Values of characters and orders of elements

Juan Martínez Madrid
supervised by
Alexander Moretó Quintana

This dissertation is submitted for the degree of International Doctor in Mathematics

Facultat de Ciències Matemàtiques

Programa de Doctorat en Matemàtiques

April, 2025

A mi familia

Contents

Resumen xv
Guión de la tesis xxv

Acknowledgements xxvii

Introduction xxix
Structure of the work xxxviii

Chapter 1. Preliminaries on group theory 1
1.1. Simple groups 1
1.2. Sylow and Hall Theory, solvability and nilpotency 3
1.3. Some special subgroups 6

Chapter 2. Character theory 9
2.1. Definitions and basics 9
2.2. Induction and restriction of characters 11
2.3. Factor groups 12
2.4. Normal subgroups 12
2.5. Fields of values 14
2.6. Rational classes and characters 19
2.7. Modular representations 21

Chapter 3. Fields of values of characters 23
3.1. Introduction 23
3.2. Bounding the size of the group 24
3.3. Proof of Theorem B 32
3.4. Proof of Theorem C 48
3.5. Further questions 54

Chapter 4. Commuting probability and average character degree 57
4.1. Introduction 57
4.2. Preliminary results on commuting probability 62
4.3. Nilpotent groups of odd order 66
4.4. Supersolvable groups of odd order 68
4.5. Average character degree 70
4.6. Number-theoretical questions 74

Chapter 5. Proportion of classes of π-elements 77

5.1. Introduction 77
5.2. Reducing to simple groups 79
5.3. Simple groups 84
5.4. Examples and open problems 94

Chapter 6. Commuting probability of π-elements 97
6.1. Introduction 97
6.2. Preliminary results 98
6.3. Proof of Theorem I 101
6.4. Results on $\Pr_\pi(G)$ 113
6.5. Open problems 115

Appendix A: Graphs, coverings and characters 117
A.1. Coverings and graph theory 117
A.2. Redundant Sylows and picky elements 121
A.3. Subnormalizers 125
A.4. Picky and Subnormalizer Conjectures 127
A.5. Picky and Subnormalizer Conjectures in simple groups 129

Bibliography 131

Declaro que esta disertación titulada *values of characters and orders of elements* y el trabajo presentado en ella son míos. Lo confirmo:

- Este trabajo se realizó total o principalmente mientras se cursaban los estudios para la obtención del título de Doctor en la Universidad de Valencia.
- Cuando se han consultado las publicaciones de otras personas, siempre se ha indicado claramente.
- Donde se han citado los trabajos de otras personas, siempre se ha dado la fuente de tales publicaciones. Con la excepción de tales citas, esta disertación es completamente trabajo propio.
- Han sido reconocidas todas las fuentes de ayuda.

Burjassot, 10 de abril del 2025

Juan Martínez Madrid

Declaro que esta disertación presentada por **Juan Martínez Madrid** titulada *Values of characters and orders of elements* se ha realizado bajo mi supervisión en la Universitat de València. También indico que este trabajo corresponde al proyecto de tesis aprobado por esta institución y cumple todos los requisitos para obtener el título de Doctor en Matemáticas.

Burjassot, 10 de abril del 2025

Alexander Moretó Quintana

Esta memoria ha sido redactada en el Departament de Matemàtiques de la Universitat de València durante el periodo de disfrute de un Contrato Predoctoral CIACIF/2021/228 dentro del programa I+D+I de la Generalitat Valenciana.

Esta investigación ha sido parcialmente financiada por los proyectos: Ministerio de Ciencia e Innovación PID2019-103854GB-I00 y PID2022-137612NB-I00 (financiado por MCIN/AEI/10.13039/501100011033 y "ERDF A way of making Europe") y Generalitat Valenciana CIAICO/2021/163.

Resumen

Todos los grupos considerados en este trabajo serán finitos salvo que se indique lo contrario. Los principales resultados de esta tesis se enuncian en la introducción de los capítulos del 3 al 6 y aparecen como Theoremas del A al Theorem J. Estos resultados pueden encontrarse los artículos [**51, 79, 80, 81, 84**], los cuales han sido publicados, con la excepción de [**84**], el cual, se encuentra aún en preparación. A continuación, presentamos los temas de estudio de esta tesis:

(I) Los cuerpos de valores de clases (de conjugación) y de caracteres.

(II) La *commuting probability* y otros invariantes relacionados.

(III) Las conexiones entre los recubrimientos de grupos, la teoría de grafos y la teoría de la representación.

Comenzamos introduciendo los resultados en el primer bloque, que aparecen Capítulo 3. Antes de exponer los resultados correspondientes a este bloque, introducimos algumos resultados previos que ayudarán a contextualizar los problemas que se estudiarán en este bloque. El Problema 1 de la famosa lista de problemas de Brauer [**12**] es la clasificación de las álgebras de grupos finitos sobre los números complejos, salvo isomorfismo. Sea G un grupo y sean $\{\chi_1, \ldots, \chi_k\}$ el conjunto de caracteres irreducibles de G. Definimos la secuencia de grados de G como el multiconjunto $\{\chi_1(1), \ldots, \chi_k(1)\}$. Por el Teorema de Wedderburn tenemos que

$$\mathbb{C}G \cong \bigoplus_{i=1}^{k} M_{\chi_i(1)}(\mathbb{C}).$$

Por lo tanto, el Problema 1 de Brauer es equivalente a clasificar todos las posibles secuencias de grados de grupos finitos.

Aunque la clasificación completa de todas las posibles secuencias de grados parece imposible de obtener, existen algunas restricciones sobre las secuencias de grados de un grupo. Por ejemplo, si $\{n_1, \ldots, n_f\}$ es la secuencia de grados de un grupo G, entonces el número de 1's en esta secuencia es $|G : G'|$, que divide $|G| = \sum_{i=1}^{f} n_i^2$. Además, tenemos que cada n_i es el grado de un carácter irreducible de G y por lo tanto debe dividir a $\sum_{i=1}^{f} n_i^2$.

Estamos interesados en resultados menos triviales sobre las secuencias de grados. Un resultado clásico de Landau [**62**] afirma que $|G|$ está acotado en función de

$k(G) = |\mathrm{Cl}(G)|$, donde $\mathrm{Cl}(G)$ denota el conjunto de clases de conjugación en G. Equivalentemente, para cualquier entero $n \geqslant 1$ existe una cantidad finita de grupos con exactamente n clases de conjugación. Desde el punto de vista del Problema 1 de Brauer, el Teorema de Landau afirma que existe una cantidad finita de secuencias de grado de una longitud dada.

Sea G un grupo. En 2007, Moretó [**86**] definió el invariante $m(G)$ como

$$m(G) = \max_{d \in \mathbb{N}} |\{\chi \in \mathrm{Irr}(G) \mid \chi(1) = d\}|.$$

Es decir, $m(G)$ es el número máximo de caracteres con el mismo grado. Se conjeturó [**86**, Conjecture A] que $|G|$ está acotado en función de $m(G)$. Por [**86**, Theorem A], esta conjetura es cierta si y solo si es cierta para los grupos simétricos. Finalmente, Craven [**25**, Theorem 1.2] demostró que la conjetura es cierta resolviendo el caso simétrico.

Por lo tanto, $|G|$ está acotado en función de $m(G)$. Observamos que esto significa que, para cualquier $k \geqslant 1$, existe una cantidad finita de secuencias de grados con a lo sumo k componentes con el mismo grado. En general, $m(G)$ es mucho menor que $k(G)$. Así pues, se trata de una forma generalizada del Teorema de Landau.

No es completamente trivial ver que $m(G) = 1$ si y solo si $G = 1$ (véase [**82**, Theorem 2.3]). Moretó sugirió al autor las siguientes conjeturas.

Conjetura. *Sea $\mathbb{B}$ el Baby Monster Group. Si G es un grupo con $m(G) = 2$, entonces $|G| \leqslant |\mathbb{B}|$.*

Conjetura. *Sea $\mathbb{M}$ el Monster Group. Si G es un grupo con $m(G) = 3$, entonces $|G| \leqslant |\mathbb{M}|$.*

La primera de estas conjeturas fue demostrada por el autor de esta tesis en [**82**, Theorem A]. De hecho, la prueba de esta conjetura fue una consecuencia de [**82**, Theorem B], que clasifica todos los grupos con $m(G) = 2$. La segunda conjetura sigue abierta. Decidimos excluir estos resultados de esta tesis porque sus pruebas dependen de cálculos informáticos complejos.

Hay muchos resultados que generalizan el Teorema de Landau reemplazando $k(G)$ por un invariante más pequeño. Dado un grupo G, escribimos $k_{pp}(G)$ para denotar el número de clases de conjugación de elementos de orden potencia primo en G. Héthelyi y Külshammer [**48**] demostraron que $|G|$ está acotado en función de $k_{pp}(G)$. Mientras que la demostración del Teorema de Landau es elemental, la demostración del Teorema de Héthelyi–Külshammer depende de la clasificación de los grupos simples finitos (en lo que sigue, la *CFSG*).

En el caso de los grupos simples, se pueden probar resultados mas fuertes. Sea S un grupo simple no abeliano y sea p un primo divisor de $|S|$. Definimos $m_p(S)$ como el número de órbitas de $\mathrm{Aut}(S)$ actuando en el conjunto de p-elementos de

S. También definimos $L(S)$ como el mayor $m_p(S)$ entre todos los primos p que dividen a $|S|$. Recientemente, Giudici, Morgan y Praeger [**36**] han demostrado que $|S|$ está acotado en función de $L(S)$ para un grupo simple S. Observamos que los invariantes $m_p(S)$ fueron estudiados previamente en [**95**].

En este primer bloque de contenidos de la tesis, buscamos demostrar versiones del Teorema de Landau que involucren los cuerpos de valores. Para ello, introducimos algunos conceptos nuevos.

Dado un caracter χ de G, defininmos el cuerpo de valores de χ como el cuerpo generado por los valores de $\chi(K)$, donde K recorre $\mathrm{Cl}(G)$. Denotamos este subcuerpo de $\mathbb{C}$ por

$$\mathbb{Q}(\chi) = \mathbb{Q}(\chi(K) \mid K \in \mathrm{Cl}(G)).$$

Es bien sabido que existe una dualdidad entre caracteres irreducibles y clases de conjugación de un grupo. Con esto, nos referimos al hecho de que la mayoría de conceptos y resultados sobre caracteres irreducibles tienen una versión equivalente para clases de conjugación, y *vice versa*. En este caso, existe una definición dual para el cuerpo de valores de una clase de conjugación. Dado $K \in \mathrm{Cl}(G)$, definimos el cuerpo de valores de K como la extensión de $\mathbb{Q}$ generada por los valores $\chi(K)$, donde χ recorre $\mathrm{Irr}(G)$. Esto es

$$\mathbb{Q}(K) = \mathbb{Q}(\chi(K) \mid \chi \in \mathrm{Irr}(G)).$$

Por último, definimos el cuerpo de valores de G como el cuerpo generado por los valores $\chi(K)$, donde χ recorre $\mathrm{Irr}(G)$ y K recorre $\mathrm{Cl}(G)$. Esto es

$$\mathbb{Q}(G) = \mathbb{Q}(\chi(K) \mid \chi \in \mathrm{Irr}(G), K \in \mathrm{Cl}(G)).$$

Actualmente, el estudio de los cuerpos de valores es un área de investigación muy importante en la teoría de caracteres. Antes de continuar, resulta conveniente hacer un breve resumen de los resultados obtenidos en este área. Dado un grupo G, escribimos $\pi(G)$ para denotar el conjunto de divisores primos de $|G|$. En el caso de grupos resolubles, es posible acotar los divisores primos de $|G|$ en función de los cuerpos de valores del grupo. Un resultado clásico de Gow [**39**] prueba que $\pi(G) \subseteq \{2, 3, 5\}$ para cualquier grupo resoluble G con $\mathbb{Q}(G) = \mathbb{Q}$. Chillag y Dolfi [**23**, Theorem 2] demostraron que si G es un grupo resoluble de forma que $\mathbb{Q}(K)$ es $\mathbb{Q}$ o una extensión cuadrática de $\mathbb{Q}$ para cada $K \in \mathrm{Cl}(G)$, entonces $\pi(G) \subseteq \{2, 3, 5, 7, 13, 17\}$. A día de hoy, no se sabe si 17 puede aparecer realmente como un divisor primo de un grupo que satisfaga esta propiedad. Además, Tent [**120**, Theorem A] demostró una versión análoga para caracteres. Más concretamente, él demostró que si G es un grupo resoluble que satisface que $\mathbb{Q}(\chi)$ es $\mathbb{Q}$ o una extensión cuadrática de $\mathbb{Q}$ para cada $\chi \in \mathrm{Irr}(G)$, entonces $\pi(G) \subseteq \{2, 3, 5, 7, 13\}$.

De manera más general, [**120**, Theorem C] prueba que si G es un grupo resoluble que satisface que $|\mathbb{Q}(\chi) : \mathbb{Q}| \leqslant k$ para cualquier $\chi \in \mathrm{Irr}(G)$, entonces $|\pi(G)|$ está

acotado en función de k. Chillag y Dolfi [**23**, Problem 2] preguntaron si la versión dual para clases es cierta.

En 2021, Moretó [**88**] definió el invariante $f(G)$ como la mayor multiplicidad con la que un cuerpo puede aparecer como cuerpo de valores de un caracter irreducible. Esto es

$$f(G) = \max_{F/\mathbb{Q}} |\{\chi \in \mathrm{Irr}(G) \mid \mathbb{Q}(\chi) = F\}|.$$

donde el máximo se considera sobre todas las extensiones $F/\mathbb{Q}$. Utilizando este invariante, Moretó [**88**, Theorem A] demostró que $|G|$ está acotado en función de $f(G)$. Esto es de nuevo una forma generalizada del Teorema de Landau. Además, se trata de una forma alternativa a la cota de $|G|$ en función de $m(G)$. Sin embargo, en lugar de considerar multiplicidades de grados de caracteres, consideramos multiplicidades de cuerpos de valores.

Por otra parte, Moretó [**88**] también demostró que $f(G) = 1$ si y solo si $G = 1$. En el mismo trabajo, Moretó también preguntó por la clasificación de todos los grupos con $f(G) \in \{2, 3\}$. En esta tesis proporcionamos dicha clasificación. Esta clasificación constituye el Teorema B de esta tesis, el cual ha sido publicado en [**79**].

Es natural considerar las versiones duales con clases de conjugación. Dado G un grupo, definimos el invariante $h(G)$ como

$$h(G) = \max_{F/\mathbb{Q}} |\{K \in \mathrm{Cl}(G) \mid \mathbb{Q}(K) = F\}|.$$

El mayor problema del invariante $h(G)$ es que no se comporta bien con respecto a cocientes. No es difícil ver que $f(G/N) \leqslant f(G)$ para cualquier subgrupo normal N de G. Sin embargo, no ocurre lo mismo con $h(G)$. Existen ejemplos de grupos que tienen un subgrupo normal N con $h(G/N) > h(G)$ (véase la introducción de la Sección 3.1). Para evitar este problema, introducimos un invariante ligeramente más fuerte. Definimos $\hat{h}(G)$ como

$$\hat{h}(G) = \max_{N \trianglelefteqslant G} \{h(G/N)\}.$$

Por definición del invariante $\hat{h}(G)$, tenemos que $h(G) \leqslant \hat{h}(G)$ y que $\hat{h}(G) \geqslant \hat{h}(G/N)$ para cualquier $N \trianglelefteqslant G$.

En un trabajo conjunto con Vergani [**84**], hemos demostrado que $|G|$ está acotado en función de $\hat{h}(G)$ para cualquier grupo G. Cabe mencionar que la prueba de este resultado utiliza el resultado anteriormente mencionado de Giudici et al. [**36**]. Para acotar $|G|$ en función de $\hat{h}(G)$, bastará con acotar $|\pi(G)|$ en función de $\hat{h}(G)$. Para ello utilizaremos las técnicas introducidas en [**29**]. El resultado que acota $|G|$ en función de $\hat{h}(G)$ constituye el Teorema A de esta tesis y se publicará en [**84**].

Inspeccionando los grupos que aparecen en la clasificación proporcionada por el Teorema B, deducimos que si $f(G) \in \{1, 2, 3\}$, entonces $h(G) = f(G)$. Por tanto, es natural preguntarse si el recíproco es cierto, es decir, si $f(G) = h(G)$ para todos los grupos con $h(G) \leqslant 3$. Nuestro siguiente resultado responde afirmativamente a esta pregunta. Este resultado es el Teorema C y se publicará también en [**84**].

A continuación, presentamos los resultados sobre el segundo bloque de contenidos de esta tesis. Los resultados correspondientes a este bloque se desarrollarán en los Capítulos 4, 5 to 6. A fin de exponer estos contenidos, empezamos por introducir la *commuting probability*.

Definimos la *commuting probability* de un grupo G como la probabilidad de que dos elementos, aleatoriamente elegidos, de G conmuten y la denotaremos por $\Pr(G)$. Esto es

$$\Pr(G) = \frac{|\{(x, y) \in G \times G \mid xy = yx\}|}{|G|^2}.$$

Observamos que la *commuting probability* puede definirse también para grupos no finitos (véase, por ejemplo, [**122**] o la Sección 2 de [**42**]). Sin embargo, en este trabajo solo estudiaremos el caso finito.

Nuestro objetivo en este segundo bloque es utilizar la *commuting probability* y otros invariantes relacionados para estudiar la estructura de los grupos y para obtener resultados *local-global*. Por resultados *local-global*, entendemos cualquier resultado que determine la estructura de un p-subgrupo de Sylow o un π-subgrupo de Hall en función de invariantes definidos sobre todo el grupo. En los últimos años, se han producido imporatantes avances en el estudio de conjeturas *local-global*. Por ejemplo, una de las conjeturas *local-global* mas famosas es la *Brauer's Height Zero Conjecture*, la cual fue establecida en 1955 por Brauer [**11**]. Tras muchos esfuerzos, la *Brauer's Height Zero Conjecture* fue finalmente resuelta por Malle, Navarro, Schaefer Fry and Tiep [**73**]. Procedemos a introducir los resultados correspondiente a este segundo bloque.

En 1973, Gustafson [**42**] demostró que si $\Pr(G)$ es mayor que $5/8$, entonces G es abeliano. La demostración de este resultado es muy corta y ademas es completamente elemental. Ademas, la cota $5/8$ no puede ser mejorada. Cabe mencionar que un resultado más general era ya conocido. Más concretamente, Joseph [**58**] probó un resultado mas general reemplazando la cota $5/8$ por $(p^2 + p - 1)/p^3$, donde p es el menor primo que divide a $|G|$. En la Sección 3 de [**42**], Gustafson indica cómo obtener la cota $(p^2 + p - 1)/p^3$. Por esta razón, nos referiremos a este resultado como el Teorema de Gustafson–Joseph.

En 2023, Burness, Guralnick, Moretó y Navarro [16, Theorem A] demostraron que, dado un primo p y un grupo G, se cumple que si la probabilidad $\mathrm{Pr}_p(G)$ de que dos p-elementos G conmuten supera $(p^2+p-1)/p^3$, entonces G tiene un p-subgrupo de Sylow normal y abeliano (en cuyo caso, la probabilidad es 1). Este resultado es una versión local del Teorema de Gustafson–Joseph. Al contrario que la demostración del Teorema de Gustafson–Joseph, la demostración de [16, Theorem A] es compleja y depende de la *CFSG*.

Cabe recordar que el Teorema de Itô–Michler [57, 85] afirma que G tiene un p-subgrupo de Sylow normal y abeliano si y solo si p no divide el grado de ningún caracter irreducible de G. Así pues, [16, Theorem A] proporciona una condición para la existencia de un p-subgrupo de Sylow normal y abeliano que no está basada en la teoría de caracteres.

De hecho, [16, Theorem A] es una consecuencia directa de [16, Theorem C], que afirma que, para cualquier p-elemento fijo $x \in G \backslash \mathbf{O}_p(G)$, la proporción de p-elementos de G que conmutan con x es a lo sumo $1/p$. Por otra parte, [16, Theorem D] afirma que lo mismo ocurre para $x \in \mathbf{O}_p(G) \backslash \mathbf{Z}(\mathbf{O}_p(G))$. Observamos que

$$\frac{|\mathbf{C}_G(x)_p|}{|G_p|} = \frac{\Psi(x)}{\Psi(1)},$$

donde X_p denota el conjunto de p-elementos de un grupo X y Ψ denota el caracter de permutación de la acción de G sobre sus p-elementos por conjugación. En el lenguaje de los grupos de permutaciones, a esta proporción se la denomina el *fixed ponit ratio* con respecto a esta acción. Por esta razón, la demostración de [16, Theorem C] depende de los importantes resultados sobre los *fixed ponit ratios* demostrados en [15].

Se preguntó en [16] si era posible extender estos resultados a un conjunto general de primos π. En esta tesis, respondemos afirmativamente a esta pregunta. Sea π un conjunto de primos y sea p el menor primo en π. Demostramos que si x es un π-elemento de G con $x \in G \backslash \mathbf{O}_\pi$, entonces la proporción de π-elementos de G que conmutan con x es como máximo $1/p$. De este resultado deduciremos que si la probabilidad de que dos π-elementos de G conmuten es superior a $(p^2+p-1)/p^3$, entonces G posee un π-subgrupo de Hall normal y abeliano. Estos resultados son los Teoremas I y J del Capítulo 6 y aparecieron publicados en [80].

En segundo lugar, estudiamos un invariante local distinto. Gustafson [42] demostró que

$$\mathrm{Pr}(G) = \frac{k(G)}{|G|}.$$

Cabe destacar que esta identidad ya era conocida por Erdős y Turán [28, Theorem IV]. A partir de esta identidad es posible definir un invariante local que proporciona información sobre los π-elementos de un grupo. Sea π un conjunto de primos y sea $k_\pi(G)$ el número de clases de conjugación de π-elementos de un

grupo G. Hung y Maróti [**76**] definieron el invariante $\mathrm{d}_\pi(G)$ como

$$\mathrm{d}_\pi(G) = \frac{k_\pi(G)}{|G|_\pi}.$$

Este invariante es a lo sumo 1 por un resultado de Robinson (véase el Lema 5.10). Este invariante está fuertemente relacionado con $\Pr(G)$. Por ejemplo, si q es un primo en π y Q es un q-subgrupo de Sylow de G, entonces $\mathrm{d}_\pi(G) \leqslant \Pr(Q)$ (esto se observó en la introducción de [**76**]).

Hung y Maróti [**76**, Theorem 1] demostraron que si $\mathrm{d}_\pi(G)$ es mayor que $5/8$, entonces G posee π-subgrupos de Hall abelianos. Este resultado es una versión local del Teorema de Gustafson–Joseph diferente de [**16**, Theorem A]. Trabajando conjuntamente con Hung y Maróti [**51**], se ha ampliado [**76**, Theorem 1] sustituyendo la cota $5/8$ por $(p^2+p-1)/p^3$, donde p es el menor primo en π. Además, se ha demostrado que si $\mathrm{d}_\pi(G)$ supera $1/p$, entonces G tiene un π-subgrupo de Hall nilpotente (con clase de nilpotencia a lo sumo 2). Recordemos que, por un resultado clásico de Wielandt [**128**], tenemos que si G contiene un π-subgrupo de Hall nilpotente, entonces los π-subgrupos de Hall se comportan como subgrupos de Sylow. Estos resultados constituyen el Teorema H del Capítulo 5 y fueron publicados en [**51**].

Ahora, nos centramos en el estudio de la nilpotencia y la supersolubilidad de un grupo en función de su *commuting probability*. Lescot [**65**] demostró que si $\Pr(G)$ supera $1/2$, entonces G es nilpotente. Además, Guralnick y Robinson [**41**] mejoraron este resultado sustituyendo $1/2$ por $1/p$, donde p es el menor primo dividiendo $|G|$. No es difícil ver que la cota $1/p$ no es óptima para $p > 2$. Además, Barry, MacHale y Ni Shé [**5**] demostraron que si $\Pr(G)$ es mayor que $1/3$, entonces G es supersoluble. Observamos que este resultado fue ampliado y la prueba fue simplificada por Hung, Lescot y Yang [**67**].

Nuestros siguientes resultados determinan la mejor función posible $g_n(p)$ (respectivamente, $g_s(p)$) de modo que si $\Pr(G) > g_n(p)$ (resp. $\Pr(G) > g_s(p)$), donde p es el menor primo que divide a $|G|$, entonces G es nilpotente (resp. supersoluble). Las definiciones de las funciones $g_n(p)$ y $g_s(p)$ dependen de algunos conceptos de teoría de números y se pospondrán al Capítulo 4. Estos resultados son los Teoremas D y E del Capítulo 4 y aparecieron publicados en [**81**].

Por último, centramos nuestra atención en el estudio de otra variante de $\Pr(G)$. De acuerdo con [**56**], definimos el *average character degree* de G como la media aritmética de los grados de los caracteres irreducibles de G y escribiremos $\mathrm{acd}(G)$ para denotarlo. Es decir

$$\mathrm{acd}(G) = \frac{\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)}{|\,\mathrm{Irr}(G)|}.$$

Es bien sabido que $1/\Pr(G) \leqslant \mathrm{acd}(G)^2$ para todo grupo G (véase la introducción del Capítulo 4).

Como en el caso de $\Pr(G)$, hay muchos resultados que prueban que la estructura de G está más restringida a medida que $\operatorname{acd}(G)$ disminuye. Hung y Moretó [**92**] demostraron que si $\operatorname{acd}(G)$ es menor que $16/5$, entonces G es resoluble (esto había sido conjeturado en [**56**]). Isaacs, Loukaki y Moretó [**56**] demostraron que si $\operatorname{acd}(G)$ es menor que $4/3$, entonces G es nilpotente. En [**56**] también se demostró que si $\operatorname{acd}(G)$ es menor que $3p/(p+2)$, donde p es el menor primo que divide a $|G|$, entonces G es supersoluble.

Nuestros últimos resultados determinan las mejores cotas posibles $h_n(p)$ y $h_n(p)$ tales que si $\Pr(G) > h_n(p)$, donde p es el menor primo que divide a $|G|$, entonces G es nilpotente y si $\Pr(G) > h_s(p)$, entonces G es supersoluble. Como en el caso de nuestros resultados sobre la *commuting probability*, las definiciones de nuestras cotas dependen de resultados no triviales sobre teoría de números y se pospondrán al Capítulo 4. Estos resultados constituyen los Teoremas F y G del Capítulo 4 y aparecieron publicados en [**81**].

Por último, el tercer y último bloque de contenidos de esta tesis aparece en el Apéndice A. Se ha decidido exponer estos contenidos en un apéndice porque aún se está llevando a cabo mucho trabajo sobre ellos. Es de esperar que las cuestiones tratadas en este apéndice sean relevantes en el futuro.

Nuestro primer objetivo en el Apendice A es introducir el concepto de los elementos *picky*. El origen de este concepto es un trabajo conjunto con Maróti y Moretó [**77**], donde tratamos una variación de cuestiones clásicas sobre recubrimientos de grupos. Es bien sabido que la *commuting probability* tiene conexiones con la teoría de grafos y los recubrimientos de grupos. Sorprendentemente, también es cierto que los recubrimientos de grupos tienen conexiones con la teoría de la representación. Esto nos llevará a presentar y discutir la *Picky Conjecture*, la cual ha sido recientemente enunciada por Moretó and Rizo [**93**]. La *Picky Conjecture*, junto con algunas de sus generalizaciones, están siendo estudiadas por varios autores en diferentes trabajos [**13, 70, 83, 93, 119**], todavía en preparación.

El *non-commuting graph* de un grupo G es un grafo cuyos vértices son los elementos no centrales de G y dos elementos están conectados si no conmutan. Observamos que $1-\Pr(G)$ es igual a la densidad de aristas en el *non-commuting graph*. Además, el número *clique* de este grafo coincide con el tamaño del conjunto más grande de elementos de G cuyos elementos no conmutan dos a dos. A este número se le suele denotar por $n(G)$. Aplicando el Teorema de Turán [**125**], se deduce que

$$\frac{1}{\Pr(G)} \leqslant n(G).$$

Esta desigualdad muestra cómo la teoría de grafos puede ayudar a relacionar conceptos dentro de la teoría de grupos.

El *non-commuting graph* también puede estudiarse desde el punto de vista de los recubrimientos de grupos. En 1926, Scorza [**114**] demostró que un grupo no puede ser expresado como la unión de 2 subgrupos propios. La demostración de este resultado es completamente elemental. Esto motivó la definición de número de recubrimiento de un grupo. Dado un grupo G, decimos que el número de recubrimiento de G es d, y escribiremos $\sigma(G) = d$, si G puede expresarse como la unión de d subgrupos propios pero no puede expresarse como la unión de $d-1$ subgrupos propios. Observamos que si $\sigma(G) = d$ y $x_1, \dots, x_d \in G \backslash \mathbf{Z}(G)$, entonces $G \neq \mathbf{C}_G(x_1) \cup \cdots \cup \mathbf{C}_G(x_d)$ y por lo tanto $x_1, \dots, x_d$ tienen un vértice vecino común en el *non-commuting graph*.

Inspirándose en el número de recubrimiento, Maróti, Moretó y el autor de esta tesis [**78**] introdujeron el número de p-recubrimiento. Sea p un primo y sea G un grupo. Definimos el número de p-recubrimiento, y lo denotamos por $\sigma_p(G)$, como el número mínimo de subgrupos propios cuya unión contiene al conjunto de p-elementos de G. Por [**78**, Theorem A], tenemos que $\sigma_p(G) \geqslant \sigma(G) - 1$ para G, un grupo resoluble y generado por sus p-elementos. Además, $\sigma_p(G) = \sigma(G) - 1$ si y solo si G no es un p-grupo. Eso sugiere que $\sigma_p(G)$ debe comportarse como $\sigma(G)$ para grupos generados por sus p-elementos.

La primera pregunta natural que se plantea es si existe una versión del Teorema de Scorza para $\sigma_p(G)$. En [**78**] se conjeturó que $\sigma_p(G) > p$ para grupos generados por sus p-elementos. El caso p-resoluble de esa conjetura se demostró en [**78**, Theorem B], pero la versión general fue demostrada por Guralnick [**40**, Theorem F]. Observamos que la demostración Guralnick no depende de la *CFSG*.

Sea G un grupo generado por sus p-elementos y sean $x_1, \dots, x_p \in G_p$ elementos no centrales. Entonces $G_p \nsubseteq \mathbf{C}_G(x_1) \cup \cdots \cup \mathbf{C}_G(x_p)$ por [**40**, Theorem F]. Por tanto, existe $y \in G_p$ de manera que y está conectado a $x_1, \dots, x_p$ en el *non-commuting graph* de G. Como consecuencia, el subgrafo inducido por el *non-commuting graph* de G en $G_p \backslash \mathbf{Z}(G)_p$ es conexo y tiene diametro acotado por 2.

Esto motiva la definición de los p-subgrupo de Sylow redundante. De acuerdo con [**77**], decimos que un grupo tiene un p-subgrupos de Sylow redundante si el conjunto de p-elementos de G se puede expresar como la unión de $|\mathrm{Syl}_p(G)| - 1$ p-subgrupos de Sylow. No es difícil ver que G no posee ningún p-subgrupo de Sylow redundante si y solo si existen p-elementos que se encuentran en un único p-subgrupo de Sylow (véase el Lema A.11). Llamaremos elementos *picky* a cualquier elemento satisfaciendo esta propiedad. Se observó en [**77**, Corollary 2.5], que los elementos *picky* tienen buenas propiedades desde el punto de vista de la teoría de caracteres. Recientemente, Moretó y Rizo [**93**] observaron que

esta conexión es más profunda de lo que cabría esperar. Pra poder explicar esta conexión, necesitamos introducir algo de contexto.

Dado un grupo G y un primo p, denotamos

$$\mathrm{Irr}_{p'}(G) = \{\chi \in \mathrm{Irr}(G) \mid \gcd(p, \chi(1)) = 1\}.$$

Ademas de la anteriormente mencionada *Brauer's Height Zero Conjecture*, una de las conjeturas *local-global* más famosas es la *McKay Conjecture*, la cual afirma que

$$|\mathrm{Irr}_{p'}(G)| = |\mathrm{Irr}_{p'}(\mathbf{N}_G(P))|$$

para cualquier $P \in \mathrm{Syl}_p(G)$. Tras muchos esfuerzos, esta conjetura fue finalmente demostrada por Cabanes y Späth [**17**]. Recordamos que el caso $p = 2$ había sido demostrado previamente por Malle y Späth [**74**].

Dado $x \in G$, escribimos $\mathrm{Irr}^x(G)$ para denotar el conjunto de caracteres irreducibles de G que no se anulan en x. Esto es

$$\mathrm{Irr}^x(G) = \{\chi \in \mathrm{Irr}(G) \mid \chi(x) \neq 0\}.$$

Supongamos que $x \in$ es un elemento *picky* y que $P \in \mathrm{Syl}_p(G)$ es el único p-subgrupo de Sylow conteniendo a x. Moretó y Rizo han propuesto varias conjeturas local-global que involucran conexiones profundas entre $\mathrm{Irr}^x(G)$ y $\mathrm{Irr}^x(\mathbf{N}_G(P))$ y los valores de estos caracteres en x. Enunciamos la más básica de estas conjeturas.

Conjetura (*Picky Conjecture*). *Sea p un primo, sea G un grupo y sea $P \in \mathrm{Syl}_p(G)$. Supongamos que $x \in P$ es un elemento picky. Entonces existe una biyección*

$$\Gamma : \mathrm{Irr}^x(G) \to \mathrm{Irr}^x(\mathbf{N}_G(P))$$

que satisface las siguientes propiedades.

(I) $\Gamma(\chi)(1)_p = \chi(1)_p$ para todo $\chi \in \mathrm{Irr}^x(G)$.

(II) $\mathbb{Q}(\Gamma(\chi)(x)) = \mathbb{Q}(\chi(x))$ para todo $\chi \in \mathrm{Irr}^x(G)$.

También observaron que, en la mayoría de los casos, existe una biyección que satisface que $\Gamma(\chi)(x) = \pm\chi(x)$ para todo $\chi \in \mathrm{Irr}^x(G)$. Dado $x \in G$ un p-elemento *picky*, decimos que la *Strong Picky Conjecture* se cumple para (G, x) si existe una biyección Γ que satisfaciendo esta condición

Observamos que si $\chi \in \mathrm{Irr}_{p'}(G)$ y $x \in G_p$, entonces $\chi(x) \neq 0$, por [**99**, Corollary 4.20]. Por lo tanto, $\mathrm{Irr}_{p'}(G) \subseteq \mathrm{Irr}^x(G)$. De esto deducimos que, si $x \in G$ es p-elemento *picky* y la *Picky Conjecture* se cumple para (G, x), entonces la *McKay Conjecture* se cumple para G.

La *Picky Conjecture*, junto con varias generalizaciones, se presentarán en el Apéndice A. Discutiremos brevemente algunos de los avances que se han efectuado sobre estas conjeturas. Probablemente, la demostración de estas conjeturas para un grupo arbitrario requerirá del desarrollo de técnicas aún desconocidas.

Guión de la tesis

Este trabajo se divide en seis capítulos y un apéndice.

El Capítulo 1 contiene los resultados básicos sobre teoría de grupos que utilizaremos durante el resto del trabajo.

El Capítulo 2 introduce la teoría de la representación y la teoría de caracteres. En la Sección 2.5 introduciremos los resultados clásicos sobre los cuerpos de valores de clases y caracteres. Por último, en la Sección 2.6 presentamos los resultados de Navarro y Tiep [**100**] y Rossi [**110**] sobre grupos con, a lo sumo, 3 clases racionales, o 3 caracteres irreducibles y racionales.

En el Capítulo 3 demostramos los resultados sobre cuerpos de valores de clases y caracteres. En la Sección 3.2 demostraremos los resultados que acotan el tamaño de un grupo en función de $\hat{h}(G)$. Comenzaremos demostrando que, dado un grupo G, el orden de G está acotado en función de $|\pi(G)|$ y de $h(G)$. A continuación, utilizaremos las herramientas desarrolladas por Farias e Soares [**29**], junto con el resultado antes mencionado de Giudici et al. [**36**] para acotar $|\pi(G)|$ en función de $\hat{h}(G)$.

La clasificación de los grupos con $f(G) \leqslant 3$ se demuestra en la Sección 3.3 Estudiaremos el caso resoluble y el caso no resoluble por separado. En primer lugar, clasificaremos los grupos no resolubles con $f(G) \leqslant 3$. Es fácil ver que estos grupos tienen como máximo 3 caracteres racionales. Esto permitirá utilizar los resultados antes mencionados de Navarro, Rossi y Tiep. Una vez demostrado el caso no resoluble, probaremos el caso resoluble de la clasificación. Empezaremos clasificando los grupos metabelianos con $f(G) \leqslant 3$ y luego probaremos que cualquier grupo resoluble con $f(G) \leqslant 3$ es metabeliano.

En la Sección 3.4 demostramos que $f(G) = h(G)$ para cualquier grupo G con $h(G) \leqslant 3$. Todos los grupos con $h(G) \leqslant 3$. tendrán como máximo 3 clases de conjugación racionales y, por tanto, aplicaremos de nuevo los resultados de Navarro, Rossi y Tiep para deducir que el número de caracteres racionales es igual al número de caracteres racionales en estos grupos. Esta igualdad, junto con una cuidadosa aplicación de un resultado clásico de Brauer [**53**, Theorem 6.32], demostrarán la igualdad $f(G) = h(G)$. Finalmente, la Sección 3.5 contiene algunas cuestiones abiertas sobre cuerpos de valores de clases y caracteres.

En el Capítulo 4 demostramos los resultados sobre la nilpotencia y la supersolubilidad en términos de la *commuting probability* y el *average character degree*. En las Secciones 4.3 y 4.4 probamos los resultados que determinan la nilpotencia y la supersolubilidad en términos de $\Pr(G)$. En cada caso, demostraremos que, para obtener la mejor cota posible, basta con estudiar una determinada familia de grupos. Después, estableceremos la cota en la familia correspondiente y encontraremos un grupo en esa familia que la alcance. Nuestros resultados sobre el *average character degree* se demostrarán en la Sección 4.5. Utilizaremos las

técnicas introducidas por Isaacs, Loukaki y Moretó [**56**] para establecer las cotas y luego encontraremos grupos en los que se alcanzan dichas cotas. La Sección 4.6 contiene los resultados y la discusión sobre la teoría de números de esta tesis. Como hemos mencionado anteriormente, las definiciones de las cotas para $\Pr(G)$ y $\operatorname{acd}(G)$ dependen de funciones no explícitas, las cuales dependen de los números primos. En el caso de las funciones para $\operatorname{acd}(G)$, la definición de las cotas depende de la existencia de números que satisfagan algunas condiciones específicas. En la Sección 4.6, demostraremos la existencia de tales números. Además, también discutiremos la forma de las cotas utilizadas en los resultados sobre $\Pr(G)$.

El Capítulo 5 contiene los resultados sobre $\mathrm{d}_\pi(G)$. Sea π un conjunto de primos y sea p ele menor primo en π. Comenzaremos demostrando que la cota $(p^2+p-1)/p^3$ para la conmutatividad de los π-subgrupos de Hall se deduce "fácilmente" del límite $1/p$ para la nilpotencia. A continuación, reduciremos la demostración de la cota $1/p$ a una cuestión sobre grupos simples finitos. Finalmente, esta cuestión se resolverá utilizando la *CFSG* y estudiando cada caso por separado.

El caso alternado se demostrará mediante un argumento elemental, y el caso esporádico se demostrará examinando la información proporcionada por el *ATLAS* [**24**]. Para grupos de tipo Lie en característica s, estudiaremos por separado el caso en que $s \in \pi$ y el caso en que $s \notin \pi$. Si $s \in \pi$, entonces el resultado se seguirá por los resultados en [**31**], mientras que el resultado se seguirá de [**72**, Theorem 3.15] para $s \notin \pi$.

En el Capítulo 6 demostramos los resultados sobre la probabilidad de que dos π-elementos conmuten. Primero, probaremos que la proporción $|\mathbf{C}_G(x)_\pi|/|G_\pi|$ es como mucho $1/p$ para todo π-elemento x que no esté en $\mathbf{O}_\pi(G)$. Empezaremos por demostrarlo para grupos en los que $\mathbf{F}^*(G)$ es un π'-grupo. Utilizaremos este caso, junto con los teoremas sobre los *fixed point ratios* demostrados por Burness y Guralnick [**15**], para extender nuestro resultado a cualquier grupo. A partir de este resultado, deduciremos que posee un π-subgrupo de Hall normal y abeliano siempre que la probabilidad de que dos π-elementos conmuten supere $(p^2+p-1)/p^3$.

En el Apéndice A exploramos el último tema principal de esta tesis. En la Sección A.1 examinamos la relación entre la *commuting probability*, la teoría de grafos y el recubrimiento de p-elementos por subgrupos propios. Esto motivará la introducción de los p-subgrupos de Sylow redundantes en la Sección A.2. En la Sección A.4 introduciremos la Conjetura Picky, junto con algunas generalizaciones de esta. Finalmente, en la Sección A.5 presentamos algunos avances sobre estas conjeturas en grupos simples.

Acknowledgements

Supongo que es correcto (y casi imperativo legal) empezar dando las gracias a Alex, mi director de tesis. Muchísimas gracias por guiarme a lo largo de esta tesis y por toda la paciencia a la hora de dirigirme (y ha hecho falta esta paciencia). Si he llegado a escribir algo con cierto sentido en estos cuatro años, ha sido gracias a ti.

Por supuesto, hay mucha mas gente en esta universidad a la que me gustaría dar las gracias. En primer lugar, está Miquel, mi antiguo compañero de despacho. Por empujarme en la dirección correcta cuando no veía muy claro si meterme en un doctorado (o no). Además de ello, también quería darte las gracias por tu hospitalidad conmigo cuando estaba empezando la tesis.

En segundo lugar, quería darte las gracias a ti, Lucía, por las buenas conversaciones contigo y por tu ayuda a lo largo de todo este tiempo. Sin ti, aún seguiría atascado con el primer formulario de la tesis. Gracias por todo, y no dejes de ayudar a la gente.

No podría continuar los agradecimientos sin acordarme de Gabriel, mi compañero de despacho. Me siento obligado a darte las gracias por la compañía y por los buenos ratos juntos. ¡Por muchos más cafés juntos y muchas más vueltas por Burjassot!

Además de los anteriormente mencionados, quiero dar las gracias a Joan, Noelia, Marcos y David Beltrán. Muchas gracias a todos y todas por el buen rollo que me habéis transmitido, tanto en la facultad como a la hora de la comida. Aprovecho para decir que, digan lo que digan, la cafetería de campus es mejor que la de farmacia.

I would like to dedicate a very special thank to Attila Maróti. Thanks you for the kindness you have always shown me, even when you didn't have to. I would also like to thank you for your hospitality with me during my stay in Budapest. As a mathematician you are good, but as a person there is no better. For many more years of mathematics together! Köszönöm szépen!

I would also like to thank the members of my thesis committee for their many helpful comments and suggestions (and there were lots of them), which have helped to improve this manuscript.

Llegados a este punto, quería mandar un agradecimiento muy especial a mis amigas Fénix, María y Eva. Habéis estado a mi lado en los buenos y en los malos momentos durante los últimos cuatro años, y habéis cuidado mucho de mí durante todo este tiempo. Sois unas personas geniales y unas amigas insuperables. Me siento muy afortunado de teneros en mi vida. Muchos dan algo, pero solo unas pocas lo dais todo.

Además de ellas, no puedo dejar de dar las gracias a Susana, Tomás, María Peretó y Daniel Isert. Gracias de corazón a todos y todas por los buenos momentos juntos y por los que están por llegar.

