GF}(5), \alpha \neq 0\} = \{(\alpha, b) | \alpha, b \in \mathrm{GF}(5),\ \alpha \neq 0\}$
$\mathcal{C}_1 = \{1\}$, $\mathcal{C}_{\alpha=1} = \{(1, b) | b \neq 0\}$, $\mathcal{C}_{\alpha=2} = \{(2, b)\}$, $\mathcal{C}_{\alpha=3} = \{(3, b)\}$, $\mathcal{C}_{\alpha=4} = \{(4, b)\}$.

D_5	$\mathcal{C}_1$	$\mathcal{C}_t$	$\mathcal{C}_f$	$\mathcal{C}_{f^2}$
1	1	1	1	1
λ	1	-1	1	1
χ	2	0	$-\frac{1+\sqrt{5}}{2}$	$-\frac{1-\sqrt{5}}{2}$
ψ	2	0	$-\frac{1-\sqrt{5}}{2}$	$-\frac{1+\sqrt{5}}{2}$

3.1. táblázat. A D_5 karaktertáblája

Aff(5)	$\mathcal{C}_1$	$\mathcal{C}_{\alpha=1}$	$\mathcal{C}_{\alpha=2}$	$\mathcal{C}_{\alpha=3}$	$\mathcal{C}_{\alpha=4}$
1	1	1	1	1	1
λ_1	1	1	-1	-1	1
λ_2	1	1	i	$-i$	-1
λ_3	1	1	$-i$	i	-1
χ	4	-1	0	0	0

3.2. táblázat. Az Aff(5) karaktertáblája

3.2.8 Megjegyzés:

Meggondolható, hogy Aff(p) (p prím) karaktertáblái hasonló szerkezetűek, mint a példában szereplő Aff(5) karaktertáblája.

A mag (az eltolások) egy konjugált osztályt alkotnak. Aff(p) elsőfokú irreducibilis karakterei a magon 1-et vesznek fel, különben megfelelnek Z_{p-1} irreducibilis karaktereinek. Továbbá létezik egy $(p-1)$-edfokú irreducibilis karakter, amely a magon -1-et vesz fel, különben pedig 0-t.

4. fejezet

A Frobenius-mag nilpotenciája

A Frobenius-csoportokkal kapcsolatban felmerülő egyik legfontosabb kérdés a mag nilpotenciájának eldöntése. A probléma igen sokáig nyitott volt, mielőtt Thompson megoldotta volna 1959-es híres Ph.D.-dolgozatában. A bizonyítás meglehetősen bonyolult volt. 1964-ben ennek egy egyszerűbb változatát publikálta a Journal of Algebra legelső számában, [8]. Ennek gondolatmenetét követjük végig a fejezetben Isaacs kiváló könyve [6] segítségével.

4.1. Néhány szó mátrixcsoportokról

Szükségünk lesz mátrixcsoportokkal kapcsolatos különböző ismeretekre, ezeket mutatjuk be alább. A rész végén egy a mátrixcsoportok p-Sylowjaival kapcsolatos fontos tétel is bizonyításra kerül.

4.1.1 Állítás:
Legyen p prím, f és n természetes számok, és $q = p^f$.
(i) $\mathrm{SL}(n,q) \lhd \mathrm{GL}(n,q)$ és $\mathrm{GL}(n,q)/\mathrm{SL}(n,q) \cong \mathrm{GF}(q)^*$
(ii) $|\mathrm{GL}(n,q)| = \prod\limits_{i=0}^{n-1}(q^n - q^i)$ és $|\mathrm{SL}(n,q)| = q^{n-1}\prod\limits_{i=0}^{n-2}(q^n - q^i)$
Bizonyítás:
(i) A $\det : \mathrm{GL}(n,q) \to \mathrm{GF}(q)^*$ epimorfizmus magja $\mathrm{SL}(n,q)$.
(ii) Egy lineáris leképezés pontosan akkor invertálható, ha oszlopvektorai függetlenek. Számoljuk le, hogy hányféleképpen választhatjuk meg az oszlopokat, úgy, hogy a függetlenség teljesüljön. Az elsőt $q^n - 1$-féleképp választhatjuk, hisz a nullvektoron kívül bármit választha-

tunk. A második vektor nem lehet benne az első lineáris burkában, ezért őt $q^n - q$-féleképpen választhatjuk. A harmadik nem lehet benne az első kettő lineáris burkában, ezért őt $q^n - q^2$-féleképpen választhatjuk. Az eljárást folytatva, és a kapcsolódó számolásokat elvégezve, kapjuk a kívánt eredményeket.■

4.1.2 Állítás:
Legyen $p > 2$ prím, f természetes szám, $q = p^f$. Az $\mathrm{SL}(2, q)$ csoportnak pontosan egy másodrendű eleme van, az egységmátrix -1-szerese, $-I$.
Bizonyítás:
Tegyük fel, hogy $t \in \mathrm{SL}(2, q)$ másodrendű és $t \neq -I$. Ekkor t gyöke a $p(x) = x^2 - 1$ polinomnak, de nem gyöke sem $x - 1$-nek, sem $x + 1$-nek. Tehát p t minimál polinomja. Mivel p foka 2, így p t karakterisztikus polinomja is. t sajátértékei tehát csak $+1$ és -1 lehetnek. Mivel $\det t = 1$, így a két sajátérték meg kell, hogy egyezzen. Ekkor azonban $t = I$ vagy $t = -I$, így ellentmondásra jutottunk.■

4.1.3 Következmény:
Legyen $p > 2$ prím, f természetes szám, $q = p^f$. Az $\mathrm{SL}(2, q)$ csoport 2-Sylowjai általánosított kvaterniócsoportok.
Bizonyítás:
A 4.1.2 Állítás és 2.3.8 Tétel alapján világos, hogy a 2-Sylow csak ciklikus vagy általánosított kvaternió lehet. Megmutatjuk, hogy $\mathrm{SL}(2, q)$-nak mindig van a kvaterniócsoporttal izomorf részcsoportja.
$K = \mathrm{GF}(q)$-ban léteznek a, b elemek, hogy $a^2 + b^2 = -1$. Tekintsük az $f(x) = x^2$ leképezést, ekkor $\mathrm{Im} f$-ben a 0-t leszámítva mindegyik elemnek két őse van, ezért $|\mathrm{Im} f| = \frac{q+1}{2}$. A skatulya-elv miatt találhatunk a, b K-beli elemeket, hogy $a^2 + 1 = -b^2$, azaz $a^2 + b^2 = 1$.
A fenti a és b segítségével definiáljuk a következő mátrixokat: $x = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$ és $y = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}$. Könnyen látható, hogy $y^4 = 1$, $x^2 = y^2$, $y^x = y^{-1}$. Mivel $|\langle x, y \rangle| \geqq 8$, így a Dyck-tétel miatt $\langle x, y \rangle \cong Q_{2^3}$ ($Q_{2^n} = \langle a, b | a^{2^{n-1}} = 1,\, b^2 = a^{2^{n-2}},\, a^b = a^{-1} \rangle$).■

4.1.4 Megjegyzés:
Egyszerű számolás mutatja, hogy $\mathrm{SL}(2,3) \cong Q_{2^3} \rtimes \mathrm{Z}_3$, és a szemidirekt szorzat izomorfia erejéig egyértelmű.

4.1.5 Lemma:
Legyen $p > 2$ prím, és jelölje G $\mathrm{GL}(2,p)$-t. Ha $P \leq G$ p-csoport, $L \leq G$ p'-csoport, továbbá $P \leq \mathrm{N}_G(L)$, és L 2-Sylowjai Abel-csoportok, akkor $P \leq \mathrm{C}_G(L)$.
Bizonyítás:
Indukciót alkalmazunk L rendje szerint. Ha L rendje 1 vagy 2, triviálisan teljesül az állítás.
Keresünk L-ben olyan valódi részcsoportokat, melyeket P normalizál, ekkor az indukciós feltevésünk szerint centralizálja is őket. Legyen q $|L : \mathrm{C}_L(P)|$ egy prímosztója. Az 1.1.5 Tétel miatt létezik $Q \in Syl_q L$ P-invariáns részcsoportja L-nek. Q-t P nem centralizálhatja, hisz Q rendjét q magasabb hatványa osztja mint $\mathrm{C}_L(P)$ rendjét. Ez csak úgy teljesülhet, ha Q L-nek nem valódi részcsoportja, azaz $L = Q$ q-csoport.
Az $[L,P]$ csoport nyilvánvalóan P-invariáns. Az indukciós feltevés miatt, ha $[L,P] < L$, akkor $[L,P,P] = 1$. Az 1.1.8 Tétel miatt, ekkor $1 = [L,P,P] = [L,P]$. Tehát $[L,P] < L$ esetén a lemma állítás teljesül. Ezért vizsgáljuk a továbbiakban azt az esetet, amikor $[L,P] = L$. Ekkor $L \leq G' \leq \mathrm{SL}(2,p)$.
Tegyük fel, hogy $q = 2$. Mivel $L \leq \mathrm{SL}(2,p)$, ezért L pontosan egy involúciót tartalmazhat a 4.1.2 Állítás szerint. A feltételeink szerint L Abel-csoport, így ciklikus. Ciklikus 2-csoport automorfizmusainak rendje az 1.3.4 Állítás szerint 2-hatvány, így P centralizálja L-et.
Feltehetjük tehát, hogy $q \neq 2$. Mivel $|\mathrm{SL}(2,p)| = p(p-1)(p+1)$ és a q prím $p-1$ és $p+1$ közül pontosan az egyiket osztja, továbbá $L \leq \mathrm{SL}(2,p)$, ezért $|L| \leqq p+1$. Ha a P p-csoport az L-en nemtriviálisan hat, akkor van egy legalább p számosságú orbitja. Ez az egységelemmel együtt L-nek legalább $p+1$ elemét adja. Tehát $|L| = p+1$, ami páros, így elletmondásra jutottunk.■

4.1.6 Tétel:
Legyen G véges csoport, $p > 2$ prím és $P \in Syl_p G$. Továbbá teljesüljenek az alábbi feltételek:
(i) G p-feloldható
(ii) G 2-Sylowjai Abel-csoportok
(iii) G hűségesen hat egy V p-csoporton
(iv) $|V : \mathrm{C}_V(P)| \leqq p$.
Ekkor $P \trianglelefteq G$.

Bizonyítás:

Tegyük fel, hogy létezik ellenpélda. Legyen G közülük olyan, melynek rendje minimális. Mivel $P \in Syl_p G$ ekkor nem normálosztó, így létezik G-nek egy tőle különböző $Q \in Syl_p G$ részcsoportja is. A $\langle P, Q \rangle$ csoport olyan részcsoportja G-nek, mely szintén teljesíti a tételben szabott feltételeket, és P, Q különböző p-Sylowok benne. G rendjének minimalitása miatt $G = \langle P, Q \rangle$.

A Sylow-tételek szerint létezik $g \in G$, hogy $P^g = Q$. Ezért $\mathrm{C}_V(Q) = \mathrm{C}_V(P^g) = \mathrm{C}_V(P)^g$, speciálisan $|V : \mathrm{C}_V(Q)| \leqq p$. Vegyük észre, hogy az indexük miatt $\mathrm{C}_V(P)$ és $\mathrm{C}_V(Q)$ is normálosztó V-ben. Tekintsük az $U = \mathrm{C}_V(P) \cap \mathrm{C}_V(Q)$ csoportot. $U \trianglelefteq V$, hisz normálosztók metszete. $U \leq \mathrm{C}_V(G)$, hisz U-t a G-t generáló P és Q is centralizálja. U indexe kisebb, mint p^2, $|V : U| = |V : \mathrm{C}_V(P)||\mathrm{C}_V(P) : \mathrm{C}_V(P) \cap \mathrm{C}_V(Q)| = |V : \mathrm{C}_V(P)||\mathrm{C}_V(P)\mathrm{C}_V(Q) : \mathrm{C}_V(Q)| \leqq p^2$.

U egy G-invariáns normálosztó V-ben, így nézhetjük G hatását V/U-n. Legyen ennek magja K, a hozzátartozó természetes homomorfizmust pedig jelöljük felülvonással. Belátjuk, hogy K p-csoport. K definíciója miatt $[V, K] \leq U$, és mivel U-n G triviálisan hat, így $[V, K, K] = 1$. Tegyük fel, hogy létezik K-nak p-től különböző prímosztója, r. Legyen $R \in Syl_r K$, ekkor $[V, R, R] = 1$, és az 1.1.8 Tétel miatt $[V, R] = [V, R, R] = 1$. Tehát R triviálisan hat V-n, ami ellentmond G hűségességének. K tehát p-csoport.

A tételben megfogalmazott első három feltétel nyilvánvalóan teljesül a $\overline{G}$, $\overline{P}$, V/U hármasra. A negyedik is teljesül, hisz $\overline{P}$ centralizálja $\mathrm{C}_V(P)/U$ elemeit. K p-normálosztó, ezért valódi része mindegyik p-Sylownak (hisz legalább 2 p-Sylow van). Így $\overline{P}$ és $\overline{Q}$ különböző $\overline{G}$-beli p-Sylowok. Csak akkor nem kapunk G-nél kisebb rendű ellenpéldát $\overline{G}$-sal, ha $K = 1$. G tehát hűségesen hat V/U-n. Jelölje W a továbbiakban V/U-t. Ekkor W-re is teljesülnek a tételben megfogalmazott feltételek, és $|W| \leqq p^2$.

Mivel G hűségesen hat W-n, így azonosíthatjuk $\mathrm{Aut}(W)$ egy részcsoportjával. Ha W ciklikus lenne, akkor az 1.3.4 Tétel miatt G Abel-csoport lenne, és így $P \trianglelefteq G$ teljesülne, ami ellentmondás. Tehát W a p^2 rendű elemi Abel-csoport, és G $\mathrm{GL}(2, p)$ részcsoportja. $|\mathrm{GL}(2, p)| = p(p-1)^2(p+1)$, így $|P| \leqq p$. Mivel P nem normálosztó, $\mathrm{O}_p(G) = 1$.

