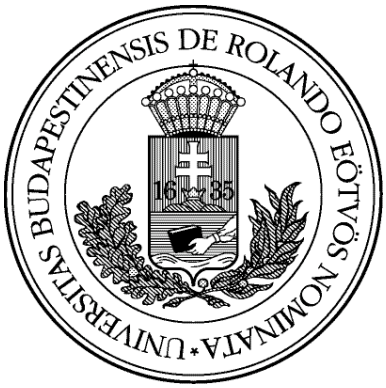
Eötvös Loránd Tudományegyetem
Természettudományi Kar

Gyarmati Máté
Matematika BSc
Matematikus szakirány

Számelméleti feltételek csoportok feloldhatóságára

Szakdolgozat

Témavezető: Pálfy Péter Pál egyetemi tanár
Algebra és Számelmélet Tanszék



Budapest, 2015

Köszönetnyilvánítás

Szeretném megköszönni témavezetőmnek Pálfy Péter Pálnak az ajánlott szakirodalmat, és a szakdolgozat alapos átnézését.

Tartalomjegyzék

Tartalomjegyzék **4**

1. Bevezetés **5**

2. Ciklikus, Abel és nilpotens számok **6**

2.1. Ciklikus számok 6

2.2. Abel számok 7

2.3. Nilpotens csoportok 9

3. Feloldható csoportok **12**

3.1. Transzfer 12

3.2. Modulusok, reprezentációk 15

3.3. Karakterek 19

3.4. Algebrai egészek és a Burnside tétel 25

3.5. További eredmények 27

4. A PSL(n,q) csoportok egyszerűsége **29**

4.1. Iwasava tétele 29

4.2. Transzvekció 30

5. Hivatkozások **37**

1. Bevezetés

A szakdolgozat írásakor az elsődleges célom a csoportok egy bizonyos fajtájának, a feloldható csoportoknak vizsgálata volt. A feloldható csoportok vizsgálata elég szerteágazó, nagyon sok féle elmélet foglalkozik velük. A szakdolgozatomban különböző számelméleti feltételeket fogok majd adni csoportok feloldhatóságára. Azonban mielőtt ennek nekikezdek, előtte néhány egyszerűbb tulajdonsággal foglalkozok. Legyen egy szám ciklikus, Abel, nilpotens, ha minden n rendű csoport ciklikus, Abel, nilpotens ebben a sorrendben. Az első fejezetben ezeket a számokat fogom meghatározni. A probléma már elég régi, a ciklikus számokat valószínűleg már a 19. században sikerült megadni. Az Abel eset is meg volt már az 1900-as évek elején, Miller és Morena 1903-as cikkében, [1], azokat a nem Abel csoportokat vizsgálta, aminek minden valódi részcsoportja Abel. Ezen cikk segítségével Dicksonnak 1905-ben sikerült megadnia az Abel számokat [2]. A nilpotens számok pontos meghatározása még egy kicsit váratott magára, de az 1940-es évek végére már sikerült karakterizálni őket [3].

A következő fejezetben rátérek a feloldható esetre; nevezzünk egy n számot feloldhatónak, ha minden n rendű csoport feloldható. A feloldható számokra Burnside adott két fontos kritériumot. Ezeket veszem sorra, és közben bemutatom a csoport elmélet két hasznos eszközét is. Az első esetben azt fogom megmutatni, hogy a négyzetmentes számok feloldhatók, és ehhez egy speciális homomorfizmust, a transzfert fogom használni. Burnside másik tétele, a reprezentáció elmélet egyik leghíresebb eredménye. Az 1904-ben publikált tétel szerint [4] ha egy számnak legfeljebb két prímosztója van, akkor feloldható. A tétel bizonyításához vezető úton megismerkedhetünk a karakterekkel, és néhány egyéb alapfogalommal, alapállítással. Persze Burnside tétele óta született újabb eredmény a témakörben, a legjelentősebb az 1963-ban publikált Feit-Thompson tétel [5], miszerint minden páratlan rendű csoport feloldható. A tételnek nem csak a feloldható számok meghatározásában volt fontos szerepe, hanem az egyszerű csoportok vizsgálatára is igen nagy hatással volt.

A véges feloldható csoportok elmélete szoros kapcsolatban áll a véges egyszerű csoportokéval, hiszen ha egy véges csoport nem feloldható, akkor valamelyik faktora nem Abel egyszerű csoport. Tehát a feloldható számok meghatározásához elég megadni a véges egyszerű csoportok rendjét. Az 1980-as évekre sikerült meghatározni a véges egyszerű csoportokat[6], és így sikerült teljesen megadni a feloldható számokat is. Egy nem Abel egyszerű csoport rendjének többszöröse nem lehet feloldható, így ez ad egy feltételt a feloldható számokra. Meglepő, hogy a véges egyszerű csoportok két végtelen sorozata már minden feltételt megad. Az egyik ilyen sorozat elemei a $PSL(n, q)$ csoportok (projectiv special linear groups). Az utolsó fejezetben bebizonyítom, hogy a $PSL(n, q)$ csoportok egyszerűek két kivételtől eltekintve, és megvizsgálom milyen feltételeket adnak a feloldható számokra.

2. Ciklikus, Abel és nilpotens számok

2.1. Ciklikus számok

2.1.1. Definíció. *Az n számot nevezzük ciklikusnak, ha minden n rendű csoport ciklikus.*

Nyílvánvaló, hogy ha egy n szám ciklikus, akkor csak egy n rendű csoport van. Mielőtt kimondanám és bebizonyítanám a ciklikus számokra vonatkozó tételt, bebizonyítok két lemmát, amire a bizonyítás során szükség lesz.

2.1.2. Lemma. *Adott G nem Abel csoport, aminek bármely két maximális részcsoportja triviálisan metszi egymást. Ekkor G nem lehet egyszerű.*

Bizonyítás: Először is mivel G nem Abel, így létezik maximális részcsoportja, ami nem triviális. Továbbá legyen M maximális részcsoport G-ben. Mivel M maximális, így G-nek csak két részcsoportja bővebb, M és G. Ha $N_G(M) = G$, akkor M normálosztó és készen vagyunk. Már csak azt az esetet kell vizsgálni, amikor minden maximális részcsoport normalizátora önmaga.

Legyen M rendje m, és G rendje pedig n. M konjugáltjainak száma a normalizátor indexe, tehát n/m, és ezek egyetlen közös eleme az 1, így M konjugáltjainak uniója $n(m-1)/m + 1 = n - n/m + 1$ elemű. $n/2 + 1 \leq n - n/m + 1$, hiszen m legalább 2, és $n - n/m + 1 < n$, mert $m < n$. Tehát egy maximális részcsoport és ennek konjugáltjai még nem adják ki G-t, viszont ha G-ben van legalább két maximális részcsoport, amik nem konjugáltak, akkor ezek konjugáltjainak uniója már legalább $n/2+n/2+1 = n+1 > n$ elemű ami ellentmondás. Tehát nem lehet minden maximális részcsoport normalizátora önmaga, és így kész vagyunk.

2.1.3. Állítás. *Ha a G nem Abel csoport minden valódi részcsoportja Abel, akkor nem egyszerű*

Bizonyítás: Tegyük fel, hogy G egyszerű, nem Abel, de minden valódi részcsoportja Abel. Mivel a centrum normálosztó egy csoportban, és G nem Abel, így nem lehet az egész csoport, tehát a centrum csak triviális lehet.

Vegyünk két maximális részcsoportot G-ben, legyen ez A és B. Tegyük fel, hogy $\exists g \in A \cap B, g \neq 1$. Ekkor g cenralizátora tartalmazza A-t és B-t, hiszen mindkettő Abel, így $\langle A, B\rangle \subseteq C_G(g)$. De mivel A, B maximálisak. így $\langle A, B\rangle = G$, tehát g-t az egész csoport centralizálja, de ekkor g benne van a centrumban, ami ellentmondás. Tehát bármely két maximális részcsoport metszete triviális. Alkalmazzuk az előző lemmát, amiből következik, hogy G nem egyszerű.

2.1.4. Tétel. *n ciklikus, akkor és csak akkor, ha n és $\varphi(n)$ relatív prímek, ahol φ az euler-függvény.*

Bizonyítás: Először tegyük fel, hogy $n = p_1^{t_1}...p_r^{t_r}$, és $(n, \varphi(n)) > 1$. Megmutatjuk, hogy ekkor létezik nem ciklikus csoport. Ha $(n, \varphi(n)) > 1$ teljesül, akkor a két következő eset közül legalább az egyik fennáll.

Első eset: Ha n nem négyzetmentes, vagyis $p_i^2|n$, akkor a p_i-Sylow megválasztható nem ciklikusnak is. Ezt direkt szorozva prímrendű egyszerű csoportokkal nem ciklikus n rendű csoportot kapunk.

Második eset: Ha $p_i|p_j-1$, akkor létezik $\mathbb{Z}_{(p_i)} \ltimes \mathbb{Z}_{(p_j)}$, ami nem ciklikus. Nyilvánvaló, hogy ezt ugyanúgy direktszorozva prímrendű egyszerű csoportokkal n rendű nem ciklikus csoporthoz jutunk.

Most azt kell megmutatni, hogy ha G rendje az n ciklikus szám, akkor az n rendű ciklikus csoport az egyetlen n rendű csoport. Az állítást n szerinti indukcióval látjuk be. $n = 1$ esetén nyilvánvaló az állítás. Tegyük fel, hogy minden n-nél kisebb rendű csoportra igaz a feltétel. Ha G rendje ciklikus szám, akkor G minden részcsoportjának rendje is az, így az indukciós feltevésünk miatt G minden valódi részcsoportja ciklikus. Ha G Abel, akkor a Sylowjainak direkt szorzata, amik ciklikusak, így G is ciklikus. Ha G nem Abel, de minden valódi részcsoportja Abel, akkor van normálosztója, ezt mondta ki az előző lemma. Legyen $N \lhd G$ és $|N| = d$. Ekkor N ciklikus, és így

$$|Aut(N)| = \varphi(d) = \prod_{p_i|d} (p_i - 1).$$

N-nek G elemeivel való konjugálása az N egy automorfizmusát adja, ami meghatároz egy $\phi : G \to Aut(N)$ homomorfizmust. Mivel $(n, \varphi(n)) = 1$, így $(n, p_i - 1) = 1$ $\forall p_i|n$ prímre, tehát $(n, |Aut(d)) = 1$, így ϕ magja G, és $N \subset Z(G)$. $Z(G)$ nem triviális normálosztó, vehetjük a $G/Z(G)$ faktorcsoportot, ami rendje osztja G rendjét, így az indukció miatt ciklikus. Ha a generálja $G/Z(G)$-t, akkor $\langle a, Z(G)\rangle = G$. Legyen $g_1, g_2 \in G$ tetszőleges, $g_1 = a^s z_1$, $g_2 = a^t z_2$ ahol $z_1, z_2 \in Z(G)$ és $s, t \in \mathbb{N}$. $g_1 g_2 = a^s z_1 a^t z_2 = z_1 z_2 a^{s+t} = a^t z_2 a^s z_1$ miatt G Abel, ami ellentmond a korábbi feltevésnek. Tehát G ciklikus.

2.2. Abel számok

2.2.1. Definíció. *Az n számot nevezzük Abelnek, ha minden n rendű csoport Abel.*

2.2.2. Állítás. *Az n szám akkor és csak akkor Abel, ha $n = p_1^{t_1}...p_r^{t_r}$, ahol p_i-k különböző prímek, $t_i \leq 2, t_i \in \mathbb{N}$ $i = 1, ..., r$, továbbá p_i nem osztja $p_j^k - 1$-et $1 \leq k \leq$ $\leq t_j, k \in \mathbb{N}$.*

Ha adott p prím, akkor létezik p^3 rendű nem Abel csoport. Ez alapján nyilvánvaló, hogy ha n nem köbmentes, akkor létezik nem Abel csoport, hiszen a p^3 rendű

nem Abel csoportot direkt szorozva prím rendű Abel csoportokkal n rendű csoportot kapunk. Ha n két prímosztójára $p_i \mid p_j^k - 1$ teljesül akkor létezik nem Abel n rendű csoport. Sőt létezik nem nilpotens csoport is, és ezt az erősebb állítást fogjuk belátni. Azt már látjuk, hogy ha n nem Abel szám, akkor létezik nem Abel csoport.

Most foglalkozzunk a megfordítással, ehhez belátok egy lemmát.

2.2.3. Lemma. *Legyen G nem Abel csoport, melynek minden valódi részcsoportja Abel. Ekkor*

(a) G rendje legfeljebb két prímmel osztható

(b) Ha G nem p-csoport, akkor az egyik prímhez tartozó Sylow normálosztó, a másik prímhez tartozó Sylow pedig ciklikus.

Bizonyítás: (lemma) Nem lehet G minden Sylowja normálosztó G-ben, mert akkor G Sylowjainak direktszorzata, amik Abelek így G is Abel lenne. Legyen P p-sylow nem normálosztó. Ekkor $N_G(P)$ valódi részcsoport G-ben, tehát Abel, így $C_G(P) = N_G(P)$. Alkalmazzuk a 3.1.7-es Burnside tételt, ezt majd később be fogom bizonyítani. Az tétel állítása szerint, mivel $C_G(P) = N_G(P)$ fennáll, ezért $\exists N \lhd G$, hogy $NP = G$ és $N \subset P = 1$, továbbá a feltétel miatt N is Abel, azaz G Sylowjainak direktszorzata. Ha N q-Sylowját tetszőleges G-beli elemmel konjugálom, akkor is N-ben lesz, és mivel N-ben egyetlen q-Sylow van, így N minden Sylowja normálosztó G-ben is. Legyen Q tetszőleges Sylow N-ben. Ha N nem q-csoport, akkor $PQ < G$, vagyis P az N minden Sylowjával felcserélhető, de ezek generálják N-et, tehát P felcserélhető N-el, ami ellentmondás, mert P nem normálosztó. Ezzel az állítás első felét beláttuk. N helyett írjunk Q-t jelezve, hogy q-Sylowról van szó.

Ha P nem ciklikus, akkor véges sok elem generálja, legyenek ezek $p_1, ..., p_s$, és az általuk generált ciklikus csoportok $P_1, ..., P_s$. Ekkor tetszőleges $i \in \{1, ..., s\}$-re $\langle p_i, Q\rangle = P_iQ < PQ = G$, tehát P_iQ Abel és p_i felcserélhető Q-val. Q felcserélhető P generátor elemeivel, így P-vel is, ami ellentmondás.