Me gustaría cerrar estas líneas dando las gracias a mi familia. En primer lugar, me gustaría dar las gracias a mis padres, José Gil e Inocencia, así como a mi hermano José Gil. Muchas gracias por todo el cariño a lo largo de estos años. Esta tesis no sería posible sin vosotros. En segundo lugar, quería dar las gracias a mis abuelas, Leandra y Luisa, por todo su amor y por todos los buenos momentos en La Roda y Mazarrón. Finalmente, me gustaría cerrar estos agradecimientos recordando a mi abuelo José Gil, quien, desgraciadamente, no está aquí para ver este día tan importante. Siempre estarás en nuestra memoria.

Introduction

All groups considered in this work will be finite, unless stated otherwise. The main results in this thesis are stated in the introduction of Chapters 3 to 6 and they are presented as Theorems B to J. They have appeared in the following papers [**51, 79, 80, 81, 84**], all of which have been published, with the exception of [**84**], which is a work in preparation. The main topics we consider are the following:

(I) The fields of values of (conjugacy) classes and characters.

(II) The commuting probability and related invariants.

(III) The connection between coverings of groups with graph theory and representation theory.

We start by introducing the results in the first topic, which appear in Chapter 3. Before presenting our first topic, we introduce some historical background, which will contextualized the results discussed in this topic. Problem 1 in Brauer's list of problems [**12**] asks for the classification of the complex group algebras up to isomorphism. Let G be a group and let $\{\chi_1, \ldots, \chi_k\}$ be the set of irreducible (complex) characters of G. We define the degree pattern of G as the multiset $\{\chi_1(1), \ldots, \chi_k(1)\}$. Wedderburn's Theorem shows that

$$\mathbb{C}G \cong \bigoplus_{i=1}^{k} M_{\chi_i(1)}(\mathbb{C}).$$

Hence, Brauer's Problem 1 is equivalent to classifying all possible degree patterns of groups.

Even though the complete classification of all degree patterns seems impossible to reach, there are some restrictions on the possible degree patterns of groups. For example, if $\{n_1, \ldots, n_f\}$ is the degree pattern of a group G, then the number of 1's in this pattern is $|G : G'|$, which divides $|G| = \sum_{i=1}^{f} n_i^2$. In addition, we have that each n_i is the degree of an irreducible character of G and hence it must divide $\sum_{i=1}^{f} n_i^2$.

We are interested in less trivial results on the degree patterns. A classical result of Landau [**62**] asserts that $|G|$ is bounded in terms of $k(G) = |\mathrm{Cl}(G)|$, where $\mathrm{Cl}(G)$ is the set of conjugacy classes in G (so in terms of the above notation,

$k = k(G)$). Equivalently, for any integer $n \geqslant 1$ there exists finitely many groups with exactly n conjugacy classes. From the point of view of Brauer's Problem 1, Landau's Theorem asserts that there exist finitely many degree patterns of a given length.

In 2007, Moretó [**86**] defined the invariant $m(G)$ as follows:

$$m(G) = \max_{d \in \mathbb{N}} |\{\chi \in \mathrm{Irr}(G) \mid \chi(1) = d\}|.$$

That is, $m(G)$ is the maximum number of irreducible characters with the same degree. It was conjectured [**86**, Conjecture A] that $|G|$ is $m(G)$-bounded. By [**86**, Theorem A] the conjecture holds if and only if it holds for symmetric groups. Finally, Craven [**25**, Theorem 1.2] proved that this result is true for symmetric groups.

Thus, $|G|$ is $m(G)$-bounded. We observe that this means that, for any $k \geqslant 1$, there exist finitely many degree patterns with at most k components with the same degree. In general, $m(G)$ is much smaller than $k(G)$. This is a strengthened form of Landau's Theorem.

It is not completely trivial to see that $m(G) = 1$ if and only if $G = 1$ (see [**82**, Theorem 2.3]). In private communication, Moretó suggested the following conjectures to the author.

Conjecture. *Let $\mathbb{B}$ be the Baby Monster group. If G is a group with $m(G) = 2$, then $|G| \leqslant |\mathbb{B}|$.*

Conjecture. *Let $\mathbb{M}$ be the Monster group. If G is a group with $m(G) = 3$, then $|G| \leqslant |\mathbb{M}|$.*

The first of these conjectures was proved by the author in [**82**, Theorem A]. In fact, this is a consequence of [**82**, Theorem B], which classifies all groups with $m(G) = 2$. The second conjecture remains open. We decided to exclude these results from this thesis because their proofs depend on detailed computer calculations.

There are many results generalizing Landau's Theorem by replacing $k(G)$ by a smaller invariant. Given a group G, we write $k_{pp}(G)$ to denote the number of conjugacy classes of elements of prime power order in G. Héthelyi and Külshammer [**48**] proved that $|G|$ is bounded in terms of $k_{pp}(G)$. While the proof of Landau's Theorem is elementary, the proof of the Héthelyi–Külshammer Theorem relies on the classification of finite simple groups (in what follows, we refer to this as *CFSG* for short).

In the case of simple groups, much more can be said. Let S be a non-abelian simple group and let p be a prime dividing $|S|$. We define $m_p(S)$ to be the number of orbits of $\mathrm{Aut}(S)$ on the set of p-elements of S. We also write $L(S)$ for the maximal value of $m_p(S)$ over all prime divisors p dividing $|S|$. Recently,

Giudici, Morgan and Praeger [**36**] have proved that $|S|$ is bounded in terms of $L(S)$ for a simple group S. We remark that the invariants $m_p(S)$ where previously studied in [**95**].

The results in the first topic of this thesis prove versions of Landau's Theorem involving fields of values. To introduce these results, we introduce some new concepts.

Given a character χ of G, we can associate a finite extension of $\mathbb{Q}$ to χ, namely the field generated by the values $\chi(K)$ for K in $\mathrm{Cl}(G)$. We denote this subfield of $\mathbb{C}$ by

$$\mathbb{Q}(\chi) = \mathbb{Q}(\chi(K) \mid K \in \mathrm{Cl}(G)).$$

The extension $\mathbb{Q}(\chi)$ is called the *field of values* of χ.

It is well known that there exists a duality between irreducible characters and conjugacy classes. By this we mean that, for most concepts and results on irreducible characters there exists an equivalent version with conjugacy classes, and *vice versa*. In this case, there exists a dual definition for the field of values of a conjugacy class. Given $K \in \mathrm{Cl}(G)$, we define the field of values of K as the field extension of $\mathbb{Q}$ generated by the values $\chi(K)$, where χ runs through $\mathrm{Irr}(G)$. That is

$$\mathbb{Q}(K) = \mathbb{Q}(\chi(K) \mid \chi \in \mathrm{Irr}(G)).$$

Finally, we define the field of values of G as the field generated by the values $\chi(K)$ where χ runs through $\mathrm{Irr}(G)$ and K runs through $\mathrm{Cl}(G)$. This is

$$\mathbb{Q}(G) = \mathbb{Q}(\chi(K) \mid \chi \in \mathrm{Irr}(G), K \in \mathrm{Cl}(G)).$$

Nowadays, the study of fields of values is a very active area of research in character theory. Before continuing, we make a brief summary with some of the results in this area. Given a group G we write $\pi(G)$ to denote the set of prime divisors of $|G|$. In the case of solvable groups, it is possible to bound the prime divisors of $|G|$ in terms of fields of values of classes and irreducible characters. A classical result of Gow [**39**] shows that $\pi(G) \subseteq \{2, 3, 5\}$ for any solvable group G with $\mathbb{Q}(G) = \mathbb{Q}$. Chillag and Dolfi [**23**, Theorem 2] proved that if G is a solvable group such that $\mathbb{Q}(K)$ is either $\mathbb{Q}$ or a quadratic extension of $\mathbb{Q}$ for every $K \in \mathrm{Cl}(G)$, then $\pi(G) \subseteq \{2, 3, 5, 7, 13, 17\}$. It is not known whether 17 can actually occur as a prime divisor of a group satisfying this property. Moreover, Tent [**120**, Theorem A] provided a dual version for characters. More precisely, this result shows that if G is a solvable group such that $\mathbb{Q}(\chi)$ is either $\mathbb{Q}$ or a quadratic extension of $\mathbb{Q}$ for every $\chi \in \mathrm{Irr}(G)$, then $\pi(G) \subseteq \{2, 3, 5, 7, 13\}$.

In a more general way, [**120**, Theorem C] shows that if G is a solvable group such that $|\mathbb{Q}(\chi) : \mathbb{Q}| \leqslant k$ for any $\chi \in \mathrm{Irr}(G)$, then $|\pi(G)|$ is bounded by a function on k. Chillag and Dolfi [**23**, Problem 2] asked whether the dual version for classes is true.

In 2021, Moretó [88] defined the invariant $f(G)$ to be the largest multiplicity of a field as a field of values of an irreducible character. That is

$$f(G) = \max_{F/\mathbb{Q}} |\{\chi \in \mathrm{Irr}(G) \mid \mathbb{Q}(\chi) = F\}|,$$

where the maximum is over all field extensions $F/\mathbb{Q}$. Using this invariant, Moretó [88, Theorem A] proved that $|G|$ is bounded in terms of $f(G)$. This is again a strengthened form of Landau's Theorem. Moreover, this is an alternative form of the bound on $|G|$ in terms of $m(G)$. However, instead of looking at multiplicities of character degrees, we consider multiplicities of fields of values of characters.

In [88], Moretó also proved that $f(G) = 1$ if and only if $G = 1$. He also also asked for the classification of all groups with $f(G) \in \{2, 3\}$. In this thesis, we provide such a classification. That constitutes Theorem B of this thesis, which has been published in [79].

It is natural to consider the dual version for conjugacy classes. We define the invariant $h(G)$ as follows:

$$h(G) = \max_{F/\mathbb{Q}} |\{K \in \mathrm{Cl}(G) \mid \mathbb{Q}(K) = F\}|.$$

The biggest issue with the invariant $h(G)$ is that it does not behave well with respect to quotients. It is not hard to see that $f(G/N) \leqslant f(G)$ for any normal subgroup N of G. However, the same does not hold for $h(G)$. Indeed, there exist examples with $h(G/N) > h(G)$ for some $N \trianglelefteq G$, as explained in Section 3.1. To overpass this issue, we introduce a slightly stronger invariant. We define $\hat{h}(G)$ by

$$\hat{h}(G) = \max_{N \trianglelefteq G} \{h(G/N)\}.$$

By definition, we have that $h(G) \leqslant \hat{h}(G)$ and $\hat{h}(G/N) \leqslant \hat{h}(G)$ for all $N \trianglelefteq G$.

In joint work with Vergani [84], we have proved that $|G|$ is bounded in terms of $\hat{h}(G)$ for any group G. It is worth to mention that the proof of this result uses the the aforementioned result of Giudici et al. in [36]. In order to bound $|G|$ in terms of $\hat{h}(G)$, it will be enough to bound $|\pi(G)|$. To do so, we will use the techniques introduced in [29]. The result bounding $|G|$ in terms of $\hat{h}(G)$ constitute Theorem A of Chapter 3 and it will appear in [84].

Inspecting the groups appearing in the classification provided by Theorem B, we deduce that if $f(G) \in \{1, 2, 3\}$, then $h(G) = f(G)$. Thus, it is natural to ask whether the converse is true, that is, if $f(G) = h(G)$ for all groups with $h(G) \leqslant 3$. Our next main result answers this question affirmatively. This result is Theorem C and it will also appear in [84].

Next we introduce the second topic of this thesis. The results on this topic are proved in Chapters 4, 5 to 6. In order to introduce these results, we begin by introducing the commuting probability.

We define the *commuting probability* of a group G to be the probability that two random elements of G commute and we will denote it by $\Pr(G)$. That is

$$\Pr(G) = \frac{|\{(x,y) \in G \times G \mid xy = yx\}|}{|G|^2}.$$

We remark that the definition can be suitably extended to certain families of infinite groups (see, for example, [**122**] or Section 2 of [**42**]). However, in this work we will only study the finite case.

The goal of the second topic of this thesis is to use the commuting probability and some related invariants to study the structure of groups and to prove local-global results. By local-global results we mean every result determining the structure of the Sylow p-subgroups or the Hall π-subgroups of a group in terms of invariants defined on the whole group. In the latest years, relevant progresses have been made on the study of local-global results. For example, one of the most important local-global conjectures is Brauer's Height Zero Conjecture, which was put forward in 1955 by Brauer [**11**]. After many efforts, Brauer's Height Zero Conjecture was solved by Malle, Navarro, Schaefer Fry and Tiep [**73**]. Let us introduce the results on the second topic of this thesis.

In 1973, Gustafson [**42**] proved that if $\Pr(G)$ exceeds $5/8$, then G is abelian. It is worth commenting that the proof of Gustafson's theorem is very short and entirely elementary. Also worth mentioning that the bound is optimal. However, a more general result was already known. More precisely, Joseph [**58**] replaced the bound $5/8$ by $(p^2+p-1)/p^3$, where p is the smallest prime dividing $|G|$. In Section 3 of [**42**], Gustafson indicates how to obtain the bound $(p^2+p-1)/p^3$. For this reason, we will refer to the following result as the Gustafson–Joseph Theorem.

In 2023, Burness, Guralnick, Moretó and Navarro [**16**, Theorem A] proved that, given a prime p, if the probability $\Pr_p(G)$ that two random p-elements of G commute exceeds $(p^2+p-1)/p^3$, then G has a normal and abelian Sylow p-subgroup (in which case, the probability is 1). This result is a local version of the Gustafson–Joseph Theorem. In contrast to the Gustafson–Joseph Theorem, it is worth mentioning here that the proof of the main theorem in [**16**] requires *CFSG*.

We recall that the Itô–Michler Theorem [**57, 85**] asserts that G has a normal and abelian Sylow p-subgroup if and only if p does not divide the degree of any irreducible character of G. Thus, [**16**, Theorem A] provides a character-free condition for the existence of normal and abelian Sylow p-subgroups.

In fact, [16, Theorem A] was a direct consequence of [16, Theorem C], which asserts that, for a fixed p-element, x, not lying in $\mathbf{O}_p(G)$, the proportion of p-elements of G commuting with x is at most $1/p$. Moreover, [16, Theorem D] asserts that the same holds for $x \in \mathbf{O}_p(G) \backslash \mathbf{Z}(\mathbf{O}_p(G))$. We notice that

$$\frac{|\mathbf{C}_G(x)_p|}{|G_p|} = \frac{\Psi(x)}{\Psi(1)},$$

where X_p denotes the set of p-elements of a group X and Ψ denotes the permutation character for the action of G on its p-elements by conjugation. In the language of permutation groups, this number is called the *fixed point ratio* with respect to this action. For this reason, the proof of [16, Theorem C] depends on the deep results on fixed point ratios proved in [15].

It was asked in [16] whether it was possible to extend their results to a general set of primes π. We answer this question affirmatively. Let π be a set of primes and let p be the smallest prime in π. We prove that if x is a π-element of G not lying in $\mathbf{O}_\pi(G)$, then the proportion of π-elements not commuting with x is at most $1/p$. From this result, we will deduce that if the probability $\Pr_\pi(G)$ that two random π-elements commute exceeds $(p^2+p-1)/p^3$, then G possesses a normal and normal and abelian Hall π-subgroup. These results are Theorems I and J of Chapter 6 and they have been published in [80].

Secondly, we study a different local invariant. Gustafson [42] proved that

$$\Pr(G) = \frac{k(G)}{|G|}.$$

It is worth to mention that this was known by Erdős and Turán [28, Theorem IV]. From this identity it is possible to define a local invariant providing information on the π-elements of a group. For a set π of primes, let $k_\pi(G)$ be the number of conjugacy classes of π-elements of the group G. Hung and Maróti [76] defined the invariant $\mathrm{d}_\pi(G)$ as

$$\mathrm{d}_\pi(G) = \frac{k_\pi(G)}{|G|_\pi}.$$

This invariant is always at most 1 by a result of Robinson (see Lemma 5.10), and it is strongly related to the commuting probability. For example, if q is a prime in π and Q is a Sylow q-subgroup of G, then $\mathrm{d}_\pi(G) \leqslant \Pr(Q)$ (this was observed in the introduction of [76]).

Hung and Maróti [76, Theorem 1] proved that if $\mathrm{d}_\pi(G)$ is larger than $5/8$, then then G possesses an abelian Hall π-subgroups. This result is a local version of Gustafson–Joseph's Theorem, different from [16, Theorem A]. In joint work with Hung and Maróti [51], we extended [76, Theorem 1] by replacing the bound $5/8$ by $(p^2+p-1)/p^3$, where p is the smallest prime in π. Moreover, we prove that if $\mathrm{d}_\pi(G)$ exceeds $1/p$, then G has a nilpotent Hall π-subgroup (of nilpotency class at most 2). We recall that, by a classical theorem of Wielandt [128], if G contains a nilpotent Hall π-subgroup, then the Hall π-subgroups behave like

Sylow subgroups in the sense that they are pairwise conjugate and every π-subgroup of G is contained in one of them. These results constitute Theorem H of Chapter 5 and they are published in [**51**].

Now, we turn our attention to the study of the nilpotency and the supersolvability of groups in terms of the commuting probability. Lescot [**65**] proved that if $\Pr(G)$ exceeds $1/2$, then G is nilpotent. Moreover, Guralnick and Robinson [**41**] improved this result by replacing the $1/2$ by $1/p$, where p is the smallest prime dividing $|G|$. It is not hard to see that the bound $1/p$ is not sharp for $p > 2$. In addition, Barry, MacHale and Ni Shé [**5**] proved that if $\Pr(G)$ is larger than $1/3$, then G is supersolvable. We remark that this result was extended and the proof was simplified by Hung, Lescot and Yang [**67**].

Our next results determine the best possible function $g_n(p)$ (respectively, $g_s(p)$) such that if $\Pr(G) > g_n(p)$ (resp. $\Pr(G) > g_s(p)$), where p is the smallest prime dividing $|G|$, then G is nilpotent (resp. supersolvable). The definition of the functions $g_n(p)$ and $g_s(p)$ depend on some concepts in number theory and will be postponed to Chapter 4. These results are Theorems D and E of Chapter 4, which are published in [**81**].

Finally, we consider further variations of the invariant $\Pr(G)$. Following [**56**], we define the *average character degree* of G as the arithmetic mean of the character degrees of the irreducible characters of G and we will write $\operatorname{acd}(G)$ to denote it. That is

$$\operatorname{acd}(G) = \frac{\sum_{\chi \in \operatorname{Irr}(G)} \chi(1)}{|\operatorname{Irr}(G)|}.$$

It is well known that $1/\Pr(G) \leqslant \operatorname{acd}(G)^2$ for every group G (see the introduction of Chapter 4).

As in the case of $\Pr(G)$, there are many results that prove that the structure of G is more restricted as $\operatorname{acd}(G)$ decreases. Hung and Moretó [**92**] proved that if $\operatorname{acd}(G)$ is smaller than $16/5$, then G is solvable (this was conjectured in [**56**]). Isaacs, Loukaki and Moretó [**56**] proved that if $\operatorname{acd}(G)$ is smaller than $4/3$, then G is nilpotent. In that paper, it was proved that if $\operatorname{acd}(G)$ is smaller than $3p/(p+2)$, where p is the smallest prime dividing $|G|$, then G is supersolvable.

Our final results in this direction determine the best possible functions $h_n(p)$ and $h_s(p)$ such that if $\operatorname{acd}(G) < h_n(p)$, where p is the smallest prime dividing $|G|$, then G is nilpotent and if $\operatorname{acd}(G) < h_s(p)$, then G is supersolvable. As in the case of our results on the commuting probability, the definition of our sharp bounds depends on non-trivial results in number theory and will be postponed to Chapter 4. These results constitute Theorems F and G of Chapter 4 and they are published in [**81**].

The third and final topic of this thesis appears in Appendix A. We decided to leave this topic as an appendix because there is still a lot of work in progress on it. It is expected that some of the questions discussed in this appendix will be relevant in the future.

The main goal of Appendix A is to introduce concept of *picky* elements and the Picky Conjecture. The origin of this concept is a joint work with Maróti and Moretó [**77**], where we deal with a variation of classical questions on coverings of groups. It is known that the commuting probability has several connections with graph theory and coverings of groups. Surprisingly, it is also true that coverings of groups have connections with representation theory. That will lead us to state and discuss the Picky Conjecture, recently stated by Moretó and Rizo [**93**]. The Picky Conjecture, together with some generalizations, are still being studied by several authors in different papers [**13, 70, 83, 93, 119**] still in preparation.

The *non-commuting graph* of a group G is a graph whose vertices are the non-central elements of G and two elements are joined by an edge if they do not commute. We notice that $1 - \Pr(G)$ is equal to the density of edges in the non-commuting graph. Moreover, the clique number of this graph coincides with the size of the largest set of pairwise non-commuting elements in G. This number is usually denoted by $n(G)$. A direct application of Turán's Theorem [**125**], gives

$$\frac{1}{\Pr(G)} \leqslant n(G).$$

This inequality shows how graph theory can help to link group theoretical concepts.

The non-commuting graph can be studied from the point of view of covering of groups. In 1926, Scorza [**114**] proved that a group cannot be covered by using two proper subgroups. The proof of this result is completely elementary. This motivated the definition of the covering number of a group. Given a group G we say that the covering number of G is equal to d, and we will write $\sigma(G) = d$, if G can be expressed as the union of d proper subgroups, but it cannot be expressed as the union of $d-1$ proper subgroups. We observe that if $\sigma(G) > d$ and $x_1, \dots, x_d \in G \backslash \mathbf{Z}(G)$, then $G \neq \mathbf{C}_G(x_1) \cup \cdots \cup \mathbf{C}_G(x_d)$ and hence $x_1, \dots, x_d$ have a common linked vertex in the non-commuting graph.

Inspired by the covering number, Maróti, Moretó and the author of this thesis [**78**] introduced the *p-covering number*. Let p a prime and let G be a group. We define the p-covering number of G, denoted $\sigma_p(G)$, as the minimum number of proper subgroups whose union contains the set of p-elements of G. By [**78**, Theorem A], we have that $\sigma_p(G) \geqslant \sigma(G) - 1$ for a solvable group generated by its p-elements. Moreover, $\sigma_p(G) = \sigma(G) - 1$ if and only if G is not a p-group. This suggests that $\sigma_p(G)$ should behave as $\sigma(G)$ for groups generated by its p-elements.

The first natural question is to ask whether there exists version of Scorza's Theorem for $\sigma_p(G)$. It was conjectured in [78] that $\sigma_p(G) > p$ for groups generated by its p-elements. The p-solvable case of that conjecture was proved in [78, Theorem B], but the general proof was provided by Guralnick [40, Theorem F]. We remark that this proof does not depend on *CFSG*.

Now, let G be a group generated by its p-elements and let $x_1, \dots, x_p \in G_p$ be non-central p-elements. Then $G_p \nsubseteq \mathbf{C}_G(x_1) \cup \cdots \cup \mathbf{C}_G(x_p)$ by [40, Theorem F]. Thus, there exists $y \in G_p$ such that y is adjacent to $x_1, \dots, x_p$ in the non-commuting graph of G. As a consequence, the induced subgraph of the non-commuting graph of G on $G_p \backslash \mathbf{Z}(G)_p$ is connected with diameter at most 2.

This motivates the definition of *redundant Sylow p-subgroup*. Following [77], we say that a group has a redundant Sylow p-subgroup if the set of p-elements of G can be expressed as the union of $|\operatorname{Syl}_p(G)| - 1$ Sylow p-subgroups. It is not hard to see that G does not possess a redundant Sylow p-subgroup if and only if there exists p-elements lying in a unique Sylow p-subgroup (see Lemma A.11). Such elements are called *picky* elements. It was observed in [77, Corollary 2.5] that the picky elements have good properties from the point of view of characters. Recently, Moretó and Rizo [93] observed that this connection is deeper than one might expect. In order to explain this connection, we need to introduce some more context.

Given a group G and a prime p, we write $\operatorname{Irr}_{p'}(G)$ to denote the set of irreducible characters of G whose degree is not divisible by p. That is

$$\operatorname{Irr}_{p'}(G) = \{\chi \in \operatorname{Irr}(G) \mid \gcd(p, \chi(1)) = 1\}.$$

Another of the most famous local-global conjectures is McKay Conjecture, which asserts that

$$|\operatorname{Irr}_{p'}(G)| = |\operatorname{Irr}_{p'}(\mathbf{N}_G(P))|$$

for any $P \in \operatorname{Syl}_p(G)$. After many efforts, this conjecture was finally proved by Cabanes and Späth [17]. We remark that the case $p = 2$ was previously proved by Malle and Späth [74].

Given $x \in G$, we write $\operatorname{Irr}^x(G)$ to denote the set of irreducible characters of G that do not vanish on x. That is

$$\operatorname{Irr}^x(G) = \{\chi \in \operatorname{Irr}(G) \mid \chi(x) \neq 0\}.$$

Assume now that $x \in G$ is a picky element and that $P \in \operatorname{Syl}_p(G)$ is the unique Sylow p-subgroup of G containing x. Moretó and Rizo [93] have put forward several local-global conjectures involving strong relations between $\operatorname{Irr}^x(G)$ and $\operatorname{Irr}^x(\mathbf{N}_G(P))$ and the values of these characters at x. We state the most basic of these conjectures.

Conjecture (Picky Conjecture). *Let p be a prime, let G be a group and let $P \in \mathrm{Syl}_p(G)$. Assume that $x \in P$ is a picky element. Then there exists a bijection*

$$\Gamma : \mathrm{Irr}^x(G) \to \mathrm{Irr}^x(\mathbf{N}_G(P))$$

satisfying the following properties:

(I) $\Gamma(\chi)(1)_p = \chi(1)_p$ for every $\chi \in \mathrm{Irr}^x(G)$.

(II) $\mathbb{Q}(\Gamma(\chi)(x)) = \mathbb{Q}(\chi(x))$ for every $\chi \in \mathrm{Irr}^x(G)$.

They also observed that, for most cases, there exists a bijection such that $\Gamma(\chi)(x) = \pm\chi(x)$ for every $\chi \in \mathrm{Irr}^x(G)$. Given a picky p-element $x \in G$, we say that the Strong Picky Conjecture holds for (G, x) if there exists a bijection Γ satisfying $\Gamma(\chi)(x) = \pm\chi(x)$ for every $\chi \in \mathrm{Irr}^x(G)$.

We observe that if $\chi \in \mathrm{Irr}_{p'}(G)$ and $x \in G_p$, then $\chi(x) \neq 0$ by [**99**, Corollary 4.20]. Therefore, $\mathrm{Irr}_{p'}(G) \subseteq \mathrm{Irr}^x(G)$. Thus, if $x \in G$ is a picky p-element and the Picky Conjecture holds for (G, x), then the McKay Conjecture holds for G.

The Picky Conjecture together, with several generalizations, will be presented in Appendix A. We will briefly discuss some of the advances on these conjectures. The proof of these conjectures will probably require a lot of work.

Structure of the work

This work is divided into six chapters and one appendix.

Chapter 1 contains the basics of group theory that we will use throughout the rest of work.

Chapter 2 introduces the representation theory and the character theory. We will use Section 2.5 to introduce the classical results on the fields of values of classes and characters. Finally, in 2.6 we present results by Navarro and Tiep [**100**] and Rossi [**110**] on groups with at most 3 rational classes or 3 rational irreducible characters.

In Chapter 3 we prove the results on the fields of values of classes and characters. In Section 3.2 we bound the size of a group $|G|$ in terms of $\hat{h}(G)$. We will begin by proving that $|G|$ is $(|\pi(G)|, h(G))$-bounded for any group G. Then, we will use the tools developed by Farias e Soares [**29**], together with the results of Giudici et al. [**36**], to bound $|\pi(G)|$ in terms of $\hat{h}(G)$.

The classification of groups with $f(G) \leqslant 3$ is proved in Section 3.3. We will study the solvable and the non-solvable cases separately. First, we will classify the non-solvable groups with $f(G) \leqslant 3$. It is easy to see that these groups have at most 3 rational characters. Then, we will use the aforementioned results by Navarro, Rossi and Tiep. After that, we will prove the solvable case of the classification. We will begin by classifying the metabelian groups with $f(G) \leqslant 3$ and then we will prove that any solvable group with $f(G) \leqslant 3$ is metabelian.

In Section 3.4 we prove that $f(G) = h(G)$ for any group G with $h(G) \leqslant 3$. All groups with $h(G) \leqslant 3$ will have at most 3 conjugacy classes and hence, we will apply the results by Navarro, Rossi [**100**] and Tiep [**110**] to deduce that the number of rational characters equals the number of rational characters in these groups. This equality, together with a careful application of a classical result of Brauer [**53**, Theorem 6.32], will prove the equality $f(G) = h(G)$. Finally, Section 3.5 contains some open questions on the fields of values.

In Chapter 4 we prove our results on the nilpotency and supersolvabilty in terms of the commuting probability and the average character degree. In Sections 4.3 and 4.4 we prove the results determining the nilpotency and the supersolvability in terms of $\Pr(G)$. In each case, we will prove that, in order to obtain the best possible bound, it is enough to study a certain family of groups. After that, we will establish the bound in the corresponding family and we will find a group (in that family) attaining the bound. Our results on the average character degree will be proved in Section 4.5. We will use the techniques introduced by Isaacs, Loukaki and Moretó [**56**] to establish the bounds and then will find groups for which the bounds are attained. Section 4.6 contains the number-theoretical discussion of this thesis. As we mentioned above, the definitions of the bounds for $\Pr(G)$ and $\mathrm{acd}(G)$ depend on non-explicit quantities depending on prime numbers. In the case of the quantities for $\mathrm{acd}(G)$, they depend on numbers satisfying some specific conditions. Moreover, we will also discuss about the quantities involved in the results on $\Pr(G)$.

Chapter 5 contains our main results on $\mathrm{d}_\pi(G)$. Let π be a set of primes and let p be the smallest prime in π. We will begin by proving that the bound $(p^2+p-1)/p^3$ for the commutativity of Hall π-subgroups follows "easily" from the bound $1/p$ for the nilpotence. After that, we will reduce the proof of the bound $1/p$ to a question on finite simple groups. Finally, this question will be solved by using *CFSG* and studying each case separately. The alternating case will be proved by an elementary argument and the sporadic case will follow by examination of the information in the *ATLAS* [**24**]. For groups of Lie type in characteristic s, we will study separately the case when $s \in \pi$ and the case $s \notin \pi$. If $s \in \pi$, then the result will follow by the results in [**31**], while the result will follow from [**72**, Theorem 3.15] for $s \notin \pi$.

In Chapter 6 we prove our results on the probability that two π-elements commute. We will first prove that the proportion $|\mathbf{C}_G(x)_\pi|/|G_\pi|$ is at most $1/p$ for every π-element x not lying in $\mathbf{O}_\pi(G)$, where p is the smallest prime in π. We will begin by proving it for groups in which $\mathbf{F}^*(G)$ is a π'-group. We will use this case, together with the results on fixed point ratio introduced by Burness and Guralnick [**15**], to extend our result to any group. We will use this result to deduce that G possesses a normal and abelian Hall π-subgroup whenever the probability that two random π-elements commute exceeds $(p^2+p-1)/p^3$.

In Appendix A we explore the final main topic of this thesis. In Section A.1 we will study the relationship between the commuting probability, graph theory and covering of p-elements by proper subgroups. This will motivate our definition of the redundant Sylow p-subgroups in Section A.2. In Section A.4 we will introduce the Picky Conjecture, together with some generalizations of this conjecture. Finally, in Section A.5 we present the recent advances of these conjecture for simple groups.

CHAPTER 1

Preliminaries on group theory

In this thesis, our group theoretical notation follows [54]. We remind the reader that all groups in this thesis are finite, unless stated otherwise.

1.1. Simple groups

We begin by recalling the classification of finite simple groups. For the remainder of the thesis, we will refer to this as *CFSG*.

THEOREM 1.1 (Classification of finite simple groups). *Let G be a non-abelian simple group. Then G is isomorphic one of the following:*

(i) An alternating group A_n for $n \geqslant 5$.

(ii) A classical simple group of Lie type over the field of q elements (where q is a prime power). In particular, G is one of the following:

(ii.1) $\mathrm{PSL}(n,q)$ for $n \geqslant 2$ and $(n,q) \notin \{(2,2),(2,3)\}$,

(ii.2) $\mathrm{PSU}(n,q) = \mathrm{PSL}^-(n,q)$ for $n \geqslant 3$ and $(n,q) \neq (3,2)$,

(ii.3) $\mathrm{PSp}(2n,q)$ for $n \geqslant 2$, q odd and $(n,q) \neq (2,2)$,

(ii.4) $\Omega(2n+1,q) = O(2n+1,q)$ for $n \geqslant 3$ and $(n,q) \neq (2,2)$,

(ii.5) $\mathrm{P}\Omega^+(2n,q) = O^+(2n,q)$ for $n \geqslant 4$,

(ii.6) $\mathrm{P}\Omega^-(2n,q) = O^-(2n,q)$ for $n \geqslant 4$.

(iii) An exceptional simple group of Lie type over $\mathbb{F}_q$, where $\mathbb{F}_q$ denotes the field of q elements. In particular, G is one of the following:

(iii.1) $E_6(q), E_7(q), E_8(q), F_4(q), {}^3D_4(q), {}^2E_6(q)$ for $q \geqslant 2$,

(iii.2) $G_2(q)$ for $q \geqslant 3$,

(iii.3) ${}^2B_2(q), {}^2F_4(q)$ for $q = 2^{2f+1}$ and $f \geqslant 1$,

(iii.4) ${}^2G_2(q)$ for $q = 3^{2f+1}$ and $f \geqslant 1$.

(iv) One of the 27 *sporadic simple groups listed here:*

$$\mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{22}, \mathrm{M}_{23}, \mathrm{M}_{24}, \mathrm{J}_1, \mathrm{J}_2, \mathrm{J}_3, \mathrm{J}_4, \mathrm{Co}_1, \mathrm{Co}_2, \mathrm{Co}_3, \mathrm{Fi}_{22}, \mathrm{Fi}_{23},$$
$$\mathrm{Fi}'_{24}, {}^2\mathrm{F}_4(2)', \mathrm{HS}, \mathrm{McL}, \mathrm{He}, \mathrm{Ru}, \mathrm{Suz}, \mathrm{ON}, \mathrm{HN}, \mathrm{Ly}, \mathrm{Th}, \mathbb{B}, \mathbb{M}.$$

Some authors do not consider ${}^2\mathrm{F}_4(2)'$, the Tits group, as a sporadic group. We have included it in the sporadic groups because it cannot be studied with the same techniques as the groups of Lie type. The *Atlas of finite groups* [**24**] contains the (ordinary) character tables, as well as information on maximal subgroups and conjugacy classes, of the small finite simple groups. It contains information of all sporadic simple groups and the "small" alternating groups and groups of Lie type. For the remainder, we will refer to it as the *ATLAS*.

Before continuing, we digress about the simple groups of Lie type. For this purpose we follow [**75**]. Let $q = p^f$ for a prime p and an integer $f \geqslant 1$. We write $\mathbb{F}_q$ to denote the field of q elements and we write $\overline{\mathbb{F}_q}$ to denote the algebraic closure of $\mathbb{F}_q$. Let us consider a linear algebraic group $\mathbf{G} \leqslant \mathrm{GL}(n, \overline{\mathbb{F}_q})$. We remark that $\mathbf{G}$ is a non-finite group.

Let $F_q : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$ be the Frobenius endomorphism, that is, $F_q(x) = x^q$. This map can be extended to a map $F_q : \mathrm{GL}(n, \overline{\mathbb{F}_q}) \to \mathrm{GL}(n, \overline{\mathbb{F}_q})$ defined by $F_q(\{a_{ij}\}) = \{a_{ij}^q\}$ and this naturally induces a group homomorphism $F_q : \mathbf{G} \to \mathbf{G}$ (see Section 21.1 of [**75**] for more information). This map will be called the Frobenius endomorphism of $\mathbb{G}$. We say that $F : \mathbf{G} \to \mathbf{G}$ is a **Frobenius morphism** if there exists $m \geqslant 1$ such that F^m coincides with the Frobenius endomorphism of $\mathbf{G}$. Given $F : \mathbf{G} \to \mathbf{G}$ an Steinber endormorphism, we will write $\mathbf{G}^F$ to denote the set of elements of $\mathbf{G}$ fixed by F. That is

$$\mathbf{G}^F = \{x \in \mathbf{G} \mid F(x) = x\}.$$

By [**75**, Theorem 24.17], every simple group of Lie type is of the form $S = \mathbf{G}^F/\mathbf{Z}(\mathbf{G}^F)$ for some simple algebraic group $\mathbf{G}$ of simply connected type (see [**75**, Definition 9.14] for a definition) and a suitable Frobenius morphism F on $\mathbf{G}$.

Definition. We say that a group T is **almost simple** if there exists a non-abelian simple group S such that $S \trianglelefteq T \leqslant \mathrm{Aut}(S)$.

For many years, the Schreier Conjecture asked whether $\mathrm{Out}(S) = \mathrm{Aut}(S)/S$ is solvable for every non-abelian simple group S. Finally, the Schreier Conjecture was proved as a consequence of *CFSG*, just by determining $\mathrm{Out}(S)$ for all non-abelian simple groups S.

1.2. Sylow and Hall Theory, solvability and nilpotency

Let $n \geqslant 1$ be an integer and let π be a set of primes. We write n_π and $n_{\pi'}$ to denote the unique numbers such that $n = n_\pi n_{\pi'}$, all the prime divisors of n_π lie in π and any prime of π divides $n_{\pi'}$. The numbers n_p and $n_{\pi'}$ will be called the π-part of n and the π'-part of n, respectively.

Let G be a group and let π be a set of primes. We will say that G is a π-**group** if all prime divisors of $|G|$ lie in π. A subgroup $H \leqslant G$ will be said to be a π-**subgroup** if it is a π-group. Moreover, $g \in G$ will be said to be a π-**element** if every prime divisor of $o(g)$ lies in π (equivalently, if $\langle g \rangle$ is a π-subgroup). We will write G_π to denote the set of π-elements of G.

Let p be a prime and let G be a group. We will say that $P \leqslant G$ is a **Sylow** p**-subgroup** of G if $|P| = |G|_p$. We will write $\mathrm{Syl}_p(G)$ to denote the set of Sylow p-subgroups of G.

Analogously, if π is a set of primes, we will say that $H \leqslant G$ is a **Hall** π**-subgroup** of G if $|H| = |G|_\pi$. We will write $\mathrm{Hall}_\pi(G)$ to denote the set of Hall π-subgroups of G. Given a prime p, we write p' to denote the set of primes different from p. If $H \in \mathrm{Hall}_{p'}(G)$, then we will say that H is a p**-complement**.

We remark that, contrary to the situation for Sylow subgroups, there exist groups without Hall π-subgroups for some set of primes. For example, A_5 does not possess a Hall $\{3,5\}$-subgroup. This observation, together with Sylow Theorems, motivates the definition of the classes of groups $\mathcal{E}_\pi, \mathcal{C}_\pi$ and $\mathcal{D}_\pi$.

Definition. Let π be a non-empty set of primes. We define the following classes of groups:

- Class $\mathcal{E}_\pi$: The class of groups such that $\mathrm{Hall}_\pi(G) \neq \varnothing$.
- Class $\mathcal{C}_\pi$: The class of groups such that $\mathrm{Hall}_\pi(G) \neq \varnothing$ and for any $H, R \in \mathrm{Hall}_\pi(G)$, there exists $g \in G$ such that $R = H^g$.
- Class $\mathcal{D}_\pi$: The class of groups such that $\mathrm{Hall}_\pi(G) \neq \varnothing$ and for any $H \in \mathrm{Hall}_\pi(G)$ and any π-subgroup $T \leqslant G$, there exists $g \in G$ such that $T \leqslant H^g$.

By definition, we have that $\mathcal{D}_\pi \subseteq \mathcal{C}_\pi \subseteq \mathcal{E}_\pi$. With these definitions, we observe that, Sylow Theorems imply that if p is a prime, then $G \in \mathcal{D}_p$ for any group G.

Given $x, y \in G$, we define the **commutator** of x and y by $[x,y] := x^{-1}y^{-1}xy$. Given $H, T \leqslant G$, we define

$$[H,T] = \langle [x,y] \mid x \in H, y \in T \rangle.$$

Let us write $G' := [G,G]$. This subgroup will be called the **commutator subgroup** of G. We recall that $N \leqslant G$ is said to be characteristic in G if it is invariant under every automorphism of G. It is easy to observe that G is a

characteristic subgroup of G. Moreover, if N is a normal subgroup of G such that G/N is abelian, then $G' \leqslant N$. That is, G' is the smallest normal subgroup with an abelian quotient. In particular, G is abelian if and only if $G' = 1$.

Given $k \geqslant 0$, we define $G^{(k)}$ as

$$G^{(0)} = G, \text{ and } G^{(k)} = [G^{(k-1)}, G^{(k-1)}] \text{ for } k \geqslant 1.$$

The series of groups $G = G^{(0)} \geqslant G^{(1)} \geqslant G^{(2)} \geqslant \dots$ will be called the derived series of G. For historical reasons, the groups $G^{(1)}, G^{(2)}$ and $G^{(3)}$ will be denoted by G', G'' and G''', respectively.

A group G, is said to be **solvable** if there exists $k \geqslant 1$ such that $G^k = 1$. In such a case, the **derived length** of G will be the smallest integer k satisfying $G^k = 1$. If $G'' = 1$, then we will say that the group is **metabelian**. Finally, when $G' = G$ we will say that G is **perfect**. The following result provides an alternative characterization of solvable groups.

Proposition 1.2. *Let G be a group. Then G is solvable if and only if there exists a series of subgroups*

$$1 = N_0 < N_1 < \dots < N_r = G$$

such that $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i is cyclic of prime order for every $0 \leqslant 1 < r$.

This result motivates the definition of supersolvable group.

Definition. We say that G is **supersolvable** if there exists a series of subgroups

$$1 = N_0 < N_1 < \dots < N_r = G$$

such that $N_i \trianglelefteq G$ and N_{i+1}/N_i is cyclic of prime order for every $0 \leqslant 1 < r$.

We notice that A_4 is a solvable group, which is non-supersolvable. There are many results on the solvability of groups. We state here the two most important results: Burnside's Theorem and the Feit–Thompson Theorem.

Theorem 1.3 (Burnside). *Let G be a group such that $|G|$ is divisible by at most 2 primes. Then G is solvable.*

Proof. This is [**53**, Theorem 3.10]. □

Theorem 1.4 (Feit and Thompson). *Let G be a group with $|G|$ odd. Then G is solvable.*

Proof. This is the main result of [**30**]. □

Here we have cited the classical proof of Burnside's Theorem. This proof requires character-theoretical tools. There exists a character-free proof, which follows from the main results of [8, 37].

Now, we introduce notions of π-separability and π-solvability.

DEFINITION. We say that a group G is **π-separable** if there exists a series of subgroups

$$1 = N_0 \lhd N_1 \lhd \ldots \lhd N_r = G$$

such that each factor N_i/N_{i-1} is either a π-group or a π'-group. If moreover each π-factor appearing is solvable, then G is said to be **π-solvable**. The **π-length** of a π-separable group, G, is the minimum possible number of factors that are π-groups in any normal series for G in which each factor is either a π-group or a π'-group.

THEOREM 1.5. *Let π be a set of primes and let G be a π-separable group. Then $G \in \mathcal{D}_\pi$.*

PROOF. This is [55, Theorem 3.10]. □

Now, we introduce the nilpotency. Given $k \geqslant 0$, we define $\gamma_k(G)$ as

$$\gamma_0(G) = G, \text{ and } \gamma_k(G) = [G, \gamma_{k-1}(G)] \text{ for } k \geqslant 1.$$

The series of groups $G = \gamma_0(G) \geqslant \gamma_1(G) \geqslant \gamma_2(G) \geqslant \ldots$ will be called the **lower central series** of G. A group will be said to be **nilpotent** if there exists $k \geqslant 1$ such that $G^k = 1$. In such a case, the **nilpotency class** of G will be the smallest k satisfying $\gamma_k(G) = 1$. We observe that G has nilpotency class 2 if and only if every commutator is central in G.