Legyen $L = \mathrm{O}_{p'}(G)$. Ekkor P normalizálja L-et, és mivel G 2-Sylowjai Abel-csoportok, így ez L-re is teljesül. Alkalmazhatjuk a 4.1.5 Lemmát, azaz P centralziálja L-et. G p-feloldható, így p'-szeparábilis, és $\mathrm{O}_p(G) = 1$. Teljesülnek a Hall-Higman Lemma feltételei, így $P \leq \mathrm{C}_G(L) \leq L$. P p-csoport, L pedig p'-csoport, ezért $P = 1 \lhd G$, ami ellentmondás.■

4.2. A Thompson-részcsoport

A Thompson-részcsoport egy adott p-csoport egy karakterisztikus részcsoportja. A Thompson-féle p-komplementum tételen keresztül, központi szerepet játszik a mag nilpotenciájával kapcsolatos vizsgálódásainkban. Ebben a fejezetben megismerkedünk definíciójával, alapvető tulajdonságaival. Majd zárásképpen, az önmagában is igen fontos, normál $\mathrm{J}(P)$-tételt bizonyítjuk. Utóbbi tétel egyik érdekes alkalmazása Burnside híres $p^a q^b$-tételének tisztán csoportelméleti eszközökkel történő bizonyítása.

4.2.1 Definíció:
Legyen P p-csoport (p prím). Jelölje $\mathcal{E}(P)$ a P-beli maximális rendű elemi Abel-csoportok halmazát. A $\mathrm{J}(P) = \langle \mathcal{E}(P) \rangle$ csoportot P Thompson-részcsoportjának nevezzük.

4.2.2 Megjegyzés:
(i) Az irodalomban a Thompson-részcsoportnak több nem ekvivalens definíciója is létezik. Maga Thompson sem ezt használta, hanem a P maximális rangú Abel-részcsoportjai által generált csoportot tekintette.
(ii) $\mathrm{J}(P) \operatorname{char} P$
(iii) $\mathrm{J}(P) \leq Q \leq P$ esetén $\mathrm{J}(Q) = \mathrm{J}(P)$.

4.2.3 Tétel:
Legyen A véges, nem ciklikus Abel-csoport, N véges csoport, $(|A|, |N|) = 1$. Hasson A N-en automorfizmusokon keresztül. Ekkor $N = \langle \mathrm{C}_N(a) | 1 \neq a \in A \rangle$.
Bizonyítás:
Indukciót alkalmazunk N rendje szerint. $|N| = 1$ esetén nyilvánvaló az állítás.
Legyen $K = \langle \mathrm{C}_N(a) | 1 \neq a \in A \rangle$. Az indukciós feltevésünk szerint, ha M A-invariáns valódi részcsoport, akkor $M = \langle \mathrm{C}_M(a) | 1 \neq a \in A \rangle \leq K$. Tegyük fel, hogy $|N : K|$-nak létezik p prímosztója. Mivel A feloldható (hisz Abel-csoport), és koprím módon hat N-en, ezért az 1.1.5 Tétel szerint létezik N-nek A-invariáns p-Sylowja, jelölje őt P. $P \nsubseteq K$, hisz p magasabb hatványon osztja P rendjét, mint K rendjét. Mivel P A-invariáns, és nem része K-nak, ezért $P = N$, hisz K N összes A-invariáns valódi részcsoportját tartalmazza. Tehát N p-csoport. Ezért N' N valódi részcsoportja. Mivel N' karakterisztikus, így A-invariáns is. Ezek szerint $N' \leq K$, ami mutatja, hogy $K \trianglelefteq N$.

Tekintsük az N/K faktorcsoportot, és jelölje felülvonás a természetes homomorfizmust. Könnyen meggondolható, hogy K A-invariáns, tehát teljesülnek az 1.1.6 Tétel (i) pontjának feltételei, azaz $\mathrm{C}_{\overline{N}}(a) = \overline{\mathrm{C}_N(a)}$ $(\forall a \in A)$. Mivel $\mathrm{C}_N(a) \leq K$, ezért $\mathrm{C}_{\overline{N}}(a)$ triviális $(\forall 1 \neq a \in A)$. A fixpontmentesen hat $\overline{N}$-on, így A Frobenius-komplementum. Mivel A Abel csoport is, így szükségképpen ciklikus. Ezzel ellentmondásra jutottunk. Nem létezik tehát prímosztója $|N : K|$-nak, azaz $N = K$. És ez épp a kívánt állítás.■

4.2.4 Következmény:

Legyen A véges Abel-csoport, N véges csoport, $(|A|, |N|) = 1$, és hasson A automorfizmusokon keresztül hűségesen N-en. Legyen A hatása N összes valódi A-invariáns részcsoportján triviális. Ekkor A ciklikus.

Bizonyítás:

Mivel A Abel csoport, így $\mathrm{C}_N(a)$ A-invariáns $(\forall a \in A)$. Mivel A hűségesen hat N-en, ezért $\mathrm{C}_N(a) < N$ $(\forall 1 \neq a \in A)$. Tehát $\mathrm{C}_N(a)$ valódi A-invariáns részcsoport, azért $\mathrm{C}_N(a) \leq \mathrm{C}_N(A)$ $(\forall\, 1 \neq a \in A)$, és így a csoportok között az egyenlőség is fennáll. Az előző tétel alapján, ha A nem ciklikus, akkor $\mathrm{C}_N(A) = N$. Ez A hűségessége miatt, csak úgy teljesülhet, ha A a triviális csoport. Ekkor azonban ciklikus, ami ellentmondás.■

4.2.5 Tétel:

Legyen G véges csoport, $p > 2$ prím, $P \in Syl_p G$. Továbbá teljesüljenek az alábbi feltételek:

(i) G p-feloldható

(ii) G 2-Sylowjai Abel-csoportok

(iii) $\mathrm{O}_{p'}(G) = 1$

(iv) $P = \mathrm{C}_G(\mathrm{Z}(P))$.

Ekkor $\mathrm{J}(P) \trianglelefteq G$.

Bizonyítás:

Tegyük fel, hogy létezik ellenpélda. Legyen G közülük olyan, melynek rendje minimális.

Mivel G p-feloldható, és $\mathrm{O}_{p'}(G) = 1$, ezért $1 < \mathrm{O}_p(G)$ (hisz a triviális csoport nem ellenpélda). Jelöljük a legnagyobb p-normálosztót U-val, és a hozzátartozó természetes homomorfizmust felülvonással. $\overline{G}$ p-feloldható, és benne a legnagyobb p-normálosztó csak a triviális csoport lehet. Ezért $1 < \mathrm{O}_{p'}(\overline{G})$, jelölje a csoport ősét L (természetesen $L \trianglelefteq G$). A bizonyítás további részeit lépésekre bontjuk.

1.Lépés
(a) $\mathrm{Z}(P) \leq U$
(b) $\mathrm{C}_{\overline{G}}(\overline{L}) \leq \overline{L}$
(c) $U \leq H \leq G$ esetén $\mathrm{O}_{p'}(H) = 1$
1.Lépés bizonyítása:
(a) U a legnagyobb p-normálosztó, így $U \leq P$, ezért $\mathrm{Z}(P) \leq \mathrm{C}_G(U)$. Alkalmazhatjuk a Hall-Higman Lemmát (1.2.14 Tétel), azaz $\mathrm{Z}(P) \leq \mathrm{C}_G(U) \leq U$.
(b) Mivel $\overline{G}$ p-feloldható, így p'-szeparábilis, és $\mathrm{O}_p(\overline{G}) = 1$, a Hall-Higman Lemmából azonnal kapjuk az állítást.
(c) Jelölje M $\mathrm{O}_{p'}(H)$-t. Ekkor $M \cap U = 1$, hisz egyikük p'-, másikuk p-csoport. $[M, U] \leq M \cap U = 1$ miatt $M \leq \mathrm{C}_G(U) \leq U$, amiből adódik, hogy $M = 1$.

2.Lépés
Létezik $A \in \mathcal{E}(P)$, hogy $A \nsubseteq U$.
2.Lépés bizonyítása:
Ha minden $A \in \mathcal{E}(P)$ U-ban lenne, akkor $\mathrm{J}(P) \leq U$. Tehát $\mathrm{J}(P) = \mathrm{J}(U) \operatorname{char} U \trianglelefteq G$ miatt, $\mathrm{J}(P) \trianglelefteq G$ teljesülne, ami ellentmond a feltevéseinknek.

A következő két lépésben kihasználjuk, hogy $\overline{L}$ centralizátora „pici” $\overline{G}$-ben (1.Lépés). Keresünk olyan csoportokat, melyek centralizálják $\overline{L}$ részcsoportjait. Mindezt azon észrevétel alapján tesszük, hogy, ha két normálosztó triviálisan metszi egymást, akkor centralizálják is egymást. A keresett csoportok segítségével G-t szorzat alakban írhatjuk.

3.Lépés
Legyen H olyan valódi részcsoport, melyre $UA \leq H < G$, és $P \cap H \in Syl_p H$. Ekkor $\overline{A}$ centralizálja $\overline{H \cap L}$-et.
3.Lépés bizonyítása:
Jelöljük $H \cap P$-t S-sel. H-ra és S-re a tétel feltételeinek első három pontja teljesül. Belátjuk, hogy a (iv) feltétel is teljesül. $\mathrm{Z}(P) \leq U \leq S$ és $S \leq P$ miatt, $\mathrm{Z}(P) \leq \mathrm{Z}(S)$. Ezért $\mathrm{C}_G(\mathrm{Z}(S)) \leq \mathrm{C}_G(\mathrm{Z}(P)) = P$, véve a H-val való metszetet $\mathrm{C}_H(\mathrm{Z}(S)) \leq S$. A másik irányú tartalmazás triviális, tehát teljesülnek H-ra és S-re a tétel feltételei. Mivel $|H| < |G|$, ezért $\mathrm{J}(S) \trianglelefteq H$. $A \in \mathcal{E}(P)$ és $A \leq P \cap H = S$ miatt, $A \leq \mathrm{J}(S)$. Tekintsük a $[H \cap L, A]$ csoportot. $[H \cap L, A] \leq [H \cap L, \mathrm{J}(S)] \leq (H \cap L) \cap \mathrm{J}(S) = L \cap \mathrm{J}(S) \leq U$, a második egyenlőtlenség teljesül, mert $H \cap L$ és $\mathrm{J}(S)$ normálosztók H-ban, az utolsó pedig amiatt, mert U L egyetlen p-Sylowja. Ezek alapján $\overline{[H \cap L, A]} = 1$, és épp ezt akartuk bizonyítani.

4.Lépés

$G = LA$ és $P = UA$.

4.Lépés bizonyítása:

Válasszuk H-t LA-nak, és tegyük fel, hogy $H < G$. Belátjuk, hogy $S = H \cap P \in Syl_p H$, és alkalmazzuk az előző Lépés állítását.

$|H : UA| = |LA : UA| = |L(UA) : UA| = |L : L \cap UA|$, és $|L : L \cap UA|$ osztja $|L : U|$-t. Mivel $|L : U|$ relatív prím p-hez, így $|L : L \cap UA| = |H : UA|$ is az. UA tehát H olyan p-részcsoportja, melynek indexe relatív prím p-hez, így $UA \in Syl_p H$. Továbbá U-t és A-t is tartalmazza az S H-beli p-csoport, tehát $S = UA \in Syl_p H$.

$H \cap L = L$, így a 3.Lépést alkalmazva kapjuk, hogy $\overline{A}$ centralizálja $\overline{L}$-t. Viszont az 1.Lépés (b) pontja szerint $\mathrm{C}_{\overline{G}}(\overline{L}) \leq \overline{L}$. Ez csak úgy teljesülhet, ha $\overline{A}$ triviális, azaz $A \leq U$, de ez ellentmond A 2.Lépésbeli választásának. Ellentmondásra jutottunk, így $G = LA$. Továbbá $UA = S = H \cap P = G \cap P = P$.

5.Lépés

$|\overline{A}| = p$

5.Lépés bizonyítása:

Mivel A elemi Abel-csoport, ezért $\overline{A}$ is az. Elegendő tehát belátni, hogy $\overline{A}$ ciklikus. $\overline{A}$ hatása hűséges $\overline{L}$-en ugyanis, $\mathrm{C}_{\overline{G}}(\overline{L}) \leq \overline{L}$ és $\overline{L} \cap \overline{A} = 1$. Alkalmazva a 4.2.4 Következményt, elég megmutatni, hogy $\overline{A}$ triviálisan hat $\overline{L}$ minden valódi részcsoportján.

Válasszunk $\overline{L}$-ben egy tetszőleges $\overline{A}$-invariáns valódi részcsoportot, és jelöljük a természetes homomorfizmus által vett ősét M-mel. A 3.Lépés segítségével megmutatjuk, hogy $\overline{A}$ centralizálja $\overline{M}$-et. Könnyen látható, hogy $A \leq \mathrm{N}_G(M)$, így MA csoport. $UA \leq MA$ nyilvánvaló. $\overline{M} < \overline{L}$ miatt létezik $q \neq p$ prím, mely L rendjét magasabb hatványon osztja, mint M rendjét. Ezen q G rendjét is magasabb hatványon osztja, mint MA rendjét. Ezek szerint $MA < G$ is teljesül, alkalmazzuk a 3.Lépést. $\overline{A}$ centralizálja $\overline{MA \cap L}$-et, és mivel $\overline{M} \leq \overline{MA \cap L}$, ezért $\overline{M}$-et is. Az 5.Lépés bizonyítását ezzel befejeztük.

Definiáljuk a V p-csoportot a következőképpen, $V = \{z \in \mathrm{Z}(U) \,|\, z^p = 1\}$. V elemi Abel-csoport, és karakterisztikus G-ben. G a konjugálás által hat V-n. Mivel $V \leq \mathrm{Z}(U)$, így U triviálisan hat V-n. Ezért tekinthetjük $\overline{G}$ hatását. Megmutatjuk, hogy $\overline{G}$, $\overline{P}$ és V kielégítik a 4.1.6 Tétel feltételeit. $\overline{G}$ p-feloldható, és 2-Sylowjai Abel-csoportok. A következő lépésekben belátjuk a másik két feltételt is.

6.Lépés

$\overline{G}$ hűségesen hat V-n.

6.Lépés bizonyítása:

Jelöljük K-val $\mathrm{C}_G(V)$-t. $K \trianglelefteq G$ és $\overline{K}$ a magja $\overline{G}$ hatásának. Megmutatjuk, hogy K p-csoport. Ekkor $K \leq U$ miatt, $\overline{K} = 1$, így $\overline{G}$ hatása hűséges.

