Universitat Autònoma de Barcelona

Treball final de Grau en Matemàtiques

Sobre la classificació dels grups finits de $\mathrm{GL}_n(K)$ i $\mathrm{PGL}_n(K)$

Gerard Gonzalo Calbetó

Supervisat per **Dr. Francesc Bars Cortina**

Curs: 2023/2024

Convocatòria Juliol

Índex

1 Introducció

La classificació dels subgrups finits de $\mathrm{GL}_n(K)$ i $\mathrm{PGL}_n(K)$ és un problema clàssic que s'inicia al voltant dels anys 1870 quan Klein (1875) [Kle75] classifica per mitjans geomètrics els subgrups finits de $\mathrm{PGL}_2(\mathbb{C})$. Més endavant Gordan (1877) [Gor77] s'allunya de l'enfocament geomètric donant una visió depenent de les solucions d'una certa equació per $\mathrm{PGL}_3(\mathbb{C})$. Un dels articles més coneguts del camp és publicat per Jordan el 1878 [Jor78] on es demostra el Teorema de Jordan dels grups finits lineals. Els esforços en aquesta àrea continuen de la mà de Valentiner (1889) [Val89] i Frobenius (1896) [Fro68], el darrer donant inici al que avui en dia es coneix com la teoria de representacions lineals dels grups finits. Uns anys més tard, Schur dona inici en una sèrie de tres articles (1904 [Sch04], 1907 [Sch07], 1911 [Sch11]) a la teoria de representacions projectives de grups finits, menys present en la literatura que la seva contrapart lineal. L'esforç per la classificació és continuat per Blichfeldt en la sèrie d'articles "On the order of linear homogenious groups" (1904-1911) [Bli03][Bli04][Bli06][Bli11] que culminen en el llibre "Finite collineation groups" (1917) [Bli17] on es presenta la classificació de $\mathrm{PGL}_4(\mathbb{C})$ i $\mathrm{GL}_4(\mathbb{C})$ juntament amb un recull de les tècniques desenvolupades fins al moment, recollint els diversos resultats dispersos en articles i revistes fins al moment.

Posteriorment a Blichfeldt, l'interès matemàtic de l'època en aquest àmbit es desplaça majoritàriament al desenvolupament de la teoria de representacions lineals de grups finits i l'esforç de més d'un segle que portarà a la classificació dels grups finits simples. Cal esperar fins a Brauer (1942) [Bra42a] [Bra42b] que amplia el treball de Blichfeldt mentre, paral·lelament, desenvolupa la teoria de caràcters de grups finits sobre cossos de característica positiva. El 1967 [Bra67] publica la classificació dels subgrups finits de $\mathrm{PGL}_5(\mathbb{C})$ i $\mathrm{GL}_5(\mathbb{C})$. Quatre anys més tard (1971) Feit [Fei71] recull en un article la classificació dels $\mathrm{PGL}_n(\mathbb{C})$ i $\mathrm{GL}_n(\mathbb{C})$ per $n = 3$ fins a $n = 7$ la qual es trobava dispersa en diversos articles de diferents autors.

Situant-nos ja a finals del segle XX, els avenços en la teoria de representacions projectives dels grups finits simples i la classificació d'aquests porten a la classificació, el 1998, dels subgrups finits de $SL(p, \mathbb{C})$ amb p primer, deguda a Dixon i Zalesskii [DZ98], amb una correcció publicada el 2008 [DZ08]. Pel que fa a la classificació sobre cossos de característica positiva, la millor referència que coneixem actualment és de B.S. Huggins (2005) [Hug05] en la seva tesi doctoral "Fields of Moduli and Fields of Definition of Curves", on es dona la classificació de $\mathrm{PGL}_2(K)$ i $\mathrm{PGL}_3(K)$ per cossos algebraicament tancats de característica $p \geq 0$.

La classificació dels subgrups finits de $\mathrm{PGL}_n(K)$ és encara d'ampli interès avui en dia. En el context de la geometria algebraica, el famós teorema de Hurwitz [FCB17, Teorema 1.1] enuncia que si $\overline{C}$ és una corba algebraica no singular de gènere $g \geq 2$ sobre $\overline{K}$ aleshores el seu grup d'automorfismes $\mathrm{Aut}(\overline{C})$ és finit. A més a més, és conegut que si $\overline{C}$ té gènere $g \geq 2$ i no és hiperel·líptica, aleshores admet un model d'equació a $\mathbb{P}^{g-1}(\overline{K})$ en g variables i $\mathrm{Aut}(\overline{C}) \leq \mathrm{PGL}_g(\overline{K})$ [FCB17, Teorema 1.1.7]. És a dir, conèixer els subgrups finits de $\mathrm{PGL}_n(\overline{K})$ ens permet saber quins són els possibles grups d'automorfismes $\mathrm{Aut}(\overline{C})$.

Conèixer els subgrups finits de $\mathrm{PGL}_n(\overline{K})$ també ens permet preguntar-nos si tots aquests són grup d'automorfismes d'alguna corba $\overline{C}$. Trobem avenços recents en aquest sentit deguts a Harui en [Har19] per corbes planes i a Avila, Ortiz i Troncoso per superfícies quàrtiques [AOT24] emprant la classificació de $\mathrm{PGL}_4(\mathbb{C})$ de Blichfeldt [Bli17].

Essent novells en aquest camp d'estudi, hem recorregut cronològicament els avenços descrits per tal de descobrir fins a quin punt s'havia desenvolupat la classificació. És per aquest motiu que un dels principals objectius d'aquest treball és servir com a recull dels diferents articles que, més enllà del llibre d'en Blichfeldt [Bli17], es troben dispersos en la literatura matemàtica. Es destaca especialment que s'aporten les taules amb els subgrups primitius finits de $\mathrm{SL}_n(\mathbb{C})$ per $n = 4, 5, 6, 7$, donats per Feit en [Fei71]. Es poden consultar en el teorema (5.1).

Alhora, és també l'objectiu d'aquest document proveir de definicions bàsiques unificades i actualitzades, tot aclarint-les respecte l'ús que se'n fa en la literatura tant de finals del segle XIX, com actualment. Aquest procès comprèn les seccions 2 i 3. En la secció 2 també es pretén posar llum a la diferència entre classificar $\mathrm{GL}_n(K)$ i $\mathrm{PGL}_n(K)$, sovint sobreentesa i que rarament es comenta més enllà dels treballs originals de Schur. Finalment, també es considera rellevant la modernització d'alguns dels resultats clàssics més àmpliament acceptats, en particular, en la secció 4 es dona una demostració en llenguatge actual del teorema de Blichfeldt [Bli17, §64, Thm. 5], estenent-la de $\mathbb{C}$ a un cos K algebraicament tancat de característica 0.

L'últim objectiu del treball és contribuir a la classificació dels grups finits primitius de $\mathrm{PGL}_n(\mathbb{C})$. En la secció 5.2 s'aporta un programa que permet determinar una llista de grups finits simples entre els quals apareixen tots els possibles grups finits simples primitius de $\mathrm{PGL}_n(\mathbb{C})$, per un n fix, però que no permet determinar quins dels grups donats són els primitius. La descripció del programa es dona en la secció 5.2.1. Els resultats obtinguts pel programa per $\mathrm{PGL}_n(\mathbb{C})$ per $n = 8, 9, 10$ es comenten en 5.2.2. Les taula de candidats a grups finits simples primitius de $\mathrm{PGL}_n(\mathbb{C})$ per $12 \leq n \leq 20$ es pot consultar en l'annex D taula 7.

2 Definicions i resultats preliminars

2.1 Convenis i definicions bàsiques per la classificació

En primer lloc, cal donar algunes definicions, convenis i notacions que s'empraran al llarg de tot el document.

- La lletra K sempre denotarà un cos. Les propietats del cos K varien en funció de la secció i resultat.
- Es defineix $\mathrm{GL}(V)$ com el grup dels isomorfismes lineals $f : V \to V$. Notem que si $\dim(V) = n$ aleshores sempre es poden prendre coordenades sobre K^n i treballar amb $\mathrm{GL}_n(K) \coloneqq \mathrm{GL}(K^n)$. Per tant, parlarem sempre de $\mathrm{GL}_n(K)$.
- Siguin $A, B \in \mathrm{GL}_n(K)$, aleshores es defineix la relació d'equivalència $A \sim B \Leftrightarrow A = kB$ per algun $k \in K$. Aleshores, es defineix el grup quocient $\mathrm{PGL}_n(K) \coloneqq \mathrm{GL}_n(K)/_\sim$.
- Es denotarà el centre d'un grup G com $Z(G)$. El centre de $\mathrm{GL}_n(K)$, $Z(\mathrm{GL}_n(K))$, és el grup de les matrius diagonals amb diagonal constant, és a dir, els múltiples de la identitat.
- Des del punt de vista de teoria de grups es pot donar una definició equivalent de $\mathrm{PGL}_n(K)$ emprant el centre: $\mathrm{PGL}_n(K) \coloneqq \mathrm{GL}_n(K)/Z(\mathrm{GL}_n(K))$.
- El concepte *classificació* d'un grup G fa referència al conjunt dels subgrups finits de G quocient una relació d'equivalència. Hi ha dues relacions d'equivalència que es consideren: la isomorfia i la conjugació.
- La classificació que volem determinar és llevat d'isomorfia. Ara bé, per tal que el problema sigui viable és necessari estudiar una classificació llevat conjugació. Així, en general, quan es parla de classificació d'un grup és fa referència a la classificació llevat conjugació.
- Quan K és algebraicament tancat, $\mathrm{PGL}_n(K)$ i $\mathrm{PSL}_n(K)$ són isomorfs [JS87, p.20]. En aquest cas, tant una classificació de $\mathrm{GL}_n(K)$ com una classificació de $\mathrm{SL}_n(K)$ indueixen una classificació de $\mathrm{PGL}_n(K)$.

Al llarg d'aquest document es farà servir diverses tècniques i notació de teoria de representacions lineals i projectives dels grups finits. Pels detalls sobre la diferència entre ambdues vegeu la secció 2.2, aquí fixem algunes primeres nocions.

- A no ser que es digui el contrari, sempre que es faci referència a una representació d'un grup G, $\rho : G \to \mathrm{GL}_n(K)$ ($\rho : G \to \mathrm{PGL}_n(K)$) o es parli de "representar", es considera una representació injectiva (faithfull) de tal manera que el grup $\rho(G) \leq \mathrm{GL}_n(K)$ ($\rho(G) \leq \mathrm{PGL}_n(K)$) on $\rho(G)$ és isomorf a G.
- Habitualment es prescindirà d'escriure $\rho(G)$ per denotar la representació (lineal o projectiva) del grup G. En aquests casos es definirà G com a subgrup de $\mathrm{GL}_n(K)$ o $\mathrm{PGL}_n(K)$ i es parlarà indistintament de grup o representació.

Per tal de dur a terme una classificació de $\mathrm{GL}_n(K)$, clàssicament es divideixen els possibles grups en tres tipus disjunts. A continuació es dona la definició clàssica d'aquests tipus de grups prenent-se com a referència les definicions de [Bli17, §14, §60]. Les definicions per a $\mathrm{PGL}_n(K)$ és donen en la secció 2.2.

Definició 2.1 (Grup transitiu/intransitiu)**.** Sigui $G \leq \mathrm{GL}_n(K)$ un grup finit, es diu que G és *intransitiu* si existeix una conjugació del grup $B \in \mathrm{GL}_n(K), G_B = B^{-1}GB$ tal que tots els elements de G_B s'escriuen com a matrius bloc diagonals amb almenys dos blocs. En cas contrari, es diu que el grup és *transitiu.*

Definició 2.2 (Grup primitiu/imprimitiu)**.** Sigui $G \leq \mathrm{GL}_n(K)$ un grup finit transitiu, es diu que G és *imprimitiu* si existeix una conjugació del grup $B \in \mathrm{GL}_n(K), G_B = B^{-1}GB$ tal que es pot realitzar la mateixa divisió per blocs en totes les matrius $A \in G_B$ de manera que si

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1m} \\ A_{21} & A_{22} & \cdots & A_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & \cdots & A_{mm} \end{pmatrix} \tag{1}$$

on els A_{ii} són matrius quadrades, per cada $j = 1, \dots, m$ existeix un únic $i_j \in \{1, \dots, m\}$ tal que $A_{ij} = \mathbf{0}$ si $i \neq i_j$, on $\mathbf{0}$ és la matriu de zeros de les dimensions corresponents, i $\bigcup_{i=1}^{m} \{i_j\} = \{1, \dots, m\}$. Si G és transitiu i no és imprimitiu es diu que G és *primitiu*.

La definició anterior de grup imprimitiu és equivalent a dir que es poden separar per blocs totes les matrius de G_B de tal forma que per cada matriu existeix una reordenació dels blocs tal que el resultat és una matriu bloc diagonal, en altres paraules, hi ha un únic bloc no nul per fila i columna. La separació per blocs ha de ser la mateixa per tots els elements de G_B però la posició dels blocs no nuls no ha de ser la mateixa. A més, els blocs en què es separen totes les matrius no estan restringits a tenir la mateixa dimensió.

Es donen a continuació diverses nocions bàsiques de teoria de representacions lineals. El lector es pot dirigir a [Ser77] per aprofundir en aquest tema.

Definició 2.3 (Representació irreductible)**.** [Ser77, §1.4, p.7] Sigui $\rho : G \to \mathrm{GL}_n(K)$ una representació lineal del grup G. Es diu que ρ és *irreductible* si no existeix cap subespai vectorial de K^n que sigui invariant per ρ excepte el trivial 0 i ell mateix K^n.

Teorema 2.4. *Tota representació lineal és una suma directa de representacions irreductibles.*

Demostració. [Ser77, §1.4, p.7, Thm 2] □

Definició 2.5 (Representació reduïble)**.** Sigui $\rho : G \to \mathrm{GL}_n(K)$ una representació lineal del grup G. Es diu que ρ és *reduïble* si és la suma directa de dos o més representacions irreductibles.

A partir de les nocions anteriors es té la següent caracterització dels grups intransitius i transitius.

Lema 2.6. *Sigui G un grup finit i $\rho : G \to GL_n(K)$ una representació de G. Aleshores $\rho(G) \leq GL_n(K)$ és un grup intransitiu si i només si ρ és una representació reduïble.*

Demostració. Suposis que $\rho(G)$ és intransitiu, aleshores existeix una base en la qual totes les matrius de $\rho(G)$ són bloc-diagonals. Per tant, si el nombre de blocs en que descomponen és k, aleshores existeix una descomposició de $K^n = V_1 \oplus \cdots \oplus V_k$ on V_i és el subespai vectorial associat al bloc i. Notis que per construcció si $g \in \rho(G)$ aleshores $g(V_i) = V_i$ per tot $i = 1, \dots, k$ i per tot $g \in \rho(G)$, per tant, són espais invariants i la representació ρ és reduïble.

Si ρ és una representació reduïble aleshores existeix almenys un subespai vectorial V de K^n tal que $\rho(G)(V) = V$, a més, existeix un complement V' de V tal que $K^n = V \oplus V'$ i que també és invariant sota ρ [Ser77, §1.3, p.6, Thm 1]. Així, triant com a base la suma directa de dues bases de V i V' les matrius de $\rho(G)$ descomponen en dos blocs diagonals, és a dir, $\rho(G)$ és intransitiu. □

Corol·lari 2.7. *Sigui $\rho : G \to GL_n(K)$ una representació de G. Aleshores $\rho(G) \leq GL_n(K)$ és un grup transitiu si i només si ρ és una representació irreductible.*

Igual que amb la noció d'intransitiu, la noció de representació imprimitiva també permet caracteritzar la noció de grup imprimitiu. Ara bé, a diferència del cas anterior, si ρ és una representació imprimitiva de G, $\rho(G)$ no té perquè ser un grup imprimitiu. Això és perquè la definició donada d'imprimitivitat requereix que $\rho(G)$ sigui transitiu, és a dir, que ρ sigui irreductible. En general, però, aquesta restricció no està lligada a una representació imprimitiva.

Definició 2.8 (Representació imprimitiva)**.** Sigui $\rho : G \to \mathrm{GL}_n(K)$ una representació lineal del grup finit G, siguin $V_1, \ldots, V_k$ subespais vectorials disjunts de K^n tals que $K^n = V_1 \oplus \cdots \oplus V_k$. Es diu que ρ és una representació imprimitiva si per cada $g \in G$ i per cada $1 \leq i \leq k$ es té que $\rho(g)(V_i) = V_j$ per algun $1 \leq j \leq k$.

Observació 2.9. Notem que en ser $\rho(g)$ invertible, l'aplicació que associa cada i amb una j tal que $\rho(g)(V_i) = V_j$ és bijectiva i, per tant, cada $\rho(g)$ té associada una certa permutació de S_k. Els detalls sobre aquestes permutacions i com formen un grup es discuteix en §3.2.

Un esperaria per coherència amb el llenguatge clàssic que si el grup de permutacions associat a G fos transitiu, aleshores la representació fos irreductible, però això no és cert.

Exemple 2.10. Sigui ρ la representació per matrius de permutació de A_5 a $\mathrm{GL}_5(\mathbb{C})$. Aquesta representació té associats dos caràcters irreductibles d'ordres 1 i 4 , per tant, no és irreductible. De fet, es possible donar un resultat més general. Si $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ és la representació amb matrius de permutació d'un grup $G \leq S_n$ aleshores ρ és la suma de la representació trivial i la representació estàndard[1] [Ful91, §4.3, p.55].

És per aquest motiu que potser no es convenient emprar els termes *intransitiu* i *transitiu* per fer referència a reduïble i irreductible respectivament. Amb aquest comentari, la caracterització de grup imprimitiu queda com el següent.

Lema 2.11. *Sigui G un grup finit i $\rho : G \to GL_n(K)$ una representació lineal de G. Aleshores ρ és imprimitiva i irreductible si i només si $\rho(G)$ és imprimitiu.*

Demostració. Si ρ és imprimitiva i irreductible aleshores ρ és transitiu. En ser ρ imprimitiva existeixen $V_1, \ldots, V_k$ subespais vectorials disjunts de K^n tals que $K^n = V_1 \oplus \cdots \oplus V_k$ i que per cada $g \in G$ i per cada $1 \leq i \leq k$ es té que $\rho(g)(V_i) = V_j$ per algun $1 \leq j \leq k$. Per veure la unicitat de les parelles (i, j) demanada en la definició de grup imprimitiu, notem que si $\rho(g)(V_i) = \rho(g)(V_{i'}) = V_j$ aleshores com $\rho(g^{-1}) = \rho(g)^{-1}$ es té que $V_i = V_{i'} = \rho(g)^{-1}(V_j)$. En ser els $V_l, 1 \leq l \leq k$ disjunts dos a dos forçosament $i = i'$. Triant com a base la suma directa de bases dels V_i s'obté la descomposició en blocs donada en la definició de grup imprimitiu.
Si $\rho(G)$ és imprimitiu i es prenen com a subespais vectorials $V_1, \ldots, V_k$ aquells associats als diferents blocs, s'obté que la representació és imprimitiva. ☐

Corol·lari 2.12. *Sigui $\rho : G \to GL_n(K)$ una representació de G. Aleshores $\rho(G) \leq GL_n(K)$ és un grup primitiu si i només si ρ és una representació irreductible i no imprimitiva.*

A partir d'aquestes caracteritzacions queda establert el següent fet:

Observació 2.13. Com a grup abstracte G pot tenir per un n fix representacions que resultin en grups reduïbles, imprimitius o primitius. Aquestes representacions, tot i ser isomorfes, no seran conjugades entre sí i, per tant, a nivell de classificació llevat conjugació es consideren diferents.

2.2 Les diferències entre $\mathbf{GL}_n(K)$ i $\mathbf{PGL}_n(K)$

En aquesta secció es pretén respondre essencialment dues preguntes.

1. Quina és la relació entre una classificació de $\mathrm{GL}_n(K)$ i una classificació de $\mathrm{PGL}_n(K)$? §2.2.1

2. Com s'estenen adequadament les definicions dels diferents tipus de grups a $\mathrm{PGL}_n(K)$? §2.2.2

2.2.1 Relació entre les classificacions

Per tal de respondre la primera pregunta es nota el següent fet bàsic.

Observació 2.14. Una classificació de $\mathrm{GL}_n(K)$ indueix una classificació de $\mathrm{PGL}_n(K)$, simplement cal considerar la projecció dels grups classificats per la definició donada de $\mathrm{PGL}_n(K)$.

[1] Per més informació sobre què és la representació estàndard i exemples podeu consultar https://groupprops.subwiki.org/wiki/Standard_representation_of_the_symmetric_group

El fet anterior planteja una primera qüestió molt bàsica.

Pregunta 2.15. És la classificació de $\mathrm{GL}_n(K)$ la mateixa que $\mathrm{PGL}_n(K)$?

La resposta és que no. Sigui $G \leq \mathrm{GL}_n(K)$ un grup finit i sigui $\pi : \mathrm{GL}_n(K) \to \mathrm{PGL}_n(K)$ la projecció canònica, aleshores $\pi(G) \cong G/\left(Z(G) \cap Z(\mathrm{GL}_n(K))\right)$. Si la intersecció de centres és trivial, $\pi(G) \cong G$ indueix una representació projectiva de G sobre $\mathrm{PGL}_n(K)$, de tal manera que com a grup abstracte G es pot representar tant en $\mathrm{GL}_n(K)$ com en $\mathrm{PGL}_n(K)$. En canvi, si el centre no és trivial, aleshores $\pi(G)$ no és isomorf a G i no s'indueix una representació projectiva de G.

Pregunta 2.16. És la classificació de $\mathrm{PGL}_n(K)$ un subconjunt de la classificació de $\mathrm{GL}_n(K)$?

El que planteja aquesta pregunta és si hi pot haver grups abstractes que puguin ser representats a $\mathrm{PGL}_n(K)$ però no a $\mathrm{GL}_n(K)$. Això és equivalent a preguntar-se si totes les representacions projectives venen induïdes per representacions lineals projectades a $\mathrm{PGL}_n(K)$. La resposta és que no, vegis el següent exemple.

Exemple 2.17. El grup A_5 no té cap caràcter irreductible lineal complex d'ordre 2 [GAP]. Ara bé, el grup A_5 és també conegut clàssicament com el grup icosahedral, de les simetries de l'icosahedre. Klein [Kle75] va emprar aquesta descripció per mostrar que A_5 té una representació projectiva irreductible en $\mathrm{PGL}_2(\mathbb{C})$ i, per tant, A_5 té un caràcter irreductible projectiu d'ordre 2. Una descripció computacional més detallada d'aquest fet es pot trobar en la secció de l'annex A.2.2.

Fins ara s'ha conclòs que, tot i que la classificació de $\mathrm{GL}_n(K)$ es projecta a una classificació de $\mathrm{PGL}_n(K)$, ni són iguals ni una és subconjunt de l'altra a nivell del grups abstractes que contenen. Aleshores és convenient preguntar-se què succeeix en el cas contrari.

Pregunta 2.18. Quina informació dona una classificació de $\mathrm{PGL}_n(K)$ sobre la classificació de $\mathrm{GL}_n(K)$?

La resposta ve donada per la teoria de representacions projectives. Per tal de dur-ne a terme una discussió és necessari conèixer alguns conceptes bàsics d'aquesta teoria, una introducció més completa es pot trobar en l'annex A.1 o en [Kar85]. Principalment es requereixen les definicions dels conceptes de *grup de representació* (A.5) i multiplicador de Schur (A.4). Se'n dona un breu resum a continuació.

- El multiplicador de Schur d'un grup G es defineix com $M(G) = H^2(G, K^\times)$ el segon grup de cohomologia de G.
- Els grups de representació, habitualment denotats G^*, són extensions centrals de G per un grup A tal que $|G^*| = |G||M(G)|$. En el cas que K sigui de característica $p \nmid |A|$, $p \geq 0$ i algebraicament tancat aleshores $A \cong M(G)$ (Teorema A.6).
- En la teoria de representacions projectives de grups finits es demostra que tota representació projectiva d'un grup G es pot obtenir a partir de les representacions lineals dels grups de representació G^*.

Observació 2.19. En la literatura el multiplicador de Schur $M(G)$ s'acostuma a donar segons el seu ordre, i.e. $|M(G)|$, atès que en molts casos aquest ordre és un primer petit, però en la majoria dels casos per poder realitzar les extensions és necessari conèixer l'estructura explícita del grup abelià $M(G)$. Quan $M(G)$ és trivial, aleshores les representacions lineals de G són totes les possibles representacions projectives.

Observació 2.20. La representació lineal de G^* que indueix la representació projectiva de G no té perquè ser injectiva. És possible que la imatge $\rho(G)$ correspongui a una extensió central menor. Per exemple, en el cas de A_6 el grup de representació és $6A_6$. Ara bé, si no és injectiva és possible que $\rho(6A_6) \cong 3A_6$, $\rho(6A_6) \cong 2A_6$ o $\rho(6A_6) \cong A_6$. En aquesta situació, el grup que projecta a A_6 en $\mathrm{PGL}_n(K)$ des de $\mathrm{GL}_n(K)$ seria $\rho(6A_6)$.

Així doncs, una classificació de $\mathrm{PGL}_n(K)$ no indueix de forma directa una classificació de $\mathrm{GL}_n(K)$, atès que l'únic que es pot afirmar és que si $G \leq \mathrm{PGL}_n(K)$ aleshores algun grup G^* de representació de G o subgrup de G^* es pot pensar com a subgrup de $\mathrm{GL}_n(K)$. En canvi, això permet entendre la classificació de $\mathrm{GL}_n(K)$ com un conjunt de grups de representació (o subgrups d'aquests) dels subgrups finits de $\mathrm{PGL}_n(K)$.

