

MATEMATIKUS ALGEBRA ELŐADÁS

1991. TAVASZA

A félév első részében az eddig kifejlesztett gyűrűelméleti apparátus csoportelméleti alkalmazásairól lesz szó. Célunk ízelítőt adni az egyszerű csoportokkal kapcsolatos elemi eredményekből.

1. Algebrai és algebrai egész elemek. Legyen L kommutatív test, és R részgyűrűje L -nek, mely az egységelemet tartalmazza. Jelölje K az R által L -ben generált résztestet, azaz az R -beli elemek hányadosainak halmazát (főpélda: R =egészek, K =racionális számok, L =komplex számok).

1.1. Definíció. A $b \in L$ elemet algebrainak nevezzük R felett, ha gyöke egy nem nulla, R -beli együtthatós polinomnak. A b elem (algebrai) egész az R felett, ha gyöke egy nem nulla, R -beli együtthatós, normált polinomnak.

Nyilván R és K felett ugyanazok az elemek lesznek algebraiak, és ezek K felett már algebrai egészek is. Ha b ilyen, akkor $\{p \in K[x] \mid p(b) = 0\}$ nem nulla ideál, és mivel $K[x]$ főideálgyűrű, főideál is. Normált generátorelemét a b elem K feletti minimálpolinomjának nevezzük, ennek fokát pedig a b elem K feletti fokának. Könnyen látható, hogy egy normált $K[x]$ -beli polinom, melynek b gyöke, pontosan akkor lesz a b elem K feletti minimálpolinomja, ha irreducibilis K felett (vö. Fried, 6.68).

1.2. Tétel. Az L test K felett algebrai elemei résztestet alkotnak. Az L azon elemei, melyek egészek R felett, részgyűrűt alkotnak.

Megjegyezzük, hogy Fried 8.67 bizonyítása a könyv első kiadásában hibás!

1.3. Lemma. Legyen b egész R felett, és jelölje $R[b]$ azt a részgyűrűt L -ben, melyet R és b generál. Ekkor $R[b]$, mint R -modulus, végesen generált.

Bizonyítás. Legyen $f \in R[x]$ olyan normált polinom, melynek b gyöke, és n az f foka. Ekkor az $1, b, b^2, \dots, b^{n-1}$ elemek generátorrendszert alkotnak (vö. Fried, 8.66). \square

Ha R maga test (azaz $R = K$), akkor többet is mondhatunk. Válasszuk f -et a b minimálpolinomjának. Ekkor az $1, b, b^2, \dots, b^{n-1}$ elemek lineárisan függetlenek is K felett, azaz bázist alkotnak. Ebben az esetben a $K[b]$ részgyűrű test is lesz. Valóban, tekintsük azt a $\phi : K[x] \rightarrow L$ leképezést, melynél $\phi(g) = g(b)$. Ennek magja éppen (f) , képe pedig $K[b]$. A homomorfizmus-tétel miatt tehát $K[b] \cong K[x]/(f)$. Ez utóbbi pedig test, hiszen az (f) ideál f irreducibilitása miatt maximális.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$ - $\mathcal{T}\mathcal{E}\mathcal{X}$

1.4. Lemma. *Ha $b \in L$ algebrai K felett, akkor a $K[b]$ gyűrű részteste L -nek, melynek K feletti dimenziója megegyezik a b elem K feletti fokával. \square*

Legyen S részgyűrű L -ben, mely R -et tartalmazza. Azt mondjuk, hogy az $R \subseteq S$ gyűrűbővítés *véges*, ha S , mint R -modulus, végesen generált. Eddig tehát azt láttuk be, hogy az algebrai, illetve algebrai egész elemek véges bővítésekhez vezetnek. Most belátjuk ezen állítások megfordítását.

1.5. Lemma. *Ha $S \subseteq L$ véges gyűrűbővítése R -nek, akkor S minden eleme egész R felett.*

Bizonyítás. Jelölje $\{a_1, \dots, a_n\}$ az S -nek, mint R -modulusnak egy generátorrendszerét, és legyen $b \in S$. Ekkor ba_j felírható $r_{j1}a_1 + \dots + r_{jn}a_n$ alakban, ahol $r_{ji} \in R$. Mivel nem minden a_j nulla, ez azt jelenti, hogy (az L testben gondolkozva), az $((r_{ji}))$ mátrixnak a b sajátértéke. Ezért b gyöke e mátrix karakterisztikus polinomjának, ami persze normált, és $R[x]$ -beli. \square

1.6. Lemma. *Véges gyűrűbővítések egymásutánja is véges.*

Bizonyítás. Legyen $R \subseteq S \subseteq T \subseteq L$ olyan, hogy S és T részgyűrűk, S végesen generált R -modulus, és T végesen generált S -modulus. Be kell látni, hogy T mint R -modulus is végesen generált. Jelölje $\{a_1, \dots, a_n\}$ az S -nek, mint R -modulusnak egy generátorrendszerét, és $\{b_1, \dots, b_m\}$ a T -nek, mint S -modulusnak egy generátorrendszerét. Képezzük az összes $a_i b_j$ szorzatot. Könnyű számolás mutatja, hogy ez az nm elem generálja az ${}_R T$ modulust. (A számolást lásd Fried, 7.2.) \square

Ha R, S, T testek is, és $\{a_1, \dots, a_n\}$ illetve $\{b_1, \dots, b_m\}$ bázist alkotnak az ${}_R S$ illetve ${}_S T$ vektorterekben, akkor könnyen láthatóan az iménti nm szorzat is bázist alkot az ${}_R T$ vektortérben (vö. Fried, 7.2). Ha $R \subseteq S$ két test, akkor az ${}_R S$ vektortér dimenzióját $|S : R|$ -rel jelöljük, és a bővítés *fokának* nevezzük.

1.7. Lemma. *Két véges testbővítés egymásutánja is véges, és a fokok összeszorzódnak. \square*

Most bebizonyítjuk az 1.2. Tételt. Tegyük fel, hogy $b, c \in L$ algebrai egészek R felett. Ekkor $S = R[b]$ végesen generált R -modulus (1.3. Lemma), és $T = S[c]$ is végesen generált S -modulus, hiszen c egész S felett is. Ezért az 1.6. és az 1.5. Lemma miatt T minden eleme, speciálisan $b - c$ és bc is egész R felett. Tehát az R feletti egészek tényleg részgyűrűt alkotnak L -ben. Ha most a K felett algebrai elemeket vizsgáljuk, akkor ezek egészek is K felett, és ezért az előbb bizonyítottak szerint részgyűrűt alkotnak. Ha pedig $b \neq 0$ gyöke az $a_0 + a_1x + \dots + a_nx^n \in K[x]$ nem nulla polinomnak, akkor $1/b$ nyilván gyöke lesz az $a_n + a_{n-1}x + \dots + a_0x^n \in K[x]$, szintén nem nulla polinomnak. \square

Ha speciálisan R =egészek, K =racionális számok, L =komplex számok, akkor a kapott egészeket *algebrai egészeknek*, a kapott algebrai elemeket pedig *algebrai számoknak* nevezzük.

1.8. Tétel. *Az algebrai számok algebrailag zárt testet alkotnak.*

Bizonyítás. Legyen f algebrai együtthatós polinom, és b ennek egy komplex gyöke. Ilyen b létezik, hiszen a komplex számok teste algebrailag zárt. Bővítsük a racionális számok testét

az f együtthatóival. Ekkor véges bővítést kapunk. A kapott test felett b már algebrai, és ezért b -vel tovább bővítve ismét véges bővítés adódik. Ezért b algebrai szám, hiszen \mathbf{Q} egy véges bővítésében van. Azaz f -nek van gyöke az algebrai számok testében. \square

2. Véges egyszerű csoportok és rendjeik. Ismeretes (vö. Fried, 4.99), hogy a prímszámhatványrendű csoportoknak nemtriviális centruma van, és ezért nemkommutatív egyszerű csoport nem lehet p -csoport. Feit és Thompson bebizonyították, hogy egy nemkommutatív egyszerű csoport páratlan rendű sem lehet, ez azonban igen mély tétel, 270 oldalas bizonyítással. A most következő ötletekkel is adott számokról lehet bizonyítani, hogy nincs olyan rendű véges egyszerű csoport.

2.1. Állítás. *Egy egyszerű csoport rendje nem lehet $4k+2$ alakú szám (ahol $k > 1$ egész).*

Bizonyítás. Tegyük fel, hogy G ilyen, és legyen $\{e, g\}$ a G egy 2-Sylowja. Jelölje $H \leq S_G$ a G Cayley-reprezentációjakor kapott, G -vel izomorf csoportot. Ebben a g elemhez tartozó permutáció $2k+1$ darab diszjunkt transzpozíció szorzata, azaz páratlan permutáció. Ezért H nem része az A_G alternáló csoportnak. Így $HA_G = S_G$, és az első izomorfizmus-tétel miatt $HA_G/A_G \cong H/H \cap A_G$. Tehát a H csoportban van egy 2 indexű normálosztó. \square

2.2. Definíció. *Legyen G véges csoport, és p prímszám, mely osztja G rendjét. Legyen $|G| = p^k m$, ahol már p nem osztója m -nek. Ekkor a G csoport m elemű normálosztóját G normál p -komplementumának nevezzük.*

Megjegyezzük, hogy G -ben legfeljebb egy m elemű normálosztó lehet. Ha ugyanis N ilyen, és $H \leq G$, melyre $|H|$ osztja m -et, akkor, ismét az első izomorfizmus-tétel miatt, $|HN| = |H||N|/|H \cap N|$, és ezért a HN részcsoporthoz nem osztható p -vel. Viszont m osztja $|HN|$ -et, és $|HN|$ osztja $|G| = p^k m$ -et, ami csak úgy lehet, ha $H \subseteq N$.

2.3. Állítás. *Ha G -ben van normál p -komplementum, akkor a G csoport p -hez relatív prím rendű részcsoporthai (és elemei) ebben benne vannak. \square*

Az imént tehát azt bizonyítottuk be, hogy ha G rendje $4k+2$ alakú, akkor van G -ben normál 2-komplementum. Több általános feltétel is van normál p -komplementum létezésére, ezek jelentősége tehát, hogy nem-egyszerűségi kritériumok. Közülük most egyet mondunk ki, a többitől később lesz szó.

2.4. Burnside tétele. *Legyen p a G véges csoport rendjének legkisebb prímosztója. Ha G p -Sylow részcsoportha ciklikus, akkor G -ben van normál p -komplementum.*

Látható, hogy Burnside tétele a 2.1. észrevétel általánosítása. Folytassuk most a permutációcsoportok felhasználását egyszerű csoportok vizsgálatához. A következő lemma azt mondja ki, hogy egy egyszerű csoportnak nem lehetnek kis indexű részcsoporthai.

2.5. Lemma. *Legyen G véges egyszerű csoport, és H egy n indexű valódi részcsoporth G -ben. Ekkor $|G| \leq n!$.*

Bizonyítás. Legyen $\Omega = \{H_1, \dots, H_n\}$ az összes H szerinti baloldali mellékosztály. Tetszőleges $g \in G$ elemhez rendeljük hozzá azt a permutációt az Ω halmazon, ami a H_i mellékosztályt a gH_i -ba viszi ($1 \leq i \leq n$). Az így definiált ϕ leképezés homomorfizmus lesz

G -ből az S_Ω szimmetrikus csoportba. Mivel a H -n kívüli elemek képe nem az identitás, $\text{Ker}(\phi) \neq G$, tehát G egyszerűsége miatt $|\text{Ker}(\phi)| = 1$, azaz ϕ beágyazás. \square

A következő ötlet a Sylow-tételek segítségével állít nem-egyszerűségi kritériumot.

2.6. Állítás. *Egy egyszerű csoport rendje nem lehet 260.*

Bizonyítás. Tegyük fel, hogy G ilyen. Jelölje n a G 13-Sylow részcsoporthainak a számát. A Sylow-tétel miatt $n \equiv 1 \pmod{13}$. Másrészt $n = |G : N_G(P)|$, ahol P egy 13-Sylow részcsoporth G -ben, és $N_G(P)$ ennek normalizátorát jelöli. Mivel $P \leq N_G(P)$, ezért n osztja P indexét, ami 20. De 20 osztói közül csak az 1 ad 1 maradékot mod 13, ezért $n = 1$, azaz $N_G(P) = G$, és így $P \triangleleft G$. \square

2.7. Állítás. *Egy egyszerű csoport rendje nem lehet 120.*

Bizonyítás. Az előző technikák közvetlenül most nem működnek, mert van olyan 120 rendű csoport (az S_5 szimmetrikus csoport), melynek egyik Sylowja sem normálosztó, és normál komplementuma sincs. Az ötletek kombinációja visz célhoz. Legyen G egy 120 rendű egyszerű csoport, P a G 5-Sylowja, és $H = N_G(P)$. A 2.6. Állítás bizonyításának technikájával látjuk, hogy H indexe csak 6 lehet. Tehát a 2.5. Lemma szerint G beágyazható az S_6 -sőt, a 2.1. bizonyítása szerint az A_6 csoportba is. Ebben azonban az indexe $360/120 = 3$ lenne, ami ismét 2.5. miatt ellentmond annak, hogy A_6 egyszerű csoport. \square

A 2.6. Állítás technikájából világos, hogy ha $|G| = pq$, ahol $p < q$ prímek, akkor G q -Sylowja normálosztó, ezért G nem egyszerű. A reprezentációelmélet egyik fontos első eredménye volt az alábbi tétel.

2.8. Burnside tétele. *Ha G véges, nemkommutatív egyszerű csoport, akkor rendjének legalább három különböző prímosztója van.*

Egy speciális esetet most elemi úton bebizonyítunk.

2.9. Állítás. *Legyenek p és q különböző prímek, és $|G| = p^k q$. Ekkor G nem lehet egyszerű csoport.*

2.10. Lemma. *Legyen P p -csoport, és H valódi részcsoporth P -ben. Ekkor $N_P(H) > H$.*

Bizonyítás. Indukciót alkalmazunk $|P|$ -re. Mivel $Z(P)$ (a P centruma) biztosan normalizálja H -t (azaz része $N_P(H)$ -nak), feltehetjük, hogy $Z(P) \subseteq H$. Legyen $\bar{P} = P/Z(P)$ és $\bar{H} = H/Z(P)$. Az indukciós feltevés miatt van olyan elem $\bar{P} \setminus \bar{H}$ -ban, mely normalizálja \bar{H} -t. Ennek tetszőleges ősképe P -ben eleme lesz $N_P(H) \setminus H$ -nak. \square

2.11. Lemma. *Ha A és B részcsoporthok G -ben, akkor az AB komplexusszorzat rendje $|A||B|/|A \cap B|$.*

Bizonyítás. Ha $ab = a_1 b_1$ (ahol $a, a_1 \in A$, $b, b_1 \in B$), akkor ez azzal ekvivalens, hogy $a_1 = ac^{-1}$ és $b_1 = cb$, ahol $c = a_1^{-1} a = b_1 b^{-1} \in A \cap B$. Az ilyen (a_1, b_1) párok száma, rögzített a és b esetén, éppen $|A \cap B|$. \square

A 2.9. Állítás bizonyításához tekintsük G összes p -Sylowját, és válasszuk ki ezek közül P_1 -et és P_2 -t úgy, hogy D metszetük a lehető legnagyobb elemszámú legyen. (Ha csak egy p -Sylow van, akkor ez normálosztó, tehát készen vagyunk.) Legyen $H = N_G(D)$.

Ha H p -csoport, akkor belerakható G egy P p -Sylowjába. Ekkor $P_1 \cap P$ valódi módon tartalmazza D -t, hiszen a 2.10. Lemma miatt van olyan $g \in P_1 \setminus D$, ami normalizálja D -t, és ezért benne van P -ben is. Ez ellentmond D maximalitásának.

Tehát H tartalmaz egy Q q -Sylow részcsoportot. Belátjuk, hogy a D által G -ben generált normálosztó része P_1 -nek. Ez a normálosztó úgy készül, hogy először tekintjük D összes konjugáltját, majd az ezek által generált részcsoportot. Ezért elég belátni, hogy D minden konjugáltja része P_1 -nek. A 2.11. Lemma miatt $G = QP_1$. Tehát ha $g \in G$ akkor $g = ab$, ahol $a \in Q$ és $b \in P_1$. De $Q \subseteq H = N_G(D)$, ezért

$$g^{-1}Dg = b^{-1}a^{-1}Dab \subseteq b^{-1}Db \subseteq P_1.$$

Tehát a D által generált normálosztó tényleg része P_1 -nek. Mivel G egyszerű, ez a normálosztó, és ezért maga D is, egyelemű. De D maximális volt, így azt kaptuk, hogy G bármely két p -Sylowjának metszete triviális.

A végső ellentmondást úgy kapjuk meg, hogy belátjuk: G -nek csak egyetlen q -Sylowja van (s ezért az normálosztó). Jelölje m a G azon egységtől különböző elemeinek számát, melyek rendje p -hatvány. Ezek éppen a p -Sylowok egységtől különböző elemei. Ezen Sylowok száma $|G : N_G(P_1)|$, azaz vagy 1, vagy q . De 1 nem lehet, mert akkor P_1 normálosztó lenne. Tehát q darab p -Sylow van, és mivel ezek a Sylowok az imént bizonyítottak szerint csak az egységben metszik egymást,

$$m = q(p^k - 1) = |G| - q.$$

Ezért a q rendű elemek száma legfeljebb $q - 1$, azaz tényleg csak egy q -Sylow fér el. Ezzel a 2.9. bizonyítását befejeztük. \square

Az iménti bizonyítás utolsó lépésében szereplő szituációt érdemes egy definícióba foglalni. A továbbiakban a konjugálást a kitevőbe írjuk, azaz $g^{-1}Hg$ helyett H^g -t írunk.

2.12. Definíció. Egy G csoportot Frobenius-csoportnak nevezünk, ha van olyan H részcsoportja, melyre bármely $g \in G \setminus H$ esetén $H \cap H^g$ csak az egységelemből áll. Azon elemek halmazát, melyek H egyetlen konjugáltjában sincsenek benne, az egységelemmel kibővítve a G magjának nevezzük. A H részcsoport neve G Frobenius-komplementuma.

Az előbbi bizonyítás végén szereplő szituációban H egy p -Sylow, a csoport magja pedig az egyetlen q -Sylow részcsoport volt. Ami ebben az esetben triviálisan teljesült, nevezetesen hogy a mag normálosztó, igaz általában is, de bizonyítani csak reprezentációelmélettel sikerült.

2.13. Frobenius tétele. Egy Frobenius-csoport magja mindig normálosztó.

A bizonyítás nehézsége abban van, hogy a magról kimutassuk, hogy részcsoport (hiszen az triviális, hogy a konjugáltságra nézve zárt). A Frobenius-csoportok a permutációcsoportok elméletében fontosak. A most következők megértéséhez célszerű átismételni a Fried 4.10. fejezetben található fogalmakat.

2.14. Állítás. Legyen G olyan tranzitív permutációcsoport, melynek minden, az egységtől különböző elemének legfeljebb egy fixpontja van. Ekkor G Frobenius-csoport.

Bizonyítás. Könnyen látható, hogy a stabilizátorokra teljesül a H -ra szabott feltétel. A mag a fixpontmentes permutációkból, és az identitásból áll. \square

Frobenius-csoportra példa a D_n diédercsoport páratlan n esetén. További példa minden pq rendű nem-kommutatív csoport, ahol p és q különböző prímekek. Megjegyezzük, hogy ilyen csoport pontosan akkor létezik, ha $p \equiv 1 \pmod{q}$ (vagy fordítva).

3. A transzfer. Következő célunk Burnside normál komplementumokról szóló tételének (azaz a 2.4. Tételnek) a bizonyítása. Ehhez nem szükséges még a reprezentációelmélet, de be kell vezetnünk egy speciális, igen hasznos homomorfizmus, a *transzfer* fogalmát.

Legyen H véges indexű részcsoportha a G csoportnak, és $\psi : H \rightarrow A$ egy homomorfizmus valamilyen A Abel-csoportba. Válasszunk egy y_1, \dots, y_n reprezentánsrendszert a H baloldali mellékosztályai szerint. Ha $g \in G$, akkor

$$gy_i = y_{\sigma(i,g)} h_i(g) \quad (1 \leq i \leq n),$$

ahol $h_i(g) \in H$ és $1 \leq \sigma(i,g) \leq n$. Legyen

$$\tau_H(g) = \psi(h_1(g) \dots h_n(g))$$

(a τ_H jelölésben nem tüntetjük fel a ψ homomorfizmust, amitől persze τ_H függ).

3.1. Állítás. Az imént definiált $\tau_H : G \rightarrow A$ leképezés homomorfizmus, mely nem függ az y_1, \dots, y_n reprezentánsrendszer választásától.

Bizonyítás. Legyen $g, g' \in G$, ekkor

$$y_{\sigma(i,gg')} h_i(gg') = (gg')y_i = g(g'y_i) = gy_{\sigma(i,g')} h_i(g') = y_{\sigma(\sigma(i,g'),g)} h_{\sigma(i,g')}(g) h_i(g'),$$

és ezért

$$h_i(gg') = h_{\sigma(i,g')}(g) h_i(g').$$

Szorozzuk össze ezt az összefüggést $i = 1$ -től n -ig, és alkalmazzuk a ψ homomorfizmust. Mivel A Abel, a sorrenddel nem kell törődni. A baloldalon ekkor $\tau_H(gg')$ adódik. Rögzített g' mellett a g' -vel való balszorzás permutálja H baloldali mellékosztályait, azaz a $\sigma(i,g')$ leképezés permutáció. Így a $h_{\sigma(i,g')}(g)$ elemek ugyanazok, mint a $h_i(g)$ elemek, sorrendtől eltekintve. Ezért a jobboldalon éppen $\tau_H(g)\tau_H(g')$ szerepel, vagyis a τ_H leképezés tényleg homomorfizmus.

Legyen most z_1, \dots, z_n egy másik reprezentánsrendszer, azaz $z_i = y_i t_i$, ahol $t_i \in H$. Ekkor

$$gz_i = gy_i t_i = y_{\sigma(i,g)} h_i(g) t_i = z_{\sigma(i,g)} t_{\sigma(i,g)}^{-1} h_i(g) t_i.$$

Ha tehát a z_i elemekre vonatkozólag számítjuk ki $\tau_H(g)$ értékét, akkor az eredmény

$$\psi \left(\prod_{i=1}^n t_{\sigma(i,g)}^{-1} h_i(g) t_i \right)$$

lesz. Mivel A Abel-csoport, a tényezőket ismét átrendezhetjük. De $\sigma(i,g)$ permutáció, ezért a t_i elemek kiesnek, és így az y_i elemekre vonatkoztatott τ_H értéket kapjuk. \square

3.2. Definíció. A τ_H homomorfizmust *transzfernek*, pontosabban a G csoport H részcsoportja szerinti, A -ba vezető transzferének nevezzük.

A transzfer kiszámításához igen alkalmas a következő módszer, amelyben minden g elemhez a hozzá legalkalmasabb reprezentánsrendszert választjuk. Legyen $y_1 = x_1 \in G$ tetszőleges, $y_2 = gx_1$, $y_3 = g^2x_1$, és így tovább. Mivel a g elemmel való balszorzás permutáció H bal mellékosztályain, egyszer csak visszaérünk y_1 mellékosztályába, azaz alkalmas r_1 egészre teljesül, hogy $x_1^{-1}g^{r_1}x_1 \in H$. Most válasszunk egy olyan mellékosztályt, ahol még nem jártunk, és ebből egy x_2 reprezentánszt. Legyen $y_{r_1} = x_2$, $y_{r_1+1} = gx_2$, és így tovább, ismét ameddig vissza nem érünk az x_2 mellékosztályába. Folytassuk ezt az eljárást, ameddig el nem fogynak a mellékosztályok. A transzfer definíciójából ekkor a következő állítást kapjuk.