Bizonyítás: (állítás) Tegyük fel, hogy G minimális nem Abel csoport, aminek rendje Abel szám. Ekkor G minden valódi részcsoportjának rendje Abel szám, tehát G minden valódi részcsoportja Abel G minimalitása miatt. A lemma miatt G rendje p^aq^b, ahol $a, b \leq 2$. Ha G rendje csak 1 prímmel osztható, akkor G Abel, készen vagyunk. Legyen P p-Sylow normálosztó, Q q-Sylow pedig ciklikus. P-nek Q elemeivel való konjugálása a P-nek egy automorfizmusát adja, ami meghatároz egy $\psi : Q \to Aut(P)$ homomorfizmust. A leképezés nem triviális, különben G Abel lenne, így $Aut(P)$-nek van q rendű részcsoportja. De $|Aut(P)| = p^2 - p = p(p-1)$, vagy $|Aut(P)| = (p^2-1)p(p-1)$, ami egyik esetben sem osztható q-val, hiszen G Abel szám. Ez ellentmondás, tehát G Abel csoport, és így kész vagyunk.

2.3. Nilpotens csoportok

Tovább gyengítjük a csoportra adott feltételünket, most a kommutatívitás helyett csak azt követeljük meg, hogy a csoport a Sylow részcsoportjainak direkt szorzata. Nyilvánvaló, hogy ez gyengébb feltétel a kommutativitásnál, szerencsére a problémát ebben az esetben is jól tudjuk kezelni.

2.3.1. Definíció. *Tegyük fel, hogy a G véges csoport a Sylow részcsoportjainak direkt szorzata. Ekkor a G csoport nilpotens.*

A nilpotencia végtelen csoportokra is definiálható, azonban mivel véges csoportokkal dolgozunk, ezt most nem teszem meg. Könnyen látható, hogy ha egy csoportban minden Sylow normálosztó, akkor az Sylowjainak direkt szorzata, és ez visszafele is fenn áll. A nilpotens csoportokat jellemzi még az úgynevezett normalizátor-feltétel.

2.3.2. Definíció. *A G véges csoport kielégíti a normalizátor-feltételt, ha G minden valódi részcsoportjánál normalizátora szigorúan bővebb.*

2.3.3. Állítás. *A G véges csoport akkor és csak akkor nilpotens, ha teljesül rá a normalizátor-feltétel.*

2.3.4. Definíció. *Az n szám nilpotens, ha minden n rendű csoport nilpotens.*

2.3.5. Definíció. *Legyen $n = p_1^{t_1}...p_r^{t_r}$, p_i-k különböző prímek. n-nek akkor és csak akkor van nilpotens faktorizációja, ha $p_i^k \not\equiv 1 \mod p_j$ minden pozitív egész i, j, k-ra, amire $1 \leq k \leq t_i$ teljesül.*

Ha n prímhatvány, vagy $n = pq$, ahol $p < q$ és $p \nmid q-1$, akkor n-nek van nilpotens faktorizációja, de például $n = 6$ esetén már nincsen. Az is nyilvánvaló, hogy ha n ciklikus, vagy Abel, akkor szintén van nilpotens faktorizációja.

2.3.6. Tétel. *Az n szám akkor és csak akkor nilpotens, ha van nilpotens faktorizációja. [7]*

Bizonyítás: Először tegyük fel, hogy $n = p_1^{t_1}...p_r^{t_r}$-nek nincs nilpotens faktorizációja, vagyis léteznek a pozitív egész i, j, k számok $1 \leq k \leq t_i$, hogy $p_i^k \equiv 1 \mod p_j$. Mivel $i \neq j$, az indexek átcímkézésével elérhetjük, hogy $p_1^k \equiv 1 \mod p_2$, $1 \leq k \leq t_1$. Vegyük a $V = \mathbb{Z}_{p_1}^k$ Abel csoportot, tekinthetjük ezt az $\mathbb{F}_{p_1}$ véges test feletti k-dimenziós vektortérnek. V, mint vektortér automorfizmusai az $\mathbb{F}_{p_1}$-beli együtthatójú $k \times k$-s mátrixok, amiknek determinánsa nem 0 modulo p_1, azaz $Aut(V) = GL_k(\mathbb{F}_{p_1})$. Ismert, hogy $|GL_k(\mathbb{F}_{p_1})| = (p_1^k - 1)(p_1^k - p_1)...(p_1^k - p_1^{k-1})$, ami a feltevés miatt ($p_1^k \equiv 1 \mod p_2$) osztható p_2-vel. Tehát p_2 osztja $Aut(V)$ rendjét, így a Cauchy tétel miatt $Aut(V)$-nek van $\mathbb{Z}_{p_2}$-vel izomorf részcsoportja. Tehát megadható a nemkommutatív $V \rtimes \mathbb{Z}_{p_2}$ szemi-direkt szorzat. Tekintsük a következő csoportot:

$$G = V \rtimes \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_1}^{t_1-k} \times \mathbb{Z}_{p_2}^{t_2-1} \times \mathbb{Z}_{p_3}^{t_3} \times ... \times \mathbb{Z}_{p_r}^{t_r}$$

G-t úgy konstruáltuk, hogy a rendje n legyen, és a V-beli elemek nem cserélhetők fel a $V \rtimes \mathbb{Z}_{p_2}$ szemi-direkt szorzatban a $\mathbb{Z}_{p_2}$-beli elemekkel. Viszont egy nilpotens csoportban azon elemek, amik különböző prímhez tartozó Sylow-csoportokban vannak felcserélhetők egymással. Mivel ez G-re nem teljesül, így G nem nilpotens.

A megfordításhoz meg kell mutatnunk, hogy ha az n-nek van nilpotens faktorizációja, akkor minden n rendű csoport nilpotens. Tegyük fel, hogy ez nem igaz és legyen n a minimális, nilpotens faktorizációval rendelkező nem nilpotens szám. Létezik n rendű, nem nilpotens csoport, legyen ez G. Nyilvánvaló, hogy egy szám osztóira is öröklődik a nilpotens faktorizáció, így n minden osztójának is van nilpotens faktorizációja. n minimális volta miatt G minden részcsoportja nilpotens. Tehát G nem-nilpotens csoport, aminek minden valódi részcsoportja nilpotens. Az ilyen csoportok rendjének O. J. Schmidt tétele szerint pontosan két prímosztója van (O. J. Schmidt tételét a bizonyítás befezése után mondom ki és bizonyítom). Legyen $n = p^a q^b$. Ugyanezen tétel (iii) állításából a p-Sylow normálosztó. Legyen a q-Sylowok száma s. A Sylow tételekből egyrészt $s \equiv 1 \bmod q$, másrészt $s|p^a$, tehát p hatvány. Mivel n-nek van nilpotens faktorizációja, így $s \equiv 1 \bmod q$ csak $s = 1$ esetén állhat fenn, azaz a q-Sylow is normálosztó. n mindkét prímosztójához tartozó Sylowja normálosztó, így G nilpotens a korábban leírtak miatt, ami ellentmondás. Tehát ha az n számnak van nilpotens faktorizációja, akkor az n nilpotens.

Ahogy ígértem, következik a bizonyítás közben felhasznált tétel.

2.3.7. Tétel. *(O. J. Schmidt) [8] Tegyük fel, hogy a G véges csoport minden valódi részcsoportja nilpotens, de ő maga nem. Ekkor a következők igazak:*

(i) G feloldható

(ii) $|G| = p^a q^b$

(iii) G-nek egyetlen P p-Sylow részcsoportja van, és a Q q-Sylow részcsoport ciklikus. Így $G = PQ$ és $P \lhd G$.

Bizonyítás: (i) Legyen G minimális rendű ellenpélda. Ha N valódi normálosztója G-nek, akkor N részcsoport G-ben, így nilpotens, tehát feloldható. Mivel a nilpotencia öröklődik a faktorizálásnál, így G/N minden részcsoportja is nilpotens, rendje viszont kisebb G rendjénél, tehát feloldható G minimális volta miatt. Tehát N és G/N is feloldható, így G is feloldható, ami ellentmond a feltevésnek. Tehát G egyszerű.

Legyen M és N azon maximális részcsoportok G-ben, melyekre $|M \cap N|$ maximális, és tegyük fel, hogy $|M \cap N| \neq 1$. Tudjuk hogy M és N nilpotensek, továbbá $M \cap N$ szintén nilpotens, ezért $M \cap N < N_M(M \cap N)$ és $M \cap N < N_N(M \cap \cap N)$ a normalizátor-feltétel miatt. Vegyük G olyan maximális részcsoportját, mely

tartalmazza $N_G(M \cap N)$-t (ha $M \cap N \neq 1$, akkor létezik ilyen, mert G-ben nincs valódi normálosztó). Ennek az M-el vett metszete tartalmazza $N_M(M \cap N)$-t, aminek rendje szigorúan nagyobb $M \cap N$ rendjénél, de ez ellentmond M és N megválasztásának. Tehát G bármely két maximális részcsoportja csak az egységelemben metszi egymást. Alkalmazzuk a 1. lemmát, G nem lehet egyszerű, és ezzel kész is vagyunk.

(ii) Legyen $G = p_1^{\alpha_1}...p_k^{\alpha_k}$, ahol $\alpha_i > 0$ és p_i-k különböző prímek. Tegyük fel, hogy $k \geq 3$. Ha N egy maximális normálosztó G-ben, akkor N indexe prím, mivel G feloldható. Feltehető, hogy $|G : N| = p_1$. Legyen P_i a G egy p_i-Sylow részcsoportja. Ekkor $i > 1$ esetén P_i p_i-Sylow részcsoportja N-nek is, tehát $P_i \lhd N$, hiszen N nilpotens. Ha $g \in G$, akkor $g^{-1}Ng = N$, így $g^{-1}P_ig \subset N$, továbbá $g^{-1}P_ig$ szintén p_i-Sylow részcsoport, tehát $g^{-1}P_ig = P_i$ teljesül $\forall g \in G$, azaz $P_i \lhd G$. Továbbá P_1P_j nem lehet G, hiszen a p_j rendű elemek, ahol $j \neq 1$ és $j \neq i$ nincsenek benne, ezért nilpotens, azaz Sylow részcsoportjainak direktszorzata, így $[P_1, P_j] = 1$. Mivel G-t generálják Sylow részcsoportjai, így P felcserélhető G minden elemével, vagyis $P \lhd G$, de ekkor G minden Sylow részcsoportja normálosztó, vagyis G nilpotens. Az ellentmondásból $k = 2$, azaz $G = p^aq^b$.

(iii) Legyen N maximáis normálosztó G-ben, az indexe legyen q. Ekkor N p-Sylowja normálosztó N-ben, és így G-ben is. Legyen Q q-Sylow, ekkor fennáll $PQ = = G$. Tegyük fel, hogy q nem ciklikus, ekkor tetszőleges $q \in Q$-ra $\langle q, P\rangle \neq G$, tehát $\langle q, P\rangle$ nilpotens. Mivel $[q, P] = 1$ $\forall q \in Q$, így $[P, Q] = 1$ és $G = P \times Q$ nilpotens, ami ellentmondás, ezért Q ciklikus.

3. Feloldható csoportok

3.1. Transzfer

Most bevezetünk egy új eszközt, egy homomorfizmust, ami segít nekünk eljutni az egyik fontos tételhez.

3.1.1. Definíció. *Legyen G tetszőleges csoport, H ennek véges indexű részcsoportja. Bontsuk fel G-t a H szerinti jobboldali mellékosztályok diszjunkt egyesítésére: $G = Hx_1 \cup Hx_2 \cup ... \cup Hx_n$, ahol $n = |G : H|$. Legyen $g \in G$, ekkor a g-vel való szorzás permutálja a mellékosztályokat: $Hx_ig = Hx_{j(i,g)}$, ahol $i \mapsto j(i,g)$ az $\{1,2,...,n\}$ indexek permutációja. Ekkor $x_igx_{j(i,g)}^{-1} \in H$. Definiáljuk a $\tau_{G\to H} : G \to H/H'$ leképezést a*

$$\tau_{G\to H}(g) = (\prod_{i=1}^{n} x_igx_{j(i,g)}^{-1})H'$$

képlettel. Mivel a szorzat tényezői H-beliek és a szorzatot a H/H' faktorcsoportban tekintjük, ami kommutatív, így $\tau_{G\to H}(g)$ nem függ a tényezők sorrendjétől.

Mivel a transzfer a H/H' kommutatív csoportba képez, ezért a magja mindig tartalmazza a G' kommutátor részcsoportot. Emiatt abban az esetben (és más esetekben is), amikor $G = G'$, akkor a transzfer a triviális leképezés, szerencsére azonban sok más esetben igen hasznos eszköz.

3.1.2. Állítás. *A $\tau_{G\to H}$ leképezés nem függ a mellékosztályok $x_1, ..., x_n$ reprezentánsainak megválasztásától.*

Bizonyítás: Vegyünk egy másik reprezentánsrendszert, $y_i = h_ix_i$ ($h_i \in H, i = 1, ..., n$). Ekkor $Hx_ig = Hy_ig = Hx_{j(i,g)} = Hy_{j(i,g)}$, hiszen a mellékosztályok permutációja nem függ a reprezentáns elem választásától. A szorzat a $y_1, ..., y_n$ reprezentánsokat véve a következő lesz:

$$(\prod_{i=1}^{n} y_igy_{j(i,g)}^{-1})H' = (\prod_{i=1}^{n} h_ix_igx_{j(i,g)}^{-1}h_{j(i,g)}^{-1})H' = (\prod_{i=1}^{n} x_igx_{j(i,g)}^{-1})H'$$

hiszen a H-beli elemeket tetszőleges sorrendben összeszorozhatjuk, és mivel az $i \to j(i,g)$ leképezés permutáció, így minden h_i elemnek szerepel az inverze is, tehát ezekkel lehet egyszerűsíteni.

Tehát a definiált leképezés valóban csak G-től és H-tól függ, ahogy azt a jelölés mutatja. A $\tau_{G\to H}$ leképezést transzfernek hívjuk, és a továbbiakban az egyszerűség

kedvéért $\tau_{G\to H}$ helyett már csak τ-t, $j(i,g)$ helyett j-t írunk, ha ez nem ad okot a félreértésre. Még nem láttuk be, hogy τ valóban homomorfizmus, most ennek a bizonyítása jön.