2.2.2 Nocions anàlogues pel grup projectiu lineal

En la literatura clàssica, principalment [Bli17], les definicions relatives a la primitivitat i a la transitivitat donades pels grups lineals s'empren indistintament per parlar també dels grups de col·lineacions. La idea implícita (no aclarida en cap moment) és que en donar-se les definicions en forma matricial és el mateix considerar la matriu com la seva classe. Així, les definicions clàssiques (2.1), (2.2) són exactament les mateixes canviant $\mathrm{GL}_n(K)$ per $\mathrm{PGL}_n(K)$.

Definició 2.21 (Grup transitiu/intransitiu)**.** Sigui $G \leq \mathrm{PGL}_n(K)$ un grup finit, es diu que G és *intransitiu* si existeix una conjugació del grup $B \in \mathrm{PGL}_n(K), G_B = B^{-1}GB$ tal que tots els elements de G_B s'escriuen com a matrius bloc diagonals amb almenys dos blocs. En cas contrari, es diu que el grup és *transitiu*.

Definició 2.22 (Grup primitiu/imprimitiu)**.** Sigui $G \leq \mathrm{PGL}_n(K)$ un grup finit transitiu, es diu que G és *imprimitiu* si existeix una conjugació del grup $B \in \mathrm{PGL}_n(K), G_B = B^{-1}GB$ tal que es pot realitzar la mateixa divisió per blocs en totes les matrius $A \in G_B$ de manera que si

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1m} \\ A_{21} & A_{22} & \cdots & A_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1} & A_{m2} & \cdots & A_{mm} \end{pmatrix} \tag{2}$$

on els A_{ii} són matrius quadrades, per cada $j = 1, \ldots, m$ existeix un únic $i_j \in \{1, \ldots, m\}$ tal que $A_{ij} = \mathbf{0}$ si $i \neq i_j$, on $\mathbf{0}$ és la matriu de zeros de les dimensions corresponents, i $\bigcup_{i=1}^{m} \{i_j\} = \{1, \ldots, m\}$. Si G és transitiu i no és imprimitiu es diu que G és *primitiu*.

Ara bé, traslladar directament les definicions de $\mathrm{GL}_n(K)$ a $\mathrm{PGL}_n(K)$ suggereix que un grup projectiu serà intransitiu/transitiu o primitiu/imprimitiu si i només si ho és el seu grup de representació.

Lema 2.23. *Sigui $G \leq PGL_n(K)$ un grup finit i sigui $G^* \leq GL_n(K)$ un grup de representació de G tal que $\pi(G^*) = G$. Aleshores G és intransitiu (imprimitiu) si i només si G^* és intransitiu (imprimitiu).*

Demostració. Suposem que G^* és intransitiu (imprimitiu), aleshores es pot assumir sense pèrdua de generalitat que G^* ja disposa de l'estructura per blocs donada en les definicions, aleshores és clar que la classe de cada element de G^* conserva aquesta estructura de blocs, per tant, $\pi(G^*) = G$ és intransitiu (imprimitiu). Pel mateix argument, en el cas que G sigui intransitiu (imprimitiu) tots els representants de cada element de G tindran aquesta estructura, atès que el producte per un múltiple de la identitat no l'altera, per tant, G^* també és intransitiu (imprimitiu). □

Per donar el concepte de representació projectiva reduïble i imprimitiva és convenient descriure la següent acció.

Lema 2.24. *Sigui $\rho : G \to PGL_n(K)$ una representació projectiva del grup finit G, sigui V un subespai vectorial de K^n. Sigui $g \in G$ i $\widetilde{\rho(g)} \in GL_n(K)$ un aixecament de $\rho(g)$. Es defineix l'acció de $\rho(g)$ sobre V com $\rho(g)(V) := \widetilde{\rho(g)}(V)$. Aquesta acció està ben definida i és independent del representant.*

Demostració. En efecte, notem que si $\widetilde{\rho(g)}$ i $\widetilde{\rho(g)}'$ són dos aixecaments diferents de $\rho(g)$ aleshores existeix $d \in K^\times$ una constant tal que $\widetilde{\rho(g)} = d\,\widetilde{\rho(g)}'$. Així, si es consideren $W = \widetilde{\rho(g)}(V)$ i

$W' = \widetilde{\rho(g)}'(V)$, s'observa que si $v \in K^n$ aleshores $\widetilde{\rho(g)}(v) \in W$ però $\widetilde{\rho(g)}(v) = d\,\widetilde{\rho(g)}'(v) \in W$, per tant, $W' \subseteq W$. D'altra banda, $\widetilde{\rho(g)}'(v) \in W'$ però $\widetilde{\rho(g)}'(v) = (1/d)\widetilde{\rho(g)}(v) \in W'$ i, per tant, $W = W'$. □

Per tal de donar unes caracteritzacions similars a les de (2.6) i (2.11) i que respectin la propietat del lema (2.23) s'introdueixen diverses definicions sobre representacions projectives.

Definició 2.25. Sigui $\rho : G \to \mathrm{PGL}_n(K)$ una representació projectiva del grup G. Es diu que ρ és *irreductible* si no existeix cap subespai vectorial de K^n tal que sigui invariant per ρ excepte el trivial 0 i ell mateix K^n.

Definició 2.26. Sigui $\rho : G \to \mathrm{PGL}_n(K)$ una representació projectiva del grup finit G, siguin $V_1, \ldots, V_k$ subespais vectorials disjunts de K^n tals que $K^n = V_1 \oplus \cdots \oplus V_k$. Es diu que ρ és una representació imprimitiva si per cada $g \in G$ i per cada $1 \leq i \leq k$ es té que $\rho(g)(V_i) = V_j$ per algun $1 \leq j \leq k$.

Lema 2.27. *Sigui G un grup finit, sigui $\rho : G \to PGL_n(K)$ una representació projectiva induïda per $\tau : G^* \to GL_n(K)$. Aleshores ρ és irreductible si i només si ho és τ, ρ és imprimitiva si i només si ho és τ.*

Demostració. És conseqüència de l'equivalència entre les definicions A.1 i A.2 juntament amb la definició de grup de representació A.5. □

Essencialment, es dirà que un grup $G \leq \mathrm{PGL}_n(K)$ és reduïble, irreductible, imprimitiu o primitiu en funció de quines d'aquestes propietats tingui la representació lineal del grup de representació que indueix la representació projectiva G, donant lloc a les dues següents caracteritzacions.

Lema 2.28. *Sigui G un grup finit i sigui $\rho : G \to PGL_n(K)$ una representació projectiva de G. Es diu que $\rho(G)$ és irreductible si ρ és irreductible, en cas contrari es diu que $\rho(G)$ és reduïble.*

Demostració. El lema és conseqüència directa del lema (2.23) i el lema (2.27). □

Per tal de tenir la unicitat donada en la definició de grup imprimitiu cal el següent lema.

Lema 2.29. *Sigui $G \leq PGL_n(K)$ un grup finit imprimitiu amb una descomposició per blocs associada $K^n = V_1 \oplus \cdots \oplus V_k$, sigui $g \in G$ aleshores per cada $1 \leq j \leq k$ existeix un únic $1 \leq i \leq k$ tal que $g(V_i) = V_j$.*

Demostració. Suposem que existeixen dos nombres $1 \leq i, i' \leq k$ tals que $g(V_i) = V_j$ i $g(V_{i'}) = V_j$. Atès que g és invertible es té que $g^{-1}(V_j) = g^{-1}g(V_i) = V_i$ i alhora $g^{-1}(V_j) = g^{-1}g(V_{i'}) = V_{i'}$, per tant, $V_i = V_{i'}$ i, com els $V_l, 1 \leq l \leq k$ són disjunts dos a dos, necessàriament es té que $i = i'$. □

I la caracterització corresponent als grups imprimitius és:

Lema 2.30. *Sigui G un grup finit i sigui $\rho : G \to PGL_n(K)$ una representació projectiva de G. Es diu que $\rho(G)$ és imprimitiu si ρ és imprimitiva i irreductible, en cas contrari és diu que $\rho(G)$ és primitiu.*

Demostració. El lema és conseqüència directa del lema (2.23), el lema (2.27) i el lema (2.29). □

Dos exemples de com es relacionen aquestes definicions i caracteritzacions en el cas de les propietats de ser irreductible es detallen extensament en A.2. És especialment d'interès l'exemple A.2.2 sobre A_5, que mostra com el seu grup de representació, $SL(2,5)$, disposa d'una representació lineal irreductible d'ordre 2 que indueix una representació projectiva de A_5 d'ordre 2 irreductible.

Altres exemples també es poden trobar en la secció següent, on es tracten els grups intransitius i els grups imprimitius de $\mathrm{PGL}_n(K)$.

3 Els grups no primitius

3.1 Grups intransitius

Es comença per donar una descripció completa de com són els grups finits intransitius a $\mathrm{PGL}_n(K)$ per qualsevol n. Atès que tots els grups intransitius són conjugats a un grup amb totes les matrius bloc diagonals, s'estudiaran només com són els grups finits d'aquesta forma. Es comença per fixar notació i definir alguns subgrups de $\mathrm{PGL}_n(K)$ particulars.

Definició 3.1. Sigui $\lambda \vdash n$ una partició decreixent no trivial de n, és a dir, una r-tupla $(n_1, n_2, \ldots, n_r)$ amb $r > 1$, $n_1 + n_2 + \cdots + n_r = n$ i $n_i \geq n_{i+1}$ per tot $i = 1, \ldots, r-1$. Es defineix $\mathrm{PBD}_n(\lambda) \leq \mathrm{PGL}_n(K)$ com el subgrup de les matrius bloc diagonals amb blocs de dimensions donats per λ.

Observació 3.2. Notem que sempre que es disposi d'un grup finit intransitiu es pot triar una conjugació d'aquest grup de tal manera que els blocs apareguin ordenats conformant una certa partició decreixent de n i, per tant, tot grup intransitiu finit de $\mathrm{PGL}_n(K)$ és conjugat a un subgrup finit de $\mathrm{PBD}_n(\lambda)$ per algun $\lambda \vdash n$.

Les dues proposicions següents emfatitzen que si coneixem els grups finits dels $\mathrm{PGL}_m(K)$ amb $m < n$ aleshores també es coneixen els grups finits intransitius de $\mathrm{PGL}_n(K)$ en termes de successions exactes.

Proposició 3.3. *Sigui $n > 2$, $\lambda \vdash n$ una partició de n amb $\lambda = (n_1, n_2, \ldots, n_r)$ i $n_r = 1$, $G \in PBD_n(\lambda)$ un subgrup finit de $PGL_n(K)$, aleshores existeix un diagrama commutatiu*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^* & \xrightarrow{\iota} & PBD_n(\lambda) & \xrightarrow{\sigma} & PBD_{n-1}(\tilde{\lambda}) & \longrightarrow & 1 \quad \textit{(exacta)} \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & C & \longrightarrow & G & \longrightarrow & G' & \longrightarrow & 1 \quad \textit{(exacta)} \end{array} \tag{3}$$

on C és un grup cíclic, $\tilde{\lambda} \vdash n-1$ és la partició $\tilde{\lambda} = (n_1, n_2, \ldots, n_{r-1})$ que pot ser trivial.

Demostració. Considerem $G \in \mathrm{PBD}_n(\lambda)$ i el morfisme de grups $\iota : K^* \to \mathrm{PBD}_n(\lambda)$ que satisfà

$$\iota(\alpha) = \left(\begin{array}{c|c} I_{n-1} & 0 \\ 0 & \alpha \end{array}\right), \quad \alpha \in K^* \tag{4}$$

Sigui $C \leq K^*$ un grup cíclic que té com a imatge el subgrup normal de G donat pels elements de la forma anterior. Notem que C sempre té almenys un element, la identitat, i que en alguns casos pot ser el grup trivial. Considerem $\sigma : \mathrm{PBD}_n(\lambda) \to \mathrm{PBD}_{n-1}(\tilde{\lambda})$ el morfisme de grups natural definit per

$$\left(\begin{array}{c|c} A & 0 \\ 0 & \alpha \end{array}\right) \mapsto A \in \mathrm{PBD}_{n-1}(\tilde{\lambda}),\ \alpha \in K^* \tag{5}$$

Notem que $\mathrm{Ker}(\sigma) = \iota(K^*)$ per construcció i en la restricció $\mathrm{Ker}(\sigma|_G) = \iota(C)$. A més, σ i $\sigma|_G$ són exhaustives i, per tant, s'obtenen les successions exactes. $\square$

La següent proposició tracta el cas en què no hi ha blocs de dimensió 1.

Proposició 3.4. *Sigui $n > 2$, $\lambda \vdash n$ una partició de n amb $\lambda = (n_1, n_2, \ldots, n_r)$ i $n_r > 1$, $G \in PBD_n(\lambda)$ un subgrup finit de $PGL_n(K)$, aleshores existeix un diagrama commutatiu*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & PGL_{n_r}(K) & \xrightarrow{\iota} & PBD_n(\lambda) & \xrightarrow{\sigma} & PBD_{n-n_r}(\tilde{\lambda}) & \longrightarrow & 1 \quad \textit{(exacta)} \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & G' & \longrightarrow & 1 \quad \textit{(exacta)} \end{array} \tag{6}$$

on $\tilde{\lambda} \vdash n-1$ és la partició $\tilde{\lambda} = (n_1, n_2, \ldots, n_{r-1})$.

Demostració. La construcció de les aplicacions del diagrama és anàloga al cas de la proposició anterior ara amb

$$\iota(\alpha) = \left(\begin{array}{c|c} I_{n-n_r} & 0 \\ 0 & A' \end{array}\right), \quad \sigma\left[\left(\begin{array}{c|c} A & 0 \\ 0 & A' \end{array}\right)\right] = A, \qquad A \in \mathrm{PBD}_{n-n_r}(\tilde{\lambda}),\ A' \in \mathrm{PGL}_{n_r}(K) \tag{7}$$

□

Notem que separar els casos $n_r = 1$ i $n_r > 1$ és necessari atès que $\mathrm{PGL}_1(K) = \{1\}$ i no s'estaria tenint en compte la possibilitat d'estendre els grups finits de $\mathrm{PBD}_{n-1}(\tilde{\lambda})$ per un grup cíclic finit.

3.1.1 Exemple: Els grups intransitius de $\mathbf{PGL}_5(K)$

Per tal de descriure els possibles grups intransitius de $\mathrm{PGL}_5(K)$, notem que les possibles particions de 5 (llevat de la trivial) són

$$\big\{(4,1), (3,2), (3,1^2), (2^2,1), (2,1^3), (1^5)\big\} \tag{8}$$

i, per tant, es té la següent classificació.

Proposició 3.5. *Sigui $G \in PGL_5(K)$ un subgrup finit intransitiu amb una partició associada λ, i sigui G_λ el grup conjugat a G tal que $G_\lambda \in PBD_5(\lambda)$. Aleshores es compleix una de les següents:*

(a) $\lambda = (4,1)$ *i es té un diagrama commutatiu*

$$\begin{tikzcd} 1 \arrow[r] & K^* \arrow[r, "\iota"] & PBD_5(\lambda) \arrow[r, "\sigma"] & PGL_4(K) \arrow[r] & 1 & \textit{(exacta)} \\ 1 \arrow[r] & C \arrow[r] \arrow[u, hook] & G \arrow[r] \arrow[u, hook, "\phi"] & G' \arrow[r] \arrow[u, hook] & 1 & \textit{(exacta)} \end{tikzcd} \tag{9}$$

on C és un grup cíclic.

(b) $\lambda = (3,2)$ *i es té un diagrama commutatiu*

$$\begin{tikzcd} 1 \arrow[r] & PGL_2(K) \arrow[r, "\iota"] & PBD_5(\lambda) \arrow[r, "\sigma"] & PGL_3(K) \arrow[r] & 1 & \textit{(exacta)} \\ 1 \arrow[r] & H \arrow[r] \arrow[u, hook] & G \arrow[r] \arrow[u, hook, "\phi"] & G' \arrow[r] \arrow[u, hook] & 1 & \textit{(exacta)} \end{tikzcd} \tag{10}$$

(c) $\lambda = (3,1^2), (2^2,1), (2,1^3), (1^5)$ *i per cada* $\tilde{\lambda} = (3,1), (2^2), (2,1^2), (1^4)$ *respectivament es té un diagrama commutatiu*

$$\begin{tikzcd} 1 \arrow[r] & K^* \arrow[r, "\iota"] & PBD_5(\lambda) \arrow[r, "\sigma"] & PBD_4(\tilde{\lambda}) \arrow[r] & 1 & \textit{(exacta)} \\ 1 \arrow[r] & C \arrow[r] \arrow[u, hook] & G \arrow[r] \arrow[u, hook, "\phi"] & G' \arrow[r] \arrow[u, hook] & 1 & \textit{(exacta)} \end{tikzcd} \tag{11}$$

on C és un grup cíclic.

Demostració. Els apartats (a), (b) i (c) són directes de les proposicions (3.3) i (3.4) tenint en compte ϕ l'isomorfisme que donat per la conjugació de G i G_λ. □

3.2 Grups imprimitius

L'estudi dels grups imprimitius es centra en estudiar l'acció definida en el lema (2.24) i la caracterització emprant representacions projectives donada en el lema (2.11). Es comença per una descripció de com és l'acció del grup imprimitiu.

Lema 3.6. *Sigui $G \leq GL_n(K)$ un grup finit imprimitiu amb una descomposició per blocs associada $K^n = V_1 \oplus \cdots \oplus V_k$, aleshores l'acció de G sobre el conjunt dels espais vectorials $\mathcal{X} = \{V_1, \ldots, V_k\}$ és transitiva, és a dir, per tot (i,j) amb $1 \leq i,j \leq k$ existeix $g \in G$ tal que $g(V_i) = V_j$.*

Demostració. Suposem que l'acció de G és intransitiva, aleshores existeix un V_i tal que $g(V_i) = V_i$ per tot $g \in G$. Sigui $V = V_1 \oplus \ldots V_{i-1} \oplus V_{i+1} \oplus \ldots V_k$ i considerem la descomposició $K^n = V_i \oplus V$, es té que $g(V_i) = V_i$ i $g(V) = V$ per tot $g \in G$, és a dir, G és reduïble, que contradiu que sigui imprimitiu. □

Observació 3.7. Com ja s'ha comentat anteriorment en l'exemple (2.10) el recíproc del lema anterior no és cert.

El següent resultat descriu com són les dimensions dels espais vectorials de la descomposició $K^n = V_1 \oplus \cdots \oplus V_k$.

Lema 3.8. *Sigui $G \leq GL_n(K)$ un grup finit imprimitiu amb una descomposició associada $K^n = V_1 \oplus \cdots \oplus V_k$, aleshores $\dim(V_1) = \cdots = \dim(V_k) = m$ tal que $n = mk$.*

Demostració. Pel lema (3.6) existeix $g \in G$ tal que $g(V_i) = V_{i+1}$, $1 \leq i < k$. En ser g un isomorfisme lineal es té que $\dim(V_i) = \dim(V_{i+1})$. Per tant, es té que $\dim(V_1) = \cdots = \dim(V_k)$. Si s'anomena $m = \dim(V_1)$ aleshores notem que $n = \sum_{j=1}^{k} \dim(V_j) = \sum_{j=1}^{k} m = km$. □

Observació 3.9. En termes de la definició clàssica de grup imprimitiu el lema anterior demostra que els blocs en que descomponen les matrius són quadrats i tots de la mateixa dimensió.

Definició 3.10. Sigui $G \leq \mathrm{GL}_n(K)$ un grup finit imprimitiu amb una descomposició associada $K^n = V_1 \oplus \cdots \oplus V_k$ tal que $\dim(V_1) = m$. Aleshores es diu que G te forma m-nomial.

Corol·lari 3.11. *Sigui $G \leq GL_p(K)$ un grup finit imprimitiu amb p primer, aleshores G és 1-nomial també anomenat monomial.*

Demostració. Atès que $m|p$ implica $m = 1$ o $m = p$, pel lema 3.8 la descomposició associada de K^p ha de ser $K^p = V_1 \oplus \cdots \oplus V_p$ amb $\dim(V_1) = 1$. □

EL següent teorema fou donat en la notació clàssica per Blichfeldt en [Bli17, §60, Thm 1].

Teorema 3.12. *Sigui $G \leq GL_n(K)$ un grup finit imprimitiu amb forma m-nomial, aleshores existeix un morfisme de grups $\varphi : G \to S_k$ tal que $\mathrm{Im}(\varphi) = \mathcal{S}$, i $\mathcal{S}$ és transitiu. S'anomenarà $\mathcal{S} \leq S_k$ el grup de permutacions associat a G.*

Demostració. Sigui $g \in G$ amb descomposició associada $K^n = V_1 \oplus \cdots \oplus V_k$, considerem l'aplicació $\tau_g : \{1, \ldots, k\} \to \{1, \ldots, k\}$ tal que $\tau_g(i) = j$ si i només si $g(V_i) = V_j$. Notem que aquesta aplicació és invertible amb inversa $\tau_{g^{-1}}$ ja que $\tau_{g^{-1}}(\tau_g(i)) = \tau_{g^{-1}}(j) = i$ atès que $g^{-1}(V_j) = V_i \iff g(V_i) = V_j$. Pel mateix argument $\tau_g(\tau_g^{-1}(j)) = \tau_g(i) = j$. Així, τ_g és una permutació.
Cal veure ara que $\mathcal{S} = \{\tau_g \mid g \in G\}$ és un grup sota composició. Notem a priori que $\mathcal{S}$ està tancat per inverses com a conseqüència de la discussió anterior i conté la identitat, així només és necessari comprovar que està tancat pel producte. Siguin $g, h \in G$, i considerem τ_g, τ_h, aleshores com $g(h(V_i)) = (gh)(V_i)$ es té que $(\tau_g \circ \tau_h)(i) = \tau_g(\tau_h(i)) = \tau_{gh}(i)$ per tot $1 \leq i \leq k$. Així, $\mathcal{S}$ és un grup de permutacions en k nombres, $\mathcal{S} \leq S_k$. Finalment, es defineix $\varphi : G \to S_k$ tal que $\varphi(g) = \tau_g$, clarament és morfisme de grups i $\mathrm{Im}(\varphi) = \mathcal{S}$ per construcció. □

Observació 3.13. El cas $\mathrm{PGL}_n(K)$ és el mateix emprant el lema (2.24).

3.2.1 Grups finits imprimitius monomials de $\mathrm{GL}_n(K)$ i $\mathrm{PGL}_n(K)$

Pel corol·lari (3.11) es sap que tots els grups imprimitius de $\mathrm{GL}_p(K)$ i $\mathrm{PGL}_p(K)$ amb p primer tenen forma monomial, així, descriure com són aquests grups permet descriure tots els grups imprimitius dels $\mathrm{GL}_p(K)$ i $\mathrm{PGL}_p(K)$. En l'article [DZ04] Dixon i Zalesski presenten la classificació dels grups finits imprimitius de $\mathrm{GL}_p(\mathbb{C})$, extensible també a K algebraicament tancat i amb $\mathrm{car}(K) \geq 0$ llevat d'algunes modificacions.

Nosaltres en aquest treball farem un tractament més clàssic dels grups imprimitius monomials, i sense restringir-nos a $n = p$ primer. Farem servir la següent notació:

- Sigui $e_1, \dots, e_n$ la base canònica de K^n, aleshores la matriu de permutació d'una permutació $\sigma \in S_n$ es defineix com la matriu P_σ tal que $P_\sigma(e_i) = e_{\sigma(i)}$. Es denota per $\mathcal{P}_n \leq \mathrm{GL}_n(K)$ el subgrup de les matrius de permutació de S_n en $\mathrm{GL}_n(K)$.
- S'anomena $\mathcal{D} \leq \mathrm{GL}_n(K)$ al subgrup de les matrius diagonals de $\mathrm{GL}_n(K)$.
- Quan es parli de grup imprimitiu monomial ja pren el grup en la base adequada per a què es trobi en la forma de blocs de la definició clàssica (2.2).

Matricialment, en la base adequada els elements del grup prenen una forma similar a la de les matrius de permutacions. Així doncs, l'objectiu d'aquesta subsecció és descriure els grups imprimitius monomials a partir de matrius de permutacions.

Lema 3.14. *Sigui $G \leq GL_n(K)$ un grup finit imprimitiu monomial i sigui $\mathcal{S}$ el seu grup de permutacions associat, aleshores existeix un morfisme de grups $\psi : G \to \mathcal{P}_n$ tal que $\mathrm{Im}(\psi) = \mathcal{P}$ són les matrius de permutacions de $\mathcal{S}$. En particular, existeixen $P \in \mathcal{P}_n$ i $D \in \mathcal{D}$ tals que si $g \in G$ tenim que $g = PD$.*

Demostració. Notem que el morfisme associat a G donat en el teorema (3.12) es pot estendre a través de l'isomorfisme natural $\phi : S_n \to \mathcal{P}_n$ a un morfisme $\psi : G \to \mathcal{P}_n$ tal que $\psi = \phi \circ \varphi$ i que satisfà $\psi(G) = \mathcal{P} = \phi(\mathcal{S})$. Notem que per definició de φ les posicions no nul·les de $g \in G$ correspondran a les posicions no nul·les de $\psi(g)$, així doncs, es pot escriure $g = PD$ on $P = \psi(g)$ i $D = \psi(g)^{-1}g$ és una matriu diagonal. $\square$

A partir d'aquesta descripció dels elements del grup es vol donar un conjunt de generadors per aquests grups.