3.3. Lemma. Az r_1, \dots, r_k számok összege n , azaz a H indexe. Ha $1 \leq i \leq k$, akkor $x_i^{-1}g^{r_i}x_i \in H$. Végül

$$\tau_H(g) = \psi \left(\prod_{i=1}^k x_i^{-1}g^{r_i}x_i \right). \quad \square$$

A következő tétel a transzfer egy szép alkalmazása végtelen csoportokra. Ha G csoport, akkor kommutátor-részcsoportját G' -vel jelöljük, a $[g, h]$ jelölés pedig a $g^{-1}h^{-1}gh$ elemet rövidíti.

3.4. Schur tétele. Legyen G végtelen csoport, melynek centruma véges indexű. Ekkor G kommutátor-részcsoportja véges.

3.5. Lemma. Legyen H véges indexű részcsoport egy végesen generált G csoportban. Ekkor H is végesen generált.

Bizonyítás. Legyen g_1, \dots, g_m a G egy generátorrendszere, amelyet már kiegészítettünk a benne szereplő elemek inverzeivel is. Tehát G minden eleme előáll a g_i elemek alkalmas szorzataként. Válasszunk egy y_1, \dots, y_n baloldali reprezentánsrendszert H szerint, úgy, hogy H reprezentánsa az egységelem legyen. A $g \in G$ elem reprezentánsát jelölje \bar{g} . A transzfer definíciójában alkalmazott jelölést használva legyen $h_{ij} = h_i(g_j) \in H$, azaz, mostani jelöléseinkkel, $h_{ij} = (\bar{g}_j \bar{y}_i)^{-1} g_j y_i$. Belátjuk, hogy ez az nm elem generálja H -t. Legyen $h \in H$ tetszőleges elem, ekkor $h = t_1 \dots t_k$, ahol a t_i elemek a g_1, \dots, g_m közül valók. A $p_i = t_{i+1} \dots t_k$ jelölést alkalmazva látjuk, hogy $p_k = \bar{p}_k = e$ és $p_0 = h \in H$ miatt $\bar{p}_0 = e$. Ezért

$$h = t_1 \dots t_k = \left((\bar{p}_0)^{-1} t_1 \bar{p}_1 \right) \left((\bar{p}_1)^{-1} t_2 \bar{p}_2 \right) \dots \left((\bar{p}_{k-1})^{-1} t_k \bar{p}_k \right).$$

E szorzat i -edik tagja, $(\bar{p}_{i-1})^{-1} t_i \bar{p}_i = (\bar{t}_i \bar{p}_i)^{-1} t_i \bar{p}_i = (\bar{t}_i \bar{p}_i)^{-1} t_i \bar{p}_i$, hiszen tetszőleges $a, b \in G$ elemekre $\overline{ab} = \overline{a} \bar{b}$ nyilván teljesül. Ha tehát $t_i = g_u$ és $\bar{p}_i = y_v$, akkor $(\bar{t}_i \bar{p}_i)^{-1} t_i \bar{p}_i = h_{vu}$. Így a h_{ij} elemek tényleg generálják a H részcsoportot. \square

Most belátjuk Schur tételét (3.4). Az nyilvánvaló, hogy G' végesen generált. Vegyünk ugyanis egy y_1, \dots, y_n reprezentánsrendszert a $Z(G)$ szerint. Nyilván $c_1, c_2 \in Z(G)$ esetén $[y_i c_1, y_j c_2] = [y_i, y_j]$, azaz a csoportban legfeljebb n^2 elem lehet, ami kommutátor. Az

első izomorfizmus tétel szerint $G'Z(G)/Z(G) \cong G'/(G' \cap Z(G))$, ezért a $K = G' \cap Z(G)$ részcsoport véges indexű G' -ben. Így egyrészt elég belátni, hogy K véges, másrészt az előző lemmából látjuk, hogy K végesen generált. Legyen $H = A = Z(G)$, ψ az identitás, és tekintsük a transzfert. Ha $g \in H = Z(G)$, akkor a 3.3. Lemma szerint számolva látjuk, hogy $\tau_H(g) = g^n$. Másrészt τ_H képe Abel, és ezért a magja tartalmazza a G' kommutátor-részcsoportot. Ha tehát $g \in K = G' \cap Z(G)$, akkor $e = \tau(g) = g^n$. Ezért a K végesen generált Abel-csoport minden eleme legfeljebb n -edrendű, azaz K tényleg véges. \square

A továbbiakban legyen G véges csoport, és P egy p -Sylow G -ben.

3.6. Lemma. *Legyen $K \triangleleft G$. Ekkor $K \cap P$ egy p -Sylowja K -nak, KP/P pedig p -Sylowja G/K -nak.*

Bizonyítás. Tudjuk, hogy $|KP|/|P| = |K|/|K \cap P|$, és mivel P a KP csoportnak is p -Sylowja, ezek a hányadosok nem oszthatók p -vel. Ezért $K \cap P$ p -Sylowja K -nak. Mivel pedig $KP/K \cong P/K \cap P$, ezért a rendek miatt KP/K is p -Sylow lesz G/K -ban. \square

A normál-komplementum tételek bizonyításához G olyan faktorait kell vizsgálnunk, amelyek p -csoportok. Miként G Abel-féle faktorainak vizsgálatához a G' kommutátor-részcsoport ad segítséget, úgy G azon Abel-féle faktorait, melyek p -csoportok is egyben, a $P \cap G'$, úgynevezett *fokális részcsoport* segítségével vizsgálhatjuk.

3.7. Lemma. *A G csoportnak létezik olyan N normálosztója, melyre, $K \triangleleft G$ esetén, a G/K faktor pontosan akkor Abel-féle p -csoport, ha $N \subseteq K$. Az N normálosztóra igaz, hogy $P \cap G' = P \cap N$, és $G/N \cong P/(P \cap G')$. Így a G csoport azon Abel-féle faktorcsoportjai, melyek p -csoportok, éppen a $P/(P \cap G')$ csoport faktoraival izomorfak.*

Bizonyítás. Bontsuk fel a $\overline{G} = G/G'$ Abel-csoportot a véges Abel-csoportok alaptétele szerint, és legyen \overline{N} a p -vel nem osztható rendű tényezők direkt szorzata. Így $\overline{G}/\overline{N}$ Abel-féle p -csoport, sőt, éppen \overline{G} (egyetlen) p -Sylowjával izomorf. Ugyanakkor $|\overline{N}|$ nem osztható p -vel, sőt, \overline{N} a \overline{G} azon elemeiből áll, melyek rendje p -hez relatív prím. Jelölje N az \overline{N} teljes inverz képét G -ben. Belátjuk, hogy N teljesíti a feltételeket.

A második izomorfizmus-tétel miatt $G/N \cong \overline{G}/\overline{N}$, azaz Abel-féle p -csoport. Ha pedig K olyan normálosztó G -ben, melyre G/K Abel-féle p -csoport, akkor $G' \subseteq K$ (hiszen G/K Abel), és ezért elég belátni, hogy $\overline{N} \subseteq K/G'$. Minden $g \in \overline{N}$ elem rendje p -hez relatív prím, és így g benne kell legyen minden p -hatvány indexű normálosztóban, tehát K/G' -ben is. Azaz beláttuk, hogy $N \subseteq K$.

Tudjuk, hogy $G' \subseteq N$, tehát $P \cap G' \subseteq P \cap N$. Az előző lemma miatt ez a két metszet p -Sylow G' -ben, illetve N -ben. Viszont láttuk, hogy $|N/G'|$ nem osztható p -vel, ezért e két Sylow-csoport rendje egyenlő. Tehát $P \cap N = P \cap G'$. Ismét az előző lemmából kapjuk, hogy PN/N p -Sylow G/N -ben, és mivel G/N p -csoport, $PN = G$. Ezért $G/N \cong P/(P \cap N) = P/(P \cap G')$. \square

A most következő lemma, amit a normál-komplementum tételek bizonyításához használunk majd, a transzfert alkalmazza a fokális részcsoport egy jellemzésének bizonyítására.

3.8. Lemma. *Legyen G véges és P egy p -Sylowja G -nek. Ekkor a $P \cap G'$ csoportot generálják azok az $a^{-1}a^g$ alakú elemek, ahol $a, a^g \in P$, és $g \in G$.*

Bizonyítás. Jelölje P^* az $a^{-1}a^g$ alakú elemek által generált részcsoporthat P -ben. Mivel $a^{-1}a^g = [a, g]$, a P^* tartalmazza P' -t, és ezért $P^* \triangleleft P$. Nyilván $P^* \subseteq P \cap G'$. A fordított tartalmazás igazolásához legyen $A = P/P^*$, és $\psi : P \rightarrow A$ a természetes homomorfizmus. Persze A Abel (hiszen $P' \subseteq P^*$), és így tekinthetjük a τ_P transzfert az A csoportba. Legyen $g \in P$, alkalmazzuk a 3.3. Lemma módszerét, és alakítsuk át a kapott eredményt a következőképpen:

$$\tau_P(g) = \psi \left(\prod_{i=1}^k x_i^{-1} g^{r_i} x_i \right) = \psi(g^n) \psi \left(\prod_{i=1}^k [g^{r_i}, x_i] \right).$$

De $g \in P$ miatt $[g^{r_i}, x_i] \in P^*$, és ezért a ψ leképezés az egységelembe viszi ezeket a kommutátorokat. Így ilyenkor $\tau_P(g) = \psi(g)^n$, ahol tehát $n = |G : P|$. Ha még $g \in G'$ is igaz, akkor, mivel a transzfer Abel-csoportba képez, $G' \subseteq \text{Ker}(\tau_P)$, azaz $\tau_P(g) = \psi(g)^n$ az A egységeleme. De A egy p -csoport, n pedig relatív prím p -hez, és ezért $\psi(g)$ is az egységelem, azaz $g \in \text{Ker}(\psi) = P^*$. Beláttuk tehát, hogy $P \cap G' \subseteq P^*$. \square

4. Normál-komplementum tételek. Burnside tételét (2.4.) egy lényegesen általánosabb eredményből fogjuk levezetni, amit azonban csak részben bizonyítottunk.

4.1. Frobenius tétele. *Legyen a p prím osztója a G véges csoport rendjének. A következő négy állítás ekvivalens.*

- (1) G -ben van normál p -komplementum.
- (2) Ha H nem egyelemű p -részcsoporthat G -ben, akkor $N_G(H)$ -ban van normál p -komplementum.
- (3) Ha H p -részcsoporthat G -ben, akkor $N_G(H)/C_G(H)$ p -csoport.
- (4) Ha P egy p -Sylow G -ben, és P két eleme G -ben konjugáltak, akkor ezek az elemek már P -ben is konjugáltak.

A (3) \implies (4) implikációt csak arra az esetre látjuk be, ha G p -Sylowja Abel-féle, a Burnside tétel bizonyításához ennyi is elég. Az általános eset kimutatásához még (a 2.9. Állítás bizonyításában szereplő gondolathoz hasonlóan) a p -Sylowok metszeteit is vizsgálni kell (ez egy körülbelül négy oldalas, szép, de elég technikai bizonyítás, amit az irodalomban Alperin-tétel néven lehet megtalálni).

4.2. Lemma. *Legyen P egy p -csoport, és N nem egyelemű normálosztó P -ben. Ekkor $|N \cap Z(P)| > 1$, és $[N, P] < N$.*

Bizonyítás. Állítsuk elő N -et P konjugált osztályainak egyesítéseként. Ezek elemszáma mind prímhatvány, összegük az N rendje, vagyis osztható p -vel, és e osztálya egyelemű, ezért van még egy egyelemű osztály. Így $|N \cap Z(P)| > 1$.

A második állítás bizonyításához alkalmazzunk indukciót $|P|$ -re. Ha $N \cap Z(P) = N$, akkor $[N, P] = \{e\} < N$. Egyébként pedig $\bar{N} = N/(N \cap Z(P))$ nem egyelemű normálosztója $\bar{P} = P/(N \cap Z(P))$ -nek. Az indukciós feltevés szerint $[\bar{N}, \bar{P}] < \bar{N}$. Ha tehát K jelöli az $[\bar{N}, \bar{P}]$ teljes inverz képét P -ben, akkor $K < N$, és nyilván $[N, P] \subseteq K$. \square

Most lássuk a Frobenius-tétel bizonyítását. A G csoport egy elemét nevezzük p -elemnek, ha rendje p -hatvány, és p' -elemnek, ha rendje p -hez relatív prím. A 2.3. Állítás

szerint egy csoport normál p -komplementuma éppen a p' -elemekből áll. Tehát egy csoportban pontosan akkor van normál p -komplementum, ha bármely két p' -elem szorzata is p' -elem. Mivel ez a tulajdonság részcsoportha öröklődik, azért (2) következik (1)-ből.

Tegyük most fel, hogy (2) igaz, legyen H nem egyelemű p -részcsoportha, és N az $N_G(H)$ normál p -komplementuma. Ekkor $[H, N] \subseteq H \cap N$, hiszen H és N normálosztók $N_G(H)$ -ban, és persze $|H \cap N| = 1$, hiszen H p -csoport. Ezért H és N centralizálják egymást, azaz $N \subseteq C_G(H)$. Így az $N_G(H)$ csoportban $C_G(H)$ indexe osztja N indexét, ami viszont p -hatvány, hiszen N normál p -komplementum $N_G(H)$ -ban. Ezért (3) feltétele teljesül.

A (4) \implies (1) állítás bizonyításához használjuk fel az eddig felépített eszközöket. Legyen K a G csoport p' -elemei által generált részcsoportha és $P_1 = P \cap K$. Nyilván K normálosztó G -ben, és a 3.6. Lemma miatt P_1 p -Sylow K -ban. Alkalmazzuk a 3.8. Lemmát a K csoportra. Azt kapjuk, hogy a $P_1 \cap K'$ csoportot generálják azok az $a^{-1}a^g$ alakú elemek, ahol $a, a^g \in P_1$, és $g \in K$. A (4) feltétel miatt a és a^g már P -ben is konjugáltak. Ezért $P_1 \cap K' \subseteq [P_1, P]$, ami, ha $|P_1| > 1$, valódi része P_1 -nek az előző lemma miatt. Alkalmazzuk a 3.7. Lemmát a K -ra. A kapott N -re tehát $P_1 \cap N = P_1 \cap K' < P_1$, azaz $K < N$. Másrészt K/N p -csoport, és így K tartalmazza az N összes p' -elemét. De N definíciója szerint N -et generálják a saját p' -elemei, ezért $K = N$. Ez az ellentmondás úgy oldódik fel, hogy P_1 egyelemű, azaz N p' -csoport, ezért normál p -komplementum is.

A (3) \implies (4) implikációt tehát csak akkor bizonyítjuk, ha P Abel. Legyen $a, a^g \in P$ és $C = C_G(a^g)$. Mivel P Abel, $P \subseteq C$. Ugyanezért $P \subseteq C_G(a)$, és így $P^g \subseteq (C_G(a))^g = C$ (hiszen a g -vel való konjugálás automorfizmus). De P és P^g p -Sylowok C -ben is, ezért van olyan $h \in C$, melyre $(P^g)^h = P$. Ezért $gh \in N_G(P)$, másrészt $a^{gh} = (a^g)^h = a^g$, hiszen $h \in C$, ami az a^g centralizátora. Azt kaptuk tehát, hogy a és a^g már konjugáltak $N_G(P)$ -ben is. Felhívjuk a figyelmet arra, hogy eddig nem használtuk ki a (3) feltételt, csak azt, hogy P Abel-féle. A most leírt ötlet Burnside-tól származik.

A bizonyítást úgy fejezzük be, hogy a $H = P$ részcsoportha alkalmazzuk a (3) feltételt. Mivel $P \subseteq C_G(P)$, a $C_G(P)$ indexe már p -vel nem osztható. Azaz $N_G(H)/C_G(H)$ csak úgy lehet p -csoport, ha rendje 1, azaz $N_G(P) = C_G(P)$. Ekkor tehát P benne van $N_G(P)$ centrumában, és ezért az a és a^g elemek, amik $N_G(P)$ -ben konjugáltak, megegyeznek. \square

4.3. Burnside tétele. *Legyen G véges csoport, melynek p -Sylowja benne van a saját normalizátorának a centrumában. Ekkor G -ben van normál p -komplementum.*

Bizonyítás. Ilyenkor a p -Sylow Abel, ezért az állítás következik az iménti bizonyítás utolsó bekezdéséből. Valójában közvetlenül is könnyen ellenőrizhető a 4.1. Tétel (3) feltétele. \square

Következésként lássuk be a 2.4. Tételt. Legyen p a $|G|$ legkisebb prímosztója, és P egy (ciklikus) p -Sylow G -ben. Tekintsük azt a homomorfizmust $N_G(P)$ -ből P automorfizmus-csoportjába, mely a g elemhez a g -vel való konjugálást rendeli. Ennek magja $C_G(P)$, és ezért $N_G(P)/C_G(P)$ izomorf $\text{Aut}(P)$ egy részcsoporthával. Ha $|P| = p^k$, akkor $|\text{Aut}(P)| = \varphi(p^k) = p^{k-1}(p-1)$, ahol φ az Euler-függvény (az automorfizmusok éppen a p^k -hoz relatív prím számokra való hatványozások). Mivel p a legkisebb prímosztó, $p-1$ relatív prím a csoport rendjéhez, és ezért $|N_G(P)/C_G(P)|$ osztója p^{k-1} -nek, azaz prímhatvány. Teljesül tehát az előző tétel feltétele, és így G -ben van normál p -komplementum. \square

Az A_5 alternáló csoport példája mutatja, hogy a tétel egyik feltétele sem hagyható el (hiszen a 3-Sylov, és az 5-Sylov ciklikus, a 2-Sylov pedig Klein-csoport).

Frobenius tételében az összes p -részcsoport normalizátoráról megköveteljük, hogy legyen benne normál p -komplementum. Ennél sokkal kevesebb is elég. Ha $p \neq 2$, akkor van egyetlen olyan, pusztán a P p -Sylov szerkezetének ismeretében definiálható részcsoportja is P -nek, melynek normalizátorát elég vizsgálni. Tekintsük P maximális Abel-féle részcsoportjait (azaz amelyeket már nem tartalmazza valódi módon P egy Abel-féle részcsoportja). Az ezek által generált részcsoportot P *Thompson-részcsoportjának* nevezzük, és $J(P)$ -vel jelöljük. A keresett részcsoport a Thompson-részcsoport centruma lesz.

4.4. Glauberman–Thompson tétele. *Legyen $p \neq 2$ prím, és P egy p -Sylowja G -nek. Ha az $N_G(Z(J(P)))$ részcsoportban van normál p -komplementum, akkor van G -ben is.*

E tétel bizonyítása sokkal nehezebb, mint amit eddig láttunk. A bizonyítására kidolgozott technikák (állítólag) fontos lépcsőfokok voltak a Feit–Thompson tétel bizonyításához vezető úton. D. Gorenstein: *Finite groups* című könyvében az Alperin-tételnek is, és a Glauberman–Thompson tételnek is megtalálható a bizonyítása.

Láttuk, hogy ha egy csoportban van normál p -komplementum, akkor minden részcsoportjában is van. Ha sikerülne teljes listát adni az olyan csoportokról, melyekben nincs normál p -komplementum de minden valódi részcsoportjukban már van, akkor újabb kritériumot kapnánk: egy G csoportban pontosan akkor van normál p -komplementum, ha a listán szereplő csoportok egyike sem részcsoportja G -nek.

4.5. Itô tétele. *Legyen G olyan csoport, melyben nincs normál p -komplementum, de minden valódi részcsoportjában már van. Ekkor*

- (a) G minden valódi részcsoportja nilpotens (azaz a Sylowjainak a direkt szorzata);
- (b) $|G| = p^k q^n$, ahol q prím;
- (c) A p -Sylov normálosztó G -ben, és $p \neq 2$ esetén p exponensű, $p = 2$ esetén pedig legfeljebb 4 exponensű;
- (d) A q -Sylowok ciklikusak.

A téma zárásául néhány gyakorlófeladat következik.

4.6. Feladat. *Vezessük le Frobenius tételének (3) \implies (1) állítását Itô tételéből.*

4.7. Feladat. *Legyen G véges csoport, melynek minden Sylowja ciklikus. Igazoljuk, hogy G feloldható.*

E csoportok részletesebb leírása (azaz Zassenhaus tétele) B. Huppert: *Endliche Gruppen* című művében található meg. Ugyanitt olvasható Itô tételének bizonyítása is.

4.8. Feladat. *Legyen K karakterisztikus részcsoportja a G csoport N normálosztójának (azaz N minden automorfizmusa hagyja helyben K -t). Ekkor $K \triangleleft G$.*

4.9. Feladat. *Tegyük fel, hogy G -ben van normál p -komplementum, és legyen N minimális normálosztó G -ben, melynek rendje osztható p -vel. Igazoljuk, hogy $N \leq Z(G)$.*

4.10. Feladat. Legyen A Abel-csoport, és Φ az A automorfizmusainak olyan csoportja, hogy $|A|$ és $|\Phi|$ relatív prímek. Igazoljuk, hogy

$$A = C_A(\Phi) \times [A, \Phi],$$

ahol $C_A(\Phi)$ azokból az A -beli elemekből áll, amit Φ minden eleme fixen hagy, és $[A, \Phi]$ az $a^{-1}\phi(a)$ alakú elemek által generált részcsoport ($a \in A$, $\phi \in \Phi$).

Ötlet. Írjuk A -t additívan, és legyen R az A endomorfizmus-gyűrűje (mely tartalmazza Φ elemeit). Legyen

$$\theta = \frac{1}{|\Phi|} \sum_{\phi \in \Phi} \phi.$$

Igazoljuk, hogy θ idempotens endomorfizmus, melynek képe $C_A(\Phi)$, magja $[A, \Phi]$. \square

A következő feladat Burnside 4.3. tételét általánosítja.

4.11. Feladat. Tegyük fel, hogy G p -Sylowja Abel, és legyen $N = N_G(P)$. Ekkor

- (i) $P \cap G' = P \cap N'$ és $P = (P \cap N') \times (P \cap Z(N))$.
- (ii) G maximális p -faktorcsoportha izomorf $P \cap Z(N)$ -nel.

Ötlet. Alkalmazzuk az előző feladatot az $A = P$, $\Phi = N/P$ szereposztásban, valamint Burnside ötletét és a fokális részcsoportra vonatkozó tételeket (3.7, 3.8). \square

4.12 Feladat. Legyen G nem Abel-féle csoport, melynek minden valódi részcsoportja Abel. Igazoljuk, hogy ekkor

- (a) $|G|$ legfeljebb két prímmel osztható.
- (b) Ha G nem p -csoport, akkor az egyik prímmel tartozó Sylow normálosztó és elemi Abel (azaz prímmel exponenciális), a másik prímmel tartozó Sylow pedig ciklikus.

A bizonyításhoz ne használjuk fel Itô tételét (csak a 4.3. Burnside-tételt).

5. A Schur-Zassenhaus tétel. Az alábbi tétel nemcsak az egyszerű csoportok vizsgálatában játszik fontos szerepet, hanem a feloldható csoportok elméletében is.

5.1. Schur-Zassenhaus tétele. Legyen H normálosztó a G véges csoportban, melynek rendje és indexe relatív prím. Ekkor H -nak van G -ben komplementuma (azaz olyan K részcsoport G -ben, melyre $HK = G$ és $H \cap K = \{e\}$), továbbá a H összes komplementuma konjugált G -ben.

A tételnek csak az első állítását bizonyítjuk, a konjugáltságról szólót nem. Ez utóbbinak is elemi a bizonyítása abban az esetben, ha H vagy G/H feloldható. E csoportok rendjei azonban relatív prímek a feltétel szerint, ezért legalább az egyik páratlan rendű. A Feit-Thompson tétel miatt tehát valamelyik biztosan feloldható, és így a tétel állítása minden esetben igaz.