It is not hard to see that if P is a p-group, then it is nilpotent. In fact, nilpotency can be characterized in terms of the Sylow subgroups.

THEOREM 1.6. *Let G be a group. Then, the following are equivalent:*

(i) G is nilpotent.

(ii) If $H < G$ then $H < \mathbf{N}_G(H)$.

(iii) Every maximal subgroup of G is normal in G.

(iv) Every Sylow subgroup of G is normal in G.

Since normal subgroups that intersect trivially commute, we have that if G is nilpotent then the Sylow subgroups for different primes commute. Consequently, if x and y are elements with coprime order, then x and y commute.

We close this section with a classical result of Wielandt [128]. This result will be useful for proving some of our man results.

THEOREM 1.7 (Wielandt). *Let π be a set of primes and let G be a group. If there exists a nilpotent group $H \in \mathrm{Hall}_\pi(G)$, then $G \in D_\pi$.*

Thus, if G has a nilpotent Hall π-subgroup, then the Hall π-subgroups of G behave as Sylow subgroups. There are several results in the literature on the existence of abelian or nilpotent Hall subgroups in groups. For example, [7, Theorem B] states that if G is a group and π a set of primes, then G has nilpotent Hall π-subgroups if and only if, for every pair of distinct primes $p, q \in \pi$, the class sizes of the p-elements of G are not divisible by q. Moreover, [94, Theorem D] shows that G has a nilpotent Hall π-subgroup if and only if for every pair of distinct primes $p, q \in \pi$, and given a p-element $x \in G$, and a q-element $y \in G$, we have that q divides $o(xy)$.

1.3. Some special subgroups

In this section, we introduce some special subgroups that we will need throughout this thesis. We are particularly interested in self-centralizing normal subgroups; that is, normal subgroups N of G such that $\mathbf{C}_G(N) \leqslant N$. All subgroups introduced in this section are characteristic.

Let G be a group and let π be a set of primes. We observe that the product of two normal π-subgroups is again a normal π-subgroup and hence the following is well defined.

DEFINITION. Let G be a group. We write $\mathbf{O}_\pi(G)$ to denote the largest normal π-subgroup of G.

DEFINITION. Let G be a group. We set

$$\mathbf{F}(G) = \mathbf{O}_{p_1}(G)\mathbf{O}_{p_2}(G)\dots\mathbf{O}_{p_k}(G),$$

where $\{p_1, p_2, \dots, p_k\}$ is the set of primes dividing $|G|$. The group $\mathbf{F}(G)$ will be called the **Fitting subgroup** of G.

If p and q are two distinct prime divisors of $|G|$, then $\mathbf{O}_p(G)$ and $\mathbf{O}_q(G)$ are two normal subgroups with coprime orders, and hence they commute. Thus, the product defining $\mathbf{F}(G)$ is a direct product. It is not hard to prove that $\mathbf{F}(G)$ is the largest normal and nilpotent subgroup of G.

DEFINITION. Let G be a group. We define the **Frattini subgroup** of G to be the intersection of all maximal subgroups of G. We will denote it by $\Phi(G)$.

We collect some results on the Frattini subgroup that we will use. These results have been retrieved from [52]. The author would like to thank Chris Schroeder for a translated version of this book.

THEOREM 1.8. *Let G be a group. Then the following hold:*

(i) $\Phi(G)$ is nilpotent. In particular $\Phi(G) \leqslant \mathbf{F}(G)$.

(ii) Assume that G is a p-group for a prime p. If $|G/\Phi(G)| = p^d$, then every minimal generating set of G contains exactly d elements.

(iii) G is nilpotent if and only if $G/\Phi(G)$ is nilpotent.

(iv) G is supersolvable if and only if $G/\Phi(G)$ is supersolvable.

PROOF. Statements (i) to (iv) are [**52**, Satz III.3.6, Satz III.3.15, Satz III.3.7, Satz VI.8.6(a)], respectively. □

Moreover, when G is solvable, we have the following property of $\mathbf{F}(G)$.

THEOREM 1.9. *Let G be a solvable group. Then $\mathbf{C}_G(\mathbf{F}(G)) \leqslant \mathbf{F}(G)$.*

PROOF. This is [**38**, Theorem 6.1.3]. □

This result has a generalization to π-separable groups. The following result is known as Hall–Higman's Lemma 1.2.3.

THEOREM 1.10 (Hall and Higman). *Let G be a π-separable group with $\mathbf{O}_{\pi'}(G) = 1$, then $\mathbf{C}_G(\mathbf{O}_\pi(G)) \leqslant \mathbf{O}_\pi(G)$.*

PROOF. This is [**44**, Lemma 1.2.3]. □

Note that if G is π-separable, then $G/\mathbf{O}_{\pi'}(G)$ is a π-separable group such that $\mathbf{O}_{\pi'}(G/\mathbf{O}_{\pi'}(G))$ is trivial. Thus, we can find a group with a non-trivial self-centralizing normal subgroup.

We say that a group K is **quasisimple** if K is a perfect group and $K/\mathbf{Z}(K)$ is a non-abelian simple group. Given a simple group S, there exists a unique abelian group $M(S)$ and a unique quasisimple group $\Gamma(S)$ such that $\mathbf{Z}(\Gamma(S)) \cong M(S)$, $\Gamma(S)/\mathbf{Z}(\Gamma(S)) \cong S$ and if K is any quasisimple group with $K/\mathbf{Z}(K) \cong S$, then $1 \leqslant \mathbf{Z}(K) \leqslant M(S)$ and K is an epimorphic image image of $\Gamma(S)$. The group $M(S)$ is called the **Schur multiplier** of S and $\Gamma(S)$ is called the **universal cover** of S.

DEFINITION. We say that $H \leqslant G$ is **subnormal** in G if there exists a chain of subgroups

$$H = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_n = G.$$

DEFINITION. Let G be a group. A subnormal quasisimple subgroup of G is said to be a **component** of G. We define the **layer** of G as the product of all components of G. We will write $\mathbf{E}(G)$ to denote it.

It is possible to prove that the components of G centralize each other.

DEFINITION. Let G be a group. We define the **generalized Fitting subgroup** of G by

$$\mathbf{F}^*(G) = \mathbf{F}(G)\mathbf{E}(G).$$

THEOREM 1.11. *Let G be a group. Then $\mathbf{C}_G(\mathbf{F}^*(G)) \leqslant \mathbf{F}^*(G)$. Moreover, $\mathbf{F}^*(G) = \mathbf{F}(G)$ if and only if $\mathbf{C}_G(\mathbf{F}(G)) \leqslant \mathbf{F}(G)$.*

PROOF. The first part is [**54**, Theorem 9.8] and the second is [**54**, Corollary 9.9]. □

We finish this chapter with a result that describes the structure of G for groups without non-trivial solvable normal subgroups (see, for example, [**90**, Theorem 2.2]).

THEOREM 1.12. *Let G be a group without non-trivial solvable normal subgroups.*

(i) We have $\mathbf{F}^*(G) = S_1^{n_1} \times \cdots \times S_f^{n_f}$, where each n_i is positive and the S_i are non-isomorphic non-abelian simple groups.

(ii) We have $G \leqslant \Gamma = N \rtimes H$, where $N = \mathrm{Aut}(S_1)^{n_1} \times \cdots \times \mathrm{Aut}(S_f)^{n_f}$ and $H = \mathrm{Sym}(n_1) \times \cdots \times \mathrm{Sym}(n_f)$ acts on N by permuting the copies of $\mathrm{Aut}(S_i)$.

(iii) If $K = G \cap N$, then G/K acts on $\mathbf{F}^*(G)$ by permuting the simple direct factors.

CHAPTER 2

Character theory

In this thesis, our character-theoretic notation follows [53] and [99].

2.1. Definitions and basics

Let G be a group and let F be a field. We denote by FG the set

$$FG = \{\sum_{g\in G} a_g g \mid a_g \in F\}.$$

The structure of F-vector space is given to FG by

$$f \sum_{g\in G} a_g g = \sum_{g\in G} f a_g g$$

for $f \in F$ and

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g.$$

We may identify the elements $g \in G$ with the sum $\sum_{h\in G} a_h h$ where $a_g = 1$ and $a_h = 0$ for all $h \neq g$, and in fact the elements of G form a basis for FG. Finally, to define multiplication in FG we use the product in G for the elements of the basis and extend linearly to FG. Thus FG is an F-algebra, which we call the **group algebra**.

An **F-representation** of G is a group homomorphism

$$\mathcal{X} : G \to \mathrm{GL}(n, F).$$

The integer n is the **degree** of $\mathcal{X}$. By extending linearly, we obtain an algebra homomorphism $FG \to \mathrm{Mat}(n, F)$. Conversely, an algebra homomorphism $FG \to \mathrm{Mat}(n, F)$ defines an F-representation of G by restriction. Two F-representations $\mathcal{X}$ and $\mathcal{Y}$ are said to be **similar** if there exists $M \in \mathrm{GL}(n, F)$ such that $\mathcal{X}(g) = M^{-1}\mathcal{Y}(g)M$ for all $g \in G$.

We say that an F-representation $\mathcal{X}$ is **irreducible** if it is not similar to a representation of G which can be written in block form as

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

The F**-character** afforded by an F-representation $\mathcal{X}$ is defined by $\chi(g) = \mathrm{tr}(\mathcal{X}(g))$ for all $g \in G$, where $\mathrm{tr}(A)$ denotes the trace of the square matrix A. We say that an F-character is **irreducible** if it is afforded by some irreducible F-representation. The integer $\chi(1)$ is the **degree** of χ (which is precisely the degree of $\mathcal{X}$ when the characteristic of F is 0). It follows easily from the definitions that F-characters are constant on the conjugacy classes of G. Furthermore, similar F-representations afford the same F-character.

If $\mathcal{Y}$ and $\mathcal{Z}$ are F-representations of G, then the map defined as

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

is an F-representation of G which we call the **sum** of $\mathcal{Y}$ and $\mathcal{Z}$. It follows easily that sums of F-characters are F-characters.

From now on we fix $F = \mathbb{C}$. We denote by $\mathrm{Irr}(G)$ the set of irreducible complex characters (we often omit the word *complex* and just say irreducible character). We also denote by $\mathrm{Char}(G)$ the set of characters of G. The map

$$\begin{aligned} 1_G : G &\to \mathbb{C}^\times \\ g &\mapsto 1 \end{aligned}$$

is a character of G, called the **trivial** or **principal** character. A character of degree 1 is called a **linear** character. Clearly, linear characters are irreducible. We denote by $\mathrm{Lin}(G)$ the set of linear characters of G. Notice that if λ is a linear character then λ is a group homomorphism $\lambda : G \to \mathbb{C}^\times$. It is easy to check that $\mathrm{Lin}(G)$ is an abelian group with multiplication given by $(\lambda\mu)(g) = \lambda(g)\mu(g)$ for all $g \in G$.

We denote by $\mathrm{cf}(G)$ the set of maps $G \to \mathbb{C}$ that are constant on the conjugacy classes of G (we call these maps **class functions**). It is easy to see that $\mathrm{cf}(G)$ is a $\mathbb{C}$-vector space.

We can define a hermitian inner product on $\mathrm{cf}(G)$ as follows. If α and β are class functions, then

$$[\alpha, \beta] = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{\beta(g)}$$

where $\overline{\beta(g)}$ denotes the complex conjugate of $\beta(g)$. The following is a fundamental theorem in character theory.

THEOREM 2.1. *The set* $\mathrm{Irr}(G)$ *is an orthonormal basis of* $\mathrm{cf}(G)$. *In particular,* $|\mathrm{Irr}(G)|$ *equals the number of conjugacy classes of* G.

PROOF. This is [**53**, Theorem 2.8] and the First Orthogonality Relation ([**53**, Corollary 2.14]). □

If χ is a character of G, then by Theorem 2.1 we may write

$$\chi = \sum_{\psi \in \mathrm{Irr}(G)} [\chi, \psi]\psi.$$

The characters $\psi \in \mathrm{Irr}(G)$ such that $[\chi, \psi] \neq 0$ are called the **irreducible constituents** of χ, and $[\chi, \psi]$ is the **multiplicity** of ψ in χ.

Let $\mathrm{Cl}(G) = \{K_1, \ldots, K_k\}$ be the set of conjugacy classes of G. Let $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$ and let $g_j \in K_j$. Another consequence of Theorem 2.1 is that the square matrix

$$X(G) = (\chi_i(g_j))$$

is an invertible matrix. We call $X(G)$ the **character table** of G.

2.2. Induction and restriction of characters

Let H be a subgroup of G and $\alpha \in \mathrm{cf}(H)$. Define the map $\alpha^\circ : G \to \mathbb{C}$ as $\alpha^\circ(x) = \alpha(x)$ if $x \in H$ and $\alpha^\circ(x) = 0$ otherwise.

Definition. The **induced** class function α^G is the map $\alpha^G : G \to \mathbb{C}$ defined by

$$\alpha^G(x) = \frac{1}{|H|} \sum_{g \in G} \alpha^\circ(gxg^{-1}).$$

It follows directly from the definition that α^G is a class function of G, and that $\alpha^G(1) = |G : H|\alpha(1)$.

Definition. If $\alpha \in \mathrm{cf}(G)$, then the **restriction** of α to H is defined by

$$\alpha_H(x) = \alpha(x)$$

for all $x \in H$.

Again, it is straightforward to check that α_H is a class function of H, and that if $\alpha \in \mathrm{Char}(G)$ then $\alpha_H \in \mathrm{Char}(H)$. The following easy result gives a relation between induction and restriction.

Theorem 2.2 (Frobenius reciprocity). *Let $\alpha \in \mathrm{cf}(H)$ and $\beta \in \mathrm{cf}(G)$. Then $[\alpha^G, \beta] = [\alpha, \beta_H]$.*

Proof. See [**53**, Lemma 5.2]. □

It follows that if $\alpha \in \mathrm{Char}(H)$ then $\alpha^G \in \mathrm{Char}(G)$.

2.3. Factor groups

DEFINITION. Let χ be a character of G. Then the **kernel** of χ is

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

A character with trivial kernel is said to be **faithful**.

LEMMA 2.3. *Let $\mathcal{X}$ be a representation of G affording the character χ. Then* $\ker(\chi) = \ker(\mathcal{X})$.

PROOF. See [**53**, Lemma 2.19]. □

THEOREM 2.4. *Let G be a group and $N \trianglelefteq G$. Then*

(i) *If $\chi \in \mathrm{Char}(G)$ and $N \leqslant \ker(\chi)$ then $\chi(gn) = \chi(g)$ for all $g \in G$, $n \in N$. Moreover, the function $\hat{\chi}$ on N/G defined by $\chi(gN) = \chi(g)$ is a character of G/N.*

(ii) *If $\hat{\chi} \in \mathrm{Char}(G/N)$, then the function χ on G defined by $\chi(g) = \hat{\chi}(gN)$ is a character in G with $N \leqslant \ker(\chi)$.*

(iii) *In both (i) and (ii), $\chi \in \mathrm{Irr}(G)$ if and only if $\hat{\chi} \in \mathrm{Irr}(G/N)$.*

PROOF. This [**53**, Lemma 2.22]. □

For the remainder, we will identify $\mathrm{Irr}(G/N)$ with the set $\{\chi \in \mathrm{Irr}(G) \mid N \leqslant \ker(\chi)\}$. As a consequence, we have the following corollary.

COROLLARY 2.5. *Let G be a group. Then*

(i) $G' = \bigcap\{\ker(\lambda) \mid \lambda \in \mathrm{Irr}(G), \lambda(1) = 1\}$.

(ii) $|G : G'| = |\{\lambda \in \mathrm{Irr}(G) \mid \lambda(1) = 1\}|$.

PROOF. This is [**53**, Corollary 2.23]. □

2.4. Normal subgroups

Let $N \trianglelefteq G$ and $\theta \in \mathrm{cf}(N)$. If $g \in G$ then we define θ^g by $\theta^g(n) = \theta(gng^{-1})$ for all $n \in N$. If $\theta \in \mathrm{Char}(N)$ is afforded by the representation $\mathcal{X}$ then $\theta^g \in \mathrm{Char}(N)$ is the character afforded by the representation $\mathcal{X}^g$ defined by $\mathcal{X}^g(n) = \mathcal{X}(gng^{-1})$ for all $n \in N$. In this case, we say that θ and θ^g are **conjugate** characters in G. We have that G acts on $\mathrm{Char}(N)$ and $\mathrm{Irr}(N)$ by conjugation.

THEOREM 2.6 (Clifford). *Let $\chi \in \mathrm{Irr}(G)$ and let $\theta \in \mathrm{Irr}(N)$ be an irreducible constituent of χ_N. Let $\{\theta_1, \dots, \theta_t\}$ be the set of G-conjugates of θ. Then*

$$\chi_N = e \sum_{i=1}^{t} \theta_i,$$

where $e = [\chi_N, \theta]$.

PROOF. This is [**53**, Theorem 6.2] □

Let $\theta \in \mathrm{Irr}(N)$. We denote by $\mathrm{Irr}(G|\theta)$ the set of irreducible characters of G whose restriction to N contains θ as an irreducible constituent. Notice that by Frobenius reciprocity, $\mathrm{Irr}(G|\theta)$ consists of the irreducible constituents of θ^G.

In addition, we denote by $\mathrm{Irr}(G|N)$ the set of irreducible characters of G whose restriction to N contains some non-principal irreducible component. Notice that $\mathrm{Irr}(G) = \mathrm{Irr}(G/N) \cup \mathrm{Irr}(G|N)$.

If $\theta \in \mathrm{Irr}(N)$ we denote by $I_G(\theta) = \{g \in G \mid \theta^g = \theta\}$ the **inertia subgroup** of θ in G. By the orbit-stabilizer Theorem $|G : I_G(\theta)| = t$, using the notation of the previous theorem. The following result relates $\mathrm{Irr}(I_G(\theta)|\theta)$ and $\mathrm{Irr}(G|\theta)$.

THEOREM 2.7 (Clifford Correspondence). *Let $N \trianglelefteq G$ and let $\theta \in \mathrm{Irr}(N)$. Then the map $\psi \mapsto \psi^G$ defines a bijection $\mathrm{Irr}(I_G(\theta)|\theta) \to \mathrm{Irr}(G|\theta)$.*

PROOF. This is [**53**, Theorem 6.11]. □

In the situation above, we say $\psi \in \mathrm{Irr}(I_G(\theta)|\theta)$ and $\psi^G \in \mathrm{Irr}(G|\theta)$ are **Clifford correspondents**.

Suppose that $\chi \in \mathrm{Irr}(G)$ is such that $\chi_N = \theta \in \mathrm{Irr}(N)$. Then we say that χ is an **extension** of θ to G, or that θ **extends** to G. In this situation, we have full control of the set $\mathrm{Irr}(G|\theta)$ via the following correspondence.

THEOREM 2.8 (Gallagher correspondence). *Let $N \trianglelefteq G$. Suppose $\chi \in \mathrm{Irr}(G)$ is such that $\chi_N = \theta \in \mathrm{Irr}(N)$. Then the map*

$$\begin{aligned} \mathrm{Irr}(G/N) &\to \mathrm{Irr}(G|\theta) \\ \beta &\mapsto \beta\chi \end{aligned}$$

is a well-defined bijection.

PROOF. This is [**53**, Theorem 6.17]. □

There are results that guarantee that, under certain conditions, a G-invariant character of a normal subgroup extends to the group. We introduce some notation and terminology.

Let $\chi \in \mathrm{Irr}(G)$ be afforded by a representation $\mathfrak{X}$. We define the **determinant** of χ as $\det(\chi) : G \to \mathbb{C}$ by $\det(\chi)(g) = \det(\mathfrak{X}(g))$. Since $\det(\chi)$ is the composition of two homomorphisms, then it is a homomorphism (equivalently, a linear character). It is possible to see that $\det(\chi)$ does not depend on the representation $\mathfrak{X}$ affording χ. We define the **determinantal order** of χ (sometimes called just the order of χ) as the order of $\det(\chi)$ as an element of the group $\mathrm{Lin}(G)$. That is $o(\chi) = o(\det(\chi))$. The determinants of characters are very relevant for deciding the extendibility of characters in normal subgroups.

THEOREM 2.9 (Gallagher). *Let $N \trianglelefteq G$ and let $\theta \in \mathrm{Irr}(N)$ be G-invariant. Suppose that $\gcd(|G : N|, \theta(1)) = 1$. Then θ is extendible if and only if $\det(\theta)$ is extendible.*

PROOF. This is [**53**, Theorem 8.15]. □

THEOREM 2.10. *Let $N \trianglelefteq G$ and let $\theta \in \mathrm{Irr}(N)$ be G-invariant. If $\gcd(|G : N|, o(\theta)\theta(1)) = 1$, then there exists a unique $\chi \in \mathrm{Irr}(G)$ such that $\chi_N = \theta$ and $o(\chi) = o(\theta)$.*

PROOF. This is [**53**, Corollary 8.16]. □

The extension χ in Theorem 2.10 is usually called the **canonical extension** of θ. We notice that, since both $o(\theta)$ and $\theta(1)$ divide $|N|$, the condition $\gcd(|G : N|, o(\theta)\theta(1)) = 1$ is satisfied trivially provided that $\gcd(|G : N|, |N|) = 1$.

THEOREM 2.11. *Let $N \trianglelefteq G$, let $\theta \in \mathrm{Irr}(N)$ be G-invariant and assume that G/N is cyclic. Then θ extends to G.*

PROOF. This is [**99**, Theorem 5.1]. □

2.5. Fields of values

We begin this section with a result on the values of irreducible characters.

LEMMA 2.12. *Let $\mathcal{X}$ be a representation of G affording the character χ. Let $g \in G$, let $n = o(g)$ and let $f = \chi(1)$. Then*

(i) $\mathcal{X}(g)$ is equivalent to to a matrix $\mathrm{diag}(\epsilon_1, \ldots, \epsilon_f)$.

(ii) $\epsilon_i^n = 1$ for every $1 \leqslant i \leqslant f$.

(iii) $\chi(g) = \sum_{i=1}^{f} \epsilon_i$ and $|\chi(g)| \leqslant \chi(1)$.

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

PROOF. This is [**53**, Lemma 2.15]. □

Given an integer $n \geqslant 1$, we denote $\mathbb{Q}_n = \mathbb{Q}(e^{2\pi i/n})$. From Lemma 2.12, we deduce that all entries of the character table of G are contained in $\mathbb{Q}_{\exp(G)}$, where $\exp(G)$ denotes the exponent of G. This Lemma motivates the definition of fields of values of characters and classes.

If χ is a character of G and $K \in \mathrm{Cl}(G)$, then we define $\chi(K) = \chi(g)$ for any $g \in K$. Given a character χ of G (not necessarily irreducible), we can associate a finite extension of $\mathbb{Q}$ to χ, namely the field generated by the values $\chi(K)$ for K in $\mathrm{Cl}(G)$. We denote this extension by

$$\mathbb{Q}(\chi) = \mathbb{Q}(\chi(K) \mid K \in \mathrm{Cl}(G)).$$

The extension $\mathbb{Q}(\chi)$ is called **the field of values of** χ.

Analogously, given $K \in \mathrm{Cl}(G)$, we define the **field of values of** K as the field extension of $\mathbb{Q}$ generated by the values $\chi(K)$, where χ runs through $\mathrm{Irr}(G)$. That is

$$\mathbb{Q}(K) = \mathbb{Q}(\chi(K) \mid \chi \in \mathrm{Irr}(G)).$$

Let $K \in \mathrm{Cl}(G)$ and $g \in K$. Since $\chi(g)$ can be expressed as the sum of $o(g)$-th roots of the unity for any $\chi \in \mathrm{Irr}(G)$, we have that $\mathbb{Q}(K) = \mathbb{Q}(g) \subseteq \mathbb{Q}_{o(g)}$.

Finally, we define the **field of values of** G as the field generated by the values $\chi(K)$ where χ runs through $\mathrm{Irr}(G)$ and K runs through $\mathrm{Cl}(G)$. This is

$$\mathbb{Q}(G) = \mathbb{Q}(\chi(K) \mid \chi \in \mathrm{Irr}(G), K \in \mathrm{Cl}(G)).$$

By the previous observations, we have that $\mathbb{Q}(G) \subseteq \mathbb{Q}_{\exp(G)}$, where $\exp(G)$ denotes the exponent of G.

As a consequence, if χ is a character of G (not necessarily irreducible) and $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$, we can define χ^σ by $\chi^\sigma(g) = \chi(g)$ for every $g \in G$. It is possible to prove that χ^σ is a character and that χ^σ is irreducible if and only if χ is irreducible. With this, we have an action of $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ on $\mathrm{Irr}(G)$.

Let ϵ be a $|G|$-th primitive root of unity. Then each $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ is determined by the unique r such that $0 < r < |G|$, $\gcd(r, |G|) = 1$ and $\sigma(\epsilon) = \epsilon^r$. Therefore, $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ acts on G and on $\mathrm{Cl}(G)$ as $g^\sigma = g^r$ and $(g^G)^\sigma = (g^r)^G$. Using this action we can prove the following.

LEMMA 2.13. *Let $g \in G$ and let j be a positive integer. Then $\mathbb{Q}(g^j) \subseteq \mathbb{Q}(g)$.*

PROOF. Let n be the exponent of G and let ϵ be a primitive n-th root of unity. We claim that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(g)) \leqslant \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(g^j))$. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(g))$. Assume that $\sigma(\epsilon) = \epsilon^r$ for $0 < r < |G|$ and $\gcd(r, |G|) = 1$. Since $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(g))$,

we have that $(g^G)^\sigma = g^G$. Thus, g^r is conjugate to g. It follows that $(g^j)^r$ is conjugate to g^j and hence $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(g^j))$. The claim follows.

Therefore, $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(g)) \leqslant \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(g^j))$ and hence $\mathbb{Q}(g^j) \subseteq \mathbb{Q}(g)$. □

The groups `SmallGroup(32,42)` and `SmallGroup(32,15)` in the `SmallGroup` database in GAP [**33**] show that the actions of $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ on $\mathrm{Irr}(G)$ and on $\mathrm{Cl}(G)$ are not permutation isomorphic. However, we have Brauer's Theorem, which will relate both actions.

THEOREM 2.14 (Brauer). *Let G be a group and suppose that the group A acts on $\mathrm{Irr}(G)$ and on $\mathrm{Cl}(G)$. Assume that the actions are compatible, in the sense that for every $\alpha \in A$ we have $\chi^\alpha(g^\alpha) = \chi(g)$ for every $g \in G$ and for every $\chi \in \mathrm{Irr}(G)$. Then the number of elements of $\mathrm{Irr}(G)$ fixed by α is equal to the number of elements of $\mathrm{Cl}(G)$ fixed by α.*

PROOF. This is [**53**, Theorem 6.32]. □

It is easy to see that the actions of $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ on $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$ satisfy the compatibility condition in Theorem 2.14. Next result shows that, under the same compatibility condition in Theorem 2.14, the number of orbits in the action of A on $\mathrm{Irr}(G)$ is equal to the number of orbits in the action of A on $\mathrm{Cl}(G)$. To prove this, we will use a classical formula for the number of orbits in an action of a group on a set (see [**109**, Theorem 3.22], for a modern proof). This formula is sometimes attributed to Burnside, but it is known that this result was previously known by Cauchy and Frobenius (see [**101**]). For this reason, we will refer to this formula as the Orbit-Counting Lemma.

COROLLARY 2.15 (Brauer). *Let G be a group and suppose that the group A acts on $\mathrm{Irr}(G)$ and on $\mathrm{Cl}(G)$. Assume that the actions are compatible, in the sense that for every $\alpha \in A$ we have $\chi^\alpha(g^\alpha) = \chi(g)$ for every $g \in G$ and for every $\chi \in \mathrm{Irr}(G)$. Then the number of orbits in the action of A on $\mathrm{Irr}(G)$ is equal to the number of orbits in the action of A on $\mathrm{Cl}(G)$.*

PROOF. By the Orbit-Counting Lemma [**109**, Theorem 3.22], we have that the number of orbits of a group H acting on a set X equals to

$$\frac{1}{|H|} \sum_{h \in H} |\{x \in X \mid h \cdot x = x\}|.$$

Thus, the result follows by combining Orbit-Counting Lemma with Theorem 2.14. □

Following [**23**], we define the k-semi-rational groups as follows.

DEFINITION. Let G be a group, let $g \in G$ and let $k \geqslant 1$ be an integer. Then $g \in G$ is said to be **k-semi-rational** if $|\mathbb{Q}(g) : \mathbb{Q}| \leqslant k$. The group G is said to be k-semi-rational if all its elements are k-semi-rationals.

For $k = 1$ we say that the element (or the group) is rational and for $k = 2$ we say that the element (or the group) is semi-rational. We also present the dual definition for characters.

DEFINITION. Let G be a group and let $k \geqslant 1$ be an integer. We will say that G is **k-rational** if $|\mathbb{Q}(\chi) : \mathbb{Q}| \leqslant k$ for every $\chi \in \mathrm{Irr}(G)$.

We observe that the 1-rational groups are precisely the rational groups. Moreover, we say that a group is quadratic rational if it is 2-rational. Next remark will allow us to understand k-semi-rationality from a different point of view.

REMARK 2.16. Given $g \in G$, we define $B_G(g) = \mathbf{N}_G(\langle g \rangle)/\mathbf{C}_G(g)$. We observe that $B(G)$ is naturally embedded in $\mathrm{Aut}(\langle g \rangle)$. Moreover, $|B_G(g)| = |\mathrm{Gal}(\mathbb{Q}_{o(g)}/\mathbb{Q}(g))|$ by [**99**, Theorem 3.11]. Since $\mathrm{Aut}(\langle g \rangle) \cong \mathrm{Gal}(\mathbb{Q}_{o(g)}/\mathbb{Q})$, we deduce that $|\mathbb{Q}(g) : \mathbb{Q}| = |\mathrm{Aut}(\langle g \rangle) : B_G(g)|$. As a consequence, $g \in G$ is k-semi-rational if and only if $|B_G(g)| \geqslant \varphi(o(g))/k$, where φ denotes Euler's totient function. Moreover, this happens if and only if there exist $r_1, \ldots, r_k \in \{0, \ldots, o(g)-1\}$ such that, any generator of $\langle g \rangle$ is conjugated to g^{r_i} for some i.

DEFINITION. We say that $x \in G$ is **inverse semi-rational** if every generator of $\langle x \rangle$ is conjugated to either x or to x^{-1}. A group is said to be inverse semi-rational if all its elements are inverse semi-rational.

We remark that many authors refer the inverse semi-rational groups as **cut** groups. It is possible to decide whether a group is inverse semi-rational by looking at the fields of values of its irreducible characters. The following is [**4**, Proposition 2.1].

PROPOSITION 2.17. *Let G be a group. Then the following are equivalent:*

(i) G is inverse semi-rational.

(ii) For any $x \in G$, we have that either $\mathbb{Q}(x) = \mathbb{Q}$ or $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{-d})$ for some $d \geqslant 1$.

(ii) For any $\chi \in \mathrm{Irr}(G)$, we have that either $\mathbb{Q}(\chi) = \mathbb{Q}$ or $\mathbb{Q}(\chi) = \mathbb{Q}(\sqrt{-d})$ for some $d \geqslant 1$.

In particular, inverse semi-rational groups are both quadratic rational and semi-rational.

In the case of a solvable group G, the properties of k-rationality and k-semi-rationality provide much information about the set of prime divisors of $|G|$. Given a group G, we write $\pi(G)$ to denote the set of prime divisors of $|G|$. The following result is a compilation of results in [**3**, **23**, **39**, **120**].

THEOREM 2.18. *Let G be a solvable group. Then*

(i) If G is rational, then $\pi(G) \subseteq \{2, 3, 5\}$.

(ii) If G is semi-rational, then $\pi(G) \subseteq \{2, 3, 5, 7, 13, 17\}$.

(iii) If G is quadratic rational, then $\pi(G) \subseteq \{2, 3, 5, 7, 13\}$.

(iv) If G is inverse semi-rational, then $\pi(G) \subseteq \{2, 3, 5, 7\}$.

PROOF. (i) is [**39**, Corollary], (ii) is [**23**, Theorem 2], (iii) is [**120**, Theorem A] and (iv) is [**3**, Theorem 1.2]. □

It is not known whether there exists a semi-rational solvable group whose order is divisible by 17. Apart from this case, all other primes are necessary. As we pointed in the Introduction, Problem 2 of [**23**] asks whether it is possible to bound the prime divisors of solvable k-semi-rational groups in terms of k.

CONJECTURE 2.19 (Problem 2 of [**23**]). *Let $k \geqslant 1$ and let G be a solvable k-semi-rational group. Then $|\pi(G)|$ is bounded in terms of k.*

The dual version for solvable k-rational groups was proved by Tent [**120**].

THEOREM 2.20 (Tent). *There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that if G is a solvable k-rational group for $k \geqslant 1$, and $p \in \pi(G)$, then $p \leqslant f(k)$.*

PROOF. This is [**120**, Theorem C]. □

We observe that these results cannot be extended to non-solvable groups. Let $n \geqslant 1$, and let $x \in \mathsf{S}_n$. If $\gcd(m, o(x)) = 1$, then x and x^m have the same cycle structure and hence they are conjugated. It follows that $\mathbb{Q}(x) = \mathbb{Q}$ for any $x \in \mathsf{S}_n$. Thus, S_n is a rational group for any n and we conclude that it is impossible to bound the primes dividing the size of a non-solvable group in terms of its fields of values. However, there are many results studying their structure. A classical example is the following result from [**121**].

THEOREM 2.21 (Thompson). *Let G be a rational group. If p is a prime such that G has a composition factor of order p, then $p \leqslant 11$.*

This result is the case $k = 1$ of the following conjecture proposed by Moretó [**89**, Conjecture D].

CONJECTURE 2.22 (Moretó). *Let G be a k-rational group. If p is a prime such that G has a composition factor of order p, then p is k-bounded.*

The case $k = 2$ of this conjecture remains open. On the other hand, Trefethen [**124**, Theorem 1.2] classified the non-alternating composition factor of quadratic rational groups.

THEOREM 2.23 (Trefethen). *Let G be a quadratic rational group and let S be a non-abelian composition factor of G. Then one of the following holds:*

(i) $S = \mathsf{A}_n$ *for some* $n \geqslant 5$.

(ii) S *is contained in a finite and explicit set of non-alternating simple groups.*

We remark that all groups appearing in Theorem 2.23 can actually occur as a composition factor of a quadratic rational group. From Theorem 2.23, Moretó [**89**, Theorem C] proved the following result.

THEOREM 2.24 (Moretó). *Let G be a k-rational group. Let q be the largest prime divisor of the orders of the non-cyclic composition factors of G. If p is a prime divisor of $|G|$ then $p \leqslant \max\{q, 240k^2 + 1\}$. If moreover $k = 2$, then $p \leqslant \max\{q, 241\}$.*

There exists a common ingredient in the proofs of many of these results. In many cases, they use the techniques developed in [**29**], especially the concept of h-eigenvalue property. We will also use these techniques in Chapter 3 of this work.

2.6. Rational classes and characters

Let $\mathbb{F}$ be a field extension of $\mathbb{Q}$. We define

$$\mathrm{Cl}_{\mathbb{F}}(G) = \{K \in \mathrm{Cl}(G) \mid \mathbb{Q}(K) \subseteq \mathbb{F}\}$$

and

$$\mathrm{Irr}_{\mathbb{F}}(G) = \{\chi \in \mathrm{Irr}(G) \mid \mathbb{Q}(\chi) \subseteq \mathbb{F}\}.$$

It is easy to see that $\chi \in \mathrm{Irr}_{\mathbb{R}}(G)$ and $K \in \mathrm{Cl}_{\mathbb{R}}(G)$ if and only if they are fixed by σ, where σ denotes the complex conjugation automorphism. Thus, using Theorem 2.14, we deduce that $|\mathrm{Cl}_{\mathbb{R}}(G)| = |\mathrm{Irr}_{\mathbb{R}}(G)|$.

In a similar way, we notice that $\chi \in \mathrm{Irr}_{\mathbb{Q}}(G)$ and $K \in \mathrm{Cl}_{\mathbb{Q}}(G)$ if and only if they are fixed points of the respective actions of $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$. In general, $|\mathrm{Irr}_{\mathbb{Q}}(G)| \neq |\mathrm{Cl}_{\mathbb{Q}}(G)|$. For example the `SmallGroup(32,42)` group in GAP [**33**] has 10 rational characters and 8 rational classes, while the group `SmallGroup(32,15)` has 6 rational characters and 4 rational classes.

The study of groups with few rational classes or characters will be important for the purpose of this work. The main results in [100] and [110] study the groups with $|\operatorname{Irr}_{\mathbb{Q}}(G)| \leqslant 3$ or $|\operatorname{Cl}_{\mathbb{Q}}(G)| \leqslant 3$. Summarizing the results there we have the following theorem.

THEOREM 2.25 (Navarro and Tiep; Rossi). *Let G be a group. Then the following hold:*

(i) $|\operatorname{Cl}_{\mathbb{Q}}(G)| = 1$ *if and only if* $|\operatorname{Irr}_{\mathbb{Q}}(G)| = 1$ *if and only if* $|G|$ *is odd.*

(ii) $|\operatorname{Cl}_{\mathbb{Q}}(G)| = 2$ *if and only if* $|\operatorname{Irr}_{\mathbb{Q}}(G)| = 2$.

(iii) If $|\operatorname{Cl}_{\mathbb{Q}}(G)| = 3$, *then* $|\operatorname{Irr}_{\mathbb{Q}}(G)| = 3$.

In particular, if $|\operatorname{Cl}_{\mathbb{Q}}(G)| \leqslant 3$, *then* $|\operatorname{Irr}_{\mathbb{Q}}(G)| = |\operatorname{Cl}_{\mathbb{Q}}(G)|$.

It is conjectured that if $|\operatorname{Irr}_{\mathbb{Q}}(G)| = 3$, then $|\operatorname{Cl}_{\mathbb{Q}}(G)| = 3$. Moreover, [110, Theorem C] determines the structure of a possible counterexample to this conjecture. In a similar direction, Souza [118] asked the following question.

QUESTION 2.26. *Let G be a group with $|\operatorname{Irr}_{\mathbb{Q}}(G)| \leqslant 5$. Is it true that $|\operatorname{Cl}_{\mathbb{Q}}(G)| = |\operatorname{Irr}_{\mathbb{Q}}(G)|$?*

In addition, Navarro and Tiep [100, Theorem C] determined the structure of non-solvable groups with exactly two rational characters. Given a group G and a prime p, we write $\mathbf{O}^{p'}(G)$ to denote the smallest normal subgroup N of G such that G/N is a p'-group.

THEOREM 2.27 (Navarro and Tiep). *Let G be a non-solvable group. If G has exactly two irreducible rational characters, then $M/N \cong \operatorname{PSL}(2, 3^{2f+1})$ for some $f \geqslant 1$, where $M = \mathbf{O}^{2'}(G)$ and $N = \mathbf{O}_{2'}(M)$.*

Rossi [110, Theorem B] obtained a similar result for groups with exactly three rational characters.

THEOREM 2.28 (Rossi). *Let G be a non-solvable group with exactly three rational characters. If $M = \mathbf{O}^{2'}(G)$ and $N = \mathbf{O}_{2'}(M)$, then M/N is one of the following groups:*

(i) $\operatorname{PSL}(2, 3^{2f+1})$, *where* $f \geqslant 1$.

(ii) $\operatorname{PSL}(2, q)$, *where* $q \equiv \pm 5 \pmod{24}$.

(iii) $\operatorname{PSL}(2, 2^f)$, *where* $f \geqslant 2$.

(iv) ${}^2B_2(2^{2f+1})$, *where* $f \geqslant 1$.

(v) $\operatorname{SL}(2, 3^{2f+1})$, *where* $f \geqslant 1$.

We restate Theorem 2.28 in a different way (which will be more convenient for its use in this work).

THEOREM 2.29. *Let G be a non-solvable group with exactly three rational characters. If $M = \mathbf{O}^{2'}(G)$, then there exists a solvable normal subgroup $N \lhd G$ such that $N \leqslant M$ and M/N is one the following simple groups:*

(i) $\mathrm{PSL}(2,q)$, *where* $q \equiv \pm 5 \pmod{24}$.

(ii) $\mathrm{PSL}(2,2^f)$, *where* $f \geqslant 2$.

(iii) ${}^2B_2(2^{2f+1})$, *where* $f \geqslant 1$.

(iv) $\mathrm{PSL}(2,3^{2f+1})$, *where* $f \geqslant 1$.

Moreover, if M/N is one of the groups in (i),(ii) or (iii), then $N = \mathbf{O}_{2'}(M)$.

2.7. Modular representations

Richard Brauer introduced the concepts of Brauer characters and blocks as a way to connect representations in characteristic 0 and in prime characteristic. We discuss some basic properties of these objects in this section. Our reference is Chapter 2 of [97].

Let $\mathbf{R}$ denote the ring of algebraic integers in $\mathbb{C}$. If $\chi \in \mathrm{Irr}(G)$ and $g \in G$ then by elementary linear algebra $\chi(g)$ is a sum of roots of unity and therefore irreducible characters take values in $\mathbf{R}$. Let p be a fixed prime and choose a maximal ideal M of $\mathbf{R}$ containing p. Let $F = \mathbf{R}/M$, which is a field of characteristic p, and consider the canonical ring epimorphism $^* : \mathbf{R} \to F$. We set

$$\mathcal{S} = \{\frac{r}{s} \mid r \in \mathbf{R}, s \in \mathbf{R} \backslash M\} \subseteq \mathbb{C}.$$

We have that $\mathcal{S}$ is a ring with $\mathbf{R} \subseteq \mathcal{S}$. We extend $^* : \mathbf{R} \to F$ in the natural way, i.e.

$$\left(\frac{r}{s}\right)^* = r^*(s^*)^{-1}.$$

Let

$$\mathbf{U} = \{\xi \in \mathbb{C} \mid \xi^m = 1 \text{ for some integer } m \text{ not divisible by } p\} \subseteq \mathbf{R}.$$

LEMMA 2.30. *The restriction of * to $\mathbf{U}$ defines an isomorphism $\mathbf{U} \to F^\times$ of multiplicative groups. Also, F is algebraically closed.*

PROOF. See [97, Lemma 2.1]. □

Let G^0 be the set of p'-elements of G. We remark that p'-elements are also called **p-regular**. Suppose $\mathcal{X} : G \to \mathrm{GL}_n(F)$ is an F-representation of G. If $g \in G^0$ then the eigenvalues of $\mathcal{X}(g)$ lie in $F^\times$. By Lemma 2.30, these eigenvalues are of the form $\xi_1^*, \ldots, \xi_n^*$ for unique $\xi_1, \ldots, \xi_n \in \mathbf{U}$. We say the **Brauer character** of G afforded by $\mathcal{X}$ is the map $\varphi : G^0 \to \mathbb{C}$ defined by $\varphi(g) = \xi_1 + \cdots + \xi_n$. We remark that φ is uniquely determined up to choice of the maximal ideal M. We say that φ is **irreducible** if $\mathcal{X}$ is irreducible, and denote the set of irreducible Brauer characters of G by $\mathrm{IBr}(G)$. Brauer characters are also sometimes called **modular characters**.

Exactly as it happens with ordinary characters the sums of Brauer characters are Brauer characters.