Lema 3.15. *Sigui $G \leq GL_n(K)$ un grup finit imprimitiu en forma monomial, sigui $\psi(G) = \mathcal{P} \leq \mathcal{P}_n$ la representació del grup de permutacions de S_n associat a G. Aleshores, existeix un subgrup de matrius diagonals $\mathcal{Y} \leq G \cap \mathcal{D}$ i per cada $P_i \in \mathcal{P}$, $1 \leq i \leq |\mathcal{P}|$ una matriu diagonal $D_i \in \mathcal{D}$ tals que $G = \langle \mathcal{Y}, P_1D_1, \dots, P_{|\mathcal{P}|}D_{|\mathcal{P}|} \rangle$.*

Demostració. Es parteix de $G = \langle G \rangle$ com a conjunt de generadors i es procedeix a reduir-lo pel següent procediment:
Sigui $g \in G$ i $\psi(g) = P$, suposem que existeix un altre $g' \in G$ tal que $\psi(g') = P$, aleshores, notem que $g = PD$, $g' = PD'$ on $D, D' \in \mathcal{D}$ són matrius diagonals. Aleshores, $g^{-1}g' = (DP)^{-1}D'P = D^{-1}PP^{-1}D' = D^{-1}D' \in \mathcal{D} \cap G$. Iterant aquest procès per cada $P \in \mathcal{P}$ i considerant $\mathcal{Y}$ com el subgrup normal $\mathcal{Y} = G \cap D$ de les matrius diagonals de G, s'obté el conjunt de generadors donat en el lema. $\square$

La següent proposició redueix encara més el conjunt de generadors considerant un conjunt de generadors de $\mathcal{P}$.

Proposició 3.16. *Sigui $G \leq GL_n(K)$ un grup finit imprimitiu en forma monomial, sigui $\psi(G) = \mathcal{P} \leq \mathcal{P}_n$ la representació del subgrup de permutacions de S_n associat a G, i sigui un subconjunt $\mathcal{L} \subseteq \mathcal{P}$ tal que $\langle \mathcal{L} \rangle = \mathcal{P}$. Aleshores, existeix un subgrup de matrius diagonals $\mathcal{Y} \leq G \cap \mathcal{D}$ tal que $G = \langle \mathcal{Y}, L_1D_1, \dots, L_{|\mathcal{L}|}D_{|\mathcal{L}|} \rangle$, on $1 \leq i \leq |\mathcal{L}|$, $L_i \in \mathcal{L}$ i $D_i \in \mathcal{D}$ són matrius diagonals.*

Demostració. Del lema anterior (3.15) es té que $G = \langle \mathcal{Y}, P_1\tilde{D}_1, \dots, P_{|\mathcal{P}|}\tilde{D}_{|\mathcal{P}|} \rangle$, notem que com $\mathcal{L} \subseteq \mathcal{P}$ aleshores hi ha certs P_j que es corresponen als L_i generadors, es tria com a D_i els $\tilde{D}_j$ associats a aquests P_j. Aleshores notem que com $\mathcal{L}$ genera $\mathcal{P}$, cada element P_j es pot escriure com $P_j = \prod_\alpha L_\alpha^{\delta_\alpha}$ un producte finit dels L_i i els seus inversos, on els $\delta_\alpha \in \{-1, 1\}$. Considerem ara el producte $\tilde{P}_j = \prod_\alpha (L_\alpha D_\alpha)^{\delta_\alpha} \in G$ i observem que $\varphi(\tilde{P}_j) = \varphi(P_j)$ tenen la mateixa permutació associada. Així, el producte $\tilde{P}_j^{-1}P_jD_j \in G$, notem que $\varphi(\tilde{P}_j^{-1}P_jD_j) = id$ i, per tant, és diagonal. Així, $\tilde{P}_j^{-1}P_jD_j \in \mathcal{Y}$ i $\tilde{P}_j(\tilde{P}_j^{-1}P_jD_j) = P_jD_j$, per tant, es pot obtenir P_jD_j a partir dels L_iD_i i un element de $\mathcal{Y}$, així, es pot treure del conjunt de generadors sense alterar el grup. □

Aquesta darrera reducció del conjunt de generadors és significativa, considerem el següent exemple.

Exemple 3.17. Sigui $n \geq 3$ i considerem els grups de permutacions S_n i A_n els grups simètric i alternat. Aquests grups són 2-generats [Cona, Thm. 2.5, Thm 3.5] i transitius. Sigui $G \leq \mathrm{GL}_n(K)$ un grup imprimitiu tal que $\varphi(G) = S_n$ o bé $\varphi(G) = A_n$, per tant, és suficient considerar el subgrup de les matrius diagonals $\mathcal{Y} = G \cap \mathcal{D}$ i dos elements de G tals que tinguin per imatge de φ els corresponents generadors. Per contra, en el cas del lema (3.15) s'havien de donar $n!$ generadors a part del grup diagonal per S_n i $n!/2$ per A_n.

Observació 3.18. El cas $\mathrm{PGL}_n(K)$ és el mateix emprant el lema (2.24).

El següent resultat és exclusiu a $\mathrm{PGL}_n(K)$. Quan un dels generadors del grup en qüestió té associat un cicle d'ordre n aleshores es pot simplificar més el conjunt de generadors via conjugació.

Lema 3.19. *Sigui $G \leq PGL_n(K)$ un grup finit imprimitiu, $\mathcal{Y} = G \cap \mathcal{D}$ el subgrup de les matrius diagonal de G i un conjunt $H \subseteq G$ tal que $G = \langle \mathcal{Y}, H \rangle$. Sigui $h \in H$ tal que $\varphi(h)$ és un cicle d'ordre n i considerem $h = DT$ on $D \in \mathcal{D}$ és diagonal i $\psi(h) = T$, aleshores si $\gamma = \left(\prod_{i=1}^{n-1} a_i\right)^{-\frac{1}{n}} \in K$ existeix $B \in PGL_n(K)$ tal que $\tilde{G} = B^{-1}GB$ i $\tilde{G} = \langle \tilde{\mathcal{Y}}, T, \tilde{H} \rangle$ on $\tilde{H} = B^{-1}(H \backslash \{h\})B$ i $\tilde{\mathcal{Y}} = B^{-1}\mathcal{Y}B$.*

Demostració. En primer lloc notem que si T és un cicle d'ordre n aleshores existeix una matriu de permutació P tal que $P^{-1}TP = T_n$ [McK13, Prop. 6.6].

$$T_n = \left(\begin{array}{c|c} 0 & 1 \\ \hline I_{n-1} & 0 \end{array}\right) \tag{12}$$

A més a més, $P^{-1}\mathcal{Y}P$ continua essent un grup de matrius diagonals i $P^{-1}GP$ manté la forma monomial. Per tant, només cal veure que si $\varphi(h) = T_n$ aleshores existeix una conjugació que transformi T_nD en T_n. Considerem la matriu diagonal $B = \mathrm{diag}(1, a_1\gamma, a_1a_2\gamma, \ldots, \gamma\prod_{i=1}^{n-1} a_i)$ on $\gamma = \left(\prod_{i=1}^{n-1} a_i\right)^{-\frac{1}{n}}$. Una simple computació mostra que $BT_nB^{-1} = \frac{1}{\gamma}DT_n = DT_n$ i, per tant, $B^{-1}DT_nB = T_n$. □

3.2.2 Exemple: Els grups imprimitius de $\mathbf{GL}_5(K)$ i $\mathbf{PGL}_5(K)$

Per tal de comprendre com poden ser els grups imprimitius de $\mathrm{GL}_5(K)$ i $\mathrm{PGL}_5(K)$ primer és necessari conèixer quins són els subgrups transitius de S_5. Aquests subgrups són coneguts llevat conjugació i es poden trobar en la base de dades sobre grups de permutacions transitius del [GAP].

Lema 3.20. *Sigui $\mathcal{S} \leq S_5$ un subgrup transitiu, aleshores és conjugat a un dels grups següents:*

(a) $S_5 = \langle (1,2,3,4,5), (1,2) \rangle$.

(b) $A_5 = \langle (1,2,3,4,5), (1,2,3) \rangle$.

(c) $H_5 = \langle (1,2,3,4,5), (2,3,5,4) \rangle \cong GA(1,5) \cong Sz(2)$.

(d) $D_5 = \langle (1,2,3,4,5), (2,5)(3,4) \rangle$

(e) $C_5 = \langle (1,2,3,4,5) \rangle \cong \mathbb{Z}/5\mathbb{Z}$.

Es fixa la següent notació relativa a les matrius de permutació dels generadors anteriors.

$$T=\begin{pmatrix}0&0&0&0&1\\1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\end{pmatrix}, R_1=\begin{pmatrix}0&1&0&0&0\\1&0&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}, R_2=\begin{pmatrix}0&0&1&0&0\\1&0&0&0&0\\0&1&0&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}, \tag{13}$$

$$R_3=\begin{pmatrix}1&0&0&0&0\\0&0&0&1&0\\0&1&0&0&0\\0&0&0&0&1\\0&0&1&0&0\end{pmatrix}, R_4=\begin{pmatrix}1&0&0&0&0\\0&0&0&0&1\\0&0&0&1&0\\0&0&1&0&0\\0&1&0&0&0\end{pmatrix} \tag{14}$$

Es dona primer una classificació reduïda pel cas $\mathrm{PGL}_5(K)$ amb K algebraicament tancat.

Proposició 3.21. *Sigui K algebraicament tancat, sigui $G \leq PGL_5(K)$ un subgrup imprimitiu finit en forma monomial i considerem $\mathcal{Y} = G \cap \mathcal{D}$ el subgrup de les matrius diagonals, aleshores G és conjugat a un dels següents grups G'.*

(a) Si $\varphi(G) = S_5$ aleshores $G' = \langle \mathcal{Y}, T, D_1R_1\rangle$.

(b) Si $\varphi(G) = A_5$ aleshores $G' = \langle \mathcal{Y}, T, D_2R_2\rangle$.

(c) Si $\varphi(G)$ és conjugat a H_5 aleshores $G' = \langle \mathcal{Y}, T, D_3R_3\rangle$.

(d) Si $\varphi(G)$ és conjugat a D_5 aleshores $G' = \langle \mathcal{Y}, T, D_4R_4\rangle$.

(e) Si $\varphi(G)$ és conjugat a C_5 aleshores $G' = \langle \mathcal{Y}, T\rangle$

On D_1, D_2, D_3, D_4 són matrius diagonals d'ordre finit.

Demostració. Pel lema (3.20) tots els grups $\varphi(G)$ han de ser conjugats a un dels donats en aquest, a més, com A_5 i S_5 són normals a S_5 es té la igualtat. Aleshores per la proposició (3.16), es sap que $G = \langle \mathcal{Y}, \mathcal{L}\rangle$ on $\mathcal{Y}$ és el subgrup de matrius diagonals de G, $\mathcal{L}$ és un conjunt de generadors de $\psi(G) = \mathcal{P}$. Prenent els generadors donats en el lema (3.20) es construeix el $\mathcal{L} = \{T, R_i\}$ corresponent. A més, pel lema (3.19) existeix una conjugació B que porta $\langle \mathcal{Y}, DT\rangle$ a $\langle \mathcal{Y}, T\rangle$, així, emprant la mateixa conjugació sobre G es pot passar de $\langle \mathcal{Y}, DT, \tilde{D}_iR_i\rangle$ a $\langle \mathcal{Y}, T, B^{-1}\tilde{D}_iR_iB\rangle$, notem però que com B és diagonal $\varphi(B^{-1}\tilde{D}_iR_iB) = \varphi(R_i)$ i, per tant, existeix D_i tal que $B^{-1}\tilde{D}_iR_iB = D_iR_i$. Finalment s'obté $G' = \langle \mathcal{Y}, T, D_iR_i\rangle$. ◻

Proposició 3.22. *Sigui $G \leq GL_5(K)$ o bé $G \leq PGL_5(K)$ un subgrup imprimitiu finit en forma monomial i considerem $\mathcal{Y} = G \cap \mathcal{D}$ el subgrup de les matrius diagonals, aleshores G és conjugat a un dels següents grups G'.*

(a) Si $\varphi(G) = S_5$ aleshores $G' = \langle \mathcal{Y}, DT, D_1R_1\rangle$.

(b) Si $\varphi(G) = A_5$ aleshores $G' = \langle \mathcal{Y}, DT, D_2R_2\rangle$.

(c) Si $\varphi(G)$ és conjugat a H_5 aleshores $G' = \langle \mathcal{Y}, DT, D_3R_3\rangle$.

(d) Si $\varphi(G)$ és conjugat a D_5 aleshores $G' = \langle \mathcal{Y}, DT, D_4R_4\rangle$.

(e) Si $\varphi(G)$ és conjugat a C_5 aleshores $G' = \langle \mathcal{Y}, DT\rangle$

On D, D_1, D_2, D_3, D_4 són matrius diagonals d'ordre finit.

Demostració. La demostració és anàloga però sense poder fer ús del lema (3.19). ◻

3.3 Identificació de grups imprimitius i intransitius

El teorema (3.24) degut a Blichfeldt dona condicions suficients per decidir que un grup no és primitiu. La demostració requereix el lema següent:

Lema 3.23. *Sigui $G \leq GL_n(K)$ un grup finit d'ordre g, sigui $T \in G$ una transformació qualsevol del grup i considerem K tal que té totes les arrels g-èssimes de la unitat i $(\mathrm{car}(K), g) = 1$. Aleshores es compleixen les següents propietats:*

(a) Existeix $B \in GL_n(K)$ tal que $\tilde{T} = B^{-1}TB$ és diagonal.

(b) Els valors propis de T són arrels de la unitat.

Demostració. Si T té ordre $m \mid g$ aleshores el polinomi mínim de T divideix $X^m - 1$ que, com K té totes les arrels g-èssimes de la unitat i $(\mathrm{car}(K), g) = 1$ totes les arrels de $X^m - 1$ són diferents i, per tant, el polinomi mínim descompon completament en arrels diferents, per [Conb, Thm. 4.11] es té que T diagonalitza. Sigui B la matriu tal que $T = B\Lambda B^{-1}$ amb Λ la matriu de valors propis de T, notem que $T^m = B\Lambda^m B^{-1} = I$ i, per tant, $\Lambda^m = I$ que implica que els valors propis λ_i satisfan $\lambda_i^m - 1 = 0$ i, per tant, són arrels de la unitat.

□

Teorema 3.24. *[Bli17, §61, Lemma 1, p.79] Sigui $G \leq GL_n(K)$ un grup finit on K amb les condicions del lema (3.23), sigui $H \trianglelefteq G$ un subgrup normal abelià de G no format únicament per múltiples de la identitat, aleshores G és imprimitiu o intransitiu.*

Demostració. Pel lema 3.23 tots els elements de H diagonalitzen en alguna base, en ser H abelià aquests diagonalitzen simultàniament. Siguin $K^n = V_1 \oplus \cdots \oplus V_k$ subespais propis tals que H diagonalitza simultàniament, és a dir, per tot $h \in H$, $v \in V_i$, $h(v) = \lambda_i(h)v$ on $\lambda_i(h) \in K$ n'és el valor propi associat. Aleshores, si $V \subseteq K^n$ és un subespai vectorial que compleix per tot $h \in H$, $v \in V$, $h(v) = \mu(h)v$, $\mu(h) \in K$ necessàriament $V \subseteq V_j$ per algun $1 \leq j \leq k$. Sigui ara $g \in G$, atès que H és un subgrup normal es compleix que per tot $h \in H$, $g^{-1}hg = \tilde{h} \in H$. Notem aleshores que si $v \in V_i$, $g^{-1}hg(v) = \tilde{h}(v) = \lambda_i(\tilde{h})v$ per tot $1 \leq i \leq k$, fet que implica que $h(g(v)) = \lambda_i(\tilde{h})g(v)$. Definint $U_i := g(V_i)$ obtenim que per tot $u \in U_i$ es compleix $h(u) = \lambda_i(\tilde{h})u$, per tant, $\lambda_i(\tilde{h})$ és valor propi de h i $U_i \subseteq V_{j_i}$ per algun $1 \leq j_i \leq k$. Com l'anterior és cert per tot $1 \leq i \leq k$ veiem que g permuta els espais vectorials V_i, per tant, G és imprimitiu o intransitiu. □

Corol·lari 3.25. *Sigui $G \leq PGL_n(K)$ un grup finit, sigui $H \trianglelefteq G$ un subgrup normal abelià de G no trivial, aleshores G és imprimitiu o intransitiu.*

La condició que dona el teorema és suficient, per veure que no és necessària es dona un exemple d'un grup simple imprimitiu.

Exemple 3.26. Considerem el grup simple de Mathieu M_{11}. Aquest grup simple té una única representació irreductible de grau 11 sobre $\mathbb{Z}$ [GAP] i, a més, aquesta representació és imprimitiva i es pot posar en forma monomial emprant els següents dos generadors[2]:

$$M_1 = \begin{pmatrix} 0&1&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1 \end{pmatrix}, M_2 = \begin{pmatrix} -1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&0&0&0&-1&0 \\ 0&0&0&0&0&0&1&0&0&0&0 \end{pmatrix}$$

[2] Es poden consultar més detalls sobre aquesta representació en l'enllaç https://brauer.maths.qmul.ac.uk/Atlas/v3/matrep/M11G1-Zr11B0

En estar en forma monomial els generadors es poden donar com a matrius de permutació producte una matriu diagonal, en aquest cas observem que

$$\varphi(M_1) = (1,2)(3,4)(6,7)(9,10) \in S_{11}, \quad \varphi(M_2) = (2,6,5,3)(7,11,9,8) \in S_{11} \tag{15}$$

La matriu M_1 ja és una matriu de permutació, per tant té associada la identitat com a matriu diagonal $D_1 = I$, en canvi, M_2 presenta dos nombres diferents de 1, la matriu diagonal

$$D_2 = \mathrm{diag}(-1,1,1,1,1,1,1,1,1,-1,1)$$

tal que $M_2 = \psi(M_2)D_2 \implies \psi(M_2) = M_2D_2$.

Observació 3.27. En la introducció de l'article [Wal69] es dona la condició del Teorema (3.24) com a condició equivalent a ser grup primitiu, però l'anterior exemple demostra que no és cert.

4 Cotes sobre l'ordre de grups primitius

4.1 Primers que poden dividir l'ordre d'un grup primitiu

L'objectiu d'aquesta secció és donar una demostració en llenguatge actual del teorema (4.1) de Blichfeldt. La demostració original per $K = \mathbb{C}$ es pot consultar en [Bli17, §64, Thm. 5] o bé en [Bli03, Thm. 4].

Teorema 4.1. *[Bli17, §64, Thm. 5] Considerem K algebraicament tancat de $car(K) = 0$. Sigui $G \leq SL_n(K)$ grup finit primitiu, sigui ℓ un nombre primer, aleshores $\ell \nmid |G|$ si $\ell > (2n+1)(n-1)$.*

La demostració segueix una estructura similar a la de Blichfeldt:

1. Trobar una equació $F = 0$ sobre K on F és una expressió formada per sumes i productes d'arrels de la unitat.

2. Descriure una congruència mòdul ℓ a partir de $F = 0$.

3. Trobar un grup abelià normal $H \trianglelefteq G$ amb $|H| = \ell^k$ per algun $k > 0$.

Abans però, són necessaris diversos resultats previs.

4.1.1 Resultats previs

Teorema 4.2 (Kronecker/Rédei, Bruijn, Schoenberg)**.** *Considerem un cos K de característica zero algebraicament tancat. Sigui $A = \{\alpha_i, i = 1, \ldots, n\}$ un conjunt d'arrels de la unitat de K tals que*

$$\sum_{i=1}^{n} \alpha_i = 0 \tag{16}$$

aleshores existeixen subconjunts disjunts A_{p_j}, $j = 1, \ldots, k$ tals que $|A_{p_j}| = p_j$ primers,

$$A_{p_j} = \{\xi_{p_j}^m, m = 0, \ldots, p_j - 1\}$$

on ξ_p és una arrel primitiva de la unitat que satisfà $x^p - 1 = 0$ i $\{\eta_{p_j}, j = 1, \ldots, k\}$ arrels de la unitat tals que la suma anterior descompon en

$$\sum_{j=1}^{k} \left(\eta_j \sum_{\alpha \in A_{p_j}} \alpha \right) = 0 \tag{17}$$

Demostració. La demostració d'un teorema més general es discuteix en [LL00], que en particular tracta aquest cas al principi. Blichfeldt en [Bli17, §132] atribueix el teorema a Kronecker en [Kro54] i tot que és Blichfeldt qui el demostra explícitament en [Bli03]. □

Corol·lari 4.3. *Sota les hipòtesis i notació del teorema (4.2), la suma d'arrels de la unitat que s'anul·la es pot escriure com*

$$\sum_{j=1}^{k} \left(\eta_j \sum_{\alpha \in A_{p_j}} \alpha \right) = 0 \tag{18}$$

on η_{p_j} té ordre m_j tal que o bé és coprimer amb p_j o bé $p_j^2 \mid m_j$.

Demostració. Denotem l'ordre de η_{p_j} per β, $\beta = \prod_{i=1}^{k} l_i^{m_i}$ la descomposició en factors primers de β, aleshores η_{p_j} es pot escriure com a producte d'arrels primeres de la unitat ζ_{l_i} d'ordres $l_i^{m_i}$ de tal manera que $\eta_{p_j} = \prod_{i=1}^{k} \zeta_{l_i}$. Suposem que $p_j \mid m$ però $p_j^2 \nmid m$, aleshores existeix un ζ_{l_i}, que es denotarà ζ, que satisfà $\zeta \in A_{p_j}$. Notem que en conseqüència,

$$\zeta \sum_{\alpha \in A_{p_j}} \alpha = \sum_{\alpha \in A_{p_j}} \alpha \tag{19}$$

atès que només permuta les arrels de posició en la suma, per tant, es pot escriure $\eta_{p_j} = \tilde{\eta}_{p_j}\zeta$ amb l'ordre de $\tilde{\eta}_{p_j}$ coprimer amb p_j i

$$\eta_{p_j} \sum_{\alpha \in A_{p_j}} \alpha = \tilde{\eta}_{p_j} \sum_{\alpha \in A_{p_j}} \alpha \tag{20}$$

□

A continuació s'introdueix una estructura que resultarà de gran utilitat per executar el segon pas de la demostració.

Definició 4.4. Sigui $Z \subset K$ subanell de K tal que $Z \cong \mathbb{Z}$ isomorfisme d'anells. Sigui $\mathcal{U} \leq (K, \cdot)$ el subgrup multiplicatiu de K format per totes les arrels de la unitat. S'anomena $Z\mathcal{U} = Z[\mathcal{U}]$ al grup-anell que pren Z com anell i $\mathcal{U}$ com a grup multiplicatiu.

Observació 4.5. Notem que l'estructura de grup-anell implica que $Z\mathcal{U}$ és alhora un Z-mòdul amb base $\mathcal{U}$ i un anell. A més a més, com Z,$\mathcal{U}$ són subestructures de K, es pot definir un morfisme $\varphi : Z\mathcal{U} \to K$ tal que si $t \in Z\mathcal{U}$, $a_j \in Z$, $\alpha_j \in \mathcal{U}$, $m \in \mathbb{N}$

$$t = \sum_{j=1}^{m} a_j \alpha_j, \qquad \varphi(t) = \sum_{j=1}^{m} i(a_j)\iota(\alpha_j) \tag{21}$$

on $i : Z \to K$, $\iota : U \to K$ són les inclusions de Z i U a K. Aquesta aplicació és morfisme d'anells i no és injectiva. En particular, observem que $\operatorname{Ker}\varphi$ estarà format per totes aquelles sumes d'arrels de la unitat tals que siguin nul·les en K, per exemple, si $\xi^k = 1, \xi \in Z\mathcal{U}$ aleshores es pot construir $s = \sum_{i=0}^{k-1} \xi^i \in Z\mathcal{U}$ i $\varphi(s) = 0$ on $s \neq 0$.

Del Teorema (4.2) s'obté de forma directa el següent lema.

Lema 4.6. $\operatorname{Ker}\varphi$ *és l'ideal de* $Z\mathcal{U}$ *generat per les sumes* $\sum_{i=0}^{p-1} \xi_p$ *on* p *primer i* $\xi_p^p - 1 = 0$ *arrel primitiva de la unitat.*

Es pot interpretar aquest lema com una traducció del Teorema (4.2) i del Corol·lari (4.3) a $Z\mathcal{U}$ en relació a com descomponen els elements del $\operatorname{Ker}(\varphi)$. Per últim, considerem el següent lema.

Lema 4.7. *Sigui* $T \in GL_n(K)$ *una transformació d'ordre finit* m*, aleshores el caràcter* $\chi(T)$ *es pot expressar com una suma d'arrels de la unitat.*

Demostració. El caràcter $\chi(T)$ és la traça de T com endomorfisme lineal en K^n. A més a més, la traça d'una matriu és correspon amb la suma dels seus valors propis i, pel lema 3.23, els valors propis de T són arrels de la unitat. □

El lema anterior permet donar la següent definició.

Definició 4.8. Sigui un grup finit $G \in \mathrm{GL}_n(K)$, es defineix el caràcter $\Psi : G \to Z\mathcal{U}$ amb $\Psi(T) = \sum_{i=1}^{n} \lambda_i$ on $T \in G$ i λ_i són els valors propis de T com a elements de $Z\mathcal{U}$.

Observació 4.9. El morfisme φ permet recuperar el caràcter habitual $\chi : G \to K$ de G a través de $\chi = \varphi \circ \Psi$.

4.1.2 Obtenció de l'equació $F = 0$

A partir d'aquí s'adopta la notació descrita en el Teorema (4.1) i es considera $\ell > n$. En primer lloc, observem que pel primer teorema de Sylow, si $\ell \mid |G|$ aleshores existeix $T \in G$ tal que l'ordre de T és ℓ i es pot considerar G com el grup en el qual T és diagonal i té determinant 1. Aleshores, pel lema (3.23) es compleix que

$$T = (\alpha_1, \ldots, \alpha_n), \quad \alpha_i^\ell = 1, \quad \prod_{i=1}^{n} \alpha_i = 1 \tag{22}$$

Observació 4.10. T no pot ser múltiple de la identitat, so ho fos, es tindria que $\det(T) = \alpha_i^n = 1$ i alhora $\alpha_i^\ell = 1$, com $\ell > n$ primer es té que els α_i han de ser 1. Per tant, es pot assumir que es tenen almenys dos elements diferents en la diagonal. Per simplicitat es considera que els α_i són tots diferents, en cas que no ho fossin la discussió és equivalent.