5.2. Frattini–elv. Legyen $H \triangleleft G$ és P egy p -Sylow H -ban. Ekkor $G = HN_G(P)$.

Bizonyítás. Legyen $g \in G$. Ekkor P^g a rendje miatt szintén p -Sylow H -ban, ezért P és P^g már konjugáltak H -ban is. Ha tehát $h \in H$ olyan, hogy $P^g = P^h$, akkor $gh^{-1} \in N_G(P)$, és ezért $g = (gh^{-1})h \in N_G(P)H = HN_G(P)$. \square

A Schur–Zassenhaus tétel bizonyítását visszavezetjük arra az esetre, amikor H Abel-féle. Vegyük észre először is, hogy ha K olyan részcsoport G -ben, melynek rendje $|G/H|$, akkor K komplementuma H -nak. Valóban, ekkor $|H \cap K|$ osztja H rendjét is és G/H rendjét is, amik relatív prímek. Ezért $H \cap K = \{e\}$, és így $|HK| = |H||K|/|H \cap K| = |G|$, azaz $HK = G$.

Indukciót alkalmazunk G rendje szerint. Legyen P egy p -Sylowja H -nak, tehát a Frattini–elv miatt $G = HN_G(P)$. Tegyük fel, hogy $N_G(P) < G$, és alkalmazzuk az indukciós feltevést az $N_G(P)$ csoportra, és annak $H \cap N_G(P)$ normálosztójára. E normálosztó rendje osztja H rendjét, indexe pedig $|N_G(P)/(H \cap N_G(P))| = |HN_G(P)/H| = |G/H|$. Ezek relatív prímek, így az indukciós feltevés miatt van $N_G(P)$ -ben $H \cap N_G(P)$ -nek egy K komplementuma. Így K rendje $|G/H|$, és ezért a fenti megjegyzésünk szerint K komplementuma H -nak G -ben.

Azt kaptuk tehát, hogy $N_G(P) = G$, azaz H minden Sylowja normálosztó G -ben. Így H izomorf a Sylowjainak a direkt szorzatával, és ezért $|Z(H)| > 1$. Mivel $Z(H)$ karakterisztikus részcsoport H -ban, a 4.8. Feladat miatt $Z(H) \triangleleft G$. Legyen $\overline{G} = G/Z(H)$ és $\overline{H} = H/Z(H)$. Az indukciós feltevés szerint a \overline{G} -ben a \overline{H} -nak van egy \overline{L} komplementuma. Legyen L az \overline{L} teljes inverz képe G -ben. Tehát $|\overline{L}| = |\overline{G}/\overline{H}| = |G/H|$, és így $|L| = |Z(H)||G/H|$. Ha $L < G$, akkor alkalmazzuk az indukciós feltevést az L csoportra, és ennek $Z(H)$ normálosztójára. A kapott $|G/H|$ elemű részcsoport komplementuma lesz G -ben H -nak, és így készen vagyunk. A fennmaradó eset az, amikor $L = G$, azaz $Z(H) = H$, vagyis H Abel-féle.

Hasonlóan okoskodunk, mint annak bizonyításakor, hogy a transzfer homomorfizmus. Válasszunk egy $\{y_\alpha \mid \alpha \in G/H\}$ reprezentánsrendszert H mellékosztályaiból, ahol felte tesszük, hogy y_α az $\alpha \in G/H$ mellékosztály eleme. A célunk az, hogy ezeket a reprezentánsokat úgy módosítsuk, hogy a kapott új reprezentánsok már részcsoportot alkossanak, ami a keresett komplementum lesz.

A transzfer definíciójában is alkalmazott jelöléssel

$$y_\alpha y_\beta = y_{\alpha\beta} h_\beta(y_\alpha) \quad (\alpha, \beta \in G/H),$$

ahol $h_\beta(y_\alpha) \in H$. Az asszociativitás miatt, a múltkorihoz hasonló, de nem teljesen azonos számolással

$$(y_\alpha y_\beta) y_\gamma = (y_{\alpha\beta}) h_\beta(y_\alpha) y_\gamma = y_{\alpha\beta\gamma} h_\gamma(y_{\alpha\beta}) (h_\beta(y_\alpha))^{y_\gamma},$$

valamint

$$y_\alpha (y_\beta y_\gamma) = y_\alpha y_{\beta\gamma} h_\gamma(y_\beta) = y_{\alpha\beta\gamma} h_{\beta\gamma}(y_\alpha) h_\gamma(y_\beta),$$

és ezért

$$h_\gamma(y_{\alpha\beta}) (h_\beta(y_\alpha))^{y_\gamma} = h_{\beta\gamma}(y_\alpha) h_\gamma(y_\beta).$$

A transzfer definíciójában a $h_\alpha(g)$ értékeket szorozzuk össze az összes $\alpha \in G/H$ -ra. Most éppen ellenkezőleg, a h indexét tartjuk fixen, azaz $\delta \in G/H$ esetén legyen

$$g_\delta = \prod_{\alpha \in G/H} h_\delta(y_\alpha).$$

Az asszociativitásból kapott összefüggések összeszorzása a transzfer esetében annak bizonyításához vezetett, hogy a transzfer homomorfizmus. Szorozzuk most össze a fenti egyenleteket úgy, hogy α befutja G/H -t, és közben β, γ fixen marad. Az eredmény a következő lesz:

$$g_\gamma g_\beta^{y_\gamma} = g_{\beta\gamma} (h_\gamma(y_\beta))^n,$$

ahol $n = |G/H|$. Legyen r olyan egész, melyre rn kongruens 1-gyel modulo $|H|$. Ekkor a fenti egyenletből az adódik, hogy

$$h_\gamma(y_\beta) \left(g_\beta^{y_\gamma} g_\gamma \right)^{-r} = g_{\beta\gamma}^{-r}.$$

Legyen $\delta \in G/H$ esetén

$$z_\delta = y_\delta g_\delta^{-r}.$$

Belátjuk, hogy ezek az elemek részcsoportot alkotnak (mely persze komplementuma lesz H -nak, hiszen minden mellékosztályból pontosan egy elemet tartalmaz). Valóban,

$$z_\beta z_\gamma = y_\beta g_\beta^{-r} y_\gamma g_\gamma^{-r} = y_\beta y_\gamma \left(g_\beta^{y_\gamma} g_\gamma \right)^{-r} = y_{\beta\gamma} h_\gamma(y_\beta) \left(g_\beta^{y_\gamma} g_\gamma \right)^{-r} = y_{\beta\gamma} g_{\beta\gamma}^{-r} = z_{\beta\gamma}.$$

Ezzel a Schur–Zassenhaus tétel első felét beláttuk. \square

Bizonyítás nélkül megemlítjük Philip Hall feloldható csoportokról szóló tételét, ami a Sylow-tételek általánosítása. Ha π tetszőleges részhalma a prímszámok halmazának, akkor azt mondjuk, hogy k egy π -szám, ha minden prímosztója π -beli. Egy csoportot, vagy csoportelemet akkor nevezünk π -csoportnak illetve π -elemnek, ha rendjük π -szám. A π halmaz komplementumát (a prímelek halmazában) π' jelöli. A korábban már használt p -csoport illetve p' -elem fogalma a most bevezetett terminológia speciális esete, ha $\pi = \{p\}$. A G csoport egy H részcsoportját π -Hall részcsoportnak nevezzük, ha π -csoport, és indexe π' -szám.

5.3. Hall tétele. *Legyen G feloldható csoport, és π egy prímhalmaz.*

- (a) G -nek létezik π -Hall részcsoportja.
- (b) G bármely két π -Hall részcsoportja konjugált G -ben.
- (c) G bármely π -részcsoportja része G egy π -Hall részcsoportjának.

A bizonyítás nem nehéz indukcióval, a Schur–Zassenhaus tételt felhasználva. Megjegyezzük, hogy nem feloldható csoportokra a tétel nem igaz. Például az A_5 alternáló csoportnak sem $\{2, 5\}$ -, sem $\{3, 5\}$ -Hall részcsoportja nem lehet a 2.5. Lemma miatt. Az alábbi feladatok között megtalálhatjuk a Hall-tétel megfordítását is.

5.4. Feladat. *Bizonyítsuk be a Hall-tételt.*

Ötlet. Indukció $|G|$ szerint. Legyen N minimális normálosztó G -ben, akkor 4.8. Feladat és G feloldhatósága miatt N Abel-féle p -csoport. Alkalmazzuk az indukciós feltevést a G/N csoportra. Az egyetlen további ötlet a következő: ha H Hall-féle normálosztó G -ben, K komplementuma H -nak, és $H \subseteq A \subseteq G$, akkor $A \cap K$ komplementuma H -nak A -ban — a rendje miatt. \square

5.5. Feladat. *Legyen G csoport, melynek van három, páronként relatív prím indexű, feloldható részcsoporja. Igazoljuk, hogy G feloldható.*

Ötlet. Legyen G minimális rendű ellenpélda és A, B, C a három részcsopor. A rendek miatt bármely kettő szorzata G . Ha N minimális normálosztó A -ban, akkor N p -csoport, és így a B és a C közül amelyik indexe nem osztható p -vel, annak egy alkalmas D konjugáltja (a Sylow-tétel miatt) tartalmazza N -et. Ekkor $G = AD$ miatt az N által generált G -beli normálosztó része D -nek (lásd a 2.9. bizonyítását), és ezért G nem egyszerű. Mivel a feltétel öröklődik faktorcsoporra, G minimalitása miatt készen vagyunk. \square

A következő feladat a Hall-tétel (szintén Hall-tól származó) ígért megfordítása.

5.6. Feladat. *Tegyük fel, hogy a G csoport a rendjének minden p prímosztójára tartalmaz p' -Hall részcsoporatot. Ekkor G feloldható.*

Ötlet. Igazoljuk, hogy e részcsoporatok metszeteként minden π -re kapunk egy π -Hall részcsoporatot. Alkalmazzuk az előző feladatot, és Burnside két prímes tételét (2.8.). \square

5.7. Feladat. *Tegyük fel, hogy a G csoport minden maximális részcsoporja prímindexű. Bizonyítsuk be, hogy G feloldható.*

Ötlet. Legyen p a G csoport rendjének legnagyobb prímosztója és P egy p -Sylow G -ben. Mutassuk meg, hogy P normálosztó. (Legyen $N_G(P) \subseteq H$ egy maximális részcsopor. Hattassuk G -t a H mellékosztályain, és mutassuk meg, hogy P benne van e homomorfizmus magjában. Alkalmazzuk a Frattini-elvet). \square

5.8. Feladat. *Legyen G véges egyszerű csoport, melynek rendje nem osztható nyolccal. Igazoljuk, hogy az A_4 alternáló csoport előáll G egy alkalmas részcsoporjának homomorf képeként (azaz G involválja A_4 -et).*

Ötlet. Legyen P a G 2-Sylowja. Ez a Burnside-tétel miatt a Klein-csoport, melynek automorfizmus-csoportja S_3 . Így $N_G(P)/C_G(P)$ a Burnside-tétel miatt csak \mathbf{Z}_3 lehet. Legyen K a P (a Schur-Zassenhaus tétel szerint létező) komplementuma $C_G(P)$ -ben. Ekkor K centralizálja P -t, ezért normálosztó, s így karakterisztikus $C_G(P)$ -ben. A $H = N_G(P)/K$ csoport ekkor izomorf A_4 -gyel (ami a Klein-csoport és a \mathbf{Z}_3 egyetlen nem Abel-féle szemidirekt szorzata). \square

5.9. Feladat. *Legyen G nemkommutatív egyszerű csoport, melynek rendje kisebb, mint 168. Bizonyítsuk be, hogy G izomorf A_5 -tel.*

Ötlet. Ha $|G| = 60$, akkor az előző feladat miatt G -ben van 5 indexű részcsopor. Az eddigi tételek és módszerek felhasználásával az összes többi rend kizárható. \square

5.10. Feladat. *Tegyük fel, hogy a G csoport 2-Sylowja a nyolc elemű kvaterniócsoport. Bizonyítsuk be, hogy ha G nem involválja A_4 -et, akkor G -ben van normál 2-komplementum.*

Ötlet. Legyen G minimális ellenpélda. A Frobenius-tétel (4) \implies (1) állítása miatt a Q 2-Sylownak van két eleme, ami G -ben konjugált, de P -ben nem. Ezek csak negyedrendűek lehetnek Q szerkezete miatt, és így a konjugáló elem centralizálja közös négyzetüket, azaz a Q c centrumelemét. Ezért $C_G(c)$ nem valódi részcsoporth G minimalitása miatt. Faktorizáljunk le $\{e, c\}$ -vel, és alkalmazzuk az 5.8. Feladat megoldásának gondolatait. \square

REPREZENTÁCIÓ-ELMÉLET

6. Féligegyszerű Artin-algebrák. A Wedderburn–Artin tétel bizonyítása során szerzett ismereteket (lásd Fried 9.1. fejezet) egészítjük ki az alábbiakban. Minden szereplő gyűrűről feltesszük, hogy egységelemes, és minden modulusról, hogy unitér, és ha mást nem mondunk, baloldali. Egy modulus *teljesen reducibilisnek* nevezünk, ha minimális (= irreducibilis = egyszerű) modulusok összege. Ezek sok tekintetben úgy viselkednek, mint a vektorterek. Független vektorok (egy dimenziós alterek) helyett *független részmodulusokról* beszélünk.

6.1. Definíció. *Az M modulus M_α ($\alpha \in A$) részmodulusait akkor nevezzük függetlennek, ha összegük direkt összeg (azaz bármelyiknek a többi összegével vett metszete csak a nullából áll).*

Vegyük észre, hogy független halmaz része is független, és egy halmaz akkor és csak akkor független, ha minden véges részhalmaza az.

6.2. Lemma. *Legyen az M modulus az M_α ($\alpha \in A$) egyszerű részmodulusainak összege, és N egy részmodulusa N -nek. Ekkor van olyan $B \subseteq A$, hogy M_β ($\beta \in B$) függetlenek, és ha (direkt) összegüket K jelöli, akkor $M = N \oplus K$.*

Bizonyítás. Tekintsük az $\{N\} \cup \{M_\alpha \mid \alpha \in A\}$ halmaz azon részhalmazait, amelyek függetlenek, és N -et tartalmazzák. A Zorn-lemma miatt ezek között van maximális, mondjuk $\{N\} \cup \{M_\beta \mid \beta \in B\}$. Legyen $K = \sum \{M_\beta \mid \beta \in B\}$, ez persze direkt összeg, miként $N + K$ is az. Ha $\alpha \in A \setminus B$, akkor M_α egyszerűsége miatt vagy $M_\alpha \subseteq N + K$, vagy $M_\alpha \cap (N + K) = \{0\}$. Az utóbbi eset ellentmond az $\{N\} \cup \{M_\beta \mid \beta \in B\}$ halmaz maximalitásának, azaz $N + K = M$. \square

6.3. Tétel. *Legyen M teljesen reducibilis modulus, azaz az M_α ($\alpha \in A$) egyszerű részmodulusainak összege. Ekkor*

- (a) M az M_α modulusok közül néhánynak a direkt összege;
- (b) M minden része és faktora is teljesen reducibilis, és minden része direkt összeadandó;
- (c) M minden egyszerű részmodulusa és minden egyszerű faktormodulusa izomorf valamelyik M_α modulussal.

Bizonyítás. Az (a) állítás az előző lemmából adódik, ha $N = \{0\}$. A (b) állítás faktorokra vonatkozó része igaz, mert egyszerű modulus homomorf képe egyszerű, vagy nulla. Ha N

része M -nek, akkor az előző lemma miatt direkt összeadandó, és ha $M = N \oplus K$, akkor $N \cong M/K$, azaz teljesen reducibilis. Végül (c) bizonyításához legyen M/N egyszerű. Ekkor (b) miatt $M = N \oplus K$ alkalmas K -ra, azaz $M/N \cong K$. Így elég részmodulusra bizonyítani. Legyen N egyszerű részmodulus, és alkalmazzuk az előző lemmát. Mivel $K < M$, van olyan $\alpha \in A$, hogy $M_\alpha \not\subseteq K$. Ekkor $M = K \oplus M_\alpha$, hiszen $M/K \cong N$ egyszerű, és ezért $N \cong M/K \cong M_\alpha$. \square

6.4. Lemma. *Legyen M egyszerű modulus az R gyűrű felett. Ekkor M homomorf képe az ${}_R R$ modulusnak.*

Bizonyítás. Legyen $0 \neq m \in M$. Ekkor az $\psi(r) = rm$ képlettel definiált leképezés modulus-epimorfizmus. \square

6.5. Tétel. *Legyen R egyszerű gyűrű, melynek van egy J minimális balideálja. Ekkor ${}_R R$ teljesen reducibilis modulus, és minden egyszerű R -modulus izomorf ${}_R J$ -vel.*

Bizonyítás. Legyen $r \in R$, ekkor az r elemmel való jobbszorzás modulus-endorfizmusa ${}_R R$ -nek. Így ${}_R(Jr)$ vagy nulla, vagy izomorf ${}_R J$ -vel. Másrészt $I = \sum\{Jr \mid r \in R\}$ nyilván ideál, és így R egyszerűsége miatt $I = R$, azaz R teljesen reducibilis. Legyen M egyszerű R -modulus, akkor az előző lemma miatt M faktora ${}_R R$ -nek, és így 6.3.c miatt izomorf ${}_R J$ -vel. \square

6.6. Következmény. *Legyen $R = D^{n \times n}$ teljes mátrixgyűrű a D ferdetest felett. Ekkor bármely két R feletti egyszerű modulus izomorf.*

Bizonyítás. Tudjuk, hogy R egyszerű, és Artin-féle (Fried, 9.4). \square

Megjegyezzük, hogy közvetlen számolással is igazolható, hogy R minimális balideáljai izomorf R -modulusok, az alábbi állítás felhasználásával.

6.7. Feladat. *Legyen $R = D^{n \times n}$ teljes mátrixgyűrű a D ferdetest felett. Ekkor R balideáljai kölcsönösen egyértelmű megfeleltetésben állnak a D^n jobboldali D -vektortér altéréivel. A J balideálhoz tartozó altér $\{v \in D^n \mid Jv = 0\}$. A V altérhez tartozó balideál $\{r \in R \mid rV = 0\}$.*

Ötlet. Legyen J balideál, és a hozzá rendelt altér r dimenziós. Vegyünk egy maximális rangú lineáris transzformációt J -ben. Igazoljuk, hogy rangja $n - r$, és ezért generálja J -t.

6.8. Tétel. *Legyen R féligegyszerű Artin-gyűrű, amely k teljes mátrixgyűrű direkt szorzata. Ekkor R felett pontosan k darab nemizomorf egyszerű modulus van.*

Bizonyítás. Legyen $R = A_1 \times \cdots \times A_k$ a teljes mátrixgyűrűk direkt szorzatára való felbontás, és J_i az A_i egy minimális balideálja. Mivel $j \neq i$ esetén $A_j J_i = 0$, azért ${}_R J_i$ is egyszerű modulus, az A_i minimális balideáljai mint R -modulusok is izomorfak, és ${}_R J_i$ nem izomorf ${}_R J_j$ -vel (hiszen A_i másképp hat rajtuk). Ezért ha ${}_R R$ -et előállítjuk az összes A_i összes minimális balideáljainak összegeként, akkor éppen k -féle izomorfiatípus fog szerepelni. Ezért 6.3.c és 6.4. miatt R felett pontosan k -féle egyszerű modulus van. \square

Ha D ferdetest, akkor az $R = D^{n \times n}$ teljes mátrixgyűrűben az egységmátrix skalárszoroszai (az úgynevezett skalármátrixok) a D -vel izomorf részttestet alkotnak. E fölött a részttest fölött R pontosan akkor lesz algebra, ha D kommutatív.

6.10. Lemma. *Legyen D ferdetest. Ekkor az $R = D^{n \times n}$ centruma a dE skalármátrixokból áll, ahol $d \in Z(D)$ és E az egységmátrix.*

Bizonyítás. Legyen V egy n -dimenziós jobb vektortér D felett, melyen az R -beli mátrixok balszorzással hatnak, és $C \in Z(R)$. Ha $0 \neq v \in V$, akkor v és $w = Cv$ nem lehet lineárisan független D felett, hiszen különben volna olyan $A \in R$, hogy $Av = 0$, és $Aw \neq 0$, azaz az $Aw = ACv = CAv = 0$ ellentmondást kapnánk. Tehát $Cv = vd$ alkalmas $d \in D$ elemre. Ha most $u \in V$ tesztoljuk, akkor alkalmas $B \in R$ transzformációra $u = Bv$, és ezért $Cu = CBv = BCv = Bvd = ud$. Azaz C a d elemmel való jobbszorzás. Speciálisan ha $d' \in D$, akkor $C(vd') = vd'd$, de a C -vel való balszorzás D -linearitása miatt $C(vd') = (Cv)d' = vdd'$. Ezért $d \in Z(D)$. \square

6.11. Tétel. *Legyen F algebrailag zárt, kommutatív test és R véges dimenziós, féligegyszerű algebra F felett. Ekkor*

$$R \cong F^{n_1 \times n_1} \times \dots \times F^{n_k \times n_k}$$

alkalmas k és n_1, \dots, n_k egészekre. Az R felett izomorfia erejéig k darab irreducibilis modulus van, melyek vektorterek F felett, és dimenzióik rendre n_1, \dots, n_k . Végül $Z(R) \cong F^k$ (mint F -algebra).

Bizonyítás. Mivel R egységelemes, minden balideálja részalgebra is F felett. Ezért R Artin-gyűrű. Alkalmazzuk a Wedderburn–Artin tételt. A kapott teljes mátrixgyűrű komponensek ideálok R -ben, és ezért F feletti algebrák. Legyen $A = D^{n \times n}$ egy ilyen komponens, E ennek egységeleme. Ekkor $f \in F$ esetén az $f \circ E$ szorzat az algebra-axiómák miatt benne van A centrumában, azaz az előző lemma miatt egy dE skalármátrix-szal egyenlő, ahol $d \in Z(D)$. Az $f \mapsto d$ leképezés ismét az algebra-axiómák miatt gyűrűhomomorfizmus, ezért $Z(D)$ -nek van egy F -fel izomorf F' részteste.

Legyen $d' \in D$. Ekkor $F'(d')$ kommutatív test, mely F' -nek véges bővítése. Ezért d' algebrai F' felett. Mivel F algebrailag zárt, a d minimálpolinomja elsőfokú, azaz $d' \in F'$. Tehát $D = F' \cong F$.

Tehát R felbontása a kívánt alakú. A 6.8. Tétel szerint R felett k darab irreducibilis modulus van, melyek rendre izomorfak a mátrixgyűrű-komponensek minimális balideáljával. Mivel R egységelemes, az R centrumának is van F -fel izomorf részteste, és ezért ez a modulus-izomorfizmus F feletti vektortér-izomorfizmus is. Tehát elegendő $F^{n \times n}$ felett egy n -dimenziós, irreducibilis moduluszt konstruálni (hiszen ekkor a 6.5. Tétel miatt az összes többi is n -dimenziós lesz). Vegyük az F^n vektorteret mint oszlopvektorokat, és hassanak ezen az $F^{n \times n}$ mátrixai balszorzással. A kapott modulus nyilván irreducibilis lesz.

Végül R centruma a komponensek centrumainak direkt szorzata lesz. Ezek a centrumok a 6.10. Lemma miatt F -fel izomorfak. \square

7. Reprezentációk és a csoportalgebra. Legyen V n -dimenziós vektortér az F kommutatív test felett. A V invertálható lineáris transzformációi csoportot alkotnak a kompozícióra nézve, melyet $GL(V)$ -vel jelölünk (General Linear Group). Ezzel izomorf az $n \times n$ -es invertálható F feletti mátrixok csoportja, melynek jele $GL(n, F)$. Ha G véges csoport, akkor, mint a második fejezetben láttuk, hasznos eszköz tekinteni a G homomorfizmusait (illetve beágyazásait) az S_n szimmetrikus csoportba. Ugyanezt most az imént definiált lineáris csoportokkal fogjuk tenni.

7.1. Definíció. A G véges csoport egy \mathbf{X} homomorfizmusát a $GL(V)$ illetve $GL(n, F)$ csoportba a G csoport F feletti, n -edfokú (lineáris) reprezentációjának nevezzük.