THEOREM 2.31. *If p does not divide $|G|$, then $\mathrm{IBr}(G) = \mathrm{Irr}(G)$.*

PROOF. This is [**97**, Theorem 2.12]. □

Let $\mathbb{F}_p$ be the field of p elements. We are interested in the relation between Brauer characters and $\mathbb{F}_p$-representations. The $\mathbb{F}_p$-representations of groups appear in a natural way in the study of groups.

For example, let G be a group and let V be a solvable minimal normal subgroup of G. We know that V is an elementary abelian p-group for some prime p. Thus, V can be viewed as an irreducible G/V-module over $\mathbb{F}_p$. Thus, we can associate an irreducible $\mathbb{F}_p$-representation of G/V to V.

Let $\mathcal{X}$ be a $\mathbb{F}_p$-representation. Let F be as in Lemma 2.30. Then $\mathbb{F}_p \subseteq F$ and hence $\mathcal{X}$ can be realized over F. Let $\mathcal{X}^F$ be the representation $\mathcal{X}$ when we consider it as a representation over F.

LEMMA 2.32. *Let $\mathcal{X}$ be an irreducible $\mathbb{F}_p$-representation of G and let μ be the Brauer character of G afforded by $\mathcal{X}^F$. If $\psi, \phi \in \mathrm{IBr}(G)$ are irreducible constituents of μ, then $\psi^\sigma = \phi$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$. In particular, $\mathbb{Q}(\mu) \subseteq \mathbb{Q}(\phi)$.*

PROOF. This is [**120**, Lemma 3]. □

CHAPTER 3

Fields of values of characters

3.1. Introduction

We recall that given $\chi \in \mathrm{Irr}(G)$, we define the field of values of χ as

$$\mathbb{Q}(\chi) = \mathbb{Q}(\chi(K) \mid K \in \mathrm{Cl}(G)).$$

Analogously, given $K \in \mathrm{Cl}(G)$, we define the field of values of K as

$$\mathbb{Q}(K) = \mathbb{Q}(\chi(K) \mid \chi \in \mathrm{Irr}(G)).$$

As we saw in Sections 2.5 and 2.6, the fields of values provide information on the prime divisors and the structure of groups. In this chapter, we are interested in obtaining versions of Landau's Theorem based on fields of values. We recall the classical result of Landau [**68**].

THEOREM 3.1 (Landau). *Let G be a group. Then $|G|$ is bounded in terms of $k(G)$.*

The classification of groups with $k(G) \leqslant 14$ can be found in [**112**, **126**, **127**]. This classification will be relevant for the results in this chapter.

Given a group G, Moretó [**88**] defined the invariant $f(G)$ as

$$f(G) = \max_{F/\mathbb{Q}} |\{\chi \in \mathrm{Irr}(G) \mid \mathbb{Q}(\chi) = F\}|.$$

The main result of that paper is the following.

THEOREM 3.2 (Moretó). *Let G be a group. Then $|G|$ is bounded in terms of $f(G)$.*

Our goal is to prove a dual version of this result for fields of values of conjugacy classes. For a group G, we define the invariant $h(G)$ by

$$h(G) = \max_{F/\mathbb{Q}} |\{K \in \mathrm{Cl}(G) \mid \mathbb{Q}(K) = F\}|.$$

It is possible to prove that $|\mathbb{Q}(K) : \mathbb{Q}| \leqslant h(G)$ for any $K \in \mathrm{Cl}(G)$ (see Lemma 3.3). The biggest issue with the invariant $h(G)$ is that it does not behave well with respect to quotients. For $f(G)$, we have that $f(G/N) \leqslant f(G)$ for any normal subgroup N of G. However, the same does not hold for $h(G)$. Let us

take $G = \texttt{SmallGroup(32,42)}$ in the `SmallGroup` database in GAP [**33**]. Then $h(G) = 8$ but there exists $N \lhd G$ with $|N| = 2$ and $h(G/N) = 10$. We remark that G is the unique group of order at most 32 such that $h(G/N) > h(G)$ for some normal subgroup N of G. To avoid this issue, we define a slightly stronger invariant.

$$\hat{h}(G) = \max_{N \trianglelefteq G}\{h(G/N)\}.$$

By definition of $\hat{h}(G)$, we have $h(G) \leqslant \hat{h}(G)$ and $\hat{h}(G/N) \leqslant \hat{h}(G)$ for any $N \trianglelefteqslant G$. With this new invariant, we have the following.

THEOREM A. *Let G be a group. Then $|G|$ is $\hat{h}(G)$-bounded.*

We recall that [**23**, Problem 2] asks whether $|\pi(G)|$ is k-bounded for a solvable k-semi-rational group. Theorem 3.8 shows that if that question has a positive answer, then we can replace $\hat{h}(G)$ by $h(G)$ in Theorem A for solvable groups. Conjecture 3.55 of Section 3.5 asks whether it is possible to replace $\hat{h}(G)$ by $h(G)$ for any group G.

It was also proved in [**88**] that $f(G) = 1$ if and only if $G = 1$. The same paper asks for the classification of all groups with $f(G) \in \{2, 3\}$. Our Theorem B provides this classification.

THEOREM B. *Let G be a group. Then*

(i) $f(G) = 2$ *if and only if* $G \in \{\mathsf{C}_2, \mathsf{C}_3, \mathsf{C}_4, \mathsf{D}_{10}, \mathsf{A}_4, \mathsf{C}_7 \rtimes \mathsf{C}_3\}$.

(ii) $f(G) = 3$ *if and only if* $G \in \{\mathsf{S}_3, \mathsf{D}_{14}, \mathsf{D}_{18}, \mathsf{C}_5 \rtimes \mathsf{C}_4, \mathsf{C}_{13} \rtimes \mathsf{C}_4, \mathsf{A}_5, \mathrm{PSL}(2,8), {}^2B_2(8)\}$.

Inspecting the groups arising in Theorem B, we observe that if $f(G) \in \{1, 2, 3\}$, then $h(G) = f(G)$. So we asked whether $f(G) = h(G)$ for all groups with $h(G) \leqslant 3$. Our Theorem C answers this question affirmatively.

THEOREM C. *Let G be a group. If $h(G) \leqslant 3$, then $f(G) = h(G)$.*

We remark that there exist examples of groups with $h(G) \neq f(G)$. Inspecting the groups of order at most 128 (using the `SmallGroup` database in GAP [**33**]), we have not found an example of group with $h(G) \neq f(G)$ such that either $f(G) \leqslant 5$ or $h(G) \leqslant 5$. Thus, it is not clear whether Theorem C is best possible.

3.2. Bounding the size of the group

3.2.1. Preliminaries. In this subsection we present the basic results that will be used in this section. We begin by relating $h(G)$ with the action of $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ on $\mathrm{Cl}(G)$. More precisely, we prove that any group G is $h(G)$-semi-rational.

LEMMA 3.3. *Let $g \in G$. Then $|\mathbb{Q}(g) : \mathbb{Q}| \leqslant h(G)$.*

PROOF. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(g)/\mathbb{Q})$. We can extend σ to an element in $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$. Then $\mathbb{Q}(g) = \mathbb{Q}(g^\sigma)$ and $g^G \neq (g^G)^\sigma$. It follows that there exist at least $|\mathrm{Gal}(\mathbb{Q}(g)/\mathbb{Q})|$ different conjugacy classes with the same field of values. It follows that $|\mathbb{Q}(g) : \mathbb{Q}| = |\mathrm{Gal}(\mathbb{Q}(g)/\mathbb{Q})| \leqslant h(G)$. □

Before continuing, we recall the structure of Galois groups of cyclotomic fields. Let $n = p^a$ for a prime p and an integer $a \geqslant 1$. Then

$$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathsf{C}_{p^{a-1}(p-1)}$$

for $p > 2$ and

$$\mathrm{Gal}(\mathbb{Q}_{2^a}/\mathbb{Q}) \cong \begin{cases} 1 & \text{for } a = 1 \\ \mathsf{C}_2 & \text{for } a = 2 \\ \mathsf{C}_{2^{a-2}} \times \mathsf{C}_2 & \text{for } a \geqslant 3 \end{cases}$$

for $p = 2$. Assume now that $n = p_1^{a_1} \cdots p_t^{a_t}$ for some primes $p_1 < p_2 \ldots < p_t$ and some integers $a_i \geqslant 1$. Then

$$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}_{p_1^{a_1}}/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}_{p_t^{a_t}}/\mathbb{Q}).$$

LEMMA 3.4. *Assume that G is a k-semi-rational group for an integer $k \geqslant 1$. Then $\exp(\mathrm{Gal}(\mathbb{Q}(G)/\mathbb{Q})) \leqslant k!$. In particular, $\exp(\mathrm{Gal}(\mathbb{Q}(G)/\mathbb{Q})) \leqslant h(G)!$ for any group G.*

PROOF. Since G is k-semi-rational, we have that $\mathrm{Gal}(\mathbb{Q}(G)/\mathbb{Q})$ is generated by elements of order at most k. On the other hand, $\mathrm{Gal}(\mathbb{Q}(G)/\mathbb{Q}) \leqslant \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ is a product of cyclic groups. We deduce that $\exp(\mathrm{Gal}(\mathbb{Q}(G)/\mathbb{Q}))$ is at most $k!$. □

Given a group G and a prime p, we write $k_p(G)$ to denote the number of conjugacy classes whose elements are p-elements. The following result bounds $k_p(G)$ in terms of $h(G)$.

LEMMA 3.5. *Let G be a group and let p be a prime divisor of $|G|$. Then $k_p(G) \leqslant 3h(G)^2$ if $p = 2$ and $k_p(G) \leqslant h(G)^2$ if $p > 2$. In particular, if $g \in G$ is an element of order p^a, then $a \leqslant 3h(G)^2$ if $p = 2$ and $a \leqslant h(G)^2$ if $p > 2$.*

PROOF. Let us assume that $\exp(G)$ divides $p^n m$ with $\gcd(p, m) = 1$. It is no loss to assume that $n \geqslant 3$.

Let $x_1, x_2, \ldots, x_t$ be t pairwise non-conjugated p-elements of G. Thus, for any $1 \leqslant i \leqslant t$ we have that $\mathbb{Q} \subseteq \mathbb{Q}(x_i) \subseteq \mathbb{Q}_{p^n}$ and $|\mathbb{Q}(x_i) : \mathbb{Q}| \leqslant h(G)$.

Assume first that $p > 2$. In this case, $\mathrm{Gal}(\mathbb{Q}_{p^n}/\mathbb{Q})$ is cyclic and hence, there exist at most $h(G)$ different fields $\mathbb{F}$ such that $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{Q}_{p^n}$ and $|\mathbb{F} : \mathbb{Q}| \leqslant h(G)$.

Let $\mathbb{F}$ be any of these fields. Then there exist at most $h(G)$ classes whose field of values is $\mathbb{F}$. Thus, $t \leqslant h(G)^2$.

Assume now that $p = 2$. Without loss of generality, we may assume that $n \geqslant 3$. In this case, $\mathrm{Gal}(\mathbb{Q}_{p^n}/\mathbb{Q}) \cong \mathsf{C}_2 \times \mathsf{C}_{2^{n-2}}$ and hence there exist at most $3h(G)$ different fields $\mathbb{F}$ such that $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{Q}_{p^n}$ and $|\mathbb{F} : \mathbb{Q}| \leqslant h(G)$. Thus, reasoning as before, we have $t \leqslant 3h(G)^2$. The claim follows.

The "in particular" part follows from the fact that if $o(g) = p^a$, then $1, g, g^p$, $g^{p^2}, \ldots, g^{p^{a-1}} \in G$ form a system of non-conjugated p-elements (they have pairwise different orders). □

The conclusion of this lemma does not hold if we replace $h(G)$ by the smallest integer k such that G is k-semi-rational. For instance, let p be a prime, let $a \geqslant 1$ and let S_{p^a} be the symmetric group on p^a letters. Then S_{p^a} is rational, but there exists $x \in \mathsf{S}_{p^a}$ of order p^a.

3.2.2. Solvable case. In this subsection we prove the solvable case of Theorem A. We begin by reducing the problem to bounding the prime divisors in terms of $\hat{h}(G)$.

Lemma 3.6. *Let G be a group. Then $|G|$ is $(|\pi(G)|, h(G))$-bounded.*

Proof. Let $h = h(G)$ and let $t = |\pi(G)|$. Let $\{p_1, \ldots, p_t\}$ be the set of prime divisors of $|G|$. Let n be the exponent of G. Let us write $n = p_1^{a_1} \cdots p_t^{a_t}$ for some integers $a_i \geqslant 1$.

We claim that the number of fields $\mathbb{F}$ with $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{Q}(G)$ and $|\mathbb{F} : \mathbb{Q}| \leqslant h$ is (t, h)-bounded. Since $\mathbb{Q}(G) \subseteq \mathbb{Q}_n$, it suffices to prove that the number subgroups of $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ with index at most h in is (t, h)-bounded. In addition,

$$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}_{p_1^{a_1}}/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}_{p_t^{a_t}}/\mathbb{Q}),$$

where each $\mathrm{Gal}(\mathbb{Q}_{p_i^{a_i}}/\mathbb{Q})$ is cyclic unless when $p_1 = 2$ and $a_1 \geqslant 3$, in which case, $\mathrm{Gal}(\mathbb{Q}_{p_i^{a_i}}/\mathbb{Q})$ is isomorphic to $\mathsf{C}_{2^{a_1-2}} \times \mathsf{C}_2$. Thus, the claim follows.

By Lemma 3.3, we have $|\mathbb{Q}(K) : \mathbb{Q}| \leqslant h$ for any $K \in \mathrm{Cl}(G)$. By the claim, we have that the number of fields $\mathbb{F} \subseteq \mathbb{Q}(G)$ such that $|\mathbb{F} : \mathbb{Q}| \leqslant h$ is (t, h)-bounded. For any of these fields say $\mathbb{F}$, there exists at most h different classes whose field of values is $\mathbb{F}$.

We deduce that $k(G)$ is (t, h)-bounded. The result now follows by Landau's Theorem. □

Remark 3.7. We notice that Lemma 3.6 could have been proved by applying the Héthelyi–Külshammer Theorem (see Theorem [48, Theorem 1.1]). By Lemma 3.5, $k_p(G) \leqslant 3h(G)^2$ for each prime p dividing $|G|$. It follows that the number

of classes of elements of prime power order is at most $(3h(G)^2)^{|\pi(G)|}$ and then $|G|$ is $(|\pi(G)|, h(G))$-bounded by the Héthelyi–Külshammer Theorem.

We decided to include the above proof because the Héthelyi–Külshammer Theorem depends on *CFSG*, while Landau's Theorem is elementary.

We recall that [**23**, Problem 2] asks whether $|\pi(G)|$ is k-bounded for a solvable k-semi-rational group. Next result proves that if that question has a positive answer, we can replace $\hat{h}(G)$ by $h(G)$ in Theorem A for solvable groups.

THEOREM 3.8. *Assume that* [**23**, Problem 2] *has a positive answer. Let G be a solvable group. Then $|G|$ is $h(G)$-bounded.*

PROOF. By Lemma 3.3, we have that $|\mathbb{Q}(K) : \mathbb{Q}| \leqslant h(G)$ for any $K \in \mathrm{Cl}(G)$. Since we are assuming that [**23**, Problem 2] has a positive answer, we have that $|\pi(G)|$ is $h(G)$-bounded. The result follows by Lemma 3.6. □

Now, we work towards a proof of Theorem A. Let us introduce some notation. We introduce the concept of the h-eigenvalue property. This was defined in [**29**], but it is inspired in the work developed in [**39**] (see Lemma 6 of [**39**]).

DEFINITION. Let H be a group and let V be an H-module over a finite field $\mathbb{F}$. Let h be a positive integer. We say that the action of H on V possesses the **h-eigenvalue property** if for every $v \in V$ and any $\mu \in \mathbb{F}^\times$ of order h, there exists $x \in H$ such that $xv = \mu v$.

Before continuing, we make two observations.

REMARK 3.9. It follows from the definition that if the action of H on V possesses the h-eigenvalue property, then the action possesses the r-eigenvalue property for any r dividing h.

REMARK 3.10. If the action of H on V possesses the h-eigenvalue property, then H contains an element of order h. Indeed, given $\mu \in \mathbb{F}^\times$ of order h and $v \in V\backslash\{0\}$, there exists $x \in H$ such that $xv = \mu v$. Then $v = 1v = x^{o(x)}v = \mu^{o(x)}v$ and hence $\mu^{o(x)} = 1$. Thus, $h = o(\mu)$ divides $o(x)$ and hence, there exists a power of x with order h.

The h-eigenvalue property may look a technical condition, but the following result shows that it will appear in a natural way in the context of k-semi-rational groups.

LEMMA 3.11. *Let $k \geqslant 2$ be an integer let G be a k-semi-rational group. Suppose that G has a normal subgroup V such that V is an elementary abelian p-group for a prime p not dividing $|G/V|$. Then the action of G on V has the h-eigenvalue property for some $h \geqslant (p-1)/k!$.*

Before proving Lemma 3.11, we introduce the following elementary result from number theory (see [**120**, Lemma 9]).

LEMMA 3.12. *Let k, n be positive integers. Suppose that $a_1, \dots, a_s$ are distinct positive divisors of n satisfying $\frac{n}{a_i} \leqslant k$. Then*

$$\gcd(a_1, \dots, a_s) \geqslant \frac{n(k-s)!}{k!}.$$

PROOF OF LEMMA 3.11. Let $v \in V \backslash \{1\}$. Since $o(v) = p$, we may identify $\mathrm{Aut}(\langle v \rangle)$ with $\mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times$. With this identification, we have that an element $\mu \in \mathbb{F}_p^\times$ acts on $\langle v \rangle$ by $\mu v = v^\mu$ (we also identify an element in $\mathbb{Z}$ with its class in $\mathbb{Z}/p\mathbb{Z}$). We recall that $B_G(v)$ is defined as $\mathbf{N}_G(\langle v \rangle)/\mathbf{C}_G(v) \leqslant \mathrm{Aut}(\langle v \rangle)$ and that $|\mathbb{Q}(v) : \mathbb{Q}| = |\mathrm{Aut}(\langle v \rangle) : B_G(v)|$ (see Remark 2.16). Thus, with the above identification, we have that

$$B_G(v) = \{\mu \in \mathbb{F}_p^\times \mid v^\mu = v^g \text{ for some } g \in G\}.$$

Since $\mathbb{F}_p^\times$ is cyclic, we know that $B_G(v) = \langle \mu(v) \rangle$ for some $\mu(v) \in \mathbb{F}_p^\times$. Moreover, since G is k-semi-rational, we have that $|\mathbb{Q}(v) : \mathbb{Q}| \leqslant k$. This is equivalent to having $|\mathrm{Aut}(\langle v \rangle) : B_G(v)| \leqslant k$. Thus, $o(\mu(v)) \geqslant (p-1)/k$. In particular, there exists $g(v) \in G$ such that $v^{\mu(v)} = v^{g(v)}$.

We define h as

$$h = \gcd\{o(\mu) \mid \mu \in \mathbb{F}_p^\times, o(\mu) \geqslant (p-1)/k\}.$$

We observe that there are at most k divisors or $p-1$, which are at least $(p-1)/k$. Thus, we deduce that $h \geqslant (p-1)/k!$ by applying Lemma 3.12.

We claim that the action of G on V has the h-eigenvalue property. Let $\eta \in \mathbb{F}_p^\times$ be an element of order h. Let $v \in V \backslash \{1\}$. We know that $o(\mu(v)) \geqslant (p-1)/k$ and hence h divides $o(\mu(v))$. It follows that $\eta \in \langle \mu(v) \rangle$ and hence $\eta = \mu(v)^i$ for some integer i. Since $v^{\mu(v)} = v^{g(v)}$, we deduce that $v^\eta = v^{\mu(v)^i} = v^{g(v)^i}$ and the claim follows. □

We will use the following result about groups acting with the h-eigenvalue property. It is essentially [**29**, Theorem B]. It is the key ingredient for proving most of the results in Section 2.5, and it is also essential for the proof of Theorem A.

THEOREM 3.13 (Farias e Soares). *Let G be a group acting on a finite-dimensional vector space V over a finite field $\mathbb{F}$ of characteristic p, where p is a prime not dividing $|G|$. Assume that the action has the h-eigenvalue property for some positive integer h. Let ϕ be the p-Brauer character afforded by V.*

(i) If G is solvable, then either $|\mathbb{Q}(\phi) : \mathbb{Q}| \geqslant |\mathbb{F}|/\sqrt{3}$ or $\mathbb{F}$ contains a primitive $(h/\gcd(h,4))$-th root of unity. In any case, if q is a prime divisor of h, then $\mathbb{Q}(\phi)$ contains a primitive q-th root of unity, unless $q = 3$ and $|\mathbb{F}| \leqslant 7$.

(ii) *Write* $h = 2^a 3^b 5^c k$ *for* $\gcd(k, 30) = 1$. *Then either* $|\mathbb{Q}(\phi) : \mathbb{Q}| \geqslant |\mathbb{F}|/(6\sqrt{3})$ *or* $\mathbb{Q}(\phi)$ *contains a primitive* k*-th root of unity and* $a \leqslant 3$, $b \leqslant 1$ *and* $c \leqslant 1$. *In any case, if* q *is prime divisor of* k, *then* $\mathbb{Q}(\phi)$ *contains a primitive* q*-th root of unity.*

(iii) *In particular,* $\mathbb{Q}(\phi)$ *contains a primitive* q*-th root of unity for any prime* $q \geqslant 7$ *dividing* h.

Now, we prove Theorem A for solvable groups.

THEOREM 3.14. *Let* G *be a solvable group. Then* $|G|$ *is* $\hat{h}(G)$*-bounded.*

PROOF. Since $h(G) \leqslant \hat{h}(G)$, we only have to prove that $|\pi(G)|$ is $\hat{h}(G)$-bounded, by Lemma 3.6.

Given $n \geqslant 1$, we define

$$g(n) := 120^{n^2}(n!)(n! + 1)^{(n^2)(n!+1)} + 1.$$

Let $k = \hat{h}(G)$. We claim that $p \leqslant g(k)$ for any prime p dividing $|G|$.

Assume that G is a counterexample to the claim of minimal order. Assume that G possesses two different minimal normal subgroups V and W. Since $\hat{h}(G/V), \hat{h}(G/W) \leqslant \hat{h}(G) = k$ and G is a counterexample of minimal order, then $r \leqslant g(k)$ for any prime r dividing either $|G/V|$ or $|G/W|$. Now, we observe that G can be embedded in $G/V \times G/W$. Thus, $r \leqslant g(k)$ for any prime r dividing $|G|$, a contradiction.

Thus, we may assume that G possesses a unique minimal normal subgroup, say V. We know that V is an elementary abelain p-group for a prime p. Reasoning as before, we have that $r \leqslant g(k)$ for any prime r dividing $|G/V|$. If $p \leqslant g(k)$, then G is not a counterexample. Thus, $p > g(k)$ and hence $\gcd(|G/V|, |V|) = 1$. Therefore, by the Schur–Zassenhaus Theorem $G = V \rtimes H$ for some complement $H \cong G/V$.

Let $\mathbb{F}_p$ be the field of p elements and let $\overline{\mathbb{F}_p}$ be the algebraic closure of $\mathbb{F}_p$. Since V is a minimal normal subgroup, V is an irreducible H-module over $\mathbb{F}_p$. Let $\mathfrak{X}$ be the $\mathbb{F}_p$-representation of H given by V. We can extend $\mathfrak{X}$ to a representation $\mathfrak{X}^{\overline{\mathbb{F}_p}}$ over $\overline{\mathbb{F}_p}$. Let ϕ be the p-Brauer character of H provided by $\mathfrak{X}^{\overline{\mathbb{F}_p}}$. By Lemma 2.32, we have that $\mathbb{Q}(\phi) \subseteq \mathbb{Q}(\psi)$ for any component ψ of ϕ. Moreover, since $\gcd(|H|, p) = 1$, the irreducible p-Brauer character ψ is in fact an ordinary (complex) irreducible character of H. Therefore, $\mathbb{Q}(\phi) \subseteq \mathbb{Q}(\psi) \subseteq \mathbb{Q}(G)$ (here, we view ψ as a character of G).

By Lemma 3.3, we have that $|\mathbb{Q}(g) : \mathbb{Q}| \leqslant h(G) \leqslant \hat{h}(G) = k$. Thus, applying Lemma 3.11, we deduce that the action of H on V has the h-eigenvalue property for some $h \geqslant \frac{p-1}{k!}$.

Write $h = p_1^{a_1} \cdots p_t^{a_t}$, where $p_1 < p_2 < \ldots < p_t$ are primes. By taking $a_i = 0$ if necessary, we may assume that $p_1 = 2$, $p_2 = 3$ and $p_3 = 5$. Our aim is to bound each p_i and each a_i in terms of k with explicit bounds. Fix an $1 \leqslant i \leqslant t$. Let $q = p_i$ and $a = a_i$.

We begin by bounding a. Since the action of H on V possesses the h-eigenvalue property, it also has the q^a-eigenvalue property. In particular, H contains an element of order q^a say x. Thus, $a \leqslant 3k^2$ by Lemma 3.5. Moreover, if $i \geqslant 2$, then p_i is odd and thus $a \leqslant k^2$.

Now, we bound q. Let us assume that $q \geqslant 7$, or equivalently, that $i \geqslant 4$. We have that the action of H on V has the q-eigenvalue property. Thus, by Theorem 3.13 the field $\mathbb{Q}(\phi)$ contains a primitive q-th root of unity, so by the previous discussion, we have that $\mathbb{Q}(G)$ contains a primitive q-th root of unity. Now, since $\exp(\mathrm{Gal}(\mathbb{Q}(G)/\mathbb{Q}))$ divides $k!$, we have that $q \leqslant k! + 1$.

From the above discussion, we deduce that

$$\frac{p-1}{k!} \leqslant h = p_1^{a_1} \cdots p_t^{a_t} \leqslant 2^{3k^2} 15^{k^2} (k!+1)^{(k^2)(k!+1)} = 120^{k^2} (k!+1)^{(k^2)(k!+1)},$$

which implies $p \leqslant 120^{k^2}(k!)(k!+1)^{(k^2)(k!+1)} + 1 = g(k)$. This contradiction completes the proof. □

3.2.3. General case. In this subsection we prove that $|G|$ is $\hat{h}(G)$-bounded for any group G. We recall that the solvable radical is the largest normal and solvable subgroup of G. We will denote it by $R(G)$. We first prove that $|G|$ is $\hat{h}(G)$-bounded for groups with trivial solvable radical.

THEOREM 3.15. *If G is a group with $R(G) = 1$, then $|G|$ is $\hat{h}(G)$-bounded.*

Before proving Theorem 3.15, we have make a brief discussion. Let T be a non-abelian simple group and let p be a prime dividing $|T|$. We recall that $m_p(T)$ denotes the number of $\mathrm{Aut}(T)$-orbits on the set of p-elements of T and $L(T)$ denotes the largest $m_p(T)$ for p a prime dividing $|T|$. We recall and restate the result of Giudici, Morgan and Praeger [**36**] that we mentioned in the Introduction. The following result is [**36**, Theorem 1.1].

THEOREM 3.16 (Giudici, Morgan and Praeger). *Let T be a non-abelian simple group. Then $|T|$ is bounded in terms of $L(T)$.*

PROOF OF THEOREM 3.15. Assume that G is a group with $R(G) = 1$. In this case, $\mathbf{F}^*(G) = T_1^{n_1} \times \cdots \times T_t^{n_t}$ for simple groups T_i with $T_i \neq T_j$ for $i \neq j$. We know that $\mathbf{C}_G(\mathbf{F}^*(G)) \leqslant \mathbf{F}^*(G)$ (see Theorem 1.11) and hence $|G| \leqslant |\mathbf{F}^*(G)|!$. Therefore, it suffices to bound each $|T_i|$ and each n_i in terms of $\hat{h}(G)$.

Let $i \in \{1, \dots, t\}$, let $T = T_i$ and $n = n_i$. Then

$$G/\mathbf{C}_G(T^n) \leqslant \mathrm{Aut}(T^n) = \mathrm{Aut}(T) \wr \mathsf{S}_n$$

and $\hat{h}(G/\mathbf{C}_G(T^n)) \leqslant \hat{h}(G)$. Thus, we may assume that $T^n \leqslant G \leqslant \mathrm{Aut}(T) \wr \mathsf{S}_n$.

We begin by bounding n. By the Feit–Thompson Theorem, we know that there exists an involution $z \in T$. For any $1 \leqslant r \leqslant n$, we define $z_r = (z, \dots, z, 1, \dots, 1) \in T^n$ with r copies of z. If $1 \leqslant r < s \leqslant n$, then z_r and z_s are not conjugate in $\mathrm{Aut}(T) \wr \mathsf{S}_n$ and hence, they are not conjugate in G. Moreover, $\mathbb{Q}(z_r) = \mathbb{Q}$ for any r (notice that $o(z_r) = 2$). Thus, $n \leqslant |\mathrm{Cl}_{\mathbb{Q}}(G)| \leqslant h(G) \leqslant \hat{h}(G)$.

Now, we bound $|T|$. We claim that $m_p(T) \leqslant k_p(G)$ for any prime p dividing $|T|$. Let $a, b \in T_p$ be two p-elements lying in different orbits of $\mathrm{Aut}(T)$. Then the elements $(a, \dots, a), (b, \dots, b) \in T^n \leqslant G$ are p-elements, which are not G-conjugated.

By Lemma 3.5, $m_p(T) \leqslant k_p(G) \leqslant 3h(G)^2 \leqslant 3\hat{h}(G)^2$ for any prime p dividing $|T|$. Thus, we deduce that $L(T) \leqslant 3\hat{h}(G)^2$ and hence $|S|$ is $\hat{h}(G)$-bounded by Theorem 3.16. □

Finally, we can prove Theorem A for any group. Our proof will be very similar to the proof of Theorem 3.14. For this reason, we will omit some details.

THEOREM 3.17. *Let G be a group. Then $|G|$ is $\hat{h}(G)$-bounded.*

PROOF. By Lemma 3.6, it suffices to prove that $|\pi(G)|$ is $\hat{h}(G)$-bounded.

Let $n \geqslant 1$. Let $g(n)$ be the function defined in Theorem 3.14. We define $q(n)$ as the largest prime dividing $|T|$ for a group T with $R(T) = 1$ and $\hat{h}(T) \leqslant n$. The invariant $q(n)$ is well defined by Theorem 3.15.

Let $k = \hat{h}(G)$. We claim that if p divides $|G|$, then $p \leqslant \max\{q(k), g(k)\}$.

Assume that G is a minimal counterexample. Reasoning as in Theorem 3.14, we can assume that G possesses a unique minimal normal subgroup V. If V is non-solvable, then $R(G) = 1$ and hence all prime divisors of $|G|$ are at most $q(k)$, a contradiction. Thus, we have that V is an elementary abelian p-group for some prime p. By minimality of G, we have that all prime divisors of $|G/V|$ are smaller than $\max\{q(k), g(k)\}$. It follows that $p > \max\{q(k), g(k)\}$ and hence $\gcd(|G/V|, |V|) = 1$.

Therefore, $G = V \rtimes H$ and the action of H on V has the h-eigenvalue property for some $h \geqslant (p-1)/k!$ by Lemma 3.11. Reasoning as in Theorem 3.14, we can prove that $p \leqslant g(k)$, a contradiction.

The claim follows and we conclude that $|\pi(G)|$ is $\hat{h}(G)$-bounded. □

3.3. Proof of Theorem B

3.3.1. Preliminaries. In this subsection we present the basic results that will be used for studying groups with $f(G) \leqslant 3$.

LEMMA 3.18. *Let G be a group. If N is a normal subgroup of G, then $f(G/N) \leqslant f(G)$.*

PROOF. This follows easily from the fact that $\mathrm{Irr}(G/N) \subseteq \mathrm{Irr}(G)$. □

LEMMA 3.19. *Let G be a group and $\chi \in \mathrm{Irr}(G)$. Then $|\mathbb{Q}(\chi) : \mathbb{Q}| \leqslant f(G)$.*

PROOF. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$. Then $\chi^\sigma \in \mathrm{Irr}(G)$ and $\mathbb{Q}(\chi^\sigma) = \mathbb{Q}(\chi)$. It follows that $|\mathbb{Q}(\chi) : \mathbb{Q}| = |\mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})| \leqslant f(G)$. □

As a consequence of this result, if $f(G) \leqslant 3$, then $|\mathbb{Q}(\chi) : \mathbb{Q}| \leqslant 3$ for every $\chi \in \mathrm{Irr}(G)$. Therefore, $\mathbb{Q}(\chi)$ is either $\mathbb{Q}$, a quadratic extension of $\mathbb{Q}$ or a cubic extension of $\mathbb{Q}$. We deduce that if $f(G) \leqslant 3$ and $\chi \in \mathrm{Irr}(G)$, then there exists $g \in G$ such that $\mathbb{Q}(\chi) = \mathbb{Q}(\chi(g))$. Indeed, if $(\chi) = \mathbb{Q}$, then we may take $g = 1$ and if $\mathbb{Q}(\chi) \neq \mathbb{Q}$, then we may take $g \in G$ such that $\chi(g) \notin \mathbb{Q}$.

LEMMA 3.20. *Let G be a group with $f(G) \leqslant 3$ and suppose that there exists $\chi \in \mathrm{Irr}(G)$ such that $|\mathbb{Q}(\chi) : \mathbb{Q}| = 2$. Then $\{\psi \in \mathrm{Irr}(G) | \mathbb{Q}(\psi) = \mathbb{Q}(\chi)\} = \{\chi, \chi^\sigma\}$, where $\mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}) = \{1, \sigma\}$.*

PROOF. Clearly $\{\chi, \chi^\sigma\} \subseteq \{\psi \in \mathrm{Irr}(G) \mid \mathbb{Q}(\psi) = \mathbb{Q}(\chi)\}$. Suppose that there exists $\psi \in \mathrm{Irr}(G) \backslash \{\chi, \chi^\sigma\}$ with $\mathbb{Q}(\psi) = \mathbb{Q}(\chi)$. Then $\chi, \chi^\sigma, \psi, \psi^\sigma$ are four irreducible characters with the same field of values, which is incompatible with $f(G) \leqslant 3$. □

As a consequence, if $f(G) \leqslant 3$, we deduce that for each quadratic extension F of $\mathbb{Q}$, there exist at most two irreducible characters of G whose field of values is F.

By Lemma 2.12, we have that $\mathbb{Q}(\chi(g)) \subseteq \mathbb{Q}_{o(g)}$ for every $\chi \in \mathrm{Irr}(G)$ and for every $g \in G$. The following two lemmas will be useful for dealing with $\mathbb{Q}_{o(g)}$, where $g \in G$.

LEMMA 3.21. *Assume that G'' is an elementary abelian p-group, for a prime p, and that $G/G'' \cong \mathsf{C}_q \rtimes \mathsf{C}_r$, where the action is Frobenius, and $G/G' \cong \mathsf{C}_r$ is the Frobenius complement of G/G''. Then $o(g)$ divides rp, for every $g \in G \backslash G'$.*

PROOF. Let $g \in G \backslash G'$. Then $gG'' \in (G/G'') \backslash (G'/G'')$ is an element of order dividing r. Since G'' is an elementary abelian p-group, the result follows. □

LEMMA 3.22. *Let n be a positive integer. Then the following hold:*

(i) *If $n = p$, where p is an odd prime, then $\mathbb{Q}_n$ contains only one cubic subextension if $n \equiv 1 \pmod 3$ and contains no cubic subextension if $n \not\equiv 1 \pmod 3$.*

(ii) *If $n = p^k$, where p is an odd prime and $k \geqslant 1$, then $\mathbb{Q}_n$ contains only one quadratic subextension.*

(iii) *If $n = p^k$, where p is an odd prime and $k \geqslant 2$, then $\mathbb{Q}_n$ contains one cubic subextension if $p \equiv 1 \pmod 3$ or $p = 3$, and contains no cubic subextension if $p \equiv -1 \pmod 3$.*

(iv) *If $n = p^k q^t$, where p and q are odd primes and $k, t \geqslant 1$, then $\mathbb{Q}_n$ contains exactly 3 quadratic subextensions.*

(v) *If $n = p^k q^t$, where p and q are odd primes and $k, t \geqslant 1$, then $\mathbb{Q}_n$ contains exactly 4 cubic subextensions if both $\mathbb{Q}_{p^k}$ and $\mathbb{Q}_{q^t}$ contain cubic subextensions, contains one cubic subextensions if only one of $\mathbb{Q}_{p^k}$ or $\mathbb{Q}_{q^t}$ contains a cubic subextension and does not contain cubic subextensions if neither $\mathbb{Q}_{p^k}$ nor $\mathbb{Q}_{q^t}$ contain cubic subextensions.*

(vi) *If n is odd, then $\mathbb{Q}_n = \mathbb{Q}_{2n}$.*

PROOF. This result follows from Galois Correspondence and the description of $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ given before. As an example, we prove (ii) and (iii). We know that $\mathrm{Gal}(\mathbb{Q}_{p^k}/\mathbb{Q}) \cong \mathsf{C}_{p^{k-1}(p-1)}$. Since $\mathbb{Q}_{p^k}$ has as many quadratic subextensions as the number subgroups of index 2 in $\mathrm{Gal}(\mathbb{Q}_{p^k}/\mathbb{Q})$, we deduce that $\mathbb{Q}_{p^k}$ has only one quadratic subextension. Now, we observe that $\mathbb{Q}_{p^k}$ has cubic subextensions if and only if 3 divides $p^{k-1}(p-1)$. This occurs if and only if $p = 3$ or if 3 divides $p - 1$. If $\mathbb{Q}_{p^k}$ has cubic subextensions, we can argue as in the quadratic case to prove that it has only one cubic extension. Thus, (iii) follows. □

The following result is a direct consequence of Theorem 2.10. This was observed by Navarro and Tiep in the comments before [**100**, Theorem 2.3].

LEMMA 3.23. *Let N be a normal subgroup of G and let $\theta \in \mathrm{Irr}(N)$ be G-invariant. If $(|G : N|, o(\theta)\theta(1)) = 1$, then there exists a unique $\chi \in \mathrm{Irr}(G)$ such that $\chi_N = \theta$, $o(\chi) = o(\theta)$ and $\mathbb{Q}(\chi) = \mathbb{Q}(\theta)$. In particular, if $\gcd(|G : N|, |N|) = 1$, then every G-invariant character of N has an unique extension to G with the same order and the same field of values.*

PROOF. By [**53**, Theorem 8.16], there exists an unique extension $\chi \in \mathrm{Irr}(G)$ of θ such that $o(\chi) = o(\theta)$. Clearly, $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\chi)$. Assume that $\mathbb{Q}(\theta) \neq \mathbb{Q}(\chi)$, then there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}(\theta))\backslash\{1\}$. Then χ^σ extends θ and $o(\chi) = o(\theta) = o(\chi^\sigma)$, which is impossible by uniqueness of χ. Hence, $\mathbb{Q}(\theta) = \mathbb{Q}(\chi)$ as we claimed. □

We introduce some notation in order to state the results deduced from [126]. We recall that the **socle** of a group G is the (direct) product of all minimal normal subgroups of G. We will write $S(G)$ to denote the socle of G and $\alpha(G)$ to denote the number of G-conjugacy classes contained in $G\backslash S(G)$.

THEOREM 3.24. *Let G be a group such that $k(G) \leqslant 11$. If $f(G) \leqslant 3$, then G is one of the following:*

$$\mathsf{C}_2, \mathsf{C}_3, \mathsf{C}_4, \mathsf{D}_{10}, \mathsf{A}_4, \mathsf{C}_7 \rtimes \mathsf{C}_3, \mathsf{S}_3, \mathsf{D}_{14}, \mathsf{D}_{18},$$

$$\mathsf{C}_5 \rtimes \mathsf{C}_4, \mathsf{C}_{13} \rtimes \mathsf{C}_4, \mathsf{A}_5, \mathrm{PSL}(2,8), {}^2B_2(8).$$

PROOF. Using the classification in [126] of the groups with $k(G) \leqslant 11$, we can easily read off the groups with $f(G) \leqslant 3$ and $k(G) \leqslant 11$. □

THEOREM 3.25. *Let G be a solvable group with $\alpha(G) \leqslant 3$. Then either $G = \mathsf{S}_4$ or G is metabelian.*

PROOF. If G is a group with $\alpha(G) \leqslant 3$, then G must be one of the examples listed in [126, Lemmas 2.18, 2.19 and 2.20]. We see that except for S_4, every solvable group in these lemmas is metabelian. □

THEOREM 3.26. *Let G be a group such that $S(G)$ is abelian, $k(G) \geqslant 12$, $4 \leqslant \alpha(G) \leqslant 9$ and $k(G/S(G)) \leqslant 10$. Then $f(G) > 3$.*

PROOF. If G is a group such that $4 \leqslant \alpha(G) \leqslant 9$ and $k(G/S(G)) \leqslant 10$, then G must be one of the examples listed in [126, Lemmas 4.2, 4.5, 4.8, 4.11 and 4.14]. We see that $f(G) > 3$ for all groups in those lemmas with $k(G) > 11$. □

Now, we classify all nilpotent groups with $f(G) \leqslant 3$.

THEOREM 3.27. *If G is a nilpotent group with $f(G) \leqslant 3$, then $G \in \{\mathsf{C}_2, \mathsf{C}_3, \mathsf{C}_4\}$.*

PROOF. Let p be a prime dividing $|G|$. Then there exists $K \trianglelefteq G$ such that $G/K = \mathsf{C}_p$. Therefore, $f(\mathsf{C}_p) = f(G/K) \leqslant f(G) \leqslant 3$, and hence $p \in \{2,3\}$. Therefore, we have $\pi(G) \subseteq \{2,3\}$.

If 6 divides $|G|$, then there exists N, a normal subgroup of G, such that $G/N = \mathsf{C}_6$. However, $f(\mathsf{C}_6) = 4 > 3$ and so we deduce that G must be a p-group. It follows that $G/\Phi(G)$ is an elementary abelian 2-group or an elementary abelian 3-group with $f(G/\Phi(G)) \leqslant 3$. Since $f(\mathsf{C}_2 \times \mathsf{C}_2) = 4$ and $f(\mathsf{C}_3 \times \mathsf{C}_3) = 8$, we have that $G/\Phi(G) \in \{\mathsf{C}_2, \mathsf{C}_3\}$. Thus, by part (ii) of 1.8 we have that G is either a cyclic 2-group or a cyclic 3-group. Since $f(\mathsf{C}_8) > 3$ and $f(\mathsf{C}_9) > 3$, it follows that $G \in \{\mathsf{C}_2, \mathsf{C}_4, \mathsf{C}_3\}$. □

For the remainder of Section 3.3, we will assume that G is not a nilpotent group. As a consequence of Theorem 3.27, we obtain the following result.

COROLLARY 3.28. *If G is a group with $f(G) \leqslant 3$, then either $G = G'$ or $G/G' \in \{\mathsf{C}_2, \mathsf{C}_3, \mathsf{C}_4\}$.*

PROOF. Suppose that $G' < G$, then G/G' is an abelian group with $f(G/G') \leqslant 3$. Thus, by Theorem 3.27, $G/G' \in \{\mathsf{C}_2, \mathsf{C}_3, \mathsf{C}_4\}$. □

In the proof of the solvable case of Theorem B, we need to show that there are no groups G with $f(G) \leqslant 3$ of certain orders. Let $\mathcal{A}$ be set consisting of the following positive integers:

$$30, 42, 48, 50, 54, 70, 84, 98, 100, 126, 147, 156, 234, 260, 342, 558, 666, 676,$$
$$774, 882, 903, 954, 1098, 1206, 1314, 1404, 2756, 4108, 6812, 8164.$$

With this definition, we have the next result.