Sigui $V \in G$ una altra transformació d'ordre ℓ. Es denota per $v_1, v_2, \dots, v_n$ els valors de la diagonal de V. Es considera ara els productes de la forma $VT^k, k \in \mathbb{N}$ i els seus corresponents caràcters $\chi(VT^k) = \sum_{i=1}^n v_i \alpha_i^k$. Es pren ara el conjunt d'expressions

$$\left\{\chi(VT^k) = \sum_{i=1}^n v_i \alpha_i^k \mid k = 0, \dots, n-1\right\} \cup \left\{\chi(VT^m) = \sum_{i=1}^n v_i \alpha_i^m\right\} \tag{23}$$

on s'ha pres un $0 \leq m \leq \ell - 1$ natural. Aquest conjunt d'expressions es pot codificar de forma matricial com

$$\tilde{\mathcal{A}}\vec{v} = \begin{pmatrix} \chi(V) & 1 & 1 & \dots & 1 \\ \chi(VT) & \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & & & & \vdots \\ \chi(VT^{n-1}) & \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \\ \chi(VT^m) & \alpha_1^m & \alpha_2^m & \dots & \alpha_n^m \end{pmatrix} \begin{pmatrix} -1 \\ v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{24}$$

Fixant-nos ara només en la matriu $\tilde{\mathcal{A}}$, observem que la primera columna és combinació lineal de la resta (emprant el vector de l'expressió com a aquesta combinació lineal) i així, $\det(\tilde{\mathcal{A}}) = 0$. Ara bé, observem que els elements de la matriu $\tilde{\mathcal{A}}$ es troben tots en $\mathrm{Im}(\varphi)$, en el cas de la traça a través de $\chi = \varphi \circ \Psi$. Per tant, s'anomena $\mathcal{A} \in \mathcal{M}_{n+1}(Z\mathcal{U})$ la matriu que té els mateixos coeficients que $\tilde{\mathcal{A}}$ però pensats sobre $Z\mathcal{U}$. Observem que el que ens interessa no és tant la matriu sinó el seu determinant, així que definim

$$\mathcal{D}(\tilde{\mathcal{A}}) = \begin{vmatrix} \Psi(V) & 1 & 1 & \dots & 1 \\ \Psi(VT) & \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & & & & \vdots \\ \Psi(VT^{n-1}) & \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \\ \Psi(VT^m) & \alpha_1^m & \alpha_2^m & \dots & \alpha_n^m \end{vmatrix} \in Z\mathcal{U} \tag{25}$$

Notem que en ser φ un morfisme d'anells podem entrar-lo dins el determinant i es recupera $(\varphi \circ \mathcal{D})(\mathcal{A}) = \det(\tilde{A}) = 0$, en particular, $\mathcal{D}(\mathcal{A}) \in \operatorname{Ker}\varphi$.

Es procedeix a continuació a reescriure $\mathcal{D}(\mathcal{A})$. En primer lloc, es desenvolupa el determinant per la primera columna i es denoten els menors corresponents a cada columna $\mathcal{A}_i$.

$$\mathcal{D}(\mathcal{A}) = \sum_{i=0}^{n-1} \Psi(VT^i)\mathcal{A}_i + \Psi(VT^m)\mathcal{A}_n \tag{26}$$

Observem que $\mathcal{A}_n = (-1)^n \mathcal{V}$ on $\mathcal{V}$ és el determinant de Vandermonde en $\alpha_1, \dots, \alpha_n$ i la resta de menors $\mathcal{A}_i$ són el mateix determinant però on s'ha eliminat la i-èssima fila i s'han afegit en l'última fila $\alpha_1^m, \dots, \alpha_n^m$. Els determinants que prenen la forma dels menors $\mathcal{A}_i$ es poden escriure com $\mathcal{A}_i = \mathcal{V}\mathcal{B}_i = \mathcal{A}_n\mathcal{B}_i$ on els $\mathcal{B}_i \in Z\mathcal{U}$ són uns certs polinomis de Schur avaluats en $\alpha_1, \dots, \alpha_n$ que es discuteixen en detall a l'annex B, així, es pot reescriure:

$$\mathcal{D}(\mathcal{A}) = \mathcal{V}\left(\Psi(VT^m)\mathcal{B}_n + \sum_{i=0}^{n-1} \Psi(VT^i)\mathcal{B}_i\right) = \mathcal{V}\mathcal{F} \tag{27}$$

Ara notem que $(\varphi \circ \mathcal{D})(\mathcal{A}) = \varphi(\mathcal{V})\varphi(\mathcal{F}) = 0$ però $\varphi(\mathcal{V}) = \prod_{1 \leq i < j \leq n}(\alpha_j - \alpha_i)$ i com s'ha pres $\alpha_i \neq \alpha_j$ aquest terme no s'anul·la, és a dir, $\varphi(\mathcal{F}) = 0 \Rightarrow \mathcal{F} \in \operatorname{Ker}(\varphi)$. Així, pel Lema (4.6), $\mathcal{F}$ admet la reordenació següent

$$\mathcal{F} = a_1 \sum_{i=0}^{\ell_1 - 1} \xi_{\ell_1}^i + a_2 \sum_{i=0}^{\ell_2 - 1} \xi_{\ell_2}^i + \dots + a_k \sum_{i=0}^{\ell_k - 1} \xi_{\ell_k}^i = \sum_{j=1}^k a_j \sum_{i=0}^{\ell_j - 1} \xi_{\ell_j}^i \tag{28}$$

on $k > 0$ és un nombre natural desconegut, ℓ_j són primers diferents dos a dos, ξ_{ℓ_j} són arrels de la unitat primitives que satisfan $x^{\ell_j} - 1 = 0$ i els coeficients $a_j \in Z\mathcal{U}$ tal que satisfan les condicions del Corol·lari (4.3).

Notem ara que les imatges $\varphi(\mathcal{B}_i)$ es corresponen als menors de $\det(\tilde{A})$ desenvolupats de la mateixa manera que els $\mathcal{A}_i$, els anomenem $\tilde{\mathcal{A}}_i$. Així, es té que $\tilde{\mathcal{A}}_n = \varphi(\mathcal{V}) \neq 0$ i es correspon que $\varphi(\mathcal{B}_i) = \tilde{\mathcal{A}}_i/\tilde{\mathcal{V}} = \tilde{\mathcal{B}}_i$. Així, es defineix l'expressió F com

$$F = \varphi(\mathcal{F}) = (\varphi \circ \Psi)(VT^m)\varphi(\mathcal{B}_n) + \sum_{i=0}^{n-1}(\varphi \circ \Psi)(VT^i)\varphi(\mathcal{B}_i) = \chi(VT^m)\tilde{\mathcal{B}}_n + \sum_{i=0}^{n-1}\chi(VT^i)\tilde{\mathcal{B}}_i = 0 \quad (29)$$

4.1.3 Obtenció d'una congruència mòdul ℓ a partir de F

L'objectiu d'aquesta part de la demostració és crear $f : Z\mathcal{U} \to \mathbb{Z}$ de tal forma que $f(\mathcal{F}) \equiv 0 \mod \ell$. Per fer-ho s'introdueixen les següents definicions:

- S'anomena $\mathcal{U}_\ell \subset \mathcal{U}$ al subconjunt que conté totes les arrels de la unitat d'ordre ℓ (inclosa la identitat 1).
- S'anomena $\mathfrak{B} \subset \mathcal{U}$ un subconjunt que per cada primer $p \neq \ell$ conté una única arrel ξ_p d'ordre p, és a dir, de les $\xi_p^j, j = 1, \ldots, p-1$ el conjunt $\mathfrak{B}$ en conté únicament una d'elles.
- Donats $X, Y \in \mathcal{U}$ dos conjunts es denota per $X \cdot Y = \{xy \mid x \in X, y \in Y\}$.

A partir de les definicions anteriors es construeix una partició en tres conjunts de $\mathcal{U}$: $\mathcal{U}_1, \mathcal{U}_0, \mathcal{U}_{-1} \subset \mathcal{U}$ disjunts dos a dos:

$$\begin{aligned} \mathcal{U}_\ell \subseteq \mathcal{U}_1 &= \mathcal{U}_\ell \cdot \left\{ \prod_{\xi \in X} \xi \;\middle|\; X \subset \mathfrak{B}, |A| < \infty \text{ i parell} \right\}, \prod_{\xi \in \varnothing} \xi := 1 \\ \mathcal{U}_{-1} &= \mathcal{U}_\ell \cdot \left\{ \prod_{\xi \in X} \xi \;\middle|\; X \subset \mathfrak{B}, |A| < \infty \text{ i senar} \right\} \\ \mathcal{U}_0 &= \mathcal{U} \backslash (\mathcal{U}_1 \uplus \mathcal{U}_{-1}) \end{aligned} \quad (30)$$

on el símbol $\uplus$ denota la unió disjunta.

Observació 4.11. El conjunt $\mathcal{U}_\ell$ és de fet un subgrup $\mathcal{U}_\ell \leq \mathcal{U}$, mentre que $\mathcal{U}_1, \mathcal{U}_{-1}, \mathcal{U}_0$ són simplement conjunts.

A continuació, es defineix l'aplicació $g : \mathcal{U} \to \{-1, 0, 1\}$ tal que

$$g(\xi) = \begin{cases} 1 \text{ si } \xi \in \mathcal{U}_1 \\ -1 \text{ si } \xi \in \mathcal{U}_{-1} \\ 0 \text{ si } \xi \in \mathcal{U}_0 \end{cases} \quad (31)$$

A partir d'aquesta aplicació g es defineix l'aplicació $f : Z\mathcal{U} \to \mathbb{Z}$.

Definició 4.12. Sigui $t \in Z\mathcal{U}$, $b_j \in Z$, $\beta_j \in \mathcal{U}$,

$$t = \sum_{j=1}^{k} b_j \beta_j, \qquad f(t) = \sum_{j=1}^{k} i(b_j) g(\beta_j) \quad (32)$$

On i és la inclusió donada en l'observació (4.5)

Observació 4.13. f preserva l'estructura de Z-mòdul en el sentit que $f(t+s) = f(t) + f(s), s \in Z\mathcal{U}$ i si $a \in Z$ aleshores $f(at) = af(t)$. Ara bé, com g no preserva l'estructura de grup f tampoc. Per tant, f no és morfisme d'anells i en general $f(ts) \neq f(t)f(s)$.

Els dos següents lemes ens donen condicions sobre quan $f(ts) = f(t)f(s)$.

Lema 4.14. *Sigui $t \in Z\mathcal{U}$ i $s \in Z\mathcal{U}_\ell$ aleshores $f(ts) = f(s)f(t)$*

Demostració. Considerem $a_j, b_r \in Z$, $\alpha_j \in \mathcal{U}, \beta_r \in \mathcal{U}_\ell$ aleshores descrivim

$$ts = \left(\sum_{j=1}^{k} a_j\alpha_j\right)\left(\sum_{r=1}^{h} b_r\beta_r\right) = \sum_{j=1}^{k}\sum_{r=1}^{h} a_j b_r \alpha_j \beta_r \implies f(ts) = \sum_{j=1}^{k}\sum_{r=1}^{h} i(a_j)i(b_r)g(\alpha_j\beta_r) \quad (33)$$

Observem que si $g(\alpha_j\beta_r) = g(\alpha_j)g(\beta_r)$ aleshores f també es separa, així, és suficient veure que donats $\alpha \in \mathcal{U}, \beta \in \mathcal{U}_\ell$ es compleix que $g(\alpha\beta) = g(\alpha)g(\beta)$. Es consideren els tres casos $\alpha \in \mathcal{U}_1$, $\alpha \in \mathcal{U}_{-1}$ i $\alpha \in \mathcal{U}_0$:

(i) Si $\alpha \in \mathcal{U}_1$ aleshores com $\beta \in \mathcal{U}_\ell$, $\alpha\beta \in \mathcal{U}_1$ per definició de $\mathcal{U}_1$, per tant, $g(\alpha\beta) = 1$ i $g(\alpha)g(\beta) = 1 \cdot 1 = 1$.

(ii) Si $\alpha \in \mathcal{U}_{-1}$ aleshores com $\beta \in \mathcal{U}_\ell$, $\alpha\beta \in \mathcal{U}_{-1}$ per definició de $\mathcal{U}_{-1}$, per tant, $g(\alpha\beta) = -1$ i $g(\alpha)g(\beta) = 1(-1) = -1$.

(iii) Si $\alpha \in \mathcal{U}_0$, en primer lloc observem que α no pot ser un element de $\mathcal{U}_\ell$. Sigui N l'ordre de α, aleshores $N = q_1 \dots q_l$ on $q_i = p_i^{N_i}$ i p_i primers diferents, és a dir, el desenvolupament de N en factors primers. Aleshores $\alpha = \xi_{q_1} \cdots \xi_{q_l}$ on ξ_{q_i} són arrels primitives de la unitat d'ordre q_i. Atès que $\alpha \in \mathcal{U}_0$ existeix algun d'aquests factors que no pertany a $\mathfrak{B}$ ni a $\mathcal{U}_\ell$, aleshores $\alpha\beta$ també conté aquest factor i, per tant, no pertany ni a $\mathcal{U}_1$ ni a $\mathcal{U}_{-1}$, és a dir, $\alpha\beta \in \mathcal{U}_0$ i tenim $g(\alpha\beta) = 0$, $g(\alpha)g(\beta) = 0 \cdot 1 = 0$.

□

Lema 4.15. *Si $t = \sum_{r=1}^{k} b_r\beta_r \in Z\mathcal{U}$ tal que $b_r \in Z$, $\beta_r \in \mathcal{U}$ satisfent que si m_r és l'ordre de β_r aquest sigui coprimer amb p primer o $p^2 \mid m_r$, i $s = \sum_{j=0}^{p-1} \xi^j$ on $\xi^p - 1 = 0$, aleshores $f(ts) = f(t)f(s)$.*

Demostració. En la notació anterior i pel mateix argument que en el Lema (4.14) és suficient veure que $g(\alpha\xi^j) = g(\alpha)g(\xi^j)$ on $\alpha \in \mathcal{U}_\xi = \mathcal{U}\backslash(\mathcal{U} \cdot \{\xi, \dots, \xi^{p-1}\})$. En primer lloc observem que un dels $\xi^j \in \mathfrak{B}$, sense pèrdua de generalitat podem suposar que $\xi \in \mathfrak{B}$. Al llarg de la demostració es fa referència a la descomposició d'una arrel, aquesta descomposició és la que s'empra en el Lema (4.14) part (iii) on s'expressa una arrel com el producte d'arrels d'ordre potències de primers. Així, es vol veure que si es té $\alpha \in \mathcal{U}_\xi$ i $\beta = \xi^j$ per algun $j = 1, \dots, p-1$ aleshores $g(\alpha\beta) = g(\alpha)g(\beta)$. Els primers dos casos que cal separar són

(a) $\beta = \xi$, és a dir, $\beta \in \mathcal{U}_{-1}$ i $g(\beta) = -1$.

(b) $\beta = \xi^j, j \neq 1$, és a dir, $\beta \in \mathcal{U}_0$ i $g(\beta) = 0$.

Dins de cada cas s'han de considerar 3 casos més: $\alpha \in \mathcal{U}_1 \cap \mathcal{U}_\xi$, $\alpha \in \mathcal{U}_{-1} \cap \mathcal{U}_\xi$ i $\alpha \in \mathcal{U}_0 \cap \mathcal{U}_\xi$. Es comença per provar (a):

(a.i) Si $\alpha \in \mathcal{U}_1 \cap \mathcal{U}_\xi$ aleshores α és un producte parell o zero de diferents elements de $\mathfrak{B}$ que no conté ξ i producte d'elements de $\mathcal{U}_\ell$, notem doncs que $\alpha\beta = \xi\alpha$ és un producte senar d'elements diferents de $\mathfrak{B}$ i producte d'elements de $\mathcal{U}_\ell$, per tant, $\alpha\beta \in \mathcal{U}_{-1}$. Així, $g(\alpha\beta) = -1, g(\alpha)g(\beta) = 1(-1) = -1$.

(a.ii) Si $\alpha \in \mathcal{U}_{-1} \cap \mathcal{U}_\xi$, com α és producte senar d'elements de $\mathfrak{B}$ i producte d'elements de $\mathcal{U}_\ell$ que no conté β, similarment a l'anterior en fer el producte $\alpha\beta$ obtenim que ara el producte d'elements de $\mathfrak{B}$ és parell, per tant, $\alpha\beta \in \mathcal{U}_1$ i $g(\alpha\beta) = 1, g(\alpha)g(\beta) = (-1)(-1) = 1$.

(a.iii) Si $\alpha \in \mathcal{U}_0 \cap \mathcal{U}_\xi$ aleshores α conté en la seva descomposició algun factor que no pertany a $\mathfrak{B}$ o $\mathcal{U}_\ell$. Observem que el factor en qüestió tampoc és ξ^j per cap $j = 1, \dots p-1$ per definició. Per tant, $\alpha\beta = \xi\alpha$ també conté aquest factor i $\alpha\beta \in \mathcal{U}_0$. Així, $g(\alpha\beta) = 0, g(\alpha)g(\beta) = 0(-1) = 0$.

Es demostra ara el cas (b) quan $\beta = \xi^j$ per algun $j \neq 1$.

(b.i) Si $\alpha \in \mathcal{U}_1 \cap \mathcal{U}_\xi$ aleshores és un producte parell o zero de diferents elements de $\mathfrak{B}$ que no conté ξ i producte d'elements de $\mathcal{U}_\ell$. Observem que com $\beta = \xi^j \in \mathcal{U}_0$ el producte $\alpha\beta$ deixa de complir els requisits de $\mathcal{U}_1$ i no compleix els de $\mathcal{U}_{-1}$, per tant, $\alpha\beta \in \mathcal{U}_0$. Així, $g(\alpha\beta) = 0, g(\alpha)g(\beta) = 1 \cdot 0 = 0$.

(b.ii) Si $\alpha \in \mathcal{U}_{-1} \cap \mathcal{U}_\xi$, com α és producte senar d'elements de $\mathfrak{B}$ i producte d'elements de $\mathcal{U}_\ell$ que no conté β, similarment a l'anterior en fer el producte $\alpha\beta$ aquest deixa de complir els requisits de $\mathcal{U}_{-1}$ i no compleix els de $\mathcal{U}_1$, per tant, $\alpha\beta \in \mathcal{U}_0$. Així, $g(\alpha\beta) = 0, g(\alpha)g(\beta) = -1 \cdot 0 = 0$.

(b.iii) Si $\alpha \in \mathcal{U}_0 \cap \mathcal{U}_\xi$ l'única forma de que $\alpha\beta$ no estigui a $\mathcal{U}_0$ és que α sigui producte d'elements diferents de $\mathfrak{B}$ i elements de $\mathcal{U}_\ell$ i un ξ^k tal que $\xi^k\beta = 1, \xi$. D'aquesta manera passaria a formar part de $\mathcal{U}_1$ o $\mathcal{U}_{-1}$, però per definició α no conté tal ξ^k i, per tant, $\alpha\beta \in \mathcal{U}_0$. Així, $g(\alpha\beta) = 0, g(\alpha)g(\beta) = 0 \cdot 0 = 0$.

□

De l'últim lema es té immediatament el següent resultat.

Proposició 4.16. *Si $t \in \mathrm{Ker}(\varphi)$ aleshores $f(t) \equiv 0 \mod \ell$.*

Demostració. Pel Lema (4.6) tot element $t \in \mathrm{Ker}(\varphi)$ es pot expressar com una suma d'elements que satisfan les hipòtesis del Lema (4.15). Així, si veiem que $f\left(\sum_{j=0}^{p-1} \xi^j\right) \equiv 0 \mod \ell$, $\xi^p - 1 = 0$ aleshores es compleix l'enunciat. Suposem que $\xi \notin \mathcal{U}_\ell$, aleshores

$$f\left(\sum_{j=0}^{p-1} \xi^j\right) = \sum_{j=0}^{p-1} f(\xi^j) = 1 - 1 = 0 \tag{34}$$

atès que tenim $f(\xi^0) = f(1) = 1$, tenim una $j = k$ tal que $\xi^k \in \mathfrak{B}$ i, per tant, $f(\xi^k) = -1$ mentre que per les altres $j \neq 0, k$ que es troben en $\mathcal{U}_0$ tenim $f(\xi^j) = 0$. Ara només queda comprovar què succeeix quan $\xi \in \mathcal{U}_\ell$, és a dir, si ξ té ordre ℓ. Aleshores observem que $f(\xi^j) = 1, \forall j = 0, \ldots, \ell - 1$ i, per tant,

$$f\left(\sum_{j=0}^{\ell-1} \xi^j\right) = \sum_{j=0}^{\ell-1} f(\xi^j) = \sum_{j=0}^{\ell-1} 1 = \ell \tag{35}$$

D'aquesta manera tenim que $f(t)$ és múltiple de ℓ i, per tant, es té l'enunciat. □

Corol·lari 4.17. *Sigui $\mathcal{F}$ l'expressió donada en (27), aleshores $f(\mathcal{F}) \equiv 0 \mod \ell$.*

4.1.4 Les conseqüències de la transformació f

Recordem que de (27) es té

$$\mathcal{F} = \Psi(VT^m)\mathcal{B}_n + \sum_{i=0}^{n-1} \Psi(VT^i)\mathcal{B}_i \tag{36}$$

L'objectiu d'aquesta secció és inferir propietats de $\Psi(VT^i)$, $\Psi(VT^m)$ i $\mathcal{B}_i$ emprant f. Per fer-ho notem que els $\mathcal{B}_i$ provenien de $\mathcal{A}_i = \mathcal{V}\mathcal{B}_i = (-1)^n \mathcal{A}_n \mathcal{B}_i$ i $\mathcal{A}_i \in Z\mathcal{U}_\ell, \forall i = 0, \ldots, n$ ja que estaven formades únicament per sumes i productes d'arrels de la unitat d'ordre ℓ, així, $\mathcal{B}_i \in Z\mathcal{U}_\ell$. Per tant, en aplicar f a la suma, pel Lema (4.14) es té que

$$f(\mathcal{F}) = (f \circ \Psi)(VT^m) f(\mathcal{B}_n) + \sum_{i=0}^{n-1} f\left(\Psi(VT^i)\mathcal{B}_i\right) = (f \circ \Psi)(VT^m) f(\mathcal{B}_n) + \sum_{i=0}^{n-1} (f \circ \Psi)(VT^i) f\left(\mathcal{B}_i\right) \tag{37}$$

Lema 4.18. *Per tot $0 < i < \ell$ es té $-n \leq (f \circ \Psi)(VT^i) \leq n$ i per $i = 0$ es té $(f \circ \Psi)(V) = n$, on n és el grau de $SL_n(K)$.*

Demostració. Pel Lema (4.7) els caràcters de la forma $\Psi(VT^i)$ són la suma de n arrels de la unitat. Per tant, com aquestes arrels són desconegudes i poden caure en qualsevol dels conjunts $\mathcal{U}_{-1}, \mathcal{U}_0, \mathcal{U}_1$ l'únic que es pot dir és que han estat canviades per $1, 0, -1$, així, el valor de $(f \circ \Psi)(VT^i)$ ha d'estar entre n i $-n$. En el cas de $(f \circ \Psi)(V)$ sabem que V és d'ordre ℓ i, per tant, els valors propis són arrels de la unitat d'ordre ℓ que han estat canviades per 1. Així, $(f \circ \Psi)(V) = n$. □

Pel que fa als $\mathcal{B}_i$, recordem que provenien d'avaluar polinomis de Schur a arrels de la unitat α_i d'ordre ℓ. Observem a més que l'aplicació $f|_{Z\mathcal{U}_\ell}$ és un morfisme d'anells que envia els α_i a 1, per tant, és el mateix que avaluar directament els polinomis de Schur a 1 en cada variable, el qual es realitza en detall a l'annex B. S'obtenen els valors:

$$f(\mathcal{B}_i) = (-1)^i(-1)^{\lfloor n/2 \rfloor} \frac{m(m-1)\cdots(m-i+1)\widehat{(m-i)}(m-i-1)\cdots(m-n+1)}{\binom{n-1}{i-1}(n-2)!} \tag{38}$$

$$f(\mathcal{B}_0) = (-1)^{\lfloor n/2 \rfloor} \frac{(m-1)\ldots(m-n+1)}{(n-1)!} \tag{39}$$

si $0 \leq i < n$ i $m \geq n$. Si $m < n, m \neq i$ aleshores clarament $f(\mathcal{B}_i) = 0$ ja que tenim dues files iguals, fet que també es compleix emprant la fórmula anterior. Si $m = i$ aleshores $f(\mathcal{B}_i) = (-1)^i(-1)^{n-i-1} = (-1)^{n-1}$. Es pot concloure que l'expressió de $f(\mathcal{B}_i)$ és o bé constant o bé un polinomi en m de grau $n-1$.