Ezeket a reprezentációkat moduluselméleti eszközökkel fogjuk vizsgálni. Első lépésként bevezetjük a *csoportalgebra* fogalmát. Tekintsük a G elemeinek az F -beli együtthatókkal készített formális lineáris kombinációit. Ezeket komponensenként össze lehet adni, F -beli skalárral szorozni, és két ilyen lineáris kombinációt össze is szorozhatunk úgy, hogy a disztributivitás alapján szétbontjuk a szorzatot, a G -beli elemek között elvégezzük a szorzást, majd összevonjuk minden egyes G -beli elem együtthatóit. Könnyen látható, hogy F feletti algebrát kapunk, melyet csoportalgebrának nevezünk, és $F[G]$ -vel jelölünk.

Bár az iménti definíció nem precíz, könnyen azzá tehető lenne. Hasznosabb azonban a csoportalgebra egy másik megközelítését megvizsgálni. Tekintsük a G -ből az F testbe vezető összes függvényt. Ezek a pontonkénti összeadásra és skalárral szorzásra egy $|G|$ -dimenziós vektorteret alkotnak F fölött. E függvényeket azonosíthatjuk az imént definiált formális lineáris kombinációkkal, mégpedig a $\phi : G \rightarrow F$ függvényt a

$$\sum_{g \in G} \phi(g)g$$

összeggel. A $g \in G$ elemhez tehát az a függvény tartozik, amely a g helyen 1, a többi helyen 0 értéket vesz fel. A fenti szorzási szabályt áttranszformálva a következőt kapjuk:

$$(\phi \cdot \psi)(g) = \sum_{hk=g} \phi(h)\psi(k) = \sum_{h \in G} \phi(h)\psi(h^{-1}g).$$

Definiálhatnánk a szorzást tehát ezzel a képlettel is. Az alábbiakban a csoportalgebra mindkét formáját használni fogjuk, amelyik éppen kényelmesebb. További konvencióként G egységelemére az 1 jelet használjuk, mely persze egységeleme $F[G]$ -nek is. Az $f \cdot 1$ ($f \in F$) elemek az F -fel izomorf részttestet alkotnak a csoportalgebra centrumában, melyet F -fel azonosítunk.

Most kölcsönösen egyértelmű megfeleltetést létesítünk G reprezentációi, és a csoportalgebra feletti modulusok között. Legyen M modulus $F[G]$ felett. Ekkor M vektortér F felett (hiszen $F \subseteq F[G]$). Ha $g \in G \subseteq F[G]$, akkor legyen $\mathbf{X}(g)$ a g elemmel való bal-szorítás M -en. Ez F -lineáris transzformáció, hiszen g invertálható, és $\mathbf{X} : G \rightarrow GL(FM)$ csoporthomomorfizmus a modulusaxiómák miatt. Ezért ez reprezentáció. Megfordítva, ha $\mathbf{X} : G \rightarrow GL(V)$ egy reprezentáció, akkor ez kiterjeszthető lineárisan a csoportalgebrára is, azaz legyen

$$\left(\sum_{g \in G} \phi(g)g \right) \cdot v = \sum_{g \in G} (\mathbf{X}(g))(v).$$

Ez a művelet nyilván modulussá teszi V -t $F[G]$ felett. Könnyen látható, hogy ez a megfeleltetés a reprezentációk és a modulusok között kölcsönösen egyértelmű. Az izomorf modulusokhoz tartozó reprezentációkat *hasonló*, vagy *ekvivalens* reprezentációknak nevezzük.

7.2. Lemma. *A G csoport két reprezentációja a V vektortéren akkor és csak akkor hasonló, ha egymásba bázistranszformációval átvihetők (azaz mindkettőhöz alkalmas bázist választva, a kapott mátrixok G minden elemére megegyeznek). \square*

A reprezentációk leírásához tehát jó lenne ismerni a modulusokat a csoportalgebra felett. Az előző fejezetben bizonyított 6.11. Tételt akarjuk felhasználni. A csoportalgebra véges dimenziós F -algebra, hiszen $\dim_F(F[G]) = |G|$. A féligegyszerűséget az alábbi tétel fogja biztosítani.

7.3. Maschke tétele. *Tegyük fel, hogy F karakterisztikája nem osztja G rendjét. Ekkor $F[G]$ féligegyszerű gyűrű.*

A tétel bizonyítása nem nehéz (lásd Fried, 9.9. Tétel). Mivel nekünk csak a komplex test feletti reprezentációk vizsgálatára lesz szükségünk, mostantól kezdve *feltesszük, hogy minden reprezentáció a \mathbf{C} test feletti* (bár az algebrai számok teste felett például eredményeink szó szerint átvihetők lennének). A csoportelméletben igen fontos az az eset is, amikor az alaptest karakterisztikája osztja a csoport rendjét (az ún. moduláris reprezentációelmélet), ezzel azonban nem foglalkozunk.

Most egy alternatív bizonyítást mutatunk a Maschke-tételre (a komplex felett). A bizonyításhoz be kell vezetnünk egy, a későbbiekben is nélkülözhetetlen skaláris szorzatot $\mathbf{C}[G]$ -n. Legyen

$$[\phi, \psi]_G = \frac{1}{|G|} \sum_{g \in G} \phi(g) \overline{\psi(g)},$$

ahol a felülhúzás komplex konjugáltat jelöl. Ez természetesen euklideszi térré teszi $\mathbf{C}[G]$ -t \mathbf{C} felett. A G indexet általában el fogjuk hagyni.

7.4. Lemma. *Az imént definiált skalárszorzat G -invariáns, vagyis $g \in G$ esetén a g -vel való balszorzás unitér (azaz skalárszorzat-tartó) transzformáció.*

Bizonyítás.

$$[g\phi, g\psi] = \frac{1}{|G|} \sum_{h \in G} \phi(g^{-1}h) \overline{\psi(g^{-1}h)} = [\phi, \psi]. \quad \square$$

A Maschke-tételt a következőképpen bizonyítjuk. A Wedderburn–Artin tétel szerint (lásd Fried, 9.4) elég azt igazolni, hogy $\mathbf{C}[G]$ minden balideálja, mint $\mathbf{C}[G]$ -modulus, direkt összeadandó. Legyen J balideál, és tekintsük J ortogonális kiegészítő alterét, azaz azon elemek halmazát $\mathbf{C}[G]$ -ben, melyeknek J minden elemével vett skaláris szorzata nulla. Mivel a skalárszorzat G -invariáns, ez a kiegészítő altér zárt a G elemeivel való balszorzásra, azaz részmodulus. \square

A Wedderburn–Artin tétel miatt tehát minden $\mathbf{C}[G]$ -modulus teljesen reducibilis, azaz irreducibilis modulusok direkt összege. Az irreducibilis modulusok leírását a 6.11. Tételből kapjuk. Tekintsük a $\mathbf{C}[G]$ csoportalgebrát, mint saját maga feletti modulusot. Ennek neve a G reguláris reprezentációja.

7.5. Tétel. Jelölje k a G csoport \mathbf{C} feletti irreducibilis reprezentációinak számát, és n_1, \dots, n_k ezek fokait.

- (a) A G reguláris reprezentációjában mindegyik irreducibilis reprezentáció akkora multiplicitással szerepel, amennyi a foka.
- (b) $n_1^2 + \dots + n_k^2 = |G|$.
- (b) A k értéke megegyezik G konjugált osztályainak számával.

Bizonyítás. Az (a) és a (b) állítás azonnal következik a 6.11. Tételből. A (c) bizonyításához nevezzünk egy $\phi \in \mathbf{C}[G]$ elemet *osztályfüggvénynek*, ha G minden konjugált osztályán állandó. Jelölje $\mathcal{K}_1, \dots, \mathcal{K}_k$ a G konjugált osztályait, és K_i az i -edik osztály elemeinek összegét $\mathbf{C}[G]$ -ben. A K_i -nek megfelelő függvény tehát a K_i elemein 1, másutt nulla. A bizonyítás befejezéséhez elegendő a következő állítást igazolni.

7.6. Lemma. A $\mathbf{C}[G]$ csoportalgebra centruma éppen az osztályfüggvényekből áll. A K_1, \dots, K_k elemek bázist alkotnak $Z(\mathbf{C}[G])$ -ben (azaz az osztályfüggvények alterében), és ha

$$K_i \cdot K_j = \sum_{\nu=1}^k a_{ij\nu} K_\nu,$$

akkor az $a_{ij\nu}$ számok nemnegatív egészek.

Bizonyítás. A

$$g^{-1} \left(\sum_{h \in G} \phi(h)h \right) g = \sum_{h \in G} \phi(h)g^{-1}hg = \sum_{h \in G} \phi(ghg^{-1})h$$

összefüggés szerint $\mathbf{C}[G]$ centrumában tényleg az osztályfüggvények vannak. A másik állítás azért igaz, mert ha $g \in \mathcal{K}_\nu$, akkor

$$a_{ij\nu} = |\{(x, y) \mid x \in \mathcal{K}_i, y \in \mathcal{K}_j, xy = g\}|. \quad \square$$

7.7. Következmény. A G csoport pontosan akkor Abel, ha minden irreducibilis reprezentációja elsőfokú.

Bizonyítás. Ha G Abel, akkor a 7.5. Tétel miatt $k = |G|$, és ezért mindegyik $n_i = 1$. Megfordítva, ha minden $n_i = 1$, akkor $\mathbf{C}[G]$ testek direkt összege, azaz kommutatív, és így G is az. \square

Az eddigiek alkalmazásaképpen belátunk egy tisztán lineáris algebrai állítást, melyre később szükségünk lesz.

7.8. Lemma. Legyen A lineáris transzformáció a V (komplex) vektortéren, melyre A^m az identitás. Ekkor V alkalmas bázisában A mátrixa diagonális.

Bizonyítás. Tekintsük a $G = \mathbf{Z}_m$ ciklikus csoportot, és g legyen ennek egy generátoreleme. Ekkor a $g^i \mapsto A^i$ leképezés a G egy reprezentációja $GL(V)$ -be. A 7.7. Következmény miatt G minden irreducibilis reprezentációja elsőfokú, azaz a kapott modulus felbomlik egydimenziós részmodulusok direkt összegére. Ezek az egydimenziós alterek A -invariánsak, és így A sajátvektoraiból állanak. A direkt felbontás tehát olyan bázist eredményez, mely A sajátvektoraiból áll, és ebben a bázisban A mátrixa diagonális. \square

8. Csoportkarakterek. Ha \mathbf{X} a G csoport n -edfokú mátrix-reprezentációja, akkor ez $|G|$ darab mátrix, vagyis $|G|n^2$ szám megadását jelenti. Ezek a számok azonban jórészt feleslegesek, arra szolgálnak, hogy hasonló reprezentációkat (melyek egymáshoz képest nem adnak új információt G -ről), egymástól megkülönböztessenek. Megmutatjuk, hogy a reprezentáló mátrixok nyoma már elegendő információt tartalmaz a reprezentáció felismeréséhez. Az A mátrix nyomát (azaz főátlóbeli elemeinek összegét) $\text{tr}(A)$ jelöli. A most következő állítást, melyet igen könnyű igazolni, lineáris algebrából ismertnek tételezzük fel.

8.1. Lemma. *Az A $n \times n$ -es komplex elemű mátrix nyoma éppen a sajátértékeinek (multiplicitásokkal vett) összege, és az A karakterisztikus polinomjában az x^{n-1} együtthatójának $(-1)^{n+1}$ -szerese. Ha B is $n \times n$ -es mátrix, akkor $\text{tr}(AB) = \text{tr}(BA)$, és ezért ha C $n \times n$ -es invertálható mátrix, akkor $\text{tr}(C^{-1}AC) = \text{tr}(A)$. \square*

8.2. Definíció. *A \mathbf{X} reprezentáció karaktere a $\chi(g) = \text{tr}(\mathbf{X}(g))$ összefüggéssel definiált függvény.*

Ha $\mathbf{X} : G \rightarrow GL(V)$, akkor a $\mathbf{X}(g)$ lineáris transzformáció nyomán tetszőleges bázisban vett mátrixának nyomát értjük; az előző lemma miatt ez nem függ a bázis választásától. Egy karakter tehát G -ből \mathbf{C} -be képez, azaz a csoportalgebrának eleme. Megjegyezzük azonban, hogy miként \mathbf{X} kiterjeszthető a csoportalgebrára lineárisan, ugyanúgy karaktere is kiterjed, azaz a karaktereket felfoghatjuk a csoportalgebrát \mathbf{C} -be képző lineáris funkcionáloknak is. Az alábbiakban a karakterekre vonatkozó elemi tudnivalókat foglaljuk össze.

8.3. Lemma. *Legyen G véges csoport, $g, h \in G$, \mathbf{X} a G egy n -edfokú reprezentációja \mathbf{C} felett, és χ ennek karaktere.*

- (a) *A χ karakter osztályfüggvény és $\chi(gh) = \chi(hg)$. \square*
- (b) *Hasonló reprezentációk karaktere megegyezik. \square*
- (c) *$n = \chi(1)$ (ahol 1 a G egységeleme). \square*
- (d) *Reprezentációk direkt összegéhez a karakterek összege tartozik. \square*
- (e) *$\chi(g)$ előáll, mint n darab $|g|$ -edik egységgyök összege (és így algebrai egész).*
- (f) *$\chi(g^{-1}) = \overline{\chi(g)}$.*
- (g) *$|\chi(g)| \leq n$.*
- (h) *Ha $|\chi(g)| = n$, akkor $\mathbf{X}(g)$ az identitás $|g|$ -edik egységgyökszöröse.*
- (i) *$\text{Ker}(\mathbf{X}) = \{g \in G \mid \chi(g) = n\}$.*

Bizonyítás. Az (e) állítás igazolásához vegyük észre, hogy $g^{|g|} = 1$ miatt $\mathbf{X}(g)^{|g|}$ az identitás, és ezért $\mathbf{X}(g)$ minden sajátértéke $|g|$ -edik egységgyök. Mivel egységgyök inverze a konjugáltja, (f) is adódik. Legyen $\chi(g) = \varepsilon_1 + \dots + \varepsilon_n$, ahol $\varepsilon_1, \dots, \varepsilon_n$ egységgyökök. A háromszög-egyenlőtlenség miatt $|\chi(g)| \leq n$. Egyenlőség csak akkor lehet, ha valamennyi ε_i egy irányba áll, azaz egyenlőek. A 7.8. Lemma miatt azonban $\mathbf{X}(g)$ alkalmas bázisban diagonális, és így ugyanebben a bázisban skalármátrix is, azaz (h) igaz. Végül (i) speciális esete (h)-nak. \square

Ebből a lemmából már érezhető, hogy a karakterek ismeretében a csoportról is sok információt kaphatunk — belátjuk majd, hogy például G centrumát és normálosztóit is meg lehet határozni.

Első célunk annak kimutatása, hogy a karakterek (a 7.4. Lemmában szereplő skalárszorozatra nézve) ortonormált bázist alkotnak az osztályfüggvények között. Rögzítsük egyszer s mindenkorra a csoportalgebra $\mathbf{C}[G] = A_1 \oplus \cdots \oplus A_k$ ideálokra való felbontását, ahol tehát $A_i \cong F^{n_i \times n_i}$. Jelölje e_i az A_i egységelemét. Legyen \mathbf{X}_i az a reprezentáció, amely a csoportalgebra (és így G) tetszőleges eleméhez annak A_i -beli komponensét rendeli (amit egy $n_i \times n_i$ -s mátrixnak tekinthetünk). Végül legyen χ_i a \mathbf{X}_i karaktere (ekkor tehát $n_i = \chi_i(1)$). Emlékeztetünk arra, hogy a G csoport reguláris reprezentációja a csoportalgebrából, mint saját maga feletti modulusból kapott reprezentáció.

8.4. Lemma. *Legyen ρ a G reguláris reprezentációjához tartozó karakter. Ekkor*

$$(a) \quad \rho(g) = \begin{cases} |G| & \text{ha } g = 1 \\ 0 & \text{ha } g \neq 1. \end{cases}$$

$$(b) \quad \rho = \sum_{i=1}^k n_i \chi_i.$$

$$(c) \quad e_1 + \cdots + e_n = 1 \quad (\text{a } G \text{ egységeleme}).$$

$$(d) \quad e_i = \frac{n_i}{|G|} \sum_{g \in G} \chi_i(g^{-1})g.$$

Bizonyítás. Tekintsük a csoportalgebrának azt a bázisát, mely G elemeiből áll. Ebben az $1 \in G$ -vel való balszorozás mátrixa az egységmátrix, ha viszont $g \neq 1$, akkor a g -vel való balszorozás mátrixának diagonálisában csupa nulla áll, és ezért (a) igaz. A (b) állítás csak átfogalmazza 7.5.b-t karakterekre. A (c) bizonyításához legyen $1 = a_1 + \cdots + a_k$, $a_i \in A_i$. Ezt e_i -vel szorozva $e_i = a_i$ adódik. Végül legyen $e_i = \sum \phi(g)g$. Jobbról g^{-1} -gyel szorozva (a)-ból azt kapjuk, hogy $\rho(e_i g^{-1}) = \phi(g)|G|$. Ezért (b) miatt

$$\phi(g)|G| = \sum_{j=1}^k n_j \chi_j(e_i g^{-1}).$$

A jobboldalt azonban ki tudjuk számolni. Az \mathbf{X}_j reprezentáció ugyanis nullába viszi az A_i ideált ha $i \neq j$, az A_j ideálon viszont identikusan hat, s így $\mathbf{X}_j(e_i g^{-1}) = \mathbf{X}_j(e_i) \mathbf{X}_j(g^{-1}) = 0$ ha $i \neq j$, és $\mathbf{X}_j(g^{-1})$ különben. Karakterekre áttérve $\chi_j(e_i g^{-1}) = \chi_j(g^{-1}) \delta_{ij}$, ahol δ_{ij} a Kronecker-delta. Ezt a fenti képletbe helyettesítve (d) adódik. \square

A (d) állítást úgy is fogalmazhatjuk, hogy az e_i elemnek megfelelő függvény a csoportalgebrában éppen az i -edik karakter konjugáltjának $n_i/|G|$ -szerese.

8.5. Általánosított ortogonalitási reláció. *Legyen $h \in G$. Ekkor*

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(gh) \chi_j(g^{-1}) = \delta_{ij} \frac{\chi_i(h)}{n_i}.$$

Bizonyítás. Helyettesítsük be az $e_j e_i = \delta_{ij} e_i$ egyenletbe az előző lemma (d) pontjának képletét, és nézzük meg h^{-1} együtthatóját. Ekkor $\chi_i(gh) = \chi_i(hg)$ miatt a kívánt egyenlőséget kapjuk. \square

8.6. Tétel. *Az irreducibilis karakterek (a $[\ , \]_G$ skalárszorzatra nézve) ortonormált bázist alkotnak az osztályfüggvények között.*

Bizonyítás. Alkalmazzuk az előző lemmát $h = 1$ -re. A 8.3.f miatt azt kapjuk, hogy az irreducibilis karakterek ortonormált rendszert alkotnak az osztályfüggvények terében. Mivel e tér k dimenziós, ez a rendszer bázis is. \square

8.7. Következmény. *Két reprezentáció akkor és csak akkor hasonló, ha karakterük megegyezik. A $c_1\chi_1 + \dots + c_k\chi_k$ akkor és csak akkor karakter, ha a c_i számok nemnegatív egészek. A χ karakter akkor és csak akkor irreducibilis, ha $[\chi, \chi] = 1$.*

Bizonyítás. Legyen χ egy karakter. Ekkor a hozzá tartozó reprezentáció irreducibilisek direkt összege. Ha az i -edik irreducibilis reprezentáció c_i -szer szerepel, akkor $\chi = c_1\chi_1 + \dots + c_k\chi_k$, és ezért $c_i = [\chi, \chi_i]$. Azaz a c_i számokat már χ meghatározza. A másik két állítás hasonlóan igazolható. \square

9. A karaktertábla. A G csoport irreducibilis karaktereinek értékeit egy mátrixba foglaljuk a következő módon. A mátrix sorai a χ_1, \dots, χ_k karaktereknek, oszlopai pedig a G csoport $\mathcal{K}_1, \dots, \mathcal{K}_k$ konjugált osztályainak felelnek meg. Az i -edik sor j -edik eleme az a szám, amelyet a χ_i a \mathcal{K}_j tetszőleges elemén felvesz. Jelölje T az így kapott mátrixot, melynek neve G karaktertáblája. A karaktertáblát azért érdemes tekinteni, mert egyrészt nagyon sok hasznos információt tartalmaz a csoportról, másrészt *sokszor elkészíthető a reprezentációk ismerete nélkül is.*

9.1. Második ortogonalitási reláció. *Legyen $g, h \in G$. Ekkor*

$$\sum_{i=1}^k \chi_i(g)\chi_i(h) = \delta_{gh}|C_G(g)|,$$

ahol δ_{gh} értéke 1 ha g és h konjugáltak, és 0 ha nem.

Bizonyítás. Legyen T a G karaktertáblája, és D az a diagonális mátrix, melynek főátlójában a $|\mathcal{K}_j|$ értékek állnak. Az, hogy a karakterek ortonormáltak, azt jelenti, hogy $TDT^* = |G|E$, ahol T^* a T transzponáltjának konjugáltját jelöli, és E az egységmátrix. Tudjuk, hogy négyzetes mátrixok körében a balinverz egyben jobbinverz is, ezért $DT^*T = |G|E$. A szorzást elvégezve, és a $g \in \mathcal{K}_j$ esetén fennálló $|\mathcal{K}_i||C_G(g)| = |G|$ összefüggést felhasználva éppen az állítást kapjuk. \square

Most megvizsgáljuk, mi az összefüggés a G normálosztói és a karaktertábla között. A 8.3.i miatt egy tetszőleges \mathbf{X} reprezentáció χ karaktere meghatározza a reprezentáció magját, ami tehát a $\chi(g) = \chi(1)$ összefüggést teljesítő g elemekből áll. Ezt a normálosztót a továbbiakban $\text{Ker}(\chi)$ jelöli.

9.2. Lemma. *Legyen $\chi = m_1\chi_1 + \dots + m_k\chi_k$ a χ karakter felbontása irreducibilisek összegére. Ekkor*

$$\text{Ker}(\chi) = \bigcap \{\text{Ker}(\chi_i) \mid m_i > 0\}.$$

Az összes irreducibilis karakter magjának metszete $\{1\}$.

Bizonyítás. Legyen $g \in G$. A háromszög-egyenlőtlenséget alkalmazva, 8.3.g miatt

$$|\chi(g)| \leq m_1|\chi_1(g)| + \cdots + m_k|\chi_k(g)| \leq m_1\chi_1(1) + \cdots + m_k\chi_k(1) = \chi(1),$$

és egyenlőség csak akkor állhat, ha $m_i > 0$ esetén $|\chi_i(g)| = \chi_i(1)$, továbbá e komplex számok egyállásúak. Ha tehát $\chi(g) = \chi(1)$, akkor $m_i > 0$ esetén $\chi_i(g) = \chi_i(1)$, ami az első állítást bizonyítja. A kapott képlet szerint a második állítás igazolásához elegendő találni egy olyan reprezentációt, melynek magja $\{1\}$. A G reguláris reprezentációja nyilván ilyen. \square

9.3. Lemma. *Legyen $N \triangleleft G$. Ekkor a G/N reprezentációi kölcsönösen egyértelmű megfeleltetésben állnak a G azon reprezentációival, melyek magja N -et tartalmazza. Irreducibilis reprezentációk egymásnak felelnek meg. Ha $\hat{\chi}$ karaktere G/N -nek, akkor az ennek megfelelő G -karakter $\chi(g) = \hat{\chi}(gN)$. Megfordítva, ha $N \subseteq \text{Ker}(\chi)$, akkor χ konstans az N mellékosztályain, és a $\hat{\chi}(gN) = \chi(g)$ képlet a faktorcsoport karakterét értelmezi.* \square

9.4. Következmény. *Legyen $N \triangleleft G$. Ekkor*

- (a) $N = \bigcap \{\text{Ker}(\chi_i) \mid N \subseteq \text{Ker}(\chi_i)\}$.
- (b) $|G : N| = \sum \{n_i^2 \mid N \subseteq \text{Ker}(\chi_i)\}$.