LEMMA 3.29. *There exists no group G with $f(G) \leqslant 3$ and $|G| \in \mathcal{A}$.*

PROOF. We observe that all numbers in $\mathcal{A}$ are smaller than 2000, except $\{2756, 4108, 6812, 8164\}$. However, these numbers are cube-free. Thus, we can use `SmallGroup` database in GAP [**33**] to check the result. □

3.3.2. Non-solvable case. In this section we classify the non-solvable groups with $f(G) \leqslant 3$.

THEOREM 3.30. *Let G be a non-solvable group with $f(G) \leqslant 3$. Then $f(G) \leqslant 3$ and $G \in \{\mathsf{A}_5, \mathrm{PSL}(2,8), {}^2B_2(8)\}$.*

If G is a group with $f(G) \leqslant 3$, it follows trivially that G possesses at most 3 irreducible rational characters. Therefore, we will use Theorems 2.27 and 2.29, which classify the non-solvable groups with two or three rational characters, respectively. From Theorems 2.27 and 2.29, we deduce that if S is a simple group with at most three rational characters, then S is one of the groups listed in those theorems.

We observe that the simple groups appearing in that Theorem 2.29 are either $\mathrm{PSL}(2,q)$ or ${}^2B_2(q)$. Looking at the character tables of the groups $\mathrm{PSL}(2,q)$ (see Chapter 38 of [**26**]) and ${}^2B_2(q)$ (see Section 4.6 of [**34**]), we see that there is always an entry of the form $e^{(2\pi i)/(q-1)} + e^{(-2\pi i)/(q-1)}$. For this reason, we study whether $e^{(2\pi i)/r} + e^{(-2\pi i)/r}$ is rational, quadratic or cubic for an integer r. As before, we use φ to denote Euler's totient function.

LEMMA 3.31. *Let $r \geqslant 3$ be a positive integer, let $\nu = e^{(2\pi i)/r}$ and let $\omega = \nu + \nu^{-1}$. Then the following hold*

(i) ω *is rational if and only if* $r \in \{3, 4, 6\}$.

(ii) ω *is quadratic if and only if* $r \in \{5, 8, 10, 12\}$.

(iii) ω *is cubic if and only if* $r \in \{7, 9, 14, 18\}$.

PROOF. Given $k \in \{1, \dots, r-1\}$ with $\gcd(r, k) = 1$, we write σ_k to denote the unique automorphism in $\mathrm{Gal}(\mathbb{Q}(\nu)/\mathbb{Q})$ such that $\sigma_k(\nu) = \nu^k$.

Suppose that $\omega \in \mathbb{Q}$. Thus, $\nu^k + \nu^{-k} = \sigma_k(\omega) = \omega = \nu + \nu^{-1}$ for every $k \in \{1, \dots, r-1\}$ with $\gcd(r, k) = 1$. This forces, $\{r \mid 1 \leqslant k \leqslant r \gcd(r, k) = 1\} = \{1, k-1\}$, which implies $\varphi(r) = 2$ and hence $r \in \{3, 4, 6\}$.

Suppose now that ω is quadratic. Then there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}(\nu)/\mathbb{Q})$ such that $\sigma(\omega) \neq \omega$. We deduce that $\sigma(\nu) = \nu^{k_0}$, where $k_0 \in \{2, \dots, r-2\}$ and $\gcd(r, k_0) = 1$. Since ω is quadratic, it follows that $\sigma(\omega)$ is the only Galois conjugate of ω and hence $\{k \leqslant r \mid \gcd(r, k) = 1\} = \{1, k_0, r - k_0, r - 1\}$. Thus, $\varphi(r) = 4$ and (ii) follows.

Reasoning as in the previous case, we can deduce that ω is cubic if and only if $\varphi(r) = 6$ and hence (iii) follows. □

THEOREM 3.32. *Let* S *be a non-abelian simple group with* $f(S) \leqslant 3$. *Then* $S \in \{\mathsf{A}_5, \mathrm{PSL}(2, 8), {}^2B_2(8)\}$.

PROOF. Since $f(S) \leqslant 3$, S has at most three rational characters. Thus, S has the form described in Theorem 2.29. We claim that the only groups in those families with $f(S) \leqslant 3$ are A_5 (which is isomorphic to $\mathrm{PSL}(2, 4)$), $\mathrm{PSL}(2, 8)$ and ${}^2B_2(8)$.

Let $S = \mathrm{PSL}(2, q)$, where q is a prime power, or let $S = {}^2B_2(q)$ where $q = 2^{2t+1}$ and $t \geqslant 1$. We know that there exists $\chi \in \mathrm{Irr}(S)$ and $a \in S$ such that $\chi(a) = e^{(2\pi i)/(q-1)} + e^{(-2\pi i)/(q-1)}$. The condition $f(S) \leqslant 3$ implies that $|\mathbb{Q}(\chi(a)) : \mathbb{Q}| \leqslant 3$. By Lemma 3.31, we deduce that $q - 1 \in \{3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 18\}$. If $S = \mathrm{PSL}(2, q)$, we have that $q = 2^n$, $q = 3^{2m+1}$ or $q \equiv \pm 5 \pmod{24}$. Thus, we only have to consider the cases $q \in \{5, 8, 13, 19\}$. Finally, we have that $3 = f(\mathrm{PSL}(2, 5)) = f(\mathrm{PSL}(2, 8))$ and $f(\mathrm{PSL}(2, 13)) = f(\mathrm{PSL}(2, 19)) = 4$. For $S = {}^2B_2(q)$, we only have to consider the case $q = 8$ and we find that $f({}^2B_2(8)) = 3$.

Therefore, up to isomorphism, the only simple groups with $f(S) = 3$ are A_5, $\mathrm{PSL}(2, 8)$ and ${}^2B_2(8)$. □

We also need a result on characters of simple groups. The following result is [**103**, Lemma 4.1].

THEOREM 3.33. *Let* S *be a non-abelian simple group. There exists a rational non-principal character* $\psi \in \mathrm{Irr}(S)$ *such that* ψ *is extendible to* $\mathrm{Aut}(S)$.

Using Theorem 2.27 and Theorem 3.33 we prove that a non-solvable group with $f(G) \leqslant 3$ has exactly three rational characters.

THEOREM 3.34. *Let G be a non-solvable group with $f(G) \leqslant 3$. Then G has exactly three rational irreducible characters. In particular, $f(G) = 3$.*

PROOF. By Theorem 2.25 and the Feit–Thompson Theorem, G has at least two rational irreducible characters. Assume for contradiction that G has exactly two rational irreducible characters. Applying Theorem 2.27, we have that $M/N \cong \mathrm{PSL}(2, 3^{2f+1})$ for some $f \geqslant 1$, where $M = \mathbf{O}^{2'}(G)$ and $N = \mathbf{O}_{2'}(M)$. Taking the quotient by N, we may assume that $N = 1$.

By Theorem 3.32, $f(M) = f(\mathrm{PSL}(2, 3^{2f+1})) > 3$ and hence we deduce that $M < G$. Now, we claim that there exists a rational character of M that can be extended to a rational character of G.

By Theorem 3.33, there exists $\psi \in \mathrm{Irr}(M)$, which is rational and is extendible to a rational character $\phi \in \mathrm{Irr}(\mathrm{Aut}(M))$. If $H = G/\mathsf{C}_G(M)$, then we can identify H with a subgroup of $\mathrm{Aut}(M)$ which contains M. Therefore, ψ is extendible to $\gamma := \phi_H \in \mathrm{Irr}(H) \subseteq \mathrm{Irr}(G)$ and it is rational, as we wanted.

Let $\chi \in \mathrm{Irr}(G/M)\backslash\{1_{G/M}\}$. Since $|G/M|$ is odd, χ cannot be rational. Thus, there exists $\rho \neq \chi$, a Galois conjugate of χ. Then $\mathbb{Q}(\chi) = \mathbb{Q}(\rho)$. Since ψ is extendible to the rational character $\gamma \in \mathrm{Irr}(G)$, applying Gallagher's Theorem (see Theorem 2.8), we have that $\chi\gamma \neq \rho\gamma$ are two irreducible characters of G and $\mathbb{Q}(\chi) = \mathbb{Q}(\rho) = \mathbb{Q}(\chi\gamma) = \mathbb{Q}(\rho\gamma)$. Therefore, we have 4 irreducible characters with the same field of values, which is impossible. □

Now, we use Theorem 2.29 to determine $G/\mathbf{O}_{2'}(G)$.

THEOREM 3.35. *Let G be a finite non-solvable group with $f(G) = 3$. Then $G/\mathbf{O}_{2'}(G) \in \{\mathsf{A}_5, \mathrm{PSL}(2,8), {}^2B_2(8)\}$.*

PROOF. Let M and N be as in Theorem 2.29. We assume for the moment that $N = 1$.

Suppose first that $M < G$. Reasoning as in Theorem 3.34, we can prove that there exists $\psi \in \mathrm{Irr}(M)$ such that it is extendible to a rational character $\varphi \in \mathrm{Irr}(G)$. As in Theorem 3.34, if we take $\chi \in \mathrm{Irr}(G/M)\backslash\{1_{G/M}\}$ and ρ a Galois conjugate of χ, then $\mathbb{Q}(\chi) = \mathbb{Q}(\rho) = \mathbb{Q}(\varphi\chi) = \mathbb{Q}(\varphi\rho)$, where all of these characters are different, which is a contradiction.

Thus, $M = G$ and hence G is a simple group with $f(G) = 3$. By Theorem 3.32, $G \in \{\mathsf{A}_5, \mathrm{PSL}(2,8), {}^2B_2(8)\}$.

If we apply the previous reasoning to G/N, then we have that G/N is one of the desired groups. In either case, G/N has the form (i),(ii) or (iii) of Theorem 2.29 and hence $N = \mathbf{O}_{2'}(G)$. □

To complete our proof of Theorem 3.30 (i.e. Theorem B for non-solvable groups) it only remains to prove that $\mathbf{O}_{2'}(G) = 1$. However, before doing so, we need to study before two special cases. First, we handle the case where n $\mathbf{O}_{2'}(G) = \mathbf{Z}(G)$.

THEOREM 3.36. *There is no quasisimple group G such that $\mathbf{O}_{2'}(G) = \mathbf{Z}(G)$, $\mathbf{O}_{2'}(G) \neq 1$ and $G/\mathbf{Z}(G) \in \{\mathsf{A}_5, \mathrm{PSL}(2,8), {}^2B_2(8)\}$.*

PROOF. Suppose that such a group exists. Then $|\mathbf{Z}(G)|$ divides $|M(S)|$, where $S = G/\mathbf{Z}(G)$. The Schur multipliers of A_5, ${}^2B_2(8)$ and $\mathrm{PSL}(2,8)$ can be found in the *ATLAS* [**24**] and they are C_2, $\mathsf{C}_2 \times \mathsf{C}_2$ and the trivial group, respectively. It follows that $\mathbf{Z}(G)$ is a 2-group. However, $\mathbf{Z}(G) = \mathbf{O}_{2'}(G)$ and hence $|\mathbf{Z}(G)|$ has odd order. Thus, $\mathbf{Z}(G) = 1$, a contradiction. □

We need to introduce more notation to deal with the remaining case. For any group G, we define $o(G) = \{o(g) \mid g \in G\backslash\{1\}\}$. Suppose that $f(G) \leqslant 3$ and let $\chi \in \mathrm{Irr}(G)$ be a non-rational character. Then $\mathbb{Q}(\chi) = \mathbb{Q}(\chi(g))$ for some $g \in G\backslash\{1\}$. Thus, $\mathbb{Q}(\chi)$ is a quadratic subextension or a cubic subextension of $\mathbb{Q}_n$, where $n = o(g)$.

THEOREM 3.37. *There is no group G with $f(G) \leqslant 3$ such that $G/\mathbf{O}_{2'}(G) \in \{\mathsf{A}_5, \mathrm{PSL}(2,8), {}^2B_2(8)\}$ and $\mathbf{O}_{2'}(G)$ is both an elementary abelian p-group and a non-trivial irreducible $\mathbb{F}_p$-module for $G/\mathbf{O}_{2'}(G)$.*

PROOF. Seeking for a contradiction, suppose that such a group G exists. Write $V = \mathbf{O}_{2'}(G)$ and let $|V| = p^d$ with $p > 2$. Then V can be viewed as an irreducible $\mathbb{F}_p[G/V]$-module of dimension d. Let $\mathcal{X}$ be the irreducible $\mathbb{F}_p$-representation of G/V afforded by V. We know that $\mathbb{F}_p \subseteq \overline{\mathbb{F}_p}$ and hence $\mathcal{X}$ can be realized over $\overline{\mathbb{F}_p}$. Let $\mathcal{X}^{\overline{\mathbb{F}_p}}$ be the representation $\mathcal{X}$ when we consider it as a representation over $\overline{\mathbb{F}_p}$. It follows that $\mathcal{X}^{\overline{\mathbb{F}_p}}$ can be expressed as a sum of irreducible representations of G/V over $\overline{\mathbb{F}_p}$ (see the comments before Theorem 2.32). In particular, we have that $d \geqslant b_p(G/V)$, where $b_p(G/V)$ denotes the smallest degree of a non-linear p-Brauer character of G/V. We have to distinguish two different cases: p divides $|G/V|$ and p does not divide $|G/V|$.

Case p does not divide $|G/V|$: In this case, each Brauer character of G/V is an ordinary character. Thus, $|V| \geqslant p^d$ where d is at least the smallest degree of an irreducible non-trivial (complex) character of G/V. The smallest degree of the irreducible non-trivial character of A_5, ${}^2B_2(8)$ and $\mathrm{PSL}(2,8)$ can be found in the *ATLAS* [**24**].

Now, let $\lambda \in \mathrm{Irr}(V)\backslash\{1\}$. Then $\mathbb{Q}(\lambda) \subseteq \mathbb{Q}_p$. Since $\gcd(|G/V|, |V|) = 1$, we have that $\gcd(|I_G(\lambda)/V|, |V|) = 1$. Thus, by Lemma 3.23, we deduce that λ has an extension $\psi \in \mathrm{Irr}(I_G(\lambda))$ with $\mathbb{Q}(\psi) = \mathbb{Q}(\lambda) \subseteq \mathbb{Q}_p$. By the Clifford Correspondence $\psi^G \in \mathrm{Irr}(G)$ and $\mathbb{Q}(\psi^G) \subseteq \mathbb{Q}(\psi) \subseteq \mathbb{Q}_p$. Thus, given ζ, an orbit of G/V on $\mathrm{Irr}(V)\backslash\{1_V\}$, there exists $\chi_\zeta \in \mathrm{Irr}(G|V)$ such that $\mathbb{Q}(\chi_\zeta) \subseteq \mathbb{Q}_p$.

Let F be the unique quadratic subextension of $\mathbb{Q}_p$ and let T be the unique cubic subextension of $\mathbb{Q}_p$ (if such a subextension exists). Since $\mathrm{Irr}(G/V)$ contains three rational characters, we deduce that $\mathbb{Q}(\chi_\zeta) \in \{T, F\}$ and since F is quadratic, then there are at most 2 characters whose field of values is F. Thus, the action of G/V on $\mathrm{Irr}(V)\backslash\{1_V\}$ has at most 5 orbits. Therefore, $|V| = |\mathrm{Irr}(V)| \leqslant 5|G/V| + 1$.

(i) Case $G/V = \mathsf{A}_5$: In this case $|V| \geqslant 7^3 = 343$ (because 7 is the smallest prime not dividing $|G/V|$ and 3 is the smallest degree of a non-linear irreducible character of A_5). On the other hand, we have $|V| \leqslant 5|G/V| + 1 \leqslant 5 \cdot 60 + 1 = 301 < 343$, which is a contradiction.

(ii) Case $G/V = \mathrm{PSL}(2,8)$: Here $|V| \geqslant 5^7 = 78125$ and $|V| \leqslant 5 \cdot 504 + 1 = 2521$, which is a contradiction.

(iii) Case $G/V = {}^2B_2(8)$: Here $|V| \geqslant 3^{14} = 4782969$ and $|V| \leqslant 5 \cdot 29120 + 1 = 145601$, which is a contradiction.

Case p divides $|G/V|$: Given $S \in \{\mathsf{A}_5, \mathrm{PSL}(2,8), {}^2B_2(8)\}$ and given a prime p dividing $|S|$, the p-Brauer character table of S can be calculated in GAP [**33**]. From the Brauer character tables of $\{\mathsf{A}_5, \mathrm{PSL}(2,8), {}^2B_2(8)\}$, we deduce that $b_p(\mathsf{A}_5) = 3$ for $p \in \{3,5\}$, $b_p(\mathrm{PSL}(2,8)) = 7$ for $p \in \{3,7\}$ and $b_p({}^2B_2(8)) = 14$ for $p \in \{5,7,13\}$.

(i) Case $G/V = \mathrm{PSL}(2,8)$:

a) $p = 7$: In this case $|V| = 7^d$ with $d \geqslant 7$ and $o(G) = \{2, 3, 7, 9, 2 \cdot 7, 3 \cdot 7, 7 \cdot 7, 9 \cdot 7\}$. On the one hand, the number of non-trivial G-conjugacy classes contained in V is at least $\frac{|V|}{|G/V|} \geqslant \frac{7^7}{504} \geqslant 1634$. Therefore, we deduce that $|\mathrm{Irr}(G)| \geqslant 1634$. On the other hand, we have that there are at most 3 quadratic extensions and at most 4 cubic extensions contained in $\mathbb{Q}_n$, where $n \in o(G)$. Since $f(G) \leqslant 3$, the number of non-rational characters in G is at most $2 \cdot 3 + 3 \cdot 4 = 18$. Counting the rational characters, we have that $|\mathrm{Irr}(G)| \leqslant 21 < 1634$, which is a contradiction.

b) $p = 3$: In this case $|V| = 3^d$ with $d \geqslant 7$ and by calculation we get $k(G) = |\mathrm{Irr}(G)| \leqslant 3 + 2 \cdot 3 + 3 \cdot 2 = 15$. We know that $V = S(G)$, and hence if $4 \leqslant \alpha(G) \leqslant 9$, then $f(G) > 3$ by Theorem 3.26 (clearly $\alpha(G) \geqslant 4$ because $k(G/S(G)) = 9$). Thus, $\alpha(G) \geqslant 10$. Since $V = S(G)$ and $k(G) \leqslant 15$, we deduce that V contains at most 4

non-trivial G-conjugacy classes. Thus, $|V| \leqslant 504 \cdot 4 + 1 = 2017 < 3^7$ and hence we have a contradiction.

(ii) Case $G/V = {}^2B_2(8)$: In this case $|V| \geqslant 5^{14}$ and as before $|\operatorname{Irr}(G)| \geqslant 209598$.

a) $p = 5$: By calculation, $|\operatorname{Irr}(G)| \leqslant 3 + 2 \cdot 7 + 3 \cdot 2 = 23 < 209598$, which is a contradiction.

b) $p \in \{7, 13\}$: By calculation, $|\operatorname{Irr}(G)| \leqslant 3 + 2 \cdot 7 + 3 \cdot 4 = 29 < 209598$, which is a contradiction.

(iii) Case $G/V = \mathsf{A}_5$:

a) $p = 3$: In this case $|V| = 3^d$, where $d \geqslant 3$ and we compute $|\operatorname{Irr}(G)| \leqslant 3 + 2 \cdot 3 + 3 \cdot 1 = 12$. As before, applying Theorem 3.26, we deduce that $|V|$ contains at most one non-trivial G-conjugacy class. Thus, $|V| \leqslant 61$ and since V is a 3-group we deduce that $|V| = 3^3$. We also deduce that 26 is the size of a G-conjugacy class. That is impossible since 26 does not divide $|G/V| = 60$.

b) $p = 5$: In this case $k(G) \leqslant 9$ and by Theorem 3.24 there is no group with the required properties.

We conclude that there is no group with the desired form and hence $V = 1$, which is a trivial $\mathbb{F}_p[G/V]$-module, a contradiction □

Now, we are ready to prove of Theorem 3.30

Proof of Theorem 3.30. By Theorem 3.35, we know that $G/\mathbf{O}_{2'}(G) \in \{\mathsf{A}_5, \mathrm{PSL}(2,8), {}^2B_2(8)\}$. We aim to prove that $\mathbf{O}_{2'}(G) = 1$. Suppose that $\mathbf{O}_{2'}(G) > 1$. Taking an appropriate quotient, we may assume that $\mathbf{O}_{2'}(G)$ is a minimal normal subgroup of G. Since $\mathbf{O}_{2'}(G)$ is solvable, we have that $\mathbf{O}_{2'}(G)$ is an elementary abelian p-group for some odd prime p. There are two possibilities for $\mathbf{O}_{2'}(G)$. The first one is that $\mathbf{O}_{2'} = \mathbf{Z}(G)$, and the second one is that $\mathbf{O}_{2'}(G)$ is irreducible as a module for $G/\mathbf{O}_{2'}(G)$. The first one is impossible by Theorem 3.36 and the second one is impossible by Theorem 3.37. Thus, $\mathbf{O}_{2'}(G) = 1$ and the result follows. □

Therefore, the only non-solvable groups with $f(G) \leqslant 3$ are $\mathsf{A}_5, \mathrm{PSL}(2,8)$ and ${}^2B_2(8)$. The rest of this section is devoted to classifying all solvable groups with $f(G) \leqslant 3$.

3.3.3. Metabelian case. In this subsection we classify all the metabelian groups with $f(G) \leqslant 3$. Let G be a finite metabelian group with $f(G) \leqslant 3$. By Corollary 3.28, we have $G/G' \in \{\mathsf{C}_2, \mathsf{C}_3, \mathsf{C}_4\}$ and hence we can divide this case into different subcases. We begin by studying the case when G' is an elementary abelian p-group.

LEMMA 3.38. *Let G be a group such that $f(G) \leqslant 3$ and $G' \neq 1$ is an elementary abelian p-group. Then $G \in \{\mathsf{S}_3, \mathsf{D}_{10}, \mathsf{A}_4, \mathsf{D}_{14}, \mathsf{C}_7 \rtimes \mathsf{C}_3, \mathsf{C}_5 \rtimes \mathsf{C}_4, \mathsf{C}_{13} \rtimes \mathsf{C}_4\}$.*

PROOF. Assume first that p divides $|G : G'|$. By the above observation, we have that G/G' is cyclic of prime order. Thus, if p divides $|G : G'|$, then G is a p-group. In such a case, G is nilpotent and hence $G' = 1$ by Theorem 3.27, a contradiction. Therefore, we have that $\gcd(|G : G'|, p) = 1$

Let $\psi \in \mathrm{Irr}(G')\backslash\{1_{G'}\}$ and let $I_G(\psi)$ be the inertia group of ψ in G. Since $\mathrm{Irr}(G/G')$ is the set of linear characters of G and ψ is linear, we have that ψ cannot be extended to G. Moreover, since G/G' is cyclic, we have that ψ can be extended to an irreducible character of $I_G(\psi)$ by Theorem 2.11. It follows that $I_G(\psi) < G$. Now, we study separately the case $G/G' \in \{\mathsf{C}_2, \mathsf{C}_3\}$ and the case $G/G' = \mathsf{C}_4$.

Assume first that $G/G' \in \{\mathsf{C}_2, \mathsf{C}_3\}$. Since $I_G(\psi) < G$, we deduce that $I_G(\psi) = G'$ for every $\psi \in \mathrm{Irr}(G')\backslash\{1_{G'}\}$. Thus, by the Clifford Correspondence, $\psi^G \in \mathrm{Irr}(G)$.

Therefore, if $\chi \in \mathrm{Irr}(G|G')$, then χ has the form $\chi = \psi^G$, where $\psi \in \mathrm{Irr}(G')\backslash\{1_{G'}\}$. Since $\mathbb{Q}(\psi) \subseteq \mathbb{Q}_p$, we have that $\mathbb{Q}(\psi^G) \subseteq \mathbb{Q}_p$. We know that there exists at most one quadratic subextension in $\mathbb{Q}_p$ and at most one cubic subextension in $\mathbb{Q}_p$. Since $\mathrm{Irr}(G/G')$ contains at least one rational character and $f(G) \leqslant 3$, we have that $|\mathrm{Irr}(G|G')| \leqslant 2 + 1 \cdot 2 + 1 \cdot 3 = 7$. Since $|\mathrm{Irr}(G/G')| \leqslant 3$, we have

$$k(G) = |\mathrm{Irr}(G)| = |\mathrm{Irr}(G|G')| + |\mathrm{Irr}(G/G')| \leqslant 7 + 3 = 10.$$

By Theorem 3.24, we deduce that the only groups such that $|G : G'| \in \{2, 3\}$, G' is elementary abelian, $f(G) \leqslant 3$ and $k(G) \leqslant 10$ are $\{\mathsf{S}_3, \mathsf{D}_{10}, \mathsf{A}_4, \mathsf{D}_{14}, \mathsf{C}_7 \rtimes \mathsf{C}_3\}$.

Assume now that $G/G' = \mathsf{C}_4$. If $\psi \in \mathrm{Irr}(G')\backslash\{1_{G'}\}$, then $I_G(\psi) < G$ and hence we have two possible options.

The first one is that $I_G(\psi) = G'$. In this case, applying the Clifford Correspondence, we have $\psi^G \in \mathrm{Irr}(G)$ and hence $\mathbb{Q}(\psi^G) \subseteq \mathbb{Q}(\psi) \subseteq \mathbb{Q}_p$. The other one is that $|G : I_G(\psi)| = 2$. In this case, applying Lemma 3.23, we have that ψ is extendible to $\varphi \in \mathrm{Irr}(I_G(\psi))$ and $\mathbb{Q}(\varphi) = \mathbb{Q}(\psi) \subseteq \mathbb{Q}_p$. Let $\mathrm{Irr}(I_G(\psi)/G') = \{1, \rho\}$. By Gallagher's Theorem, φ and $\varphi\rho$ are all the extensions of ψ to $I_G(\psi)$. Since $\mathbb{Q}(\rho) = \mathbb{Q}$, we have $\mathbb{Q}(\varphi\rho) = \mathbb{Q}(\varphi) \subseteq \mathbb{Q}_p$. Let $\tau \in \{\varphi, \varphi\rho\}$. Then $\tau^G \in \mathrm{Irr}(G)$, and hence $\mathbb{Q}(\tau^G) \subseteq \mathbb{Q}(\tau) \subseteq \mathbb{Q}_p$. Therefore, $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_p$ for every $\chi \in \mathrm{Irr}(G|G')$.

As before, we can deduce that $\mathrm{Irr}(G|G')$ contains at most 5 non-rational characters. On the other hand, $\mathrm{Irr}(G/G')$ contains two rational characters and hence $\mathrm{Irr}(G|G')$ contains at most one rational character. Therefore, $|\mathrm{Irr}(G|G')| \leqslant 6$ and hence $k(G) = |\mathrm{Irr}(G/G')| + |\mathrm{Irr}(G|G')| \leqslant 4 + 6 = 10$. By Theorem 3.24, our only possible options are $\{\mathsf{C}_5 \rtimes \mathsf{C}_4, \mathsf{C}_{13} \rtimes \mathsf{C}_4\}$. □

THEOREM 3.39. *Let G be a metabelian group with $f(G) \leqslant 3$ and $|G : G'| = 2$. Then $G \in \{\mathsf{S}_3, \mathsf{D}_{10}, \mathsf{D}_{14}, \mathsf{D}_{18}\}$.*

PROOF. Assume for the moment that G' is a p-group for a prime p. We note that $\mathbf{F}(G) = G'$. Therefore, $G'/\Phi(G) = \mathbf{F}(G)/\Phi(G)$ is an elementary abelian p-group. Thus, by Lemma 3.38, we have that $G/\Phi(G) \in \{\mathsf{S}_3, \mathsf{D}_{10}, \mathsf{D}_{14}\}$ and hence $G'/\Phi(G)$ is cyclic. Therefore, G' is a cyclic p-group and and we have only three possibilities for p. We analyze the cases $p = 3$, $p = 5$ and $p = 7$ separately.

If $p = 3$, then G' is a cyclic group of order 3^l. If $l \geqslant 3$, then there exists K characteristic in G' of order 3^{l-3}. Thus, $|G/K| = 2 \cdot 3^3 = 54$ and $f(G/K) \leqslant 3$. However, by Lemma 3.29, there is no group of order 54 with $f(G) \leqslant 3$. Thus, $l \in \{1, 2\}$. If $l = 1$, then $G = \mathsf{S}_3$ and if $l = 2$, then $G = \mathsf{D}_{18}$.

If $p \in \{5, 7\}$, then G' is a cyclic group of order p^l. If $l \geqslant 2$, then there exists K characteristic in G' of order p^{l-2}. Thus, $|G/K| = 2 \cdot p^2$ and $f(G/K) \leqslant 3$. For $p = 5$, we have that $|G/K| = 2 \cdot 5^2 = 50$ and for $p = 7$, we have that $|G/K| = 2 \cdot 7^2 = 98$. However, by Lemma 3.29, there is no group of order 50 or 98 with $f(G) \leqslant 3$.

Therefore, if G' is a p-group, then $G \in \{\mathsf{S}_3, \mathsf{D}_{18}, \mathsf{D}_{10}, \mathsf{D}_{14}\}$. From here, we also deduce that the prime divisors of $|G'|$ are contained in $\{3, 5, 7\}$. To complete the classification it only remains to prove that $|G'|$ is not divisible by two different primes. Suppose that both 3 and 5 divide $|G'|$. Taking a quotient by a Sylow 7-subgroup of G', we may assume that the only prime divisors of $|G'|$ are 3 and 5. By the case when G' is a p-group, we deduce that the Sylow 3-subgroups and Sylow 5-subgroups of G' are both cyclic. Thus, $f(G/\Phi(G)) \leqslant 3$ and $G'/\Phi(G) = \mathsf{C}_3 \times \mathsf{C}_5$. Therefore, $G/\Phi(G)$ is a group of order 30 with $f(G/\Phi(G)) \leqslant 3$, which is impossible by Lemma 3.29. Analogously, we can prove that if any of the pairs $\{3, 7\}$ or $\{5, 7\}$ divide $|G'|$ at the same time, then there exists a group L with $f(L) \leqslant 3$ of order 42 or 70, respectively. Applying again Lemma 3.29, we reach a contradiction. Thus, G' is a p-group and the result follows. □

THEOREM 3.40. *Let G be a metabelian group with $f(G) \leqslant 3$ such that $|G : G'| = 3$. Then $G \in \{\mathsf{A}_4, \mathsf{C}_7 \rtimes \mathsf{C}_3\}$.*

PROOF. As in Theorem 3.39, we assume first that G' is a p-group. By Proposition 3.38, we have that $G/\Phi(G) \in \{\mathsf{A}_4, \mathsf{C}_7 \rtimes \mathsf{C}_3\}$. Therefore, we have that $p \in \{2, 7\}$. We analyze each case separately.

First, assume that $p = 7$, so $G'/\Phi(G) = \mathsf{C}_7$. Thus, G' is a cyclic group of order 7^l. If $l \geqslant 2$, then there exists K characteristic in G' of order 7^{l-2}. Thus, $|G/K| = 3 \cdot 7^2 = 147$ and $f(G/K) \leqslant 3$. However, by Lemma 3.29, there is no group of order 147 with $f(G) \leqslant 3$. Thus, $l = 1$ and hence $G = \mathsf{C}_7 \rtimes \mathsf{C}_3$.

Now suppose $p = 2$, in which case $G'/\Phi(G) = \mathsf{C}_2 \times \mathsf{C}_2$. Then, $G' = U \times V$, where U is cyclic of order 2^n, V is cyclic of order 2^m and $n \geqslant m \geqslant 1$. Assume first that $n > m$. Then, we can take H to be the unique subgroup of U of order 2^m. Thus, $K = H \times V$ is normal in G and $(G/K)'$ is a cyclic 2-group. Thus,

$f(G/K) \leqslant 3$, $|G/K : (G/K)'| = 3$ and $(G/K)'$ is a cyclic 2-group, which is not possible by Lemma 3.38. It follows that $n = m$ and hence G' is a product of 2 cyclic groups of size 2^n. If $n \geqslant 2$, then there exists T characteristic in G' such that $G'/T = \mathsf{C}_4 \times \mathsf{C}_4$. Thus, $f(G/T) \leqslant 3$ and $|G/T| = 48$, which contradicts Lemma 3.29. It follows that $n = 1$ and hence $G = \mathsf{A}_4$.

Therefore, we have that the prime divisors of $|G'|$ are contained in $\{2, 7\}$ and if G' is a p-group, then $G \in \{\mathsf{A}_4, \mathsf{C}_7 \rtimes \mathsf{C}_3\}$. Assume now that both 2 and 7 divide $|G'|$. Then $G'/\Phi(G) = \mathsf{C}_2 \times \mathsf{C}_2 \times \mathsf{C}_7$. Thus, $|G/\Phi(G)| = 84$ and $f(G/\Phi(G)) \leqslant 3$, which is impossible by Lemma 3.29. Then G' must be a p-group and the result follows. □

THEOREM 3.41. *Let G be a metabelian group with $f(G) \leqslant 3$ such that $|G : G'| = 4$. Then $G \in \{\mathsf{C}_5 \rtimes \mathsf{C}_4, \mathsf{C}_{13} \rtimes \mathsf{C}_4\}$.*

PROOF. As in the proof of Theorem 3.39, we assume first that G' is a p-group. By Lemma 3.38, we have $G/\Phi(G) \in \{\mathsf{C}_5 \rtimes \mathsf{C}_4, \mathsf{C}_{13} \rtimes \mathsf{C}_4\}$ and hence G' is a cyclic p-group, where $p \in \{5, 13\}$.

In both cases G' is a cyclic group of order p^l. If $l \geqslant 2$, then there exists K characteristic in G' of order p^{l-2}. Thus, $|G/K| = 4 \cdot p^2$ and $f(G/K) \leqslant 3$. For $p = 5$, we have that $|G/K| = 4 \cdot 5^2 = 100$ and for $p = 13$, we have that $|G/K| = 4 \cdot 13^2 = 676$. However, by Lemma 3.29, there is no group L of order 100 or 676 with $f(L) \leqslant 3$.

Therefore, the prime divisors of $|G'|$ are contained in $\{5, 13\}$ and if G' is a p-group then $G \in \{\mathsf{C}_5 \rtimes \mathsf{C}_4, \mathsf{C}_{13} \rtimes \mathsf{C}_4\}$. Assume now that 5 and 13 and divide $|G'|$. Then $G'/\Phi(G) = \mathsf{C}_5 \times \mathsf{C}_{13}$. Thus, $f(G/\Phi(G)) \leqslant 3$ and $|G/\Phi(G)| = 4 \cdot 5 \cdot 13 = 260$, which contradicts Lemma 3.29. Therefore, G' must be a p-group and the result follows. □

3.3.4. Solvable case. In this subsection we classify all solvable groups with $f(G) \leqslant 3$. In particular, we complete the proof of Theorem B. By the results of the previous subsection, we have that

$$G/G'' \in \{\mathsf{C}_2, \mathsf{C}_3, \mathsf{C}_4, \mathsf{S}_3, \mathsf{D}_{10}, \mathsf{A}_4, \mathsf{D}_{14}, \mathsf{D}_{18}, \mathsf{C}_5 \rtimes \mathsf{C}_4, \mathsf{C}_7 \rtimes \mathsf{C}_3, \mathsf{C}_{13} \rtimes \mathsf{C}_4\}.$$

Therefore, the result will be completed once we show that $G'' = 1$. We will begin by determining all possible $\mathbb{Q}(\chi)$ for $\chi \in \mathrm{Irr}(G|G'')$ and then, we will use this to bound $k(G)$. Finally, the result will follow from Theorems 3.24 and 3.26, together with some calculations.

LEMMA 3.42. *Let G be a group such that $G'' \neq 1$, $G/G'' \in \{\mathsf{S}_3, \mathsf{D}_{10}, \mathsf{D}_{14}, \mathsf{C}_7 \rtimes \mathsf{C}_3, \mathsf{C}_5 \rtimes \mathsf{C}_4, \mathsf{C}_{13} \rtimes \mathsf{C}_4\}$ and G'' is an elementary abelian p-group for some prime p not dividing $|G'/G''|$. If $r = |G : G'|$, then $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_{rp}$ for every $\chi \in \mathrm{Irr}(G|G'')$.*

PROOF. By Lemma 3.21, we know that $\chi(g) \in \mathbb{Q}_{rp}$ for every $g \in G\backslash G'$ and for every $\chi \in \mathrm{Irr}(G)$. Therefore, we only have to prove that $\mathbb{Q}(\chi_{G'}) \subseteq \mathbb{Q}_{rp}$ for every $\chi \in \mathrm{Irr}(G|G'')$. In particular, it suffices to prove that $\mathbb{Q}(\psi) \subseteq \mathbb{Q}_{rp}$ for every $\psi \in \mathrm{Irr}(G'|G'')$.

Let $\lambda \in \mathrm{Irr}(G'')\backslash\{1_{G''}\}$. Reasoning as in Lemma 3.38, we have that λ cannot be extended to an irreducible character of G'. Moreover, we have that $\mathbb{Q}(\lambda) \subseteq \mathbb{Q}_p$. Since $|G' : G''|$ is prime, we deduce that $\lambda^{G'} \in \mathrm{Irr}(G')$. Now, we have $\mathbb{Q}(\lambda^{G'}) \subseteq \mathbb{Q}(\lambda) \subseteq \mathbb{Q}_p \subseteq \mathbb{Q}_{rp}$ and the result follows. □

LEMMA 3.43. *Let G be a group such that $G'' \neq 1$, $G/G'' = \mathsf{D}_{18}$ and G'' is an elementary abelian p-group for some prime $p \neq 3$. If $f(G) \leqslant 3$, then $k(G) \leqslant 15$. Moreover, if $p = 2$, then $k(G) \leqslant 10$ and if p is an odd prime with $p \equiv -1 \pmod 3$, then $k(G) \leqslant 12$.*

PROOF. First, we claim that $\mathbb{Q}(\chi_{G'}) \subseteq \mathbb{Q}_{3p}$ for every $\chi \in \mathrm{Irr}(G|G'')$.

To see this, let $\lambda \in \mathrm{Irr}(G'')$ be any non-trivial character and let $T = I_{G'}(\lambda)$. We know that $\mathbb{Q}(\lambda) \subseteq \mathbb{Q}_p$ and λ cannot be extended to an irreducible character of G'. Since $(|G''|, |G' : G''|) = 1$, Lemma 3.23 implies that λ extends to $\mu \in \mathrm{Irr}(T)$ with $\mathbb{Q}(\mu) = \mathbb{Q}(\lambda) \subseteq \mathbb{Q}_p$. It follows that $T < G'$ and hence we have two different possibilities. The first one is that $T = G''$. In this case, $\lambda^{G'} \in \mathrm{Irr}(G')$ and hence $\mathbb{Q}(\lambda^{G'}) \subseteq \mathbb{Q}(\lambda) \subseteq \mathbb{Q}_p \subseteq \mathbb{Q}_{3p}$. The second one is that $|T : G''| = 3$. In this case, $\mathrm{Irr}(T/G'') = \{1, \rho, \rho^2\}$. By Gallagher's Theorem, we have that $\mathrm{Irr}(T|\lambda) = \{\mu, \rho\mu, \rho^2\mu\}$ and since $\mathbb{Q}(\rho) = \mathbb{Q}_3$, we deduce that $\mathbb{Q}(\psi) \subseteq \mathbb{Q}_{3p}$ for every $\psi \in \mathrm{Irr}(T|\lambda)$. Now, let $\psi \in \mathrm{Irr}(T|\lambda)$. Thus, by the Clifford Correspondence, $\psi^{G'} \in \mathrm{Irr}(G')$ and hence $\mathbb{Q}(\psi^{G'}) \subseteq \mathbb{Q}(\psi) \subseteq \mathbb{Q}_{3p}$. Thus, $\mathbb{Q}(\chi_{G'}) \subseteq \mathbb{Q}_{3p}$ for every $\chi \in \mathrm{Irr}(G|G'')$.

Assume that $f(G) \leqslant 3$. Since $\mathrm{Irr}(G/G'')$ contains 3 rational characters, we deduce that $\mathrm{Irr}(G|G'')$ does not contain any rational characters.

Assume first that p is odd. By Lemma 3.21, we know that $\chi(g) \in \mathbb{Q}_{2p} = \mathbb{Q}_p \subseteq \mathbb{Q}_{3p}$ for every $g \in G\backslash G'$ and for every $\chi \in \mathrm{Irr}(G)$. Thus, by the previous claim, if $\chi \in \mathrm{Irr}(G|G'')$, then $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_{3p}$ and hence it is either a quadratic subextension of $\mathbb{Q}_{3p}$ or a cubic subextension of $\mathbb{Q}_{3p}$. We know that $\mathbb{Q}_{3p}$ has three quadratic subextensions and at most one cubic subextension. Thus, $|\mathrm{Irr}(G|G'')| \leqslant 3 \cdot 2 + 1 \cdot 3 = 9$ and hence $k(G) = |\mathrm{Irr}(G)| = |\mathrm{Irr}(G/G'')| + |\mathrm{Irr}(G|G'')| \leqslant 6 + 9 = 15$. We also observe that $\mathbb{Q}_{3p}$ has a cubic subextension if and only if $p \equiv 1 \pmod 3$. Thus, if $p \equiv -1 \pmod 3$, then $k(G) \leqslant 12$.

Assume now that $p = 2$. In this case, $\mathbb{Q}_{3p} = \mathbb{Q}_3$. By Lemma 3.21, we know that for every $g \in G\backslash G'$ and for every $\chi \in \mathrm{Irr}(G)$, $\chi(g) \in \mathbb{Q}_{2p} = \mathbb{Q}(i)$. Thus, if $\chi \in \mathrm{Irr}(G|G'')$, then either $\mathbb{Q}(\chi) = \mathbb{Q}_3$ or $\mathbb{Q}(\chi) = \mathbb{Q}(i)$. Since $\mathbb{Q}(i)$ and $\mathbb{Q}_3$ are both quadratic, we have that $|\mathrm{Irr}(G|G'')| \leqslant 2 \cdot 2$ and hence $k(G) \leqslant 6 + 4 = 10$. □

LEMMA 3.44. *Let G be a group such that $G'' \neq 1$, $G/G'' = \mathsf{A}_4$ and G'' is an elementary abelian p-group for some prime p. If $f(G) \leqslant 3$, then $k(G) \leqslant 12$. Moreover, if $p \not\equiv 1 \pmod 3$, then $k(G) \leqslant 9$.*

PROOF. First, we study the orders of the elements of G. If $g \in G''$, then $o(g)$ divides p. If $g \in G'\backslash G''$, then $o(g)$ divides $2p$. Finally, if $g \in G\backslash G'$, then $o(g)$ divides $3p$.

Let $\chi \in \operatorname{Irr}(G)$. Then, $\mathbb{Q}(\chi_{G''}) \subseteq \mathbb{Q}_p$. If $g \in G\backslash G'$, then $\chi(g) \in \mathbb{Q}_{3p}$. Finally, if $g \in G'\backslash G''$, then $\chi(g) \in \mathbb{Q}_{2p}$. Thus, $\mathbb{Q}(\chi)$ is contained in $\mathbb{Q}_{2p}$ or in $\mathbb{Q}_{3p}$.

If $p = 2$, then $\mathbb{Q}_{2p} = \mathbb{Q}(i)$ and $\mathbb{Q}_{3p} = \mathbb{Q}_3$. Therefore, we have that $k(G) = |\operatorname{Irr}(G)| \leqslant 2 \cdot 2 + 3 = 7 < 9$.