3.1.3. Állítás. *A transzfer művelettartó leképezés G-ből H/H'-ba.*

Bizonyítás: Legyen $f,g \in G, Hx_if = Hx_j, Hx_jg = Hx_k$. Ekkor $Hx_i(fg) = = Hx_k$ és

$$\tau(f)\tau(g) = (\prod_{i=1}^{n} x_i f x_j^{-1})H'(\prod_{j=1}^{n} x_j g x_k^{-1})H' = (\prod_{i=1}^{n}(x_i f x_j^{-1})(x_j g x_k^{-1}))H' = \tau(fg)$$

A transzfer kiszámítását segíti a következő lemma.

3.1.4. Lemma. *A g által a mellékosztályokon meghatározott permutáció minden ciklusából vegyünk egy indexet, legyenek ezek $i_1, ..., i_k$, és legyen az i_r ciklus hossza λ_r. Ekkor*

$$\tau(g) = (\prod_{r=1}^{k} x_{i_r} g^{\lambda_r} x_{i_r}^{-1})H'$$

Bizonyítás: Mivel a mellékosztályok reprezentánsai tetszőlegesen választhatók, megtehetjük, hogy az x_{i_r} ciklusához tartozó mellékosztályokból az $x_{i_r}, x_{i_r}g, ..., x_{i_r}g^{\lambda_r-1}$ reprezentánsokat választjuk. Vegyük a τ-t definiáló szorzat egy tényezőjét:

$x_{i_r}g^t g(x_{i_r}g^{t+1})^{-1} = 1$, ha $t \neq \lambda_r - 1$, és $t = \lambda_r - 1$ esetén $x_{i_r}g^{\lambda_r-1}gx_{i_r}^{-1} = x_{i_r}g^{\lambda_r}x_{i_r}^{-1}$, amiből kapjuk a lemma állítását.

3.1.5. Lemma. *Ha egy G véges csoport P Sylow-részcsoportja kommutatív, akkor két P-beli elem pontosan akkor konjugált G-ben, ha $N_G(P)$-ben is konjugáltak.*

Bizonyítás: Legyen $a, b \in P$ G-ben konjugált, és legyen $b = g^{-1}ag$. Mivel P Abel-csoport, így $P \leqslant C_G(a)$, és $P \leqslant C_G(b)$, amiből $g^{-1}Pg \leqslant g^{-1}C_G(a)g$. $g^{-1}C_G(a)g = C_G(g^{-1}ag) = C_G(b)$, hiszen $h \in C_G(a)$ esetén $g^{-1}hg$ nyilván benne van $C_G(g^{-1}ag)$-ben. Így $g^{-1}Pg \leqslant C_G(b)$ miatt P és $g^{-1}Pg$ is Sylow-részcsoport $C_G(b)$-ben, így a II.Sylow-tétel miatt $\exists h \in C_G(b)$, hogy $P = h^{-1}g^{-1}Pgh$. Tehát $gh \in N_G(P)$, továbbá $(gh)^{-1}a(gh) = h^{-1}(g^{-1}ag)h = h^{-1}bh = b$, hiszen $h \in C_G(b)$.

3.1.6. Definíció. *Legyen G véges csoport, és p prímszám, mely osztja G rendjét. Legyen $N \lhd G$, melynek rendje a G-beli p-Sylowok indexe. Ekkor N-et a G normál p-komplementumának nevezzük.*

3.1.7. Tétel. *(Burnside) Legyen G véges csoport, melynek p-Sylowja benne van saját normalizátorának centrumában. Ekkor G-ben van normál p-komplementum.*

3.1.8. Megjegyzés. *A tétel feltétele (P benne van a normalizátorának centumában) $\Leftrightarrow N_G(P) = C_G(P)$, hiszen mindkettő azt fejezi ki, hogy P elemei pontosan $N_G(P)$ elemeivel cserélhetők fel.*

Bizonyítás: (tétel) Legyen a feltételben adott p-Sylow részcsoport P. Mivel $P \subset C_G(P)$, így a feltételből következik, hogy P Abel. Tekintsük a $\tau_{G\to P}$ transzfert. Ekkor $P' = 1$ mert P Abel, és vegyünk egy $g \in P$ elemet a Sylow részcsoportból. Az 3.1.4 Lemmát alkalmazva $\tau(g) = \prod x_{i_r} g^{\lambda_r} x_{i_r}^{-1}$, ahol g^{λ_r} és konjugáltja $x_{i_r} g^{\lambda_r} x_{i_r}^{-1}$ is P-beli. Az előző lemma szerint $N_G(P)$-ben is konjugáltak, és a feltevésünk szerint P elemei felcserélhetők az $N_G(P)$ normalizátor elemeivel, így $x_{i_r} g^{\lambda_r} x_{i_r}^{-1} = g^{\lambda_r}$. Felhasználva ezt az összefüggést a $\tau(g) = \prod x_{i_r} g^{\lambda_r} x_{i_r}^{-1} = \prod g^{\lambda_r} = g^{\sum \lambda_r} = g^{|G:P|}$, ahol a kitevő relatív prím p-hez. Ezért létezik olyan k, hogy $k|G:P| \equiv 1 \mod |P|$, így bármely $x \in P$ esetén $\tau(x^k) = x^{k|G:P|} = x$, tehát τ ráképez P-re ($Im\tau = P$). Legyen $N = \ker \tau$ a leképezés magja. Ekkor N normálosztó G-ben, és a homomorfizmus tétel miatt $|G|/|N| = |P|$, amiből azonnal adódik, hogy N indexe relatív prím p-hez, vagyis N normál p-komplementum.

3.1.9. Lemma. *Legyen $H \leq G$. Ekkor $N_G(H)/C_G(H)$ izomorf H automorfizmus csoportjának egy részcsoportjával.*

Bizonyítás: Az $N_G(H)$ normalizátor bármely eleme meghatároz egy automorfizmust a H csoporton a vele való konjugálás által. Vegyük ezt a $N_G(H) \to Aut(H)$ leképezést. Világos, hogy ennek magja $C_G(H)$, így a homomorfizmus tételből adódik az állítás.

3.1.10. Következmény. *Legyen G véges csoport rendjének legkisebb prím osztója p. Ha G p-Sylow részcsoportja ciklikus, akkor G-ben van normál p-komplementum.*

Bizonyítás: Legyen P az egyik ciklikus p-Sylow részcsoport. Mivel P ciklikus, így Abel, tehát $P \leq C_G(P)$. Így $|N_G(P)/C_G(P)| = |N_G(P)|/|C_{G(P)}|$ nem osztható p-vel, de mivel p volt a $|G|$ legkisebb prímosztója, így p-nél kisebb prímekkel sem osztható. Ugyanakkor $|Aut(P)| = \varphi(|P|) = (p-1)|P|/p$, így az előző lemma miatt $|N_G(H)/C_G(H)|$-nek p-nél nagyobb prímosztója sincsen, tehát $N_G(P) = C_G(P)$, azaz a Burnside tétel alkalmazható.

3.1.11. Következmény. *Ha egy véges csoport összes Sylow-részcsoportja ciklikus, akkor feloldható.*

Bizonyítás: Alkalmazzunk indukciót $|G|$ különböző prímosztóinak számára. Ha G p-csoport, akkor feloldható. Ha G rendjének több prímosztója is van, akkor az előző következmény miatt G-ben van normál p-komplementum, jelölje ezt N (p a legkisebb prímosztója $|G|$-nek). A G/N p-csoport feloldható, N az indukciós feltevés miatt feloldható, így G is feloldható.

3.1.12. Megjegyzés. *Mivel az indukció során növekvő sorrendben megyünk végig $|G|$ prímosztóin, a bizonyítás akkor is működik, ha a legnagyobb prímosztó Sylow-ja nem ciklikus, hiszen minden prímhatvány rendű csoport feloldható*

3.1.13. Tétel. *Ha a G véges csoport rendje négyzetmentes, akkor a csoport feloldható.*

Bizonyítás: A 3.1.11 Következmény speciális esete, hiszen minden Sylow részcsoport ciklikus.

3.2. Modulusok, reprezentációk

Az alábbi fejezetben egy másik feloldható csoportokra vonatkozó tétel bizonyítunk, miszerint ha egy véges csoport rendjének legfeljebb kettő prímosztója van, akkor feloldható. A tétel bizonyításához azonban szükségünk az egyik legerősebb csoportelméleti eszközre, a reprezentáció elméletre. Ebben az alfejezetben gyorsan végigmegyek a reprezentációk modulus elméleti alapjain, de az állításokat csak bizonyítás nélkül hozom. A most következő három alfejezet tartalma fellelhető Martin Isaacs *Character Theory of Finite Groups* című művében.

3.2.1. Definíció. *Legyen F test, és legyen A egy vektortér, ami egyúttal egységelemes gyűrű is. Tegyük fel, hogy minden $c \in F$-re, és $x, y \in A$-ra teljesül:*

$$c(xy) = (cx)y = x(cy)$$

Ekkor A-t F feletti algebrának nevezzük.

Legyen G véges csoport. Ekkor $F[G]$ legyen $\sum_{g \in G} a_g g$ formális összegek halmaza, ahol $a_g \in F$. Erre tekinthetünk úgy, mint egy F feletti vektortérre, melyben az az elem, amire $a_g = 1$, $a_h = 0$, $g \neq h$ teljesül, azonosítható g-vel. Ez az azonosítás beágyazza G-t $F[G]$-be, ráadásul G elemei egy bázisát adják $F[G]$-nek. Az azonosítás egy új értelmet is adott a $\sum a_g g$ összegeknek, hiszen most már tekinthetünk rájuk, mint valódi összegekre, mint a bázis vektorok lineáris kombinációira. Végül definiálható a szorzás is $F[G]$ elemein. A bázis vektorok szorzata legyen G-beli szorzatuk, és ez a szorzás lineárisan kiterjeszthető $F[G]$ elemeire is. Könnyen ellenőrizhető, hogy $F[G]$ az imént definiált szorzással F feletti algebra.

Mivel a továbbiakban csak véges algebrákkal fogunk dolgozni, ezért algebrán véges algebrát fogok érteni.

3.2.2. Definíció. *Legyen A, B F feletti algebra, és tegyük fel, hogy $\varphi : A \to B$-re teljesülnek a következők:*

a) $\varphi(xy) = \varphi(x)\varphi(y)$ minden $x, y \in A$

b) $\varphi(1) = 1$

c) φ F-lineáris transzformáció

Ekkor φ algebra homomorfizmus.

3.2.3. Definíció. *Legyen A F feletti algebra, és legyen V véges dimenziós F feletti vektortér. Tegyük fel, hogy létezik olyan $V \times A \to V$ leképezés, ami $\forall x, y \in A$,$\forall v.w \in \in V$,$\forall c \in F$-re kielégíti a következő tulajdonságokat:*

a) $(v + w)x = vx + wx$

b) $v(x + y) = vx + vy$

c) $(vx)y = v(xy)$

d) $(cv)x = c(vx) = v(cx)$

e) $v1 = v$

Ekkor V egy A feletti modulus.

Legyen A F feletti algebra. Tekinthetünk A-ra F feletti véges dimenziós vektortérként. Nyilvánvaló, hogy az algebrán vett jobbról szorzás kielégíti a modulus definíciójában megadott leképezést, tehát tekinthetünk A-ra, mint önmaga feletti modulusra. Az így megadott modulust reguláris modulusnak nevezzük, és $\tilde{A}$-vel jelölöm.

3.2.4. Definíció. *Legyen V, W A feletti modulusok, és legyen adva $\varphi : V \to W$ lineáris leképezés, amire $\varphi(va) = \varphi(v)a$ teljesül. Ekkor φ A feletti modulus homomorfizmus.*

Az A feletti $V \to W$ modulus homomorfizmusok halmaza $Hom_A(V, W)$. Ezek meghatároznak egy F-lineáris struktúrát, hiszen tetszőleges $\varphi, \psi \in Hom_A(V, W)$ esetén $\varphi(v) + \psi(v) = (\varphi + \psi)(v)$ és $\varphi(cv) = c\varphi(v)$ nyilvánvalóan teljesül $\forall v \in V$ és $c \in F$ esetén. A $Hom(V, V)$ téren szorzás is definiálható, $\varphi\psi(v) = \varphi(\psi(v))$ módon, tehát $Hom(V, V)$ F feletti algebra. Jelölje $\mathbf{E}_A(V)$ az így meghatározott algebrát.

3.2.5. Definíció. *Legyen V nemnulla A feletti modulus. Ha V-nek csak a 0 és V a részmodulusai, akkor V irreducibilis modulus.*

Nyilvánvaló, hogy ha $\varphi \in Hom(V, W)$, akkor $\ker \varphi$, és $Im\varphi$ részmodulusa V-nek illetve W-nek.

3.2.6. Lemma. *(Schur) Ha V és W irreducibilis A feletti modulusok, akkor minden nemnulla $Hom(V, W)$-beli elemnek van inverze $Hom(W, V)$-ben.*

A lemmából nyilvánvaló, hogy $Hom(V, V)$ minden eleme invertálható.

3.2.7. Lemma. *Legyen F algebrailag zárt test, és legyen A F feletti algebra, V pedig irreducibilis A feletti modulus. Ekkor $\mathbf{E}_A(V) = c \cdot I$, valamely $c \in F$ esetén.*

3.2.8. Definíció. *Legyen V A feletti modulus. Tegyük fel, hogy minden $W \subseteq V$ részmodulus esetén létezik olyan $U \subseteq V$ részmodulus, hogy $V = W \bigoplus U$. Ekkor a V modulus teljesen lebontható.*

3.2.9. Definíció. *Az A algebra félig egyszerű, ha $\tilde{A}$ reguláris modulus teljesen lebontható.*

3.2.10. Tétel. *(Maschke) Legyen G véges csoport, V $F[G]$ modulus, ahol F karakterisztikája nem osztja G rendjét. Ekkor V teljesen lebontható.*

3.2.11. Lemma. *Legyen V modulus az A algebra felett. A következő tulajdonságok ekvivalensek:*

a) V teljesen lebontható

b) $V = \sum V_\alpha$, ahol V_α irreducibilis modulus minden α-ra, azaz irreducibilis modulusok összege.

c) $V = \bigoplus V_\alpha$, ahol V_α irreducibilis modulus minden α-ra, azaz irreducibilis modulusok direkt összege.