Finalment, observem que com $f(\mathcal{F}) \equiv 0 \mod \ell$ tenim

$$(f \circ \Psi)(VT^m) \equiv (-1)^n \sum_{i=0}^{n-1} (f \circ \Psi)(VT^i) f(\mathcal{B}_i) \mod \ell \tag{40}$$

i es pot definir:

$$P_{n-1}(m) = (-1)^n \sum_{i=0}^{n-1} (f \circ \Psi)(VT^i) f(\mathcal{B}_i) \tag{41}$$

Que és un polinomi constant o de grau $n-1$ amb coeficients a $\mathbb{Q}$ i que pren valors enters per cada $m \in \{0, \ldots, \ell-1\}$. S'obté finalment l'expressió

$$(f \circ \Psi)(VT^m) \equiv P_{n-1}(m) \mod \ell \tag{42}$$

Lema 4.19. *Si $\ell > (2n+1)(n-1)$ aleshores necessàriament $P_{n-1}(m)$ ha de ser constant.*

Demostració. Sabem que $(f \circ \Psi)(VT^m)$ pren valors entre $-n$ i n i, per (42), els valors de $P_{n-1}(m)$ també ho han de fer mòdul ℓ. Si $P_{n-1}(m)$ no és constant, donat $k \in \{-n, \ldots, n\}$ com a molt existeixen $n-1$ valors diferents de m pels quals $P_{n-1}(m) = k$. Per tant, com a molt podem tenir $(2n+1)(n-1)$ valors diferents de m. Si $\ell > (2n+1)(n-1)$ forçosament necessitem que el polinomi sigui constant. □

Demostració (Teorema (4.1)). Suposem que $\ell > (2n+1)(n-1)$. Aleshores $P_{n-1}(m) = c$ constant, en particular, per $m = 0$ tenim que $(f \circ \Psi)(V) \equiv c \mod \ell$ i, per tant, pel lema (4.18) $c = n$. En particular, això també implica que $(f \circ \Psi)(VT) = n$ i, per tant, ha de ser suma d'1 o arrels de la unitat d'ordre ℓ. És a dir, VT és d'ordre ℓ o 1 ja que els seus valors propis ho són. Així, com V era una transformació d'ordre ℓ qualsevol de G, tenim que el producte de dues transformacions d'ordre ℓ en G és d'ordre ℓ. El conjunt de totes les transformacions d'ordre ℓ juntament amb la identitat formen un subgrup $H \leq G$ amb $|H| = \ell^k$ per algun k. Atès que una la conjugació d'una transformació d'ordre ℓ té ordre ℓ, $H \trianglelefteq G$ és subgrup normal. A més, $H \cong (\mathbb{Z}/(q))^k$ que és abelià. Pel Lema (3.23), G no pot ser primitiu, per tant, ℓ no pot ser major a $(2n+1)(n-1)$. □

Corol·lari 4.20. *Sigui $G \in GL_n(K)$ tal que $\ell \geq 2(n+1)(n-1)$ primer divideix l'ordre de G, aleshores els productes dels elements de G d'ordre ℓ tenen ordre ℓ i formen un subgrup normal abelià d'ordre ℓ^k per algun $k > 0$.*

4.2 Millores del teorema i altres cotes

En aquesta secció s'exposen diversos resultats pel que fa als nombres primers que poden dividir l'ordre d'un grup primitiu de $\mathrm{GL}_n(K)$ o $\mathrm{PGL}_n(K)$ en funció de n i quines són les potències màximes de cada primer que poden dividir l'ordre. No es donen les demostracions, simplement es fa referència a l'article on es poden trobar.

Després de generalitzar el resultat del teorema (4.1) a K cos algebraicament tancat $\mathrm{car}(K) = 0$, resseguir la demostració de Brauer en [Bra42b], i analitzar els resultats usats de Feit [Fei64] i de Feit-Thompson [FT61], podem afirmar (comunicació personal del tutor) que es pot enunciar el següent resultat per K algebraicament tancat amb $\mathrm{car}(K) = 0$ enlloc de $\mathbb{C}$.

Teorema 4.21 (Brauer)**.** *[Bra42b] [Bra67, p.75, 2B, 2C] Sigui $G \leq SL_n(K)$ un grup finit primitiu on K és un cos algebraicament tancat amb $car(K) = 0$. Sigui p un nombre primer que divideix $|G|$ l'ordre de G aleshores $p \leq 2n + 1$. A més a més, si $p > n + 1$ aquest és l'únic nombre primer major a $n + 1$ que pot dividir l'ordre del grup i $p^2 \nmid |G|$. En el cas que $p = 2n + 1$ primer aleshores $G/Z(G) \cong PSL_2(\mathbb{F}_p)$.*

Brauer en [Bra67] usant la tesi de Hayden [Hay63] i el treball de Tuan [Tua44] obté el següent teorema.

Teorema 4.22 (Brauer-Hayden-Tuan)**.** *[Bra67, p.75, 2D] Sigui $G \leq SL_n(\mathbb{C})$ un grup finit primitiu amb $5 \leq n \leq 10$, sigui p un nombre primer que divideix $|G|$ l'ordre de G aleshores $p \leq n$ excepte en el cas que $G/Z(G) \cong PSL_2(\mathbb{F}_p)$.*

El següents teoremes donen cotes superiors per les potències dels primers que divideixen l'ordre d'un grup finit primitiu.

Teorema 4.23. *[Bli17, §74] Sigui $G \leq SL_n(\mathbb{C})$ un grup finit primitiu, sigui p un nombre primer que divideix $|G|$ l'ordre de G aleshores si $p^k \mid |G|$ aquest compleix $p^k \leq (n!)_p 6^{n-1}$ on $(n!)_p$ denota la potència màxima de p que divideix $n!$.*

Observació 4.24. En [Bli17, §74] la cota que es presenta és $p^k \leq (n!)_p 5^{n-1}$ enlloc de l'anterior, ara bé, com indica Brauer en [Bra67, p.74] la reducció de la cota de 6 a 5 és presenta com un fet pendent de publicació, no se'n dona la demostració i la suposada futura publicació no s'ha trobat.

Teorema 4.25. *[Bli11, p.42, Cor.] Sigui $G \leq SL_n(\mathbb{C})$ un grup finit primitiu, sigui p un nombre primer tal que $p \nmid n$ i que divideix l'ordre de G. Sigui $k > 0$ tal que $p^k \mid |G|$ l'ordre de G aleshores $p^k \mid n! p^{n-1}$.*

Observació 4.26. En el cas del teorema (4.22), no tenim accés a la tesi [Hay63] de Hayden, per tant, no podem estudiar-ne la demostració. En el cas de (4.23) i (4.25), alguns dels resultats empren funcions de variable complexa, fet pel qual una generalització a K algebraicament tancat de característica 0 no sembla clara.

5 Sobre la classificació grups finits primitius d'ordre n

5.1 Classificacions de grups primitius per a $n \leq 7$

En aquesta secció es donen diverses llistes dels grups finits primitius de $\mathrm{SL}_n(\mathbb{C})$ per diferents valors de n, juntament amb les referències d'on s'han extret. Per n fix les classificacions que donem són les úniques conegudes en la literatura, sota el nostre coneixement.

Abans de donar els resultats, són necessàries les següents definicions:

- Sigui G un grup finit, s'anomena $G' = [G, G]$ el grup generat pels commutadors de G, és a dir, els elements $[g, h] = ghg^{-1}h^{-1}$.

- Es defineix l'exponent d'un grup finit G com el mínim comú múltiple de l'ordre de tots els elements del grup.

- Es diu que un grup G és una extensió d'un grup H per Q si existeix una successió curta exacta

$$1 \longrightarrow H \xrightarrow{\iota} G \xrightarrow{\pi} Q \longrightarrow 1 \quad \text{(exacta)} \tag{43}$$

  es diu que aquesta extensió és de separació si existeix un morfisme de grups $s : H \to G$ tal que $\pi \circ s = \mathrm{id}_H$.

- Per un $p > 2$ primer anomenem H_p a l'extensió de separació d'un grup no abelià P per $SL_2(p)$, on P és un grup d'ordre p^3 i exponent p.

$$1 \longrightarrow P \xrightarrow{\iota} H_p \xrightarrow{\pi} SL_2(p) \longrightarrow 1 \quad \text{(exacta)} \tag{44}$$

  Es denota per I_p la classe de tots els subgrups primitius de H_p que contenen P. La descripció explícita d'aquest grups es pot trobar en [Kan+09], en particular, I_3 correspon a [Kan+09, Teorema 1.2], I_5 correspon a [Kan+09, Teorema A.3] i I_7 correspon a [Kan+09, Teorema A.6].

- Siguin A, B dos grups finits, $A \times B$ denota el producte directe dels grups A i B.

- Es denoten per $2A_m$, $5 \leq m \in \mathbb{N}$ els dobles recobriments de Schur A_m. Per $m = 6, 7$, $3A_m$ i $6A_m$ denoten els triple i sèxtuple recobriments de Schur de A_m. Es denoten per S_m^+, S_m^-, $m \geq 4$ els dobles recobriments de Schur de S_m. Per més informació sobre aquests grups vegeu [Hof92, §1].

- Per informació sobre les diferents nomenclatures emprades per denotar els grups simples de tipus Lie vegeu la taula 6 de l'annex D.

A continuació es resumeixen les classificacions per $2 \leq n \leq 7$ extretes de [Fei71, §8.5].

Teorema 5.1. *Sigui $G \leq SL_n(\mathbb{C})$ un subgrup finit primitiu amb $Z(G) \subseteq G'$ i sigui $z = |Z(G)|$. Aleshores G és isomorf a un dels següents grups o famílies:*

$n = 2$	G	$\lvert G\rvert$	z
(i)	$S_4^{\pm}$, $SL_2(3), SL_2(5) \cong 2A_5$	$24z, 12z, 60z$	2

$n = 3$	G	$\lvert G\rvert$	z
(i)	I_3	-	-
(ii)	$A_5, PSL_2(7)$	$60, 168$	1
(iii)	$3A_6$	$360z$	3

$n=4$	G	$\|G\|$	z
(i)	$A \times B/Z$ on A, B són grups primitius per $n=2$ i Z és el subgrup central d'ordre 2 que no està contingut ni en A ni en B	-	-
(ii)	A subgrup d'índex 2 en $GL_2(3) \times GL_2(3)/Z$ que no apareix en (i)	$288z$	2
(iii)	Sigui G el grup de (ii), hi ha dues possibles extensions de G que intercanvien els factors	$576z, 576z$	2
(iv)	Una extensió de $SL_2(3) \times SL_2(3)/Z$ que intercanvia els factors i amb Z com (i)	$288z$	2
(v)	A_5, S_5	$60, 120$	1
(vi)	$2A_5, 2A_6, S_6^{\pm}, 2A_7$	$60z, 360z, 720z, \frac{7!}{2}z$	2
(vii)	$SL_2(7)$	$168z$	2
(viii)	$2PSU_4(2)$	$2^6 3^4 5z$	2
(ix)	G és un subgrup primitiu que conté T de l'extensió d'un grup extra especial T d'ordre 2^5 pel seu grup d'automorfismes	-	-

$n=5$	G	$\|G\|$	z
(i)	I_5	-	-
(ii)	A_5, A_6, S_5, S_6	$60, 360, 120, 720$	1
(iii)	$PSL_2(11)$	660	1
(iv)	$PSU_4(2)$	$2^6 3^4 5$	1

$n=6$	G	$\|G\|$	z
(i)	$A \times B$ on A és grup primitiu per $n=2$ i B és grup primitiu per $n=3$	-	-
(ii)	$2A_5, S_5^{\pm}$	$60z, 120z$	2
(iii)	$3A_6 \cong 3PSL_2(9)$, una extensió per un automorfisme d'ordre 2 que és el producte de l'automorfisme del cos per l'automorfisme de $GL_2(9)$	$360z, 720z$	3
(iv)	$3A_7$	$\frac{7!}{2}z$	3
(v)	A_7, S_7	$\frac{7!}{2}, 7!$	1
(vi)	$6A_6, 6A_7$	$360z, \frac{7!}{2}z$	6
(vii)	$PSL_2(7), PGL_2(7)$	$168, 336$	1
(viii)	$SL_2(7)$ i una extensió per un automorfisme d'ordre 2 de $GL_2(7)$	$168z, 336z$	2
(ix)	$SL_2(11), SL_2(13)$	$660z, 1092z$	2
(x)	$PSU_2(4)$ i una extensió per un automorfisme d'ordre 2	$2^6 3^4 5, 2^7 3^4 5$	1
(xi)	$SU_3(3)$ i una extensió per l'automorfisme del cos	$6048, 12096$	1
(xii)	$6PSU_4(3)$ i una extensió per un automorfisme d'ordre 2	$2^7 3^6 5^1 7^1 z, 2^8 3^6 5^1 7^1 z$	6
(xiii)	$2J_2$	$604800z$	2
(xiv)	$6PSL_3(4)$ i una extensió per un automorfisme d'ordre 2 que és el producte d'un automorfisme de grafs i un automorfisme de cossos	$20160z, 40320z$	6

$n=7$	G	$\lvert G\rvert$	z
(i)	I_7	-	-
(ii)	A_8, S_8	$\frac{8!}{2}, 8!$	1
(iii)	$PSL_2(13), PSL_2(7), PGL_2(7), PSp_6(2)$	$1092, 168, 336, 2^9 3^4 5^1 7^1$	1
(iv)	$PSU_3(3), G_2(2)$	$6048, 12096$	1
(v)	$PSL_2(8), R(3)$	$504, 1512$	1

Demostració. La demostració dels casos $n = 2, 3, 4$ es pot trobar en [Bli17]. La demostració del cas $n = 5$ és de Brauer i es pot consultar en [Bra67]. La demostració de $n = 6$ es deguda a Lindsey i es pot trobar en [Lin71]. La demostració de $n = 7$ és deguda a Wales i es pot trobar en [Wal70]. □

Observació 5.2. Les classificacions per $n = 2, 3$ són problemes clàssics i estan més presents en la literatura que la resta de casos. En la tesi [Hug05, §2] es poden consultar la classificació dels subgrups finits de $\mathrm{PGL}_2(K)$ i $\mathrm{PGL}_3(K)$ on K és un cos de característica $p \geq 0$ algebraicament tancat.

En els articles [DZ98] i [DZ08] es pot trobar una classificació menys explícita de tots els grups primitius de $\mathrm{SL}_p(\mathbb{C})$ on p primer. Aquesta classificació només descriu quins són els grups primitius simples i quins són els subgrups imprimitius que poden ser subgrups normals d'un grup primitiu. Aquesta classificació està fonamentada en la classificació dels grups finits simples i en l'article [LS74] i la seva versió revisada [SZ93]. Aquests dos darrers articles proporcionen cotes inferiors sobre el grau mínim de les representacions projectives dels grups simples de tipus Lie.

Un dels passos més importants en la determinació de totes les classificacions donades és l'obtenció dels possibles grups primitius simples, vegeu [Bli17, §§102-117]. A més a més, la llista dels grups primitius simples de $\mathrm{SL}_n(\mathbb{C})$ és subconjunt de la llista de subgrups primitius simples de $\mathrm{PGL}_n(\mathbb{C})$, vegeu el següent exemple:

Exemple 5.3. En la taula del Teorema (5.1) els grups que es mostren són grups de representació, és a dir, són extensions centrals dels grups primitius de $\mathrm{PGL}_n(\mathbb{C})$. Així, en el cas de $\mathrm{SL}_2(\mathbb{C})$ es veu que no hi ha grups simples primitius, mentre que en $\mathrm{PGL}_2(\mathbb{C})$ s'hi té A_5, que té com a grup de representació $2A_5 \cong SL_2(5)$. En el cas $n = 3$, A_6 no és grup simple primitiu de $\mathrm{SL}_3(\mathbb{C})$ però si que és present en $\mathrm{PGL}_3(\mathbb{C})$, atès que $3A_6$ és grup de representació de A_6.

Aquest fet motiva un estudi computacional de quins poden ser els grups primitius simples de $\mathrm{PGL}_n(\mathbb{C})$, en els casos fora del nostre coneixement, és a dir, $n \geq 8$ no primer.

5.2 Classificació dels grups simples primitius d'ordre n fixat

Com a novetat per la comunitat matemàtica, en aquesta secció presentem un programa que, donat n fix, és capaç de determinar una llista finita de grups simples que conté tots els possibles grups finits primitius de $\mathrm{PGL}_n(\mathbb{C})$.

El programa no és capaç de decidir quins dels grups tenen representacions primitives en $\mathrm{PGL}_n(\mathbb{C})$, però garanteix que els que en tinguin hi són presents. Pels n més petits és possible reduir les llistes i determinar representacions irreductibles comparant amb les bases de dades del [GAP].

Per a la presentació i exemples de com s'empra el programa, referiu-vos a la secció 5.2.1. El programa està disponible a GitHub en `https://github.com/GeraGC/FiSGO`.

Per a la discussió dels resultats del programa sobre els grups simples finits primitius de $\mathrm{PGL}_n(\mathbb{C})$ amb $8 \leq n \leq 10$ referiu-vos a la secció 5.2.2.

Finalment, en l'annex D es pot consultar la taula 7 amb els candidats a grups finits simples primitius de $\mathrm{PGL}_n(\mathbb{C})$ per $12 \leq n \leq 20$.

5.2.1 FiSGO: Finite Simple Groups by Order

El programa dissenyat per determinar una llista finita de grups simples candidats a ser grups simples primitius s'anomena *FiSGO: Finite Simple Groups by Order*. Actualment el programa està escrit en SageMath Notebook i està pensat per a ser utilitzat en l'entorn de Jupyter Notebook. Al llarg d'aquesta secció en descrivim els seus objectius, les seves funcions i altres programes que el complementen.

L'objectiu principal del *FiSGO* és respondre la següent pregunta:

Pregunta 5.4. Donat un nombre $b = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ on $p_1, p_2, \ldots, p_k$ són nombres primers diferents i $n_1, \ldots, n_k$ són nombres naturals positius, quins són els grups finits simples els ordres dels quals divideixen b?

Respondre a aquesta pregunta és necessari emprar la classificació dels grups finits simples i les fórmules que donen els ordres d'aquests grups simples. Així, les funcionalitats que incorpora el programa són les següents:

- La classe principal `SimpleGroupsOrder` permet, donat un diccionari detallant els nombres primers i les seves potències $p_i : n_i$, determinar per cada família de grups simples quins divideixen l'ordre b donat.
- La classe `SimpleGroupsOrder` també inclou la funció `full_check()` que permet determinar tots els grups simples d'ordre que divideix b de totes les famílies simultàniament.
- La notació emprada per defecte per descriure els grups finits simples és la del paquet [Wil+22] de [GAP]. Aquesta notació no és estàndard actualment però permet el processament de la llista de grups obtinguda amb [GAP] sense haver de canviar els noms. La funció `standard_notation()` permet llegir els resultats en una notació alternativa.
- Els noms de les funcions associades a cada família de grups simples corresponen als noms donats en la llista de grups simples de [Wik24].
- Alguns dels grups entre famílies es solapen, el programa elimina per defecte els duplicats quan s'empra la funció `full_check()`.
- Habilitant la opció `multipliers = True` la cerca retorna els possibles grups i el multiplicador de Schur de cada grup calculat emprant les expressions de [Wik24].

A part de la classe principal `SimpleGroupsOrder` el programa també inclou altres funcions diverses:

- Una cel·la amb una taula de conversió entre els noms de les famílies emprats en [Wil+22] i en [Wik24].
- Funcions que generen l'ordre d'un grup simple de la família triada a partir dels paràmetres i les fórmules donades en [Wik24] (exceptuant els esporàdics). El resultat es retorna com una llista preparada per ser usada per la classe `SimpleGroupsOrder`.
- La funció `report(simplegroups: SimpleGroupsOrder, filename: str)` que donat un objecte `SimpleGroupsOrder` i un nom crea un arxiu de text amb un resum dels grups obtinguts per l'ordre especificat, juntament amb l'ordre d'aquests grups emprant la notació alternativa. També presenta diverses llistes dels grups obtinguts per a ser emprades directament amb [GAP].
- La funció `build_bound(n)` que donat $n \geq 2$ natural genera una cota per l'ordre dels grups primitius simples de $\mathrm{PGL}_n(\mathbb{C})$ a partir dels teoremes (4.21), (4.23) i (4.25).

Observació 5.5. La funció `build_bound(n)` tria per cada primer p quina de les dues cotes dels teoremes (4.23) i (4.25) és més fina en cada cas, sempre que es puguin emprar ambdues.

A continuació es dona un exemple de com s'empraria el programa per determinar els candidats a grups simples primitius de $\mathrm{PGL}_6(\mathbb{C})$ emprant tant la cota proporcionada per la funció `build_bound(6)` com la reducció donada pel Teorema (4.22).

Exemple 5.6. Es comença calculant les dues diferents cotes per l'ordre dels grups simples primitius de $\mathrm{PGL}_6(\mathbb{C})$.

```
In[1]: order6 = build_bound(6); order6
Out[1]: {2: 16, 3: 10, 5: 6, 7: 4, 11: 3, 13: 3}
In[2]: order6extra = order6;
       for prime in list(order6extra.keys()):
         if prime > 7:
           del order6extra[prime]
       order6extra
Out[2]: {2: 16, 3: 10, 5: 6, 7: 4}
```

Notem que `order6extra` conté la cota reduïda en el·liminar els primers majors a $n+1=7$. Podem procedir a calcular els grups simples que divideixen les cotes:

```
In[3]: boundSimpleGroups = SimpleGroupsOrder(multipliers=False)
       boundSimpleGroups.set_order(order6)
       boundSimpleGroups.full_check()
       print(boundSimpleGroups.get_calculated_groups())
Out[3]: ['A5', 'A6', 'A7', 'A8', 'A9', 'A10', 'A11', 'A12', 'A13', 'A14', 'A15',
        ↪ 'A16', 'M11', 'M12', 'M22', 'J2', 'HS', 'McL', 'Suz', 'L3(2)', 'L3(4)',
        ↪ 'L2(8)', 'L2(64)', 'L3(3)', 'L4(3)', 'L5(3)', 'L3(9)', 'L2(27)', 'L2(25)',
        ↪ 'L2(49)', 'L2(11)', 'L2(13)', 'O7(2)', 'O5(8)', 'O7(3)', 'S6(3)', 'O5(5)',
        ↪ 'O5(7)', 'O8+(2)', 'G2(4)', 'G2(3)', 'U4(2)', 'U5(2)', 'U6(2)', 'U3(4)',
        ↪ 'U3(3)', 'U4(3)', 'U3(5)', 'U4(5)', '3D4(2)', 'Sz(8)', "2F4(2)'"]
In[4]: bound2SimpleGroups = SimpleGroupsOrder(multipliers=False)
       bound2SimpleGroups.set_order(order6extra)
       bound2SimpleGroups.full_check()
       print(bound2SimpleGroups.get_calculated_groups())
Out[4]: ['A5', 'A6', 'A7', 'A8', 'A9', 'A10', 'J2', 'L3(2)', 'L3(4)', 'L2(8)',
        ↪ 'L2(49)', 'O7(2)', 'O5(7)', 'O8+(2)', 'U4(2)', 'U3(3)', 'U4(3)', 'U3(5)']
```

En cas de voler els multiplicadors de Schur de cada grup es pot canviar la opció `multipliers=True`, s'obté el següent (només ho fem pel cas reduït).

```
In[5]: bound2SimpleGroups.set_multipliers(True)
       bound2SimpleGroups.full_check()
       print(bound2SimpleGroups.get_calculated_groups())
Out[5]: {'A5': 2, 'A6': 6, 'A7': 6, 'A8': 2, 'A9': 2, 'A10': 2, 'J2': 2, 'L3(2)': 2,
        ↪ 'L3(4)': 48, 'L2(8)': 1, 'L2(49)': 2, 'O7(2)': 2, 'O5(7)': 2, 'O8+(2)': 4,
        ↪ 'U4(2)': 2, 'U3(3)': 1, 'U4(3)': 36, 'U3(5)': 3}
```

En el cas de voler la resposta en la notació alternativa es pot escriure:

```
In[6]: print(boundSimpleGroups.standard_notation())
Out[6]: {'A5': 2, 'A6': 6, 'A7': 6, 'A8': 2, 'A9': 2, 'A10': 2, 'J2': 2, 'PSL3(2)': 2,
        ↪ 'PSL3(4)': 48, 'PSL2(8)': 1, 'PSL2(49)': 2, 'PSO7(2)': 2, 'PSO5(7)': 2,
        ↪ 'PSO8+(2)': 4, 'PSU4(2)': 2, 'PSU3(3)': 1, 'PSU4(3)': 36, 'PSU3(5)': 3}
```

Si es vol generar un arxiu de text amb tota la informació de `bound2SimpleGroups` es pot emprar la funció `report` de la següent manera:

In[7]:
```
bound2SimpleGroups.set_multipliers(True)
bound2SimpleGroups.full_check()
report(boundSimpleGroups, 'PGL6_autobuild.txt')
```

Out[7]:
```
True
```

En la versió actual del *FiSGO* la funció `report` només està implementada quan s'empra l'opció `multipliers=True`.

Observació 5.7. El programa *FiSGO* únicament és capaç de determinar els candidats als grups simples primitius de $\mathrm{PGL}_n(\mathbb{C})$ donat un n. En cap cas assegura que els grups obtinguts tinguin les representacions corresponents.

A partir dels grups que proporciona el programa *FiSGO* es pot estudiar si aquests grups tenen representacions lineals o projectives irreductibles primitives de grau corresponent al n que s'estigui estudiant. Per grups finits simples d'ordre petit la base de dades del [GAP] té molta informació ja disponible sobre les representacions lineals i projectives d'aquests grups. Així, conjuntament amb el *FiSGO* també s'ha programat un script[3] de [GAP] que per cada grup obtingut comprovi si existeix una representació (lineal o projectiva) irreductible del grau desitjat.

Aquest script en [GAP] intenta fer el següent:

1. Donada la llista de grups simples segons si tenen multiplicador de Schur trivial o no trivial, comprova si hi ha informació existent sobre els caràcters irreductibles del grup donat en la seva base de dades, principalment en [Wil+22] i [Bre22].

2. Si no existeix informació sobre el grup, notifica que no ha estat trobat i passa al següent. En cas de disposar d'informació sobre el grup, comprova si hi ha caràcters lineals irreductibles del grau desitjat i ho retorna.

3. Si el multiplicador de Schur del grup no és trivial, comprova si hi ha informació sobre les representacions projectives o del grup de representació. En cas d'haver-ne, comprova si hi ha caràcters projectius del grau desitjat i ho retorna.