Assume now that $p \neq 2$. Then $\mathbb{Q}_{2p} = \mathbb{Q}_p$ and it follows that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_{3p}$ for every $\chi \in \operatorname{Irr}(G)$. Assume first that $p = 3$, then $\mathbb{Q}_{3p} = \mathbb{Q}_9$ contains only one quadratic subextension and one cubic subextension. Therefore, $k(G) = |\operatorname{Irr}(G)| \leqslant 2 \cdot 1 + 3 \cdot 1 + 3 = 8 < 9$. Finally, assume that $p \neq 3$ is an odd prime. Then $\mathbb{Q}_{3p}$ has three quadratic subextensions and at most one cubic subextension. It follows that $k(G) \leqslant 2 \cdot 3 + 3 \cdot 1 + 3 = 12$. In addition, if $p \equiv -1 \pmod 3$, then $\mathbb{Q}_{3p}$ has no cubic subextension, and hence $k(G) \leqslant 9$. □

The next result completes the proof of Theorem B.

THEOREM 3.45. *Let G be a solvable group with $f(G) \leqslant 3$. Then G is one of the following groups:*

$$\mathsf{C}_2, \mathsf{C}_3, \mathsf{C}_4, \mathsf{S}_3, \mathsf{D}_{10}, \mathsf{A}_4, \mathsf{D}_{14}, \mathsf{D}_{18}, \mathsf{C}_5 \rtimes \mathsf{C}_4, \mathsf{C}_7 \rtimes \mathsf{C}_3, \mathsf{C}_{13} \rtimes \mathsf{C}_4.$$

PROOF. If G is metabelian, then G is one of the groups listed above by Theorems 3.39, 3.40 and 3.41. Therefore, we only have to prove that $G'' = 1$.

Assume for contradiction that $G'' > 1$. Taking an appropriate quotient, we may assume that G'' is a minimal normal subgroup of G. Since G is solvable, we have that G'' is an elementary abelian p-group for some prime p. We also have that G/G'' is a metabelian group with $f(G/G'') \leqslant 3$. Thus, $G/G'' \in \{\mathsf{S}_3, \mathsf{D}_{10}, \mathsf{A}_4, \mathsf{D}_{14}, \mathsf{D}_{18}, \mathsf{C}_5 \rtimes \mathsf{C}_4, \mathsf{C}_7 \rtimes \mathsf{C}_3, \mathsf{C}_{13} \rtimes \mathsf{C}_4\}$.

We claim that we can assume that G'' is the unique minimal normal subgroup of G. Suppose that there exists M, a minimal normal subgroup of G different from G''. Then MG''/G'' is a minimal normal subgroup of G/G''. On the one hand, if $G/G'' \neq D_{18}$, then the only minimal normal subgroup of G/G'' is G'/G''. Thus, $G' = M \times G''$ and hence G' is abelian, which is a contradiction. On the other hand, if $G/G'' = D_{18}$, then the only possibility is that $|M| = 3$. Let $\overline{G} = G/M$ and let $\bar{\cdot}$ denote the image in G/M. We have that $f(\overline{G}) \leqslant 3$, $\overline{G}'' = \overline{G''} = MG''/M \cong G''/(M \cap G'') = G''$ and $\overline{G}/\overline{G}'' \cong G/MG'' \cong \mathsf{S}_3$. Therefore, $\overline{G}$ will be one of the studied cases. So in any case, we may assume

that G is the only minimal subgroup of G, this is $G'' = S(G)$. In particular, $k(G/S(G)) = k(G/G'') \leqslant 7 \leqslant 10$ and so the hypothesis of Theorem 3.26 is satisfied.

Since we are assuming that G is not metabelian and $f(\mathsf{S}_4) = 5 > 3$, we may apply Theorem 3.25 to deduce that $\alpha(G) \geqslant 4$. In addition, if $k(G) \leqslant 11$, then Theorem 3.24 implies that $G'' = 1$ is the only possibility, which is a contradiction. Thus, we will assume that $k(G) \geqslant 12$. As a consequence, if $4 \leqslant \alpha(G) \leqslant 9$, then Theorem 3.26 gives $f(G) > 3$, which is impossible. Therefore, for the reminder we will assume that $k(G) \geqslant 12$ and $\alpha(G) \geqslant 10$.

Now, we proceed to study case by case. We study the cases $G/G'' = \mathsf{A}_4$ and $G/G'' \neq \mathsf{A}_4$ separately. Let us recall that G'' is an elementary abelian p-group for some prime p.

Case $G/G'' = \mathsf{A}_4$: By Lemma 3.44, if $p \not\equiv 1 \pmod 3$, then $k(G) \leqslant 9 < 12$, which is impossible. Thus, we may assume that $p \equiv 1 \pmod 3$ and $k(G) = 12$. Since $\alpha(G) \geqslant 10$, we have that G'' contains a unique G-conjugacy class of non-trivial elements. As a consequence, $|G''| \leqslant 12+1 = 13$ and we recall that $|G''| = p^k$ and that $p \equiv 1 \pmod 3$. Thus, the only possibilities are $|G''| \in \{7, 13\}$ and hence $|G| \in \{84, 156\}$. By Lemma 3.29, there is no group L of order 84 or 156 with $f(L) \leqslant 3$ and hence, we have a contradiction.

Case $G/G'' \neq \mathsf{A}_4$: In this case G'/G'' is a cyclic group. First we claim that $\gcd(|G' : G''|, p) = 1$. To see this, suppose that p divides $|G' : G''|$. Then G' is a p-group and hence $G'' \leqslant \Phi(G')$. Therefore, G' is cyclic and hence it is abelian, which is a contradiction. Thus, the claim follows. Now, we study separately the case $G/G'' = \mathsf{D}_{18}$ and the case $G/G'' \in \{\mathsf{S}_3, \mathsf{D}_{10}, \mathsf{D}_{14}, \mathsf{C}_7 \rtimes \mathsf{C}_3, \mathsf{C}_5 \rtimes \mathsf{C}_4, \mathsf{C}_{13} \rtimes \mathsf{C}_4\}$.

- Case $G/G'' = \mathsf{D}_{18}$: Since $p \neq 3$, we may apply Lemma 3.43. If $p = 2$, then $k(G) \leqslant 10 < 12$ and hence we have a contradiction. Thus, we may assume that p is odd.

  Assume now that p is an odd prime such that $p \not\equiv 1 \pmod 3$, in which case case $k(G) \leqslant 12$. Thus, $k(G) = 12$ and reasoning as in the case $G/G'' = \mathsf{A}_4$ we can deduce that G'' contains a unique G-conjugacy class of non-trivial elements. It follows that there exists $H \leqslant \mathsf{D}_{18}$ such that $|G| = 18/|H| + 1$. Since $|G''| = p^k$, for an odd prime p with $p \not\equiv 1 \pmod 3$, we get a contradiction.

  Now assume that $p \equiv 1 \pmod 3$. Here $k(G) \leqslant 15$ and as before, we can deduce that G'' contains at most 4 non-trivial conjugacy classes and hence $|G''| \leqslant 4 \cdot 18 + 1 = 73$. Therefore, $|G''| \in \{7, 13, 19, 31, 37, 43, 49, 53, 61, 67, 73\}$ and hence $|G| \in \{126, 234, 342, 558, 666, 774, 882, 954, 1098, 1206, 1314\}$. Applying again Lemma 3.29, we have a contradiction.

- Case $G/G'' \in \{\mathsf{S}_3, \mathsf{D}_{10}, \mathsf{D}_{14}, \mathsf{C}_7 \rtimes \mathsf{C}_3, \mathsf{C}_5 \rtimes \mathsf{C}_4, \mathsf{C}_{13} \rtimes \mathsf{C}_4\}$: We know that $(|G' : G''|, p) = 1$ and hence, we may apply Lemma 3.42. Thus, if $r = |G : G'|$ and $\chi \in \mathrm{Irr}(G|G'')$, we have that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_{rp}$. We study the cases $r = 2, 3, 4$ separately.

  (i) Case $G/G'' \in \{\mathsf{S}_3, \mathsf{D}_{10}, \mathsf{D}_{14}\}$: Here $|G : G'| = 2$ and hence for all $\chi \in \mathrm{Irr}(G|G'')$ we have that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_{2p} = \mathbb{Q}_p$. Thus, $\mathrm{Irr}(G|G'')$ contains at most 5 non-rational characters. We also observe that $\mathrm{Irr}(G/G'')$ possesses at most 3 non-rational character. Counting the rational characters, we get $k(G) \leqslant 3 + 3 + 5 = 11 < 12$, which is a contradiction.

  (ii) Case $G/G'' = \mathsf{C}_7 \rtimes \mathsf{C}_3$: If $\chi \in \mathrm{Irr}(G|G'')$ then $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_{3p}$. Assume first that $p \notin \{2, 3\}$. Then, $\mathbb{Q}_{3p}$ contains three quadratic extensions and at most one cubic extension and one of these quadratic extensions is $\mathbb{Q}_3$. Since we have two characters in $\mathrm{Irr}(G/G'')$ whose field of values is $\mathbb{Q}_3$ there is no character in $\mathrm{Irr}(G|G'')$ whose field of values is $\mathbb{Q}_3$. Thus, $\mathrm{Irr}(G|G'')$ contains at most $2 \cdot 2 + 3 \cdot 1 = 7$ non-rational characters, which implies $k(G) \leqslant 7 + 4 + 3 = 14$. Since $\mathbb{Q}_{3p}$ contains a cubic extension if and only if $p \equiv 1 \pmod 3$, we deduce that if $p \equiv -1 \pmod 3$, then $k(G) \leqslant 11 < 12$. Therefore, we must have $p \equiv 1 \pmod 3$. Now, reasoning as in the case $G/G'' = \mathsf{D}_{18}$, we may assume that G'' contains at most 3 non-trivial G-conjugacy classes. Therefore, $|G''|$ is a power of a prime p with $p \equiv 1 \pmod 3$, and $|G''| - 1$ must be the sum of at most three divisors of $|G/G''| = 21$. It follows that $|G''| \in \{7, 43\}$. Since $\gcd(|G' : G''|, p) = 1$, we deduce that $|G''| = 43$ and hence $|G| = 21 \cdot 43 = 903$. However, by Lemma 3.29, there is no group L of order 903 with $f(L) \leqslant 3$.

  Reasoning similarly, we can deduce that if $p = 2$, then $k(G) \leqslant 7 < 12$ and hence we have a contradiction.

  Finally, assume that $p = 3$. In this case $\mathbb{Q}_{3p} = \mathbb{Q}_9$ contains only one quadratic extension and one cubic extension. Since the unique quadratic extension of $\mathbb{Q}_9$ is $\mathbb{Q}_3$, we deduce that $\mathrm{Irr}(G|G'')$ contains at most 3 non-rational characters. Thus, $k(G) \leqslant 3+4+3 = 10 < 12$ and hence we have a contradiction.

  (iii) Case $G/G'' \in \{\mathsf{C}_5 \rtimes \mathsf{C}_4, \mathsf{C}_{13} \rtimes \mathsf{C}_4\}$: Here $G/G'' = \mathsf{C}_q \rtimes \mathsf{C}_4$ for $q \in \{5, 13\}$. Thus, applying Lemma 3.42, we have that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_{4p}$ for every $\chi \in \mathrm{Irr}(G|G'')$. Reasoning as in the case $G/G'' = \mathsf{C}_7 \rtimes \mathsf{C}_3$, we deduce that if $p \neq 2$, then $\mathrm{Irr}(G|G'')$ contains at most 7 non-rational characters and there are none if $p = 2$. Therefore, if $p = 2$ then $k(G) \leqslant 8 < 12$, which is a contradiction. Thus, we may assume that p is an odd prime.

Before studying the remaining cases, we claim that $|G''| \equiv 1 \pmod{q}$. Since $\gcd(|G : G''|, p) = 1$, applying the Schur–Zassenhaus Theorem, we have that G'' is complemented in G by $U \rtimes V$, where U is cyclic of order 4 and V is cyclic of order q. We claim that V cannot fix any non-trivial element of G''.

To see this, first we note that the action of V on G'' is coprime. Thus, by [54, Theorem 4.34], $G'' = [G'', V] \times \mathbf{C}_{G''}(V)$. Since $\mathbf{C}_{G''}(V) \leqslant G''$ is normal in G and G'' is minimal normal, either $\mathbf{C}_{G''}(V) = 1$ or $\mathbf{C}_{G''}(V) = G''$. If $\mathbf{C}_{G''}(V) = G''$, then G' is abelian, which is a contradiction. Thus, $\mathbf{C}_{G''}(V) = 1$ and hence V does not fix any non-trivial element in G''. Therefore, $|G''| \equiv 1 \pmod{q}$ as we claimed. We now consider the two possibilities for G/G'' in turn.

a) Case $G/G'' = \mathsf{C}_5 \rtimes \mathsf{C}_4$: It is easy to see that $k(G) \leqslant 12$. Moreover, if $p \not\equiv 1 \pmod{3}$, then $k(G) \leqslant 9$, which is impossible. Thus, as in the case $G/G'' = \mathsf{A}_4$, we may assume that $p \equiv 1 \pmod{3}$ and that G'' possesses a unique non-trivial G-conjugacy class. Therefore, $|G''| \leqslant 20 + 1 = 21$, $|G''| \equiv 1 \pmod{5}$ and we recall that $|G''|$ is a power of p. It is easy to see that there is no integer with the required properties, and hence we have a contradiction.

b) Case $G/G'' = \mathsf{C}_{13} \rtimes \mathsf{C}_4$: It is easy to see that $k(G) \leqslant 15$. As in the case $G/G'' = \mathsf{D}_{18}$, we may assume that G'' contains at most 4 non-trivial G-conjugacy classes. Therefore, $|G''| \leqslant 4 \cdot 52 + 1 = 209$. It follows that $|G''| \equiv 1 \pmod{13}$, $|G''| \leqslant 209$ and $|G''|$ is a power of p. Thus, $|G''| \in \{27, 53, 79, 131, 157\}$ and hence $|G| \in \{1404, 2756, 4108, 6812, 8164\}$, which contradicts Lemma 3.29.

We conclude that $G'' = 1$ and the result follows. □

Now, Theorem B follows from Theorems 3.30 and 3.45.

3.4. Proof of Theorem C

3.4.1. Special cases. In this subsection, we prove that Theorem C holds for groups satisfying some special conditions. We begin by using Lemma 3.3 to prove Theorem C for groups with $h(G) = 1$.

PROPOSITION 3.46. *Let G be a group. Then $h(G) = 1$ if and only if $G = 1$.*

PROOF. Assume that G is a group with $h(G) = 1$. By Lemma 3.3, all conjugacy classes of G are rational. Now, the condition $h(G) = 1$ implies that G possesses only one rational conjugacy class, and hence G is a group with a unique conjugacy class. Thus, $G = 1$. □

There are specific situations in which the actions of $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ on $\mathrm{Irr}(G)$ and on $\mathrm{Cl}(G)$ are isomorphic. For example, [4, Theorem A] proves that the actions of $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ on $\mathrm{Irr}(G)$ and on $\mathrm{Cl}(G)$ are permutation isomorphic for inverse semi-rational groups. In particular, $|\mathrm{Cl}_{\mathbb{Q}}(G)| = |\mathrm{Irr}_{\mathbb{Q}}(G)|$ for inverse semi-rational groups. The key for proving this result is the following lemma, which was proved as a claim during the proof of [4, Theorem 3.1].

LEMMA 3.47. *Let Γ be a group acting on two finite sets X and Y satisfying the following conditions:*

(i) Each $\sigma \in \Gamma$ fixes the same number of points in X and Y.

(ii) Each Γ-orbit on X and Y has size at most 2.

Then the actions of Γ on X and Y are permutation isomorphic.

Let G be any group, let $\Gamma = \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$, $X = \mathrm{Cl}(G)$ and $Y = \mathrm{Irr}(G)$. Condition (i) of Lemma 3.47 holds by Theorem 2.14. Observe also that Condition (ii) of Lemma 3.47 holds if G is both quadratic rational and semi-rational. With these comments, we have the following.

COROLLARY 3.48. *Let G be a quadratic rational and semi-rational group. Then, the actions of $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ on $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$ are permutation isomorphic.*

Now, we prove the following result.

THEOREM 3.49. *Let G be a group with $|\mathrm{Irr}_{\mathbb{Q}}(G)| = |\mathrm{Cl}_{\mathbb{Q}}(G)|$. Then G is quadratic rational if and only if G is semi-rational. Moreover, in such a case, the actions of $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ on $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$ are permutation isomorphic.*

PROOF. Let $\Gamma = \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ and let $t = |\mathrm{Irr}_{\mathbb{Q}}(G)| = |\mathrm{Cl}_{\mathbb{Q}}(G)|$. By Corollary 2.15, we have that Γ has the same number of orbits on $\mathrm{Irr}(G)$ and on $\mathrm{Cl}(G)$. Let k be this number and observe that $k \geqslant t$. Now, if we decompose $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$ into Γ-orbits, then

$$\mathrm{Irr}(G) = \mathrm{Irr}_{\mathbb{Q}}(G) \cup \Big(\bigcup_{i=t+1}^{k} T_i \Big)$$

and

$$\mathrm{Cl}(G) = \mathrm{Cl}_{\mathbb{Q}}(G) \cup \Big(\bigcup_{i=t+1}^{k} L_i \Big),$$

where the T_i and the L_i are the non-trivial Γ-orbits of its respective actions (in particular, $|T_i| \geqslant 2$ and $|L_i| \geqslant 2$).

Assume first that G is quadratic rational. In this case, $|T_i| = 2$ for all i. Since $|\operatorname{Irr}(G)| = |\operatorname{Cl}(G)|$, we have

$$|\operatorname{Irr}_{\mathbb{Q}}(G)| + 2(k-t) = |\operatorname{Irr}(G)| = |\operatorname{Cl}(G)| = |\operatorname{Cl}_{\mathbb{Q}}(G)| + \sum_{i=t+1}^{k} |L_i|.$$

Finally, by hypothesis, we have that

$$\sum_{i=t+1}^{k} |L_i| = 2(k-t).$$

Since $|L_i| \geqslant 2$ for all i, this forces $|L_i| = 2$ for all i, or equivalently, that G is semi-rational.

Now, if G is semi-rational, then with a very similar argument we can deduce that G is quadratic rational.

The second part follows from Corollary 3.48. □

We mention that when $|G|$ is odd (equivalently, $|\operatorname{Irr}_{\mathbb{Q}}(G)| = |\operatorname{Cl}_{\mathbb{Q}}(G)| = 1$) a strengthened version of Theorem 3.49 was known. By [**98**, Theorem A], if $|G|$ is odd, then the number of quadratic character coincides with the number of semi-rational classes. In particular, if G is odd, then $|G|$ is quadratic rational if and only if it is semi-rational. This was observed in the first paragraph of Section 6 of [**120**].

Next we prove Theorem C for groups with $h(G) = 2$.

THEOREM 3.50. *Let G be a group. Then $f(G) = 2$ if and only if $h(G) = 2$.*

PROOF. If $f(G) = 2$, then G is one of the groups listed in Theorem B. Thus, it suffices to observe that $h(G) = 2$ in each case.

Assume now that $h(G) = 2$. In this case, G is a group $|\operatorname{Cl}_{\mathbb{Q}}(G)| \leqslant 2$ and hence, by the previous comments, we have $|\operatorname{Irr}_{\mathbb{Q}}(G)| = |\operatorname{Cl}_{\mathbb{Q}}(G)| = 2$. In addition, by Lemma 3.5, we have that $|\mathbb{Q}(K) : \mathbb{Q}| \leqslant 2$ for all $K \in \operatorname{Cl}(G)$ and hence G is a semi-rational group.

Thus, G is a semi-rational group with $|\operatorname{Irr}_{\mathbb{Q}}(G)| = |\operatorname{Cl}_{\mathbb{Q}}(G)|$ and hence, by Theorem 3.49, the actions of $\operatorname{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ on $\operatorname{Irr}(G)$ and $\operatorname{Cl}(G)$ are permutation isomorphic. Therefore, $f(G) = h(G) = 2$. □

As a consequence, we can prove Theorem C for groups with $|\operatorname{Cl}_{\mathbb{Q}}(G)| = 1$.

PROPOSITION 3.51. *Let G be a group with $h(G) \leqslant 3$ and $|\mathrm{Cl}_{\mathbb{Q}}(G)| = 1$. Then the actions of $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ on $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$ are permutation isomorphic. In particular, $f(G) = h(G)$.*

PROOF. Since $|\mathrm{Cl}_{\mathbb{Q}}(G)| = 1$, it follows that $|G|$ is odd. By hypothesis, we know that $|\mathbb{Q}(g) : \mathbb{Q}| \leqslant 3$ for any $g \in G$.

We claim that $|\mathbb{Q}(g) : \mathbb{Q}| \leqslant 2$ for any $g \in G$. Assume for contradiction that there exists $g \in G$ such that $|\mathbb{Q}(g) : \mathbb{Q}| = 3$. Since $|\mathbb{Q}(g) : \mathbb{Q}| = 3$, we have that $|\mathrm{Aut}(\langle g \rangle) : B_G(g)| = 3$. Then $\varphi(o(g)) = |\mathrm{Aut}(\langle g \rangle)| = 3|B_G(g)|$. Now, we observe that $|B_G(g)|$ is odd (since it divides $|G|$, which is odd), and hence $\varphi(o(g))$ is odd. This forces $g = 1$, which is impossible. The claim follows.

We conclude that G is a group with $h(G) = 2$ and the result follows by Theorem 3.50. □

3.4.2. The general case. In this subsection we complete the proof of Theorem C. By the results in the previous subsection, we may assume that $h(G) = 3$ and $|\mathrm{Cl}_{\mathbb{Q}}(G)| \in \{2, 3\}$.

PROPOSITION 3.52. *Let G be a group with $|\mathrm{Cl}_{\mathbb{Q}}(G)| \in \{2, 3\}$. Then $\{o(g) \mid \mathbb{Q}(g) = \mathbb{Q}\}$ is one of the following:*

(i) $\{1, 2\}$.

(ii) $\{1, 2, 4\}$.

(iii) $\{1, 2, q\}$, *where q is an odd prime.*

PROOF. Since $|\mathrm{Cl}_{\mathbb{Q}}(G)| > 1$, we have that $|G|$ is even and hence, there exists $z \in G$ an involution. Then $\{1^G, z^G\}$ are two rational classes. If $|\mathrm{Cl}_{\mathbb{Q}}(G)| = 2$, then they are the only rational classes in G and hence case (i) holds.

Assume now that $|\mathrm{Cl}_{\mathbb{Q}}(G)| = 3$. Let $x \in G$ be a rational element such that $x^G \notin \{1^G, z^G\}$. Thus, the rational conjugacy classes of G are $\{1^G, z^G, x^G\}$. It only remains to determine the order of x.

Assume first that there exists q an odd prime dividing $o(x)$. Then $o(x) = qm$ for an integer $m \geqslant 1$. We have that $\mathbb{Q} \subseteq \mathbb{Q}(x^m) \subseteq \mathbb{Q}(x) = \mathbb{Q}$ and hence $(x^m)^G$ is a rational class. Since $o(x^m) = q > 2$, we deduce that $(x^m)^G \notin \{1^G, z^G\}$. Thus, $(x^m)^G = x^G$, which forces $m = 1$, or equivalently, $o(x) = q$. Thus, case (iii) holds.

Assume now that $o(x) = 2^a$ for some $a \geqslant 1$. Assume that $a \geqslant 3$. Reasoning as before, we have that x^2 is a rational element with $2 < o(x^2) < o(x)$. Thus, $(x^2)^G \notin \{1^G, z^G, x^G\}$, which is a contradiction. This forces either $o(x) = 2$ or $o(x) = 4$. If $o(x) = 2$, then case (i) holds and if $o(x) = 4$, then case (ii) holds. □

PROPOSITION 3.53. *Let G be a group with $h(G) \leqslant 3$ and $|G|$ even. Then for each $g \in G$ there exists a prime p such that $\mathbb{Q}(g) \subseteq \mathbb{Q}_{p^3}$.*

PROOF. Since $h(G) \leqslant 3$ and $|G|$ is even, then one of the cases (i), (ii) or (iii) of Proposition 3.52 must hold. It suffices to study the possible values of $o(g)$ in each of the cases.

Let $g \in G$ and first assume that $\{o(x) \mid \mathbb{Q}(x) = \mathbb{Q}\} = \{1, 2\}$. If $\mathbb{Q}(g) = \mathbb{Q}$, then the result holds by taking any prime p. Assume that $\mathbb{Q}(g) \neq \mathbb{Q}$.

Let $1 < j$ be a divisor of of $o(g)$. Then $\mathbb{Q} \subseteq \mathbb{Q}(g^j) \subseteq \mathbb{Q}(g)$. Since $|\mathbb{Q}(g) : \mathbb{Q}| \in \{2, 3\}$, we deduce that either $\mathbb{Q}(g^j) = \mathbb{Q}$ or $\mathbb{Q}(g^j) = \mathbb{Q}(g)$. If $\mathbb{Q}(g^j) = \mathbb{Q}(g)$, then counting the Galois conjugates of g^G and $(g^j)^G$, we have at least 4 classes whose field of values is $\mathbb{Q}(g)$, so we must have $\mathbb{Q}(g^j) = \mathbb{Q}$ since $h(G) \leqslant 3$. Thus, $o(g^j) \in \{1, 2\}$ for any $j > 1$ dividing $o(g)$. This forces $o(g) = 2$, $o(g) = 4$ or $o(g) = p$ for a prime p. In the first two cases $\mathbb{Q}(g) \subseteq \mathbb{Q}_8$, and in the third case $\mathbb{Q}(g) \subseteq \mathbb{Q}_p \subseteq \mathbb{Q}_{p^3}$.

Assume now that $\{o(x) \mid \mathbb{Q}(x) = \mathbb{Q}\} = \{1, 2, 4\}$. In this case, reasoning as before, we have that either $o(g) = p$, for a prime p, or $o(g) \in \{1, 2, 4, 8\}$. In the first case $\mathbb{Q}(g) \subseteq \mathbb{Q}_{p^3}$ and in the second case $\mathbb{Q}(g) \subseteq \mathbb{Q}_8$.

Finally, let us assume that $\{o(x) \mid \mathbb{Q}(x) = \mathbb{Q}\} = \{1, 2, q\}$ for an odd prime q. In this case, we have that either $o(g) = p$ for a prime p, or $o(g) \in \{1, 2, 4, 2q, q^2\}$. Since $\mathbb{Q}_{2q} = \mathbb{Q}_q$, we have that if $o(g) \in \{2q, q^2\}$, then $\mathbb{Q}(g) \subseteq \mathbb{Q}_{q^3}$. □

Now, we restate and prove Theorem C.

THEOREM 3.54. *Let G be a group with $h(G) \leqslant 3$, then $h(G) = f(G)$.*

PROOF. Since $h(G) \leqslant 3$, we have that $|\mathrm{Cl}_{\mathbb{Q}}(G)| \leqslant 3$ and that $|\mathrm{Cl}_{\mathbb{Q}}(G)| = |\mathrm{Irr}_{\mathbb{Q}}(G)|$ by Theorem 2.25. If $|\mathrm{Cl}_{\mathbb{Q}}(G)| = 1$, then the result follows by Proposition 3.51. Let us assume that $|\mathrm{Cl}_{\mathbb{Q}}(G)| \in \{2, 3\}$.

By Proposition 3.53, we have that $\mathbb{Q}(G) \subseteq \mathbb{Q}_n$ for some $n = 2^3 p_2^3 \cdots p_t^3$ for $2 = p_1 < p_2 < \ldots < p_t$ primes. If $i > 2$, then p_i is odd and hence $\mathrm{Gal}(\mathbb{Q}_{p_i^3}/\mathbb{Q}) = \langle \sigma_i \rangle$ for an automorphism σ_i with $o(\sigma_i) = (p_i - 1)p_i^2$. In the case $p_1 = 2$, we have that $\mathrm{Gal}(\mathbb{Q}_8/\mathbb{Q}) = \langle \sigma_0 \rangle \times \langle \sigma_1 \rangle$ with $o(\sigma_0) = o(\sigma_1) = 2$.

Let $K \in \mathrm{Cl}(G)$ with $\mathbb{Q}(K) \neq \mathbb{Q}$. Our aim is to prove that

$$|\{T \in \mathrm{Cl}(G) \mid \mathbb{Q}(T) = \mathbb{Q}(K)\}| = |\{\chi \in \mathrm{Irr}(G) \mid \mathbb{Q}(\chi) = \mathbb{Q}(K)\}|.$$

By Proposition 3.53, there exists $i \in \{1, \ldots, t\}$ such that $\mathbb{Q}(K) \subseteq \mathbb{Q}_{p_i^3}$. In any case, we have that $\mathrm{Gal}(\mathbb{Q}_{p_i^3}/\mathbb{Q}(K)) = \langle \tau \rangle$, where τ does not fix any element in $\mathbb{Q}_{p_i^3} \backslash \mathbb{Q}(K)$.

Assume first that $i = 1$, that is $\mathbb{Q}(K) \subseteq \mathbb{Q}_8$. Let us set

$$\sigma = (\tau, \sigma_2, \dots, \sigma_t) \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}).$$

By Theorem 2.14, we have

$$|\{T \in \mathrm{Cl}(G) \mid T^\sigma = T\}| = |\{\chi \in \mathrm{Irr}(G) \mid \chi^\sigma = \chi\}|.$$

Let $\chi \in \mathrm{Irr}(G)$ and $g \in G$. We claim that $\chi(g)^\sigma = \chi(g)$ if and only if $\chi(g) \in \mathbb{Q}(K)$. To see this, first recall that exists j such that $\chi(g) \in \mathbb{Q}(g) \subseteq \mathbb{Q}_{p_j^3}$. If $j \geqslant 2$, then $\chi(g) = \chi(g)^\sigma = \chi(g)^{\sigma_j}$, which forces $\chi(g) \in \mathbb{Q}$. If $j = 1$, then $\chi(g) \in \mathbb{Q}_8$ and $\chi(g) = \chi(g)^\sigma = \chi(g)^\tau$, which implies that $\chi(g) \in \mathbb{Q}(K)$. Thus, $\chi(g)^\sigma = \chi(g)$ if and only if $\chi(g) \in \mathbb{Q}(K)$.

Thus,

$$\{T \in \mathrm{Cl}(G) \mid T^\sigma = T\} = \mathrm{Cl}_{\mathbb{Q}}(G) \cup \{T \in \mathrm{Cl}(G) \mid \mathbb{Q}(T) = \mathbb{Q}(K)\}$$

and

$$\{\chi \in \mathrm{Irr}(G) \mid \chi^\sigma = \chi\} = \mathrm{Irr}_{\mathbb{Q}}(G) \cup \{\chi \in \mathrm{Irr}(G) \mid \mathbb{Q}(\chi) = \mathbb{Q}(K)\}.$$

Therefore, applying Theorem 2.14, and the fact that $|\mathrm{Cl}_{\mathbb{Q}}(G)| = |\mathrm{Irr}_{\mathbb{Q}}(G)|$, we deduce that $|\{T \in \mathrm{Cl}(G) \mid \mathbb{Q}(T) = \mathbb{Q}(K)\}| = |\{\chi \in \mathrm{Irr}(G) \mid \mathbb{Q}(\chi) = \mathbb{Q}(K)\}|$.

Thus, the result holds when $\mathbb{Q}(K) \subseteq \mathbb{Q}_8$. Therefore, we deduce that $|\mathrm{Irr}_{\mathbb{Q}_8}(G)| = |\mathrm{Cl}_{\mathbb{Q}_8}(G)|$.

Now, let us assume that $\mathbb{Q}(K) \subseteq \mathbb{Q}_{p_i^3}$ for some $i \geqslant 2$. Let us set

$$\sigma = (1, \sigma_2, \dots, \sigma_{i-1}, \tau, \sigma_{i+1}, \dots, \sigma_t).$$

Applying Theorem 2.14 again, we have that

$$|\{T \in \mathrm{Cl}(G) \mid T^\sigma = T\}| = |\{\chi \in \mathrm{Irr}(G) \mid \chi^\sigma = \chi\}|.$$

Reasoning as before, we see that if $\chi \in \mathrm{Irr}(G)$ and $g \in G$, then $\chi(g)^\sigma = \chi(g)$ if and only if $\chi(g) \in \mathbb{Q}(K)$ or $\chi(g) \in \mathbb{Q}_8$. Moreover, by Proposition 3.53, we have that either $\mathbb{Q}(T) = \mathbb{Q}(K)$ or $\mathbb{Q}(T) \subseteq \mathbb{Q}_8$ for any $T \in \mathrm{Cl}(G)$ satisfying $T^\sigma = T$. Thus,

$$\{T \in \mathrm{Cl}(G) \mid T^\sigma = T\} = \mathrm{Cl}_{\mathbb{Q}_8}(G) \cup \{T \in \mathrm{Cl}(G) \mid \mathbb{Q}(T) = \mathbb{Q}(K)\}$$

and

$$\{\chi \in \mathrm{Irr}(G) \mid \chi^\sigma = \chi\} = \mathrm{Irr}_{\mathbb{Q}_8}(G) \cup \{\chi \in \mathrm{Irr}(G) \mid \mathbb{Q}(K) \subseteq \mathbb{Q}(\chi)\}.$$

Since $|\mathrm{Irr}_{\mathbb{Q}_8}(G)| = |\mathrm{Cl}_{\mathbb{Q}_8}(G)|$, and $|\mathrm{Gal}(\mathbb{Q}(K)/\mathbb{Q})| = |\{T \in \mathrm{Cl}(G) \mid \mathbb{Q}(T) = \mathbb{Q}(K)\}|$ we deduce that

$$|\mathrm{Gal}(\mathbb{Q}(K)/\mathbb{Q})| = |\{\chi \in \mathrm{Irr}(G) \mid \mathbb{Q}(K) \subseteq \mathbb{Q}(\chi)\}|.$$

Let $\psi \in \mathrm{Irr}(G)$ with $\mathbb{Q}(K) \subseteq \mathbb{Q}(\psi)$. If $\gamma \in \mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q})$, then $\mathbb{Q}(K) \subseteq \mathbb{Q}(\psi^\gamma)$ and hence

$$|\mathrm{Gal}(\mathbb{Q}(K)/\mathbb{Q})| = |\{\chi \in \mathrm{Irr}(G) \mid \mathbb{Q}(K) \subseteq \mathbb{Q}(\chi)\} \geqslant |\mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q})|.$$

This forces $\mathbb{Q}(\psi) = \mathbb{Q}(K)$ and the set $\{\chi \in \mathrm{Irr}(G) \mid \mathbb{Q}(K) \subseteq \mathbb{Q}(\chi)\}$ is just the set of Galois conjugates of ψ. As a consequence,

$$|\{T \in \mathrm{Cl}(G) \mid \mathbb{Q}(T) = \mathbb{Q}(K)\}| = |\{\chi \in \mathrm{Irr}(G) \mid \mathbb{Q}(\chi) = \mathbb{Q}(K)\}|$$

and the result follows. □

3.5. Further questions

Theorem 3.8 suggests that the invariant $h(G)$ should be enough to control $|G|$, without involving $\hat{h}(G)$. This motivates the following conjecture.

CONJECTURE 3.55. *Let G be a group. Then $|G|$ is bounded in terms of $h(G)$.*

There are few examples of groups for which $h(G) < \hat{h}(G)$. For example, only 182 of the 3596 groups of order at most 128 satisfy that $h(G) < \hat{h}(G)$. Moreover, we have that $h(G) \leqslant \hat{h}(G) < 2h(G)$ for every group with $|G| \leqslant 128$. This suggests that there should be a way to bound $\hat{h}(G)$ in terms of $h(G)$. If that was the case, then Conjecture 3.55 would follow from Theorem A.

On the other hand, our work shows that, as expected, the bounds that are attainable from [**88**] are far from best possible. Following the proof in [**88**] we can see that if $f(G) = 2$ and G is solvable, then G has at most 256 conjugacy classes. It follows from Brauer's [**12**] bound, that $|G| \leqslant 2^{2^{256}}$ for groups with $f(G) = 2$. However, Theorem B shows that the biggest group with $f(G) = 2$ has size 21. We remark that, even though there exist better bounds arising in more recent works (see, for example, [**6, 59, 105**]), they depend on non-explicit constants and it is not clear if they are better for groups with at most 256 conjugacy classes.

Theorems B and C show that, as one could expect, $f(G)$ and $h(G)$ are usually much smaller than $k(G)$. Therefore, it would be surprising to find bounds for $f(G)$ and $h(G)$ that are asymptotically of similar order of magnitude as the known bounds for $k(G)$. By Brauer's [**12**] bound, we know that $k(G) \geqslant \log_2 \log_2 |G|$. Theorems B and C show that this bound does not hold if we replace $k(G)$ by $f(G)$ or $h(G)$ when $f(G) = 2$ or 3, but it is not far off.

We propose the following conjecture. Here $\lfloor x \rfloor$ to denote the integer part of a real number x.

CONJECTURE 3.56. *We have $\min\{f(G), h(G)\} \geqslant \lfloor \log_2 \log_2 |G| \rfloor$ for every group G.*

Another interesting problem on the number of conjugacy classes of a group was proposed by Bertram in [**9**]. He asked whether $k(G) \geqslant \omega(|G|)$, where if $n = p_1^{a_1} \cdots p_t^{a_t}$ is the decomposition of the positive integer n as a product of

powers of pairwise different primes, then $\omega(n) = a_1 + \ldots + a_t$. Theorems B and C show that this definitely does not hold if we replace $k(G)$ by $f(G)$. However, it could be true that $f(G)$ and $h(G)$ control the chief length of G.

CONJECTURE 3.57. *If G is a group with exactly k chief factors, then*

$$\min\{f(G), h(G)\} \geqslant k.$$

CHAPTER 4

Commuting probability and average character degree

4.1. Introduction

In this chapter we prove results that give restrictions on the structure of a group in terms of the probability that two elements commute.

Definition. Let G be a group. We define the **commuting probability** of G to be the probability that two uniformly random elements of G commute and we will denote it by $\Pr(G)$. That is

$$\Pr(G) = \frac{|\{(x, y) \in G \times G \mid xy = yx\}|}{|G|^2}.$$

Gustafson [42] proved that

$$\Pr(G) = \frac{k(G)}{|G|},$$

where $k(G)$ is the number of conjugacy classes of G. It is worth remarking that Gustafson's proof of this result is elementary.

Remark 4.1. Some authors consider the **average class size**, defined by $\operatorname{acs}(G) = |G|/k(G)$, instead of considering the commuting probability. However, they are dual to each other, in the sense that the bound $\Pr(G) > f$ for $f \in (0, 1]$ is equivalent to $\operatorname{acs}(G) < 1/f$.

There are many results in the literature showing that the structure of G is more restricted as $\Pr(G)$ increases. Our starting point is a classical result generally attributed to Gustafson [42], which states that if $\Pr(G) > \frac{5}{8}$, then G is abelian. Moreover, since D_8 is a non-abelian group with $\Pr(\mathsf{D}_8) = \frac{5}{8}$, the bound is sharp. However, a more general result was already known. More precisely, Joseph [58] replaced the $\frac{5}{8}$ by $\frac{p^2+p-1}{p^3}$, where p is the smallest prime dividing $|G|$. It is worth remarking that in Section 3 of [42], Gustafson indicates how to obtain the bound $\frac{p^2+p-1}{p^3}$. For this reason, we will refer to the following result as the Gustafson–Joseph Theorem.

Theorem 4.2 (Gustafson; Joseph). *Let G be a group and let p be the smallest prime dividing $|G|$. Then G is abelian if and only if $\Pr(G) > \frac{p^2+p-1}{p^3}$.*

For a proof of this result, see Proposition 4.9 below. As a natural extension, Lescot [**65**] proved that if $\Pr(G) > \frac{1}{2}$, then G is nilpotent. Lescot's Theorem was extended by Guralnick and Robinson [**41**]. More precisely, they observed that if $\Pr(G) > \frac{1}{p}$, where p is the smallest prime dividing $|G|$, then G is nilpotent. This result was refined in [**51**] (see Theorem 4.14 below).

THEOREM 4.3. *Let G be a group and let p be the smallest prime dividing $|G|$. If $\Pr(G) > \frac{1}{p}$, then $|G'| = p$. In particular, $G' \leqslant \mathbf{Z}(G)$ and G is nilpotent with nilpotency class at most 2.*

Since $\Pr(\mathsf{S}_3) = \frac{1}{2}$, the bound $\frac{1}{2}$ cannot be improved when $p = 2$. However, for $p > 2$, there exists no group G such that $\Pr(G) = \frac{1}{p}$ and p is the smallest prime dividing $|G|$ (this follows from Theorems 4.14 and 4.17 below). This suggested that the bound $\Pr(G) > \frac{1}{p}$ is not sharp for odd p.

In addition, Barry, MacHale and Ni Shé [**5**] provided a bound for the supersolvabilty of a group (see Section 1.2 for the definition of supersolvable group).

THEOREM 4.4 (Barry, MacHale and Ni Shé). *Let G be a group. If $\Pr(G) > \frac{1}{3}$, then G is supersolvable.*

We remark that this result was extended, and the proof was simplified, by Hung, Lescot, and Yang [**67**]. We notice that A_4 is a non-supersolvable group with $\Pr(\mathsf{A}_4) = \frac{1}{3}$ and hence the bound $\frac{1}{3}$ is sharp.

Our goal is to determine the best possible functions $g_n(p)$ and $g_s(p)$ such that if $\Pr(G) > g_n(p)$, where p is the smallest prime dividing $|G|$, then G is nilpotent and if $\Pr(G) > g_s(p)$, then G is supersolvable. In order to define these functions, we have to introduce some notation.

Let p, q be two primes and let $r \geqslant 1$ be an integer. We say that p is a Zsigmondy prime for $\langle q, r\rangle$ if p divides $q^r - 1$ but does not divide $q^k - 1$ for $k < r$. If $\langle q, r\rangle \neq \langle 2, 6\rangle$, then a classical result of Zsigmondy [**130**] shows that there exists a Zsigmondy prime for $\langle q, r\rangle$. Given a prime $p > 2$, and $l \geqslant 1$ we define

$$\mathrm{T}(p, l) = \{q^r \mid q > p, r \geqslant l, q \text{ is a prime, } p \text{ is a Zsigmondy prime for } \langle q, r\rangle\}.$$

With this notation, we set $t(p) = \min \mathrm{T}(p, 1)$ and $r(p) = \min \mathrm{T}(p, 2)$. We recall that Dirichlet's Theorem (see [**2**, Theorem 7.9]) asserts that given $a, n \in \mathbb{N}$ with $(a, n) = 1$, then there exist infinitely many primes of the form $k \cdot n + a$ with $k \in \mathbb{N}$. As a consequence, we have that there exists a prime q such that p divides $q + 1$. In particular, p divides $q^2 - 1$. Since $p > 2$, we deduce that p cannot divide $q - 1$ and hence $q^2 \in \mathrm{T}(p, 2) \subseteq \mathrm{T}(p, 1)$. Therefore, $\mathrm{T}(p, 2)$ and $\mathrm{T}(p, 1)$ are both non-empty and hence both $t(p)$ and $r(p)$ are well-defined. Now, we define

two functions depending on p, namely

$$f_n(p) = \frac{1 + \frac{p^2-1}{t(p)}}{p^2} \tag{4.1.1}$$

and

$$f_s(p) = \frac{1 + \frac{p^2-1}{r(p)}}{p^2}. \tag{4.1.2}$$

Since $t(p), r(p) \geqslant p+1$, then both functions are bounded above by $\frac{1}{p}$. Therefore, both $f_n(p)$ and $f_s(p)$ tend to 0 as p tends to infinity and thus, we can define

$$g_n(p) = \max_{q \geqslant p, q \text{ is prime}} \{f_n(q)\} \tag{4.1.3}$$

and

$$g_s(p) = \max_{q \geqslant p, q \text{ is prime}} \{f_s(q)\}. \tag{4.1.4}$$

Before continuing, we calculate $g_n(3)$ and $g_s(3)$ as an example.