3.2.12. Definíció. *Legyen V teljesen lebontható A feletti modulus, és legyen M irreducibilis A feletti modulus. A V M-homogén részén a V-beli M-el izomorf részmodulusok összegét értjük, és $M(V)$-vel jelöljük.*

3.2.13. Lemma. *Legyen $V = \bigoplus W_i$, ahol W_i irreducibilis A feletti modulus minden i-re. Legyen M irreducibilis A feletti modulus.*

a) $M(V) = \{\sum W_i | W_i \simeq M\}$

b) Az M-hez izomorf W_i-k száma, amit $n_M(V)$ jelöl, nem függ a V irreducibilis modulusok direkt összegére való felbontásától.

3.2.14. Lemma. *Legyen A F feletti algebra. Ekkor minden irreducibilis A feletti modulus izomorf az $\tilde{A}$ egy faktormodulusával. Ha az A algebra féligegyszerű, akkor $\tilde{A}$ egy részmodulusával is izomorfak.*

Mivel A véges dimenziós, így a lemma egyszerű következménye, hogy A feletti irreducibilis modulusokból csak véges sok lehet.

3.2.15. Tétel. *(Wedderburn) Legyen A féligegyszerű algebra, és legyen M irreducibilis A feletti modulus.*

a) $M(A)$ minimális ideál A-ban.

b) Ha W irreducibilis, akkor $W \simeq M$, vagy annulál $M(A)$-val.

3.2.16. Lemma. *Legyen A féligegyszerű algebra az algebrailag zárt F test fölött, és legyen M irreducibilis A feletti modulus. Továbbá jelölje $\mathcal{M}(A)$ az A feletti irreducibilis modulusok egy reprezentáns halmazát. Ekkor teljesülnek a következők:*

a) $n_M(\tilde{A}) = \dim(M)$

b) $\dim(A) = \sum_{M \in \mathcal{M}(A)} (\dim M)^2$

c) $\dim Z(A) = |\mathcal{M}(A)|$

Most végre el kezdhetünk foglalkozni a reprezentációk elméletével.

3.2.17. Definíció. *Legyen A F feletti algebra. Az A n-ed fokú reprezentációján $\mathfrak{X}$: : $A \to GL(n,F)$ algebra homomorfizmust értjük. $\mathfrak{X}$ és $\mathfrak{Y}$ reprezentációk hasonlók, ha létezik P nem szinguláris $n \times n$-es mátrix, amire $P^{-1}\mathfrak{X}(a)P = \mathfrak{Y}(a)$ minden $a \in A$.*

Nyilvánvaló, hogy a reprezentációk közötti hasonlóság ekvivalencia relációt ad meg a reprezentációk között.

Könnyű megmutatni, hogy a modulusokból felépíthetők a reprezentációk, és a reprezentációkból a modulusok. Ugyanis legyen először A F feletti algebra, $\mathfrak{X}$ az A egy n-ed fokú reprezentációja. Az F feletti n dimenziós sorvektorok egy F feletti n-dimenziós V vektorteret határoznak meg. Legyen $v \in V$, és definiáljuk a szorzást a $v \cdot a = v\mathfrak{X}(a)$ képlettel. Könnyen ellenőrizhető, hogy az így definiált szorzással V egy A feletti modulus lesz.

Megfordítva legyen adva az F feletti A algebra, és a V A feletti modulus. Vegyük V egy bázisát, és írjuk fel ebben a bázisban a_V-t. Legyen $\mathfrak{X}(a) = a_V$. Könnyű ellenőrizni, hogy az így kapott függvény valóban A egy reprezentációját adja.

Tegyük fel, hogy V és W A feletti modulusok, és legyen $\varphi \in Hom(V,W)$. Tekintsük V és W egy-egy bázisát, legyenek ezek e_v, és e_w. Mivel φ lineáris leképezés ezért megadható a mátrixa az a e_v és e_w bázisokon. Mivel $\varphi(va) = \varphi(v)a$ fennáll $\forall v \in V$ és $\forall a \in A$, így $\mathfrak{X}(a)P = P\mathfrak{Y}(a)$, ahol $\mathfrak{X}$ és $\mathfrak{Y}$ az e_v és e_w bázisok által V-n és W-n meghatározott reprezentáció. Ha φ modulus izomorfizmus, akkor P nem szinguláris mátrix, és az előbbi mátrix egyenletből $\mathfrak{X} \simeq \mathfrak{Y}$. Tehát a modulus különböző bázisai által meghatározott reprezentációk hasonlóak.

Az előző gondolatmenet megfordítható, azaz ha a V és W modulusok e_v és e_w bázisai által meghatározott reprezentációk hasonlók, akkor V és W izomorfak. Tehát megadható egy kölcsönösen egyértelmű megfeleltetés az A algebra feletti izomorf modulusok, és hasonló reprezentációi között.

Legyen V A algebra feletti modulus, és $W < V$. Válasszuk W-nek az e_w bázisát, ez kiegészíthető V e_v bázisává. Legyen $\mathfrak{X}$ az A egy reprezentációja, ami a V modulus e_v bázisához tartozik, és legyen $\mathfrak{Y}$ a W e_v bázisához tartozó reprezentáció. Könnyen megmutatható, hogy $\forall a \in A$-ra teljesül:

$$\mathfrak{X}(a) = \begin{pmatrix} \mathfrak{Z}(a) & \mathfrak{U}(a) \\ 0 & \mathfrak{Y}(a) \end{pmatrix}$$

Továbbá $\mathfrak{Z}$ egy V/W-nek megfelelő reprezentáció. Ha $\mathfrak{X}$ az előbbi alakban írható, akkor azt mondjuk, hogy $\mathfrak{X}$ lebontható. Tehát az irreducibilis modulusokhoz irreducibilis reprezentációk tartoznak. Ha $W \subseteq V$-hez létezik olyan $U \subseteq V$, hogy $W \bigoplus U = V$, akkor W bázisa kiterjeszthető V bázisává, az U bázisának elemeit

hozzávéve. Ilyenkor $\mathfrak{U}(a) = 0$ minden $a \in A$ esetén. Tehát ha az $\mathfrak{X}$ reprezentáció egy teljesen lebontható modulushoz tartozik, akkor $\mathfrak{X}$ hasonló egy blokkdiagonális reprezentációhoz, ahol minden blokk egy irreducibilis reprezentáció.

Választhatjuk algebrának az $F[G]$ F feletti algebrát. Mivel a reprezentáció algebra homomorfizmus, így lineáris is. Tehát ha a reprezentációt megadom az algebra egy bázisán, akkor megadtam magán az algebrán is. $F[G]$-nek G bázisa, tehát elég a reprezentációt G elemein megadni. Így értelmezhető G reprezentációja is.

3.2.18. Definíció. *Legyen G csoport és F test. Ekkor a $X : G \to GL(n, F)$ homomorfizmust F feletti, n-edfokú reprezentációnak nevezzük.*

Tegyük fel, hogy $F = \mathbb{C}$. Mivel $\mathbb{C}$ karakterisztikája 0, így Maschke tétele miatt $\mathbb{C}[G]$ féligegyszerű. Továbbá $\mathbb{C}$ algebrailag zárt, így alkalmazni tudjuk a fejezetben bizonyított tételeket.

3.3. Karakterek

Ha G az $\mathfrak{X}$ n-ed fokú reprezentációja, akkor $|G|$ darab mátrix, vagyis összesen $n^2|G|$ szám megadását jelenti. Azonban ezen számok nagy része nem ad új információt, mert csak a hasonló reprezentációk megkülönböztetésére szolgál. Habár a reprezentáló mátrixok nyoma sokkal kevesebb információt tartalmaz, mégis elegendően sokat, hogy a különböző reprezentációkat meg tudjuk különböztetni. Jelölje az A mátrix nyomát $tr(A)$.

3.3.1. Lemma. *Legyen $A, B \in M_n(F)$, ekkor $tr(AB) = tr(BA)$. Ha $P \in GL(n, F)$, akkor $tr(P^{-1}AP) = tr(A)$.*

3.3.2. Definíció. *Az $\mathfrak{X}$ reprezentáció karaktere a $\chi(g) = tr(\mathfrak{X}(g))$ összefüggéssel meghatározott függvény.*

Ahogy a reprezentáció is kiterjed az egész csoportalgebrára, úgy a karakter is kiterjeszthető F-re. A karakter a reprezentációval ellentétben általában nem homomorfizmus. Azonban ha $\mathfrak{X}$ reprezentáció elsőfokú, akkor ennek λ karakterére $\mathfrak{X}(g) = \lambda(g)$, tehát λ homomorfizmus lesz. Az elsőfokú reprezentációhoz tartozó karaktert lineáris karakternek szokás nevezni.

3.3.3. Lemma. *A következő igazak:*

a) Hasonló reprezentációkhoz tartozó karakterek megegyeznek.

b) A karakter konstans a konjugált osztályokon.

Bizonyítás: Az a) állítás nyilvánvaló a 3.3.1 Lemma miatt. A b) állításhoz vegyük az $\mathfrak{X}$ F feletti reprezentációt. Mivel $\mathfrak{X}(g^{-1}hg) = \mathfrak{X}(g^{-1})\mathfrak{X}(h)\mathfrak{X}(g)$, így $tr(g^{-1}hg) = tr(h)$ szintén a 3.3.1 Lemma miatt.

Még egy általános észrevétel. Ha $\mathfrak{X}$ és $\mathfrak{Y}$ mindketten F feletti reprezentációi a G csoportnak, akkor

$$\mathfrak{Z}(g) = \begin{pmatrix} \mathfrak{X}(g) & 0 \\ 0 & \mathfrak{Y}(g) \end{pmatrix}$$

szintén F feletti reprezentációja G-nek. Mivel a reprezentációk nyomaira fennáll $tr(\mathfrak{Z}) = tr(\mathfrak{X}) + tr(\mathfrak{Y})$, így a G csoport F feletti karaktereinek halmaza zárt az összeadásra.

A továbbiakban már csak az $F = \mathbb{C}$ esetben vizsgáljuk a reprezentációkat. Legyen G rögzített véges csoportot. Mivel G véges, az a $\mathbb{C}[G]$ algebra is véges dimenziós, tehát véges sok $\mathbb{C}[G]$ feletti modulus van, vegyük ezek egy reprezentatív halmazát, jelölje ezt $\mathcal{M}(\mathbb{C}[\mathbb{G}]) = \{M_1, ..., M_k\}$. Válasszunk mindegyik reprezentáns irreducibilis modulusban egy bázist, ezek meghatároznak egy-egy reprezentációt, legyenek ezek $\mathfrak{X}_1, ..., \mathfrak{X}_k$. Legyen az $\mathfrak{X}_i$-hez tartozó karakter χ_i. Ekkor $Irr(\mathbb{C}[G]) = \{\chi_1, ...\chi_k\}$ az irreducibilis $\mathbb{C}$ feletti karakterek halmaza (karakter irreducibilis, ha az őt meghatározó reprezentáció irreducibilis).

Mivel karakterek összege is karakter, így a $\chi = \sum_{i=1}^{k} n_i\chi_i$ is karakter, ha n_i nemnegatív egészek nem mind 0-k. Megfordítva, ha adott a G csoport $\mathfrak{X}$ reprezentációhoz tartozó χ karaktere, akkor az $\mathfrak{X}$ reprezentációhoz tartozzon a V modulus. V lebomlik irreducibilis modulusok direkt összegére, így a χ karakter is felírható irreducibilis karakterek összegeként, azaz $\chi = \sum n_i\chi_i$.

A 3.2.16 lemma alapján $\dim(\mathbb{C}[G]) = \sum_{i=1}^{k}(\dim M_i)^2$. Mivel $\dim(\mathbb{C}[G]) = |G|$, és $\dim M_i = deg\mathfrak{X}_i = \chi(1)$, így fennáll

$$|G| = \sum_{i=1}^{k} \chi_i(1)^2$$

Jogos a kérdés, hogyan tudjuk meghatározni az irreducibilis karakterek számát. A 3.2.16 Lemma c) részéből már tudjuk, hogy $|\mathcal{M}(\mathbb{C}[G])| = \dim Z(\mathbb{C}[G])$. A következő tétel segítségével azonban közvetlenül a csoport ismeretében megmondható az irreducibilis karakterek száma.

3.3.4. Tétel. *Legyen G véges csoport, és legyenek $\mathcal{K}_1, ..., \mathcal{K}_r$ a G-beli konjugált osztályok. Továbbá legyen $K_i = \sum_{x \in \mathcal{K}_i} x$ ($K_i \in \mathbb{C}[G]$), azaz a $\mathcal{K}_i$ konjugált osztályon 1, azon kívül 0. Ekkor $\{K_1, ..., K_r\}$-k bázis $Z(\mathbb{C}[G])$-ben, továbbá ha $K_iK_j = \sum a_{ijv}K_v$, akkor az a_{ijv} nemnegatív egész.*

Bizonyítás: Világos, hogy $K_i \in Z(\mathbb{C}[G])$, hiszen K_i felcserélhető tetszőleges $g \in$ $\in G$-vel. Továbbá K_i-k függetlenek, hiszen diszjunkt halmazok elemeit adjuk össze. Ha $z = a_g g \in Z(\mathbb{C}[G])$, akkor $z = h^{-1}zh = \sum a_g g^h$. Összehasonlítva a g^h együtthatóit z kétfajta felírásában, adódik, hogy $a_g = a_{g^h}$, azaz z együtthatója konstans $g \in K_i$ konjugált osztály elemein. Ez tetszőleges $g \in G$-re fennáll, így z előáll K_i-k lineáris kombinációjaként, tehát K_i-k kifeszítik $Z(\mathbb{C}[G])$-t.

Az a_{ijv} meghatározásához legyen $g \in K_v$ tetszőleges. Ekkor a_{ijv} a g együtthatója a K_iK_j szorzatban. A $\mathbb{C}[G]$-beli szorzás definiciójából

$$a_{ijv} = |\{(x, y)|x \in K_i, y \in K_j, xy = g\}|,$$

azaz a_{ijv} egy halmaz számossága, és így nemnegatív egész.

3.3.5. Következmény. *A $\mathbb{C}[G]$ feletti, egymáshoz nem hasonló irreducibilis reprezentációk száma megegyezik G konjugált osztályainak számával.*

3.3.6. Következmény. *A G csoport akkor és csak akkor Abel, ha minden irreducibilis karaktere lineáris.*

Bizonyítás: Ha G Abel, akkor a konjugált osztályainak száma $|G|$, vagyis az irreducibilis karaktere száma $|G|$. A $|G| = \sum_{i=1}^{k} \chi_i(1)^2$ csak akkor állhat fenn, ha $\chi_i(1) = 1$ minden karakterre.