Bizonyítás. Tekintsük a G/N reguláris reprezentációját, ennek magja éppen N . E reprezentációban G azon irreducibilis reprezentációi szerepelnek, melyek magja tartalmazza N -et, mindegyik annyiszor, amennyi a foka. Ezért a hozzá tartozó karakter,

$$\rho_N = \sum \{n_i\chi_i \mid N \subseteq \text{Ker}(\chi_i)\}.$$

Innen (a) következik 9.2. miatt. Mivel ρ_N az N elemein $|G/N|$, másutt nulla, (b) is adódik úgy, hogy az előbbi képletbe behelyettesítjük a csoport egységelemét. \square

9.5. Feladat. *Legyen $N \triangleleft G$ és tegyük fel, hogy N nem része a χ_i irreducibilis karakter magjának. Igazoljuk, hogy*

$$\sum_{g \in N} \chi_i(g) = 0.$$

Ötlet. Számítsuk ki a $[\rho_N, \chi_i]_G$ skalárszorzatot. \square

A 9.4. Következmény szerint tehát G minden normálosztója előáll, mint egy alkalmas karakter magja, azaz G néhány irreducibilis karaktere magjának metszeteként. Ezért a karaktertáblából megkaphatók G normálosztói, sőt ezek rendjei is 9.4.(b) miatt. Megjegyezzük, hogy e rendet másképp is kiszámolhatjuk, a második ortogonalitási reláció miatt ugyanis ismerjük G konjugált osztályainak rendjét, N pedig ilyenek uniója. A normálosztók és rendjeik ismeretében persze az is eldönthető, hogy G egyszerű-e, illetve feloldható-e.

Könnyen láthatóan a G/N karaktertábláját is ki lehet számolni G karaktertáblájából. Az N karaktertáblájával más a helyzet, bár vannak igen hasznos tételek (pl. *Clifford* tétel), amelyek G és N reprezentációinak kapcsolatáról szólnak. Az sem igaz, hogy G

izomorfia erejéig meghatározható lenne a karaktertáblából, látni fogjuk például, hogy a nyolcelemű diéder- és kvaterniócsoportnak ugyanaz a karaktertáblája. A G kommutátor-részcsoportja azonban meghatározható, ez következő célunk.

A G elsőfokú karaktereit *lineáris karaktereknek* nevezzük, ezek (és csak ezek) lesznek homomorfizmusok \mathbf{C} -be. Ezek persze irreducibilisek is. Lineáris karaktere minden csoportnak van, mégpedig az a χ_1 függvény, mely minden csoportelemhez az 1-et rendeli. Ezt a karaktert a karaktertábla első sorába írjuk, és G főkarakterének nevezzük.

9.6. Állítás. *A G lineáris karaktereinek száma $|G : G'|$, magjaik metszete pedig G' .*

Bizonyítás. Ha λ lineáris karakter, akkor egy homomorfizmus is a \mathbf{C} multiplikatív csoportjába, ami kommutatív. Ezért $G' \subseteq \text{Ker}(\lambda)$. Megfordítva, mivel G/G' Abel, 7.7 miatt minden karaktere lineáris, és ezt G -re felemelve is lineáris karaktert kapunk. Ezért G lineáris karakterei éppen azok, melyek magja tartalmazza G' -t, vagyis ezek G/G' összes karakterével állnak kölcsönösen egyértelmű megfelelésben. Ezért az állítás a 9.4. Következmény speciális esete. \square

Hogyan lehet a karaktertáblából leolvasni a csoport centrumát? Ebben a 8.3.h állítás lesz segítségünkre. Ha χ karaktere G -nek, akkor legyen

$$Z(\chi) = \{g \in G \mid |\chi(g)| = \chi(1)\}.$$

E fogalom vizsgálatához először is általánosítanunk kell a 6.10. Lemmát.

9.7. Lemma. *Legyen \mathbf{X} n -edfokú irreducibilis reprezentációja G -nek. Ha az M $n \times n$ -es mátrix felcserélhető $\mathbf{X}(g)$ -vel minden $g \in G$ -re, akkor M skalármátrix.*

Bizonyítás. Legyen V az \mathbf{X} reprezentációhoz tartozó modulus. Ekkor tehát V egy n -dimenziós \mathbf{C} -vektortér, és feltételünk azt mondja ki, hogy az M mátrixhoz tartozó lineáris transzformáció endomorfizmusa a ${}_{\mathbf{C}[G]}V$ modulusnak. A Schur-lemma miatt ezek az endomorfizmusok egy D ferdetestet alkotnak. Persze D tartalmazza a nyújtásokat, amik egy \mathbf{C} -vel izomorf \mathbf{C}' részttestet alkotnak D centrumában, és mivel D elemei \mathbf{C} -lineáris transzformációk V -n, a D véges dimenziós algebra \mathbf{C} felett. Mivel \mathbf{C} algebrailag zárt, (a 6.11. Tétel szerint) $D = \mathbf{C}'$. \square

A következő állítás a reprezentációelmélettől függetlenül is igen fontos.

9.8. Tétel. *Legyen G véges részcsoportja az F kommutatív test multiplikatív csoportjának. Ekkor G ciklikus. Speciálisan véges test multiplikatív csoportja ciklikus.*

Bizonyítás. Az $x^d - 1$ polinomnak legfeljebb d gyöke lehet F -ben, és így G -ben is. Ezt az észrevételt G rendjének prímosztóira alkalmazva látjuk, hogy állításunk következik a véges Abel-csoportok alaptételéből. \square

9.9. Feladat. *Legyen G nem feltétlenül kommutatív véges csoport. Tegyük fel, hogy minden d -re legfeljebb d darab olyan elem van G -ben, melynek d -edik hatványa az egysegelem. Igazoljuk, hogy G ciklikus.*

Ötlet. Legyen $|G| = n$ és d_G a d rendű elemek száma. A $H = \mathbf{Z}_n$ csoportról mutassuk ki, hogy $d_H = \varphi(d)$, ahol φ az Euler-függvény, és ezért

$$\sum_{d|n} \varphi(d) = n.$$

A feltétel miatt $d_G \leq \varphi(d)$, és ezért G -ben kell lennie n -edrendű elemnek. \square

Most már megfogalmazhatjuk a centrumra vonatkozó állításokat. Ha H részcsoportja G -nek, és \mathbf{X} reprezentációja G -nek, melynek karaktere χ , akkor ezek megszorítását H -ra jelölje $\mathbf{X}|_H$, illetve $\chi|_H$. Nyilván $\mathbf{X}|_H$ reprezentáció, és ezért $\chi|_H$ karaktere H -nak.

9.10. Tétel. *Legyen χ karaktere G -nek, $n = \chi(1)$ ennek foka, és $Z = Z(\chi)$.*

- (a) Z normálosztó G -ben.
- (b) $Z/\text{Ker}(\chi) \subseteq Z(G/\text{Ker}(\chi))$. Ha χ irreducibilis, egyenlőség áll.
- (c) $Z(G) = \bigcap \{Z(\chi_i) \mid 1 \leq i \leq k\}$.
- (d) $Z/\text{Ker}(\chi)$ ciklikus csoport.
- (e) $\chi|_Z = n\lambda$, ahol λ lineáris karaktere Z -nek.

Bizonyítás. Legyen \mathbf{X} egy χ -hez tartozó reprezentáció. Ekkor $g \in Z$ esetén 8.3.h miatt $\mathbf{X}(g) = \lambda(g)E$ alkalmas $\lambda(g)$ komplex számra, ahol E az egységmátrix. Mivel \mathbf{X} homomorfizmus, λ is az, ami (e)-t bizonyítja. Azt is látjuk, hogy Z részcsoport, és mivel χ osztályfüggvény, normálosztó is. Nyilván $\text{Ker}(\lambda) = \text{Ker}(\chi) \subseteq Z$, és így a homomorfizmus-tétel miatt $Z/\text{Ker}(\chi)$ izomorf \mathbf{C} multiplikatív csoportjának egy részcsoportjával, azaz 9.8 miatt ciklikus. A (b) állítás kimutatásához vegyük észre, hogy $G/\text{Ker}(\chi)$ a \mathbf{X} által beágyazódik a $GL(n, \mathbf{C})$ csoportba, és $Z/\text{Ker}(\chi)$ a centrumba képződik. Ezért $Z/\text{Ker}(\chi) \subseteq Z(G/\text{Ker}(\chi))$. Ha χ irreducibilis, akkor a 9.7. Lemma miatt egyenlőség áll.

Végül belátjuk (c)-t. Ha $g \in Z(G)$, akkor $\text{Ker}(\chi_i)$ szerint faktorizálva is a centrumban marad, azaz (b) miatt $g \in Z(\chi_i)$. Megfordítva, ha $g \in Z(\chi_i)$ minden i -re, akkor (b) miatt g tetszőleges $h \in G$ -vel felcserélhető modulo $\text{Ker}(\chi_i)$. Azaz $[g, h] \in \text{Ker}(\chi_i)$, és így a 9.2. Lemma miatt $[g, h] = 1$. \square

Az eddigi eredmények alkalmazásaképpen meghatározzuk a nyolcelemű nemkommutatív csoportok karaktertábláját. Legyen G ilyen csoport. Mivel $G/Z(G)$ nem lehet ciklikus, $Z(G)$ kételemű, ezért $G/Z(G)$ négyelemű, s így Abel. Azaz G' része $Z(G)$ -nek, és mivel G nem Abel, egyenlők is. Ezért G -nek négy lineáris karaktere van, melyek a $G/Z(G)$, azaz a Klein-csoport karaktereinek felelnek meg. Az $n_1^2 + \dots + n_k^2 = |G| = 8$ összefüggésből azt kapjuk, hogy $k = 5$, $n_1 = n_2 = n_3 = n_4 = 1$, és $n_5 = 2$. Mivel minden homomorfizmus G -ből \mathbf{C} multiplikatív csoportjába reprezentáció, és így egyben karakter is, továbbá irreducibilis kell legyen, hiszen elsőfokú, azért a Klein-csoport karaktertáblája a következő:

\mathbf{Z}_2^2	1	a	b	c
χ_1	1	1	1	1
χ_2	1	-1	-1	1
χ_3	1	-1	1	-1
χ_4	1	1	-1	-1

Soroljuk most fel G konjugált osztályait. Ezek $\mathcal{K}_1 = \{1\}$, $\mathcal{K}_2 = \{z\}$, ahol z a centrum másik eleme, $\mathcal{K}_3, \mathcal{K}_4, \mathcal{K}_5$. Ez utóbbi osztályok rendje egynél nagyobb kettő-hatvány, és így csak kettő lehet, hiszen a rendek összege nyolc. A centrum szerinti faktor kommutativitása miatt a konjugált osztályok képe egyelemű, azaz a három kételemű konjugált osztály a centrum szerinti mellékosztály is egyben. A 9.3. Lemma miatt tehát kitölthetjük

G karaktertáblájának első négy sorát. A második ortogonalitási reláció miatt χ_5 értéke nulla az utolsó három helyen, és $|\chi_5(z)| = 2$. Mivel χ_1 és χ_5 ortogonális, $\chi_5(z) = -2$.

D_4, Q	1	z	\mathcal{K}_3	\mathcal{K}_4	\mathcal{K}_5
χ_1	1	1	1	1	1
χ_2	1	1	-1	-1	1
χ_3	1	1	-1	1	-1
χ_4	1	1	1	-1	-1
χ_5	2	-2	0	0	0

Annak bizonyítása, hogy G csak D_4 vagy Q lehet, megtalálható a Fried-könyv 4.17 fejezetében.

9.11. Feladat. Az iménti karaktertáblából határozzuk meg G összes normálosztóit és a $Z(\chi_i)$ -ket. Adjuk meg a D_4 , illetve a Q a χ_5 karakterhez tartozó (egyik) reprezentációját.

9.12. Feladat. Számítsuk ki az S_3 , A_4 , D_6 , S_4 csoportok karaktertábláit. Ellenőrzés céljából megadjuk a válaszokat. Legyen $\omega = e^{2\pi i/3}$. A konjugált osztályokat egy-egy reprezentánssal adjuk meg, elemeik száma a második sorban szerepel.

S_3	1	(123)	(12)	D_6	1	f^3	$\{f, f^5\}$	$\{f^2, f^4\}$	$\{t, tf^2, tf^4\}$	$\{tf, tf^3, tf^5\}$
6	1	2	3	12	1	1	2	2	3	3
χ_1	1	1	1	χ_1	1	1	1	1	1	1
χ_2	1	1	-1	χ_2	1	1	1	1	-1	-1
χ_3	2	-1	0	χ_3	1	-1	-1	1	-1	1
				χ_4	1	-1	-1	1	1	-1
				χ_5	2	2	-1	-1	0	0
				χ_6	2	-2	1	-1	0	0

A_4	1	(12)(34)	(123)	(132)	S_4	1	(12)(34)	(123)	(12)	(1234)
12	1	3	4	4	24	1	3	8	6	6
χ_1	1	1	1	1	χ_1	1	1	1	1	1
χ_2	1	1	ω	$\bar{\omega}$	χ_2	1	1	1	-1	-1
χ_3	1	1	$\bar{\omega}$	ω	χ_3	2	2	-1	0	0
χ_4	3	-1	0	0	χ_4	3	-1	0	1	-1
					χ_5	3	-1	0	-1	1

A megoldáshoz használjuk fel a 9.3. Lemmát és az ortogonalitási relációkat.

9.13. Feladat. Legyen G véges Abel-csoport. Igazoljuk, hogy G karakterei a pontonkénti szorzásra nézve csoportot alkotnak, mely G -vel izomorf.

Ötlet. Ha G ciklikus, az állítás közvetlen számolással adódik. Az általános eset igazolásához használjuk fel, hogy ha A, B, C Abel-csoportok, akkor $\text{Hom}(A \times B, C) \cong \text{Hom}(A, C) \times \text{Hom}(B, C)$. \square

9.14. Feladat. Legyen $g \in G$. Igazoljuk, hogy g pontosan akkor konjugált az inverzével, ha G minden karakterére $\chi(g)$ valós.

Ötlet. Mivel az irreducibilis karakterek bázist alkotnak az osztályfüggvények között, bármely két nem konjugált elemhez van olyan irreducibilis karakter, mely ezeken különbözik. \square

9.15. Feladat. Mutassuk meg, hogy $\chi(1)^2 \leq |G : Z(\chi)|$ teljesül a G csoport minden irreducibilis χ karakterére.

Ötlet. Használjuk fel, hogy $[\chi, \chi] = 1$. \square

9.16. Feladat. Legyen G véges csoport, és A valódi, Abel-féle részcsoporthoz G -ben. Tegyük fel, hogy G -nek van $|G : A|$ fokú irreducibilis reprezentációja. Igazoljuk, hogy G -nek van nemtriviális, Abel-féle normálosztója.

Ötlet. Legyen χ irreducibilis, $|G : A|$ fokú karakter, és $\chi|_A = m_1\lambda_1 + \dots + m_t\lambda_t$ az A irreducibilis (elsőfokú) karaktereire való felbontás. Tehát m_i pozitív egész, és

$$1 = [\chi, \chi]_G \geq \frac{|A|}{|G|} [\chi|_A, \chi|_A]_A = \frac{|A|}{|G|} (m_1^2 + \dots + m_t^2),$$

továbbá $|G : A| = \chi(1) = m_1 + \dots + m_t$. Ez csak úgy lehet, ha minden $m_i = 1$, és $\chi(g) = 0$ ha $g \notin A$. Mivel $[\chi, \chi_1]_G = 0$, ahol χ_1 a főkarakter, van olyan $a \in A$, $a \neq 1$, hogy $\chi(a) \neq 0$. Mutassuk meg, hogy a G azon elemei, melyeken χ értéke nem nulla, egy olyan nemtriviális normálosztót generálnak, mely része A -nak. \square

10. Oszthatóság. A két prímek 2.8. Burnside-tétel bizonyításához, és további alkalmazásokhoz is az a gondolat vezet el, hogy elemi számelméletet alkalmazunk algebrai egészek között.

10.1. Lemma. Legyen r racionális szám, mely algebrai egész. Ekkor r racionális egész.

Bizonyítás. Legyen $r = p/q$, ahol $p, q \in \mathbf{Z}$, relatív prímek. Elemi megfontolás mutatja, hogy ha r gyöke egy egész együtthatós polinomnak, akkor q osztja annak főegyütthatóját. Ha r algebrai egész, akkor tehát $q = \pm 1$. \square

E gondolat első alkalmazása egy igen fontos oszthatóság bizonyítása.

10.2. Tétel. Legyen χ irreducibilis karaktere G -nek. Ekkor $\chi(1) \mid |G : Z(\chi)|$.

Speciálisan az irreducibilis karakterek fokai osztják a csoport rendjét. A karaktertáblák kiszámításához ez igen hasznos tulajdonság. Erősebb tétel is igaz, ezt később, indukált karakterekkel bizonyítjuk.

10.3. Itô Tétele. Az irreducibilis karakterek fokai osztják minden Abel-féle normálosztó indexét.

Mind a fenti eredményekhez, mind a Burnside-tételhez a 7.6. Lemmában bevezetett $a_{ij\nu}$ számok vizsgálata vezet el. Mostantól kezdve az ottani jelöléseket használjuk. Legyen $1 \leq m \leq k$. A \mathbf{X}_m irreducibilis reprezentáció a $\mathbf{C}[G]$ centrumát a $\mathbf{C}^{n_m \times n_m} \cong A_m$ centrumába, azaz a skalármátrixok részalgebrájába képi. Ha $z \in Z(\mathbf{C}[G])$, akkor tehát $\mathbf{X}_m(z) = \omega_m(z)E_m$, ahol $\omega_m(z) \in \mathbf{C}$, és E_m az egységmátrix. Nyilván ω_m algebra-homomorfizmus (hiszen valójában \mathbf{X}_m megszorítása).

10.4. Lemma. *Az alábbi összefüggések teljesülnek ($1 \leq i, j, m \leq k$).*

- (a) *Ha $g_j \in \mathcal{K}_j$, akkor $\omega_m(K_j) = \chi_m(g_j)|\mathcal{K}_j|/n_m$.*
- (b) *Az $\omega_m(K_j)$ szám algebrai egész.*
- (c) *$K_j e_m = \omega_m(K_j) e_m$.*
- (d) *Ha $g_\nu \in \mathcal{K}_\nu$ ($1 \leq \nu \leq k$), akkor*

$$a_{ij\nu} = \frac{|\mathcal{K}_i||\mathcal{K}_j|}{|G|} \sum_{m=1}^k \frac{\chi_m(g_i)\chi_m(g_j)\chi_m(g_\nu^{-1})}{n_m}.$$

Bizonyítás. A (c) állítás a definícióból világos, hiszen $\mathbf{X}_m(z)$ éppen a $z e_m \in A_m$ elemnek megfelelő mátrix. Az (a) következik a $\mathbf{X}_m(K_j) = \omega_m(K_j)E_m$ összefüggésből, ha mindkét oldal nyomát vesszük, hiszen a jobboldal $|\mathcal{K}_j|\chi_m(g_j)$ lesz. A (b) bizonyításához használjuk fel, hogy ω_m algebra-homomorfizmus, és ezért

$$\omega_m(K_i)\omega_m(K_j) = \sum_{\nu=1}^k a_{ij\nu}\omega_m(K_\nu).$$

Tehát az $\omega_m(K_1), \dots, \omega_m(K_k)$ számok által generált Z -modulus részgyűrűje is \mathbf{C} -nek, ezért az 1.5. Lemma miatt minden eleme algebrai egész. Végül a (d) állítás igazolásához tekintsük a

$$v_\nu = \begin{pmatrix} \omega_1(K_\nu) \\ \vdots \\ \omega_k(K_\nu) \end{pmatrix} = |\mathcal{K}_\nu| \begin{pmatrix} \chi_1(g_\nu)/n_1 \\ \vdots \\ \chi_k(g_\nu)/n_k \end{pmatrix}$$

oszlopvektorokat, ahol az m -hez tartozó komponensek n_m^2 -szer vannak felsorolva (tehát összesen $n_1^2 + \dots + n_k^2 = |G|$ komponens van). A második ortogonalitási reláció miatt a közönséges $\mathbf{C}^{|G|}$ -beli skalárszorzatra nézve a v_ν vektorok páronként merőlegesek, és v_ν skalárnégyzete $|\mathcal{K}_\nu||G|$. Ezért a

$$\sum_{\mu=1}^k a_{ij\mu} v_\mu = \begin{pmatrix} \omega_1(K_i)\omega_1(K_j) \\ \vdots \\ \omega_k(K_i)\omega_k(K_j) \end{pmatrix}$$

összefüggést skalárisan v_ν -vel szorozva éppen (d) adódik. \square

10.5. Gyakorlat. *Az előbbi lemma (a) és (c), valamint a 8.4. Lemma (c) és (d) pontjából vezessük le a második ortogonalitási relációt.*

Most belátjuk a 10.2. Tételt. Legyen $\chi = \chi_m$ irreducibilis karaktere G -nek. A 9.3. Lemma miatt χ a $G/\text{Ker}(\chi)$ faktoron irreducibilis karaktert indukál, melynek foka ugyanaz, mint χ foka, centruma tehát éppen $Z(\chi)/\text{Ker}(\chi)$. Ezért az állítást elég $G/\text{Ker}(\chi)$ -re bizonyítani, vagyis feltehető, hogy $\text{Ker}(\chi) = \{1\}$, amikor is 9.10.b miatt $Z(\chi) = Z(G)$.

Jelölje $\omega = \omega_m$ az imént definiált, χ -hez tartozó függvényt, és legyen $n = \chi(1)$ a χ foka. Az első ortogonalitási reláció miatt, az előző tétel jelöléseivel

$$|G| = \sum_{g \in G} \chi(g)\chi(g^{-1}) = n \left(\sum_{\nu=1}^k \omega(K_\nu)\chi(g_\nu^{-1}) \right).$$

A zárójelben álló összeg algebrai egész az előző lemma miatt, és ezért $|G|/n$ algebrai egész is, racionális is, azaz n osztója G rendjének.

Azt akarjuk belátni, hogy n osztja $Z(G)$ indexét. Ehhez a zárójelbeli kifejezésről kell megmutatni, hogy $|Z(G)|$ -vel osztható. Meg fogjuk mutatni, hogy ennek az összegnek a nem nulla tagjai $|Z(G)|$ nagyságú csoportokba oszthatók úgy, hogy az egyes csoportokon belül az összeadandók ugyanazok.

Legyen $K = K_\nu$, $\mathcal{K} = \mathcal{K}_\nu$ és $z, z' \in Z(G)$. Ha $\omega(K) = 0$, akkor ezzel a taggal nem kell foglalkozni. Vegyük észre, hogy $a, b \in G$ pontosan akkor konjugáltak, ha az és bz azok, vagyis $\mathcal{K}z$ ismét egy konjugált osztály, azaz valamelyik \mathcal{K}_i . Mivel a K és z elemek a csoportalgebra centrumában vannak, $\omega(Kz) = \omega(K)\omega(z)$. Ha tehát $Kz = Kz'$, akkor $\omega(z) = \omega(z')$, vagyis $\omega(z^{-1}z') = 1$. Az ω definíciója miatt $n\omega(z^{-1}z') = \chi(z^{-1}z')$. Mivel $\text{Ker}(\chi) = \{1\}$, azt kapjuk, hogy $z = z'$. Azaz beláttuk, hogy a Kz elemek páronként különböznek. A bizonyítás befejezéséhez elegendő tehát azt megmutatni, hogy a zárójelben álló összeg K -hoz és Kz -hez tartozó tagja megegyezik. A \mathcal{K} osztályból a g , a $\mathcal{K}z$ -ből a gz reprezentánst választva

$$\omega(Kz)\chi((gz)^{-1}) = \frac{|\mathcal{K}z|\chi(gz)}{n}\chi((gz)^{-1}) = \frac{|\mathcal{K}z|}{n}|\chi(gz)|^2.$$

Ez valóban független z -től, ha ugyanis \mathbf{X} a χ -hez tartozó reprezentáció, akkor $z \in Z(\chi)$ miatt $\mathbf{X}(gz) = \mathbf{X}(g)\mathbf{X}(z)$, és mivel $\mathbf{X}(z) = \omega(z)E$ skalármátrix, $|\chi(gz)| = |\chi(g)||\omega(z)|$, tehát $|\omega(z)| = 1$ miatt készen vagyunk.