Tegyük fel, hogy $|K|$-nak van egy p-től különböző q prímosztója, és legyen $Q \in Syl_q K$. Q koprím módon hat a $\mathrm{Z}(U)$ Abel-csoporton. Továbbá, centralizálja annak minden p-edrendű elemét, hisz azok V-beliek, míg $Q \leq K$. Fitting tétele alapján $\mathrm{Z}(U) = \mathrm{C}_{\mathrm{Z}(U)}(Q) \times [\mathrm{Z}(U), Q]$. Mivel az összes p-edrendű elem a direkt szorzat első tényezőjében van, ezért a második a triviális csoport. Tehát $Q \leq \mathrm{C}_G(\mathrm{Z}(U))$. Az 1.Lépés (a) pontja alapján $\mathrm{Z}(P) \leq U$, így $\mathrm{Z}(P) \leq \mathrm{Z}(U)$, tehát $\mathrm{C}_G(\mathrm{Z}(U)) \leq \mathrm{C}_G(\mathrm{Z}(P)) = P$. Összevetve az előző állításokat kapjuk, hogy $Q \leq P$, amiből következik, hogy $Q = 1$. Ezzel az ellentmondással a bizonyítást befejeztük.

7.Lépés

$|V : V \cap A| \leqq p$

7.Lépés bizonyítása:

Legyen $D = U \cap A$ és $E = V \cap A$. $|V : E| = |V : V \cap D| = |VD : D|$. $|VD|$ pedig felülbecsülhető $|A|$-val, ugyanis $D \leq U$ elemi Abel-csoport, és $V \leq \mathrm{Z}(U)$ elemi Abel-csoport U centrumában. Tehát VD elemi Abel-csoport $U \leq P$-ben és A maximális rendű elemi Abel-csoport P-ben. Így $|VD| \leqq |A|$. Ezek szerint $|VD : D| \leqq |A : D| = |A : U \cap A| = |AU : U| = |\overline{A}| = p$. Tehát $|V : V \cap A| = |V : E| \leqq p$.

8.Lépés

Ellentmondásra jutottunk.

8.Lépés bizonyítása:

Belátjuk, hogy $|V : \mathrm{C}_V(\overline{P})| \leqq p$ és alkalmazzuk az 4.1.6 Tételt. $P = UA$, ezért $\overline{P} = \overline{A}$. Tehát $\overline{P}$ centralizálja $V \cap A$-t, hisz A Abel-csoport. Ekkor pedig $|V : \mathrm{C}_V(\overline{P})| \leqq |V : V \cap A| \leqq p$. A 4.1.6 Tétel szerint $\overline{P} \trianglelefteq \overline{G}$, így $P \trianglelefteq G$. Mivel $\mathrm{J}(P)\,\mathrm{char}\,P$, ezért $\mathrm{J}(P) \trianglelefteq G$. Ezzel ellentmondásra jutottunk, így a tétel bizonyítását befejeztük.■

4.3. Thompson normál p-komplementum tétele

A mag nilpotenciáját bizonyító érvelés lelke Thompson normál p-komplementum tétele. Az alfejezetet szinte egészében ennek szenteljük.

4.3.1 Lemma:
Legyen G véges csoport, p prím. $N \trianglelefteq G$ p'-csoport, $P \leq G$ pedig p-csoport. Jelöljük a természetes homomorfizmust felülvonással. Ekkor
(i) $\mathrm{N}_{\overline{G}}(\overline{P}) = \overline{\mathrm{N}_G(P)}$
(ii) $\mathrm{C}_{\overline{G}}(\overline{P}) = \overline{\mathrm{C}_G(P)}$.
Bizonyítás:
(i) Világos , hogy $\overline{\mathrm{N}_G(P)} \leq \mathrm{N}_{\overline{G}}(\overline{P})$, ezért elég az ellenkező irányú tartalmazást megmutatnunk. $\mathrm{N}_{\overline{G}}(\overline{P})$ ősét jelöljük M-mel. $\overline{PN} = \overline{P} \trianglelefteq \overline{M}$. Tehát $PN \trianglelefteq M$, és $P \in Syl_p(PN)$, mivel N p'-csoport. A Frattini-elv szerint $M = \mathrm{N}_M(P)(PN) = \mathrm{N}_M(P)N \leq \mathrm{N}_G(P)N$, alkalmazva a természetes homomorfizmust kapjuk, hogy $\overline{M} = \mathrm{N}_{\overline{G}}(\overline{P}) \leq \overline{\mathrm{N}_G(P)}$.
(ii) Világos , hogy $\overline{\mathrm{C}_G(P)} \leq \mathrm{C}_{\overline{G}}(\overline{P})$, ezért elég az ellenkező irányú tartalmazást megmutatnunk. $\mathrm{C}_{\overline{G}}(\overline{P})$ ősének $\mathrm{N}_G(P)$-vel vett metszetét jelölje C. Az (i) pont szerint $\mathrm{N}_G(P)$-t a természetes homomorfizmus ráképezi $\mathrm{N}_{\overline{G}}(\overline{P})$-re, és $\mathrm{C}_{\overline{G}}(\overline{P}) \leq \mathrm{N}_{\overline{G}}(\overline{P})$. Ezért $\overline{C} = \mathrm{C}_{\overline{G}}(\overline{P})$. Tehát $C \leq \mathrm{N}_G(P)$, így $[P, C] \leq P$. $1 = [\overline{P}, \overline{C}] = \overline{[P, C]}$-ből következően $[P, C] \leq N$. Tehát $[P, C] \leq P \cap N = 1$, azaz $C \leq \mathrm{C}_G(P)$. Alkalmazva a természetes homomorfizmust $\overline{C} = \mathrm{C}_{\overline{G}}(\overline{P}) \leq \overline{\mathrm{C}_G(P)}$.■

4.3.2 Tétel: (Thompson normál p-komplemtum tétele)
Legyen G véges csoport, $p > 2$ prím és $P \in Syl_pG$ tetszőleges p-Sylow. G-nek pontosan, akkor létezik normál p-komplemetuma, ha $\mathrm{C}_G(\mathrm{Z}(P))$-nek és $\mathrm{N}_G(\mathrm{J}(P))$-nek létezik normál p-komplemetuma.
Bizonyítás:
Az 1.3.2 Megjegyzés (ii) pontja miatt, világos, ha G-nek van normál p-komplementuma, akkor a tételben szereplő két részcsoportnak is van.
A másik irányú állítás bizonyításához tegyük fel, hogy létezik ellenpélda, és válasszunk közülük egy minimális rendűt. $H \leq G$ esetén jelöljük $|H|_p$-vel azt a legnagyobb p-hatványt, amely osztja H rendjét. Frobenius normál p-komplementum tétele szerint léteznek P-nek olyan nemtriviális részcsoportjai, melyek normalizátorának nincs normál p-komplementumuk. Legyen közülük U olyan, hogy $|\mathrm{N}_G(U)|_p$ maximális, és az ezen feltételt teljesítő csoportok közül U rendje is maximális. A bizonyítás további részeit lépésekre bontjuk.

1.Lépés

$U = \mathrm{O}_p(G)$

1.Lépés bizonyítása:

Jelölje N $\mathrm{N}_G(U)$-t, és tegyük fel, hogy $N < G$. Legyen $S \in Syl_p N$. Megmutatjuk, hogy a $\mathrm{J}(S)$ vagy a $\mathrm{Z}(S)$ S-beli karakterisztikus csoportok normalizátorának rendjét p magasabb hatványa osztja, mint N-ét.

N rendje kisebb G rendjénél, így N nem ellenpélda. Mivel N-nek nincs p-komplementuma, így $\mathrm{C}_N(\mathrm{Z}(S))$-nek vagy $\mathrm{N}_N(\mathrm{J}(S))$-nek nincs p-komplementuma. S tehát nem p-Sylowja G-nek, így S normálosztóként beletehető G egy nagyobb p-csoportjába, T-be.

Jelölje X a $\mathrm{J}(S)$ és a $\mathrm{Z}(S)$ csoportok egyikét, melyre $\mathrm{N}_G(X)$-nek nincs normál p-komplementuma. (Ha egy részcsoportnak nincs normál p-komplementuma, akkor az őt tartalmazó csoportnak sincs. Ezért találhatunk megfelelő X-et.) $X \operatorname{char} S \trianglelefteq T$ miatt $|\mathrm{N}_G(X)|_p \geqq |T| > |S| = |\mathrm{N}_G(U)|_p$, ami ellentmond U választásának. Tehát U p-normálosztó. Ezek szerint $1 < U \leq \mathrm{O}_p(G)$. Mivel G-nek, $\mathrm{O}_p(G)$ normalizátorának, nincs p-komplementuma, és $\mathrm{O}_p(G)$ rendje legalább akkora, mint U rendje, így $U = \mathrm{O}_p(G)$.

Jelöljük az U-hoz tartozó természetes homomorfizmust felülvonással.

2.Lépés

$\overline{G}$-nek van normál p-komplementuma, így G p-feloldható.

2.Lépés bizonyítása:

$|\overline{G}| < |G|$, tehát $\overline{G}$ nem ellenpélda. Elegendő megmutatnunk, hogy $\mathrm{C}_{\overline{G}}(\mathrm{Z}(\overline{P}))$-nek és $\mathrm{N}_{\overline{G}}(\mathrm{J}(\overline{P}))$-nek létezik normál p-komplementuma. Ha $\overline{P}$ triviális, akkor ez nyilvánvaló. Különben jelölje X $\mathrm{Z}(\overline{P})$ és $\mathrm{J}(\overline{P})$ őseinek valamelyikét. Ekkor $1 < \overline{X} \trianglelefteq \overline{P}$ miatt $U < X \trianglelefteq P$. Így $|\mathrm{N}_G(X)|_p = |P| = |\mathrm{N}_G(U)|_p$, $|U| < |X|$. Tehát U választása miatt $\mathrm{N}_G(X)$-nek kell, hogy legyen normál p-komplementuma. Mivel $U < X$, ezért $\overline{\mathrm{N}_G(X)} = \mathrm{N}_{\overline{G}}(\overline{X})$. Ebből pedig következik, hogy $\mathrm{C}_{\overline{G}}(\mathrm{Z}(\overline{P}))$-nek és $\mathrm{N}_{\overline{G}}(\mathrm{J}(\overline{P}))$-nek létezik normál p-komplementuma, és így $\overline{G}$-nek is.

Jelöje L $\overline{G}$ normál p-komplementumának ősét, ekkor az $1 \leq U \leq L \leq G$ invariáns lánc bizonyítja, hogy G p-feloldható.

3.Lépés

$\mathrm{O}_{p'}(G) = 1$

3.Lépés bizonyítása:

Legyen $K = \mathrm{O}_{p'}(G)$. Tegyük fel, hogy $1 < K$. A bizonyítás többi részétől eltérően, ebben a

Lépésben jelölje a felülvonás a K-hoz tartozó természetes homomorfizmust. Megmutatjuk, hogy $\overline{G}$-nek létezik normál p-komplementuma, és mivel K p'-csoport, ezért ennek őse normál p-komplementum G-ben, ami ellentmond a feltevéseinknek.
K p'-csoport, így a felülvonás egy izomorfizmust ad P és $\overline{P}$ között, ezért $\overline{\mathrm{J}(P)} = \mathrm{J}(\overline{P})$ és $\overline{\mathrm{Z}(P)} = \mathrm{Z}(\overline{P})$. A 4.3.1 Lemmának köszönhetően $\mathrm{N}_{\overline{G}}(\mathrm{J}(\overline{P})) = \mathrm{N}_{\overline{G}}(\overline{\mathrm{J}(P)}) = \overline{\mathrm{N}_G(\mathrm{J}(P))}$ és $\mathrm{C}_{\overline{G}}(\mathrm{Z}(\overline{P})) = \mathrm{C}_{\overline{G}}(\overline{\mathrm{Z}(P)}) = \overline{\mathrm{C}_G(\mathrm{Z}(P))}$. Tehát $\mathrm{N}_{\overline{G}}(\mathrm{J}(\overline{P}))$-nek és $\mathrm{C}_{\overline{G}}(\mathrm{Z}(\overline{P}))$-nek létezik normál p-komplementuma, mivel $|\overline{G}| < |G|$, így $\overline{G}$-nek is. Ezzel megkaptuk a kívánt ellentmondást.

4.Lépés
P maximális részcsoportja G-nek.
4.Lépés bizonyítás:
Legyen H olyan részcsoport, melyre $P \leq H < G$. Ekkor H-nak létezik normál p-komplementuma. Ehhez $|H| < |G|$ miatt elegendő megmutatni, hogy $\mathrm{N}_H(\mathrm{J}(P))$-nek és $\mathrm{C}_H(\mathrm{Z}(P))$-nek van normál p-komplementuma. Ez pedig nyilvánvaló, hisz tetszőleges normál p-komplementummal bíró csoport részcsoportjának van normál p-komplementuma. Jelölje H normál p-komplementumát K. K és U normálosztók H-ban, és a rendek miatt $K \cap U = 1$. Mivel $[K, U] \leq K \cap U = 1$, így K centralizálja U-t. A 2. és 3.Lépések miatt alkalmazhatjuk a Hall-Higman Lemmát. Eszerint $K \leq \mathrm{C}_G(U) \leq U$. Tehát $K = 1$, ami mutatja, hogy H p-csoport. Mivel H tartalmazza P-t, így szükségképpen egyenlő is vele.

5.Lépés
$\mathrm{C}_G(\mathrm{Z}(P)) = P$
5.Lépés bizonyítása:
Nyilvánvaló, hogy $P \leq \mathrm{C}_G(\mathrm{Z}(P))$. $\mathrm{C}_G(\mathrm{Z}(P)) < G$, hisz G-nek nincs normál p-komplementuma, és $\mathrm{C}_G(\mathrm{Z}(P))$-nek van. P maximalitása folytán $\mathrm{C}_G(\mathrm{Z}(P)) = P$.