A megfordítás ugyanígy megy, ha minden karakter lineáris, akkor $|G| = \sum_{i=1}^{k} \chi_i(1)^2$ összefüggésből az irreducibilis karakterek száma $|G|$, vagyis G minden konjugált osztálya 1 elemű, és ezzel be is láttuk az állítást.

Még nem bizonyítottuk, hogy χ_i irreducibilis karakterek különbözők. Ennek belátásához segítségül hívunk egy korábbi állítást.

$$\mathbb{C}[G] = \bigoplus_{i=1}^{k} M_i(\mathbb{C}[G])$$

Ez alapján $1 = \sum e_i$, ahol $e_i \in M_i([G])$. Korábban már láttuk, hogy ha $i \neq j$, akkor az $M_j(\mathbb{C}[G])$ modulus annulálja $M_i(\mathbb{C}[G])$-t, így $\mathfrak{X}_i(e_j) = 0$. Ennek egyszerű következménye, hogy $\mathfrak{X}_i(e_i) = \mathfrak{X}(1) = I$. Mivel $\chi_i(e_j) = 0$ ha $i \neq j$, és $\chi_i(e_i) =$ $= \chi(1) \neq 0$, tehát a χ_i-k különböző függvények $\mathbb{C}[G]$-n, és így a χ_i-k a G-n is különböző függvények.

3.3.7. Definíció. *A $\phi : G \to \mathbb{C}$ függvényt osztályfüggvénynek nevezzük, ha konstans G konjugált osztályain.*

Nyilvánvaló, hogy a karakterek is osztályfüggvények, de ennél többet is megállapíthatunk róluk.

3.3.8. Tétel. *A következők teljesülnek:*

a) Ha ϕ osztályfüggvény, akkor $\phi = \sum_{\chi \in Irr(G)} a_\chi \chi$, ahol $a_\chi \in \mathbb{C}$.

b) A ϕ osztályfüggvény karakter, akkor és csak akkor, ha a_χ nem negatív egész minden $\chi \in Irr(G)$-re, és $\phi \neq 0$.

Bizonyítás: Az osztályfüggvények vektorteret alkotnak alkotnak $\mathbb{C}$ fölött, és ennek dimenziója a konjugált osztályok száma, ami megegyezik az irreducibilis karakterek számával. Már csak azt kell bizonyítani, hogy az irreducibilis karakterek lineárisan függetlenek, azaz ha $\sum a_\chi \chi = 0$, akkor $a_\chi = 0$ minden $\chi \in Irr(G)$ esetén. Ha egy pillanatra G-t kiterjesszük $\mathbb{C}[G]$-re, és a $\sum a_\chi \chi = 0$ egyenletbe sorban behelyettesítjük e_i-t minden i-re, akkor kapjuk, hogy $a_{\chi_i} = 0$. Mivel a kiterjesztés lineáris volt, így az a) állítással kész is vagyunk. A b) állítás pedig már korábban láttuk.

3.3.9. Következmény. *Legyen $\mathfrak{X}$ és $\mathfrak{Y}$ két $\mathbb{C}$ feletti reprezentációja a G csoportnak. Akkor és csak akkor hasonlók, ha ugyanaz a karakter tartozik hozzájuk.*

Bizonyítás: Az állítás egyik felét már láttuk. A megfordításhoz legyen $\mathfrak{X}$ karaktere $\sum n_{M_i}(V)\chi_i$, és a $\mathfrak{Y}$ karaktere pedig $\sum n_{M_i}(W)\chi_i$, ahol V és W a $\mathfrak{X}$, és $\mathfrak{Y}$ reprezentációkhoz tartozó modulus. A karakterek megegyeznek, így $\sum n_{M_i}(V)\chi_i = \sum n_{M_i}(W)\chi_i$. Az egyenlőség csak úgy állhat fenn, ha $n_{M_i}(V) = n_{M_i}(W)$ minden i-re, vagyis V és W ugyanazon irreducibilis modulusok direkt összege, tehát izomorfak egymással. Így a hozzájuk tartozó reprezentációk hasonlóak.

Tekintsük a $\widetilde{\mathbb{C}[\mathbb{G}]}$ reguláris modulust. Ehhez is megfeleltethető egy $\mathbb{C}$ feletti reprezentáció, és legyen ρ az ehhez tartozó karakter, amit *reguláris karakternek* nevezünk. Következőkben hasznos lesz ρ-t kétféleképpen is kiszámítani.

3.3.10. Lemma. *Ha $g \in G$ és $g \neq 1$, akkor $\rho(g) = 0$, és $\rho(1) = |G|$.*

Bizonyítás: Tekintsük a csoportalgebrának azt a bázisát, mely G elemeiből áll. Ekkor $\mathfrak{X}$ a g-vel való jobbról szorzás mátrixát adja, és mivel tetszőleges $h \in G$-re $hg = h$ csak $g = 1$ esetben áll fenn, így ha $g \neq 1$, akkor a főátlóban csupa 0 van, tehát $\rho(g) = 0$. Ha $g = 1$, akkor pedig minden főátlóbeli elem 1 lesz, azaz $\rho(1) = |G|$.

3.3.11. Lemma. $\rho = \sum_{\chi \in Irr(G)} \chi_1(1)\chi$

Bizonyítás: Ha V $\mathbb{C}[G]$ feletti modulus, akkor V lebontható irreducibilis modulusok direkt összegére. A V-nek megfelelő reprezentációhoz tartozó karakter tehát $\sum n_{M_i}(V)\chi_i$. Azt meg már láttuk, hogy $n_{M_i}(\widetilde{\mathbb{C}[G]}) = \dim(M_i) = \chi_i(1)$.

3.3.12. Lemma. *Legyen $\mathfrak{X}$ a G csoport egy reprezentációja, a $\mathfrak{X}$-hez tartozó karakter pedig χ. Legyen $g \in G$ tetszőleges, és g rendje pedig n.*

a) $\mathfrak{X}(g)$ hasonló olyan diagonális mátrixhoz, melynek főátlójában lévő elemek $\varepsilon_1, ..., \varepsilon_n$.

b) $\varepsilon_i^n = 1$

c) $\chi(g) = \sum_{i=1}^{n} \varepsilon_i$, és $|\chi(g)| \leq \chi(1)$. Az utóbbi esetén az egyenlőség pontosan akkor áll fenn, ha $\varepsilon_1 = \varepsilon_2 = ... = \varepsilon_n$.

d) $\chi(g^{-1}) = \overline{\chi(g)}$

Bizonyítás: A $\mathfrak{X}$ reprezentáció megszorítása a $< g >$ részcsoportra a $< g >$-nek is egy reprezentációját adja, ezért elég a $G =< g >$ esetre belátni. A reprezentáció hasonló egy blokk diagonális mátrixhoz, melynek a blokkjaiban irreducibilis reprezentációk vannak. Mivel G ciklikus, így Abel, ezért a 3.3.9. Következmény miatt minden irreducibilis karaktere lineáris. Tehát a blokkok 1×1-es mátrixok, és ezzel az a) állítást beláttuk.

Mivel a g elem rendje n, így $\mathfrak{X}(g)^n = \mathfrak{X}(g^n) = \mathfrak{X}(1) = I$, amiből a b) is azonnal adódik.

Diagonális mátrix esetén a mátrix nyoma a főátlóban lévő elemek összege. A $\chi(g) = \sum_{i=1}^{n} \varepsilon_i$ összefüggésre alkalmazva a háromszög egyenlőtlenséget, kapjuk $|\chi(g)| \leq$ $\leq \chi(1)$-t. A háromszög egyenlőtlenségben egyenlőség pontosan akkor áll fenn, ha a vektorok egy irányba mutatnak, tehát $\varepsilon_1 = \varepsilon_2 = ... = \varepsilon_n$.

$\mathfrak{X}(g)$ diagonális felírásában az egységgyökök vannak a főátlóban, $\mathfrak{X}(g)^{-1}$ esetén pedig ezek reciprokai. Az egységgyökök reciprokai saját konjugáltjuk, ezeket összeadva pedig kapjuk $\chi(g^{-1}) = \overline{\chi(g)}$-t.

3.3.13. Lemma. *Legyen a $\mathfrak{X}$ reprezentáció karaktere χ. $\chi(g) = \chi(1)$ akkor és csak akkor, ha $g \in \ker \mathfrak{X}$ fennáll.*

Bizonyítás: Először legyen $\chi(g) = \chi(1)$. Ekkor az előző lemma c) állítása miatt, ha a $\mathfrak{X}(g)$-hoz hasonló, diagonális mátrixú reprezentációban $\varepsilon_1, ..., \varepsilon_n$ elemek vannak a főátlóban, akkor $\varepsilon_1 = \varepsilon_2 = ... = \varepsilon_n$. Tehát $\chi(g) = n\varepsilon_1$, $\chi(1) = n$, $\epsilon_1 = 1$, azaz $\mathfrak{X}(g) = I$.

A megfordítás nyilvánvaló, hiszen $g \in \ker \mathfrak{X}$ esetén $\mathfrak{X}(g) = I = \mathfrak{X}(1)$.

3.3.14. Definíció. *Legyen χ a G egy karaktere.* $\ker \chi = \{g \in G | \chi(g) = \chi(1)\}$.

3.3.15. Lemma. *Legyen χ a G $\mathfrak{X}$ reprezentációjához tartozó karakter, és legyen $\chi = \sum_{\chi \in Irr(G)} n_i \chi_i$.*

a) $\ker\chi = \bigcap\{\ker\chi_i | n_i > 0\}$.

b) $\bigcap\limits_{\chi_i\in Irr(G)} \ker\chi = 1$

Bizonyítás: $|\chi_i(g)| \leq \chi(1)$ a 3.3.12 Lemma miatt, és $\chi(g) = \chi(1)$, tehát $\chi_i(g) = \chi(1)$, ha $n_i \neq 0$. A fordított tartalmazás nyilvánvaló.

A b) állítás bizonyításához vegyük a ρ reguláris karaktert. A 3.3.10. Lemma miatt $\ker\rho = 1$, továbbá a 3.3.11. lemma miatt $\rho = \sum\limits_{\chi\in Irr(G)} \chi(1)\chi_i$. $\chi_i(1) \neq 0$ minden i-re, így az állítás a) feléből következik $\bigcap\limits_{\chi\in Irr(G)} \ker\chi = \ker\rho = 1$.

3.3.16. Megjegyzés. *Mivel* $\ker\chi = \ker\mathfrak{X}$ *normálosztó* G*-ben, így* G *csoport pontosan akkor egyszerű, ha* $\ker\chi = 1$ *minden nemtriviális irreducibilis karakterre.*

3.3.17. Lemma. *Legyen* $\mathfrak{X}$ *a* G *csoport* n*-ed fokú irreducibilis reprezentációja,* A *pedig* $\mathbb{C}$ *feletti* $n \times n$*-es mátrix, ami felcserélhető* $\mathfrak{X}(g)$*-vel minden* $g \in G$ *esetén. Ekkor* $A = cI$ *valamely* $C \in \mathbb{C}$*-re.*

Bizonyítás: Legyen M n dimenziós sorvektor $\mathbb{C}$ fölött. Ekkor M tekinthető $\mathbb{C}[G]$ feletti irreducibilis modulusnak, amin a szorzást a $m \cdot a = m\mathfrak{X}(a)$ $m \in M$,$a \in \mathbb{C}[G]$ összefüggés definiálja. Legyen $\vartheta : M \to M$ homomorfizmus, amire $m\vartheta = mA$. Mivel $(ma)\vartheta = (m\mathfrak{X}(a))A = (mA)\mathfrak{X}(a) = (m\vartheta)a$, így ϑ modulus homomorfizmus, azaz $\vartheta \in \mathbf{E}_{\mathbb{C}[G]}(M)$. Mivel $\mathbb{C}$ algebrailag zárt test, így a 3.2.7. Lemma alapján $\mathbf{E}_{\mathbb{C}[G]}(M) = \mathbb{C} \cdot 1$, amiből $\vartheta = \gamma \cdot 1$, $\gamma \in \mathbb{C}$.

3.3.18. Definíció. *Legyen* χ *a* G *csoport karaktere. Ekkor* $Z(\chi) = \{g \in G \mid |\chi(g)| = \chi(1)\}$.

3.3.19. Lemma. *Legyen* $\mathfrak{X}$ *a* G *reprezentációja,* χ *a reprezentációhoz tartozó karakter. Jelölje* $Z = Z(\chi)$.

a) $Z = \{g \in G \mid \mathfrak{X}(g) = \varepsilon I, \varepsilon \in \mathbb{C}\}$

b) $Z/\ker\chi \subseteq Z(G/ker\chi)$

c) Ha χ *irreducibilis, akkor* $Z/ker\chi = Z(G/ker\chi)$

Bizonyítás: A 3.3.12. lemma a) része szerint $\mathfrak{X}(g)$ mátrixa hasonló a diagonálishoz, melynek főátlójában lévő elemek egységnyi abszolútértékűek. Ha $g \in Z$, akkor ugyanezen lemma c) része miatt pedig egyenlők, tehát $\mathfrak{X}(g)$ skalár mátrix. Viszont a skalár mátrixhoz csak önmaga hasonló.

$Z/\ker\chi = Z/\ker\mathfrak{X} \simeq \mathfrak{X}(Z)$, $Z(G/\ker\chi)Z(G/\ker\mathfrak{X}) \simeq Z(\mathfrak{X}(G))$ a homomorfizmus tétel miatt. Mivel $\mathfrak{X}(Z)$ elemei diagonálisok, így felcserélhetők $\mathfrak{X}(g)$-vel minden $g \in G$ esetén, tehát $\mathfrak{X}(Z) \subseteq Z(\mathfrak{X})(G)$.

Legyen most χ irreducibilis karakter és $g\ker\chi \in Z(G/\ker\chi)$. Ekkor $\mathfrak{X}(g) \in Z(\mathfrak{X}(G)$ is teljesül, tehát alkalmazható a 3.3.17. Lemma. Így $\mathfrak{X}(g)$ skalár mátrix, tehát g benne van Z-ben.

3.3.20. Lemma. $Z(G) = \bigcap\{Z(\chi) \mid \chi \in Irr(G)\}$

Bizonyítás: $Z(G)/\ker\chi \subseteq Z(G/\ker\chi) = Z(\chi)/\ker\chi$ az előző lemma d) része miatt. Így $Z(G) \subseteq Z(\chi)$. A megfordításhoz tegyük fel, hogy $g \in Z(\chi)$ minden irreducibilis karakterre, így $g\ker\chi \in Z(G/\ker\chi)$. Legyen $x \in G$ tetszőleges, $[g,x] = = g^{-1}x^{-1}gx \in \ker\chi$. Így $[g,x] \in \bigcap\{\ker\chi \mid \chi \in Irr(G)\} = 1$, tehát $g \in Z(G)$.