4. Si hi ha diversos caràcters compatibles amb els criteris desitjats, el grup serà retornat per més d'un cop.

Observació 5.8. El procès descrit anteriorment determina l'existència de representacions irreductibles en funció de si existeixen caràcters irreductibles del grau desitjat. No és capaç de decidir si els caràcters en qüestió admeten representacions primitives o imprimitives.

Com major l'ordre del grup més probable és que no hi hagi informació sobre aquest. En aquesta situació es poden emprar les cotes sobre el mínim grau de les representacions projectives dels grups de tipus Lie donades en els articles [LS74] i [SZ93]. Aquest procès de comparació es podria programar com a un filtre addicional en *FiSGO*, i es pretén implementar-ho de cara a futures versions.

Observació 5.9. En el cas particular dels grups alternats A_n, les representacions projectives d'aquests grups estan àmpliament estudiades en la literatura, vegeu [Hof92] pel cas complex i [Kle05] pel cas K algebraicament tancat i de característica $p \geq 0$.

5.2.2 Discussió de l'algoritme per ordres 8,9 i 10

En aquesta secció comentarem els resultats obtinguts per $n = 8, 9, 10$. En la taula 1 es mostren les cotes emprades per determinar els candidats a grups primitius simples emprant *FiSGO* i la reducció de Brauer del teorema (4.21). La taula mostra per cada n i per $p \leq 11$ primers els exponents màxims corresponents a cada primer.
A partir de les cotes anteriors s'obtenen les llistes de grups finits simples candidats a ser grups simples primitius de $\mathrm{PGL}_n(K)$, es mostren en la taula 2.
La notació emprada per descriure els grups finits simples emprada en la taula 2 no és completament estàndard, com a referència, es dona la correspondència amb els noms donats en [Wik24]:

[3] Aquest script també està disponible a GitHub: `https://github.com/GeraGC/FiSGO`

Taula 1: Cotes superiors als ordres dels grups primitius simples de $\mathrm{PGL}_n(\mathbb{C})$

n	2	3	5	7	11
8	25	9	8	7	0
9	15	17	9	8	0
10	31	13	12	9	6

Taula 2: Candidats a grups simples primitius de $\mathrm{PGL}_n(K)$

n	Grups simples candidats
8	$A_5, A_6, A_7, A_8, A_9, A_{10}, J_2$ $PSL_3(2), PSL_3(4), PSL_2(8), PSL_2(49), \Omega_7(2), \Omega_5(7), O_8^+(2)$, $PSU_4(2), PSU_3(3), PSU_4(3), PSU_3(5)$
9	$A_5, A_6, A_7, A_8, A_9, A_{10}, J_2$, $PSL_3(2), PSL_3(4), PSL_2(8), PSL_2(49), \Omega_7(2), \Omega_5(7), O_8^+(2)$, $PSU_4(2), PSU_3(3), PSU_4(3), PSU_3(5)$
10	$A_5, A_6, A_7, A_8, A_9, A_{10}, A_{11}, A_{12}, M_{11}, M_{12}, M_{22}, J_2, HS, McL$, $PSL_3(2), PSL_3(4), PSL_2(8), PSL_2(49), PSL_2(11), \Omega_7(2), \Omega_5(7)$, $O_8^+(2), PSU_4(2), PSU_5(2), PSU_6(2), PSU_3(3), PSU_4(3), PSU_3(5)$

- Els grups J_2, HS, McL són grups esporàdics, respectivament són el segon grup de Janko (també conegut com el grup de Hall-Janko-Wales), el grup de Higman-Sims i el grup de McLaughlin.
- Els grups $PSL_{n+1}(q)$ són els grups projectius especials lineals de dimensió $n+1$ sobre els cossos finits $\mathbb{F}_q$. També es coneixen com els grups clàssics de Chevalley de tipus $A_n(q)$.
- Els grups $\Omega_{2n+1}(q)$ són els grups de Chevalley de tipus $B_n(q)$, els grups $O_{2n}^+(q)$ són els grups de Chevalley de tipus $D_n(q)$.
- Els grups $PSU_{n+1}(q)$ són els grups projectius especials unitaris de dimensió $n+1$ sobre el cos finit $\mathbb{F}_q$. També es coneixen com els grups clàssics de Chevalley de tipus ${}^2A_n(q^2)$
- Per més informació sobre les diferents nomenclatures dels grups simples de tipus Lie vegeu la taula 6 de l'annex D.

A partir de les llistes de la taula 2 es contrasten els grups obtinguts amb les bases de dades del [GAP]. Els grups finalment obtinguts es classifiquen segons si la representació projectiva obtinguda és d'una extensió trivial (és a dir, és una representació lineal del grup) o si són representacions projectives obtingudes d'un grup de representació amb extensió central no trivial. Els resultats es mostren en la taula 3.

Taula 3: Grups simples amb representacions irreductibles candidats a ser primitius en $\mathrm{PGL}_n(\mathbb{C})$

n	Trivials	No trivials
8	$A_6, A_9, PSL_3(2), PSL_2(8)$	$A_6, A_8, A_9, PSL_3(2), PSL_3(4), \Omega_7(2), O_8^+(2)$
9	$A_6, A_{10}, PSL_2(8)$	A_6
10	$A_6, A_7, A_{11}, M_{11}, PSL_2(11), PSU_4(2)$, $PSU_5(2)$	$A_6, M_{12}, M_{22}, PSL_3(4), PSL_2(11)$

Distingir entre si les representacions projectives provenen del propi grup o d'un grup de representació donat per una extensió central no trivial permet decidir si els grups simples tenen representacions a $\mathrm{GL}_n(\mathbb{C})$ o no. Vegeu el següent exemple:

Exemple 5.10. Per $n = 8$ el grup A_6 té ambdós tipus de representacions, per tant, la representació trivial és una representació lineal que projecta a $\mathrm{PGL}_8(\mathbb{C})$, mentre que la representació no trivial en aquest cas prové del doble recobriment de Schur $2A_6$, per tant, el grup present a $\mathrm{GL}_8(\mathbb{C})$ és $2A_6$

i no A_6. En el cas de $PSL_2(4)$, la representació és únicament no trivial, per tant, el grup simple $PSL_2(4)$ no té representacions lineals en $\mathrm{GL}_8(\mathbb{C})$, per tant, no pot ser un grup primitiu simple, ara bé, el seu 6-recobriment de Schur $6PSL_3(4)$ sí que té una representació lineal a $\mathrm{GL}_n(\mathbb{C})$ que indueix una representació projectiva de $PSL_3(4)$. Pel mateix motiu, tot grup que tingui multiplicador de Schur trivial sempre que es pugui representar en $\mathrm{PGL}_n(\mathbb{C})$ també es podrà representar en $\mathrm{GL}_n(\mathbb{C})$.

Observació 5.11. En els tres casos $n = 8, 9, 10$ el grup $\Omega_5(7)$ apareix com a candidat a grups simple primitiu (vegeu taula 2). En comprovar les representacions projectives en [GAP] el script emprat retorna que no hi ha informació sobre les representacions projectives, només sobre les lineals. Per poder descartar aquest grup de la llista s'ha comprovat en [LS74, Thm.1] que la cota inferior al grau mínim per les representacions projectives d'aquest grup és 24.

Finalment, en la taula 4 es resumeixen els grups finits simples candidats a ser primitius a $\mathrm{GL}_n(\mathbb{C})$ i els que projecten a candidats a grups simples primitius a $\mathrm{PGL}_n(\mathbb{C})$, que serien grups primitius de $\mathrm{GL}_n(\mathbb{C})$.

Taula 4: Candidats a grups primitius simples de $\mathrm{GL}_n(\mathbb{C})$ i grups de representació

n	Grups
8	$A_6, A_9, PSL_3(2), PSL_2(8)$, $2A_6, 2A_8, 2A_9, 2PSL_3(2), 4PSL_3(4), 2\Omega_7(2), 2O_8^+(2)$
9	$A_6, A_{10}, PSL_2(8)$, $3A_6$
10	$A_6, A_7, A_{11}, M_{11}, PSL_2(11), PSU_4(2), PSU_5(2)$, $2A_6, 2M_{12}, 2M_{22}, 2PSL_3(4), 2PSL_2(11)$

Per acabar, en l'annex C es poden consultar les cotes calculades pels exponents dels grups primitius de $\mathrm{PGL}_n(\mathbb{C})$ per $8 \leq n \leq 32$, calculades emprant la funció `build_bound` de *FiSGO*. En l'annex D es poden trobar les llistes dels grups simples candidats a ser primitius en $\mathrm{PGL}_n(\mathbb{C})$ per $8 \leq n \leq 20$, n no primer, un cop comparats amb la base de dades del [GAP].

Tots els codis i arxius resultants dels programes emprats per l'elaboració de totes les taules es poden consultar en `https://github.com/GeraGC/FiSGO`. El seu ús és lliure.

A Teoria de representacions projectives i exemples

A.1 Introducció a la teoria de representacions projectives

La teoria de representacions de grups finits sobre el grup lineal ha estat desenvolupada àmpliament en el darrer segle, en part, degut a l'esforç realitzat per la classificació dels grups simples. En aquest annex es pretén introduir la seva contrapart projectiva, és a dir, una teoria que faci el mateix paper que l'anterior però aplicada a entendre com poden representar-se grups finits dins els espais $\mathrm{PGL}_n(K)$. Al llarg de tota la secció es treballarà sobre un cos K de característica 0 algebraicament tancat.

Definició A.1. Sigui V un espai vectorial de dimensió finita amb cos K, sigui G un grup finit, es diu que $\rho : G \to \mathrm{PGL}(V)$ és una *representació projectiva* del grup G en $\mathrm{PGL}(V)$ si ρ és un morfisme de grups.

Si un és coneixedor de la teoria de representacions lineals de grups finits, i tenint en compte el morfisme projecció $\pi : \mathrm{GL}(V) \to \mathrm{PGL}(V)$, és clar que qualsevol representació lineal d'un grup finit indueix una representació projectiva d'aquest via composició amb la projecció, la pregunta és si totes les representacions projectives són d'aquesta tipologia, essencialment reduint-se a l'estudi de la contrapart lineal. Un dels exemples més senzills de que aquest no és el cas ve donat per les representacions del grup alternat A_5. A través del [GAP] es poden obtenir els ordres dels caràcters irreductibles lineals de A_5 que són $1, 3, 4, 5$, per tant, A_5 no té cap representació injectiva ("faithful") a $\mathrm{GL}_2(K)$. Si la tingués, aquesta hauria de ser resultat de la suma directa de l'únic caràcter irreductible d'ordre 1, que és el trivial. Per tant, no es té cap subgrup de $\mathrm{GL}_2(K)$ isomorf a A_5, també és diu que no té cap realització en $\mathrm{GL}_2(K)$. Ara bé, és conegut que A_5 és un subgrup de $\mathrm{PGL}_2(K)$ ja que A_5 representa les simetries d'un icosaedre. Així, es té una representació projectiva de A_5 que no ve induïda per una representació lineal.

Per poder relacionar completament les representacions lineals i les representacions projectives és convenient la següent definició equivalent de representació projectiva donada en [Kar85] i [Hof92]:

Definició A.2. Sigui V un espai vectorial de dimensió finita amb cos K, sigui G un grup finit, es diu que $\rho : G \to \mathrm{GL}(V)$ és una *representació projectiva* del grup G si existeix una aplicació $\alpha : G \times G \to K^\times$ tal que

(a) $\rho(x)\rho(y) = \alpha(x, y)\rho(xy)\ \forall x, y \in G$.

(b) $\rho(1) = 1_V$ on 1 és la identitat a G i 1_V és la identitat de $\mathrm{GL}(V)$.

La demostració de l'equivalència entre les definicions es pot trobar en [Men17].
Notem que si $\alpha(x, y) = 1\, \forall x, y \in G$ aleshores la representació projectiva ρ és de fet una representació lineal. S'observa que l'aplicació α satisfà les propietats del que és coneix com un 2-cocicle:

Lema A.3. *Sigui $\rho : G \to GL(V)$ una representació projectiva amb una aplicació $\alpha : G \times G \to K^\times$ associada, aleshores compleix $\forall x, y, z \in G$:*

(a) $\alpha(x, 1) = \alpha(1, x) = 1$.

(b) $\alpha(x, yz)\alpha(y, z) = \alpha(x, y)\alpha(xy, z)$

Sense entrar en molt de detall, les representacions donades directament sobre $\mathrm{PGL}(V)$ com en la primera definició no donen una única tria de α per obtenir una representació en el sentit de la segona definició, és a dir, donada $\rho : G \to \mathrm{PGL}(V)$ es poden trobar 2-cocicles diferents α_1, α_2 tals que es tinguin representacions ρ_1, ρ_2 diferents en el sentit de la segona definició però que indueixen el mateix morfisme ρ en projectar-se. Per tal que això passi, els 2-cocicles han de ser cohomòlegs, que constitueix una relació d'equivalència. Així, es pot definir el grup $M(G) = H^2(G, K^\times)$ com el grup de les classes d'equivalència dels 2-cocicles de G a $K^\times$.

Proposició A.4. *Sigui G un grup finit, s'anomena al grup $M(G) = H^2(G, K^\times)$ el multiplicador de Schur de G. Aquest és un grup finit i abelià.*

El multiplicador de Schur és un dels objectes més importants en la teoria de representacions projectiva, és l'objecte que dicta com són els grups que donaran les representacions projectives. Cal remarcar que habitualment en la literatura es fa referència al multiplicador de Schur com a un nombre, indicant simplement l'ordre del grup. La següent definició descriu com s'utilitza el multiplicador de Schur en aquesta teoria.

Definició A.5. Sigui G un grup finit, es diu que G^* és un *grup de representació* de G si existeix una extensió central finita

$$1 \longrightarrow A \longrightarrow G^* \longrightarrow G \longrightarrow 1 \quad \text{(exacta)} \tag{45}$$

tal que $|G^*| = |G||M(G)|$.

Les extensions centrals i les possibles diferents extensions no equivalents estan relacionades amb el segon grup de cohomologies $H^2(G, K^\times)$, per això la definició anterior. Per més informació es pot consultar [Kar85, §2]. La següent caracterització acaba de perfilar el que es vol d'un grup de representació.

Teorema A.6 (Schur, 1907)**.** *Sigui K un cos algebraicament tancat de característica $p \geq 0$. Aleshores G^* és un grup de representació de G sobre K si i només si*

(a) Existeix $A \leq G$ subgrup tal que $A \subseteq Z(G^*) \cap (G^*)'$.

(b) $G \cong G^*/A$.

(c) $|A| = |M(G)|$.

A més a més, per qualssevol A i G^* satisfent (a),(b) i $p \nmid |A|$ aleshores $A \cong M(G)$.

Observació A.7. En el teorema, si G és un grup finit aleshores $(G^*)' = [G^*, G^*]$ és el grup generat pel conjunt de commutadors de G^*.

Demostració. Es pot trobar en [Kar85, §3.3, Teorema 3.7] □

Notem que en característica zero, el grup pel qual es duu a terme les extensions del grup que es vol representar és isomorf al multiplicador de Schur. El resultat anterior s'interpreta considerant el següent diagrama de successions exactes:

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r] \arrow[d] & G^* \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] & 1 & \text{(exacta)} \\ 1 \arrow[r] & K^\times \arrow[r] & \mathrm{GL}(V) \arrow[r] & \mathrm{PGL}(V) \arrow[r] & 1 & \text{(exacta)} \end{tikzcd} \tag{46}$$

L'anterior diagrama commuta sota les condicions del teorema, aleshores les representacions lineals dels grups de representació indueixen representacions projectives del grup que representen i són només els grups de representació els que juguen aquest paper. Així, en característica zero, conèixer les representacions projectives d'un grup es redueix a calcular el multiplicador de Schur i els grups de representació, també anomenats els recobriments pel multiplicador de Schur.

El problema de conèixer A i G i trobar els grups G^* no isomorfs que satisfan la successió exacta pot provar molt complex i està relacionat amb els productes semidirectes de grups. Afortunadament, el següent resultat dona una cota superior a la quantitat de grups de representació no isomorfs que pot tenir un grup.

Teorema A.8 (Schur, 1907)**.** *Sigui G un grup finit i K un cos tal que G^* és un grup de representació de G sobre K. Siguin*

$$G/G' = \mathbb{Z}_{\alpha_1} \times \cdots \times \mathbb{Z}_{\alpha_n}, \qquad M(G) = \mathbb{Z}_{\beta_1} \times \cdots \times \mathbb{Z}_{\beta_m} \tag{47}$$

les descomposicions en factors cíclics, aleshores el nombre de grups de reprensentació de G no isomorfs és menor o igual que

$$\prod_{\substack{1\leq i\leq n\\1\leq j\leq m}} (\alpha_i,\beta_j) \tag{48}$$

En particular, si les ordres de G/G' i $M(G)$ són coprimers aleshores només hi ha un grup de representació G^* llevat isomorfisme.

Demostració. Es pot consultar en [Kar85, §3.4, Teorema 4.4] □

Aquest resultat és especialment útil si G/G' és el grup trivial, atès que aleshores es pot parlar d'un únic grup de representació. Un grup que satisfà la condició $G/G' = \{id\}$ s'anomena un *grup perfecte*, en particular, tot grup simple no abelià és un grup perfecte, per tant, aquest fet facilita molt l'estudi de les representacions projectives dels grups simples.

A.2 Exemples de representacions projectives

En aquesta secció l'objectiu és desenvolupar alguns exemples concrets de representacions projectives i grups de representació. En particular es centraran els esforços en els grups simètrics i els grups alternats. Els grups alternats A_n a partir de $n \geq 5$ són simples i no abelians, per tant, són grups perfectes i només tindran un únic grup de representació, ara bé, la resta dels A_n i els S_n no són grups perfectes, per determinar quants grups de representació no isomorfs tenim caldrà conèixer el multiplicador de Schur.

Teorema A.9. *Si $n \geq 4$ aleshores $M(S_n) = \mathbb{Z}_2$ mentre que si $n < 4$ aleshores $M(S_n) = 1$. Si $n \leq 3$ aleshores $M(A_n) = 1$, si $n = 4,5$ o $n > 7$ aleshores $M(A_n) = \mathbb{Z}_2$, en els casos $n = 6,7$ es té que $M(A_n) = \mathbb{Z}_6$.*

Demostració. Es poden consultar en [Hof92, §2, Teoremes 2.9, 2.11]. □

A partir del multiplicador de Schur es pot deduir el següent resultat.

Proposició A.10. *Si $n \geq 4$ aleshores S_n té com a molt dos grups de representació no isomorfs i A_n en té únicament un (llevat d'isomorfia). Si $n \leq 4$ només hi ha un únic grup de representació en ambdós casos, que és el propi grup.*

Demostració. Pel que fa als A_n amb $n \geq 5$ aquests són grups perfectes. Pel que fa a $n \leq 3$ tant per A_n i S_n, en ser el multiplicador de Schur trivial només hi pot haver un únic grup de representació que és el propi grup. En el cas A_4, es pot veure que $|A_4'| = 4$ és el grup de Klein, la instrucció `DerivedSubgroup(AlternatingGroup(4))` del GAP ho dona. Així, com l'índex del grup és 3, coprimer a 2, només existeix un únic grup de representació. Pel que fa als S_n quan $n \geq 4$, és conegut que $S_n' = A_n$ i, per tant, la cota superior indica que es poden tenir com a molt dos grups de representació no isomorfs. □

La construcció explicita dels dos grups de representació de S_n no isomorfs i el fet que no són isomorfs excepte per $n = 6$ es pot trobar en [Hof92, §2, Teoremes 2.8, 2.11]. Per $n = 6$ els grups són isomorfs i, per tant, resulta només haver-hi un grup de representació.

A.2.1 Representacions projectives de S_4

A continuació es procedirà a construir i estudiar algunes de les característiques de les representacions projectives de S_4 emprant el GAP. En principi el GAP no té perquè conèixer a priori quines són les representacions projectives d'un grup, ara bé, la quantitat d'informació i algoritmes del GAP sobre representacions lineals fa que es pugui treballar amb els grups de representació si són coneguts.

En el cas del grup simètric, la funció `S4p:=SchurCoverOfSymmetricGroup(4,0,1)` retorna un dels recobriments de S_4 i l'anomena `S4p`, mentre que si es canvia 1 per -1 s'obté l'altra que s'anomenarà `S4m`.

```
gap> S4p := SchurCoverOfSymmetricGroup(4,0,1);
Group(
[ [ [ 2/3*E(8)+1/3*E(8)^2-2/3*E(8)^3, -2/3+1/3*E(8)+1/3*E(8)^3 ],
[ 1/3+1/3*E(8)+1/3*E(8)^3, 1/3*E(8)-1/3*E(8)^2-1/3*E(8)^3 ] ], [ [ E(4), -1 ],
[ 0, -E(4) ] ] ])
gap> S4m := SchurCoverOfSymmetricGroup(4,0,-1);
Group(
[ [ [ 1/3-2/3*E(8)-2/3*E(8)^3, 1/3*E(8)+2/3*E(8)^2-1/3*E(8)^3 ],
[ 1/3*E(8)-1/3*E(8)^2-1/3*E(8)^3, -1/3-1/3*E(8)-1/3*E(8)^3 ] ], [ [ -1, -E(4) ],
[ 0, 1 ] ] ])
gap> Order(S4p);
48
gap> Order(S4m);
48
```

La primera cosa que es pot comprovar és que, en efecte, no són isomorfs. En aquest cas, com els grups són d'ordre prou petit es pot mirar si estan en la base de dades de grups d'ordre petit del GAP amb la instrucció `IdGroup` i, en efecte, aquesta fa referència a dos grups diferents.

```
gap> IdGroup(S4p);
[ 48, 28 ]
gap> IdGroup(S4m);
[ 48, 29 ]
```

Si l'objectiu fos saber per quins n es pot representar S_4 en $\mathrm{PGL}_n(K)$, el primer que es consideraria és mirar quins són els ordres dels caràcters lineals irreductibles i quins d'ells són injectius. Els caràcters irreductibles injectius són els que donen representacions injectives del grup en les matrius de l'ordre corresponent, i és el que interessa per fer una classificació. Es detalla a continuació.

```
gap> IrrTableS4 := Irr(CharacterTable(SymmetricGroup(4)));
[ Character( CharacterTable( Sym( [ 1 .. 4 ] ) ), [ 1, -1, 1, 1, -1 ] ),
Character( CharacterTable( Sym( [ 1 .. 4 ] ) ), [ 3, -1, -1, 0, 1 ] ),
Character( CharacterTable( Sym( [ 1 .. 4 ] ) ), [ 2, 0, 2, -1, 0 ] ),
Character( CharacterTable( Sym( [ 1 .. 4 ] ) ), [ 3, 1, -1, 0, -1 ] ),
Character( CharacterTable( Sym( [ 1 .. 4 ] ) ), [ 1, 1, 1, 1, 1 ] ) ]
gap> List(IrrTableS4, DegreeOfCharacter);
[ 1, 3, 2, 3, 1 ]
gap> List(IrrTableS4, i->Order(KernelOfCharacter(i)));
[ 12, 1, 4, 1, 24 ]
```

Notem que el primer caràcter de la llista `IrrTableS4` és el signe de la permutació i el darrer és el caràcter trivial, aquest dos caràcters no són injectius en ser d'ordre 1 i S_4 no abelià, la resta de caràcters són d'ordre 2 i 3. Notem però que els únics que són injectius són els d'ordre 3, mentre que el d'ordre 2 té un nucli d'ordre 4 que es correspon al grup de Klein, subgrup normal dins de S_4. En aquest cas es pot intentar ser més explícits i construir la representació per alguns d'aquests caràcters, així es pot veure computacionalment que el nucli és, en efecte, el grup de Klein i quina és la imatge. S'empraran funcions del paquet [DG19].

```
gap> IrrRep1 := IrreducibleAffordingRepresentation(IrrTableS4[3]);
[ (1,2,3,4), (1,2) ] -> [ [ [ 0, E(3) ], [ E(3)^2, 0 ] ], [ [ 0, 1 ], [ 1, 0 ] ] ]
gap> IrrRep2 := IrreducibleAffordingRepresentation(IrrTableS4[2]);
[ (1,2,3,4), (1,2) ] -> [ [ [ 0, 0, -1 ], [ 0, 1, 0 ], [ 1, 0, 0 ] ],
```

```
[ [ 0, -1, 0 ], [ -1, 0, 0 ], [ 0, 0, -1 ] ] ]
gap> Kernel(IrrRep1);
Group([ (1,3)(2,4), (1,4)(2,3) ])
gap> Image(IrrRep1);
Group([ [ [ 0, E(3) ], [ E(3)^2, 0 ] ], [ [ 0, 1 ], [ 1, 0 ] ] ])
gap> StructureDescription(Image(IrrRep1));
"S3"
gap> Kernel(IrrRep2);
Group(())
gap> Image(IrrRep2);
Group([ [ [ 0, 0, -1 ], [ 0, 1, 0 ], [ 1, 0, 0 ] ],
[ [ 0, -1, 0 ], [ -1, 0, 0 ], [ 0, 0, -1 ] ] ])
gap> StructureDescription(Image(IrrRep2));
"S4"
gap> Center(SymmetricGroup(4));
Group(())
```

Sobre si les representacions injectives lineals constituiran representacions injectives projectives, Notem que com el centre de S_4 és trivial aleshores no es té cap representació amb elements múltiples de la identitat (elements del centre de GL) i, per tant, la injectivitat es preservarà via la projecció. Com ja es sap però, aquests no tenen perquè ser els únics caràcters irreductibles que donin representacions projectives de S_4, per conèixer la resta s'estudien de la mateixa manera els dos recobriments.

```
gap> IrrTableS4p := Irr(CharacterTable(S4p));
(...)
gap> IrrTableS4m := Irr(CharacterTable(S4m));
(...)
gap> List(IrrTableS4p, DegreeOfCharacter);
[ 1, 1, 2, 2, 2, 3, 3, 4 ]
gap> List(IrrTableS4p, i->Order(KernelOfCharacter(i)));
[ 48, 24, 8, 1, 1, 2, 2, 1 ]
gap> List(IrrTableS4m, DegreeOfCharacter);
[ 1, 1, 2, 2, 2, 3, 3, 4 ]
gap> List(IrrTableS4m, i->Order(KernelOfCharacter(i)));
[ 48, 24, 8, 1, 1, 2, 2, 1 ]
```

Notem que en els dos casos s'obtenen caràcters dels mateixos ordres i amb nuclis del mateix ordre. En ambdós casos els primers caràcters són el trivial i l'induït pel signe en S_4, el tercer és el caràcter induït pel grup de Klein i finalment els dos caràcters irreductibles amb nucli d'ordre dos i dimensió 3 són els que venen induïts dels caràcters irreductibles injectius de S_4. Ara bé, notem que apareixen tres caràcters irreductibles injectius nous en cada cas, dos de dimensió 2 i un de dimensió 4. Aquests tres caràcters irreductibles donaran representacions projectives injectives sobre PGL. Com a detall rellevant, observem que S_4 no tenia cap representació irreductible injectiva sobre $\mathrm{GL}_2(K)$, per tant, si es tingués una representació lineal de dimensió 2 injectiva hauria de ser suma directa de les representacions de dimensió 1, però això no pot ser, atès que un grup format únicament per representacions de dimensió 1 és abelià. Per contra, s'acaba de veure que en $\mathrm{PGL}_2(K)$ sí que es pot trobar una representació injectiva del grup S_4.