6.Lépés
$\overline{G}$ normál p-komplementuma Abel-csoport.
6.Lépés bizonyítása:
A 2.Lépésnek megfelelően jelölje $\overline{G}$ normál p-komplementumának ősét L. Megmutatjuk, hogy $(\overline{L})' = 1$.
Belátjuk, hogy $\overline{L}$-nek nincs P-invariáns valódi részcsoportja (hatáson a konjugálásból származó hatást értjük). Jelölje X $\overline{L}$ egy P-invariáns részcsoportjának az ősét. Ekkor $U \leq X \leq L$. Tekintsük a PX szorzatot. Feltevéseink szerint P normalizálja X-et, így ez egy csoportot eredményez. P maximalitása miatt PX csak P vagy G lehet. Ha $PX = P$, akkor X olyan

L-beli p-csoport, mely tartalmazza U-t. Ez a csoportok rendjei miatt csak $X = U$ esetén teljesülhet, ekkor $\overline{X} = 1$. Ha $PX = G$, akkor $|G : X| = |PX : X| = |P : X \cap P| = |P : L \cap P| = |PL : L| = |G : L|$ miatt $X = L$, így $\overline{X} = \overline{L}$.
$\overline{L}$ rendje relatív prím P rendjéhez, tehát $|\overline{L}|$ tetszőleges q prímosztójára (ilyen létezik, hisz $\overline{L}$ nem lehet triviális), létezik $\overline{L}$-nek P-invariáns q-Sylowja. Ez a q-Sylow csak akkor nem valódi részcsoport, ha $\overline{L}$ q-csoport.
$(\overline{L})' < \overline{L}$, hisz a q-csoportok feloldhatóak. $(\overline{L})'$ karakterisztikus L-ben, így P-invariáns is. Ez csak úgy lehetséges, ha $(\overline{L})' = 1$ és $\overline{L}$ Abel-csoport.

7.Lépés
Ellentmondásra jutottunk.
7.Lépés bizonyítása:
Alkalmazzuk G-re a 4.2.5 Tételt. Az előző Lépések alapján G p-feloldható, $\mathrm{O}_{p'}(G) = 1$, $P = \mathrm{C}_G(\mathrm{Z}(P))$ (és $p > 2$). A Tétel alkalmazásához elegendő tehát ellenőriznünk, hogy G 2-Sylowjai Abel-csoportok.
Legyen $Q \in Syl_2 G$. Mivel U és Q rendjeik relatív prímek, így Q izomorf $\overline{Q}$-sal. $\overline{Q}$ tehát 2-Sylow $\overline{G}$-ban. $\overline{L}$ normál p-komplementuma $\overline{G}$-nek, ezért $\overline{Q} \leq \overline{L}$. $\overline{L}$ Abel-csoport, így $\overline{Q}$ és a vele izomorf Q is az.
A 4.2.5 Tétel szerint $\mathrm{J}(P) \trianglelefteq G$. Ekkor azonban $\mathrm{N}_G(\mathrm{J}(P)) = G$-nek létezik normál p-komplementuma, ami a végső ellentmondásunkat eredményezi.■

4.4. A Frobenius-mag nilpotenciája

Eddigi munkánk gyümölcseként belátjuk Thompson Frobenius-magok nilpotenciájáról szóló híres tételét.

4.4.1 Tétel:
Legyen $G = N \rtimes A$ Frobenius-csoport A komplementummal és N maggal. Ha $|A|$ páros, akkor A-nak pontosan egy másodrendű eleme van, és N Abel-csoport.
Bizonyítás:
Legyen a egy tetszőleges A-beli másodrendű elem, és n egy tetszőleges N-beli elem. Ekkor $(nn^a)^a = n^a n = n^{-1} n n^a n = (nn^a)^n$. Ezért $an^{-1} \in \mathrm{C}_G(nn^a)$ és $an^{-1} \in G \setminus N$, ami a 2.1.10 Tétel miatt csak úgy teljesülhet, ha $nn^a = 1$, azaz $n^a = n^{-1} \quad \forall n \in N$.

Ha A-nak létezne a-tól különböző b másodrendű eleme, akkor tetszőleges $n \in N$ esetén $n^{ab} = n$. Ezzel ellentmondásra jutunk, hisz $1 \neq ab \in A$, és A fixpontmentesen hat N-en.
Legyenek n, m tetszőleges N-beli elemek és jelölje az inverzüket x és y, azaz $x^{-1} = n$, $y^{-1} = m$. Ekkor $mn = y^{-1}x^{-1} = (xy)^{-1} = (xy)^a = x^a y^a = x^{-1}y^{-1} = nm$, tehát N Abel-csoport.■

4.4.2 Tétel:
Ha a Frobenius-mag feloldható, akkor nilpotens.
Bizonyítás:
Tegyük fel, hogy létezik ellenpélda, és legyen N közülük minimális rendű. Létezik tehát A prímrendű Frobenius-komplementum ($|A| = p$), hogy $G = N \rtimes A$ Frobenius-csoport. Mivel N feloldható, így található benne U minimális normálosztó, amely elemi Abel-q-csoport, valamely q prímre. Jelöljük az U-hoz tartozó természetes homomorfizmus képét felülvonással. Megmutatjuk, hogy U az egyetlen minimális normálosztó.
A 2.1.8 Állítás miatt A Frobenius-hatást valósít meg $\overline{N}$-n. Mivel $|\overline{N}| < |N|$, így $\overline{N}$ nem ellenpélda, tehát nilpotens. Ez csak úgy lehetséges, ha $N^\infty \leq U$ (N^∞ definíciója az 1.2.16 Megjegyzésben található). N^∞ normálosztó, U minimális normálosztó, ezért $U = N^\infty$. Ez a gondolatmenet tetszőleges minimális normálosztó esetén elmondható, tehát U az egyetlen minimális normálosztó.
Feltevéseink szerint N nem lehet q-csoport. Válasszuk rendjének egy $r \neq q$ prímosztóját, és legyen $R \in Syl_r N$ egy A-invariáns r-Sylow részcsoport. (R létezése következik az 1.1.5 Tételből, de erre nincs is szükségünk. Ugyanis A tetszőleges egységtől különböző eleme generáló elem, és p-edrendű permutációt valósít meg a hozzá képest relatív prím rendű $Syl_r N$ halmazon.) Vizsgáljuk a továbbiakban N-et az $\overline{R}$ és az AR csoportok segítségével (ez csoport, hisz R A-invariáns). Először megmutatjuk, hogy $N = RU$, majd R hatását U-n AR hatásának segítségével értjük meg.
$\overline{R}$ nyilván r-Sylow az $\overline{N}$ nilpotens csoportban. Tehát $\overline{R} \trianglelefteq \overline{N}$, ezért $RU \trianglelefteq N$. RU A-invariáns, hisz R és U is az. Ha $RU < N$, akkor RU nem ellenpélda, tehát $R \in Syl_r(RU)$ karakterisztikus részcsoport RU-ban. Így $R \triangleleft N$, ami ellentmondana U unicitásának. Ezek szerint $N = RU$.
Az AR csoport Frobenius, tehát létezik P partíciója, mely A konjugáltjaiból és R-ből áll. $|\mathrm{P}| - 1 = |R|$ és $(|R|, |U|) = 1$. Ezért a 2.3.2 Lemmát alkalmazva kapjuk, hogy a partíció valamely tagja centralizálja U egy egységelemtől különböző elemét. Ez csak R lehet, hisz A és konjugáltjai fixpontmentesen hatnak U-n. Tehát $1 < \mathrm{C}_U(R) \leq \mathrm{Z}(RU) = \mathrm{Z}(N)$. Ezek szerint $\mathrm{Z}(N)$ nemtriviális normálosztó N-ben, így $U \leq \mathrm{Z}(N)$. Ekkor viszont $R \triangleleft RU = N$, ami ellentmond U unicitásának.■

4.4.3 Tétel: (Thompson)
A Frobenius-mag nilpotens.
Bizonyítás:
Az előző tétel miatt elég belátni, hogy a Frobenius-mag feloldható. A bizonyítást a mag rendje szerinti indukcióval végezzük. Az első néhány kisebb rendre az állítás nyilvánvalóan igaz.
Legyen N Frobenius-mag és hozzá A egy p prímrendű komplementum. Keressünk N-ben egy $1 < M \lhd N$ A-invariáns nemtriviális valódi normálosztót. Ez elég, ugyanis az indukciós feltevés és a 2.1.8 Állítás miatt M és N/M is nilpotens, így feloldható Frobenius-magok. Ezért N is feloldható, így nilpotens.
Ha N 2-csoport, akkor nilpotens. Feltehető tehát, hogy N-nek létezik $r > 2$ prímosztója. Akárcsak az előző tételben, válasszunk N-ben egy A-invariáns r-Sylowot, R-et. Tekintsük R nemtriviális karakterisztikus részcsoportjait.
Ha közülük valamely S-nek a normalizátora N, akkor $S \lhd N$. Mivel R A-invariáns, S pedig karakterisztikus R-ben, így S is A-inavariáns. Ezzel találtunk egy A-invariáns valódi nemtriviális normálosztót.
Ha tetszőleges X R-beli nemtriviális karakterisztikus részcsoport esetén $\mathrm{N}_N(X) < N$, akkor mivel $\mathrm{N}_N(X)$ A-inavriáns, így $|N|$-nél kisebb rendű Frobenius-mag $((\mathrm{N}_N(X))^a = \mathrm{N}_N(X^a) = \mathrm{N}_N(X) \quad (\forall a \in A))$. Az indukciós feltevés szerint $\mathrm{N}_N(X)$ nilpotens, így létezik normál r-komplementuma. Alkalmazva Thompson tételét, N-nek egy normál r-komplementumát kapjuk. Mivel a normál r-komplementum karakterisztikus, így találtunk egy valódi nemtriviális normálosztót N-ben.■

5. fejezet

Perfekt Frobenius-komplementumok

Nevezetes probléma, hogy minden Frobenius-komplementum feloldható-e. Eddigi vizsgálódásainkból már tudjuk, hogy a kérdésre a válasz negatív. A feladat komolyságát jelzi azonban, hogy a csoportelmélet olyan hatalmas alakja, mint Burnside, hibásan állította ennek ellenkezőjét, az egyébként kiemelkedő jelentőségű, Theory of Groups of Finite Order című könyvének [1] 1911-es, második kiadásában (Theorem V. a 336. oldalon).

5.1. Perfekt Frobenius-komplementumok

Belátjuk Zassenhaus tételét, mely szerint izomorfia erejéig egyetlenegy perfekt Frobenius-komplementum létezik. Majd ennek segítségével levonjuk következtetésünket a nemfeloldható komplementumokra vonatkozóan. Az alfejezet tételeit Huppert könyvének [3] 46. fejezetére támaszkodva tárgyaljuk.

5.1.1 Állítás:
Legyen G perfeket csoport, azaz $G' = G$. Ekkor G összes faktorcsoportja perfekt.
Bizonyítás:
Legyen $N \trianglelefteq G$ normálosztó. $(G/N)' = G'N/N = GN/N = G/N$.■

5.1.2 Lemma: (Thompson)

(i) Legyen G véges csoport, $i \in G$ involúció és $H < G$ olyan részcsoport, melyre $|G : H| = 2m$, ahol m páratlan. Továbbá H diszjunkt i konjugált osztályától, azaz $i^G \cap H = \emptyset$. Ekkor létezik 2 indexű normálosztó G-ben.

(ii) Legyen G olyan véges csoport, melynek nincs 2 indexű normálosztója, $P \in Syl_2 G$ pedig G olyan 2-Sylowja, melynek van 2 indexű ciklikus részcsoportja. Ekkor az összes G-beli involúció konjugált.

Bizonyítás:

(i) Legyen $\varrho : G \mapsto S_{2m}$ G reprezentációja H mellékosztályain. Ekkor i^ϱ fixpontmentes másodrendű elem, hisz $Hgi \neq Hg \quad (\forall g \in G)$. Mivel H-nak $2m$ mellékosztálya van és m páratlan, ezért i^ϱ páratlan sok transzpozíció szorzata. Ezek szerint $G^\varrho \nsubseteq \mathrm{A}_{2m}$, ekkor pedig $G^\varrho \cap \mathrm{A}_{2m}$ őse 2 indexű.

(ii) Legyen a P 2 indexű részcsoportjának generáló eleme. Alkalmazzuk az előző tételt $\langle a \rangle = H$ szereposztással. Mivel G-nek nincs 2 indexű részcsoportja, így tetszőleges involúció konjugált $\langle a \rangle$ egyetlen másodrendű elemével.■

5.1.3 Lemma:

Legyen A Frobenius komplementum. Ekkor létezik olyan V K test feletti vektortér, melyen A fixpontmentesen hat, és $(|A|, \mathrm{char} K) = 1$.