3.4. Algebrai egészek és a Burnside tétel

A Burnside tétel igazolásához a reprezentáció elmélet mellett szükség van egyéb algebrai ismeretekre, mégpedig az algebrai egészek elméletéből.

3.4.1. Definíció. *Egy komplex szám algebrai egész, ha gyöke az egész együtthatós, $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ polinomnak.*

3.4.2. Lemma. *A racionális algebrai egészek pontosan a $\mathbb{Z}$ elemei.*

3.4.3. Lemma. *Legyen $X = \{x_1, ..., x_k\}$ algebrai egészek halmaza. Ekkor létezik olyan S gyűrű, amire*

a) $X \subset S$

b) $\mathbb{Z} \subset S \subset \mathbb{C}$

c) Létezik olyan Y algebrai egészek halmaza, hogy S pontosan az Y elemeinek $\mathbb{Z}$-lineáris kombinációjából áll.

3.4.4. Lemma. *Legyen S gyűrű, amire $\mathbb{Z} \subset S \subset \mathbb{C}$ teljesül. Tegyük fel, hogy S végesen generált $\mathbb{Z}$-modulus. Ekkor S minden eleme algebrai egész.*

3.4.5. Következmény. *Az algebrai egészek gyűrűt alkotnak.*

3.4.6. Lemma. *Legyen χ a G csoport karaktere. Ekkor $\chi(g)$ algebrai egész minden $g \in G$-re.*

Bizonyítás: Legyen g elem rendje G-ben n. Ekkor $\chi(g)$ n-edik egységgyökök összege, amik algebrai egészek, hiszen az $x^n - 1$ polinom gyökei. Az előző következmény miatt algebrai egészek összege is az, tehát $\chi(g)$ is az.

Legyen G csoport, és χ irreducibilis karakter. A 3.3.17. lemma miatt minden $z \in Z(\mathbb{C}[G])$ elemre $\mathfrak{X}(z) = \varepsilon I$. Tehát definiálható az $\omega_\chi : Z(\mathbb{C}[G]) \to \mathbb{Z}$ függvény:

$$\mathfrak{X}(z) = \omega_\chi(z)I$$

Ha nem ad okot félreértésre, akkor a rövidség kedvéért csak simán ω-val jelöljük a leképezést. Mivel $\mathfrak{X}$ leképezés algebra homomorfizmus, könnyen látszik, hogy az ω is az. Így ha meg akarjuk adni ω-t, akkor elég megadni egy bázison. Korábban már láttuk, hogy $Z(\mathbb{C}[G])$-ben bázist alkotnak a K_i függvények, ahol K_i-t úgy definiáltuk, hogy a $\mathcal{K}_i$ konjugált osztályon 1, azon kívül mindenhol 0. $\mathfrak{X}(K) = \omega(K)I$ összefüggésben vegyük a nyomot:

$$\omega(K_i)\chi(1) = \chi(K_i) = \sum_{g \in \mathcal{K}_i} \chi(g) = |\mathcal{K}_i|\chi(g), \text{ és így } \omega(K_i) = \frac{|\mathcal{K}|\chi(g)}{\chi(1)}.$$

3.4.7. Tétel. *Legyen G csoport irreducibilis karaktere χ, K_i pedig ugyanúgy definiálva, ahogy eddig. Ekkor $\omega_\chi(K_i)$ algebrai egész.*

Bizonyítás: A 3.3.4. Tétel alapján $K_iK_j = \sum_{r=1}^{k} a_{ijr}K_r$. Mivel ω algebra homomorfizmus, így teljesül

$$\omega(K_i)\omega(K_j) = \sum_{r=1}^{k} a_{ijr}\omega(K_r).$$

Jelölje S az $\omega(K_1), ..., \omega(K_k)$ $\mathbb{Z}$-lineáris kombinációit. Az imént láttuk, hogy S zárt összeadásra és szorzásra, és $\omega(1) = 1$, így $\mathbb{Z} \subset S \subset \mathbb{C}$ is teljesül. Ezért a 3.4.4. lemma miatt S minden eleme algebrai egész.

3.4.8. Tétel. *(Burnside) Legyen G véges csoport, $\chi \in Irr(G)$. Tegyük fel, hogy $(|\mathcal{K}|, \chi(1)) = 1$ valamely $\mathcal{K}$ konjugált osztályra. Ekkor $g \in \mathcal{K}$ esetén $\chi(g) = 0$, vagy $g \in Z(\chi)$*

Bizonyítás: Mivel $(|\mathcal{K}|, \chi(1)) = 1$ fennáll, ezért léteznek olyan $u, v \in \mathbb{Z}$ számok, hogy $u|\mathcal{K}| - v\chi(1) = 1$. Korábban már kiszámoltuk $\omega(K)$-t, ezt felhasználva

$$u\omega(K) = \frac{u|\mathcal{K}|\chi(g)}{\chi(1)} = \frac{v\chi(1)\chi(g) + \chi(g)}{\chi(1)} = v\chi(g) + \frac{\chi(g)}{\chi(1)}$$

Mivel $\omega(K)$, és $\chi(g)$ algebrai egészek, így $u\omega(K)$ és $v\chi(g)$ is az. Az algebrai számok halmaza zárt összeadásra, tehát $\alpha = \frac{\chi(g)}{\chi(1)}$ is algebrai egész. Ha $g \notin Z(\chi)$, akkor $|\alpha| < 1$. Legyen g rendje n, és legyen F az $x^n - 1$ polinom felbontási teste. Legyen $\psi \in Gal(F|\mathbb{Q})$ Galois csoportnak. Mivel ψ automorfizmusa F-nek, így az n-edik egységgyököknek n-edik egységök lesz a ψ szerinti képe. Mivel $\chi(g)$ n-edik egységgyökök összege, így $\psi(\chi(g))$ is az, tehát $|\psi_i(\chi(g))| \leq \chi(1)$. ψ identitás $\mathbb{Q}$-n, $\psi(\chi(1)) = \chi(1)$, így $|\psi(\alpha)| \leq 1$. Legyen

$$\beta = \prod_{\psi \in Gal(F|\mathbb{Q})} \psi(\alpha).$$

Világos, hogy ekkor $|\beta| < 1$, hiszen a szorzat minden tényezőjének abszolútértékét felülről tudjuk becsülni 1-el, ráadásul az α esetén ez szigorú felső becslés. $\psi(\alpha)$ ugyanazt a racionális polinomot elégíti ki minden $\psi \in Gal(F|\mathbb{Q})$-re, hiszen ψ F egy automorfizmusa, ezért β invariáns az $Gal(F|\mathbb{Q})$ csoport elemeire, mert ezek csak permutálják a szorzótényezőket a szorzatban. Mivel a $Gal(F|\mathbb{Q})$ minden eleme fixen hagyja β-t, így β racionális. Továbbá β algebrai egészek szorzata, tehát algebrai egész. A 3.4.2. Lemma alapján a racionális algebrai egészek $\mathbb{Z}$ elemei, így $|\beta| < 1$ miatt $\beta = 0$. Valamely i-re $\alpha_i = 0$, amiből nyilvánvalóan $\alpha = 0$, tehát $\chi(g) = 0$ is teljesül.

3.4.9. Tétel. *Legyen G nem Abel, egyszerű csoport. Ekkor 1 az egyetlen olyan konjugált osztálya G-nek, melynek az elemszáma prímhatvány.*

Bizonyítás: Tegyük fel, hogy $g \in G$ elem $\mathcal{K}$ konjugáltosztályának elemszáma p^α. Legyen χ nem triviális irreducibilis karakter. Mivel G egyszerű, egy korábbi állítás szerint $\ker \chi = 1$, és így $Z(\chi) = Z(G) = 1$. Ha $p \nmid \chi(1)$, akkor $Z(\chi) = 1$ miatt $\chi(g) = 0$.

$$0 = \rho(g) = \sum_{\chi \in Irr(G)} \chi(1)\chi(g) = 1 + \sum_{p|\chi(1), \chi \in Irr(G)} \chi(1)\chi(g)$$

Ami az $1 = p\alpha$ alakban írható. Mivel az összeg megmaradt tagjaiban $p|\chi(1)$, így α algebrai egész számok $\mathbb{Z}$-lineáris kombinációja, tehát algebrai egész. De $\alpha = 1/p$ miatt racionális is, tehát $\mathbb{Z}$-beli, de ez nyilvánvalóan nem igaz. Tehát a feltevés, miszerint nem $\{1\}$ az egyetlen prímhatvány rendű konjugált osztály, hamis.

3.4.10. Tétel. *Legyen G csoport, melyre $|G| = p^a q^b$. Ekkor a G csoport feloldható.*

Bizonyítás: Tegyük fel, hogy G minimális rendű csoport, melynek rendje legfeljebb két prímhatvány szorzata, de G nem feloldható. Ha G nem egyszerű, akkor létezik $N \lhd G$, de ekkor N, és G/N rendje is legfeljebb két prímhatvány szorzata. G minimalitása miatt N, és G/N feloldható, tehát G is feloldható

Legyen G egyszerű, és vegyük egy Sylowját, ez legyen P. Prímhatvány rendű csoport centruma nem üres, tehát legyen $g \in Z(P)$. Világos, hogy $C_G(g)$ tartalmazza P-t, így $|G : C_G(g)|$ prímhatvány rendű, de ez megegyezik g konjugált osztályának elemszámával, így az előző tétel miatt G Abel csoport. Minden Abel csoport feloldható, így készen vagyunk.

3.5. További eredmények

Az eddig fejezetekben beláttuk, hogy egy csoport feloldható, ha a rendje négyzetmentes, vagy a rendjét legfeljebb két prím osztja. Viszont ennél van egy sokkal erősebb állítás, ami a csoport elmélet egyik leghíresebb állítása, ezt bizonyítás nélkül közöljük.

3.5.1. Tétel. *(Feit-Thompson) [5] Minden páratlan rendű csoport feloldható*

3.5.2. Következmény. *Ha a G csoport rendje nem osztható 4-gyel, akkor G feloldható.*

Bizonyítás: Ha G rendje páratlan, akkor a Feit-Thompson tétel szerint feloldható. Ha G rendje osztható 2-vel, akkor a legkisebb prímosztója 2, és a 2-Sylow ciklikus, így a 3.1.10 Következmény miatt van normál 2-komplementum, ezt jelölje N. N feloldható, $G/N \simeq \mathbb{Z}_2$ úgyszintén, tehát G is az.

Az egyszerű csoportok klasszifikációja segítségével konkrétan meg lehet adni azokat az n számokat, amikre minden n rendű csoport feloldható.

3.5.3. Tétel. *A G csoport feloldható, ha a rendje nem többszöröse a következő számoknak.*

(a) $2^p(2^{2p}-1)$, *ahol p prím*

(b) $3^p(3^{2p}-1)/2$, *ahol p páratlan prím*

(c) $p(p^2-1)/2$, *ahol $p>3$ prím, amire* $p^2+1 \equiv 0 \mod 5$

(d) $2^4 \cdot 3^3 \cdot 13$

(e) $2^{2p}(2^{2p}+1)(2^p-1)$, *ahol p páratlan prím*

4. A PSL(n,q) csoportok egyszerűsége

4.1. Iwasava tétele

Az előbbi két fejezetben arra kerestünk feltételeket, hogy milyen rend esetén lesz egy csoport biztosan feloldható. Most a fordított szituációt vizsgáljuk, mutatunk néhány példát egyszerű csoportokra. Ezek rendjének többszörösei nem lehetnek feloldható számok, így kapunk majd néhány szükséges feltételt a feloldhatóságra. Ahogy a cím is mondja a $PSL(n,q)$ csoportok egyszerűségét bizonyítjuk. A csoport elmélet megint másik területét fogjuk vizsgálni, csoportok hatását adott halmazon. A bizonyítást Larry C. Grove *Groups and characters* című könyvéből vettem.

Ha V n-dimenziós vektortér, akkor a lineáris leképezéseinek tere $GL(V)$. Ha V-ben választunk egy bázist, ez megad egy izomorfizmust $GL(n,F)$-vel, az F feletti $n \times n$-es invertálható mátrixok csoportjával.

A determináns a $GL(V)$ egy homomorfizmusa az F^* multiplikatív csoportjába. Ennek magját jelölje $SL(V)$. A $GL(V)$ csoportban a centrumot az $a1$ alakú leképezések adják, $SL(V)$-ben szintén, azonban az $a1$ csak akkor eleme $SL(V)$-nek, ha $a^n = 1$, azaz $Z(SL(V)) = \{a1 : a \in F^*, a^n = 1\}$.

Ha $0 \neq v \in V$, akkor tekinthetjük az $Fv = \{av : a \in F\}$ egyenest egyetlen pontnak, és ezt $[v]$ jelöli. Így kapjuk a $P(V)$ projektív teret, aminek elemei a $[v]$ projektív pontok. Megadható a $GL(V)$ természetes hatása a $P(V)$-n, $\tau[v] = [\tau v]$ minden $\tau \in GL(V)$, $[v] \in P(V)$. A hatás magja $Z(GL(V))$, hasonlóan $SL(V)$ is hat $P(V)$-n, ekkor a hatás magja $Z(SL(V))$. Legyen $PSL(V) = SL(V)/Z(SL(V))$. Tehát ez a csoport hűségesen hat a $P(V)$-n. A célunk, hogy bebizonyítsuk, hogy $PSL(2,2)$, és $PSL(2,3)$ kivételével minden $PSL(V)$ egyszerű csoport.

Legyen G csoport, ami hat az S halmazon. Jelölje az $x \in G$ elem hatását az $s \in S$ elemen s^x.

4.1.1. Definíció. *Legyen $B \subseteq S$, amire $B \neq D$, $|B| > 1$, és minden $x \in G$-re $B^x = B$ és $B \cap B^x = \emptyset$ közül pontosan az egyik teljesül. Ekkor B blokk. Ha G tranzitív S-en, és S nem tartalmaz blokkot, akkor G primitív S-en.*

4.1.2. Tétel. *(Iwasawa) Tegyük fel, hogy G hűséges és primitív S-en, továbbá $G' = G$. Rögzítsük $s \in S$-et, és $H = Stab_G(s)$. Tegyük fel, hogy $\exists K \lhd H$ feloldható csoport, amire $G = \langle \cup \{K^x : x \in G\} \rangle$. Ekkor G egyszerű.*

Bizonyítás: Tegyük fel, hogy $1 \neq N \lhd G$. Megmutatjuk, hogy $N = G$, azaz G-nek nincsen valódi normálosztója.