Finalment, s'aprofitarà la representació irreductible de dimensió 4, que s'anomenarà ρ, per calcular computacionalment la representació projectiva τ de S_4 a $\mathrm{PGL}_4(K)$ i veure que el següent diagrama commuta i obtenir:

$$\begin{tikzcd} S_4^* \arrow[r, "\tilde{\pi}"] \arrow[d, "\rho"] & S_4 \arrow[d, "\tau"] \\ \mathrm{GL}_4(K) \arrow[r, "\pi"] & \mathrm{PGL}_4(K) \end{tikzcd} \tag{49}$$

```
gap> Center(S4p);
Group([ [ [ -1, 0 ], [ 0, -1 ] ] ])
gap> piTilde := NaturalHomomorphismByNormalSubgroup(S4p, Center(S4p));
CompositionMapping( [ (1,2,4,8,7,10,5,9)(3,6,11,15,13,16,12,14),
(1,3,7,13)(2,5,10,4)(6,12,16,11)(8,14,9,15) ] ->
[ f1, f1*f2*f3*f4 ], <action isomorphism> )
gap> rho := IrreducibleAffordingRepresentation(IrrTableS4p[8]);
CompositionMapping( [ (1,2,4,8,7,10,5,9)(3,6,11,15,13,16,12,14),
(1,3,7,13)(2,5,10,4)(6,12,16,11)(8,14,9,15) ] ->
[ [ [ 0, 0, 0, E(4) ], [ 0, 0, E(4), 0 ], [ 1, 0, 0, 0 ], [ 0, 1, 0, 0 ] ],
[ [ 0, 0, -1/2*E(12)^8-1/2*E(12)^11, 1/2*E(12)^8+1/2*E(12)^11 ],
[ 0, 0, -1/2*E(12)^8+1/2*E(12)^11, -1/2*E(12)^8+1/2*E(12)^11 ],
[ 1/2*E(12)^4-1/2*E(12)^7, 1/2*E(12)^4+1/2*E(12)^7, 0, 0 ],
[ -1/2*E(12)^4+1/2*E(12)^7, 1/2*E(12)^4+1/2*E(12)^7, 0, 0 ] ] ], <action isomorphism>)
gap> Center(Image(rho));
<group of 4x4 matrices over Cyclotomics>
gap> GeneratorsSmallest(Center(Image(rho)));
[ [ [ -1, 0, 0, 0 ], [ 0, -1, 0, 0 ], [ 0, 0, -1, 0 ], [ 0, 0, 0, -1 ] ] ]
gap> pi := NaturalHomomorphismByNormalSubgroup(Image(rho), Center(Image(rho)));
CompositionMapping( [ (1,2,4,8,7,10,5,9)(3,6,11,15,13,16,12,14),
(1,3,7,13)(2,5,10,4)(6,12,16,11)(8,14,9,15) ] ->
[ f1, f1*f2*f3*f4 ], <action isomorphism> )
gap> piRho := CompositionMapping(pi,rho);
CompositionMapping( CompositionMapping( [ (1,2,4,8,7,10,5,9)(3,6,11,15,13,16,12,14),
(1,3,7,13)(2,5,10,4)(6,12,16,11)(8,14,9,15) ]->[ f1, f1*f2*f3*f4 ],<action isomorphism>),
CompositionMapping(
[ (1,2,4,8,7,10,5,9)(3,6,11,15,13,16,12,14), (1,3,7,13)(2,5,10,4)(6,12,16,11)(8,14,9,15) ]
-> [ [ [ 0, 0, 0, E(4) ], [ 0, 0, E(4), 0 ], [ 1, 0, 0, 0 ], [ 0, 1, 0, 0 ] ],
[ [ 0, 0, -1/2*E(12)^8-1/2*E(12)^11, 1/2*E(12)^8+1/2*E(12)^11 ],
[ 0, 0, -1/2*E(12)^8+1/2*E(12)^11, -1/2*E(12)^8+1/2*E(12)^11 ],
[ 1/2*E(12)^4-1/2*E(12)^7, 1/2*E(12)^4+1/2*E(12)^7, 0, 0 ],
[ -1/2*E(12)^4+1/2*E(12)^7, 1/2*E(12)^4+1/2*E(12)^7, 0, 0 ] ] ], <action isomorphism> ) )
gap> StructureDescription(Image(piRho));
"S4"
gap> tau := GroupHomomorphismByImages(Image(piTilde),Image(piRho));
[ f1, f1*f2*f3*f4 ] -> [ f1, f1*f2*f3*f4 ]
gap> tauPiTilde := CompositionMapping(tau,piTilde);
CompositionMapping( [ f1, f1*f2*f3*f4 ] -> [ f1, f1*f2*f3*f4 ], CompositionMapping(
[ (1,2,4,8,7,10,5,9)(3,6,11,15,13,16,12,14), (1,3,7,13)(2,5,10,4)(6,12,16,11)(8,14,9,15) ]
-> [ f1, f1*f2*f3*f4 ], <action isomorphism> ) )
gap> tauPiTilde = piRho;
true
```

Notem que el GAP per fer les diverses projeccions canvia com representa els grups, atès que no sap treballar a PGL com a tal, fet que dificulta obtenir directament les matrius per aquesta via. Si es volgués obtenir un representant de cada generador de S_4 en $\mathrm{PGL}_4(K)$ el que es podria fer és

```
gap> iso := GroupHomomorphismByImages(Image(piRho), SymmetricGroup(4));
[ f1, f1*f2*f3*f4 ] -> [ (1,2,3,4), (1,2) ]
gap> matrixMap := CompositionMapping(iso,pi);
CompositionMapping( [ f1, f1*f2*f3*f4 ] -> [ (1,2,3,4), (1,2) ], CompositionMapping(
[ (1,2,4,8,7,10,5,9)(3,6,11,15,13,16,12,14),
```

```
(1,3,7,13)(2,5,10,4)(6,12,16,11)(8,14,9,15) ] -> [ f1, f1*f2*f3*f4 ],
<action isomorphism> ) )
gap> PreImagesRepresentative(matrixMap,(1,2));
[ [ 0, 0, 1/2*E(12)^8+1/2*E(12)^11, -1/2*E(12)^8-1/2*E(12)^11 ],
[ 0, 0, 1/2*E(12)^8-1/2*E(12)^11, 1/2*E(12)^8-1/2*E(12)^11 ],
[ -1/2*E(12)^4+1/2*E(12)^7, -1/2*E(12)^4-1/2*E(12)^7, 0, 0 ],
[ 1/2*E(12)^4-1/2*E(12)^7, -1/2*E(12)^4-1/2*E(12)^7, 0, 0 ] ]
gap> PreImagesRepresentative(matrixMap,(1,2,3));
[ [ -1/2*E(12)^8+1/2*E(12)^11, -1/2*E(12)^8+1/2*E(12)^11, 0, 0 ],
[ 1/2*E(12)^8+1/2*E(12)^11, -1/2*E(12)^8-1/2*E(12)^11, 0, 0 ],
[ 0, 0, -1/2*E(12)^4-1/2*E(12)^7, -1/2*E(12)^4+1/2*E(12)^7 ],
[ 0, 0, 1/2*E(12)^4+1/2*E(12)^7, -1/2*E(12)^4+1/2*E(12)^7 ] ]
```

Notem que `iso` únicament identifica el grup en lletres amb la representació de permutacions de S_4 per tal que sigui més fàcil de consultar i es defineix un nou morfisme `matrixMap` que va de la imatge de S_4^* per ρ en matrius al grup S_4 representat en permutacions via π i `iso`. Així, es poden obtenir els representants en la forma matricial.

A.2.2 Representacions projectives de A_5

A continuació s'inspeccionaran quines són les representacions projectives del grup A_5. Com s'ha comentat anteriorment, A_5 és un dels grups simples més petits que no té un multiplicador de Schur trivial i que evidencia la necessitat d'anar més enllà de la teoria de representacions lineal. També es sap que en ser A_5 simple només es té un únic grup de representacions (llevat isomorfisme). En aquest cas, la base de dades del GAP, que integra l'Atlas dels grups finits simples, ja incorpora informació sobre les representacions projectives d'aquest grup i el seu recobriment. En particular, el grup de representació de A_5 s'acostuma a anomenar $2 \cdot A_5$ el doble recobriment de A_5 i és isomorf al grup $SL(2,5)$. Aquest fet té prou de sentit atès que es coneix que $PSL(2,5)$ és isomorf a A_5.

```
gap> ProjectivesInfo(CharacterTable("A5"));
[ rec( chars :=
[ [ 2, 0, -1, E(5)+E(5)^4, E(5)^2+E(5)^3 ],
[ 2, 0, -1, E(5)^2+E(5)^3, E(5)+E(5)^4 ],
[ 4, 0, 1, -1, -1 ], [ 6, 0, 0, 1, 1 ] ], name := "2.A5" ) ]
gap> Irr(CharacterTable("A5"));
[ Character( CharacterTable( "A5" ), [ 1, 1, 1, 1, 1 ] ),
Character( CharacterTable( "A5" ), [ 3, -1, 0, -E(5)-E(5)^4, -E(5)^2-E(5)^3 ] ),
Character( CharacterTable( "A5" ), [ 3, -1, 0, -E(5)^2-E(5)^3, -E(5)-E(5)^4 ] ),
Character( CharacterTable( "A5" ), [ 4, 0, 1, -1, -1 ] ),
Character( CharacterTable( "A5" ), [ 5, 1, -1, 0, 0 ] ) ]
```

Notem que `ProjectivesInfo` només dona els caràcters irreductibles que són injectius corresponents al recobriment. Els caràcters induïts directament per caràcters lineals de A_5 s'han de consultar a part. Observem que A_5 adquireix dos caràcters irreductibles de dimensions diferents dels lineals, de dimensions 2 i 6. Els caràcters que apareixen de dimensió 2 corresponen a la representació que s'obté geomètricament en considerar A_5 com el grup de simetries d'un icosaedre. Per inspeccionar tots els possibles caràcters, inclosos els no injectius es pot construir el doble recobriment i calcular-ne els caràcters irreductibles.

```
gap> 2A5 := DoubleCoverOfAlternatingGroup(5);
<matrix group of size 120 with 2 generators>
gap> StructureDescription(2A5);
"SL(2,5)"
```

```
gap> Table2A5 := CharacterTable(2A5);
CharacterTable( SL(2,5) )
gap> Irr(Table2A5);
[ Character( CharacterTable( SL(2,5) ), [ 1, 1, 1, 1, 1, 1, 1, 1, 1 ] ),
Character( CharacterTable( SL(2,5) ),
[ 2, -E(5)-E(5)^4, -E(5)^2-E(5)^3, 1, E(5)^2+E(5)^3, E(5)+E(5)^4, 0, -1, -2 ] ),
Character( CharacterTable( SL(2,5) ),
[ 2, -E(5)^2-E(5)^3, -E(5)-E(5)^4, 1, E(5)+E(5)^4, E(5)^2+E(5)^3, 0, -1, -2 ] ),
Character( CharacterTable( SL(2,5) ),
[ 3, -E(5)^2-E(5)^3, -E(5)-E(5)^4, 0, -E(5)-E(5)^4, -E(5)^2-E(5)^3, -1, 0, 3 ] ),
Character( CharacterTable( SL(2,5) ),
[ 3, -E(5)-E(5)^4, -E(5)^2-E(5)^3, 0, -E(5)^2-E(5)^3, -E(5)-E(5)^4, -1, 0, 3 ] ),
Character( CharacterTable( SL(2,5) ), [ 4, -1, -1, 1, -1, -1, 0, 1, 4 ] ),
Character( CharacterTable( SL(2,5) ), [ 4, 1, 1, -1, -1, -1, 0, 1, -4 ] ),
Character( CharacterTable( SL(2,5) ), [ 5, 0, 0, -1, 0, 0, 1, -1, 5 ] ),
Character( CharacterTable( SL(2,5) ), [ 6, -1, -1, 0, 1, 1, 0, 0, -6 ] ) ]
gap> CharacterDegrees(Table2A5);
[ [ 1, 1 ], [ 2, 2 ], [ 3, 2 ], [ 4, 2 ], [ 5, 1 ], [ 6, 1 ] ]
gap> CharacterDegrees(CharacterTable("A5"));
[ [ 1, 1 ], [ 3, 2 ], [ 4, 1 ], [ 5, 1 ] ]
gap> List(Irr(Table2A5), i->Order(KernelOfCharacter(i)));
[ 120, 1, 1, 2, 2, 2, 1, 2, 1 ]
gap> List(Irr(Table2A5), DegreeOfCharacter);
[ 1, 2, 2, 3, 3, 4, 4, 5, 6 ]
```

Així doncs, notem que no n'hi ha cap més a part dels que ja s'havien vist.

Una de les primeres comprovacions que es poden fer és veure que en efecte la imatge d'una de les representacions projectives de dimensió 2, quan la projectem a $\mathrm{PGL}_2(K)$, és isomorfa al grup A_5. Es mostra en el codi següent.

```
gap> 2A5 := Image(IsomorphismPermGroup(DoubleCoverOfAlternatingGroup(5)));;
gap> Table2A5 := CharacterTable(2A5);;
gap> IrrTable2A5 := Irr(Table2A5);;
gap> IrrDim2 := IrreducibleAffordingRepresentation(IrrTable2A5[2]);;
gap> IrrDim2Group := Image(IrrDim2);
Group(
[ [ [ 1/3*E(15)-2/3*E(15)^2+1/3*E(15)^4-1/3*E(15)^7-2/3*E(15)^8
-1/3*E(15)^11-1/3*E(15)^13-1/3*E(15)^14, -1/3*E(3)-2/3*E(3)^2 ],
[ 2/3*E(3)+1/3*E(3)^2, -1/3*E(15)-1/3*E(15)^2-1/3*E(15)^4-2/3*E(15)^7
-1/3*E(15)^8+1/3*E(15)^11-2/3*E(15)^13+1/3*E(15)^14 ] ],
[ [ E(3), 0 ], [ 0, E(3)^2 ] ] ])
gap> GeneratorsOfGroup(Center(IrrDim2Group));
[ [ [ -1, 0 ], [ 0, -1 ] ] ]
gap> IrrDim2Quotient := FactorGroup(IrrDim2Group,Center(IrrDim2Group));
Group([ (2,3,4,6,5), (1,2,4)(3,5,6) ])
gap> StructureDescription(IrrDim2Quotient);
"A5"
```

Notem que per tal que la funció `IrreducibleAffordingRepresentation` funcioni correctament cal assegurar-se de que el grup definit com `2A5` estigui un una representació per permutacions. Finalment, observem que es recupera A_5 en fer quocient pel centre del grup que és un múltiple de la identitat i, per tant, és el mateix que projectar a $\mathrm{PGL}_2(K)$.

Finalment es pot estudiar com es relacionen les representacions irreductibles obtingudes amb la representació natural de A_5 en $\mathrm{PGL}_5(K)$ en forma de matrius de permutacions. El que es voldria veure és essencialment si aquesta representació és la irreductible de dimensió 5 obtinguda o si és reduïble i, en tal cas, quines representacions irreductibles la conformen. Per tal de fer-ho, es pot crear la representació manualment i calcular-ne el seu caràcter. Un cop es tingui el caràcter es pot demanar al GAP que faci les comprovacions pertinents.

```
gap> A5 := AlternatingGroup(5);
Alt( [ 1 .. 5 ] )
gap> GeneratorsOfGroup(A5);
[ (1,2,3,4,5), (3,4,5) ]
gap> PermMatA5 := Group(PermutationMat((1,2,3,4,5),5),PermutationMat((3,4,5),5));
<matrix group with 2 generators>
gap> ConjugacyClasses(PermMatA5);;
gap> ConjClassReps := List(ConjugacyClasses(PermMatA5), Representative);
[ [ [ 1, 0, 0, 0, 0 ], [ 0, 1, 0, 0, 0 ], [ 0, 0, 1, 0, 0 ], [ 0, 0, 0, 1, 0 ],
[ 0, 0, 0, 0, 1 ] ],
[ [ 0, 0, 0, 0, 1 ], [ 0, 0, 0, 1, 0 ], [ 0, 1, 0, 0, 0 ], [ 1, 0, 0, 0, 0 ],
[ 0, 0, 1, 0, 0 ] ],
[ [ 0, 0, 0, 0, 1 ], [ 0, 0, 1, 0, 0 ], [ 0, 0, 0, 1, 0 ], [ 1, 0, 0, 0, 0 ],
[ 0, 1, 0, 0, 0 ] ],
[ [ 0, 0, 0, 0, 1 ], [ 0, 1, 0, 0, 0 ], [ 0, 0, 1, 0, 0 ], [ 1, 0, 0, 0, 0 ],
[ 0, 0, 0, 1, 0 ] ],
[ [ 0, 0, 0, 0, 1 ], [ 0, 0, 0, 1, 0 ], [ 0, 0, 1, 0, 0 ], [ 0, 1, 0, 0, 0 ],
[ 1, 0, 0, 0, 0 ] ] ]
gap> CharValuesRep := List(ConjClassReps, TraceMat);
[ 5, 0, 0, 2, 1 ]
gap> RepCharacter := Character(PermMatA5,CharValuesRep);
Character( CharacterTable( <matrix group of size 60 with 2 generators> ),
[ 5, 0, 0, 2, 1 ] )
gap> Norm(RepCharacter);
2
gap> ConstituentsOfCharacter(RepCharacter);
[ Character( CharacterTable( <matrix group of size 60 with 2 generators> ),
[ 1, 1, 1, 1, 1 ] ),
Character( CharacterTable( <matrix group of size 60 with 2 generators> ),
[ 4, -1, -1, 1, 0 ] ) ]
```

La primera comprovació que es duu a terme un cop obtingut el caràcter és si la seva norma és 1, que voldria dir que el caràcter és irreductible, ara bé, es troba que la norma és 2, per tant, el caràcter no és irreductible i es demana la seva descomposició. S'obté que el caràcter associat a la representació amb matrius de permutacions és la suma del caràcter trivial i el caràcter irreductible de dimensió 4. Així, sota un canvi de base, la representació en matrius de permutacions es pot escriure com una representació de matrius bloc-diagonals amb un bloc de dimensió 1 que conté 1 sempre i un bloc de dimensió 4 que conté la representació associada al caràcter irreductible de dimensió 4.

B Determinants de Vandermonde generalitzats i els polinomis de Schur

Els polinomis de Schur [Per] són una família de polinomis simètrics que es defineixen com

$$s_\lambda(x_1,\dots,x_n) = \prod_{1\le i<j\le n}(x_i-x_j)^{-1}\begin{vmatrix} x_1^{\lambda_1+n-1} & x_2^{\lambda_1+n-1} & \dots & x_n^{\lambda_1+n-1} \\ x_1^{\lambda_2+n-2} & x_2^{\lambda_2+n-2} & \dots & x_n^{\lambda_2+n-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\lambda_n} & x_2^{\lambda_n} & \dots & x_n^{\lambda_n}\end{vmatrix} \tag{50}$$

on $d \in \mathbb{N}$ i $\lambda \vdash d$ és una partició. Notem que

$$V^{-1} = \prod_{1\le i<j\le n}(x_i-x_j)^{-1} \tag{51}$$

és l'invers del determinant de Vandermonde i el determinant que es mostra en (50) correspon al que s'anomena un determinant de Vandermonde generalitzat. Si es pren la partició

$$\Lambda_i^m = (m-n+1, \underbrace{1,\dots,1}_{n-i-1}, \underbrace{0,\dots,0}_{i})$$

considerant $1 \le i < n, m \ge n$ aleshores el polinomi $s_{\Lambda_i^m}(x_1,\dots,x_n)$ satisfà

$$s_{\Lambda_i^m}(\alpha_1,\dots,\alpha_n) = (-1)^i(-1)^{\lfloor n/2\rfloor}\mathcal{B}_i \tag{52}$$

en la notació de la secció (4.1). Segons [Per, Specializations] es té la següent expressió:

$$s_\lambda(1,\dots,1) = \prod_{1\le j<k\le n}\frac{\lambda_k-\lambda_j+j-k}{j-k} \tag{53}$$

Per Λ_i^m es té que si $k,j \in \{n,\dots,n-(i-1)\}$ o bé $k,j\in\{n-i,\dots,2\}$ aleshores $\frac{\lambda_k-\lambda_j+j-k}{j-k}=1$. Atès que $j<k$ el valor del terme del productori serà diferent de 1 quan $k\in\{n,\dots,n-(i-1)\}$ i $j\in\{n-i,\dots,2\}$. En aquest cas, $\lambda_k=0$ mentre que $\lambda_j=1$, per tant,

$$\frac{\lambda_k-\lambda_j+j-k}{j-k} = 1-\frac{1}{j-k} = \frac{j-k-1}{j-k} \tag{54}$$

Fixat un j i considerant els termes donats per $n \le k > j$ s'obté el producte

$$\frac{j-n-1}{j-n}\frac{j-n-2}{j-n-1}\cdots\frac{j-(n-(i-1))-1}{j-(n-(i-1))} = \frac{j-n+i-1-1}{j-n} = \frac{j-n+i-2}{j-n} \tag{55}$$

A continuació, fent el producte de tots els termes anteriors per $2\le j\le n-i$ s'obté

$$\frac{(n-i)-n+i-2}{(n-i)-n}\frac{(n-i-1)-n+i-2}{(n-i-1)-n}\cdots\frac{2-n+i-2}{2-n} = \frac{2}{i}\frac{3}{i+1}\cdots\frac{n-i}{n-2} = \tag{56}$$

$$= \frac{(n-i)!(i-1)!}{(n-2)!} = \binom{n-1}{i-1}^{-1}(n-1) \tag{57}$$

Falta ara considerar els termes del producte corresponents a $k\in\{2,\dots,n\}$ i $j=1 \Rightarrow \lambda_j = m-n+1$. Els dividim en dos grups, si $k\in\{n,\dots,n-(i-1)\}\Rightarrow\lambda_k=0$ i si $k\in\{n-i,\dots,2\}\Rightarrow\lambda_k=1$. En el primer dels casos:

$$\frac{-(m-n+1)+1-n}{1-n}\frac{-(m-n+1)+1-(n-1)}{1-(n-1)}\cdots\frac{-(m-n+1)-(n+1-i)}{1-(n+1-i)} = \tag{58}$$

$$= \frac{m(m-1)\cdots(m-i+1)}{(n-1)(n-2)\cdots(n-i)} \tag{59}$$

El el segon cas:

$$\frac{1-(m-n+1)+1-(n-i)}{1-(n-i)}\frac{1-(m-n+1)+1-(n-i-1)}{1-(n-i-1)}\cdots\frac{1-(m-n+1)+1-2}{1-2} = \tag{60}$$

$$= \frac{(m-i-1)(m-i-2)\cdots(m-n+1)}{(n-i-1)\cdots 2\cdot 1} \tag{61}$$

Fent el producte dels dos casos s'obté

$$\frac{m(m-1)\cdots(m-i+1)\widehat{(m-i)}(m-i-1)\cdots(m-n+1)}{(n-1)!} \tag{62}$$

Finalment, si s'ajunten totes les diferents components calculades el resultat és

$$s_{\Lambda_i^m}(1,\ldots,1) = \frac{m(m-1)\cdots(m-i+1)\widehat{(m-i)}(m-i-1)\cdots(m-n+1)}{\binom{n-1}{i-1}(n-2)!} \tag{63}$$