Biztonyítás:

Legyen N egy A-hoz tartozó Frobenius-mag. Mivel A koprím módon hat N-en, és A és N közül legalább az egyik feloldható, ezért az 1.1.5 Tétel értelmében létezik N-nek A invariáns p-Sylowja, ahol p $|N|$ valamely prímosztója. (A feloldhatóságra tett kikötés következik, például, a mag nilpotenciájára vonatkozó Thompson-tételből, de akár elemibb úton is megmutatható. Ha a komplementum rendje páratlan, akkor a komplementum feloldható, míg, ha páros, akkor a mag Abel-csoport, így feloldható is.) Legyen $V = P/\Phi(P)$, ahol $\Phi(P)$ a Frattini-részcsoport. Ez elemi Abel-csoport. Ugyanis, ha $Q < P$ maximális részcsoport, akkor Q normálosztó és az általa vett faktorcsoport p-edrendű. Ezért $P' \leq Q$, és $g^p \in Q \quad (\forall g \in P)$. Tehát az utóbbi állítás igaz $\Phi(P)$-re is, így $P/\Phi(P)$ Abel-csoport, és minden eleme p-edrendű, ezért elemi Abel-csoport. Mivel V elemi Abel-p-csoport, így azonosítható egy $\mathrm{GF}(p)$ feletti vektortérrel. A 2.1.8 Állítás miatt A fixpontmentesen hat V-n, így a vele azonosított vektortéren is. $(|A|, \mathrm{char} K) = (|A|, p) = 1$.■

5.1.4 Lemma:
Legyen A perfekt Frobenius-komplementum. Ekkor pontosan egy z involúciót tartalmaz, $A/\langle z\rangle$ 2-Sylowjai diédercsoportok, és $A/\langle z\rangle$ összes involúciója konjugált.
Bizonyítás:
A 2.3.10 Megjegyzés (iii) pontja alapján A 2-Sylowjai csak általánosított kvaterniócsoportok lehetnek, a 4.4.1 Tétel szerint pedig, A-nak pontosan egy involúciója van. Ezekből és az 5.1.2 Lemmából pedig következnek a Lemma állításai.■

5.1.5 Állítás:
Legyen G perfekt véges csoport, és $|G| = 60$. Ekkor $G \cong \mathrm{A}_5$.
Bizonyítás:
Megmutatjuk, hogy G egyszerű. Ha létezne G-nek nemtriviális valódi normálosztója, akkor N és G/N rendjei a $\{2, 3, 4, 5, 6, 10, 12, 15, 20, 30\}$ halmaz elemei közül kerülhetnének ki. A Sylow-tételek egyszerű alkalmazásával adódik, hogy ekkor N és G/N, és így G is feloldható. Ez pedig ellentmondás.
Legyen $a = |Syl_2G|$. Ekkor a Sylow-tételek miatt a páratlan és $a|15$. $a \neq 1$, hisz G egyszerű. $a \neq 3$, különben G-t izomorfikusan beágyazhatnánk a 6 elemű S_3 egy részcsoportjába.
Tegyük fel, hogy $a = 15$. Ha P és Q G különböző 2-Sylowjai, akkor $P \cap Q = 1$. Különben, véve egy $1 \neq g \in P \cap Q$ elemet, $C = \mathrm{C}_G(g)$ rendje legalább 12, és mivel G egyszerű, így valódi részcsoport. Tekintsük G reprezentációját C mellékosztályain. Ezzel egy a legfeljebb 5-ödfokú szimmetrikus csoport valamely részcsoportjába menő izomorfizmust kapunk. Mivel G 60-adrendű és egyszerű, így az előbbi csoportok közül csak A_5-tel lehetne izomorf. Ekkor viszont nincs 15 különböző 2-Sylowja. A 15 darab egymást páronként csak az egységelemben metsző 2-Sylow összesen $3 \cdot 15 + 1 = 46$ különböző 2-hatvány rendű elemet eredményez. Mivel az 5-Sylowok nem normálosztók, így legalább 6 van belőlük, ez viszont 24 darab 5-ödrendű elemet ad, ami ellentmondáshoz vezet.
$a = 5$ esetén G hatása a Syl_2G halmazon egy izomorfizmust ad G és S_5 egy részcsoportja között. Mivel G egyszerű és 60-adrendű, így S_5 részcsoportjai közül csak A_5-tel lehet izomorf.■

5.1.6 Tétel:
Legyen G véges perfekt csoport, G összes involúciója konjugált, és $\mathrm{C}_G(i) \cong \mathrm{Z}_2 \times \mathrm{Z}_2$ valamely (így az összes) i involúció esetén. Ekkor $G \cong \mathrm{A}_5$.
Bizonyítás:
Rögzítsünk egy $i \in G$ involúciót, és jelölje S $\mathrm{C}_G(i)$-t. $\mathrm{N}_G(S)$-ből kiindulva „felépítjük" a csoportot. Vizsgáljuk $\mathrm{N}_G(S)$ konjugáltjait, Sylow-részcsoportjait és mellékosztályait. A bizonyítást lépésekre bontjuk.

1.Lépés
$S \in Syl_2 G$
1.Lépés bizonyítása:
Tekintsünk egy $P \in Syl_2 G$ csoportot. Mivel P centruma nemtriviális, így van benne egy z másodrendű elem. G összes involúciója konjugált, ezért létezik $g \in G$, hogy $z^g = i$. Ezek szerint i eleme a P^g 2-Sylow centrumának. Ebből adódik, $P^g \leq S$, ezért $S \in Syl_2 G$.

2.Lépés
$\mathrm{N}_G(S) \cong \mathrm{A}_4$
2.Lépés bizonyítása:
Ha $g \in G$ centralizálja S valamely egységelemtől különböző elemét, akkor az egész S-et centralizálja, hisz S bármely elemének a centralizátora S. $\mathrm{N}_G(S)/\mathrm{C}_G(S)$ izomorf $\mathrm{Aut}(S)$ fixpontmentes elemeinek egy csoportjával. Burnside p-komplementum tétele (1.3.3 Tétel) miatt $\mathrm{N}_G(S) = \mathrm{C}_G(S)$ nem fordulhat elő. Így $S \cong \mathrm{Z}_2 \times \mathrm{Z}_2$ miatt $\mathrm{N}_G(S)/\mathrm{C}_G(S) \cong \mathrm{Z}_3$. Ezek szerint $\mathrm{Z}_2 \times \mathrm{Z}_2 \cong S$ normálosztó a 12-edrendű, nemkommutatív $\mathrm{N}_G(S)$-ben. Ez csak úgy teljesülhet, ha $\mathrm{N}_G(S) \cong (\mathrm{Z}_2 \times \mathrm{Z}_2) \rtimes \mathrm{Z}_3 \cong \mathrm{A}_4$.

Jelöljük a továbbiakban $\mathrm{N}_G(S)$-et H-val.

3.Lépés
(i) $\mathrm{N}_G(H) \cong H$, és emiatt $Hx = Hy$ pontosan, akkor, ha $H^x = H^y$ $(x, y \in G)$
(ii) $T \in Syl_3 H$ esetén $\mathrm{N}_H(T) = \mathrm{C}_H(T) = T$ és $T \cong \mathrm{Z}_3$
3.Lépés bizonyítása:
(i) H az $S \in Syl_2 G$ normalizátora, így S H egyetlen 2-Sylowja, ezért $S \operatorname{char} H$. $H \trianglelefteq \mathrm{N}_G(H)$, így $S \trianglelefteq \mathrm{N}_G(H)$, tehát $\mathrm{N}_G(H) \leq \mathrm{N}_G(S) = H$. A másik irányú tartalmazás, akárcsak az állítás második fele nyilvánvaló.
(ii) $H \cong \mathrm{A}_4$-ből következik.

4.Lépés

S összes H-n kívül eső (jobb oldali) mellékosztálya pontosan egy involúciót tartalmaz.

4.Lépés bizonyítása:

Először belátjuk, hogy $g \in G \setminus H$ esetén Sg legfeljebb egy involúciót tartalmaz. Tegyük fel, hogy nincs így, és $Sg = Sj_1 = Sj_2$, ahol j_1, j_2 különböző involúciók. Ekkor $1 \neq j_1 j_2 \in S$. Mivel S összes egységelemtől különböző eleme másodrendű, $1 = (j_1 j_2)^2 = j_1 j_2 j_1 j_2$. Tehát $j_2 j_1 = j_1 j_2$. Ekkor azonban j_1 kommutál a $j_1 j_2$ S-beli elemmel. Eszerint $j_1 \in S$, azaz $S = Sj_1 = Sg$, ami ellentmondás.

Megmutatjuk, hogy minden H-n kívűl eső mellékosztály tartalmaz egy involúciót. Mivel G összes involúciója konjugált, így $|G : S|$ van belőlük. $H \cong \mathrm{A}_4$ 3 involúciót és S 3 mellékosztályát tartalmazza. Jelöljük $i(Sg)$-vel az Sg-beli involúciók számát. Tudjuk, hogy $i(Sg) \leqq 1 \quad (\forall g \in G \setminus H)$. Tehát $|G : S| = 3 + \sum_{Sg: g \in G \setminus H} i(Sg) \leqq 3 + (|G : S| - 3)$. Egyenlőség csak úgy állhat fenn, ha $i(Sg) = 1 \quad \forall g \in G \setminus H$. Ezzel 4.Lépés bizonyítását befejeztük.

5.Lépés

$x \in G \setminus H$ esetén $|H \cap H^x| = 3$, és tetszőleges Hx-beli j involúció invertálja $H \cap H^x$ elemeit.

5.Lépés bizonyítása:

$H = \mathrm{N}_G(H)$ és $x \in G \setminus H$ miatt $H \neq H^x$. $H \cong \mathrm{A}_4$ miatt H-nak nincs 6-odrendű részcsoportja, így $H \cap H^x$ csak első-, másod- vagy harmadrendű lehet. Hx S 3 mellékosztályát tartalmazza, -mivel ezek nem H-beliek-, így Hx 3 involúciót tartalmaz. Jelölje őket j, j_1, j_2. Az involúciók segítségével keresünk $K = H \cap H^x$-ben két az egységelemtől különböző elemet. A 3.Lépés mutatja, hogy $H^x = H^j$. $K = H \cap H^x = H \cap H^j$, ezért $K^j = (H \cap H^j)^j = H^j \cap H = K$. $Hj = Hj_1 = Hj_2$ miatt $jj_1, jj_2 \in H$, továbbá $(jj_i)^{-1} = (jj_i)^j \in H^j \quad (i = 1, 2)$ miatt, $jj_1, jj_2 \in H \cap H^j = K$. Láttuk, hogy $K = H \cap H^j = H \cap H^x$ legfeljebb harmadrendű, így $|H \cap H^x| = 3$. $K = \{1, jj_1, jj_2\}$, így j, j_1, j_2 invertálja K elemeit.

6.Lépés

$T \in Syl_3 H$ esetén $\mathrm{C}_G(T) = T$

6.Lépés bizonyítása:

Tegyük fel, hogy $\mathrm{C}_G(T) > T$, és legyen $x \in \mathrm{C}_G(T) \setminus T$. $\mathrm{C}_H(T) = T$ miatt $x \in G \setminus H$. $|H \cap H^x| = 3$ az előző Lépés miatt. $T = T^x < H^x$, így $H \cap H^x = T$. Szintén az előző Lépés szerint, tetszőleges $j \in Hx$ involúció invertálja T elemeit. Ekkor azonban az xj H-beli elem is invertálja T elemeit. Tehát a 3.Lépés miatt $xj \in \mathrm{N}_H(T) = T$, és xj invertálja T elemeit. Ez azonban ellentmondás, mivel T Abel-csoport.

7.Lépés
$|G : H| \leqq 5$
7.Lépés bizonyítása:
Tegyük fel, hogy $|G : H| > 5$. Ekkor létezik H-nak 5 páronként különböző és H-tól is különböző mellékosztálya. Válasszunk mindegyikből egy-egy involúciót. Jelölje őket $j_1, j_2, ..., j_5$. Az 5.Lépés miatt $H \cap H^{j_i} \in Syl_3 H \quad (i = 1, 2, ..., 5)$. Mivel $H \cong \mathrm{A}_4$-nek 4 különböző 3-Sylowja van, ezért létezik $k_1 \neq k_2 \in \{1, 2, ..., 5\}$, hogy $H \cap H^{j_{k_1}} = H \cap H^{j_{k_2}}$. Jelöljük az előbbi metszetet T-vel. A $j_{k_i} \in Hj_{k_i} \quad (i = 1, 2)$ elemek az 5.Lépés miatt, invertálják T elemeit. Tehát $j_{k_1} j_{k_2} \in \mathrm{C}_G(T) = T < H$. Ezek szerint $Hj_{k_1} = Hj_{k_2}$, ami ellentmondás.

8.Lépés
$G \cong \mathrm{A}_5$
8.Lépés bizonyítása:
Ha $|G : H| < 5$, akkor a H mellékosztályai szerint vett reprezentáció egy homomorfizmust ad G-ről a legfeljebb 4-edfokú szimmetrikus csoport egy részcsoportjába. Ezek mindegyike feloldható, de perfekt csoportnak nincs feloldható nemtriviális faktora. Így $|G : H| = 5$. $|G| = |G : H||H| = 60$ és $G' = G$ miatt, az 5.1.5 Állításból következik, hogy $G \cong \mathrm{A}_5$.$\blacksquare$

5.1.7 Lemma:
Legyen $H \cong \mathrm{SL}(2, 3)$, és H valósítson meg fixpontmentes hatást a V K feletti véges dimenziós vektortéren. Ha egy W altér invariáns az $\mathrm{O}_2(H) \cong \mathrm{Q}_{2^3}$ szerint, akkor W invariáns H szerint is.
Bizonyítás:
Válasszunk a, c elemeket H-ból, hogy $o(a) = 4$, $o(c) = 3$, $o(ac) = 3$. Ezt megtehetjük, hisz az $\begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$ $\mathrm{SL}(2, 3)$-beli mátrixok tudják a rendekre vonatkozó feltételeket.
Legyen $b = a^{c^2}$ és $Q = \mathrm{O}_2(H)$, vegyük észre, hogy $Q = \langle a, b \rangle$.
A $KH \leq \mathrm{Hom}(V, V)$ csoportalgebrában dolgozva megmutatjuk, hogy c kifejezhető a és b segítségével, ebből pedig adódik a Lemma állítása. Legyen z H egyetlen másodrendű eleme. Választva egy tetszőleges $v \in V$ elemet $(v + vz)z = v + vz$. Így a fixpontmentesség miatt z csak a $\mathrm{Hom}(V, V)$-beli -1 lehet, és $\mathrm{char} K \neq 2$.
$0 = c^3 - 1 = (c - 1)(1 + c + c^2)$. c fixpontmentesen hat V-n, ezért $v(1 - c) = 0 \quad (v \in V)$, csak $v = 0$ esetén teljesül, tehát $1 - c$ invertálható. Ezek szerint $1 + c + c^2 = 0$. Hasonlóan

bizonyítható, hogy $1 + ac + acac = 0$. Az előzőek miatt $0 = (1 + ac + acac)c - a(1 + c + c^2) = c - a - ac + acac^2 = c - a - ac + ab$. Átrendezve az egyenletet $(1 - a)c = a(1 - b)$-t kapjuk. Szorozzuk be az előző bekezdés végén kapott egyenletünket balról a-val. $(1 + a)c = b - 1$. Tehát $(a - 1)(b - 1) = -a(1 - b) - (b - 1) = -(1 - a)c - (1 + a)c = -2c$. Felhasználva, hogy $\mathrm{char}K \neq 2$ $c = -\frac{1}{2}(a - 1)(b - 1)$. Ezzel a bizonyítást befejeztük.■

5.1.8 Tétel:

Legyen G olyan véges perfekt csoport, hogy G 2-Sylowjai diédercsoportok, G összes involúciója konjugált. Továbbá tetszőleges $q, r > 2$ nem feltétlenül különböző prímek esetén, ha $U < G$ és $|U| = qr$, akkor U ciklikus. Legyen $S \in Syl_2G$.