Mivel G hűséges S-en, ezért $N \neq 1$ miatt létezik S-ben több mint 1 elemű N-orbit, jelölje $B = Orb_N(a)$ és $|B| \geq 2$. Ha $x \in G$, akkor $B^x = a^{Nx} = a^{xN}$ mivel $N \lhd G$. Így $B^x = Orb_N(a^x)$. Mivel N-et particionálják az N-orbitjai, ezért $B^x = B$

vagy $B^x \cup B = \emptyset$. De G primitív S-en, ezért $B = S$, különben B blokk lenne G-ben. Így $Orb_N(a) = B = S$, és ez szerint N tranzitív S-en.

Ha $x \in G$; akkor létezik $y \in N$, hogy $s^x = s^y$, hiszen N tranzitív S-en. Ekkor $s^{xy^{-1}} = s$ tehát $xy^{-1} \in Stab_G(s) = H$. $x \in Hy \subseteq HN$, tehát $G = HN$.

$G = HN = NH$, mivel N normálosztó, és $G = \langle \cup \{K^x : x \in NH\} \rangle$. $K \lhd \lhd H$, ezért $n \in N$, és $h \in H$ esetén $K^{nh} = n^{-1}h^{-1}Khn = n^{-1}K^h n = K^n$. Tehát $G = \langle \cup \{K^n : n \in N\} \rangle$. Minden G-beli elem felírható

$$x = k_1^{n_1} k_2^{n_2} ... k_r^{n_r} = n_1^{-1} k_1 n_1 n_2^{-1} k_2 n_2 ... n_r^{-1} k_r n_r$$

alakban. Mivel $N \lhd G$, így N felcserélhető G tetszőleges g elemével, azaz $ng = g\hat{n}$, ahol $n, \hat{n} \in N$. Ezt a formulát alkalmazva

$$x = n_1^{-1} k_1 n_1 n_2^{-1} k_2 n_2 ... n_r^{-1} k_r n_r,$$

amit rendezni tudunk. Előre a K-beli tagokat, hátra az N-beliek, így $x = kn$-hez jutunk, ahol $k \in K$, $n \in N$. Tehát $G = KN$.

Mivel K feloldható, így $K^{(m)} = 1$ valamely m-re.

$$(KN)' = \langle \{n_1^{-2} k_1^{-1} n_2^{-1} k_2^{-1} k_1 n_1 k_2 n_2 : k_1, k_2 \in K, n_1, n_2 \in N\} \rangle \leq \langle \{k_1^{-1} k_2^{-1} k_1 k_2 n : \\ : k_1, k_2 \in K, n \in N\} \rangle = K'N.$$

Felhasználtuk, hogy $nk = \hat{n}k$, így tudtuk rendezni a K-beli és N-beli tagokat egymás mellé. Indukciót használva kapjuk $(KN)^{(l)} \leq K^l N$ fennáll minden l-re. Mivel $G' = G$ így $G = G^{(m)} = (KN)^{(m)} \leq K^{(m)}N = N$. Tehát $N = G$, és ezt akartuk belátni.

4.2. Transzvekció

Iwasawa tételét szeretnénk alkalmazni $PSL(V)$-re, ehhez be kell látni, hogy a tétel feltételei teljesülnek rá. Tehát $PSL(V)$ primitív $P(V)$-n, $PSL(V)' = PSL(V)$, és van olyan normálosztója a $Stab_{PSL(V)}([w])$-nek, aminek konjugáltjai generálják $PSL(V)$-t. Ennek érdekében definiáljuk a transzvekciót, és ennek segítségével jutunk célhoz.

4.2.1. Definíció. *$1 \neq \tau \in GL(V)$ transzvekciónak hívjuk, ha létezik V-ben olyan W hipersík, amire $\tau|_W = 1_w$, és $\tau v - v =\in W$ minden $v \in V$. W a τ rögzített hipersíkja.*

Ha τ transzvekció, melynek W a rögzített hipersíkja, válasszuk V-nek $v_1, ..., v_n$ bázisát, hogy $v_2, ..., v_n$ bázisa legyen W-nek is. Ekkor τ-t reprezentáló mátrix determinánsa nyilvánvalóan 1, tehát $\tau \in SL(V)$.

4.2.2. Lemma. *A transzvekció inverze is transzvekció. Tegyük fel, hogy V altere V_1-nek, amire $v \in V_1 - V$ és τ transzvekció V-n, aminek rögzített hipersíkja W. Ekkor τ kiterjeszthető τ_1-re, hogy τ_1 transzvekció V_1-n, és a τ_1 rögzített hipersíkja tartalmazza v-t.*

Bizonyítás: Ha τ transzvekció, akkor $\tau w = w$ minden $w \in W$-re. Mindkét oldalra alkalmazva τ^{-1}-et, kapjuk $w = \tau^{-1}w \ \forall w \in W$. Ha $\tau v - v = w \in W$, akkor $v - \tau^{-1}v = w$ és így $\tau^{-1}v - v = -w \in W$ minden $v \in V$-re, tehát τ^{-1} is transzvekció.

Most bizonyítsuk a második állítást. Legyen V-nek bázisa $v_1, ..., v_k$, hogy W-nek bázisa legyen $v_2, ...v_k$. Terjesszük ki V bázisát V_1 bázisává, úgy hogy $v_1, ..., v_k, v = v_{k+1}, ..., v_n$ legyen a kiterjesztett bázis. Terjesszük ki τ-t V_1-re, $\tau_1|_V = \tau$, és $\tau_1 v_i = v_i$, ha $i > k$. τ_1 fixen hagyja $w_2, ...w_n$ hipersíkot, (ez lesz a W_1 rögzített hipersík) és $\tau_1 v_1 - v_1 = \tau v_1 - v_1 \in W \subseteq W_1$, tehát τ_1 transzvekció, és $\tau_1 v = v$.

4.2.3. Lemma. *Ha u és v lineárisan függetlenek V-ben, akkor létezik τ transzvekció, hogy $\tau u = v$.*

Bizonyítás: Válasszunk W hipersíkot V-ben, ami tartalmazza $u - v$-t, de $u \notin W$. Legyen $\tau|_W = 1_W$, és $\tau u = v$. Legyen $x = cu + w$, ahol $c \in F^*$, és $w \in W$. Nyilvánvaló, hogy minden V-beli elem felírható ilyen alakban. Ekkor $\tau x - x = cv + w - cu - w = c(u - v) \in W$, tehát τ transzvekció.

4.2.4. Lemma. *Legyen W_1 és W_2 különböző V-beli hipersíkok, amire $v \in V - (W_1 \cup W_2)$. Ekkor létezik τ transzvekció, amire $\tau W_1 = W_2$ és $\tau v = v$.*

Bizonyítás: Mivel $W_1 + W_2 = V$, így $\dim(W_1 \cap W_2) = \dim W_1 + \dim W_2 - \dim V = n - 2$, és $W = W_1 \cap W_2 + Fv$ szintén hipersík. Legyen $v = x + y$, ahol $x \in W_1$, és $y \in W_2$. Ekkor $x \notin W$, hiszen $x \in W$ esetén $y = v - x \in W$ is fennáll, de ekkor $V \subseteq W$, ami ellentmondás. Definiáljuk τ-t, legyen $\tau|_W = 1_W$, és $\tau x = -y$. Legyen $z = cx + w$, $w \in W$, $c \in F^*$ tetszőleges V-beli elem. Ekkor $\tau z - z = -cy + w - cx - w = -c(x + y) = cv \in W$, tehát τ transzvekció. $\tau v = v$, mert így adtuk meg τ-t. $\tau W_1 = \tau(W_1 \cap W_2 + Fx) = W_1 \cap W_2 - Fy = W_2$.

4.2.5. Tétel. *A transzvekciók halmaza generálja $SL(V)$-t.*

Bizonyítás: Legyen $\rho \in SL(V)$ tetszőleges, válaszunk egy W hipersíkot V-ben, és legyen $v \in V - W$. Ha v és ρv lineárisan függetlenek, akkor a 4.2.3 Lemma alapján létezik a τ_1 transzvekció, hogy $\tau_1 \rho v = v$. Ha v és ρv nem linárisan függetlenek, válasszunk τ_0-t, hogy $\tau_0 \rho v$ és v már az legyen. Ekkor találunk olyan τ_2 transzvekciót,

hogy $\tau_2\tau_0\rho v = v$. Ekkor $\tau_1 = \tau_2\tau_0$. Mindkét esetben találtunk olyan τ_1-et, amire $\tau_1\rho v = v$, és τ_1 transzvekciók szorzata, tehát $SL(V)$-ben van. $v \notin \tau_1\rho W$, mert $v \in$ $\in V - W$, és $\tau_1\rho v = v$. Ha $\tau_1\rho W = W$, akkor legyen $\tau = 1_V$. Ha $\tau_1\rho W \neq W$, akkor a 4.2.4. Lemma miatt létezik τ hogy $\tau\tau_1\rho W = W$, és $\tau v = v$. Legyen most $\sigma = \tau\tau_1\rho$, ekkor $\sigma W = W$, $\sigma v = v$, és $\sigma \in SL(V)$, tehát $\sigma|_W \in SL(W)$. Most indukcióval belátjuk, hogy ρ transzvekciók szorzata. Ha $\dim V = 2$, akkor $SL(W) = 1_W$, így $\sigma|_W = 1_W$. $\sigma = 1$ és ekkor $\rho = \tau_1^{-1}\tau^{-1}$, tehát transzvekciók szorzata. Ha $n > 2$, akkor $\sigma|_W$ transzvekciók szorzata W-n. A 4.2.2. Lemma alapján mindegyik transzvekció kiterjeszthető V-re úgy, hogy v-t fixen hagyja. Tehát σ kiterjesztett transzvekciók szorzata, és így $\rho = \tau_1^{-1}\tau^{-1}\sigma$ tehát transzvekciók szorzata.

4.2.6. Lemma. *Ha τ_1 és τ_2 transzvekciók V-n, akkor konjugáltak $GL(V)$-ben. Ha $n \geq 3$, akkor $SL(V)$-ben is konjugáltak.*

Bizonyítás: Legyen W_i a τ_i rögzített hipersíkja, és válasszunk $x_i \in V - W_i$ elemet, továbbá legyen $w_i = \tau_i x_i - x_i \in W_i$. Legyen $w_1, u_3, ..., u_n$ a W_1, $w_2, v_3, ..., v_n$ a W_2 egy bázisa. Minden $a \in F^*$-ra definiáljuk a $\sigma_a \in GL(V)$ leképezést, $\sigma_a x_1 = x_2$, $\sigma_a w_1 = w_2$, $\sigma_a u_i = v_i$, ha $3 \leq i \leq n-1$, és $\sigma_a u_n = a v_n$. Ekkor

$\sigma_a^{-1}\tau_2\sigma_a(x_1) = \sigma_a^{-1}\tau_2(x_2) = \sigma_a^{-1}(w_2 + x_2) = x_1 + w_1 = \tau_1(x_1)$,

$\sigma_a^{-1}\tau_2\sigma_a(w_1) = \sigma_a^{-1}\tau_2(w_2) = \sigma_a^{-1}(w_2) = w_1 = \tau_1(w_1)$ és

$\sigma_a^{-1}\tau_2\sigma_a(u_i) = \sigma_a^{-1}\tau_2(\alpha_n v_i) = \sigma_a^{-1}(\alpha_n v_i) = u_i = \tau_2(u_i)$,

ahol $\alpha_i = 0$, ha $i \neq n$, és $\alpha_n = a$. Így $\sigma_a^{-1}\tau_2\sigma_a$ és τ_1 megegyeznek az $x_1, w_1, u_3, ..., u_n$ bázison, tehát $\sigma_a^{-1}\tau_2\sigma_a = \tau_1$.

Ha $n > 2$, akkor $b = (\det\sigma_1)^{-1}$ és $\sigma_b \in SL(V)$.

4.2.7. Lemma. *Tegyük fel, hogy $\dim V = 2$, és legyen v_1, v_2 tetszőleges bázis V-ben. Minden transzvekció konjugált $SL(V)$-ben egy olyan elemmel, aminek a mátrixa a v_1, v_2 bázisban $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$ alakú valamilyen $a \in F^*$-re.*

Bizonyítás: Ha τ transzvekció a W rögzített hipersíkkal, akkor válasszunk egy $v \in V - W$ elemet, legyen $w = \tau v - v \in W$. A v, w bázisban τ $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ alakú. Ha M mátrixszal jelöljük a τ v_1, v_2 bázisbeli alakját, akkor létezik $B \in GL(2, F)$, amivel $B^{-1}MB = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ Ha $\det B = a^{-1}$, akkor legyen $A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$. $BA \in SL(2, F)$, és

$$(BA)^{-1}M(BA) = A^{-1}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}A = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}.$$

4.2.8. Tétel. *Ha $n > 2$, akkor $SL(V)' = SL(V)$, és $PSL(V)' = PSL(V)$.*

Bizonyítás: Ha $SL(V)'$ tartalmaz transzvekciót, akkor a 4.2.6 Lemma miatt minden transzvekció konjugált, tehát $SL(V)'$ tartalmaz minden transzvekciót. Az 4.2.5. tétel miatt a transzvekciók generálják $SL(V)$-t, így $SL(V) = SL(V)'$. Tehát elég mutatni $SL(V)'$-ben egy transzvekciót. Válasszunk V-ben egy bázist, legyen ez $v_1, ..., v_n$, és definiáljuk τ_1, τ_2-t:

$\tau_1 : v_1 \mapsto v_1 - v_2, v_i \mapsto v_i$ ha $2 \leq i \leq n$,

$\tau_2 : v_1 \mapsto v_1, v_2 \mapsto v_2 - v_3, v_i \mapsto v_i$ ha $3 \leq i \leq n$.

Ekkor $\tau_1^{-1}\tau_2^{-1}\tau_1\tau_2 : v_1 \mapsto v_1 + v_3, v_i \mapsto v_i$ if $2 \leq i \leq n$.