Example 4.5. We begin by calculating $t(3)$ and $r(3)$. We notice that $7 \in \mathrm{T}(3,1)$ and $25 \in \mathrm{T}(3,2)$. Moreover, elementary examination shows that they are the minimum of the respective sets and hence $t(3) = 7$ and $r(3) = 25$. Therefore

$$f_n(3) = \frac{1 + \frac{3^2-1}{7}}{3^2} = \frac{5}{21}$$

and

$$f_s(3) = \frac{1 + \frac{3^2-1}{25}}{3^2} = \frac{11}{75}.$$

We claim now that $g_n(3) = f_n(3)$ and $f_s(3) = g_s(3)$. Let $q \geqslant 5$ be a prime. Then $f_n(q) \leqslant 1/q$ and we deduce

$$f_n(q) \leqslant \frac{1}{p} \leqslant \frac{1}{5} \leqslant \frac{5}{21} = f_n(3).$$

Thus, $g_n(3) = f_n(3)$ and the claim holds in this case. Reasoning similarly, we deduce that $f_s(3) \geqslant f_s(q)$ for any prime $q \geqslant 7$. Straightforward calculations give $f_s(5) = 197/1805 < 11/75 = f_s(3)$, which completes the proof of the claim.

Here, we work with maximums because the sequences $\{f_n(q)\}$ and $\{f_s(q)\}$ are not decreasing. As an example, we have that $f_n(19) = \frac{29}{3629} < \frac{25}{1081} = f_n(23)$ and $f_s(29) = \frac{1061}{867941} < \frac{151}{115351} = f_s(31)$.

With this notation, we can state Theorems D and E.

THEOREM D. *Let $p > 2$ be a prime. Assume that $|G|$ is a group such that p is the smallest prime dividing $|G|$. If $\Pr(G) \geqslant g_n(p)$, then G is nilpotent. Moreover, the bound is best possible.*

THEOREM E. *Let $p > 2$ be a prime. Assume that $|G|$ is a group such that p is the smallest prime dividing $|G|$. If $\Pr(G) \geqslant g_s(p)$, then G is supersolvable. Moreover, the bound is best possible.*

For a given prime, say p, it is possible to calculate $g_n(p)$ and $g_s(p)$. However, since these functions depend on implicit quantities (depending on p) it is hard to understand their behavior. In Section 4.6 we will say more about the precise form of the numbers $t(p)$ and $r(p)$.

Next we turn to the average character degree, which was introduced in [**56**].

DEFINITION. Let G be a group. We define the **average character degree** of G as

$$\operatorname{acd}(G) = \frac{\sum_{\chi \in \operatorname{Irr}(G)} \chi(1)}{|\operatorname{Irr}(G)|}.$$

There exists a well-known relationship between $\operatorname{acd}(G)$ and $\Pr(G)$, namely

$$\frac{1}{\Pr(G)} = \frac{|G|}{|\operatorname{Irr}(G)|} = \frac{\sum_{\chi \in \operatorname{Irr}(G)} \chi(1)^2}{|\operatorname{Irr}(G)|} \geqslant \frac{(1/|\operatorname{Irr}(G)|)(\sum_{\chi \in \operatorname{Irr}(G)} \chi(1))^2}{|\operatorname{Irr}(G)|} = \operatorname{acd}(G)^2,$$

where the inequality follows from the Cauchy–Schwarz inequality.

There are many results showing that the structure of G is more restricted as $\operatorname{acd}(G)$ decreases. For instance, Isaacs, Loukaki and Moretó [**56**] proved that if $\operatorname{acd}(G) < \frac{3}{2}$, then G is supersolvable and if $\operatorname{acd}(G) < \frac{4}{3}$, then G is nilpotent.

On the other hand, Hung and Moretó [**92**] proved that if $\operatorname{acd}(G) < \frac{16}{5}$, then G is solvable (this was previously conjectured in [**56**]). Since $\operatorname{acd}(\mathsf{S}_3) = \frac{4}{3}$, $\operatorname{acd}(\mathsf{A}_4) = \frac{3}{2}$ and $\operatorname{acd}(\mathsf{A}_5) = \frac{16}{5}$, these bounds cannot be improved.

Our objective is to give an analogous version of Theorems D and E for the average character degree. More precisely, our goal is to improve on the following result from [**56**].

THEOREM 4.6 (Isaacs, Loukaki and Moretó). *Let G be a group and let p be the smallest prime divisor of $|G|$.*

a) If $p > 2$ and $\operatorname{acd}(G) < \frac{27}{11}$, then G is supersolvable.

b) If $\operatorname{acd}(G) < \frac{3p}{p+2}$, then G is nilpotent.

Let us observe that the bound given by a) of Theorem 4.6 is best possible. For example, there is a non-supersolvable group $G = (\mathsf{C}_5 \times \mathsf{C}_5) \rtimes \mathsf{C}_3$ with $\operatorname{acd}(G) = \frac{11}{27}$. However, this is a global bound, which does not depend on the smallest prime dividing $|G|$. Similarly, we also observe that if $2p+1$ is a prime (that is, if p is a *Sophie Germain prime*), then the bound given by b) of Theorem 4.6 cannot be improved since $\operatorname{acd}(\mathsf{C}_{2p+1} \rtimes \mathsf{C}_p) = \frac{3p}{p+2}$. However, this bound is not best possible for all primes.

Thus, our goal is to determine the best possible functions $h_n(p)$ and $h_s(p)$ such that if $\operatorname{acd}(G) < h_n(p)$, where p is the smallest prime dividing $|G|$, then G is nilpotent and if $\operatorname{acd}(G) < h_s(p)$, then G is supersolvable. In order to define $h_n(p)$ and $h_s(p)$, we introduce some notation.

Let $p > 2$ be a prime. We define $k(p)$ to be the smallest positive integer such that the smallest prime divisor of $k(p)$ is at least p and $2k(p) + 1 = q^r$, where $q \geqslant p$ is a prime. We observe that if p is a Sophie Germain prime, then $k(p) = p$. In a similar way, we define $l(p)$ as the smallest positive integer such that the smallest prime divisors of $l(p)$ is at least p and $2l(p) + 1 = q^r$, where $q \geqslant p$ is a prime and $r \geqslant 2$. In Section 4.6, we will prove that there exist integers, which satisfy the conditions defining $k(p)$ and $l(p)$ and hence both integers exist (see Theorem 4.29 below). With this notation we define

$$h_n(p) = \frac{3k(p)}{k(p)+2} \tag{4.1.5}$$

and

$$h_s(p) = \frac{3l(p)}{l(p)+2}. \tag{4.1.6}$$

We notice that $h_n(p), h_s(p) < 3$ for every prime p. Now, we state Theorems F and G.

THEOREM F. *Let $p > 2$ be a prime. Assume that G is a group such that p is the smallest prime dividing $|G|$. If $\operatorname{acd}(G) < h_n(p)$, then G is nilpotent. Moreover, the bound is best possible.*

THEOREM G. *Let $p > 3$ be a prime. Assume that G is a group such that p is the smallest prime dividing $|G|$. If $\operatorname{acd}(G) < h_s(p)$, then G is supersolvable. Moreover, the bound is best possible.*

In Theorem G, we have excluded the case $p = 3$ because $\operatorname{acd}((\mathsf{C}_5 \times \mathsf{C}_5) \rtimes \mathsf{C}_3) = \frac{27}{11} < \frac{3 \cdot 13}{13+2} = h_s(3)$ and hence the bound $h_s(3)$ is not the best possible in this case.

4.2. Preliminary results on commuting probability

As we mentioned, the commuting probability of a group G is defined as

$$\Pr(G) = \frac{|\{(x,y) \in G \times G \mid xy = yx\}|}{|G|^2}.$$

In this subsection we introduce and prove some results about the commuting probability $\Pr(G)$ that will be needed later.

PROPOSITION 4.7. *Let G be a group. Then*

$$\Pr(G) = \frac{k(G)}{|G|}.$$

PROOF. Let $k = k(G)$ and let $x_1, \ldots, x_k \in G$ be a set of representative of the conjugacy classes of G. That, is $G = \bigcup_{i=1}^{k} x_i^G$. We deduce that

$$|\{(x,y) \in G \times G \mid xy = yx\}| = \sum_{x \in G} |\mathbf{C}_G(x)| = \sum_{i=1}^{k} \sum_{x \in x_i^G} |\mathbf{C}_G(x)|,$$

where the first equality follows by fixing the first components. We also observe that $|\mathbf{C}_G(x)| = |\mathbf{C}_G(x_i)|$ for any $1 \leqslant i \leqslant k$ and any $x \in x_i^G$. It follows that $\sum_{x \in x_i^G} |\mathbf{C}_G(x)| = |x_i^G||\mathbf{C}_G(x_i)| = |G|$ for any $1 \leqslant i \leqslant k$. Then the sum above equals to $k|G|$.

Therefore,

$$\Pr(G) = \frac{|\{(x,y) \in G \times G \mid xy = yx\}|}{|G|^2} = \frac{k|G|}{|G|^2} = \frac{k}{|G|}$$

and the result follows. □

LEMMA 4.8. *Let G be a group.*

(i) For any $H \leqslant G$, we have

$$|G:H|^{-1}k(H) \leqslant k(G) \leqslant |G:H|k(H)$$

and

$$|G:H|^{-2}\Pr(H) \leqslant \Pr(G) \leqslant \Pr(H).$$

(ii) For any normal subgroup N of G, we have

$$k(G) \leqslant k(N)k(G/N)$$

and

$$\Pr(G) \leqslant \Pr(N)\Pr(G/N).$$

(iii) For any other group T, we have

$$k(G \times T) = k(G)k(T)$$

and

$$\Pr(G \times T) = \Pr(G)\Pr(T).$$

PROOF. In each part, the second statement follows immediately from the first, so we just need to establish the first statement. The fact that $|G : H|^{-1}k(H) \leqslant k(G) \leqslant |G : H|k(H)$ was proved by Gallagher [32]. The fact that $k(G) \leqslant k(N)k(G/N)$ was proved by Nagao [96]. Finally, the fact that $k(G \times T) = k(G)k(T)$ is trivial. □

For completeness, we prove the bound on $\Pr(G)$ for non-abelian groups. This was proved in [58] and an modern proof can be found in [16].

PROPOSITION 4.9. *Let G be a group and p the smallest prime dividing $|G|$. If G is not abelian, then*

$$\Pr(G) \leqslant \frac{p^2 + p - 1}{p^3}$$

with equality if and only if $G/\mathbf{Z}(G) = \mathsf{C}_p \times \mathsf{C}_p$. In particular, $\Pr(G) \leqslant 5/8$.

PROOF. Let $K_1, \ldots, K_t$ be the non-central conjugacy classes of G. We observe that $k(G) = t + |\mathbf{Z}(G)|$. Since each $|K_i|$ divides $|G|$, we have $|K_i| \geqslant p$ and thus

$$|G| = |\mathbf{Z}(G)| + \sum_{i=1}^{t} |K_i| \geqslant |\mathbf{Z}(G)| + tp,$$

which implies that $t \leqslant (|G| - |\mathbf{Z}(G)|)/p$. Thus, $k = |\mathbf{Z}(G)| + t \leqslant \frac{p-1}{p}|\mathbf{Z}(G)| + \frac{|G|}{p}$.

Moreover, since $G/\mathbf{Z}(G)$ is non-cyclic and G is non-abelian, we deduce that $|\mathbf{Z}(G)| \leqslant |G|/p^2$ and hence $k(G) \leqslant \frac{p^2+p-1}{p^3}|G|$. By Proposition 4.7, we have that $\Pr(G) = k(G)/|G| \leqslant \frac{p^2+p-1}{p^3}$ and the inequality part follows.

From the above argument, we see that the equality $\Pr(G) = \frac{p^2+p-1}{p^3}$ holds if and only if $G/\mathbf{Z}(G) = \mathsf{C}_p \times \mathsf{C}_p$ and $|K_i| = p$ for every i. It suffices to prove that if $G/\mathbf{Z}(G) = \mathsf{C}_p \times \mathsf{C}_p$, then $|x_i^G| = p$ for every $x \in G \backslash \mathbf{Z}(G)$.

Assume that $G/\mathbf{Z}(G) = \mathsf{C}_p \times \mathsf{C}_p$ and let $x \in G \backslash \mathbf{Z}(G)$. Since $x \in \mathbf{C}_G(x) \backslash \mathbf{Z}(G)$, we have that $\mathbf{Z}(G) < \mathbf{C}_G(x)$. Therefore, $|x^G| = \frac{|G|}{|\mathbf{C}_G(x)|}$ is a proper divisor of $\frac{|G|}{|\mathbf{Z}(G)|} = p^2$. On the other hand, since x is not central, $|x^G| > 1$. Thus, $|x^G| = p$, and the claim follows. □

REMARK 4.10. Note that if G is an extraspecial p-group of order p^3 with p odd or if $G = \mathsf{D}_8$ when $p = 2$, then $G/\mathbf{Z}(G) = \mathsf{C}_p \times \mathsf{C}_p$. Therefore, the bound in Lemma 4.9 is sharp for any prime.

Proposition 4.9 was proved by computing the sizes of the conjugacy classes. We next give a bound for $\Pr(G)$ by computing the character degrees. The new bound for $\Pr(G)$ will be stated in terms of the smallest prime factor of the order of G and the order of its derived subgroup G'. The following result is [**51**, Lemma 2.2].

LEMMA 4.11. *If p is the smallest prime dividing the order of a group G, then*

$$\Pr(G) \leqslant \frac{1 + (p^2 - 1)/|G'|}{p^2}.$$

PROOF. Let $\chi_1, \ldots, \chi_t$ be the non-linear irreducible characters of G and note that $t = (k(G) - |G : G'|)$. Moreover, $\chi_i(1) > 1$ and divides $|G|$ for each i. We have

$$|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = |G : G'| + \sum_{i=1}^{t} \chi_i(1)^2 \geqslant |G/G'| + p^2(k(G) - |G/G'|).$$

After dividing both sides of by $|G|$, we obtain $1 \geqslant 1/|G'| + p^2(\Pr(G) - 1/|G'|)$ and the result follows. □

REMARK 4.12. Since $\Pr(G) = k(G)/|G|$, it is easy to see that if all non-linear irreducible characters have degree $f > 1$, then $\Pr(G) = \frac{1+(f^2-1)/|G'|}{f^2}$.

LEMMA 4.13. *Let G be a group and p the smallest prime dividing $|G|$. Suppose that $|G'| \leqslant p$. Then $G' \leqslant \mathbf{Z}(G)$, and thus $G/\mathbf{Z}(G)$ is abelian. In particular, G is nilpotent with nilpotency class at most 2.*

PROOF. The case $|G'| = 1$ is obvious, so we assume $|G'| = p$. Since G' is normal and its order is the smallest prime dividing $|G|$, we deduce that G' is central in G, and the result follows. □

Next we refine Proposition 4.9. It follows from [**41**, Lemma 2(xiii)] of Guralnick and Robinson that if $\Pr(G) > \frac{1}{p}$, where p is the smallest prime dividing $|G|$, then G is nilpotent.

THEOREM 4.14. *Let G be a group and p the smallest prime dividing $|G|$. Then $\frac{1}{p} < \Pr(G) \leqslant \frac{p^2+p-1}{p^3}$ if and only if $|G'| = p$. Moreover, in this case we have*

$$\Pr(G) = \frac{1}{p} + \frac{p-1}{p|G : \mathbf{Z}(G)|}.$$

PROOF. Assume that G is a group such that p is the smallest prime dividing $|G|$. Assume first that $\Pr(G) \in (\frac{1}{p}, \frac{p^2+p-1}{p^3}]$. By Proposition 4.9 we deduce that G is non-abelian and hence $|G'| \geqslant p$. Seeking a contradiction, suppose that

$|G'| \geqslant p+1$. Then applying Lemma 4.11, we have $\Pr(G) \leqslant \frac{1}{p}$, which is a contradiction. Thus, $|G'| = p$ and the result follows.

Conversely, assume that $|G'| = p$. Then $G' \leqslant \mathbf{Z}(G)$ by Lemma 4.13. By [**53**, Problem 2.13], we have $\chi(1)^2 = |G : \mathbf{Z}(G)|$ for every $\chi \in \mathrm{Irr}(G)$ with $\chi(1) > 1$. We deduce that

$$|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = |G|/p + |G : \mathbf{Z}(G)|(k(G) - |G|/p),$$

and it follows that

$$\Pr(G) = \frac{1}{p} + \frac{p-1}{p|G : \mathbf{Z}(G)|} > \frac{1}{p},$$

as stated. □

REMARK 4.15. It is worth noting that if $G/\mathbf{Z}(G) \cong \mathsf{C}_p \times \mathsf{C}_p$, where p is the smallest prime dividing $|G|$, then, by Lemma 4.9, we have $\Pr(G) = \frac{p^2+p-1}{p^3} > \frac{1}{p}$, and hence $|G'| = p$ by Theorem 4.14.

The next theorem determines the groups with $\Pr(G) = \frac{1}{p}$, where p the smallest prime dividing $|G|$. This result could be compared with a result of Lescot [**66**] stating that $\Pr(G) = \frac{1}{2}$ if and only if G is isoclinic to the symmetric group S_3. We need to state an auxiliary lemma, which is part of [**41**, Lemma 2].

LEMMA 4.16. *Let G be a group.*

(i) If G is non-abelian with $\Pr(G) > 11/27$, then either G is nilpotent with $|G'| \in \{2, 4\}$ or $G/\mathbf{Z}(G) \cong \mathsf{S}_3$.

(ii) If π is a set of primes such that G has an abelian Sylow p-subgroup for each prime $p \in \pi$ and $Z \leqslant G$ is a central π-subgroup of G, then we have $\Pr(G) = \Pr(G/Z)$.

PROOF. Part (i) follows from the proof of [**41**, Lemma 2 (xii)] and part (ii) is [**41**, Lemma 2 (xiii)]. □

THEOREM 4.17. *Let G be a group with $|G'| > p$, where p is the smallest prime dividing $|G|$. Then $\Pr(G) \leqslant \frac{1}{p}$ with equality if and only if $p = 2$ and $G/\mathbf{Z}(G) \cong \mathsf{S}_3$.*

PROOF. Since $|G'| > p$, we have $|G'| \geqslant p+1$, so Lemma 4.11 implies that

$$\Pr(G) \leqslant \frac{1 + (p^2-1)/|G'|}{p^2} \leqslant \frac{1 + (p^2-1)/(p+1)}{p^2} = \frac{1}{p}.$$

Assume first that $\Pr(G) = \frac{1}{p}$. This forces $|G'| = p+1$. Since p is the smallest prime dividing $|G|$ and $p+1 = |G'|$ divides $|G|$, we deduce that $p = 2$ and

$|G'| = 3$. Since $\Pr(G) = \frac{1}{2} > \frac{11}{27}$, then either $|G'| \in \{2, 4\}$ or $G/\mathbf{Z}(G) \cong \mathsf{S}_3$, by (i) of Lemma 4.16. Since $|G'| = 3$, we deduce that $G/\mathbf{Z}(G) \cong \mathsf{S}_3$.

Assume now that $G/\mathbf{Z}(G) = \mathsf{S}_3$. Let q be a prime dividing $|G|$ and let $Q \in \mathrm{Syl}_q(G)$. Since $G/\mathbf{Z}(G) = \mathsf{S}_3$, we deduce that $|Q : \mathbf{Z}(Q)| \leqslant q$ and hence Q is abelian. It follows that G possesses an abelian Sylow q-subgroup for every prime q dividing $|G|$. Thus, by (ii) of Lemma 4.16, we have

$$\Pr(G) = \Pr(G/\mathbf{Z}(G)) = \Pr(\mathsf{S}_3) = \frac{1}{2}$$

and the result follows. □

4.3. Nilpotent groups of odd order

Our goal in this section is to prove Theorem D. We will assume that all groups in this subsection have odd order, so in particular, they are solvable by the Feit–Thompson Theorem. We say that G is a **minimal non-nilpotent** group if G is non-nilpotent but every proper subgroup is. We have the following result about these groups.

THEOREM 4.18 (Theorem 9.1.9 of [**107**]). *Let G be a minimal non-nilpotent group. Then there exist p and q, two different primes, such that $G = Q \rtimes P$, where $P \in \mathrm{Syl}_p(G)$ is cyclic and $Q \in \mathrm{Syl}_q(G)$.*

Now, we reduce the proof of Theorem D to bounding $\Pr(T)$ for some groups T. Let n be a positive integer. Throughout the rest of this chapter we will write C_n to denote the cyclic group of order n. Moreover, if n is a power of a prime, we will write H_n to denote the elementary abelian group of order n.

LEMMA 4.19. *Let G be a non-nilpotent group such that the smallest prime dividing $|G|$ is at least p, where p is a prime, $\Pr(G) > g_n(p)$ and it has minimal order with these properties. Then G has the form $G = \mathsf{H}_{q^l} \rtimes \mathsf{C}_r$, where $q, r \geqslant p$ are two odd primes, $l \geqslant 1$ is an integer and the action of C_r is faithful and irreducible (that is, C_r does not fix any proper non-trivial subspace of H_{q^l}).*

PROOF. By the minimality of $|G|$ and Lemma 4.8, we deduce that every proper subgroup of G is nilpotent and every proper quotient is nilpotent. Since all proper subgroups are nilpotent, we have that G is a minimal non-nilpotent group. Thus, by Theorem 4.18, we have that $G = Q \rtimes R$, where $R = \mathsf{C}_{r^k}$ for some integer $k \geqslant 1$ and some prime r.

Now, if $\mathbf{Z}(G) > 1$, then $G/\mathbf{Z}(G)$ is nilpotent and hence G is nilpotent, a contradiction. Therefore, $\mathbf{Z}(G) = 1$. If $k \geqslant 2$, then $Q\mathsf{C}_{r^{k-1}}$ is nilpotent and hence $1 \neq \mathsf{C}_{r^{k-1}}$ is central in G. This forces $k = 1$ and hence we deduce that $R = \mathsf{C}_r$.

Now, we prove Q is a minimal normal subgroup of G. Assume that there exists $1 < N < Q$ a normal subgroup of G. It follows that G/N is nilpotent and hence the action of R on Q/N is trivial. Thus, by [**54**, Corollary 3.28], we have that

$$Q/N = \mathbf{C}_{Q/N}(R) = \mathbf{C}_Q(R)/N,$$

and hence $\mathbf{C}_Q(R) = Q$, or equivalently $[Q, R] = 1$. Since $G = Q \rtimes R$, we deduce that G is nilpotent, which is impossible. That contradiction implies that Q is a minimal normal subgroup and the result follows. □

REMARK 4.20. Let V be an $\mathbb{F}_q$-vector space of dimension k for a prime q and an integer l. Then there exists $x \in \mathrm{GL}(V)$ an element of order $|V|-1$ moving every element of $V\backslash\{1\}$ (see [**117**]). The subgroup $\langle x \rangle$ is said to be a **Singer cycle**. Let $1 < d$ be a divisor of $|V| - 1$ and let $y = x^{\frac{|V|-1}{d}}$. Then $V \rtimes \langle y \rangle \cong \mathsf{H}_{q^k} \rtimes \mathsf{C}_d$ is a Frobenius group with Frobenius complement $\langle y \rangle \cong \mathsf{C}_d$.

Now, we only have to bound $\Pr(T)$ for groups T of the form described in Lemma 4.19. Let p be a prime. We define the group T_p as

$$T_p := \mathsf{H}_{t(p)} \rtimes \mathsf{C}_p, \tag{4.3.1}$$

where the action is given by Remark 4.20. We observe that T_p has the form described in Lemma 4.19 and that

$$\Pr(T_p) = \frac{1 + \frac{p^2-1}{t(p)}}{p^2} = f_n(p),$$

where $f_n(p)$ is the function defined in (4.1.1). The following result will be the key for proving Theorem D.

LEMMA 4.21. *Let $G = \mathsf{H}_{q^l} \rtimes \mathsf{C}_r$, where q, r are two odd primes, $l \geqslant 1$ and the action of C_r is faithful and irreducible. If $p = \min\{r, q\}$, then*

$$\Pr(G) \leqslant \Pr(T_p) = \frac{1 + \frac{p^2-1}{t(p)}}{p^2} = f_n(p).$$

PROOF. We observe that all non-linear characters of G have degree r. Therefore, by Remark 4.12, we have that

$$\Pr(T) = \frac{1 + \frac{r^2-1}{q^l}}{r^2}.$$

Now, we have two possibilities for p: $p = r$ or $p = q$. Assume first that $r = p$. In this case, by definition of $t(p)$, we have $q^l \geqslant t(p)$, so

$$\Pr(T) = \frac{1 + \frac{p^2-1}{q^l}}{p^2} \leqslant \frac{1 + \frac{p^2-1}{t(p)}}{p^2}$$

and the result holds in this case.

Assume now that $q = p$. Since $r > p$ and r, p are odd primes, we have that $r \geqslant p + 2$. We claim that $l > 2$. Assume for contradiction that $l = 1$. Then $r > p$ and r divides $|\operatorname{Aut}(\mathsf{C}_p)| = p - 1$, which is absurd. Similarly, if $l = 2$, then r divides $|\operatorname{Aut}(\mathsf{C}_p \times \mathsf{C}_p)| = |\mathrm{GL}(2, p)| = p(p+1)(p-1)^2$, which is impossible once again. Thus, $l \geqslant 3$ and $q^l = p^l \geqslant p^3$. Therefore, we have the following inequalities

$$\Pr(T) = \frac{1 + \frac{r^2-1}{q^l}}{r^2} \leqslant \frac{1 + \frac{(p+2)^2-1}{p^3}}{(p+2)^2} \leqslant \frac{1}{p^2} \leqslant \frac{1 + \frac{p^2-1}{t(p)}}{p^2}$$

and we conclude that the result also holds in this case. □

Now, we prove Theorem D. Before beginning the proof we recall that $g_n(p)$ was defined in (4.1.3) as the maximum of all $f_n(q)$, where q runs through all primes at least p.

Proof of Theorem D. Let G be a counterexample of minimal order. By Lemma 4.19, we may assume that G has the form $\mathsf{H}_{q^l} \rtimes \mathsf{C}_r$, where q and r are primes. Let $t = \min\{r, q\} \geqslant p$. Thus, applying Lemma 4.21, we deduce that

$$\Pr(G) \leqslant f_n(t) \leqslant g_n(p)$$

and the result follows.

It only remains to prove that the bound is sharp. Let $q \geqslant p$ be a prime such that $g_n(p) = f_n(q)$ and let $G := \mathsf{C}_p \times T_q$, where T_q is the group defined in (4.3.1). Then G is non-nilpotent, p is the smallest prime dividing $|G|$ and

$$\Pr(G) = \Pr(\mathsf{C}_p) \Pr(T_q) = \Pr(T_q) = f_n(q) = g_n(p).$$

Thus, the bound is sharp. □

4.4. Supersolvable groups of odd order

Our goal in this section is to prove Theorem E. As in the case of nilpotent groups, we will begin by reducing the problem to a special case. We say that G is a **just non-supersolvable** group if G is solvable but not supersolvable and every proper quotient of G is supersolvable. The following result determines the structure of a just non-supersolvable group.

Theorem 4.22 (Theorem 3.3 of [**108**]). *Let G be a just non-supersolvable group. Then $G = \mathbf{F}(G) \rtimes M$, where M is a supersolvable group acting faithfully on $\mathbf{F}(G)$ and (G) is the unique minimal normal subgroup of G. In particular, $\mathbf{F}(G)$ is a non-cyclic elementary abelian group and it is a faithful and simple as an M-module.*

Lemma 4.23. *Let G be solvable group which is not supersolvable. Then $\Pr(G) \leqslant \Pr(T)$, where $T = \mathsf{H}_{q^l} \rtimes \mathsf{C}_r$, q and r are two primes dividing $|G|$, $l \geqslant 2$ and the action of C_r is faithful and irreducible.*

PROOF. Let N be a normal subgroup of G such that G/N is non-supersolvable and assume that N has maximal order with this property. Then $G_0 := G/N$ is a just non-supersolvable group and hence, by Theorem 4.22, we have that $G_0 = \mathbf{F}(G_0) \rtimes (G_0/\mathbf{F}(G_0))$, where $\mathbf{F}(G_0)$ is q-elementary abelian for some prime q. Now, taking quotients and subgroups in G_0, we can obtain $T = \mathsf{H}_{q^l} \rtimes \mathsf{C}_r$, where the action of C_r is faithful and simple. Thus, by Lemma 4.8, we have the following inequalities

$$\Pr(G) \leqslant \Pr(G_0) \leqslant \Pr(T)$$

and hence, the result follows. □

Now, given a prime p, we define the group R_p as

$$R_p := \mathsf{H}_{r(p)} \rtimes \mathsf{C}_p, \tag{4.4.1}$$

where the action is given by Remark 4.20. We observe that R_p has the form as the group T described in Lemma 4.23 and that

$$\Pr(R_p) = \frac{1 + \frac{p^2-1}{r(p)}}{p^2} = f_s(p)$$

where $f_s(p)$ is the function defined in defined in (4.1.2).

LEMMA 4.24. *Let $T = \mathsf{H}_{q^l} \rtimes \mathsf{C}_r$, where q, r are two odd primes, $l \geqslant 2$ and the action of C_r is faithful and irreducible. If $p = \min\{r, q\}$, then*

$$\Pr(T) \leqslant \Pr(R_p) = \frac{1 + \frac{p^2-1}{r(p)}}{p^2} = f_s(p).$$

PROOF. We have two possibilities for p: $p = r$ or $p = q$. If $q = p$ then we can argue as in Lemma 4.21 to show that $l \geqslant 3$. Therefore, we can prove that

$$\Pr(G) \leqslant \frac{1}{p^2} \leqslant \Pr(R_p).$$

Similarly, the case $p = r$ also follows by arguing as in Lemma 4.21. □

Now, we prove Theorem E. Before beginning the proof we recall that $g_s(p)$ was defined in (4.1.4) as the maximum of all $f_s(q)$, where q runs through all primes at least p.

PROOF OF THEOREM E. Suppose that G is a non-supersolvable group of odd order. By the Feit–Thompson Theorem, we have that G is a solvable group, so Lemma 4.23, we have that $\Pr(G) \leqslant \Pr(T)$, where T has the form $T = \mathsf{H}_{q^l} \rtimes \mathsf{C}_r$ such that q, r are two primes dividing $|G|$, $l \geqslant 2$ and the action of C_r is faithful and simple. Now, let $t = \min\{q, r\} \geqslant p$. Thus, applying Lemma 4.24, we have that

$$\Pr(T) \leqslant f_s(t) \leqslant g_s(p)$$

and the result follows.

It only remains to prove that the bound is sharp. Let $q \geqslant p$ be primes such that $g_s(p) = f_s(q)$ and let $G := \mathsf{C}_p \times R_q$, where T_q is the group defined in (4.4.1). Then G is non-supersolvable, p is the smallest prime dividing $|G|$ and

$$\Pr(G) = \Pr(\mathsf{C}_p)\Pr(R_q) = \Pr(R_q) = f_s(q) = g_s(p).$$

Thus, the bound is sharp. □

4.5. Average character degree

4.5.1. Preliminaries. In this subsection we prove some preliminary results $\operatorname{acd}(G)$. We begin by proving the following easy lemma.

LEMMA 4.25. *Let G, H be groups. Then* $\operatorname{acd}(H \times G) = \operatorname{acd}(H)\operatorname{acd}(G)$.

PROOF. This follows immediately from the fact that $\operatorname{Irr}(H \times G) = \{\chi \times \psi \mid \chi \in \operatorname{Irr}(H), \psi \in \operatorname{Irr}(G)\}$. □

Our first interest is to relate $\operatorname{acd}(G)$ and $\operatorname{acd}(G/N)$ as we did in the case of the commuting probability. Let us introduce some notation. Let $N \trianglelefteq G$ and let $\theta \in \operatorname{Irr}(N)$. We set

$$\operatorname{acd}(G|\theta) = \frac{\sum_{\chi \in \operatorname{Irr}(G|\theta)} \chi(1)}{|\operatorname{Irr}(G|\theta)|}.$$

The following result was communicated to me by my advisor.

LEMMA 4.26 (Moretó). *Let G be a group and let p be the smallest prime dividing $|G|$. If* $\operatorname{acd}(G) \leqslant p$, *then* $\operatorname{acd}(G/N) \leqslant \operatorname{acd}(G)$ *for every* $N \trianglelefteq G$.

PROOF. First, we claim that if $\theta \in \operatorname{Irr}(N)$ is either non linear or not extendible, then $\chi(1) \geqslant p$ (in particular, $\chi(1) \geqslant \operatorname{acd}(G)$) for every $\chi \in \operatorname{Irr}(G|\theta)$. Assume first that θ is not linear. It follows that $\theta(1) \geqslant p$. By the Clifford Correspondence, we have that $\theta(1)$ divides $\chi(1)$. Since $\theta(1) \geqslant p$, the claim follows in this case. Assume now that θ is linear nut it is not extendible to G. It follows that $\chi(1) \geqslant p$ for any $\chi \in \operatorname{Irr}(G|\theta)$. Thus, the claim also holds in this case.

Next claim that $\operatorname{acd}(G|\lambda) = \operatorname{acd}(G/N)$ for any $\lambda \in \operatorname{Irr}(N)$ such that λ is linear and extendible to G. Suppose that $\lambda \in \operatorname{Irr}(N)$ is linear and it extends to $\mu \in \operatorname{Irr}(G)$. By Gallagher's Theorem, we have that $\operatorname{Irr}(G|\lambda) = \{\mu\rho \mid \rho \in \operatorname{Irr}(G/N)\}$ and hence $\operatorname{acd}(G|\lambda) = \operatorname{acd}(G/N)$. Thus, the claim follows.

From the two previous claims we deduce that $\operatorname{acd}(G/N) \leqslant \operatorname{acd}(G)$. Thus, the result follows. □

Note that Lemma 4.26 provides a partial positive answer to [**91**, Question 5.1], which asks if the inequality $\mathrm{acd}(G/N) \leqslant \mathrm{acd}(G)$ holds for every group G and every normal subgroup N of G.

The following result is [**56**, Theorem 3.2] and it will be the key for proving Theorems F and G.

THEOREM 4.27. *Let G be a group of odd order and suppose that $G = A \rtimes B$, where A is abelian and $B \neq 1$. If r is the number of orbits in the action of G on $\mathrm{Irr}(A)\backslash\{1_A\}$, then there exists t, the size of one of these orbits, such that $\mathrm{acd}(G) \geqslant \frac{t(r+1)}{t+r}$.*

Let us define the function

$$f(t,r) = \frac{t(r+1)}{t+r}$$

for $t, r > 0$. We observe that for $t, r > 0$, $f(t,r)$ is increasing in each of the variables. That is, if $t \geqslant t_0$ (respectively, if $r \geqslant r_0$), then $f(t,r) \geqslant f(t_0,r)$ for every r (resp. $f(t,r) \geqslant f(t,r_0)$ for every t).

We close this subsection by proving a lemma which was observed in the proof of [**56**, Theorem D]. To prove it, we will use the fact that a group of odd order does not admit any non-principal real irreducible character. This fact was proved by W. Burnside and can be found in [**53**, Problem 3.16].

LEMMA 4.28 (Isaacs, Loukaki, Moretó). *Let G be a group of odd order, let $A \leqslant G$ be normal and abelian and let r be the number of orbits in the action of G on $\mathrm{Irr}(A)\backslash\{1_A\}$. Then r is even. Moreover, if $r = 2$, then both orbits have the same size.*

PROOF. We observe that complex conjugation permutes the orbits in the action. We claim that it cannot fix any orbit. Since $|A|$ is odd, none of the characters in $\mathrm{Irr}(A)\backslash\{1_A\}$ are real and hence, no non-principal character of A is fixed by complex conjugation. Thus, the size of an orbit fixed by conjugation must be even, which is impossible. Thus, complex conjugation cannot fix any orbit and hence r is even. If $r = 2$, then the two orbits are conjugate and hence, they have the same size. □

4.5.2. Average character degree. In this subsection we prove Theorems F and G. We recall that the definitions of the functions $h_n(p)$ and $h_s(p)$ can be found in (4.1.5) and (4.1.6), respectively.

PROOF OF THEOREM F. We observe that p is a Sophie Germain prime if and only if $k(p) = p$ and hence, in this case, $h_n(p) = \frac{3p}{p+2}$. Thus, if p is a Sophie Germain prime, then the result follows by Theorem 4.6. As a consequence, we may assume that $p \geqslant 7$.

Let $p \geqslant 7$ be a prime and let G be a group such that G is non-nilpotent, p is the smallest prime dividing $|G|$, $\mathrm{acd}(G) < h_n(p)$ and it has minimal order with these properties. Let A be a minimal normal subgroup of G. Since G is solvable, we have that A is an elementary abelian l-group for a prime l (note that $l \geqslant p$) and since G is non-nilpotent we have that $A < G$. Therefore, $\mathrm{acd}(G) < h_n(p) < 3 < p$, so Lemma 4.26 yields $\mathrm{acd}(G/A) \leqslant \mathrm{acd}(G)$ and by the minimality of G, we conclude that G/A is nilpotent.

If $A \leqslant \mathbf{Z}(G)$, then $G/\mathbf{Z}(G)$ is nilpotent and hence G is nilpotent, which is impossible. Thus, we have $1 < [G, A] \leqslant A$ and $[G, A] \trianglelefteq G$. Since A is a minimal normal subgroup, we deduce that $[G, A] = A$. In addition, if $A \leqslant \Phi(G)$, then, applying part (iii) of Theorem 1.8, we have that G is nilpotent, which is impossible. Thus, there exists a maximal subgroup M of G, such that $A \nleqslant M$, which implies that $G = MA$. We claim that $M \cap A = 1$. Since $A \trianglelefteq G$, we know that $M \cap A \trianglelefteq M$ and since A is abelian we know that $M \cap A \trianglelefteq A$. Thus, $M \cap A \trianglelefteq MA = G$ and since $A \nleqslant M$, the claim follows.

Thus, $G = A \rtimes M$ and hence, using Theorem 4.27, we can deduce that

$$\frac{t(r+1)}{r+t} = f(t, r) \leqslant \mathrm{acd}(G) < h_n(p),$$

where r is the number of orbits in the action of G on $\mathrm{Irr}(A)\backslash\{1_A\}$ and t is the size of one of these orbits. By Lemma 4.28, we have that r is even.

Assume first that $r \geqslant 4$. Then $3 > h_n(p) > \mathrm{acd}(G) \geqslant f(p, 4) \geqslant f(7, 4) = \frac{35}{11} > 3$, which is a contradiction. Thus, we may assume that $r = 2$ and hence, applying Lemma 4.28, we have that both orbits have size t. Therefore, $|A| = 2t+1$, where $|A|$ is the power of a prime at least p, and the smallest prime divisor of t is at least p. If t is an integer satisfying these conditions, then $t \geqslant k(p)$. Thus, we have

$$h_n(p) = \frac{3k(p)}{k(p)+2} \leqslant \frac{3t}{t+2} \leqslant \mathrm{acd}(G) < h_n(p),$$

which is again a contradiction.

Now, it only remains to prove that the bound is sharp. Let

$$G = \mathsf{C}_p \times (\mathsf{H}_{2k(p)+1} \rtimes \mathsf{C}_{k(p)}),$$

where the group $\mathsf{H}_{2k(p)+1} \rtimes \mathsf{C}_{k(p)}$ is defined as in Remark 4.20. Then G is non-nilpotent, p is the smallest prime dividing $|G|$ and we have that

$$\mathrm{acd}(G) = \mathrm{acd}(\mathsf{H}_{2k(p)+1} \rtimes \mathsf{C}_{k(p)}) = \frac{3k(p)}{k(p)+2} = h_n(p).$$

Thus, the bound is best possible. □

Proof of Theorem G. Let $p \geqslant 5$ be a prime and let G be a group such that G is non-supersolvable, p is the smallest prime dividing $|G|$, $\mathrm{acd}(G) < h_s(p)$ and it has minimal order with these properties. Let A be a minimal normal subgroup of

G. As in the proof of Theorem C, we have that A is an elementary abelian l-group for a prime l and that $A < G$. Again, we have that $\mathrm{acd}(G) < h_s(p) < 3 < p$, so Lemma 4.26 yields $\mathrm{acd}(G/A) \leqslant \mathrm{acd}(G)$ and by the minimality of G we deduce that G/A is supersolvable. Since G is non-supersolvable, it follows that A cannot be cyclic and $A \nleqslant \mathbf{Z}(G)$, which implies that $[G, A] = A$. On the other side, if $A \leqslant \Phi(G)$, then $G/\Phi(G)$ is supersolvable and hence, applying part (iv) of Theorem 1.8, we have that G is supersolvable, which is a contradiction. Thus, reasoning as in the proof of Theorem F, we see that G splits over A and hence, applying Theorem 4.27, we have

$$f(t, r) \leqslant \mathrm{acd}(G) < h_s(p),$$

where r is the number of orbits in the action of G on $\mathrm{Irr}(A)\backslash\{1_A\}$ and t is the size of one of these orbits. Reasoning as in the proof of Theorem F, we deduce that $t \geqslant p$, and $r \geqslant 2$ is even.

Assume first that $r \geqslant 4$. If $t \geqslant 7$, then

$$3 < \frac{35}{11} = f(7, 4) \leqslant f(t, r) < h_s(p) < 3,$$

which is a contradiction. Thus, we may assume that $t < 7$, which forces $p = 5$ and $t = 5$.

We claim that the every orbit of G on $\mathrm{Irr}(A)\backslash\{1_A\}$ has size 5. Since $t = 5$ is the size of an orbit, there exists $\lambda \in \mathrm{Irr}(A)$ such that the size of the G-orbit containing λ is 5. Let T be the stabilizer of λ in G. Then $|G : T| = 5$ and since 5 is the smallest prime dividing $|G|$, we deduce that T is normal in G. Therefore, $[A, T] \trianglelefteq G$ and since $[A, T] < A$, it follows that $[A, T] = 1$. As a consequence, T is contained in the stabilizer of all characters in $\mathrm{Irr}(A)$, which implies that the size of any orbit in $\mathrm{Irr}(A)\backslash\{1_A\}$ is at most 5 and the claim follows.

Now, if $r \geqslant 6$, then

$$3 < \frac{35}{11} = f(5, 6) \leqslant f(t, r) < h_s(p) < 3,$$

which is a contradiction. Thus, we have $r = 4$ and hence $|A| = 4 \cdot 5 + 1 = 21$, which is impossible since 21 is not a prime power.

Finally, assume that $r = 2$. By Lemma 4.28, the two orbits have the same size t. Thus, $|A| = 2t + 1$, where $|A|$ is not prime, $|A|$ is a power of a prime at least p, and the smallest prime divisor of t is at least p. If t is an integer satisfying these conditions, then $t \geqslant l(p)$, by definition. Therefore, we have that

$$h_s(p) = \frac{3l(p)}{l(p) + 2} \leqslant \frac{3t}{t + 2} \leqslant \mathrm{acd}(G) < h_s(p),$$

which is a contradiction.

Now, it only remains to prove that the bound is sharp. Let

$$G = \mathsf{C}_p \times (\mathsf{H}_{2l(p)+1} \rtimes \mathsf{C}_{l(p)}),$$

where the group $\mathsf{H}_{2l(p)+1} \rtimes \mathsf{C}_{l(p)}$ is defined as in Remark 4.20. Then G is non-supersolvable, p is the smallest prime dividing $|G|$ and

$$\operatorname{acd}(G) = \operatorname{acd}(\mathsf{H}_{2l(p)+1} \rtimes \mathsf{C}_{l(p)}) = \frac{3l(p)}{l(p)+2} = h_s(p).$$

Thus, the bound cannot be improved. □

4.6. Number-theoretical questions

We begin by proving that numbers $k(p)$ and $l(p)$ defined in the introduction of this chapter do indeed exist.