(i) Legyen $p > 2$ G rendjének prímosztója, $P \in Syl_pG$. Ekkor P ciklikus, $\mathrm{N}_G(P)/\mathrm{C}_G(P)$ nemtriviális kommutatív 2-csoport. Továbbá P (és így G tetszőleges p-csoportja) összes elemét invertálja valamely 2-hatvány rendű elem.

(ii) $\mathrm{C}_G(S) \leq S$

(iii) $|S| \geqq 4$

(iv) $\mathrm{Z}(G) = 1$, $\mathrm{O}_2(G) = 1$

(v) Ha $K \cong \mathrm{Z}_2 \times \mathrm{Z}_2$ részcsoportja G-nek, akkor $3 \mid |\mathrm{N}_G(K) : \mathrm{C}_G(K)|$.

(vi) Legyen $F \lhd S$, $|F| = 2$. Ekkor $\mathrm{C}_G(F) = \mathrm{O}_{2'}(\mathrm{C}_G(F))S$

(vii) Ha $K \cong \mathrm{Z}_2 \times \mathrm{Z}_2$ G részcsoportja, és $3 \nmid |\mathrm{C}_G(K)|$, ekkor létezik G-nek A_4-gyel izomorf K-t tartalmazó részcsoportja.

(viii) Létezik G-nek A_4-gyel izomorf részcsoportja.

Bizonyítás:

(i) G qr-rendű ($q, r > 2$ prímek) csoportjaira tett feltevés és a 2.3.8 Tétel miatt P csak ciklikus lehet (hisz P centrumának valamely p-rendű eleme egy, az általa generált csoportban nem található, p-rendű elemmel elemi Abel-csoportot generálna).

Burnside normál p-komplementum tétele (1.3.3 Tétel) miatt $\mathrm{N}_G(P) > \mathrm{C}_G(P)$. Különben létezne G-nek P-vel izomorf faktora, ami feloldható, G azonban perfekt, így ez nem lehetséges. $\mathrm{N}_G(P)/\mathrm{C}_G(P)$ Abel-csoport, hisz P ciklikus (hivatkozhatunk tehát az 1.3.4 Állításra).

p szerinti indukciót alkalmazva mutatjuk meg, hogy $\mathrm{N}_G(P)/\mathrm{C}_G(P)$ 2-csoport. Legyen q prímosztója $|\mathrm{N}_G(P) : \mathrm{C}_G(P)|$-nek. Az 1.3.4 Állítás miatt $|\mathrm{Aut}(P)| = p^{k-1}(p - 1)$ ($|P| = p^k$). A faktorcsoport izomorfikusan beágyazható $\mathrm{Aut}(P)$-be, tehát $q \mid (p - 1)$, speciálisan $q < p$.

Ebből G legkisebb páratlan prímosztójára adódik, hogy a faktor 2-csoport. $\mathrm{N}_G(P)$-nek tehát létezik 2-hatványrendű $\mathrm{C}_G(P)$-n kívül eső eleme. Tekintsük az adott elemenek azt a z hatványát, melyre z nem centralizálja P generáló elemét, de z^2 igen. Mivel z másodrendű automorfizmust valósít meg a P ciklikus csoporton, így szükségképpen invertálja annak elemeit. Az indukció első lépését elvégeztük. Legyen a továbbiakban $p > 2$ G egy tetszőleges prímosztója, és tegyük fel, hogy a nála kisebb páratlan prímosztókra már beláttuk az állítást. Legyen $Q \in Syl_q(\mathrm{N}_G(P))$. $Q \nsubseteq \mathrm{C}_G(P)$ q választása folytán. A Frattini-elv alkalmazásával és az indukciós feltevéssel megmutatjuk, ha $q \neq 2$, akkor $Q \leq \mathrm{N}_G(P)'$, ez viszont ellentmond a faktorcsoport kommutativitásának.

Belátjuk, hogy létezik olyan Q-beli elem, mely centralizálja P-t. Legyen a P egyetlen p-edrendű csoportjának egy generáló eleme, b pedig Q egyetlen q-ad rendű csoportjának generáló eleme. Mivel Q normalizálja P-t, így $\langle a, b\rangle$ pq-adrendű csoport. Legyen x P generálóeleme és $x^{p^{k-1}} = a$. Megmutatjuk, ha b nem centralizálja x-et, akkor a-t sem centralizálhatja. Így $\langle a, b\rangle$ nem lenne ciklikus, ami ellentmondás.

Legyen $x^b = x^r$, ekkor $(r, p) = 1$. Tegyük fel, hogy $x \neq x^r$, ezért $p^k \nmid r - 1$. Ha $a^b = a$, akkor $(x^{p^{k-1}})^b = (x^{p^{k-1}})^r = x^{rp^{k-1}} = x^{p^{k-1}}$ miatt $rp^{k-1} \equiv p^{k-1} \pmod{p^k}$, így $r \equiv 1 \pmod{p}$. $x = x^1 = x^{b^q} = x^{r^q}$ miatt $r^q \equiv 1 \pmod{p^k}$. Tehát p^k osztja $r^q - 1 = (r-1)(r^{q-1} + r^{q-2} + ... + 1)$-et. Mivel p $(r - 1)$-et legfeljebb a $(k - 1)$-dik hatványon osztja, így $p | r^{q-1} + r^{q-2} + ... + 1$. Ez viszont nem lehetséges, hisz $r \equiv 1 \pmod{p}$ miatt $r^{q-1} + r^{q-2} + ... + 1 \equiv q \pmod{p}$.

Tehát $1 < \mathrm{C}_Q(P)$, melyet jelöljünk a továbbiakban C-vel. Az indukciós feltevés szerint létezik $y \in \mathrm{N}_G(C)$ 2-hatványrendű elem, mely invertálja C elemeit. y segítségével keresünk egy y^* elemet, mely invertálja Q elemeit és normalizálja P-t.

$P \in Syl_p\mathrm{C}_G(C)$, így a Frattini-elv szerint $\mathrm{N}_G(C) = \mathrm{C}_G(C)\mathrm{N}_{\mathrm{N}_G(C)}(P)$. $y = c_1 y_1$, ahol $c_1 \in \mathrm{C}_G(C)$, $y_1 \in \mathrm{N}_{\mathrm{N}_G(C)}(P)$. $y_1 = c_1^{-1} y$ tehát továbbra is invertálja C elemeit és normalizálja P-t.

Jelölje N $\mathrm{N}_G(P) \cap \mathrm{N}_G(C)$-t. Q ciklikus, így centralizálja C-t. Tehát $Q \in Syl_q(\mathrm{N}_G(P) \cap \mathrm{C}_G(C))$. Ismét a Frattini-elvet alkalmazva $N = (\mathrm{N}_G(P) \cap \mathrm{C}_G(C))\mathrm{N}_N(Q)$. $y_1 = c_2 y_2$, ahol $c_2 \in \mathrm{N}_G(P) \cap \mathrm{C}_G(C)$, $y_2 \in \mathrm{N}_N(Q)$. $y_2 = c_2^{-1} y_1$ tehát továbbra is invertálja C elemeit, normalizálja P-t és normalizálja Q-t is. y_2 invertálja C elemeit, így rendjét osztja 2. Tekintsük y_2-nak azt az y^* hatványát, melynek rendje 2-hatvány, nem centralizálja a Q ciklikus csoport elemeit, és y^{*2} már centralizálja Q-t. Mivel y_2 invertálja Q egy részcsoportját, így van a feltételeknek megfelelő hatványa. Ekkor y^* invertálja Q elemeit és normalizálja P-t.

Tekintsük a $[Q, y^*] = \langle [q, y^*] | q \in Q\rangle$ csoportot. $y^* \in \mathrm{N}_G(Q)$ miatt $[Q, y^*] \leq Q$. Legyen c Q generáló eleme, ekkor $[c, y^*] = c^{-1}c^{y^*} = c^{-2}$ is generálja Q-t, ha $q \neq 2$. Ebben az esetben $Q = [Q, y^*]$. Ezért $Q \leq \mathrm{N}_G(P)' \leq \mathrm{C}_G(P)$, ami ellentmond Q választásának. Tehát $q = 2$.

Az indukció első lépéséhez hasonlóan bizonyítható, hogy létezik 2-hatványrendű elem, mely invertálja P elemeit.

(ii) Ha $\mathrm{C}_G(S)$ 2-csoport, akkor nyilvánvalóan $\mathrm{C}_G(S) \leq S$. Különben létezik egy g prímrendű eleme. Tekintsük az $N = \mathrm{N}_G(\langle g\rangle)$ csoportot. $S \in Syl_2N$, továbbá az (i) pont miatt létezik egy y 2-hatványrendű elem N-ben, mely invertálja g-t. A Sylow-tételek szerint y konjugált valamely S-beli elemmel egy N-beli elem által. Azonban S centralizálja $\langle g\rangle$-t, így N-beli konjugáltjai is centralizálják. Az ellentmondás bizonyítja az állítást.

(iii) Az (i) pont miatt G páros rendű. Tegyük fel, hogy $4 \nmid |G|$. Legyen $i \in G$ egy involúció, és tekintsük a $\varrho : G \mapsto \mathrm{S}_{|G|}$ reguláris reprezentációt. i^ϱ egy páratlan involúció, ezért $G^\varrho \cap \mathrm{A}_{|G|}$ őse 2 indexű normálosztó lenne. Tehát lenne a G perfekt csoportnak Z_2-vel izomorf faktora, ami nem lehetséges. $4 \mid |G|$, ezért $|S| \geqq 4$.

(iv) Az (i) pont szerint $\mathrm{Z}(G)$ nem tartalmazhat páratlan rendű elemet. Ha $\mathrm{Z}(G)$ tartalmaz páros rendű elemet, akkor tartalmaz egy involúciót is. Ennek az involúciónak a konjugált osztálya 1-elemű, a feltételeink szerint G összes involúciója konjugált. Így G egyetlen involúciót tartalmaz. Ekkor G 2-Sylowjai nem lehetnek diédercsoportok ($|S| \geqq 4$). Tehát $\mathrm{Z}(G) = 1$.

$\mathrm{O}_2(G) \leq S$ csak ciklikus vagy diédercsoport lehet, mindkét esetben könnyen meggondolható, hogy $H = \mathrm{Aut}(\mathrm{O}_2(G))$ feloldható. $G/\mathrm{C}_G(\mathrm{O}_2(G))$ izomorfikusan beágyazható H-ba, így feloldható. Mivel G perfekt, ez csak $G = \mathrm{C}_G(\mathrm{O}_2(G))$ esetén lehetséges. $\mathrm{O}_2(G) \leq \mathrm{Z}(G) = 1$.

(v) Elég megmutatni, hogy $\mathrm{N}_G(K)$ tranzitíven hat K involúcióin. A permutáció csoportok elméletéből ismert, hogy ekkor az alaphalmaz rendje osztja a csoport rendjét. Tehát, ha $\mathrm{N}_G(K)$ tranzitíven hat $K \setminus \{1\}$-en, akkor $\mathrm{N}_G(K)/\mathrm{C}_G(K)$ is, így $3||\mathrm{N}_G(K) : \mathrm{C}_G(K)|$.

Válasszunk 2 tetszőleges involúciót K-ból, a-t és b-t. Megmutatjuk, hogy létezik $\mathrm{N}_G(K)$-nak olyan eleme, amely felcseréli őket.

Tegyük fel, hogy $K \in Syl_2G$. Mivel az összes G-beli involúció konjugált, így valamely $g \in G$-re $a^g = b$. K és K^g tehát $\mathrm{C}_G(b)$-beli 2-Sylowok. A Sylow-tételek miatt létezik $h \in \mathrm{C}_G(b)$, hogy $K^h = K^g$. $gh^{-1} \in \mathrm{N}_G(K)$ és $a^{gh^{-1}} = b^{h^{-1}} = b$.

Tegyük fel, hogy K nem 2-Sylow G-ben. Legyen $c = ab$. Az összes involúció konjugált G-ben. Konjugált elemek centralizátorai konjugáltak. Mivel tetszőleges 2-Sylow centrumában van involúció, így tetszőleges involúció centralizátora tartalmaz egy 2-Sylowot. Válasszunk $\mathrm{C}_G(c)$-ben, egy olyan $\mathrm{C}_G(c)$-beli, és így G-beli, 2-Sylowot, amely tartalmazza K-t, jelöljük őt R-rel. Vegyük észre, hogy $|R| \geqq 8$ diédercsoport, ezért $K = \mathrm{C}_R(K) < \mathrm{N}_R(K)$. Választva egy x elemet $\mathrm{N}_R(K) \setminus \mathrm{C}_R(K)$-ból, x centralizálja $c = ab$-t, és mivel nem centralizálja K-t, így szükségképpen kicseréli a-t és b-t.

(vi) Jelöljük C-vel $\mathrm{C}_G(F)$-et, és L-lel $\mathrm{O}^2(C)$-t.

Ha $2 \nmid |L|$, akkor $L = \mathrm{O}_{2'}(C)$ és $C = LS$ nyilvánvalóan teljesül.

Tegyük fel, hogy $2 \mid |L|$. L-nek nem lehet 2-hatvány indexű valódi normálosztója, hisz, ha lenne ilyen, akkor $\mathrm{O}^2(L) < L$ teljesülne. És $\mathrm{O}^2(L)\,\mathrm{char}\, L \trianglelefteq C$ miatt $\mathrm{O}^2(L) \triangleleft C$, továbbá $\mathrm{O}^2(L)$ indexe C-ben egy nagyobb 2-hatvány lenne, mint L-é, amit ellentmondana L definíciójának.

Belátjuk, hogy $L \cap S \in Syl_2 L$. Tegyük fel, hogy $Q \in Syl_2 L$, ekkor Q beletehető valamely $P \in Syl_2 C$ csoportba, és $P \cap L = Q$. Mivel $S \in Syl_2 C$, így valamely $x \in C$ elemre $P^x = S$. Tehát $|Q| = |L \cap P| = |L^x \cap P^x| = |L \cap S|$. Jelöljük a továbbiakban $L \cap S$-et T-vel.