Most Burnside tételének bizonyítására térünk. Az alábbi lemmát, melyet felhasználunk majd, a Galois-elmélet keretében fogjuk bizonyítani. Legyen ε egy primitív m -edik egységgyök. Ez algebrai \mathbf{Q} felett, és így az 1.4. Lemma miatt a $\mathbf{Q}[\varepsilon]$ gyűrűbővítés test. Ezért szokásosabb a $\mathbf{Q}(\varepsilon)$ jelölést alkalmazni erre a testre.

10.5. Lemma. *Ha $1 \leq i < m$ relatív prím m -hez, akkor a $\mathbf{Q}(\varepsilon)$ testnek pontosan egy olyan α_i automorfizmusa van, melynél \mathbf{Q} elemei fixen maradnak, és $\alpha_i(\varepsilon) = \varepsilon^i$. Ha egy számot az α_i automorfizmusok mindegyike fixen hagy, akkor az racionális.*

10.6. Lemma. *Legyen G egy csoport, $g \in G$ rendje m , \mathbf{X} egy n -edfokú reprezentáció, és χ ennek karaktere. Legyen*

$$r = \prod_{\substack{(i,m)=1 \\ 1 \leq i < m}} \chi(g^i).$$

- (a) *Az r szám racionális egész.*
- (b) *Ha $(i, m) = 1$, akkor $\chi(g^i)$ pontosan akkor nulla, ha $\chi(g) = 0$.*
- (c) *Ha $\chi(g)/n$ algebrai egész, akkor $\chi(g) = 0$ vagy $g \in Z(\chi)$.*

Bizonyítás. A 8.3. Lemma miatt $\chi(g) = \varepsilon_1 + \dots + \varepsilon_n$, ahol az $\varepsilon_1, \dots, \varepsilon_n$ m -edik egységgyökök éppen $\mathbf{X}(g)$ sajátértékei. Ekkor $\mathbf{X}(g^i)$ sajátértékei $\varepsilon_1^i, \dots, \varepsilon_n^i$, azaz $\chi(g^i) = \varepsilon_1^i + \dots + \varepsilon_n^i$. Ha $(i, m) = 1$, akkor az előző lemmában szereplő α_i automorfizmus az ε hatványait, azaz mindegyik ε_j egységgyököt is az i -edik hatványába viszi. Ezért $\alpha_i(\chi(g)) = \chi(g^i)$.

Ez a (b) állítást rögtön bizonyítja is. Az r szorzat tényezőit mindegyik α_i permutálja, és ezért r fixen marad, azaz az előző lemma miatt r tényleg racionális. Végül tegyük fel, hogy $\chi(g)/n$ algebrai egész. Ekkor az α_i -nél vett képe is az, azaz ezek szorzata, $r/n^{\varphi(m)}$ racionális egész. Ha nulla, akkor (b) miatt készen vagyunk. Ha nem, akkor abszolút értéke legalább 1. Viszont mindegyik tényező abszolút értéke 8.3.g miatt legfeljebb 1, és egyenlőség csak úgy állhat, ha mindegyik $g^i \in Z(\chi)$. \square

10.7. Burnside–lemma. *Legyen χ irreducibilis karaktere és \mathcal{K} konjugált osztálya G -nek. Tegyük fel, hogy $|\mathcal{K}|$ relatív prím χ fokához. Ekkor vagy $\mathcal{K} \subseteq Z(\chi)$, vagy χ értéke nulla a \mathcal{K} elemein.*

Bizonyítás. Legyen $\chi(1) = n$ és $u, v \in \mathbf{Z}$, melyre $un + v|\mathcal{K}| = 1$. A 10.4. Lemma miatt ha $g \in \mathcal{K}$, akkor $\chi(g)|\mathcal{K}|/n$ algebrai egész. Ezért $\chi(g)/n = u\chi(g) + v\chi(g)|\mathcal{K}|/n$ is az. Az előző lemmát alkalmazva éppen az állítást kapjuk. \square

10.8. Tétel. *Legyen G véges, nemkommutatív, egyszerű csoport. Ekkor G -ben nem lehet prímhatvány rendű konjugált osztály az $\{1\}$ kivételével.*

Bizonyítás. A feltétel szerint $G = G'$, és így G egyetlen lineáris karaktere a χ_1 főkarakter. Ha χ_i ettől különböző, akkor $\text{Ker}(\chi_i) = Z(\chi_i) = \{1\}$ (hiszen $Z(\chi_i)/\text{Ker}(\chi_i)$ 9.10.d miatt ciklikus). Legyen a $g \neq 1$ elem konjugált osztálya p -hatványrendű. Ekkor a reguláris karaktert felhasználva

$$0 = \rho(g) = 1 + \sum_{i=2}^k n_i \chi_i(g).$$

Az előző lemma miatt ha p nem osztja n_i -t, akkor $\chi_i(g) = 0$, vagy $g \in Z(\chi)$. Ez utóbbit kizártuk. Ebben az összegben tehát, mivel $\chi_i(g)$ algebrai egész, minden tag osztható p -vel az 1-et kivéve. Ez az ellentmondás bizonyítja a tételt. \square

A 2.8. Burnside tétel bizonyításához legyen $|G| = p^a q^b$. Ha z eleme egy p -Sylow centrumának akkor z centralizátorának indexe q -hatvány, tehát az előző tétel miatt kész vagyunk. Megjegyezzük, hogy indukcióval az is világos, hogy G feloldható. \square

10.9. Feladat. *Bizonyítsuk be, hogy minden nemlineáris, irreducibilis karakter felveszi a 0 értéket.*

Ötlet. Nevezzünk ekvivalensnek két G -beli elemet, ha egymás hatványai. Az első ortogonalitási relációból származó $|G| = \sum_g |\chi(g)|^2$ egyenlőséget bontsuk fel e reláció szerint. Használjuk fel, hogy a 10.6.a-ban szereplő r szám abszolút értéke legalább 1, és alkalmazzuk a számtani és a mértani közép közötti egyenlőtlenséget. \square

10.10. Feladat. *Legyen G egyszerű csoport, melynek rendjét osztja egy p prím négyzete. Igazoljuk, hogy G -nek nem lehet p fokú irreducibilis karaktere.*

Ötlet. Tegyük fel, hogy χ ilyen, és tekintsük χ megszorítását a G egy P p -Sylowjára. A 10.2. Tétel miatt P nemlineáris karakterei legalább p fokúak, ezért $\chi|_P$ vagy lineáris karakterek összege, vagy egyetlen p fokú komponense van, azaz irreducibilis. Ez utóbbi esetben

$Z(P) \subseteq Z(\chi|_P) \subseteq Z(\chi) \triangleleft G$, ami lehetetlen. Ha viszont $\chi|_P$ lineáris karakterek összege, akkor $P' \subseteq \text{Ker}(\chi)$, azaz P Abel. Mivel $Z(\chi)$ is triviális, a 10.7 miatt P minden egységtől különböző elemén χ nulla. Tekintsük χ és P főkarakterének skaláris szorzatát. \square

10.11. Feladat. Legyen A prímszámhatványindexű, kommutatív részcsoport G -ben. Igazoljuk, hogy G nem lehet nemkommutatív egyszerű csoport.

Ötlet. Alkalmazzuk 10.8-at. Megjegyezzük, hogy ez az állítás karakterek nélkül is könnyen igazolható az eddig tanultak segítségével. \square

10.12. Feladat. Igazoljuk, hogy a $g \in G$ elem pontosan akkor kommutátor, ha

$$\sum_{i=1}^k \frac{\chi_i(g)}{n_i} \neq 0.$$

Ötlet. Alkalmazzuk a 8.5. általánosított ortogonalitási relációt, majd a kapott $k|G|$ tagú összeget alakítsuk át a második ortogonalitási reláció szerint. \square

10.13. Feladat. Tegyük fel, hogy $g \in G$ kommutátor, és legyen $(i, |g|) = 1$. Igazoljuk, hogy g^i is kommutátor.

Ötlet. Használjuk fel az előző feladatot, és a 10.6 bizonyításának technikáját. \square

10.14. Feladat (Burnside). Igazoljuk, hogy páratlan rendű csoport egyetlen valós, irreducibilis karaktere a χ_1 főkarakter.

Ötlet. Ha χ valós, és χ_1 -re ortogonális, akkor $\chi(1)$ egy algebrai egész kétszerese. \square

11. Indukált karakterek. Láttuk, hogy egy G csoport reprezentációi igen egyszerűen meghatározzák G faktorcsoportjainak reprezentációit. Ebben a fejezetben azt vizsgáljuk, mi a kapcsolat a G csoport, és a G részcsoportjainak karakterei között. Legyen H részcsoport G -ben, és V egy (véges dimenziós) $\mathbf{C}[G]$ -modulus. Ekkor persze V modulus lesz $\mathbf{C}[H]$ felett is, hiszen ez részgyűrűje $\mathbf{C}[G]$ -nek, az ehhez a modulushoz tartozó karakter pedig könnyen láthatóan éppen a G csoport V -hez tartozó karakterének H -ra vett megszorítása. A $\mathbf{C}[H]V$ részmodulusait egyszerűen H -részmodulusoknak fogjuk nevezni. Ekkor V előáll, mint irreducibilis H -részmodulusok direkt összege. Elsőként azt az esetet vesszük szemügyre, amikor $H \triangleleft G$. A következő lemma elemi számolással igazolható.

11.1. Lemma. Legyen $N \triangleleft G$, és W, W' két N -részmodulusa V -nek.

- (a) Ha $g \in G$, akkor gW is N -részmodulusa V -nek. A W akkor és csak akkor irreducibilis $\mathbf{C}[N]$ felett, ha gW az.
- (b) Ha W és W' izomorf $\mathbf{C}[N]$ -modulusok, akkor gW és gW' is izomorfak.
- (c) Ha θ jelöli az N csoport W -hez tartozó karakterét, akkor a gW -hez tartozó karakter az a θ^g függvény, melyre $h \in N$ esetén $\theta^g(h) = \theta(h^g)$. \square

A θ^g karaktert a θ karakter g -vel vett konjugáltjának nevezzük. Könnyen megadható az a konjugált reprezentáció is, amihez θ^g tartozik, és ebből látjuk, hogy θ^g akkor is karakter,

ha a V nincs megadva. Legyen $T = \{g \in G \mid \theta^g = \theta\}$. A T részcsoportot a θ G -beli inerciacsoportjának nevezzük.

Tegyük most fel, hogy V , mint $\mathbf{C}[G]$ -modulus, irreducibilis. Megpróbáljuk megérteni, hogyan bomlik fel V irreducibilis N -részmodulusainak direkt összegére. Ha W irreducibilis N -részmodulusa V -nek, akkor az összes gW is az ($g \in G$), ezek összege pedig G -részmodulus is, azaz maga V . A 6.3. Tétel szerint tehát V előáll, mint néhány gW direkt összege. Vonjuk össze ennek a direkt összegnek azokat a tagjait, amelyek izomorfak mint $\mathbf{C}[N]$ -modulusok, a kapott komponenseket jelölje U_1, \dots, U_t . Ekkor persze $V = U_1 \oplus \dots \oplus U_t$. A kapott felbontásnak van egy igen fontos tulajdonsága, melyet egy definícióban foglalunk össze.

11.2. Definíció. Tegyük fel, hogy a (nem feltétlenül irreducibilis) $\mathbf{C}[G]V$ modulus előáll, mint az U_1, \dots, U_t altereinek direkt összege. Azt mondjuk, hogy ez V -nek egy *imprimitivitási felbontása*, ha G tranzitíven hat az $\{U_1, \dots, U_t\}$ halmazon, azaz bármely $g \in G$ és i esetén $gU_i = U_j$ alkalmas j -re, és bármely i, j -hez van olyan $g \in G$, hogy $gU_i = U_j$.

11.3. Lemma. Legyen $\mathbf{C}[G]V$ irreducibilis modulus.

- (a) Az imént definiált $V = U_1 \oplus \dots \oplus U_t$ a V imprimitivitási felbontása.
- (b) Minden irreducibilis N -részmodulus része valamelyik U_i -nek.
- (c) Legyen $T = \{g \in G \mid gU_1 = U_1\}$ az U_1 stabilizátora G -ben. Ha $W_0 \subseteq U_1$ irreducibilis N -részmodulus, és θ a W_0 karaktere, akkor T éppen a θ G -beli inerciacsoportja.
- (d) Az U_1 , mint $\mathbf{C}[T]$ -modulus, irreducibilis.

Bizonyítás. Legyen W' irreducibilis N -részmodulusa V -nek. A 6.3. Tétel (c) pontja miatt W' izomorf a V direkt összeg felbontásában szereplő gW modulusok valamelyikével, amely tehát direkt összeadandója valamelyik U_i -nek. A V/U_i faktor direkt felbontásában már nem szerepel gW -vel izomorf modulus (pont azok direkt összegével faktorizáltunk ki). De W' irreducibilis, ezért képe ennél a faktorizálásnál vagy nulla, vagy izomorf W' -vel. Utóbbi lehetetlen 6.3.c miatt. Ezért $W' \subseteq U_i$, amivel (b)-t igazoltuk.

Most legyen $g \in G$ és $U_i = W_1 \oplus \dots \oplus W_e$, ahol ezek a tényezők irreducibilis, izomorf N -részmodulusok. Ekkor a gW_i is izomorf modulusok, ezért részei ugyanannak az U_j -nek. Azaz $gU_i \subseteq U_j$. Ugyanezzel a gondolatmenettel adódik, hogy $g^{-1}U_j \subseteq U_i$, azaz mindkét tartalmazásnál egyenlőség áll. Végül ha U_i és U_j adott, $g_1W \subseteq U_i$, és $g_2W \subseteq U_j$, akkor a $g = g_2g_1^{-1}$ elemre $g(g_1W) = g_2W$, és ezért $gU_i = U_j$. Így (a) igaz.

A (c) bizonyításához vegyük észre, hogy ha $W_0 \subseteq U_1$ irreducibilis N -részmodulus, akkor gW_0 pontosan azokra a $g \in G$ elemekre lesz része U_1 -nek, melyekre a W_0 és gW_0 $\mathbf{C}[N]$ -modulusok izomorfak, azaz karakterük megegyezik.

Végül igazoljuk (d)-t. A G azon g elemei, melyekre $gU_1 = U_1$, egy baloldali mellékosztályt alkotnak T szerint. Válasszuk az y_1, \dots, y_t elemeket úgy, hogy $y_iU_1 = U_i$ legyen. Ekkor tehát y_1, \dots, y_t baloldali reprezentánsrendszer T szerint. Ha U egy T -részmodulusa U_1 -nek, akkor a gU alterek $g \in G$ -re vett V' összege már G -részmodulus, ezért V irreducibilitása miatt maga V . Másrészt ha $g = y_it$ ($t \in T$), akkor $gU = y_iU$, ezért $V' = y_1U \oplus \dots \oplus y_tU$. Így $V = V'$ miatt $U = U_1$, amint állítottuk. \square

Látjuk tehát, hogy imprimitivitási felbontások igen természetesen adódnak. A következő összefüggés vezet el az indukált karakter fogalmához.

11.4. Lemma. Legyen $V = U_1, \dots, U_t$ a (nem feltétlenül irreducibilis) $\mathbf{C}[G]V$ modulus egy imprimitivitási felbontása, és T az U_1 stabilizátora. Ha χ a $\mathbf{C}[G]V$ -hez, ψ a $\mathbf{C}[T]U_1$ -hez tartozó karakter, akkor

$$\chi(g) = \frac{1}{|T|} \sum_{\substack{y \in G \\ g^y \in T}} \psi(g^y).$$

Bizonyítás. Legyen y_1, \dots, y_t bal reprezentánsrendszer T szerint, melyre $y_i U_1 = U_i$, és válasszunk egy u_1, \dots, u_n bázist U_1 -ben. Ekkor az nt darab $y_i u_j$ elem bázist alkot V -ben. A g -vel való balszorítás mátrixának főátlójában lévő elemeket kell megkapni, ezek a $gy_i u_j$ elemek $y_i u_j$ -koordinátái. Ha ez nem nulla, akkor $gy_i U_1 = y_i U_1$, azaz $g^{y_i} \in T$. Egyszerű számolás mutatja, hogy ekkor az $y_i u_j$ ($1 \leq j \leq n$) bázisvektorok hozzájárulása $\chi(g)$ -hez éppen $\psi(g^{y_i})$. Mivel $\psi(g^{y_i}) = \psi(g^{y_i t})$ ha $t \in T$, éppen az állítást kapjuk. \square

11.5. Definíció. Legyen H tetszőleges részcsoportja a G csoportnak, és ψ osztályfüggvény H -n. Ekkor a ψ által indukált G -beli osztályfüggvényen a

$$\psi^G(g) = \frac{1}{|H|} \sum_{\substack{y \in G \\ g^y \in H}} \psi(g^y).$$

függvényt értjük.

Azonnal látszik, hogy ψ^G tényleg osztályfüggvény, és $\psi^G(1) = |G : H| \psi(1)$. Vonjuk most le a karakterekre vonatkozó következményeket.

11.6. Clifford tétele. Legyen $N \triangleleft G$, és χ irreducibilis karaktere G -nek.

- $\chi|_N = e\theta_1 + \dots + e\theta_t$, ahol $\theta_1, \dots, \theta_t$ éppen a θ_1 irreducibilis N -karakter összes G -beli konjugáltja, és e alkalmas pozitív egész.
- Legyen T a θ_1 G -beli inerciacsoportja. Ekkor $N \subseteq T$ és $t = |G : T|$.
- Mind t , mind e osztja $|G : N|$ -et.
- Van olyan ψ irreducibilis karaktere T -nek, melyre $\psi|_N = e\theta_1$ és $\psi^G = \chi$.

Bizonyítás. Azt, hogy $e \mid |G : N|$, nem bizonyítjuk. A többi állítás közvetlenül adódik az eddigiekből. \square

Első alkalmazásként belátjuk a 10.3. Itô-tételt. Legyen N Abel normáloszó G -ben, és χ irreducibilis karaktere G -nek. Clifford tételéből azt kapjuk, hogy $\chi|_N = e\theta_1 + \dots + e\theta_t$, ahol most θ_i lineáris karakterek, hiszen N Abel. Tekintsük a (d)-ben szereplő ψ karaktert. Ekkor $\psi|_N = e\theta_1$ miatt $N \subseteq Z(\psi)$, vagyis a 10.2. tétel miatt $\psi(1) \mid |T : Z(\psi)| \mid |T : N|$. De $\psi(1) = e$, és $\chi(1) = et$, vagyis $\chi(1) \mid t|T : N| = |G : N|$. \square

Következő célunk annak megmutatása, hogy karakter indukáltja is karakter. Ehhez elvezet az alábbi feladat megoldása is, mi azonban másik utat követünk majd.

11.7. Feladat. Legyen T részcsoportja G -nek, és U egy $\mathbf{C}[T]$ -modulus. Ekkor létezik olyan V $\mathbf{C}[G]$ -modulus, és ennek olyan $V = U_1 \oplus \dots \oplus U_t$ imprimitivitási felbontása, melyre U és U_1 izomorf $\mathbf{C}[T]$ -modulusok, és T éppen az U_1 stabilizátora.

Ötlet. Legyenek U_i ($1 \leq i \leq t = |G : T|$) izomorf példányai U -nak, ahol az $u \in U$ elemnek az $u_i \in U_i$ felel meg. Vegyünk egy y_1, \dots, y_t bal reprezentánsrendszert T szerint, melyre

$y_1 = 1 \in T$. Legyen V az U_i vektorterek direkt összege. Ahhoz, hogy ezt modulussá tegyük $\mathbf{C}[G]$ felett, a linearitás miatt elegendő megadni a gu_i szorzatokat. A transzfer definíciójában használt jelöléssel legyen $gu_i = (h_i(g)u)_{\sigma(i,g)}$. \square

11.8. Frobenius–reciprocitás. Legyen H részcsoportha G -nek, ψ osztályfüggvény H -n, és θ osztályfüggvény G -n. Ekkor

$$[\psi, \theta|_H]_H = [\psi^G, \theta]_G.$$

Bizonyítás. Ha $t \in H$ adott, akkor azon $(y, g) \in G^2$ párok száma, melyekre $g^y = t$, éppen $|G|$, hiszen minden y -hoz pontosan egy g lesz jó. Mivel θ osztályfüggvény G -n,

$$[\psi^G, \theta]_G = \frac{1}{|G||H|} \sum_{\substack{y, g \in G \\ g^y \in H}} \psi(g^y) \overline{\theta(g)} = \frac{1}{|G||H|} \sum_{t \in H} |G| \psi(t) \overline{\theta(t)} = [\psi, \theta|_H]_H. \quad \square$$

11.9. Következmény. Ha ψ karaktere H -nak, akkor ψ^G karaktere G -nek.

Bizonyítás. A 8.7. Következmény miatt elég azt megmutatni, hogy a ψ^G a G bármely χ irreducibilis karakterével skalárisan szorozva nemnegatív egész ad. De ez következik a Frobenius–reciprocitásból, hiszen $\chi|_H$ karaktere H -nak. \square

Most a 2.13. Frobenius–tétel bizonyítására térünk. Ha G Frobenius–csoport, és H ennek komplementuma, akkor H diszjunkt a konjugáltjaitól. Ezt a situációt általánosítja a következő definíció.

11.10. Definíció. Legyen X részhalmaza G -nek. Azt mondjuk, hogy X TI-részhalmaz (Trivial Intersection set), ha minden $g \in G$ esetén vagy $X^g = X$, vagy $X \cap X^g \subseteq \{1\}$.

11.11. Lemma. Legyen X TI-részhalmaza G -nek, $N = N_G(X)$, és θ, ϕ olyan osztályfüggvények N -en, melyek eltűnnek $N \setminus X$ -en. Ha $\theta(1) = 0$, akkor $\theta^G|_X = \theta|_X$ és $[\theta^G, \phi^G]_G = [\theta, \phi]_N$.

Bizonyítás. Ha $\theta(g^y) \neq 0$, akkor $1 \neq g^y \in X \cap X^y$, azaz $y \in N$. De θ osztályfüggvény N -en, ezért $\theta(g^y) = \theta(g)$, amiből az első állítás világos. A reciprocitás miatt $[\theta^G, \phi^G]_G = [\theta^G|_N, \phi]$. Mivel ϕ eltűnik $N \setminus X$ -en, $\theta^G|_N$ helyére a már bizonyított állítás miatt θ írható. \square

Lássuk tehát a Frobenius–tétel bizonyítását. Legyen G Frobenius–csoport, N a magja, és H a komplementuma. Ha már tudnánk, hogy N normálosztó, akkor $H \cong G/N$ irreducibilis karakterei kölcsönösen egyértelmű megfeleltetésben állnának a G azon irreducibilis karaktereivel, melyek magja N -et tartalmazza. Azaz minden ψ irreducibilis H -karakterhez létezne olyan ψ^* irreducibilis G -karakter, melynek H -ra vett megszorítása ψ , és melynek magja N -et tartalmazza. Tervünk az, hogy a ψ^* karaktereket megkonstruáljuk annak feltételezése nélkül, hogy N normálosztó, és N -et megkapjuk, mint ezek magjainak a metszetét.

Ha $\psi = 1_H$ a H főkarakter, akkor $\psi^* = 1_G$. Különben, ha $\psi \neq 1_H$ irreducibilis karaktere H -nak, akkor legyen $\theta = \psi - \psi(1)1_H$. A reciprocitás miatt $[\theta^G, 1_G] = [\theta, 1_H] = -\psi(1)$.