Seguint un procès similar pel cas $i=0$ s'obté:

$$s_{\Lambda_0^m}(1,\ldots,1) = \frac{(m-1)\ldots(m-n+1)}{(n-1)!} \tag{64}$$

C Taules de cotes subgrups primitius

Taula 5: Potència màxima dels primers que poden dividir l'ordre dels grups finits primitius de $PGL_n(\mathbb{C})$ i $GL_n(\mathbb{C})$

n	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61
2	2	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	3	3	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	10	4	3	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	7	5	5	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
6	16	10	6	4	1	1	0	0	0	0	0	0	0	0	0	0	0	0
7	10	8	7	6	1	1	0	0	0	0	0	0	0	0	0	0	0	0
8	25	9	8	7	1	1	1	0	0	0	0	0	0	0	0	0	0	0
9	15	17	9	8	1	1	1	1	0	0	0	0	0	0	0	0	0	0
10	31	13	12	9	6	1	1	1	0	0	0	0	0	0	0	0	0	0
11	18	14	12	10	8	1	1	1	1	0	0	0	0	0	0	0	0	0
12	38	22	13	11	9	7	1	1	1	0	0	0	0	0	0	0	0	0
13	22	17	14	12	9	9	1	1	1	0	0	0	0	0	0	0	0	0
14	44	18	15	13	10	10	1	1	1	1	0	0	0	0	0	0	0	0
15	25	28	18	14	11	10	1	1	1	1	1	0	0	0	0	0	0	0
16	53	21	18	15	12	11	9	1	1	1	1	0	0	0	0	0	0	0
17	31	22	19	16	12	12	11	1	1	1	1	0	0	0	0	0	0	0
18	59	35	20	17	13	12	11	10	1	1	1	1	0	0	0	0	0	0
19	34	26	21	18	14	13	12	11	1	1	1	1	0	0	0	0	0	0
20	67	27	25	19	15	14	13	12	1	1	1	1	1	0	0	0	0	0
21	38	41	24	21	15	14	13	13	1	1	1	1	1	1	0	0	0	0
22	73	30	25	22	17	15	14	13	12	1	1	1	1	1	0	0	0	0
23	41	31	26	23	18	16	14	14	13	1	1	1	1	1	1	0	0	0
24	81	47	27	24	19	17	15	14	14	1	1	1	1	1	1	0	0	0
25	46	34	32	25	19	17	16	15	14	1	1	1	1	1	1	0	0	0
26	87	35	31	26	20	19	16	16	15	1	1	1	1	1	1	1	0	0
27	49	55	32	26	21	20	17	16	15	1	1	1	1	1	1	1	0	0
28	94	40	33	28	22	20	18	17	16	14	1	1	1	1	1	1	0	0
29	53	41	34	29	22	21	18	18	17	15	1	1	1	1	1	1	1	0
30	100	61	39	30	23	22	19	18	17	16	15	1	1	1	1	1	1	1
31	56	44	37	31	24	22	19	19	18	16	16	1	1	1	1	1	1	1
32	111	45	38	32	25	23	20	19	18	17	17	1	1	1	1	1	1	1

D Taules de candidats a subgrups simples primitius

Taula 6: Nomenclatures dels grups simples de tipus Lie [Wik24]

Família	Wikipedia	Clàssic	[GAP]	Altres	Obs.
Classical Chevalley A	$A_n(q)$	$PSL_{n+1}(q)$	`L[n+1](q)`	$L_{n+1}(q)$	1, 4
Classical Chevalley B	$B_n(q)$	$\Omega_{2n+1}(q)$	`O[2n+1](q)`	$O_{2n+1}(q)$	1, 4, 5, 6
Classical Chevalley C	$C_n(q)$	$PSp_{2n}(q)$	`S[2n](q)`	$S_{2n}(q)$, $PSp_n(q)$	1, 4
Classical Chevalley D	$D_n(q)$	$O^+_{2n}(q)$	`O[2n]+(q)`	$P\Omega^+_{2n}(q)$	1, 4
Exceptional Chevalley E_6	$E_6(q)$	—	`E6(q)`	—	2
Exceptional Chevalley E_7	$E_7(q)$	—	`E7(q)`	—	2
Exceptional Chevalley E_8	$E_8(q)$	—	`E8(q)`	—	2
Exceptional Chevalley F_4	$F_4(q)$	—	`F4(q)`	—	2
Exceptional Chevalley G_2	$G_2(q)$	—	`G2(q)`	—	2, 4
Classical Steinberg A	${}^2A_n(q^2)$	$PSU_{n+1}(q)$	`U[n+1](q)`	$U_{n+1}(q)$, ${}^2A_n(q)$, ${}^2A_n(q,q^2)$	1, 4
Classical Steinberg D	${}^2D_n(q^2)$	$O^-_{2n}(q)$	`O[2n]-(q)`	$P\Omega^-_{2n}(q)$, ${}^2D_n(q)$	1, 4
Exceptional Steinberg E_6	${}^2E_6(q^2)$	—	`2E6(q)`	${}^2E_6(q)$	2
Exceptional Steinberg D_4	${}^3D_4(q^3)$	—	`3D4(q)`	${}^3D_4(q)$, $D_4^2(q^3)$	2
Suzuki	${}^2B_2(q)$	$Sz(2^{2n+1})$	Sz(2^{2n+1})	Suz(2^{2n+1})	3
Ree-Tits	${}^2F_4(2^{2n+1})$	—	2F4(2^{2n+1})	—	3
Tits	${}^2F_4(2)'$	—	`2F4(2)'`	—	
Ree	${}^2G_2(3^{2n+1})$	$R(3^{2n+1})$	R(3^{2n+1})	Ree(3^{2n+1}), $E_2^*(3^{2n+1})$	3

Observacions:

1. Paràmetres $n \geq 1$ natural i q potència d'un primer p, $q = p^k$, $k \geq 1$.
2. Paràmetre q potència d'un primer p, $q = p^k$, $k \geq 1$.
3. Paràmetre $n \geq 1$ natural.
4. Consulteu excepcions, duplicats i restriccions sobre n en [Wik24]
5. No es recomana l'ús de la notació $O_{2n+1}(q)$, pot donar a confusió amb el grup ortogonal sobre $\mathbb{F}_q$: $O(2n+1,q) = O_n(\mathbb{F}_q)$.
6. Notació clàssica i alternativa equivalent a la notació Wikipedia només en el cas q senar.

Taula 7: Candidats a grups simples primitius de $\mathrm{PGL}_n(\mathbb{C})$

n	Representacions confirmades	Representacions no confirmades
12	A_6, A_{13}, M_{12}, Suz, $PSL_2(25)$, $PSL_2(11)$, $PSL_2(13)$, $PSL_2(23)$, $\Omega_5(5)$, $G_2(4)$, $PSL_3(3)$, $PSU_3(4)$	A_{20}, A_{21}, A_{22}, A_{23}, A_{24}, A_{25}, A_{26}, A_{27}, A_{28}, $PSL_3(16)$, $PSL_6(3)$, $PSL_4(7)$, $PSL_2(169)$, $\Omega_5(13)$, ${}^2E_6(3)$, $PSU_4(8)$, A_14, A_{15}, A_{16}, A_{17}, A_{18}, A_{19}, $\Omega_5(7)$, $PSU_4(5)$, $P\Omega_8^-(2)$
13	A_{14}, $PSL_2(27)$, $PSL_2(25)$, $PSL_2(13)$, $PSp_6(3)$, $\Omega_5(5)$, $PSL_3(3)$, $PSU_3(4)$	A_{20}, A_{21}, A_{22}, A_{23}, A_{24}, A_{25}, A_{26}, A_{27}, $PSL_3(16)$, $PSL_6(3)$, $PSL_4(7)$, $PSL_2(169)$, $\Omega_5(13)$, $PSU_4(8)$, A_{15}, A_{16}, A_{17}, A_{18}, A_{19}, $\Omega_5(7)$, $PSU_4(5)$, $P\Omega_8^-(2)$
14	A_7, A_8, A_{15}, J_2, $PSL_2(27)$, $PSL_2(13)$, $PSp_6(3)$, $G_2(3)$, $Sz(8)$, $PSU_3(3)$	A_{20}, A_{21}, A_{22}, A_{23}, A_{24}, A_{25}, A_{26}, A_{27}, $PSL_3(16)$, $PSL_6(3)$, $PSL_4(7)$, $PSL_2(169)$, $\Omega_5(13)$, $PSU_4(8)$, A_{14}, A_{16}, A_{17}, A_{18}, A_{19}, $\Omega_5(7)$, $PSU_4(5)$, $P\Omega_8^-(2)$
15	A_6, A_7, A_{16}, $PSL_3(4)$, $\Omega_7(2)$, $PSU_4(2)$, $PSU_4(3)$, $PSL_2(16)$	A_{20}, A_{21}, A_{22}, A_{23}, A_{24}, A_{25}, A_{26}, A_{27}, $PSL_3(16)$, $PSL_6(3)$, $PSL_4(7)$, $PSL_2(169)$, $\Omega_5(13)$, $PSU_4(8)$, A_{14}, A_{15}, A_{17}, A_{18}, A_{19}, $\Omega_5(7)$, $PSU_4(5)$, $P\Omega_8^-(2)$
16	A_{10}, A_{11}, A_{17}, M_{12}, $PSL_2(17)$, M_{11}, $PSL_2(16)$, $PSL_3(3)$	A_{20}, A_{21}, A_{22}, A_{23}, A_{24}, A_{25}, A_{26}, A_{27}, $PSL_3(16)$, $PSL_6(3)$, $PSL_4(7)$, $PSL_2(169)$, $\Omega_5(13)$, $PSU_4(8)$, A_{14}, A_{15}, A_{16}, A_{18}, A_{19}, $\Omega_5(7)$, $PSU_4(5)$, $P\Omega_8^-(2)$
17	A_{18}, $PSL_2(17)$, $PSL_2(16)$	A_{20}, A_{21}, A_{22}, A_{23}, A_{24}, A_{25}, A_{26}, A_{27}, $PSL_3(16)$, $PSL_6(3)$, $PSL_4(7)$, $PSL_2(169)$, $\Omega_5(13)$, $PSU_4(8)$, A_{14}, A_{15}, A_{16}, A_{17}, A_{19}, $\Omega_5(7)$, $PSU_4(5)$, $P\Omega_8^-(2)$
18	A_{19}, J_3, $PSL_2(17)$, $PSL_2(19)$, $\Omega_5(4)$	A_{20}, A_{21}, A_{22}, A_{23}, A_{24}, A_{25}, A_{26}, A_{27}, $PSL_3(16)$, $PSL_6(3)$, $PSL_4(7)$, $PSL_2(169)$, $\Omega_5(13)$, $PSU_4(8)$, A_{14}, A_{15}, A_{16}, A_{17}, A_{18}, $\Omega_5(7)$, $PSU_4(5)$, $P\Omega_8^-(2)$
19	$PSL_2(19)$	A_{20}, A_{21}, A_{22}, A_{23}, A_{24}, A_{25}, A_{26}, A_{27}, $PSL_3(16)$, $PSL_6(3)$, $PSL_4(7)$, $PSL_2(169)$, $\Omega_5(13)$, $PSU_4(8)$, A_{14}, A_{15}, A_{16}, A_{17}, A_{18}, A_{19}, $\Omega_5(7)$, $PSU_4(5)$, $P\Omega_8^-(2)$
20	A_7, A_8, $PSL_3(4)$, $PSL_2(19)$, $PSU_4(2)$, $PSU_4(3)$, $PSU_3(5)$	A_{20}, A_{21}, A_{22}, A_{23}, A_{24}, A_{25}, A_{26}, A_{27}, $PSL_3(16)$, $PSL_6(3)$, $PSL_4(7)$, $PSL_2(169)$, $\Omega_5(13)$, $PSU_4(8)$, A_{14}, A_{15}, A_{16}, A_{17}, A_{18}, A_{19}, $\Omega_5(7)$, $PSU_4(5)$, $P\Omega_8^-(2)$

Observacions:

1. La taula mostra els grups simples candidats a ser primitius en cada $\mathrm{PGL}_n(\mathbb{C})$.
2. La columna *Representacions confirmades* denota que s'ha confirmat que el grup indicat té una representació irreductible en $\mathrm{PGL}_n(\mathbb{C})$, **NO** denota que la representació sigui primitiva.
3. La columna *Representacions no confirmades* indica els grups que satisfan la cota donada en 5 però que no s'ha pogut confirmar si té una representació irreductible.
4. Les representacions projectives del grup alternat (i del grup simètric) són conegudes a la literatura [Hof92]. Així doncs, seria possible reduir significativament els grups alternats donats en la llista.
5. És possible reduir la quantitat de grups simples de tipus Lie que apareixen en la llista a partir de les taules donades en [SZ93]. Aquestes taules indiquen una cota inferior al grau mínim de les representacions projectives dels grups simples de Lie.
6. En el cas dels n primers, els grups simples primitius de $\mathrm{PGL}_n(\mathbb{C})$ estan completament determinats en [DZ98].

Referències

[AOT24] Jose Avila, Guillermo Ortiz i Sergio Troncoso. "Invariant smooth quartic surfaces by all finite primitive subgroups of $\mathrm{PGL}_4(\mathbb{C})$". English. A: *J. Pure Appl. Algebra* 228.4 (2024). Id/No 107534, pàg. 24. ISSN: 0022-4049. DOI: 10.1016/j.jpaa.2023.107534.

[Bli03] H F Blichfeldt. "On the order of linear homogeneous groups". A: *Trans. Amer. Math. Soc.* 4 (4 1903), pàg. 387 - 397. ISSN: 0002-9947,1088-6850. DOI: 10.2307/1986408. URL: https://doi.org/10.2307/1986408.

[Bli04] H F Blichfeldt. "On the order of linear homogeneous groups. II". A: *Trans. Amer. Math. Soc.* 5 (3 1904), pàg. 310 - 325. ISSN: 0002-9947,1088-6850. DOI: 10.2307/1986460. URL: https://doi.org/10.2307/1986460.

[Bli06] H F Blichfeldt. "On the order of linear homogeneous groups (supplement)". A: *Trans. Amer. Math. Soc.* 7 (4 1906), pàg. 523 - 529. ISSN: 0002-9947,1088-6850. DOI: 10.2307/1986244. URL: https://doi.org/10.2307/1986244.

[Bli11] H F Blichfeldt. "On the order of linear homogeneous groups. IV". A: *Trans. Amer. Math. Soc.* 12 (1 1911), pàg. 39 - 42. ISSN: 0002-9947,1088-6850. DOI: 10.2307/1988733. URL: https://doi.org/10.2307/1988733.

[Bli17] H. F. Blichfeldt. *Finite collineation groups.* Ed. d'Eliakim Hastings Moore, John Merle Coulter i Robert Andrews Millikan. 1a ed. University of Chicago Press, abr. de 1917.

[Bra42a] Richard Brauer. "On groups whose order contains a prime number to the first power. I". A: *Amer. J. Math.* 64 (1942), pàg. 401 - 420. ISSN: 0002-9327,1080-6377. DOI: 10.2307/2371693. URL: https://doi.org/10.2307/2371693.

[Bra42b] Richard Brauer. "On groups whose order contains a prime number to the first power. II". A: *Amer. J. Math.* 64 (1942), pàg. 421 - 440. ISSN: 0002-9327,1080-6377. DOI: 10.2307/2371694. URL: https://doi.org/10.2307/2371694.

[Bra67] Richard Brauer. "Über endliche lineare Gruppen von Primzahlgrad". A: *Math. Ann.* 169 (1967), pàg. 73 - 96. ISSN: 0025-5831,1432-1807. DOI: 10.1007/BF01399532. URL: https://doi.org/10.1007/BF01399532.

[Bre22] T. Breuer. *CTblLib, The GAP Character Table Library, Version 1.3.4.* GAP package. Abr. de 2022. URL: https://www.math.rwth-aachen.de/~Thomas.Breuer/ctbllib.

[Cona] Keith Conrad. *GENERATING SETS.* URL: https://kconrad.math.uconn.edu/blurbs/grouptheory/genset.pdf.

[Conb] Keith Conrad. *THE MINIMAL POLYNOMIAL AND SOME APPLICATIONS.* URL: https://kconrad.math.uconn.edu/blurbs/linmultialg/minpolyandappns.pdf.

[DG19] V. Dabbaghian i T. GAP Team. *Repsn, Constructing representations of finite groups, Version 3.1.0.* https://gap-packages.github.io/repsn/. Refereed GAP package. Febr. de 2019.

[DZ04] J. D. Dixon i A. E. Zalesski. "Finite imprimitive linear groups of prime degree". A: *J. Algebra* 276.1 (2004), pàg. 340 - 370. ISSN: 0021-8693,1090-266X. DOI: 10.1016/j.jalgebra.2004.02.005. URL: https://doi.org/10.1016/j.jalgebra.2004.02.005.

[DZ08] J D Dixon i A E Zalesskii. "Corrigendum: "Finite primitive linear groups of prime degree" [J. London Math. Soc. (2) 57 (1998), no. 1, 126–134; MR1624805]". A: *J. Lond. Math. Soc. (2)* 77 (3 2008), pàg. 808 - 812. ISSN: 0024-6107,1469-7750. DOI: 10.1112/jlms/jdm103. URL: https://doi.org/10.1112/jlms/jdm103.

[DZ98] J D Dixon i A E Zalesskii. "Finite primitive linear groups of prime degree". A: *J. London Math. Soc. (2)* 57 (1 1998), pàg. 126 - 134. ISSN: 0024-6107,1469-7750. DOI: 10.1112/S0024610798005778. URL: https://doi.org/10.1112/S0024610798005778.

[FCB17] Eslam Essam Ebrahim Farag, Francesc Bars Cortina i Universitat Autònoma de Barcelona. Departament de Matemàtiques. *On the stratification of smooth plane curves by automorphism groups*. Universitat Autònoma de Barcelona, set. de 2017. ISBN: 9788449075858. URL: http://tesisenred.net/handle/10803/457868.

[Fei64] Walter Feit. "Groups which have a faithful representation of degree less than $p-1$". A: *Trans. Amer. Math. Soc.* 112 (1964), pàg. 287 - 303. ISSN: 0002-9947,1088-6850. DOI: 10.2307/1994296. URL: https://doi.org/10.2307/1994296.

[Fei71] Walter Feit. "The current situation in the theory of finite simple groups". A: *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1*. Gauthier-Villars Éditeur, Paris, 1971, pàg. 55 - 93. URL: https://www.mathunion.org/fileadmin/ICM/Proceedings/ICM1970.1/ICM1970.1.ocr.pdf.

[Fro68] Ferdinand Georg Frobenius. *Gesammelte Abhandlungen. Bände I, II, III.* Ed. de J.-P. Serre. Springer-Verlag, Berlin-New York, 1968.

[FT61] Walter Feit i John G. Thompson. "Groups which have a faithful representation of degree less than $(p-1/2)$". A: *Pacific J. Math.* 11 (1961), pàg. 1257 - 1262. ISSN: 0030-8730,1945-5844. URL: http://projecteuclid.org/euclid.pjm/1103036911.

[Ful91] William Fulton. *Representation theory : a first course*. Ed. de Joe Harris. Springer-Verlag, 1991. ISBN: 0387975276.

[GAP] *GAP – Groups, Algorithms, and Programming, Version 4.12.2*. The GAP Group. URL: https://www.gap-system.org.

[Gor77] P Gordan. "Ueber endliche Gruppen linearer Transformationen einer Veränderlichen". A: *Math. Ann.* 12 (1 1877), pàg. 23 - 46. ISSN: 0025-5831,1432-1807. DOI: 10.1007/BF01442466. URL: https://doi.org/10.1007/BF01442466.

[Har19] Takeshi Harui. "Automorphism groups of smooth plane curves". A: *Kodai Mathematical Journal* 42.2 (2019), pàg. 308 - 331. DOI: 10.2996/kmj/1562032832. URL: https://doi.org/10.2996/kmj/1562032832.

[Hay63] Seymour Hayden. *ON FINITE LINEAR GROUPS WHOSE ORDER CONTAINS A PRIME LARGER THAN THE DEGREE*. Thesis (Ph.D.)–Harvard University. ProQuest LLC, Ann Arbor, MI, 1963. URL: http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqdiss&rft_dat=xri:pqdiss:0203779.

[Hof92] P. N. (Peter Norman) Hoffman. *Projective representations of the symmetric groups : Q-functions and shifted tableaux*. Ed. de J. F. Humphreys. Clarendon Press, 1992. ISBN: 0198535562.

[Hug05] Bonnie Sakura Huggins. *Fields of moduli and fields of definition of curves*. Thesis (Ph.D.) – University of California, Berkeley. ProQuest LLC, Ann Arbor, MI, 2005, pàg. 156. ISBN: 978-0542-59793-0. URL: http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqdiss&rft_dat=xri:pqdiss:3210626.

[Jor78] M Camille Jordan. "Mémoire sur les équations différentielles linéaires à intégrale algébrique". A: *J. Reine Angew. Math.* 84 (1878), pàg. 89 - 215. ISSN: 0075-4102,1435-5345. DOI: 10.1515/crelle-1878-18788408. URL: https://doi.org/10.1515/crelle-1878-18788408.

[JS87] Gareth A Jones i David Singerman. "Introduction". A: Cambridge University Press, 1987.

[Kan+09] Ming-chang Kang et al. "Some primitive linear groups of prime degree". A: *J. Math. Soc. Japan* 61.4 (2009), pàg. 1013 - 1070. ISSN: 0025-5645,1881-1167. URL: http://projecteuclid.org/euclid.jmsj/1257520499.

[Kar85] Gregory Karpilovsky. *Projective representations of finite groups*. Marcel Dekker, 1985. ISBN: 0824773136.

[Kle05] A. S. (Aleksandr Sergeevich) Kleshchëv. *Linear and projective representations of symmetric groups / Alexander Kleshchev.* eng. Cambridge tracts in mathematics ; 163. Cambridge: Cambridge University Press, 2005. ISBN: 1-107-13981-3.

[Kle75] Felix Klein. "Ueber binäre Formen mit linearen Transformationen in sich selbst". A: *Math. Ann.* 9 (2 1875), pàg. 183 - 208. ISSN: 0025-5831,1432-1807. DOI: 10.1007/BF01443373. URL: https://doi.org/10.1007/BF01443373.

[Kro54] Léopold Kronecker. "Mémoire sur les facteurs irréductibles de l'expression $x^n - 1$". A: *Journal de mathématiques pures et appliquées 1re série* (19 1854), pàg. 177 - 192. URL: http://www.numdam.org/item?id=JMPA_1854_1_19__177_0.

[Lin71] J. H. Lindsey II. "Finite linear groups of degree six". A: *Canadian J. Math.* 23 (1971), pàg. 771 - 790. ISSN: 0008-414X,1496-4279. DOI: 10.4153/CJM-1971-086-x. URL: https://doi.org/10.4153/CJM-1971-086-x.

[LS74] Vicente Landazuri i Gary M. Seitz. "On the minimal degrees of projective representations of the finite Chevalley groups". A: *J. Algebra* 32 (1974), pàg. 418 - 443. ISSN: 0021-8693. DOI: 10.1016/0021-8693(74)90150-1. URL: https://doi.org/10.1016/0021-8693(74)90150-1.

[LL00] T. Y. Lam i K. H. Leung. "On vanishing sums of roots of unity". A: *Journal of Algebra* 224 (1 febr. de 2000), pàg. 91 - 109. ISSN: 00218693. DOI: 10.1006/jabr.1999.8089.

[McK13] James McKernan. *Conjugation in Sn.* 2013. URL: https://math.mit.edu/~mckernan/Teaching/12-13/Spring/18.703/l_6.pdf.

[Men17] Eduardo Monteiro Mendonca. *PROJECTIVE REPRESENTATIONS OF GROUPS.* 2017. URL: https://alistairsavage.ca/pubs/Mendonca-Projective_Representation_of_Groups.pdf.

[Per] Alexandersson Per. *The symmetric functions catalog: Schur polynomials.* Online. Última modificació: 20-03-2024. URL: https://www.symmetricfunctions.com/schur.htm.

[Sch04] J Schur. "Über die Darstellung der endlichen Gruppen durch gebrochen lineare Substitutionen". A: *J. Reine Angew. Math.* 127 (1904), pàg. 20 - 50. ISSN: 0075-4102,1435-5345. DOI: 10.1515/crll.1904.127.20. URL: https://doi.org/10.1515/crll.1904.127.20.

[Sch07] J Schur. "Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen". A: *J. Reine Angew. Math.* 132 (1907), pàg. 85 - 137. ISSN: 0075-4102,1435-5345. DOI: 10.1515/crll.1907.132.85. URL: https://doi.org/10.1515/crll.1907.132.85.

[Sch11] J Schur. "Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen". A: *J. Reine Angew. Math.* 139 (1911), pàg. 155 - 250. ISSN: 0075-4102,1435-5345. DOI: 10.1515/crll.1911.139.155. URL: https://doi.org/10.1515/crll.1911.139.155.

[Ser77] Jean-Pierre Serre. *Linear Representations of Finite Groups.* Vol. 42. Springer New York, 1977. ISBN: 978-1-4684-9460-0. DOI: 10.1007/978-1-4684-9458-7.

[SZ93] Gary M. Seitz i Alexander E. Zalesskii. "On the minimal degrees of projective representations of the finite Chevalley groups. II". A: *J. Algebra* 158.1 (1993), pàg. 233 - 243. ISSN: 0021-8693,1090-266X. DOI: 10.1006/jabr.1993.1132. URL: https://doi.org/10.1006/jabr.1993.1132.

[Tua44] Hsio-Fu Tuan. "On groups whose orders contain a prime number to the first power". A: *Ann. of Math. (2)* 45 (1944), pàg. 110 - 140. ISSN: 0003-486X. DOI: 10.2307/1969079. URL: https://doi.org/10.2307/1969079.

[Val89] H Valentiner. *The theory of finite transformation groups. With a summary in French.* Danish. Kjób. Skrift. (6) V. 64-235. 1889.

[Wal69] David B. Wales. “Finite linear groups of prime degree”. A: *Canadian J. Math.* 21 (1969), pàg. 1025 - 1041. ISSN: 0008-414X,1496-4279. DOI: 10.4153/CJM-1969-114-0. URL: https://doi.org/10.4153/CJM-1969-114-0.

[Wal70] David B Wales. “Finite linear groups of degree seven. II”. A: *Pacific J. Math.* 34 (1970), pàg. 207 - 235. ISSN: 0030-8730,1945-5844. URL: http://projecteuclid.org/euclid.pjm/1102976652.

[Wik24] Wikipedia contributors. *List of finite simple groups — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=List_of_finite_simple_groups&oldid=1207998351. [Online; accessed 28-March-2024]. 2024.

[Wil+22] R. A. Wilson et al. *AtlasRep, A GAP Interface to the Atlas of Group Representations, Version 2.1.6*. https://www.math.rwth-aachen.de/~Thomas.Breuer/atlasrep. Refereed GAP package. Oct. de 2022.