Tegyük fel, hogy $|T| = 2$. Ekkor $\mathrm{N}_L(T) = \mathrm{C}_L(T)$, így Burnside normál p-komplementum tétele miatt létezik L-nek 2 indexű részcsoportja. Ez pedig ellentmondás.

Tegyük fel, hogy $|T| \geqq 4$. L-nek nincs 2-indexű részcsoportja. Mivel T részcsoportja G valamely 2-Sylowjának, így csak ciklikus vagy diédercsoport lehet. $|T| \geqq 4$, így létezik T-nek 2 indexű ciklikus csoportja. Alkalmazhatjuk az 5.1.2 Lemmát, L összes involúciója konjugált. $L \trianglelefteq C$, $S \leq C$ ezért $T = L \cap S \trianglelefteq S$. Vegyük észre, hogy mivel S diéder 2-csoport, és $|F| = 2$, $F \trianglelefteq S$, $T \trianglelefteq S$, így $F < T \leq L$. Hisz F vagy a teljes centrum, és p-csoportbeli nemtriviális normálosztó nemtriviálisan metszi a centrumot, vagy S 4-elemű, így $T = S$. F része C centrumának, ezért része L centrumának is. Így L-beli konjugált osztálya 1 elemű. Mivel az összes involúció konjugált L-ben, így L pontosan egy involúciót tartalmaz. $Syl_2 L$ tehát ciklikus. Az 1.3.5 Következmény (i) pontja miatt létezik L-nek 2-hatványrendű faktora. Ezzel ismét ellentmondásra jutottunk.

(vii) Legyen $T \in Syl_3 \mathrm{N}_G(K)$. Az (v) pont miatt $1 < T$. $\mathrm{N}_G(K)/\mathrm{C}_G(K)$ izomorf $\mathrm{Aut}(\mathrm{Z}_2 \times \mathrm{Z}_2) \cong \mathrm{S}_3$ egy részcsoportjával. Mivel $\mathrm{C}_G(K)$ $3'$-csoport, így $T \cong \mathrm{Z}_3$. Ekkor pedig $KT \cong (\mathrm{Z}_2 \times \mathrm{Z}_2) \rtimes \mathrm{Z}_3 \cong \mathrm{A}_4$.

(viii) Jelölje továbbra is F az $S \in Syl_2 G$ egy másodrendű normálosztóját, és C $\mathrm{C}_G(F)$-et. Válasszunk S-ben egy tetszőleges K Klein-csoportot (azaz $K \cong \mathrm{Z}_2 \times \mathrm{Z}_2$), vegyük észre, hogy $F < K$. Ha $3 \nmid |\mathrm{C}_G(K)|$, akkor a (vii) pont alapján az állítás teljesül.

Ha $3 \mid |\mathrm{C}_G(K)|$, akkor K segítségével keresünk S-ben egy másik Klein-csoportot. Vegyük észre, hogy $K < S$. Ugyanis, az (ii) pont alapján, $K = S$ esetén $\mathrm{C}_G(K) = K$ $3'$-csoport. Tehát $F = \mathrm{Z}(S)$, hisz F nyilvánvalóan a centrum része, és mivel $|S| > 4$ diéder 2-csoport, így a centruma 2 elemű.

Legyen $T \in Syl_3 C$. $\mathrm{C}_G(K) \leq C$, így $1 < T$. Feltehetjük, hogy T S-invariáns. Hiszen a (vi) pont alapján $C = \mathrm{O}_{2'}(C)S$, ezért C összes 3-Sylowja része $\mathrm{O}_{2'}(C)$-nek. S koprím módon hat $\mathrm{O}_{2'}(C)$-n, így az 1.1.5 Tétel alapján $\mathrm{O}_{2'}(C)$-nek létezik S-invariáns 3-Sylowja, ez pedig C-nek is S-invariáns 3-Sylowja.

Megmutatjuk, hogy $T \in Syl_3 \mathrm{C}_G(K)$. Legyen $R \in Syl_3 \mathrm{C}_G(K)$. Ekkor $R \leq \mathrm{O}_{2'}(C)$ K-invariáns 3-csoport. Az 1.1.5 Tétel (ii) pontja alapján $R \leq Q$, ahol $Q \in Syl_3 \mathrm{O}_{2'}(C) = Syl_3 C$ és Q K-invariáns (hisz $K < S$ koprím módon hat $\mathrm{O}_{2'}(C)$-n). Q és T K-invariáns 3-Sylowjai $\mathrm{O}_{2'}(C)$-nek, ezért, ismét csak az 1.1.5 Tétel alapján, konjugáltak valamely $x \in \mathrm{C}_{\mathrm{O}_{2'}(C)}(K)$ elem által, azaz $Q^x = T$. Tehát $R^x \leq T$, és $R^x \leq \mathrm{C}_G(K)$. Az (i) pont szerint R^x és T is ciklikusak, ezért R^x egyetlen 3-adrendű csoportja megegyezik T egyetlen 3-rendű csoportjával. K elemei

tehát centralizálják T egyetlen 3-adrendű részcsoportját. Ezért nem invertálhatják T generáló elemét, így szükségképpen centralizálják. Tehát $T \in \mathrm{C}_G(K)$, mivel $T \in Syl_3C$ és $\mathrm{C}_G(K) \leq C$, így $T \in Syl_3\mathrm{C}_G(K)$.
$K^S = \langle K^s | s \in S\rangle$. T S-invariáns, K pedig centralizálja T-t, ezért K^S is centralizálja T-t.
S diéder 2-csoport és $|S| > 4$, ezért S involúciói 3 konjugált osztályba sorolhatók. Az egyetlen elemű konjugált osztály a centrum, a többi (tükrözéseknek megfelelő) involúció két konjugált osztályba sorolódik (a fixponttal bíró tükrözések és a fixponttal nem rendelkezőek). Bármely két nem centrumbeli, különböző konjugált osztályhoz tartozó involúció generálja a csoportot. S Klein-csoportjait egy centrumbeli és egy másik involúció generálja. Ezért S-et megkaphatjuk $S = K^SL$ alakban, ahol L egy Klein-csoport, mely nem konjugált S-ben K-val.
T S-invariáns, azaz $S \leq \mathrm{N}_G(T)$. Az (i) pont alapján S valamely eleme invertálja T elemeit. Mivel $S = K^SL$ és K^S centralizálja T-t, így L valamely eleme invertálja T elemeit.
Ha $3 \mid |\mathrm{C}_G(L)|$, akkor a (vii) pont alapján létezik G-nek A_4-gyel izomorf részcsoportja.
Ha $3 \nmid |\mathrm{C}_G(L)|$, akkor mivel a bizonyítás elején K-t tetszőlegesnek választottuk, ezért a centralizátor rendjére tett feltevés mellett, hasonló gondolatmenettel bizonyítható, hogy $T \in Syl_3\mathrm{C}_G(L)$, mint K esetében. Ekkor azonban L-nek centralizálnia kellene T-t. Ezzel a bizonyítást befejeztük.$\blacksquare$

5.1.9 Következmény:

(i) Legyen A perfekt Frobenius-komplementum. Az 5.1.4 Lemma és a 2.3.5 Következmény segítségével belátható, hogy $A/\langle z\rangle$ (ahol z A egyetlen involúciója) teljesíti az 5.1.8 Tétel feltételeit, így a Tétel állításai igazak rá.
(ii) Legyen A perfekt Frobenius-komplementum, z A egyetlen involúciója. Ekkor $A/\langle z\rangle$-nek létezik A_4-gyel izomorf részcsoportja. Jelölje az adott részcsoport ősét H. Könnyen meggondolható, hogy $H \cong \mathrm{Q}_{2^3} \rtimes \mathrm{Z}_3 \cong \mathrm{SL}(2,3)$.

5.1.10 Állítás:

Legyen A véges csoport, és hasson automorfizmusokon keresztül fixpontmentesen a V K test feletti véges dimenziós vektortéren. Legyen $L|K$ egy testbővítés. Ekkor létezik egy véges dimenziós vektortér az L test felett, hogy A rajta továbbra is fixpontmentesen hat.
Bizonyítás:
Legyen $W = L \underset{K}{\otimes} V$ K feletti vektortér. W-n ekkor megadható egy L test feletti vektortér struktúra. Legyen $l_1 \in L$, $l_2 \otimes v \in W$, ekkor definiáljuk az $l_1(l_2 \otimes v) = (l_1l_2) \otimes v$ szorzatot.

Ennek értelemszerű kiterjesztésével egy jól definiált L feletti véges dimenziós vektorteret kapunk.
Legyen $a \in A$, $v \otimes l \in W$, ekkor a hatását értelmezzük az $a(l \otimes v) = l \otimes av$ képlettel, majd ezt terjesszük ki az egész L feletti vektortérre. a karakterisztikus polinomjának ugyan lehetnek új gyökei, ám ezek mindegyike $L \setminus K$-beli. Ezért $1 \in K$ nem lehet gyöke a karakterisztikus polinomnak továbbra sem. A tehát fixpontmentesen hat a konstruált L feletti vektortéren.■

5.1.11 Állítás:
Legyen G olyan véges csoport, melynek létezik H 2 indexű Abel-részcsoportja. Ekkor G irreducibilis karakterei első- vagy másodfokúak.
Bizonyítás:
Legyen $\varphi : G \mapsto \mathrm{GL}(n, V_{\mathbb{C}})$ egy tetszőleges irreducibilis reprezentáció. $\varphi\mid_H$ H egy reprezentációja, így elsőfokú reprezentációk direkt összege. Tehát V felbomlik H-invariáns egydimenziós alterek direkt összegére. Legyen v valamely altér generálóeleme, g $G \setminus H$ tetszőleges elem. Jelölje w vg-t, W $\langle v, w\rangle$-t. Megmutatjuk, hogy W G-invariáns, így $V = W$.
Mivel $\langle v\rangle$ H-invariáns, így tetszőleges $a \in H$ esetén létezik $\lambda_a \in \mathbb{C}$, melyre $va = \lambda_a v$. H normálosztó (hisz 2 indexű), ezért tetszőleges $a \in H$ esetén létezik $b \in H$, melyekre $ga = bg$. Továbbá mivel H 2 indexű, így $g^2 \in H$, jelöljük őt c-vel. A következő számolások mutatják W G-invarianciáját: $va = \lambda_a v$, $wa = vga = vbg = \lambda_b vg = \lambda_b w$, $vg = w$, $wg = vgg = vc = \lambda_c v$.
Mivel W 1- vagy 2-dimenziós, így a hozzátartozó karakter első- vagy másodfokú.■

5.1.12 Következmény:
Legyen G olyan nemkommutatív véges csoport, melynek létezik H 2 indexű Abel-részcsoportja. Ha G fixpontmentesen hat a V $\mathbb{C}$ feletti 2-dimenziós vektortéren, akkor V irreducibilis G szerint. Ugyanis a V-hez tartozó lineáris reprezentáció másodfokú vagy elsőfokúak direkt összege. Az utóbbi esetben azonban $1 < G'$ identikusan hatna V-n, hisz tetszőleges elsőfokú reprezentáció magja tartalmazza G'-t.

5.1.13 Tétel:
Legyen G véges irreducibilis részcsoportja $\mathrm{GL}(2, \mathbb{C})$-nek. Ekkor vagy $G/\mathrm{Z}(G)$ izomorf az A_4, S_4 vagy A_5 csoportok valamelyikével, vagy létezik G-nek 2 indexű Abel-részcsoportja.

5.1.14 Tétel: (Zassenhaus)
Legyen A perfekt Frobenius-komplementum. Ekkor $A \cong \mathrm{SL}(2,5)$.
Bizonyítás: (Meierfrankenfeld)
Az 5.1.3 Lemma, illetve annak bizonyitása szerint A fixpontmentesen hat egy V (véges dimenziós) K feletti vektortéren, ahol $K = \mathrm{GF}(p)$, p pedig az A-hoz tartozó N Frobenius-mag rendjének egy prímosztója. Speciálisan $(|A|, p) = 1$. Az előbbi feltétel miatt A hatása felemelhető egy $\mathbb{Q}_p$ feletti vektortérre ($\mathbb{Q}_p$ a p-adikus számok teste). Az 5.1.10 Állítás szerint a hatás fixpontmentes lesz a $\overline{\mathbb{Q}}_p$ feletti megfelelő vektortéren is, ahol $\overline{\mathbb{Q}}_p$ $\mathbb{Q}_p$ algebrai lezártja. $\overline{\mathbb{Q}}_p$ a p-adikus értékelés által indukált metrikára nézve nem teljes, de ha tekintjük a teljessé tételével kapott $\mathbb{C}_p$ testet, az már nemcsak teljes, de algebrailag zárt is lesz. Ezek a $\mathbb{C}_p$ testek számítanak a $\mathbb{C}$ komplex test p-adikus megfelelőinek. Noha $\mathbb{C}_p$ topológikusan nagyon eltér $\mathbb{C}$-től, meglepő módon mint tisztán algebrai struktúra a $\mathbb{C}_p$ test minden p-re a $\mathbb{C}$ komplex testtel izomorf. (Mindegyikük úgy kapható, hogy $\mathbb{Q}$-hoz egy megfelelő transzcendenciabázist adjungálunk, majd vesszük a kapott test algebrai lezártját.) Végeredményben tehát feltehetjük, hogy A egy $\mathbb{C}$ feletti vektortéren hat.
Az 5.1.9 Következmény miatt létezik A-nak H $\mathrm{SL}(2,3)$-mal izomorf részcsoportja. Legyen $Q = \mathrm{O}_2(H)$ ($Q \cong \mathrm{Q}_{2^3}$) és $S \in Syl_2 A$ olyan 2-Sylow, melyre $Q \leq S$. (S általánosított kvaterniócsoport.)
Legyen z A egyetlen involúciója, jelölje a hozzátartozó természetes homomorfizmust felülvonás. Legyen $\overline{F}$ másodrendű normálosztó $\overline{S}$-ben, és F az őse. Vegyük észre, hogy F 4-edrendű, így ciklikus, továbbá $F \lhd Q$. Hiszen $|S| = 2^3$ esetén $S = Q$, míg $|S| \geqq 2^4$ esetén F S 2 indexű ciklikus csoportjának egyetlen negyedrendű részcsoportja, azaz $\mathrm{Z}(\overline{S})$ őse.
Az 5.1.11 Állítás miatt létezik V-nek 2-dimenziós W altere, melyet S invariánsa hagy és S irreducibilis W-n. Az 5.1.7 Lemmának köszönhetően H is invariánsan hagyja a szóban forgó alteret. A bizonyítás további részeit lépésekre bontjuk.