Mivel θ két karakter különbsége, és az indukálás lineáris, θ^G felírható G irreducibilis karaktereinek egész együtthatós lineáris kombinációjaként. Azt már láttuk, hogy 1_G együtthatója $-\psi(1)$. Másrészt H TI-halmaz, ahol $N_G(H) = H$, így θ teljesíti az előző lemma feltételeit, és ezért $[\theta^G, \theta^G] = [\theta, \theta] = 1 + \psi(1)^2$. Azaz θ felbontásában egyetlen további irreducibilis tényező szerepelhet, melynek együtthatója ± 1 , jelölje ezt $\pm\psi^*$, azaz legyen $\theta^G = \pm\psi^* - \psi(1)1_G$. Az előző lemma miatt $h \in H$ esetén $\theta^G(h) = \theta(h)$, vagyis $\pm\psi^*(h) = \psi(h)$. Ezért $h = 1$ -et helyettesítve látjuk, hogy a helyes előjel $+$, és $\psi^*|_H = \psi$. Ha $1 \neq g \in N$, akkor g nem konjugált H -beli elemmel, ezért $\theta^G(g) = 0$, azaz $\psi^*(g) = \psi(1) = \psi^*(1)$. A ψ^* tehát tényleg olyan, amilyennek akartuk.

Legyen most $\chi = \sum \psi(1)\psi^*$, ahol ψ befutja H irreducibilis karaktereit. Ekkor $\chi|_H$ éppen a H reguláris karaktere, azaz χ értéke nulla a H^g részcsoportok egységtől különböző elemein. Másrészt az eddigiek miatt $g \in N$ esetén $\chi(g) = \chi(1)$, azaz $\text{Ker}(\chi) = N$. Ezzel Frobenius tételét bebizonyítottuk. \square

11.12. Tétel (Thompson). *Minden Frobenius-csoport magja nilpotens (azaz Sylowjainak direkt szorzata).*

A tételt nem bizonyítjuk. Ez az állítás, ami Thompson első híres eredményeinek egyike volt, azt mutatja, hogy a Frobenius-csoportok magja egyáltalán nem lehet tetszőleges. A bizonyítás kiindulópontja az, hogy a magnak van prímrendű, fixpontmentes automorfizmusa (a komplementum egy prímrendű elemével való konjugálás).

11.13. Feladat. *Legyen G Frobenius-csoport, melynek komplementuma páros rendű. Mutassuk meg, hogy G magja Abel.*

Ötlet. Legyen α másodrendű, és (az egységelemtől eltekintve) fixpontmentes automorfizmusa az N csoportnak. Ekkor az $\alpha(g)g^{-1}$ elemek páronként különbözők, és így N végesége miatt kiadják N -et. Másrészt $\alpha(\alpha(g)g^{-1}) = (\alpha(g)g^{-1})^{-1}$, azaz α minden elemet az inverzébe visz. \square

Az alábbi állítás igen hasznos, ha egy konkrét karaktert akarunk indukálni.

11.14. Gyakorlat. *Legyen H részcsoport G -ben, és ψ osztályfüggvény H -n. Tekintsük a $g \in G$ elem G -beli konjugált osztályának és H -nak metszetét. Ez felbomlik H konjugált osztályainak egyesítésére, válasszunk ki mindegyikből egy-egy y_i elemet ($1 \leq i \leq m$). Ekkor*

$$\psi^G(g) = |C_G(g)| \sum_{i=1}^m \frac{\psi(y_i)}{|C_H(y_i)|}. \quad \square$$

11.15. Gyakorlat. *Legyen H a forgatások részcsoportja D_4 -ben. Indukáljuk D_4 -re a H lineáris karaktereit, és állítsuk ezeket elő D_4 irreducibilis karaktereivel. \square*

11.16. Feladat. *Legyen G permutációcsoport az Ω halmazon. Igazoljuk az alábbiakat.*

- (a) *Az a χ leképezés, amely minden $g \in G$ elemhez a fixpontjainak számát rendeli, karaktere G -nek.*
- (b) *A G orbitjainak száma $[\chi, 1_G]$.*
- (c) *Ha G tranzitív, és H egy elem stabilizátora, akkor $\chi = (1_H)^G$.*
- (d) *A H orbitjainak száma $[\chi, \chi]$.*

- (e) G akkor és csak akkor kettő-tranzitív, ha $\chi = 1_G + \psi$, ahol $\psi \neq 1_G$ irreducibilis karaktere G -nek.

A χ karaktert permutációs karakternek nevezzük. A G csoport akkor k -tranzitív, ha Ω tetszőleges a_1, \dots, a_k és b_1, \dots, b_k elemeihez van olyan $g \in G$, hogy g az a_i -t b_i -be viszi ($1 \leq i \leq k$).

Ötlet. Tekintsünk egy $|\Omega|$ dimenziós vektorteret. Ennek bázisvektorait permutálja G úgy, ahogy az Ω elemeit. A kapott reprezentáció karaktere χ . Ha G tranzitív, akkor a bázisvektorok generálta egydimenziós alterek imprimitivitási felbontást adnak. A reciprocitás miatt $[(1_H)^G, 1_G] = [1_H, 1_H] = 1$. A (b) belátásához alkalmazzuk ezt orbitonként. \square

11.17. Feladat. Számítsuk ki az A_5 alternáló csoport karaktertábláját. Az eredmény a következő ($\varepsilon = e^{2\pi i/5}$).

A_5	1	(12)(34)	(123)	(12345)	$(12345)^2$
60	1	15	20	12	12
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\varepsilon + \varepsilon^4 + 1$	$\varepsilon^2 + \varepsilon^3 + 1$
χ_3	3	-1	0	$\varepsilon^2 + \varepsilon^3 + 1$	$\varepsilon + \varepsilon^4 + 1$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

Megjegyezzük, hogy $\varepsilon + \varepsilon^4 + 1 = (1 + \sqrt{5})/2$ és $\varepsilon^2 + \varepsilon^3 + 1 = (1 - \sqrt{5})/2$.

Ötlet. A χ_4 a szokásos permutációs karakter mínusz a főkarakter. A χ_5 az A_4 részcsoporthoz tetszőleges nem fő, lineáris karakterének indukáltja (lásd a 9.12. Feladatot). A másik két karakter úgy kapható, hogy az 5-Sylow nem fő, lineáris karaktereit indukáljuk, és levonjuk $\chi_4 + \chi_5$ -öt. \square

11.18. Feladat. Igazoljuk, hogy a karaktertábla sorainak összege nemnegatív egész szám.

Ötlet. Hasson G a saját alaphalmazán a konjugálással, és legyen χ a megfelelő permutációs karakter. Ekkor $[\chi_i, \chi]$ nemnegatív egész. Megjegyezzük, hogy a karaktertábla oszlopösszegei is egészek, de lehetnek negatívak is. \square

11.19. Feladat. Legyen H részcsoporthoz G -ben, és ψ karaktere H -nak. Igazoljuk, hogy $\text{Ker}(\psi^G)$ épp a $\text{Ker}(\psi)^y$ részcsoporthoz metszete, ha y befutja G -t. \square

11.20. Feladat. Legyen $N \triangleleft G$ és θ irreducibilis karaktere N -nek. Igazoljuk, hogy θ^G akkor és csak akkor irreducibilis, ha a θ inerciacsoporthoz G -ben maga N .

Ötlet. A reciprocitás miatt $1 \leq [\theta^G, \theta^G] = [\theta, \theta^G|_N]$. Ezért θ szerepel $\theta^G|_N$ -ben. A θ^G akkor és csak akkor irreducibilis, ha ez a skaláris szorzat 1, azaz $\theta^G|_N$ -et a Clifford-tétel szerint felbontva a kapott e szám értéke 1. A fokokat felírva $|G : H|\theta(1) = e t \theta(1)$, ahol t az inerciacsoporthoz indexe. \square

11.21. Feladat. *Mutassuk meg, hogy G -ben akkor és csak akkor van Abel-féle normál p -komplementum, ha G minden irreducibilis karakterének foka p -hatvány.*

Ötlet. A $\sum n_i^2 = |G|$ összefüggés miatt a lineáris karakterek száma, azaz $|G : G'|$ egy egynél nagyobb p -hatvány. Megmutatjuk, hogy G' -re öröklődik a feltétel. Legyen θ irreducibilis karaktere G' -nek, és χ egy irreducibilis komponense θ^G -nek. Ekkor a reciprocitás miatt θ szerepel $\chi|_{G'}$ -ben, és ezért a Clifford-tétel szerint felírva χ -t látjuk, hogy $\chi(1) = e\theta(1)$. Így indukcióval készen vagyunk. A másik irány a 10.3. Itô-tételből következik. \square

11.22. Feladat. *Tegyük fel, hogy a G csoportnak pontosan egy darab nemlineáris karaktere van. Igazoljuk, hogy G' elemi Abel-féle p -csoport (azaz \mathbf{Z}_p direkt hatványa).*

Bizonyítás. Elég megmutatni, hogy G' bármely két, egységtől különböző eleme konjugált. Két bizonyítást is adunk. Az első: G minden konjugált osztálya része egy G' szerinti mellékosztálynak, másrészt számuk éppen e mellékosztályok száma plusz 1. A második: Legyen χ az egyetlen nemlineáris karakter, ennek foka n . A reguláris karaktert felírva irreducibilisek összegeként azt kapjuk, hogy $n\chi(g) + |G : G'| = 0$, ha $1 \neq g \in G'$. Azaz G összes irreducibilis karaktere konstans $G' \setminus \{1\}$ -en. \square

Megjegyezzük, hogy S_3, D_4, Q eleget tesz az előző feladat feltételeinek. Könnyű számo-lással adódik, hogy G' összes nem fő irreducibilis karaktere is konjugált, továbbá alkalmas a pozitív egészre $n = a(|G'| - 1)$, $|G : G'| = a^2(|G'| - 1)$. A feladatbeli tulajdonságú csoportból végtelen sok van, de ezek teljesen leírhatók.

12. Involúció–centralizátorok. Ha G véges, nem kommutatív, egyszerű csoport, akkor a Feit–Thompson tétel miatt rendje páros. Így kézenfekvőnek látszik ezeket 2–Sylow rész-csoportjuk izomorfia-típusa szerint csoportosítani. Sajnos azonban ez még nem elég finom osztályozás, mert például végtelen sok olyan egyszerű csoport van, melynek 2–Sylowja a Klein–csoport. Az ötlet, ami segít, a következő. Minden páros rendű csoport tartalmaz egy b involúciót (azaz másodrendű elemet). Látni fogjuk, hogy a $C_G(b)$ centralizátornak, mint absztrakt csoportnak az ismerete már hozzásegít G meghatározásához. A véges egyszerű csoportok klasszifikációjához alapvető volt ez a technika. Az első ilyen irányú eredmény bizonyítása nem használ karaktereket.

12.1. Tétel. *Legyen G véges egyszerű csoport, melyben egy involúció centralizátora a Klein–csoport. Ekkor $G \cong A_5$.*

Bizonyítás. Első célunk annak igazolása, hogy G 2–Sylowja maga is a Klein–csoport, továbbá, hogy az összes involúció konjugált G -ben. A következő észrevétel Thompsontól származik.

12.2. Lemma. *Legyen M kettő indexű részcsoporthoz egy G csoport 2–Sylowjában. Ekkor G' minden involúciója M -be konjugálható.*

Bizonyítás. Legyen $n = |G : M|$, és jelölje $\phi : G \rightarrow S_n$ a G hatását az M baloldali mellékosztályain (mint a 2.5. Lemma bizonyításában). Tekintsük az x involúcióhoz tartozó $\phi(x)$ permutációt. Ha ennek van egy gM fixpontja, akkor $g^{-1}xg \in M$, tehát készen vagyunk. Ha nincs, akkor $\phi(x)$ éppen $n/2$ darab, azaz páratlan sok transzpozíció szorzata. Ezért

az A_n ϕ -nél vett teljes inverz képe egy kettő indexű normálosztó G -ben, mely x -et nem tartalmazza (de G' -t igen). \square

12.3. Lemma. *Legyenek x és y involúciók G -ben, és $g = xy$ rendje n . Ekkor az x és y által generált részcsoport izomorf a D_n diédercsoporttal.*

Bizonyítás. Mivel $g^x = x^{-1}xyx = yx = g^{-1}$, teljesülnek D_n definiáló relációi. Megjegyezzük, hogy $n = 2$ esetén a Klein-csoport, $n = 1$ -re pedig \mathbf{Z}_2 adódik, melyeket elfajult diédercsoportnak tekinthetünk. \square

12.4. Lemma. *Legyen S 2-csoport. Tegyük fel, hogy S minden maximális részcsoportjában van olyan involúció, melynek S -beli centralizátora legfeljebb négyelemű. Ekkor S Abel-féle (és így maga is legfeljebb négyelemű).*

Bizonyítás. Jelölje \mathcal{I} azon S -beli involúciók halmazát, melyek centralizátora legfeljebb négyelemű. Tegyük fel, hogy \mathcal{I} bármely két eleme konjugált. Belátjuk, hogy S -nek csak egy maximális részcsoportja lehet, mégpedig a \mathcal{I} által generált K részcsoport. Legyen M maximális részcsoport, és $x \in M \cap \mathcal{I}$ a feltétel szerinti involúció. A 2.10. Lemma miatt M normálosztó, és ezért kettő az indexe. Az x összes konjugáltja, tehát \mathcal{I} minden eleme M -ben van, ezek száma az x centralizátorának indexe, vagyis legalább $|S|/4 = |M|/2$. Ezért az \mathcal{I} által generált K részcsoport elemszáma nagyobb, mint $|M|/2$ (hiszen e részcsoportban az egységelem is benne van), azaz $K = M$. Tehát tényleg K az egyetlen maximális részcsoport. De ekkor tetszőleges $a \in S \setminus K$ elem által generált részcsoport csak maga S lehet, különben benne lenne egy (K -től különböző) maximális részcsoportban. Azaz S ciklikus, és ebben az esetben készen vagyunk.

Ha viszont létezik $x, y \in \mathcal{I}$, melyek nem konjugáltak, akkor x és y generálja S -et. Valóban, különben létezik egy x -et és y -t tartalmazó M maximális részcsoport. A fenti számoláshoz képest most kétszer annyi, vagyis $|M|$ darab involúció lenne M -ben, ami lehetetlen. Ezért az x és az y tényleg generálja S -et. A 12.3 miatt tehát G izomorf egy diédercsoporttal, azaz az xy elem által generált N részcsoport maximális. A diédercsoport szerkezete miatt N egyetlen involúciója benne van S centrumában. A feltétel szerint létező $z \in N \cap \mathcal{I}$ elemre tehát $C_S(z) = S$, azaz S legfeljebb négyelemű, és így Abel. \square

Legyen most G véges egyszerű csoport, $b \in G$ olyan involúció, melynek C centralizátora a Klein-csoport, és S a G egy C -t tartalmazó 2-Sylowja. Megmutatjuk, hogy $S = C$. Legyen M maximális részcsoportja S -nek. Thompson lemmája (12.2) miatt van olyan $g \in G$, hogy $b^g \in M$. A $c = b^g$ involúció G -beli centralizátora szintén négyelemű. Ezért teljesülnek az előbbi lemma feltételei, azaz tényleg $S = C$. A Thompson-lemma miatt G összes involúciója konjugált, ezért mindegyiknek a Klein-csoport a centralizátora.

Legyen $M = N_G(C)$. Alkalmazzuk az 5.8. Feladat megoldásának gondolatmenetét. A 4.3. Burnside-tétel miatt $C_G(C)$ -ben van egy K normál 2-komplementum, ami tehát centralizálja C -t, és így a b involúciót is. Ezért $K = \{1\}$. Az 5.8. Feladat megoldása tehát azt mutatja, hogy $|M| = 12$, és az M (ciklikus) 3-Sylowjai permutálják a C három involúcióját. (Valójában $M \cong A_4$, ami mutatja, hogy közeledünk célunk felé, de ezt nem fogjuk kihasználni.)

12.5. Állítás. *A G minden olyan C szerinti mellékosztálya, mely nem része M -nek, pontosan egy involúciót tartalmaz.*

Bizonyítás. Az involúciók száma $|G|/|C| = |G|/4 = 3|G : M|$, ebből három esik az M részcsoportba (hiszen abban C az egyetlen 2-Sylow részcsoport). A C mellékosztályainak száma $3|G : M|$, ebből szintén három esik M -be. A két szám egyezése miatt elegendő megmutatni, hogy egyetlen uC ($u \in G \setminus M$) mellékosztályba sem eshet két involúció. Tegyük fel, hogy x, y két ilyen involúció, azaz $x^{-1}y = xy = a \in C$. Ekkor $ay = x$, és ezért $(ay)^2 = 1$, ahonnan $ya = ay$, tehát $y \in C_G(a) = C$, ami ellentmond annak, hogy $y \notin M$. \square

12.6. Állítás. *Legyen $u \in M$, $u \neq 1$. Ekkor $C_G(u) \subseteq M$.*

Bizonyítás. Tegyük fel, hogy ellenkezőleg, $uy = yu$ valamilyen $y \notin M$ esetén. Az előző állítás miatt $y = xa$, ahol $a \in C$ és x involúció. Az $uxa = xau$ egyenlőségből azt kapjuk, hogy $xa = x^u a^u$, azaz $x^{-1}x^u \in C$ (hiszen $u \in M$ miatt $a^u \in C$). De x és x^u involúciók, melyek ugyanabban a C szerinti mellékosztályban vannak. Mivel $x \notin M$, az előző állítás miatt $x = x^u$, vagyis $u \in C_G(x)$. Az x involúció centralizátora Klein-csoport, így maga $u \neq 1$ is involúció. Mivel $u \in M$, ezért $u \in C$, de akkor nem centralizálhatja a C -n kívüli y elemet. \square

Most befejezzük a 12.1. Tétel bizonyítását. Legyen $n = |G : M| - 1$, és x_i, y_i, z_i az M szerinti i -edik bal mellékosztályban lévő három involúció ($1 \leq i \leq n$). Belátjuk, hogy az összesen $2n$ darab $x_i y_i, x_i z_i$ szorzat páronként különböző elemei $M \setminus C$ -nek. Ezek a szorzatok nyilván M -beliek, de nincsenek C -ben (a 12.5 miatt). Tegyük fel, hogy az $x \neq y$ és $u \neq v$ involúciókra $xy = uv \in M$. A feltételt invertálva $yx = vu$, és ezért $(xy)^{xu} = uxyxu = uvuu = uv = xy$, így az előző állítás miatt $xu \in M$, azaz x és u is ugyanabban az M szerinti bal mellékosztályban vannak. Tehát az iménti $2n$ elem tényleg páronként különböző.

Azt kaptuk tehát, hogy $2n \leq |M| - |C| = 8$, azaz $|G : M| \leq 8/2 + 1 = 5$, vagyis hogy $|G| \leq 60$. A 2.5. Lemma módszerével G -t az M mellékosztályain hattatva kapjuk, hogy $G \cong A_5$, vagy $G = M$, de ez utóbbi nem egyszerű csoport. \square

Megjegyezzük, hogy az utolsó három állításban használt technikát lényegesen lehet általánosítani (lásd Feit–Suzuki–Thompson tételeit a már idézett Gorenstein–könyv kilencedik fejezetében). Ezek az eszközök igen fontosak annak vizsgálatában, hogyan lehet egy adott involúció–centralizátorhoz az összes egyszerű csoportot megtalálni. Az involúciókkal való számolásokkal bizonyítjuk a következő tételt is.

12.7. Tétel. *Adott C csoporthoz csak véges sok olyan G véges egyszerű csoport van, melyben egy involúció centralizátora C -vel izomorf.*

Bizonyítás. Legyen $u \in G$ involúció, melynek $K = C_G(u)$ centralizátora C -vel izomorf, és $t = |G : K|$ az u konjugáltjainak száma. Mivel $Z(G) = \{1\}$, azért $t > 1$. Tekintsük az összes vw szorzatot, ahol v és w konjugáltja u -nak. Ily módon t -szer kapjuk meg az egységelemet, a G többi elemét tehát átlagosan $m = (t^2 - t)/(|G| - 1)$ -szer. Azaz van olyan $1 \neq g \in G$, amit legalább m -szer megkapunk. Ha $g = vw$, akkor, mint láttuk, $g^v = g^{-1}$. Tehát legalább m darab v involúcióra lesz $g^v = g^{-1}$ (hiszen ha $vw = g = v'w'$ esetén $v = v'$, akkor $w = w'$). Azon h elemek száma, melyekre $g^h = g^{-1}$, éppen $|C_G(g)|$.

Beláttuk tehát, hogy $m \leq |C_G(g)|$. Ezért

$$|G : C_G(g)| \leq \frac{|G|(|G| - 1)}{t^2 - t} \leq \frac{|G|^2}{t^2/2} = 2|K|^2 = 2|C|^2.$$

A 2.5. Lemma szerint tehát $|G| \leq (2|C|^2)!$. \square

Utolsó involúció–centralizátoros tételünk bizonyításához már karaktereket használunk.

12.8. Tétel. *Legyen G véges egyszerű csoport, melyben egy involúció centralizátora a D_4 diédercsoport. Ekkor $|G|$ vagy 168, vagy 360.*

Megjegyezzük, hogy pontosan egy olyan egyszerű csoport létezik, melynek rendje 168, és olyan is, melynek rendje 360. Ez utóbbi az A_6 , a másíkról a következő fejezetben lesz szó. Annak könnyű volt a bizonyítása, hogy minden 60 rendű egyszerű csoport izomorf A_5 -tel. A mostani két állításhoz már sokkal többet kellene számolni, a 360 rendű eset karaktereket is használ.

Bizonyítás. Legyen G véges csoport, amelyben az u involúció C centralizátora a D_4 . Ha $S \supseteq C$ egy 2–Sylow, akkor legyen v egy involúció az S centrumában. Ekkor v centralizálja u -t, azaz $v \in C$. Továbbá v centralizálja $C \subseteq S$ -et, ezért $v \in Z(C)$. A D_4 centruma azonban kételemű, azaz $u = v$, vagyis S centralizálja u -t, és ezért $S = C$. Beláttuk tehát, hogy G 2–Sylowja izomorf D_4 -gyel. Annak dacára, hogy D_4 bonyolultabb, mint a Klein–csoport, ez a lépés sokkal egyszerűbb volt, mint az előző bizonyításban.

Legyen M a forgatások részcsoportja C -ben. Ebben csak egy involúció van, ezért a 12.2. Thompson–lemma miatt ismét tudjuk, hogy G -ben bármely két involúció konjugált, és ezért mindegyik involúció centralizátora D_4 . Belátjuk, hogy M TI–halmaz. Valóban, ha $M \cap M^g \neq \{1\}$, akkor g centralizálja az $M \cap M^g$ egyetlen involúcióját, és ezért $g \in C$, vagyis $M \triangleleft C$ miatt $M^g = M$. Nemcsak azt láttuk be tehát, hogy az M TI–halmaz, hanem még azt is, hogy $N_G(M) = C$.

Az $M \cong \mathbf{Z}_4$ csoportnak két nem valós karaktere van, legyen λ ezek valamelyike. A 11.15. Gyakorlat megoldása során kiderül, hogy $\lambda^C = \chi_4$ éppen a D_4 csoport egyetlen irreducibilis, másodfokú karaktere, míg $(1_M)^C = 1_C + \chi_2$ értéke 2 az M -en, nulla azon kívül. A $\theta = (1_M - \lambda)^D = \chi_1 + \chi_2 - \chi_4$ tehát teljesíti a 11.11. Lemma feltételeit. Ezért $[\theta^G, \theta^G] = [\theta, \theta] = 3$, és $[\theta^G, 1_G] = [\theta, 1_C] = 1$. Azaz ha $\theta^G = \sum m_i \psi_i$ a G irreducibilis karaktereire való felbontás, akkor az 1_G együtthatója ebben a felbontásban 1, és $\sum m_i^2 = 3$. Azaz még két irreducibilis karakter szerepel, ± 1 együtthatóval. Mivel $\theta^G(1) = \theta(1) = 0$, az egyik együttható pozitív, a másik negatív. Az u elemet behelyettesítve tehát

$$\theta^G = 1 + \chi - \psi, \quad 0 = 1 + \chi(1) - \psi(1), \quad 4 = 1 + \chi(u) - \psi(u).$$

A $b = \chi(u)$ és a $\psi(u) = b - 3$ egész számok, hiszen második egységgyökök összegei. A második ortogonalitási reláció miatt

$$8 = |C_G(u)| \geq 1 + \chi(u)^2 + \psi(u)^2,$$

vagyis b is és $b - 3$ is legfeljebb kettő. Ezért $b = 1$ vagy $b = 2$. Ez a két eshetőség vezet majd el a G csoport két lehetséges rendjéhez. Ahhoz azonban, hogy e karakterek

fokait is korlátozni tudjuk, még meg kell dolgoznunk. Jelölje $\mathcal{K} = \mathcal{K}_i$ a G -beli involúciók konjugált osztályát, és tekintsük az $a_{ii\nu}$ számokat. Ha $g \in \mathcal{K}_\nu$, akkor, mint a 7.6. Lemma bizonyításában láttuk,

$$a_{ii\nu} = |\{(v, w) \mid v, w \in \mathcal{K}, vw = g\}| = \phi(g),$$

ahol az így definiált ϕ persze osztályfüggvény. Ezt $1 \neq g \in M$ -re ki is tudjuk számolni. Ha ugyanis $vw = g$, akkor $v^g = g^{-1} \in M$, ezért vagy $g = u$, és akkor $v \in C$, vagy $g \neq u$, és akkor $M^v = M$, azaz ismét $v \in C$. Tehát a (v, w) párokat C -ben kell keresni, ezért $\phi(g) = 4$.