Tehát $\tau_1^{-1}\tau_2^{-1}\tau_1\tau_2$ transzvekkció $SL(V)'$-ben. $PSL(V) = SL(V)/Z(SL(V))$, így

$$PSL(V)' = \frac{SL(V)'Z(SL(V))}{Z(SL(V))} = \frac{SL(V)}{Z(SL(V))} = PSL(V)$$

4.2.9. Tétel. *Ha $n = 2$, $|F| > 3$, akkor $SL(V)' = SL(V)$.*

Bizonyítás: Válasszuk a v_1, v_2 bázist V-ben, és legyen $a \in F^*, a \neq \pm 1$. Definiálja $\sigma \in SL(V)$-t a $\sigma(v_1) = av_1$, $\sigma(v_2) = a^{-1}v_2$ összefüggések. Minden $b \in F^*$-re definiálja $\tau_b \in SL(V)$ $\tau_b(v_1) = v_1 - bv_2$ és $\tau_b(v_2) = v_2$. Ekkor $\sigma^{-1}\tau_b^{-1}\sigma\tau_b$ mátrix alakban:

$$\begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -b & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ ba(a - a^{-1}) & 1 \end{pmatrix}$$

A tétel következik az 4.2.7 Lemmából és az 4.2.5 Tételből.

4.2.10. Lemma. *Ha $n \geq 2$, akkor $SL(V)$ primitív a $P(V)$ projektív téren.*

Bizonyítás: Vegyük $[v_1] \neq [v_2]$, és $[w_1] \neq [w_2]$ $P(V)$-beli pontokat. Ekkor $\{v_1, v_2\}$ és $\{w_1, w_2\}$ lineárisan független halmazok. Ha $n = 2$, akkor bázisok. Ha $n > 2$, akkor $V_1 = Fv_1 + Fv_2$ és $V_2 = Fw_1 + Fw_2$. Vagy $V_1 = V_2 \neq V$ vagy $V_1 \neq V_2$, de ekkor $V_1 \cup V_2$ nem altere V-nek. Mindkét esetben $V_1 \cup V_2 \neq V$. Ha $v_3 \in V - (V_1 \cup V_2)$, akkor v_1, v_2, v_3 és w_1, w_2, v_3 halmazok is lineárisan függetlenek. A gondolatmenet megismételhető, így V két bázisát kapjuk, ezek $v_1, ..., v_n$ és $w_1, w_2, v_3, ..., v_n$. Minden $b \in F$ elemre definiáljuk a $\tau_b \in GL(V)$-t, $\tau_b v_1 = bw_1$, $\tau_b v_2 = w_2$, $\tau_b v_i = v_i$, ha $3 \leq i \leq n$. Ha $w_j = \sum_i a_{ij} v_i$, akkor $\det \tau_b = b(a_{11}a_{22} - a_{12}a_{21})$. Válasszuk b-t, hogy $\det \tau_b = 1$ legyen, azaz $\tau_b \in GL(V)$. Ekkor τ_b a $[v_1]$-t $[w_1]$-be, $[v_2]$-t $[w_2]$-be viszi.

Legyen $B \subseteq P(V)$, $|B| > 1$ és $B \neq P(V)$. Válasszunk $[v_1], [v_2] \in B$, és $[w] \in P(V) - B$ pontokat. Ekkor megadható olyan $\tau \in SL(V)$, amire $\tau[v_1] = v_1$, és $\tau[v_2] = w$. $[v_1] \in B$, és $[v_1] \in B^\tau$, tehát $B \cap B^\tau$ nem üres. De $[w] \notin B$, és $[w] \in B^\tau$ is fennáll, tehát $B \neq B^\tau$. Így B nem lehet blokk, ezért $SL(V)$-ben nincs blokk tehát primitív.

4.2.11. Lemma. *Ha $0 \neq v \in V$ és $A = Stab_{SL(V)}([v])$, akkor A-nak van B Abel normálosztója, aminek $SL(V)$-beli konjugáltjai generálják $SL(V) - t$.*

Bizonyítás: Válasszunk egy W hipersíkot, és $v \notin W$ elemet, amivel $V = W + Fv$. Ha $\sigma \in A$, akkor legyen $u \in V$-re $\sigma u = \sigma' u + a_u v$, ahol $\sigma u \in W$ és $a_u \in F$. Legyen $x = au_1 + bu_2$, ekkor $\sigma(au_1 + bu_2) = \sigma'(au_1 + bu_2) + a_x v$ és $\sigma(au_1 + bu_2) = a\sigma u_1 + b\sigma u_2 = a\sigma' u_1 + b\sigma' u_2 + (aa_{u_1} + ba_{a_2})v$. A két féle felírás alapján σ' lineáris. σv is felírható két féle képpen, egyrészt $\sigma v = \sigma v' + a_v v$. Másrészt σ benne van v stabilizátorában, így $\sigma v = v$. Innen $\sigma' v = 0$ adódik. $\sigma^{-1} u = (\sigma^{-1})' u + b_u v$, ezért $w \in W$-re $w = \sigma^{-1}(\sigma w) = (\sigma^{-1})'(\sigma w) = \sigma^{-1}(\sigma' w + a_w v) = (\sigma^{-1})'(\sigma' w)$. Hasonlóan adódik $\sigma'(\sigma^{-1})'(W) = w$, így $\sigma'|_W \in GL(W)$. Vegyük a $\varphi : \sigma \mapsto \sigma'|_W$ leképezést, ami A-ból $GL(W)$-be képez. $(\sigma_1\sigma_2)w = (\sigma_1\sigma_2)' w + a_w v$. Másképpen számolva $(\sigma_1\sigma_2)w = \sigma_1(\sigma_2 w) = \sigma_1(\sigma_2' w + b_w v) = \sigma_1'\sigma_2' w + a_{\sigma_2' w} v$. Így $(\sigma_1\sigma_2)' = \sigma_1'\sigma_2'$ adódik, tehát φ homomorfizmus A-ból $GL(W)$-be és így $B = \ker\varphi$ normálosztó A-ban.

Válasszunk bázist W-ben, legyen ez $w_1, ..., w_{n-1}$. Minden $b \in F^*$ esetén definiáljuk $\tau_b \in A$-t a következő módon: $\tau_b w_1 = w_1 + bv$, $\tau_b w_i = w_i$ ha $2 \leq i \leq n-1$, végül $\tau_b v = v$. Világos, hogy τ_b transzverzió a $w_2, ..., w_{n-1}, v$ vektorok által kifeszített rögzített hipersíkkal. $w \in W$ esetén $\tau_b w = w + bv$, tehát $\tau_b'|_W = 1_w$. Így $\tau_b \in B$. Ha $n = 2$, akkor a w_1, v által kifeszített bázisban $\tau_b \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$ alakban írható. A 4.2.6 és 4.2.7. Lemma miatt B és $SL(V)$-beli konjugáltjai tartalmaznak minden transzverziót, az 4.2.5 Tétel alapján ezek generálják $SL(V)$-t $n \geq 2$ esetén. Legyen $\sigma \in B$, ekkor $\sigma'|_W = 1_W$, tehát $\sigma w = w + av$ minden $w \in W$-re. Ha ezt a $w_1, ..., w_{n-1}, v$ bázisban írjuk fel, akkor a mátrixa $\begin{pmatrix} I & 0 \\ u & 1 \end{pmatrix}$ alakú, ahol I az $(n-1) \times (n-1)$-es egységmátrix, u pedig $1 \times (n-1)$-es vektor. Legyen most $\sigma_1, \sigma_2 \in B$, amik a $w_1, ..., w_{n-1}, v$ bázisban felírva $\begin{pmatrix} I & 0 \\ u_1 & 1 \end{pmatrix}$, $\begin{pmatrix} I & 0 \\ u_2 & 1 \end{pmatrix}$ alakúak. Mivel

$$\begin{pmatrix} I & 0 \\ u_1 & 1 \end{pmatrix}\begin{pmatrix} I & 0 \\ u_2 & 1 \end{pmatrix} = \begin{pmatrix} I & 0 \\ u_1 + u_2 & 1 \end{pmatrix} = \begin{pmatrix} I & 0 \\ u_2 & 1 \end{pmatrix}\begin{pmatrix} I & 0 \\ u_1 & 1 \end{pmatrix},$$

így B elemei felcserélhetők egymással, tehát B Abel.

4.2.12. Tétel. *$PSL(2,2)$ és $PSL(2,3)$ kivételével $PSL(V)$ egyszerű.*

Bizonyítás: Válasszunk $0 \neq v \in V$ elemet, és legyen $A = Stab_{SL(V)}([v])$, $B \lhd A$ amint a 4.2.11 Lemmában. Legyen $Z = Z(SL(V))$, ekkor $H = A/Z = Stab_{PSL(V)}([v])$, $K = BZ/Z \lhd H$. $PSL(V)$ hűséges $P(V)$-n, a 4.2.10 Lemma miatt primitív is, hiszen $SL(V)$ primitív $P(V)$-n, és a primitívség öröklődik a faktorcsoportokra. $K \lhd H = Stab_{PSL(V)}([v])$, továbbá K feloldható, hiszen Abel. Végül

K konjugáltjai generálják $PSL(V)$, tehát az Iwasawa tétel minden feltétele teljesül, azaz $PSL(V)$ egyszerű.

Megadtunk végtelen sok egyszerű csoportot. Nyilvánvaló, hogy ha az n számra létezik olyan $PSL(n,q)$ nem Abel egyszerű csoport, aminek a rendje a, és $a|n$ teljesül, akkor n nem lehet feloldható szám. Nézzük meg, hogy ez alapján a $PSL(n,q)$ csoportok milyen feltételeket adnak a feloldható számokra.

Először is adjuk meg $PSL(n,q)$ rendjét. Ismert, hogy $|GL(n,q)| = (q^n-1)(q^n-q)...(q^n-q^{n-1})$, innen $|SL(n,q)| = (q^n-1)(q^n-q)...(q^n-q^{n-1})/(p-1)$. $Z(SL(n,q))$ elemei azok az aI skalár mátrixok, amire $a^n = 1$, $a \in F_q^*$. Az ilyen elemek száma F_q^*-ban $(n, p-1)$, hiszen F_q^* ciklikus csoport. Ezekből már azonnal adódik, hogy

$$|PSL(n,q)| = \frac{(q^n-1)(q^n-q)...(q^n-q^{n-1})}{(q-1)(n,q-1)}$$

Ez alapján

$$|PSL(2,q)| = \frac{(q^2-1)(q^2-q)}{(q-1)(2,q-1)} = \frac{q(q^2-1)}{(2,q-1)}$$

osztja $|PSL(n,q)|$ rendjét, hiszen $(q^n-1)/(n,q-1)$ egész.

Tehát $q > 3$ esetén $n > 3$ esetben már nem kapunk további feltételeket feloldható számokra, elég $n = 2$ esetet vizsgálni. Viszont $q = 2$ és $q = 3$ esetén $PSL(2,q)$ nem lesz egyszerű, úgyhogy itt meg kell vizsgálni külön $n = 3$ esetet is. Legyen először $n = 2$.

Ha $q = 2^m$, akkor $2^m(2^{2m}-1)$ csak akkor adhat újabb feltételt a feloldható számokra, ha m prím. Tehát $2^p(2^{2p}-1)$ többszörösei nem lehetnek feloldható számok, ahol p tetszőleges prím.

Ha $q = 3^m$, akkor $3^m(3^{2m}-1)/2$ csak akkor adhat újabb feltételt, ha m prím. Azonban $m = 2$ esetén $3^2(3^4-1)/2 = 360$, ami többszöröse a $2^2(2^4-1) = 60$-nak, úgyhogy ezt kihagyhatjuk. Így kapjuk, hogy $3^p(3^{2p}-1)/2$ többszörösei nem lehetnek feloldható számok, ha p páratlan prím.

Még egy egyszerű észrevétel, $PSL(n,p)$ részcsoport $PSL(n,p^a)$-ban. Tehát ha $q > 3$, akkor elég $q = p$ esetet venni, $|PSL(2,p)| = p(p^2-1)/2$. Ha p^2-1 osztható 5-tel, akkor $|PSL(2,p)|$ osztható 60-nal is, tehát ez nem ad új feltételt, így azt kapjuk, hogy $p(p^2-1)/2$ többszörösei nem lehetnek feloldható számok, ahol $p > 3$ prím és $p^2+1 \equiv 0 \mod 5$.

Ha $n = 3$, akkor az előbbi észrevétel miatt szintén elég $q = p$-t vizsgálni. Ismert, hogy $PSL(3,2) = PSL(2,7)$, ezt pedig már vizsgáltuk. $|PSL(3,3)| = (3^3-1)(3^3-3)(3^3-3^2) = 2^4 3^2 13$, és ezzel a vizsgálatot befejeztük.

Ha összevetjük a kapott eredményeket a 3.5.3 Tétellel, akkor látjuk hogy a kapott számok megegyeznek a tételben szereplő első 4 számmal. Észrevehető, hogy a

tételben szereplő 5. szám, vagyis $2^{2p}(2^{2p}+1)(2^p-1)$ nem osztható 3-mal tetszőleges p páratlan prím esetén. Ezek, a 3-mal nem osztható rendű nem Abel egyszerű csoportok a Suzuki csoportok [10].

5. Hivatkozások

– 1.G. A. Miller and H. C. Motreno, *Non-Abelian groups in which every subgroup is Abelian*, Trans. Amer. Math. Soc. vol. 4 (1903) pp. 398-404

– 2. L. E. Dickson, *Definitions of a group and a field by independent postulates*, Trans. Amer. Math. Soc. 6 (1905) 198-204

– 3. K. Iwasawa, *Über die Structur der endlichen Gruppen, deren echte Untergruppen sämtlich nilpotent sind*, Proc. Phys.-Math. Soc. Japan vol. 23 (1941) pp. 1-4

– 4. Burnside, W. (1904), *On Groups of Order p^aq^b*, Proc. London Math. Soc. (s2-1 (1)): 388–392

– 5. Feit, Walter; Thompson, John G. (1963), *Solvability of groups of odd order*, Pacific Journal of Mathematics 13: 775–1029

– 6. Gorenstein, D. (1983), *The classification of finite simple groups*. Vol. 1. Groups of noncharacteristic 2 type, The University Series in Mathematics, Plenum Press

– 7. J. Pakianathan and K. Shankar, *Nilpotent numbers* The Amer. Math. Month., Vol. 107, No. 7 (Aug. - Sep., 2000), pp. 631-634

– 8. D. Robinson, *A course in the theory of groups*, Graduate Texts in Math. 80, Springer, New York, 1993

– 9. Suzuki, Michio (1960), *A new type of simple groups of finite order*, Proceedings of the National Academy of Sciences of the United States of America 46: 868–870