1.Lépés
Legyen R A olyan részcsoportja, melyre $H \leq R$, és R invariánsan hagyja V egy 2-dimenziós alterét. Ekkor $R/\mathrm{Z}(R)$ izomorf az A_4, S_4 vagy A_5 csoportok valamelyikével. Továbbá $4 \nmid |\mathrm{Z}(R)|$.
1.Lépés bizonyítása:
R fixpontmentessége és az 5.1.12 Következmény ($Q < R$) miatt egy hűséges, irreducibilis másodfokú lineáris reprezentációt kapunk a szóban forgó altér segítségével. Alkalmazhatjuk az 5.1.13 Tételt, vagy $R/\mathrm{Z}(R)$ izomorf az $\mathrm{A}_4, \mathrm{S}_4$ vagy A_5 csoportok valamelyikével, vagy $R/\mathrm{Z}(R)$-nek létezik 2 indexű Abel-csoportja. Az utóbbi eset nem lehetséges, ugyanis $H\mathrm{Z}(R)/\mathrm{Z}(R) \cong H/\mathrm{Z}(R) \cap H = H/\langle z \rangle \cong \mathrm{A}_4$ nem Abel-csoport, és nincs 2 indexű részcsoportja.

R 2-Sylowjai általánosított kvaterniócsoportok, melyek centruma 2 elemű, így $4 \nmid \mathrm{Z}(R)$.

2.Lépés

$|S| \leqq 2^4$

2.Lépés bizonyítása:

Alkalmazzuk az 1.Lépést $R = \langle H, S\rangle$ szereposztással. $R/\mathrm{Z}(R)$ rendjét az (i) pont szerint 2-nek legfeljebb a 3-dik hatványa osztja, míg $\mathrm{Z}(R)$ rendjét legfeljebb az első. R rendjét tehát legfeljebb 2 4-dik hatványa osztja. Mivel R tartalmaz egy teljes 2-Sylowot, így adódik az állítás.

3.Lépés

$\mathrm{O}^2(\mathrm{N}_A(F)) \leq \mathrm{C}_A(Q)$

3.Lépés bizonyítása:

Először megmutatjuk, hogy $Q \leq \mathrm{O}_2(\mathrm{N}_A(F))$. Vizsgáljuk e célból a $D = \langle Q, Q^g\rangle$ csoportot, ahol $g \in \mathrm{N}_A(F)$. $F \lhd Q$, $F = F^g \lhd Q^g$ miatt $F \lhd D$. Legyen $a \in Q \setminus F$. Világos, hogy $D/F = \langle aF, a^gF\rangle$. aF és a^gF is másodrendűek, így csak diédercsoportot generálhatnak. Ezek szerint $\langle aa^gF\rangle$ ciklikus 2 indexű részcsoport D/F-ben. Mivel Q és Q^g kvaterniócsoportok, ezért a és a^g invertálják F elemeit. aa^g centralizálja F elemeit. Tehát $\langle aa^g, F\rangle$ 2 indexű Abel-csoport D-ben. Az 5.1.12 Állítás szerint D invariánsan hagyja V-nek valamely 2-dimenziós alterét.
$Q \leq D$, tehát az 5.1.7 Lemma miatt H is invariánsan hagyja az alteret. Alkalmazzuk az 1.Lépést az $R = \langle H, D\rangle$ választás mellett. $R/\mathrm{Z}(R)$ izomorf A_4,S_4,A_5 valamelyikével.
A három permutáció csoport mindegyikben a másodrendű elemek centralizátora 2-csoport. $F\mathrm{Z}(R)/\mathrm{Z}(R)$ másodrendű, hisz A egyetlen involúcióját $\mathrm{Z}(R)$ és a 4-edrendű F is tartalmazza (és $F \nsubseteq \mathrm{Z}(R)$). $D\mathrm{Z}(R)/\mathrm{Z}(R) \leq \mathrm{C}_{R/\mathrm{Z}(R)}(F\mathrm{Z}(R)/\mathrm{Z}(R))$, ugyanis $D = \langle a, a^g, F\rangle$, és a generáló elemek mindegyik normalizálja F-et, így a nekik megfelelő elemek centralizálják a 2 elemű faktorcsoportot. $|D\mathrm{Z}(R) : \mathrm{Z}(R)| = \frac{|D|}{|D \cap \mathrm{Z}(R)|}$ tehát 2-hatvány. Megmutatjuk, hogy $|D \cap \mathrm{Z}(R)|$ 2-hatvány, és így D 2-csoport. Ha D/F 2-csoport, akkor ez nyilvánvaló. Különben D/F olyan diéder-csoport, amely nem Klein-csoport, így $|\mathrm{Z}(D/F)| \leqq 2$. $\mathrm{Z}(D)$ részcsoportja $\mathrm{Z}(D/F)$ ősének, ezért 2-csoport. Így $D \cap \mathrm{Z}(R) \leq \mathrm{Z}(D)$ is 2-csoport.
$D = \langle Q, Q^g\rangle$ tehát 2-csoport, rendje így legfeljebb 2^4, ezért $QQ^g = Q^gQ$. Ez pedig mutatja, hogy $Q^{\mathrm{N}_A(F)} = \langle Q^g | g \in \mathrm{N}_A(F)\rangle$ 2-normálosztó $\mathrm{N}_A(F)$-ben. Így $Q \leq \mathrm{O}_2(\mathrm{N}_A(F))$.
Jelölje L $\mathrm{O}_2(\mathrm{N_A(F)})$-et. Ha $|L| = 2^4$, akkor L izomorf Q_{2^4}-nel, így automorfizmus csoportja 2-csoport. Ezek szerint $\mathrm{N}_A(F)/\mathrm{C}_{\mathrm{N_A(F)}}(L)$ izomorfikusan beágyazható egy 2-csoportba. Mivel $F < Q < L$, ezért $\mathrm{C}_{\mathrm{N}_A(F)}(L) = \mathrm{C}_A(L)$. Így $\mathrm{O}^2(\mathrm{N}_A(F)) \leq \mathrm{C}_A(L) \leq \mathrm{C}_A(Q)$.
Ha $|L| = 2^3$, akkor $L = Q$. L automorfizmus csoportja ebben az esetben S_4. Azonban

$\mathrm{N}_A(F)/\mathrm{C}_{\mathrm{N}_A(F)}$ nem tartalmazhatja L harmadrendű automorfizmusait, hisz azok nem normalizálják F-et. Így az előző gondoltamenet újra végig mondható.

4.Lépés
$Q \in Syl_2 A$
4.Lépés bizonyítása:
Tegyük fel, hogy $Q < S$. Ekkor a 2.Lépés miatt $|S| = 2^4$. Így S-nek van Q-tól különböző K, kvaterniócsoporttal izomorf részcsoportja. Vegyük észre, hogy $Q \cap K = F$. (Hisz F-et, a bizonyítás elején említett okokból kifolyólag, mindkét csoport tartalmazza.)
Nézzük először azt az esetet, amikor K-t tartalmazza egy $H_1 \leq A$ $\mathrm{SL}(2,3)$-mal izomorf részcsoport. S fixpontmentesen hat a W 2-dimenziós alterén. W invariáns $Q, K < S$ szerint is, így az 5.1.7 Lemma értelmében H és H_1 szerint is. Tekintsük az $R = \langle H, H_1, S\rangle$ csoportot, és alkalmazzuk az 1. Lépést. $R/\mathrm{Z}(R) \cong \mathrm{S}_4$, ugyanis $S < R$ rendjét osztja 2^4-en, ezért a faktorcsoport rendjét legalább 2^3-nak osztania kell. Az 1.Lépésben látotthoz hasonló számolás mutatja, hogy $H\mathrm{Z}(R)/\mathrm{Z}(R) \cong \mathrm{A}_4$ és $H_1\mathrm{Z}(R)/\mathrm{Z}(R) \cong \mathrm{A}_4$. S_4-ben A_4-nek pontosan egy példánya található, ezért ennek őse $H\mathrm{Z}(R)$-rel és $H_1\mathrm{Z}(R)$-rel is egyenlő. Ezért $H\mathrm{Z}(R) \geq \langle H, H_1\rangle > \langle Q, K\rangle = S$. Ellentmondásra jutottunk, hiszen $2^4 \nmid |H\mathrm{Z}(R)| = \frac{|H||\mathrm{Z}(R)|}{|H \cap \mathrm{Z}(R)|}$.
Nézzük azt az esetet, amikor K-t nem tartalmazza $\mathrm{SL}(2,3)$-mal izomorf részcsoportot. Az 5.1.8 Tétel (vii) pontja és az 5.1.9 Következmény (ii) pontja alapján $3 \mid |\mathrm{C}_{\overline{A}}(\overline{K})|$, ekkor 3 osztja az ősének rendjét is, ami K normalizátorának részcsoportja ($\langle z\rangle < K$), azaz $3 \mid |\mathrm{N}_A(K)|$ is teljesül. Az 5.1.8 Tétel (vi) pontja alapján $\mathrm{C}_{\overline{A}}(\overline{F}) = \mathrm{O}_{2'}(\mathrm{C}_{\overline{A}}(\overline{F}))\overline{S}$. $\langle z\rangle < F$ és $\overline{F}$ másodrendű, így centralizátorának ősé éppen F normalizátora. $\mathrm{O}^2(\mathrm{C}_{\overline{A}}(\overline{F}))$ őse ezek szerint $\mathrm{N}_A(F)$-beli 2-hatvány indexű normálosztó. Így $\mathrm{N}_A(F) = \mathrm{O}^2(\mathrm{N}_A(F))S$. Mivel 3 osztja $\mathrm{N}_A(K) \leq \mathrm{N}_A(F)$ rendjét, ezért osztja $\mathrm{O}^2(\mathrm{N}_A(F))$ rendjét, és a 3.Lépés alapján $\mathrm{C}_A(Q)$-ét is. A 3-Sylowjai ciklikusak, így $\mathrm{N}_A(Q)$ 3-Sylowjai is azok. $\mathrm{C}_A(Q) \trianglelefteq \mathrm{N}_A(Q)$ tartalmazza valamely $\mathrm{N}_A(Q)$-beli 3-Sylow egyetlen 3-adrendű részcsoportját, így tartalmazza az összesét is. Tehát $\mathrm{N}_A(Q)$ összes 3-adrendű eleme $\mathrm{C}_A(Q)$-beli. Ez azonban ellentmondás, hisz $Q \triangleleft H$, de H 3-adrendű eleme nem centralizálja Q-t.

5.Lépés

$A \cong \mathrm{SL}(2,5)$

5.Lépés bizonyítása:

$\mathrm{O}^2(\mathrm{C}_{\overline{A}}(\overline{F})) \leq \overline{\mathrm{O}^2(\mathrm{N}_A(F))} \leq \overline{\mathrm{C}_A(Q)} \leq \mathrm{C}_{\overline{A}}(\overline{Q}) = \overline{Q}$. Az első tartalmazás fenn áll, mert $\overline{\mathrm{N}_A(F)} = \mathrm{C}_{\overline{A}}(\overline{F})$ (hisz $|\overline{F}| = 2$, $\langle z \rangle < F$), és 2-hatvány indexű normálosztó faktora 2-hatvány indexű normálosztó. A második tartalmazás a bizonyítás 3.Lépése miatt teljesül. Végül az utolsó egyenlőség $Q \in Syl_2 A$-nak és az 5.1.8 Tétel (ii) pontjának köszönhető. $\mathrm{O}^2(\mathrm{C}_{\overline{A}}(\overline{F})) \leq \overline{Q}$, miatt $\mathrm{C}_{\overline{A}}(\overline{F}) = \overline{Q}$. Tehát $\overline{A}$ valamely involúciójának centralizátora izomorf $\mathrm{Z}_2 \times \mathrm{Z}_2$-vel, $\overline{A}$ perfekt és minden involúciója konjugált. Alkalmazhatjuk az 5.1.6 Tételet, $\overline{A} \cong \mathrm{A}_5$. Ezért A A_5 Schur-fedőcsoportja, így $A \cong \mathrm{SL}(2,5)$.$\blacksquare$

5.1.15 Következmény:

Legyen A nemfeloldható Frobenius-komplementum, ekkor $A'' \cong \mathrm{SL}(2,5)$.

Bizonyítás:

Mivel A nemfeloldható, ezért valamely k egész számra $A^{(k)} = A^{(k+1)}$. Tehát $A^{(k)}$ perfekt komplementum, így $A^{(k)} \cong \mathrm{SL}(2,5)$. Legyen $Q \in Syl_2 A^{(k)}$, és $S \in Syl_2 A$ olyan 2-Sylow, hogy $Q \leq S$. Vegyük észre, hogy $Q = S \cap A^{(k)} \trianglelefteq S$ és S/Q ciklikus. Ezért $A/A^{(k)}$ Sylow-részcsoportjai ciklikusak. A 2.3.12 Tétel szerint $(A/A^{(k)})'' = 1$. Tehát $A'' \leq A^{(k)}$, így $A^{(k)} = A'' \cong \mathrm{SL}(2,5)$.$\blacksquare$

Irodalomjegyzék

[1] W. Burnside, Theory of Groups of Finite Order (Second edition). Cambridge University Press (1911)

[2] B. Huppert, Endliche Gruppen I. Springer, Berlin (1967)

[3] B. Huppert, Character Theory of Finite Groups. Walter de Gruyter, Berlin (1998)

[4] I. M. Isaacs, Character Theory of Finite Groups. Acad. Press, New York (1976)

[5] I. M. Isaacs, Algebra: A Graduate Course. Wadsworth Inc. (1994)

[6] I. M. Isaacs, Finite Group Theory. American Math. Society, Providence, Rhode Island (2008)

[7] E. B. Kuisch, R. W. van der Wall, Homogeneous character induction., J. Algebra **149** (1992), 454-471.

[8] J. G. Thompson, Normal p-complements for finite groups., J. Algebra **1** (1964), 43-46.