Másfelől viszont a 10.4. Lemma (d) állítása szerint

$$\phi(g) = a_{ii\nu} = \frac{|\mathcal{K}|^2}{|G|} \sum_{m=1}^k \frac{\psi_m(u)^2}{\psi_m(1)} \psi_m(g^{-1}).$$

Mind $\phi(g)$, mind $\psi_m(u)$ valós, ezért mindkét oldalt konjugálva e képletben $\psi_m(g^{-1})$ helyett $\psi_m(g)$ -t írhatunk. A θ^G -vel skalárisan szorozva kiesik G karaktereinek nagy része:

$$[\theta^G, \phi] = \frac{|\mathcal{K}|^2}{|G|} \left[1 + \frac{\chi(u)^2}{\chi(1)} + \frac{\psi(u)^2}{\psi(1)} \right].$$

Tudjuk, hogy $|G| = 8|\mathcal{K}|$, hiszen $|C_G(u)| = |C| = 8$. A reciprocitást alkalmazva

$$[\theta^G, \phi] = [\theta, \phi|_M] = \frac{1}{4}(0 + (1 - i) \cdot 4 + (1 + 1) \cdot 4 + (1 + i) \cdot 4) = 4.$$

Ezeket behelyettesítve átrendezéssel kapjuk, hogy

$$2^8 = |G| \left[1 + \frac{\chi(u)^2}{\chi(1)} + \frac{\psi(u)^2}{\psi(1)} \right].$$

Legyen most $a = \chi(1)$, ekkor tehát $\psi(1) = a + 1$. Vizsgáljuk először a $b = 1$ esetet. Közös nevezőre hozva kapjuk, hogy

$$|G| = \frac{2^8 a(a + 1)}{(a - 1)^2}.$$

Mivel $a - 1$ és a relatív prímek, $a - 1$ és $a + 1$ legnagyobb közös osztója pedig legfeljebb kettő, kapjuk, hogy a nevező kettő-hatvány, ami osztja 2^9 -t. Másfelől viszont 16 már nem osztja G rendjét, ezért a nevezőben legalább 2^5 szerepel. A $8 \mid |G|$ feltétel miatt végülis $(a - 1)^2 = 2^6$ adódik, amiből $a = 9$, és $|G| = 360$.

A másik esetben $b = 2$, és ekkor

$$|G| = \frac{2^8 a(a + 1)}{(a + 2)^2}.$$

Az előbbi érvelés most azt adja, hogy $(a + 2)^2 = 2^6$, azaz $a = 6$, és $|G| = 168$. \square

13. Egyszerű csoportok. Ebben a részben, a teljesség bármiféle igénye nélkül, a véges egyszerű csoportok klasszifikációjával kapcsolatos eredményekről lesz szó. Az, hogy A_n egyszerű csoport ha $n \geq 5$, már Galois számára is ismeretes volt, ezen múlik annak bizonyítása, hogy a 4-nél magasabb fokú egyenletekre nincsen gyökképlet. Ugyancsak régről ismeretesek az úgynevezett klasszikus egyszerű csoportok, melyek több végtelen sorozatot alkotnak. Ezek talán legfontosabb családjával, a projektív speciális lineáris csoportokkal ($PSL(n, q)$) később megismerkedünk majd.

Már a múlt században találtak olyan csoportokat, melyek nem illettek be ezekbe a végtelen sorozatokba. Az első ötöt felfedezőjükről Mathieu-csoportoknak nevezzük. Jelük M_{11} , M_{12} , M_{22} , M_{23} és M_{24} . Az index azt fejezi ki, hogy ezek az adott elemszámú halmazon ható permutációcsoportok, valójában bizonyos blokkrendszerek automorfizmus-csoportjai. Azért váltak érdekessé, mert sokszorosan tranzitívak, erről később még lesz szó.

A század elején vetette fel Burnside híres problémáját, hogy van-e páratlan rendű nemkommutatív egyszerű csoport. Noha akkoriban már több módszer létezett egyszerű csoportok vizsgálatára (többek között a transzfer is, a karakterek is), a kérdés sokáig nyitott maradt. Az 1950-es években Suzuki meghatározta az összes olyan egyszerű csoportot, melyben minden egységtől különböző elem centralizátora Abel-féle. Suzuki gondolataiból kiindulva Feit, M. Hall és Thompson bebizonyították, hogy ha egy páratlan rendű csoportban minden egységtől különböző elem centralizátora nilpotens, akkor G feloldható, majd módszereiket tovább finomítva végülis belátták, hogy minden páratlan rendű csoport feloldható. A bizonyítás (W. Feit, J. G. Thompson, Solvability of groups of odd order, *Pacific J. Math.*, **13** (1963), 775–1029) több, mint 250 oldal.

Ezután már nem sokáig váratott magára az egyszerű csoportok teljes klasszifikációja. Először Thompson egy újabb 600 oldalas cikkben meghatározta azokat az egyszerű csoportokat, melyek minden valódi részcsoportha már feloldható, ez utóbbi munkájáért Fields-Medalt (matematikai Nobel díjat) kapott. A klasszifikáció az 1980-as évek elején vált teljessé.

A véges, nemkommutatív, egyszerű csoportok 17 végtelen sorozatba tartoznak, és ezen kívül van még 26 egyszerű csoport, melyek egyik sorozatnak sem tagjai. Ezeket *spóradikus* egyszerű csoportoknak nevezzük. A végtelen sorozatok egyikét az alternáló csoportok alkotják. A többi sorozatot Chevalley foglalta egységes rendszerbe. A konstrukciók Lie-algebrák segítségével történnek. A sorozatok közül 6 két paraméteres (ilyen például a $PSL(n, q)$ csoportok sorozata), a többi 11 egy paraméteres. A spóradikus egyszerű csoportok listája az első táblázatban található a fejezet végén, a továbbiakban ennek jelöléseit használjuk. Ide tartoznak például a már említett Mathieu-csoportok is.

Érdeemes elidőzni kicsit a legnagyobb spóradikus csoportnál, mely a Monster névre hallgat. Rendje

$$808\ 017\ 424\ 794\ 512\ 875\ 886\ 459\ 904\ 961\ 710\ 757\ 005\ 754\ 368\ 000\ 000\ 000,$$

azaz $8.08 \cdot 10^{53}$. Összehasonlításképpen néhány adat: a világegyetem nukleonjainak (protonok és neutronok) száma $3 \cdot 10^{77}$, térfogata (jelenleg) 10^{85} köbcenti, a Föld tömege $3.5 \cdot 10^{51}$ -szerese egy proton tömegének (tehát a Monsternek sokkal több eleme van, mint ahány atomból a Föld áll), végül az ősrobbanás (azaz a világ kezdete) óta mindössze $4.7 \cdot 10^{17}$ másodperc telt el.

Ebből láthatjuk, hogy egy ekkora csoportot egyáltalán nem triviális megkonstruálni. A klasszifikációnak ez volt az utolsó lépése. Már tudták, hogy a Monster elemszáma a fenti, hogy 194 konjugált osztálya van, ismerték a karaktertábláját is (ez $194 \cdot 194 = 37636$ szám), csak azt nem tudták, hogy ilyen csoport létezik-e. Végül Griess talált egy 196884-dimenziós algebrát, melynek bizonyos automorfizmusai a Monsterrel izomorf csoportot alkotnak.

Érdekes észrevenni, hogy a konjugált osztályok száma milyen kicsi a csoport rendjéhez képest. Az M_{24} Mathieu-csoportnak például mindössze 26 irreducibilis karaktere van. Ez a csoport alapvető szerepet játszik a Monster, és sok más sporadikus egyszerű csoport szerkezetében is.

Emlékezzünk vissza, hogy egy G csoport akkor involválja H -t, ha H előáll G alkalmas részcsoportjának faktoraként. Ilyenkor persze H rendje osztja G rendjét. A sporadikus csoportoknál tudják, hogy melyek involválják melyeket, egyetlen kivétellel: az nem ismeretes, hogy a Monster involválja-e J_1 -et (noha az kiderült, hogy csak maximális részcsoportja lehet, és ismerik M azon konjugált osztályait, melyek egy ilyen részcsoportba belemetszhetnek). Ezen kívül M az összes sporadikus csoportot involválja, az alábbiak kivételével:

$$J_3, Ru, O'N, Ly, J_4$$

(a J_3 és a Ru csoportok egyetlen sporadikus csoportot sem involválják, és őket sem involválja egyik sporadikus csoport sem). A Monster involvál számos más egyszerű csoportot is, például a $PSL(2, q)$ csoportokat ha $2 \leq q \leq 17$ prímhatvány, ugyanakkor nem involválja az összes olyan $PSL(2, q)$ csoportokat, melyek rendje osztója M rendjének.

Lássuk az összes nemkommutatív egyszerű csoportot, melynek rendje egymilliónál kisebb. Ezek száma 56, melyből 39 izomorf a $PSL(2, q)$ csoporttal alkalmas q prímhatványra, további három izomorf $PSL(3, q)$ -val ($q = 3, 4, 5$), és egy, $A_8 \cong PSL(4, 2)$. Ezt a 43 csoportot a harmadik táblázat tartalmazza, a többi 13-at a második táblázatban soroltuk fel. Itt szerepel két alternáló csoport (A_7, A_9), öt sporadikus csoport (az első három Mathieu és az első két Janko), a maradó hat csoport pedig további végtelen sorozatoknak elemei, ezeket nem definiáljuk. Megjegyezzük, hogy két nemizomorf 20160 rendű egyszerű csoport van.

Most már itt az ideje, hogy megtudjuk, mik is ezek a $PSL(n, q)$ csoportok. Mint az eddigiekben is, jelölje $GL(n, K)$ az $n \times n$ -es nem szinguláris mátrixok csoportját. Ez még nem egyszerű csoport, több okból sem. Egyrészt Z centruma nem triviális (a 9.7. Lemma miatt éppen a skalármátrixokból áll). Másrészt a determinánsképzés homomorfizmusa $GL(n, K)$ -nak a K test multiplikatív csoportjába, jelölje ennek magját, azaz az 1 determinánsú mátrixok normálosztóját $SL(n, K)$ (speciális lineáris csoport). A $GL(n, K)/Z$ csoportnak speciális geometriai jelentése van. A valós test feletti projektív sík kollineáció-csoportja, mint ez geometriából ismeretes, éppen a $GL(3, \mathbf{R})/Z$ csoport. Ezt az állítást tetszőleges K testre lehet általánosítani (amihez kell alkotnunk a K feletti, adott dimenziós projektív tér fogalmát). Ezért a $GL(n, K)/Z$ csoport neve általános projektív lineáris csoport, jele $PGL(n, K)$. Végül $PSL(n, K)$ vagy $L_n(K)$ jelöli az $SL(n, K)$ csoportnak a benne lévő skalármátrixok által alkotott normálosztó szerinti faktorcsoportját. Ha $n = 1$, akkor csoportjaink mindegyike kommutatív, ezért a továbbiakban feltesszük, hogy $n \geq 2$.

Mivel véges csoportokat szeretnénk kapni, célszerű a K testet is végesnek választani. A Galois–elmélet keretében be fogjuk látni, hogy izomfia erejéig minden q prímszámhoz pontosan egy q elemű test létezik. Ha K a q elemű véges test, akkor a most definiált csoportok jelölésében K helyett q -t írunk.

13.1. Tétel. *A $PSL(n, q)$ csoport egyszerű, kivéve $PSL(2, 2)$ és $PSL(2, 3)$.*

A tétel bizonyítása mátrixokkal való számolás, megtalálható például a már idézett Hupert könyvben (6.13. Tétel). Ugyanitt találhatók az alábbi hasznos izomorfizmusok bizonyításai (melyek táblázatainkból is kiolvashatók).

13.2. Tétel. *Az alábbi izomorfizmusok teljesülnek.*

- (a) $PSL(2, 2) \cong SL(2, 2) = GL(2, 2) \cong S_3$.
- (b) $PSL(2, 3) \cong A_4$.
- (c) $PSL(2, 4) \cong PSL(2, 5) \cong A_5$.
- (d) $PSL(2, 7) \cong PSL(3, 2)$ (rendjük 168).
- (e) $PSL(4, 2) \cong A_8$.
- (f) $PSL(2, 9) \cong A_6$.

13.3. Tétel. *Legyen*

$$M = (q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1}) \quad \text{és} \quad d = (q - 1, n).$$

Ekkor

$$|GL(n, q)| = M; \quad |SL(n, q)| = |PGL(n, q)| = \frac{M}{q - 1}; \quad |PSL(n, q)| = \frac{M}{(q - 1)d}.$$

Bizonyítás. Legyen V egy n -dimenziós vektortér a q elemű K test felett, és v_1, \dots, v_n egy bázis. Számoljuk meg a reguláris lineáris transzformációkat. A v_1 képe tetszőleges nem nulla vektor lehet, ez $q^n - 1$ módon választható. A v_2 bárhová képződhet a v_1 generálta al-téren kívül, ez $q^n - q$ -féleképp lehetséges, és így tovább. Ezért $GL(n, q)$ rendje tényleg M . A determináns a K multiplikatív csoportjába képez, ezért $SL(n, q)$ indexe $q - 1$. Az invertálható skalármátrixok száma $q - 1$, azaz $PGL(n, q)$ egy $q - 1$ elemű normálosztó szerinti faktor. Végül az utolsó állítás bizonyításához azt kell megmutatni, hogy az 1 determinánsú skalármátrixok száma $d = (q - 1, n)$. Ehhez meg kell számolni K azon elemeit, melyek n -edik hatványa az egységelem. A 9.8. Tétel miatt K multiplikatív csoportja ciklikus, és ezért készen vagyunk. \square

Végezetül néhány híres eredményt sorolunk el, ami a klasszifikációból következik. A 11.16. feladatban definiáltuk, mit jelent egy k -tranzitív permutációcsoport. A klasszifikáció kombinatorikai alkalmazásai során is általában permutációcsoportokra vonatkozó problémák kerülnek elő. Ez szorosan összefügg a maximális részcsoporthoz leírásával, hiszen többszörösen tranzitív csoportban a stabilizátorok könnyen láthatóan maximális részcsoporthoz. Az egyszerű csoportok legtöbbszöréig már ismerik a maximális részcsoporthoz. Hadd álljon itt egy meglepő eredmény, ami a klasszifikáció bizonyítása előtt híres sejtés volt.

13.4. Tétel. Legyen p prím, és tekintsük az $S_{\{0,1,\dots,p-1\}}$ szimmetrikus csoport azon részcsoportját, melyet az $ax + b$ ($a \neq 0$) alakú permutációk alkotnak (ahol a műveletek mod p értendőek). Ekkor ez $((p - 2)!$ indexű) maximális részcsoport.

13.5. Tétel. Az A_n és S_n csoportokon kívül nincs olyan permutációcsoport, amely legalább hat-tranzitív lenne. Két öt-tranzitív csoport van, az M_{12} és M_{24} Mathieu-csoportok. A négy-tranzitív csoportok száma négy, az előző kettőn kívül még M_{11} és M_{23} .

Három-tranzitív csoport már végtelen sok van, de a klasszifikációból még a kettő-tranzitív csoportok teljes leírása is következik.

13.6. Tétel. Minden véges egyszerű csoport generálható két elemmel.

E tétel szerint ha egy G véges csoport bármely két elemmel generálható részcsoportja feloldható, akkor G is feloldható, és ezt igen nehéz bizonyítani. Ugyanakkor G nyilván pontosan akkor Abel, ha bármely két elemmel generált részcsoportja Abel, és pontosan akkor nilpotens, ha bármely két elemmel generált részcsoportja nilpotens (hiszen ekkor bármely két relatív prím rendű elem felcserélhető).

A G csoport belső automorfizmusai normálosztót alkotnak G automorfizmusainak csoportjában. Az e szerinti faktort nevezzük G külső automorfizmus-csoportjának.

13.7. Tétel. Ha G véges egyszerű csoport, akkor külső automorfizmus-csoportja feloldható.

Ez az állítás Schreier-sejtés néven volt ismeretes. Például a spóradikus csoportok külső automorfizmus-csoportja legfeljebb kételemű lehet.

1. Táblázat. A spóradikus csoportok jele, rendje és felfedezőik.

M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	Mathieu
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	Mathieu
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	Mathieu
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	Mathieu
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	Mathieu
J_2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$	Hall, Janko
Suz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	Suzuki
HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$	Higman, Sims
McL	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	McLaughlin
Co_3	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	Conway
Co_2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	Conway
Co_1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$	Conway, Leech
He	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$	Held/Higman, McKay
Fi_{22}	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	Fischer
Fi_{23}	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	Fischer
Fi'_{24}	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$	Fischer
HN	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$	Harada, Norton/Smith
Th	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$	Thompson/Smith
B	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$	Fischer/Sims, Leon
M	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$	Fischer, Griess
J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	Janko
$O'N$	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$	O'Nan/Sims
J_3	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$	Janko/Higman, McKay
Ly	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$	Lyons/Sims
Ru	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$	Rudvalis/Conway, Wales
J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$	Janko/Norton, Parker, Benson, Conway, Thackray

2. Táblázat. Az egymilliónál kisebb rendű egyszerű csoportok, I.

A_7	$2520=2^3 \cdot 3^2 \cdot 5 \cdot 7$
$U_3(3) \cong G_2(2)'$	$6048=2^5 \cdot 3^3 \cdot 7$
M_{11}	$7920=2^4 \cdot 3^2 \cdot 5 \cdot 11$
$U_4(2) \cong S_4(3)$	$25920=2^6 \cdot 3^4 \cdot 5$
$Sz(8)$	$29120=2^6 \cdot 5 \cdot 7 \cdot 13$
$U_3(4)$	$62400=2^6 \cdot 3 \cdot 5^2 \cdot 13$
M_{12}	$95040=2^6 \cdot 3^3 \cdot 5 \cdot 11$
$U_3(5)$	$126000=2^4 \cdot 3^2 \cdot 5^3 \cdot 7$
J_1	$175560=2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
A_9	$181440=2^6 \cdot 3^4 \cdot 5 \cdot 7$
M_{22}	$443520=2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
J_2	$604800=2^7 \cdot 3^3 \cdot 5^2 \cdot 7$
$S_4(4)$	$979200=2^8 \cdot 3^2 \cdot 5^2 \cdot 17$

3. Táblázat. Az egymilliónál kisebb rendű egyszerű csoportok, II.

$PSL(2, 4) \cong PSL(2, 5) \cong A_5$	$60=2^2 \cdot 3 \cdot 5$
$PSL(2, 7) \cong PSL(3, 2)$	$168=2^3 \cdot 3 \cdot 7$
$PSL(2, 9) \cong A_6 \cong S_4(2)'$	$360=2^3 \cdot 3^2 \cdot 5$
$PSL(2, 8) \cong R(3)'$	$504=2^3 \cdot 3^2 \cdot 7$
$PSL(2, 11)$	$660=2^2 \cdot 3 \cdot 5 \cdot 11$
$PSL(2, 13)$	$1092=2^2 \cdot 3 \cdot 7 \cdot 13$
$PSL(2, 17)$	$2448=2^4 \cdot 3^2 \cdot 17$
$PSL(2, 19)$	$3420=2^2 \cdot 3^2 \cdot 5 \cdot 19$
$PSL(2, 16)$	$4080=2^4 \cdot 3 \cdot 5 \cdot 17$
$PSL(3, 3)$	$5616=2^4 \cdot 3^3 \cdot 13$
$PSL(2, 23)$	$6072=2^3 \cdot 3 \cdot 11 \cdot 23$
$PSL(2, 25)$	$7800=2^3 \cdot 3 \cdot 5^2 \cdot 13$
$PSL(2, 27)$	$9828=2^2 \cdot 3^3 \cdot 7 \cdot 13$
$PSL(2, 29)$	$12180=2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 29$
$PSL(2, 31)$	$14880=2^5 \cdot 3 \cdot 5 \cdot 31$
$PSL(4, 2) \cong A_8$	$20160=2^6 \cdot 3^2 \cdot 5 \cdot 7$
$PSL(3, 4)$	$20160=2^6 \cdot 3^2 \cdot 5 \cdot 7$
$PSL(2, 37)$	$25308=2^2 \cdot 3^2 \cdot 19 \cdot 37$
$PSL(2, 32)$	$32736=2^5 \cdot 3 \cdot 11 \cdot 31$
$PSL(2, 41)$	$34440=2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 41$
$PSL(2, 43)$	$39732=2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 43$
$PSL(2, 47)$	$51888=2^4 \cdot 3 \cdot 23 \cdot 47$
$PSL(2, 49)$	$58800=2^4 \cdot 3 \cdot 5^2 \cdot 7^2$
$PSL(2, 53)$	$74412=2^2 \cdot 3^3 \cdot 13 \cdot 53$
$PSL(2, 59)$	$102660=2^2 \cdot 3 \cdot 5 \cdot 29 \cdot 59$
$PSL(2, 61)$	$113460=2^2 \cdot 3 \cdot 5 \cdot 31 \cdot 61$
$PSL(2, 67)$	$150348=2^2 \cdot 3 \cdot 11 \cdot 17 \cdot 67$
$PSL(2, 71)$	$178920=2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 71$
$PSL(2, 73)$	$194472=2^3 \cdot 3^2 \cdot 37 \cdot 73$
$PSL(2, 79)$	$246480=2^4 \cdot 3 \cdot 5 \cdot 13 \cdot 79$
$PSL(2, 64)$	$262080=2^6 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$
$PSL(2, 81)$	$265680=2^4 \cdot 3^4 \cdot 5 \cdot 41$
$PSL(2, 83)$	$285852=2^2 \cdot 3 \cdot 7 \cdot 41 \cdot 83$
$PSL(2, 89)$	$352440=2^3 \cdot 3^2 \cdot 5 \cdot 11 \cdot 89$
$PSL(3, 5)$	$372000=2^5 \cdot 3 \cdot 5^3 \cdot 31$
$PSL(2, 97)$	$456288=2^5 \cdot 3 \cdot 7^2 \cdot 97$
$PSL(2, 101)$	$515100=2^2 \cdot 3 \cdot 5^2 \cdot 17 \cdot 101$
$PSL(2, 103)$	$546312=2^3 \cdot 3 \cdot 13 \cdot 17 \cdot 103$
$PSL(2, 107)$	$612468=2^2 \cdot 3^3 \cdot 53 \cdot 107$
$PSL(2, 109)$	$647460=2^2 \cdot 3^3 \cdot 5 \cdot 11 \cdot 109$
$PSL(2, 113)$	$721392=2^4 \cdot 3 \cdot 7 \cdot 19 \cdot 113$
$PSL(2, 121)$	$885720=2^3 \cdot 3 \cdot 5 \cdot 11^2 \cdot 61$
$PSL(2, 125)$	$976500=2^2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 31$