Before beginning, we the recall the definition of the primordial of a number. Given $n \in \mathbb{N}$ we define the **primordial** of n as the product of all primes at most n and we write $n\#$ to denote it. That is

$$n\# = \prod_{q \leqslant n, q \text{ is prime}} q.$$

It is easy to see that if n is a positive integer and p is a prime, then the smallest prime divisor of n is at least p if and only if $\gcd(n, (p-1)\#) = 1$. Now, we can prove the existence of $l(p)$. We observe that if there exists an integer satisfying the condition of $l(p)$, then this integer satisfies the conditions of $k(p)$ and hence we will prove the existence of both numbers at the same time. The following result is due to Bryce Kerr (private communication), to whom we are thankful.

THEOREM 4.29 (Kerr). *Let p be a prime. Then there exists $l \in \mathbb{N}$ satisfying the following two conditions:*

(i) The smallest prime divisor of l is at least p.

(ii) $2l + 1 = q^f$ where $q \geqslant p$ is a prime and $f \geqslant 2$.

PROOF. Let r be a prime. We observe that

$$(r-1)(4(r-1)^2 + 6(r-1) + 3) \equiv -1 \pmod{r}$$

and that

$$2(r-1) + 1 \equiv -1 \pmod{r}.$$

Since $(p-1)\# = \prod_{r<p, r \text{ is prime}} r$, applying the Chinese Remainder Theorem, we have that there exists $a \in \mathbb{N}$ such that $n \equiv -1 \pmod{r}$ for every prime $r < p$ if and only if $n \equiv a \pmod{(p-1)\#}$.

Now, we claim that there exists n such that $n \equiv a \pmod{(p-1)\#}$ and $2n+1 = q$, where q is a prime larger than p. This is equivalent to showing that there exist a prime $q > p$ of the form

$$q = (2k) \cdot (p-1)\# + (2a+1)$$

for some $k \in \mathbb{N}$. Now, we have that $2a+1 \equiv 2(r-1)+1 \equiv -1 \pmod{r}$ for every $r < p$, prime. Therefore, $\gcd(2(p-1)\#, 2a+1) = 1$ and hence the prime q exists by Dirichlet's Theorem.

Now, let n be as in the previous claim and let $l = n(4n^2+6n+3)$. By the choice of n, we have that

$$q^3 = (2n+1)^3 = 2n(4n^2+6n+3)+1 = 2l+1.$$

Thus, l satisfies condition (ii) of the statement. Now, since $n \equiv a \pmod{(p-1)\#}$, we have

$$l \equiv n(4n^2+6n+3) \equiv (r-1)(4(r-1)^2+6(r-1)+3) \equiv -1 \pmod{r}$$

for every prime $r < p$.

This implies that $\gcd(l, (p-1)\#) = 1$ and hence the smallest prime divisor of l is at least p. Thus, l satisfies condition (i) of the statement and the result follows. □

Now, we discuss $t(p)$ and $r(p)$. First, we introduce some notation. Given $a, d \in \mathbb{N}$ with $0 < a < d$ and $\gcd(a,d) = 1$ we define $P(a,d)$ to be the smallest prime in the arithmetic progression $\{a+nd\}_{n\in\mathbb{N}}$ (such a prime exists by Dirichlet's Theorem). Computations in GAP [**33**] show that if $p \leqslant 1000$, then $t(p) = P(1,p)$ and $r(p) = P(p-1,p)^2$. We conjecture that the same holds for all primes.

Conjecture 4.30. *Let p be a prime. Then $t(p) = P(1,p)$ and $r(p) = P(p-1,p)^2$.*

Conjecture 4.30 depends on strong properties of the distribution of prime numbers. According to B. Kerr and T. Trudgian (private communication), it seems that Conjecture 4.30 should be true, but it may be out of reach with current techniques in number theory. Linnik [**68**] proved that there exist two positive constants c, L such that $P(a,d) \leqslant c \cdot d^L$ for every pair of integers $a < d$ with $\gcd(a,d) = 1$. Many efforts have been made to give explicit constants c and L. The best bound known for L is due to Xylouris [**129**] and it is $L = 5$. However, it is conjectured that $P(a,d) \leqslant d^2$ (see [**46**]). It is not hard to see that if this conjecture holds, then part a) of Conjecture 4.30 also holds. It is worth noting that the bound $P(a,d) \leqslant d^2$ is not known even assuming the Riemann Generalized Hypothesis. We close this chapter with a few more comments about Conjecture 4.30.

Remark 4.31. Fix a prime p. If we assume that $P(1,p), P(p-1,p) \leqslant p^k$ and p is a Zsigmondy prime for $\langle q, r\rangle$ for some $q > p$ and some $r \geqslant k$, then $q^r \geqslant p^k \geqslant t(p)$ and if $r \geqslant 2k$, then $q^r \geqslant r(p)$. We deduce the following:

a) From Xylouris's bound [**129**], we have that $P(1,p), P(p-1,p) \leqslant p^5$. If $\langle q, r\rangle$ is a counterexample for the first part of Conjecture 4.30, then $r \in \{2,3,4\}$, and if it is a counterexample for the second part, then $r \in \{3,4,5,6,7,8,9\}$.

b) Assuming the Generalized Riemann Hypothesis, we can use a result of Lazmouri, Li and Soundararajan [**63**], to deduce that $P(1,p), P(p-1,p) \leqslant (p-1)^2(\log(p))^2 < p^3$. Thus, if $\langle q, r\rangle$ is a counterexample for the first part of Conjecture 4.30, then $r = 2$, and if it is a counterexample for the second part, then $r \in \{3,4,5\}$. Note that the bound of [**63**] is not enough to prove part a) of Conjecture 4.30. For $p = 7$ we have that $r(7) = 169 \in \mathrm{T}(7,1)$, but $169 < (7-1)^2(\log(7))^2 \approx 283.72$.

CHAPTER 5

Proportion of classes of π-elements

5.1. Introduction

Let π be a set of primes and let $k_\pi(G)$ be the number of conjugacy classes of π-elements in a group G. Inspired by the identity

$$\Pr(G) = \frac{k(G)}{|G|} = \frac{|\operatorname{Irr}(G)|}{|G|},$$

we define the following invariant, which was introduced in [**76**].

Definition. Let π be a set of primes and let G be a group. We define the invariant $\mathrm{d}_\pi(G)$ as

$$\mathrm{d}_\pi(G) := \frac{k_\pi(G)}{|G|_\pi}.$$

This invariant is always at most 1 by a classical result of Robinson (see Lemma 5.10 below). We wonder whether there exists a simpler proof for this fact. This invariant appears naturally in many contexts. For instance, Sangroniz [**111**] proved that if G is p-solvable, then all irreducible p-Brauer characters of G restrict irreducibly to a subgroup H if and only if $\mathrm{d}_{p'}(H) = \mathrm{d}_{p'}(G)$.

We recall that Gustafson [**42**] proved that G is abelian if and only if $\Pr(G) > 5/8$ (see also Proposition 4.9). Hung and Maróti [**76**, Theorem 1] proved a version of Gustafson's Theorem for d_π.

Theorem 5.1 (Hung and Maróti). *Let G be a group and let π be a set of primes. If $\mathrm{d}_\pi(G) > 5/8$, then G possesses an abelian Hall π-subgroup.*

We notice that $\mathrm{d}_2(\mathsf{D}_8) = \Pr(\mathsf{D}_8) = 5/8$ and D_8 does not possess an abelian Sylow 2-subgroup. Thus, the bound $\mathrm{d}_\pi(G) > 5/8$ is best possible.

For certain sets π, Tong-Viet [**123**] proved some results on the existence of normal π-complements in groups G under the condition that $\mathrm{d}_\pi(G)$ is large. For example, we have the following result corresponds to [**123**, Theorems C and E].

Theorem 5.2 (Tong-Viet). *Let π be a set of primes and let p be the smallest prime in π. Let G be a group.*

(i) If $p > 2$ and $\mathrm{d}_\pi(G) > \frac{p+1}{2p}$, then G has a normal π-complement and an abelian Hall π-subgroup.

(ii) If $p = 2$ and $\mathrm{d}_\pi(G) > \frac{1}{2}$, then G has a normal π-complement and an abelian Hall σ-subgroup, where $\sigma = \pi \backslash \{2\}$.

We notice the the bounds in Theorem 5.2 are best possible. Given $p > 2$ prime, we notice that $\mathrm{d}_p(\mathsf{D}_{2p}) = (p+1)/2p$ but D_{2p} does not possess a normal p-complement. Moreover, if $p = 2$, then $\mathrm{d}_2(\mathsf{A}_4) = 1/2$ but A_4 does not possess a normal 2-complement.

In a similar way, Schroeder [**115**, Theorem 1.3] provided a condition for the existence of normal Sylow p-subgroups in terms of $\mathrm{d}_{p'}(G)$.

THEOREM 5.3 (Schroeder). *Let G be a group and let p be a prime. If $\mathrm{d}_{p'}(G) > \frac{2}{p+1}$, then G has a normal Sylow p-subgroup.*

The bound in Theorem 5.3 is best possible. Suppose p is a Mersenne prime $p = 2^n - 1$ and let $G = \mathsf{H}_{2^n} \rtimes \mathsf{C}_p$, where the action is defined as in Remark 4.20. Then $\mathrm{d}_{p'}(G) = 2/(p+1)$ and G does not have a normal Sylow p-subgroup. The bound is also sharp for $p = 2$. If $G = \mathsf{S}_3$, then $\mathrm{d}_{2'}(G) = 2/3$ and G does not have a normal Sylow 2-subgroup.

In [**115**], Schroeder also provides conditions for the solvability and the p-solvability of a group in terms of $\mathrm{d}_{2'}(G)$ and $\mathrm{d}_{p'}(G)$. The following result corresponds with [**115**, Theorems 1.1 and 1.2].

THEOREM 5.4 (Schroeder). *Let p be a prime and let G be a group.*

(i) If $p > 2$ and $\mathrm{d}_{p'}(G) > \frac{1}{p-1}$, then G is p-solvable

(ii) If $p = 2$ and $\mathrm{d}_{2'}(G) > \frac{4}{15}$, then G is solvable

The bound in Theorem 5.4 is best possible for any prime $p > 3$. Given a prime $p > 3$, the group $\mathrm{PSL}(2,p)$ is a non-abelian simple group with $\mathrm{d}_{p'}(\mathrm{PSL}(2,p))\frac{1}{p-1}$ (see [**115**, Theorem 1.1(ii)]). The bound in Theorem 5.4(ii) is also best possible since $\mathrm{d}_{2'}(\mathsf{A}_5) = 4/15$.

The main goal of this chapter is to extend Theorem 5.1 by giving a bound involving the smallest prime in π.

THEOREM H. *Let G be a group and let π be a set of primes and let p be the smallest prime in π.*

(i) If $\mathrm{d}_\pi(G) > \frac{1}{p}$, then G has a nilpotent Hall π-subgroup, whose derived subgroup has size at most p.

(ii) If $\mathrm{d}_\pi(G) > \frac{p^2+p-1}{p^3}$, *then* G *has an abelian Hall* π*-subgroup.*

In Section 5.4 we will present Examples 5.35 to 5.38, which show that the converse assertions are false. For both of them, we will present counterexamples for both $2 \in \pi$ and $2 \notin \pi$. Moreover, the bound $1/p$ in Theorem H is not best possible for nilpotency. We will discuss this further in Section 5.4.

5.2. Reducing to simple groups

5.2.1. Hall π-subgroups. In this subsection we prove that part (ii) of Theorem H follows from part (i) of Theorem H. The following easy observation is useful to bound $\mathrm{d}_\pi(G)$ in the case $G \in \mathcal{D}_\pi$ (see 1.2 for a definition).

LEMMA 5.5. *Let* G *be a group in* $\mathcal{D}_\pi$. *If* H *is a Hall* π*-subgroup of* G, *then*

$$\mathrm{d}_\pi(G) \leqslant \Pr(H).$$

PROOF. Since $|H| = |G|_\pi$, it suffices to see that $k_\pi(G) \leqslant k(H)$. If $x, y \in H$ are not conjugate in G, then they cannot be conjugate in H. Since $G \in \mathcal{D}_\pi$, every G-class of π-elements has a representative in H. □

It is worth to mention that a π-subgroup $T \leqslant G$ is said to be a π-**witness** if $k_\pi(G) \leqslant k(T)$. From Lemma 5.5, we can easily prove Theorem H in case $G \in \mathcal{D}_\pi$.

THEOREM 5.6. *Let* π *be a set of primes and let* G *a group in* $\mathcal{D}_\pi$. *Then Theorem H holds for* G.

PROOF. By hypothesis, G has a Hall π-subgroup H and all the Hall π-subgroups of G are G-conjugate. Thus, by Lemma 5.5, we have $\mathrm{d}_\pi(G) \leqslant \Pr(H)$. Let p be the smallest prime in π and assume that $\mathrm{d}_\pi(G) > \frac{1}{p}$, so

$$\Pr(H) > \frac{1}{p}.$$

Theorem 4.14 and Lemma 4.13 then imply that $|H'| \leqslant p$ and H is nilpotent, as claimed. Moreover, if $\mathrm{d}_\pi(G) > \frac{p^2+p-1}{p^3}$ then H is abelian by Lemma 4.9. □

As a consequence of Theorem 5.6, we see that Theorem H holds trivially if $\pi = \{p\}$ or if G is π-separable.

Next, we recall some facts about the groups in $\mathcal{D}_\pi$. The first one is the result of Wielandt [**128**] mentioned in the Introduction (see Theorem 1.7) and the second one is due to Hall (see [**43**, Theorem D5]).

LEMMA 5.7. *Let* G *be a group and let* π *a set of primes.*

(i) *If* G *possesses a nilpotent Hall* π*-subgroup, then* $G \in \mathcal{D}_\pi$.

(ii) *If N possesses nilpotent Hall π-subgroups, G/N possesses solvable Hall π-subgroups, and $G/N \in \mathcal{D}_\pi$, then $G \in \mathcal{D}_\pi$.*

THEOREM 5.8. *If part (i) of Theorem H holds, then part (ii) of Theorem H holds.*

PROOF. Assume that part (i) of Theorem H holds. Let G be a group with $\mathrm{d}_\pi(G) > \frac{p^2+p-1}{p^3} > \frac{1}{p}$. By hypothesis, G possesses a nilpotent Hall π-subgroup. It then follows that $G \in \mathcal{D}_\pi$ by Lemma 5.7(i). The result follows by Theorem 5.6. □

The rest of the section is therefore devoted to proving that G has a nilpotent Hall π-subgroup under the condition $\mathrm{d}_\pi(G) > \frac{1}{p}$.

5.2.2. A reduction to simple groups. In this subsection we prove Theorem H, assuming a result on finite simple groups. We begin by recalling two properties of $\mathrm{d}_\pi(G)$.

LEMMA 5.9. *Let G be a group and let π a set of primes.*

(i) If $\mu \subseteq \pi$, then $\mathrm{d}_\pi(G) \leqslant \mathrm{d}_\mu(G)$.

(ii) $\mathrm{d}_\pi(G) \leqslant \mathrm{d}_\pi(N)\,\mathrm{d}_\pi(G/N)$ for any normal subgroup N of G.

PROOF. Part (i) is proved in [**76**, Proposition 5], and it is essentially due to Robinson. Part (ii) follows from [**31**, Lemma 2.3]. □

Before continuing, we prove that $\mathrm{d}_\pi(G) \leqslant 1$ for every group G and every set of primes π. In fact, we prove a slightly stronger result.

LEMMA 5.10. *Let G be a group and let π be a set of primes. If $q \in \pi$, then $\mathrm{d}_\pi(G) \leqslant \mathrm{Pr}(Q)$ for every $Q \in \mathrm{Syl}_q(G)$. In particular, $\mathrm{d}_\pi(G) \leqslant 1$.*

PROOF. Let $q \in \pi$ and let $Q \in \mathrm{Syl}_q(G)$. By Sylow Theorems, we deduce that $G \in \mathcal{D}_q$. By combining Lemmas 5.5 and 5.9, we have

$$\mathrm{d}_\pi(G) \leqslant \mathrm{d}_p(G) \leqslant \mathrm{Pr}(Q) \leqslant 1$$

and the result follows. □

LEMMA 5.11. *Let G be a group, let π a set of primes, and let p the smallest prime in π. Let $q \in \pi$ and $Q \in \mathrm{Syl}_q(G)$. Suppose $\mathrm{d}_\pi(G) > \frac{1}{p}$. Then the following hold:*

(i) $Q/\mathbf{Z}(Q)$ is abelian and $|Q'| \leqslant q$.

(ii) If $q \neq p$, then Q is abelian.

PROOF. By Sylow's theorems and Lemma 5.5 we have $\mathrm{d}_q(G) \leqslant \Pr(Q)$. On the other hand, by Lemma 5.9(i), we have $\mathrm{d}_\pi(G) \leqslant \mathrm{d}_q(G)$. We deduce that

$$\frac{1}{q} \leqslant \frac{1}{p} < \Pr(Q).$$

Theorem 4.14 and Lemma 4.13 now imply that $Q/\mathbf{Z}(Q)$ is abelian and $|Q'| \leqslant q$.

Suppose $q > p$. Then $q \geqslant p+1$, and one can easily check that $\frac{q^2+q-1}{q^3} < \frac{1}{p}$. Now $\Pr(Q) > \frac{q^2+q-1}{q^3}$, and thus Q must be abelian by Lemma 4.9. □

The next lemma allows us to assume that $|\pi| = 2$.

LEMMA 5.12 (Lemma 3.1 of [**87**]). *Let G be a group and let π be a set of primes. If G possesses a nilpotent Hall τ-subgroup for every $\tau \subseteq \pi$ with $|\tau| = 2$, then G possesses a nilpotent Hall π-subgroup.*

PROPOSITION 5.13. *Suppose that part (i) of Theorem H is false for a group G. Then there exists $\pi = \{p, q\}$, where $p < q$ are two primes, such that G does not possess nilpotent Hall π-subgroups, $|P'| \leqslant p$ (in particular, $P/\mathbf{Z}(P)$ is abelian) for every $P \in \mathrm{Syl}_p(G)$ and Q is abelian for every $Q \in \mathrm{Syl}_q(G)$.*

PROOF. By Theorem 5.8, we may assume that there exists π, a set of primes, such that $\mathrm{d}_\pi(G) > \frac{1}{p}$, but G does not possess nilpotent Hall π-subgroups, where p is the smallest member of π.

If G has a nilpotent Hall τ-subgroup for every $\tau \subseteq \pi$ with $|\tau| = 2$, then by Lemma 5.12, G has nilpotent Hall π-subgroups. Thus, there exists $\{q, r\} \subseteq \pi$ with $r < q$ such that G does not possess a nilpotent Hall $\{q, r\}$-subgroup. By Lemma 5.9(i), we also have $\mathrm{d}_\pi(G) \leqslant \mathrm{d}_{\{q,r\}}(G)$, and it follows that

$$\frac{1}{r} \leqslant \frac{1}{p} < \mathrm{d}_\pi(G) \leqslant \mathrm{d}_{\{q,r\}}(G).$$

Therefore, Theorem H fails for G and the set $\{q, r\}$, and hence we may assume that $|\pi| = 2$.

Finally, the assertion on the Sylow subgroups follows from Lemma 5.11. □

PROPOSITION 5.14. *Let π be a set of primes and let p the smallest prime in π. Let G be a group with minimal order subject to the conditions that $\mathrm{d}_\pi(G) > \frac{1}{p}$ and G does not possess nilpotent Hall π-subgroups. Then G is non-abelian simple.*

PROOF. Seeking for a contradiction, let us assume that G is not simple. Let N be a non-trivial proper normal subgroup in G. By Lemma 5.9(ii), we have

$$\frac{1}{p} < \mathrm{d}_\pi(G) \leqslant \mathrm{d}_\pi(G/N)\,\mathrm{d}_\pi(N).$$

By Lemma 5.10, we have that both $\mathrm{d}_\pi(N)$ and $\mathrm{d}_\pi(G/N)$ are at most one and hence $\frac{1}{p} < \mathrm{d}_\pi(G/N)$ and $\frac{1}{p} < \mathrm{d}_\pi(N)$. By the minimality of G, it follows that N and G/N possess nilpotent Hall π-subgroups. Applying Lemma 5.7(i), we then deduce that both N and G/N are members of $\mathcal{D}_\pi$, so $G/N \in \mathcal{D}_\pi$, G/N possesses solvable Hall π-subgroups and N possesses nilpotent Hall π-subgroups. By Lemma 5.7(ii), we have $G \in \mathcal{D}_\pi$. Therefore, Theorem 5.6 implies that G possesses nilpotent Hall π-subgroups, which is a contradiction. We conclude that G is non-abelian simple. □

The following is a consequence of a result of Tong-Viet [**123**], which asserts that if $\mathrm{d}_2(G) > \frac{1}{2}$ then G possesses a normal 2-complement.

LEMMA 5.15. *Let S be a non-abelian simple group and let π be a set of primes containing 2. Then $\mathrm{d}_\pi(S) \leqslant \frac{1}{2}$.*

PROOF. Suppose that $\mathrm{d}_\pi(S) > \frac{1}{2}$. Then $\frac{1}{2} < \mathrm{d}_\pi(S) \leqslant \mathrm{d}_2(S)$. By [**123**, Theorem A], S possesses a normal 2-complement, which is impossible. □

PROPOSITION 5.16. *Let G be a group and let π a set of primes such that $\mathrm{d}_\pi(G) > \frac{1}{p}$, where p is the smallest prime in π. Let $q \in \pi \backslash \{p\}$. Then q does not divide $|\mathbf{N}_G(P) : \mathbf{C}_G(P)|$, where $P \in \mathrm{Syl}_p(G)$.*

PROOF. Assume for contradiction that q divides $|\mathbf{N}_G(P)/\mathbf{C}_G(P)|$, where $P \in \mathrm{Syl}_p(G)$. Let x be an element of order q in $\mathbf{N}_G(P)/\mathbf{C}_G(P)$ and consider the action of $X = \langle x \rangle$ on P. Let r be the number of elements of P fixed by X.

We claim that $r > \frac{|P|}{p^2}$. Assume to the contrary that $r \leqslant \frac{|P|}{p^2}$. We have $|P| = r + t \cdot q$, implying that $t = \frac{|P|-r}{q}$. Since each X-orbit on P is contained in a conjugacy class of p-elements it is easy to see that $k_p(G) \leqslant r + t$. Now we have

$$\frac{1}{p} < \mathrm{d}_\pi(G) \leqslant \mathrm{d}_p(G) \leqslant \frac{r+t}{|P|} = \frac{1}{q}\left((q-1)\frac{r}{|P|} + 1\right) \leqslant \frac{1}{q}\left((q-1)\frac{1}{p^2} + 1\right).$$

It is not hard to see that this implies $q \leqslant p$, which is a contradiction. We have shown that $r > \frac{|P|}{p^2}$.

Since r divides $|P|$, it follows that

$$r \in \{|P|, |P|/p\}.$$

If $r = |P|$ then X centralises P, which is impossible. Thus $r = |P|/p$ and hence there exists a subgroup H of order $|P|/p$ that is centralised by X. That is,

$$H = \mathbf{C}_P(X) = \{z \in P \mid z^x = z \text{ for all } x \in X\}.$$

Let $L := P \rtimes X$ be the semidirect product of the relevant action of X on P. Then $L/H \cong C \rtimes X$ for some $C \cong \mathsf{C}_p$. Since H is maximal in P, the subgroup

H is normal in P, and it is X-invariant. Thus, applying [**54**, Corollary 3.28], we have

$$\mathbf{C}_{P/H}(X) = \mathbf{C}_P(X)H/H = H/H,$$

and hence X acts non-trivially on P/H, or equivalently, on C. Let $\mathcal{O}$ be a non-trivial orbit of the action of X on C. We now have $q = |X| = |\mathcal{O}| \leqslant |C| = p$, which is a contradiction. □

COROLLARY 5.17. *Let G be a group and let $\pi = \{p, q\}$ be a set of primes with $p < q$ such that $\mathrm{d}_\pi(G) > \frac{1}{p}$. Let $P \in \mathrm{Syl}_p(G)$. Then either q divides $|\mathrm{Syl}_p(G)| = |G : \mathbf{N}_G(P)|$, or G possesses a nilpotent Hall π-subgroup.*

PROOF. We know that $|G|_q$ divides

$$|G| = |G : \mathbf{N}_G(P)||\mathbf{N}_G(P) : \mathbf{C}_G(P)||\mathbf{C}_G(P)|$$

but q cannot divide $|\mathbf{N}_G(P) : \mathbf{C}_G(P)|$ by Proposition 5.16. Assume that q does not divide $|G : \mathbf{N}_G(P)|$. Then $|G|_q$ divides $|\mathbf{C}_G(P)|$. Therefore, there exists $Q \in \mathrm{Syl}_q(G)$ with $Q \leqslant \mathbf{C}_G(P)$. Now PQ is a nilpotent Hall π-subgroup of G. □

Now we can prove Theorem H, modulo the following statement about simple groups whose proof is deferred to the next section.

THEOREM 5.18. *Let G be a non-abelian simple group and let $\pi = \{p, q\}$ be a set of two odd primes with $p < q$. Assume that there exist $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$ such that $P/\mathbf{Z}(P)$ is abelian, $|P'| \leqslant p$, Q is abelian, and q divides $|G : \mathbf{N}_G(P)|$. Then $\mathrm{d}_\pi(G) \leqslant \frac{1}{p}$.*

THEOREM 5.19. *Let G be a group, let π be a set of primes, and let p be the smallest prime in π. Assume Theorem 5.18. If $\mathrm{d}_\pi(G) > \frac{1}{p}$ then G has a nilpotent Hall π-subgroup.*

PROOF. Assume that the theorem is false and let G be a minimal counterexample. In particular, $\mathrm{d}_\pi(G) > \frac{1}{p}$ but G has no nilpotent Hall π-subgroups. By Proposition 5.14, we know that G is non-abelian simple. Using Lemma 5.15, we know furthermore that $p \neq 2$.

By Proposition 5.13, there exists $\pi = \{p, q\}$ with (odd) $p < q$ such that $\mathrm{d}_\pi(G) > \frac{1}{p}$, $P/\mathbf{Z}(P)$ is abelian, $|P'| \leqslant p$, and Q is abelian, where $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$. We also have that q divides $|G : \mathbf{N}_G(P)|$, by Corollary 5.17. We now have all the hypotheses of Theorem 5.18, and therefore deduce that $\mathrm{d}_\pi(G) \leqslant \frac{1}{p}$. This is a contradiction. □

We remark that we have indeed proved Theorem H when the set π contains the prime 2, and this result does not rely on *CFSG* (we recall that [**123**, Theorem A] does not depend on the *CFSG*).

5.3. Simple groups

In this section we prove Theorem 5.18, by using *CFSG*. We begin with the alternating groups.

LEMMA 5.20. *Let p be an odd prime, let $n \geqslant 5$ be an integer and let $P \in \mathrm{Syl}_p(\mathsf{A}_n)$.*

(i) If $n \geqslant p^2$, then $P/\mathbf{Z}(P)$ is not abelian.

(ii) If $n < p^2$, then P is elementary abelian.

PROOF. For (i) it is sufficient to exhibit a subgroup H of P such that $H/\mathbf{Z}(H)$ is not abelian. If $n \geqslant p^2$, then $H = \mathsf{C}_p \wr \mathsf{C}_p$ is such a subgroup of P. Statement (ii) follows from the description of the Sylow p-subgroups of A_n found in [**52**, Satz III.15.3]. □

THEOREM 5.21. *Let $n \geqslant 5$, let $\pi = \{p, q\}$ be a set of two odd primes with $p < q$, and let $P \in \mathrm{Syl}_p(\mathsf{A}_n)$. Assume that both p and q divide the order of A_n (equivalently, $q \leqslant n$). If $P/\mathbf{Z}(P)$ is abelian, then $\mathrm{d}_\pi(\mathsf{A}_n) \leqslant \frac{1}{p}$. In particular, Theorem 5.18 holds for alternating groups.*

PROOF. Let $P \in \mathrm{Syl}_p(\mathsf{A}_n)$ and $Q \in \mathrm{Syl}_q(\mathsf{A}_n)$. Since $P/\mathbf{Z}(P)$ is abelian, $n < p^2$ by Lemma 5.20. Let $n = rp + s = lq + t$, where $r, s \in \{0, 1, \ldots, p-1\}$ and $l, t \in \{0, 1, \ldots, q-1\}$. Then $P = (\mathsf{C}_p)^r$ and $Q = (\mathsf{C}_q)^l$ with both $r, l \geqslant 1$.

It is easy to see that every π-element of A_n can be expressed as a product of the form $xy = yx$, where x is a product of (disjoint) cycles of length p and y is a product of cycles of length q. Since $n < p^2$, the supports of x and y are disjoint.

Assume first that $n \geqslant p + q + 2$. In this case we have that $k_p(\mathsf{A}_n) = 1 + r \leqslant p$, $k_q(\mathsf{A}_n) = 1 + l \leqslant q$ and $|\mathsf{A}_n|_\pi = p^r q^l$. Thus we have

$$\mathrm{d}_\pi(\mathsf{A}_n) = \frac{k_\pi(\mathsf{A}_n)}{|\mathsf{A}_n|_\pi} \leqslant \frac{pq}{p^r q^l}.$$

If $(r, l) \neq (1, 1)$, then $\mathrm{d}_\pi(\mathsf{A}_n) \leqslant \frac{1}{p}$. Assume now that $r = l = 1$. Then $k_\pi(\mathsf{A}_n) \leqslant k_p(\mathsf{A}_n) k_q(\mathsf{A}_n) = 4$ and hence $\mathrm{d}_\pi(\mathsf{A}_n) \leqslant \frac{4}{q} \cdot \frac{1}{p} < \frac{1}{p}$, where the last inequality holds because $q \geqslant 5$.

Assume now that $n \leqslant p + q + 1$ and so $l = 1$. In this case it may happen that an S_n-conjugacy class of π-elements splits into two different A_n-conjugacy classes. We thus have $k_\pi(\mathsf{A}_n) \leqslant (1 + r)(1 + l) + 1 = 2(1 + r) + 1 = 2r + 3$. It follows that $\mathrm{d}_\pi(\mathsf{A}_n) \leqslant \frac{2r+1}{p^r q}$. If $r \geqslant 2$, then $\frac{2r+3}{p^r q} < \frac{1}{q} < \frac{1}{p}$. If $r = 1$, then $2r + 3 = 5 \leqslant q$ and so once again $\mathrm{d}_\pi(\mathsf{A}_n) \leqslant \frac{1}{p}$. □

For convenience, we will consider the Tits group ${}^2\mathrm{F}_4(2)'$ as a sporadic simple group.

THEOREM 5.22. *Let S be a sporadic simple group and let $\pi = \{p, q\}$, where $p < q$ are odd primes dividing $|S|$. If $(S, \pi) \neq (J_1, \{3, 5\})$ then $\mathrm{d}_\pi(S) \leqslant \frac{1}{p}$. In particular, Theorem 5.18 holds for S.*

PROOF. In what follows we use information in the *ATLAS* [**24**] without further notice. We may assume that π is a set of primes such that $k_\pi(S) \geqslant 6$, for otherwise

$$\mathrm{d}_\pi(S) = \frac{k_\pi(S)}{|S|_\pi} \leqslant \frac{5}{pq} \leqslant \frac{1}{p}.$$

There is no such π for the four smallest Mathieu groups. For each of the groups $\mathrm{M}_{24}, \mathrm{HS}, \mathrm{J}_2$ there are two possibilities for π, and for each pair (S, π) one checks that $k_\pi(S)$ is at most $|S|_p$ or $|S|_q$, which implies that $\mathrm{d}_\pi(S) \leqslant \frac{1}{p}$.

So we assume that S is not one of the groups already analyzed. If S is different from $\mathrm{Fi}_{23}, \mathrm{Fi}'_{24}$ and J_1, then we count the total number of conjugacy classes of S of elements of odd order. These numbers are usually less than $|S|_r$ for a given prime divisor r of $|S|$. If this is the case for a prime r, then we can assume that r does not lie in π (otherwise we would be done). This gives strong restrictions on the set π. In fact, given that $k_\pi(S) \geqslant 6$, we reduce to the case S must be J_4 and π is either $\{3, 7\}$ or $\{5, 7\}$. In each of these two cases we count the number of π-classes in S in order to obtain the bound $\frac{1}{p}$ for $\mathrm{d}_\pi(S)$.

If S is Fi_{23} or Fi'_{24}, then we again count the number of conjugacy classes in S of elements of odd order. This allows us to conclude that 3 cannot lie in π. We then count the number of conjugacy classes in S whose elements have orders divisible neither by 2 nor 3. This number is 8 in the first case and 14 in the second. By looking at the prime factorization of $|S|$, the only case to consider is $S = \mathrm{Fi}'_{24}$ and $\pi = \{11, 13\}$. But it turns out that $k_\pi(S) = 3$ in this case.

The only group remaining is $S = \mathrm{J}_1$. The number of conjugacy classes in S of elements of odd order is 11, forcing π to be a subset of $\{3, 5, 7\}$. Then $k_\pi(S) = 3$, or $\pi = \{3, 5\}$ and $k_\pi(S) = 6$, giving $\mathrm{d}_\pi(S) = \frac{2}{5}$.

The last assertion follows from the fact that if $P \in \mathrm{Syl}_3(\mathrm{J}_1)$, then 5 does not divide $|\mathrm{J}_1 : \mathbf{N}_{\mathrm{J}_1}(P)|$. □

Let S be a simple group of Lie type. The proof of Theorem 5.18 for groups of Lie type is divided into two fundamentally different cases: π contains the defining characteristic of S and π does not. For the sake of convenience, we rename the prime q in Theorem 5.18 to s in order to reserve q for the size of the underlying field of S. It is important to remark that, in our next result, p will not necessarily be the smallest prime in π.

THEOREM 5.23. *Let S be a finite simple group of Lie type in characteristic $p > 2$ and let $\pi = \{p, s\}$, where s is an odd prime divisor of $|S|$ and $s \neq p$. Then,*

$$\mathrm{d}_\pi(S) \leqslant \frac{1}{s}.$$

In particular, Theorem 5.18 holds for simple groups of Lie type when π contains the defining characteristic of S.

PROOF. Let S be a finite simple group of Lie type over a field of q elements, where $q = p^l$ for some prime $p > 2$ and $l \geqslant 1$. Let $\pi = \{p, s\}$ be a set of primes. Then

$$\mathrm{d}_\pi(S) = \frac{k_\pi(S)}{|S|_p}\frac{1}{|S|_s} \leqslant \frac{k(S)}{|S|_p}\frac{1}{s}$$

If we prove that $k_\pi(S) \leqslant |S|_p$, then we will have that

$$\mathrm{d}_\pi(S) \leqslant \frac{k(S)}{|S|_p}\frac{1}{s} \leqslant \frac{1}{s} \leqslant \max_{t\in\{p,s\}}\{\frac{1}{t}\}$$

Thus, our goal will be to obtain the inequality $k_\pi(S) \leqslant |S|_p$. We will distinguish the case of the classical groups and the case of the exceptional groups.

The classical groups: Let S be a classical simple group of Lie type, then by the results of Section 3 of [**31**], there exists a bound of the form $k(S) \leqslant b \cdot q^a$ for a positive constant b and a positive integer a (see [**31**, Tables 2 and 3] for explicit bounds). On the other hand, $|S|_p = q^h$ for an integer h. Therefore, if the inequality $b \cdot q^a \leqslant q^h$ holds, then the result follows. Thus, we analyze each inequality case by case.

(i) Case $\mathrm{PSL}(n, q)$ with $n \geqslant 2$: We know that $|S|_p = q^{\frac{n(n-1)}{2}}$. On the other hand, $k(S) \leqslant 2.5 \cdot q^{n-1}$. We have to study whether

$$\frac{k(\mathrm{PSL}(n,q)}{|\mathrm{PSL}(n,q)|_p} \leqslant \frac{2.5 \cdot q^{n-1}}{q^{\frac{n(n-1)}{2}}} \leqslant 1.$$

The inequality holds for $n \geqslant 3$. Thus, we only have to consider the case $\mathrm{PSL}(2, q)$.

In the case $\mathrm{PSL}(2, q)$, since q is odd, we know that $k(\mathrm{PSL}(2, q)) = \frac{q+5}{2}$, (see Chapter 38 of [**26**]) and $|\mathrm{PSL}(2, q)|_p = q$. Then

$$\frac{k(\mathrm{PSL}(2,q))}{|\mathrm{PSL}(2,q)|_p} = \frac{q+5}{2q} \leqslant 1$$

where the inequality holds because $q \geqslant 5$. Therefore, the result follows in this case.

(ii) Case $\mathrm{PSp}(2n,q)$ with $n \geqslant 2$: We know that $k(\mathrm{PSp}(2n,q)) \leqslant 10.8 \cdot q^n$ and $|\mathrm{PSp}(2n,q)|_p = q^{n^2}$. We analyze whether

$$\frac{k(\mathrm{PSp}(2n,q))}{|\mathrm{PSp}(2n,q)|_p} \leqslant \frac{10.8 \cdot q^n}{q^{n^2}} \leqslant 1.$$

We observe that if either $n \geqslant 3$ of $n = 2$ and $q \geqslant 5$, then the inequality holds. Thus, the only possible counterexample is $\mathrm{PSp}(4,3)$. In this case, using the information in the *ATLAS* [24], we deduce that $k(\mathrm{PSp}(4,3)) = 20 \leqslant 3^4 = |\mathrm{PSp}(4,3)|_3$.

(iii) Case $\mathrm{PSU}(n,q)$ with $n \geqslant 3$: In this case, $k(\mathrm{PSU}(n,q)) \leqslant 8.6 \cdot q^{n-1}$ and $|\mathrm{PSU}(n,q)|_p = q^{\frac{n(n-1)}{2}}$. We analyze whether

$$\frac{k(\mathrm{PSU}(n,q))}{|\mathrm{PSU}(n,q)|_p} \leqslant \frac{8.6 \cdot q^{n-1}}{q^{\frac{n(n-1)}{2}}} \leqslant 1.$$

We observe that if either $n \geqslant 4$ or $n = 3$ and $q \geqslant 9$, then the inequality holds. For the remaining cases, using the information in the *ATLAS* [24], we have that $k(\mathrm{PSU}(3,3)) = k(\mathrm{PSU}(3,5)) = 14$ and $k(\mathrm{PSU}(3,7)) = 58$. Thus, in every case, we have that $k(\mathrm{PSU}(3,q)) \leqslant p^3 = |\mathrm{PSU}(3,q)|_p$ and the result holds.

(iv) Case $\Omega(2n+1,q)$ with $n \geqslant 3$: We know that $k(\Omega(2n+1,q)) \leqslant 7.3 \cdot q^n$ and $|\Omega(2n+1q)|_p = q^{n^2}$. We analyze whether

$$\frac{k(\Omega(2n+1,q))}{|\Omega(2n+1q)|_p} \leqslant \frac{7.3 \cdot q^n}{q^{n^2}} \leqslant 1.$$

We see that the inequality holds for every $n \geqslant 3$ and every $q \geqslant 3$.

(v) Case $\mathrm{P\Omega}^\epsilon(2n,q)$, with $n \geqslant 4$ and $\epsilon \in \{+,-\}$: In this case, $k(\mathrm{P\Omega}^\epsilon(2n,q)) \leqslant 14 \cdot q^n$ and $|\mathrm{P\Omega}^\epsilon(2n,q)|_p = q^{n(n-1)}$. We analyze whether

$$\frac{k(\mathrm{P\Omega}^\epsilon(2n,q))}{|\mathrm{P\Omega}^\epsilon(2n,q)|_p} \leqslant \frac{14 \cdot q^n}{q^{n(n-1)}} \leqslant 1.$$

We observe that the inequality holds for every $n \geqslant 4$ and hence the result holds in this case.

Exceptional groups: Since we are assuming that p is odd, we do not have to consider the cases ${}^2B_2(q)$ and ${}^2F_4(q)$.

In this case, using the bounds from [31, Table 1] (see [69] for more details), we can deduce that $k(S) \leqslant g_S(q)$, where g_S is a polynomial with positive coefficients. In particular, if $g_S(x) = \sum_{i=0}^{d_S} a_i x^i$, we have that $k(S) \leqslant (\sum_{i=0}^{d_S} a_i) q^{d_S}$

If $S \in \{{}^3D_4(q), F_4(q), E_6(q), {}^2E_6(q), E_7(q), E_8(q)\}$ then $\sum_{i=0}^{d_S} a_i \leqslant 252$ and hence $\frac{q^{d_S}}{|S|_p} \leqslant \frac{1}{q^8}$. Therefore, we have that

$$\mathrm{d}_\pi(S) \leqslant \frac{k(S)}{|S|_p|S|_s} \leqslant \frac{252}{q^8}\frac{1}{s} < \frac{1}{s} \leqslant \max_{t\in\{p,s\}}\{\frac{1}{t}\},$$

where the third inequality holds because $p^8 \geqslant 3^8 = 6561 > 252$. Thus, the result holds for these cases.

In the case $G_2(q)$, we have that $k(G_2(q)) \leqslant q^2 + 2q + 9 \leqslant 12q^2$. Thus

$$\frac{k(G_2(q))}{|G_2(q)|_p} \leqslant \frac{12}{q^4} < 1$$

and the result follows as above.

In the case ${}^2G_2(q)$, we have that $k({}^2G_2(q)) \leqslant q + 8$ and hence

$$\frac{k({}^2G_2(q))}{|{}^2G_2(q)|_p} \leqslant \frac{q+8}{q^3} < 1$$

where the last inequality holds because $q \geqslant 27$. Therefore, the result holds □

LEMMA 5.24. *Let G be a group and let π be a set of primes such that $|\mathbf{Z}(G)|_\pi = 1$. Then, $k_\pi(G) = k_\pi(G/\mathbf{Z}(G))$.*

PROOF. Let $Z := \mathbf{Z}(G)$. Every coset gZ of Z in G contains at most one π-element of G since $|Z|_\pi = 1$. The π-elements of G/Z are gZ where g runs through the π-elements of G. If g is a π-element, then the conjugacy class of gZ in G/Z consists of hZ where $h \in g^G$. Thus, there is a bijection between the π-conjugacy classes of G and the π-conjugacy classes of G/Z. □

In the case when π does not contain the defining characteristic of S, the conjugacy classes of π-elements of S will be semisimple classes, which can be described in terms of the associated simple algebraic group and its Weyl subgroup.

We introduce some more notation. Let $\mathbf{G}$ be an algebraic group over a field $\overline{\mathbb{F}_q}$ and let F be an Frobenius morphism on $\mathbf{G}$. We notice that $\mathbf{G}$ is a non-finite group. We say that $\mathbf{T} \leqslant \mathbf{G}$ is a **torus** for $\mathbf{G}$ if $\mathbf{T}$ can be written as a direct product of copies of $\overline{\mathbb{F}_q}^\times$ (viewing $\overline{\mathbb{F}_q}^\times$ as a linear algebraic group). We recall that all tori of $\mathbf{G}$ are abelian. By [75, Corollary 21.12], there exist $\mathbf{T}$ a maximal F-stable torus (maximal with respect to inclusion). We define the *Weyl group* of $\mathbf{G}$ with respect to $\mathbf{T}$ as $W = \mathbf{N}_\mathbf{G}(\mathbf{T})/\mathbf{T}$. We remark that W is a finite group by [75, Theorem 3.10]. Given $w \in W$, we will write $\mathbf{T}^{wF}$ to denote the set of points in $\mathbf{T}^w$ that are fixed by F.

With this notation, we have the following result, which is [72, Theorem 3.15]. In this result we deal with reductive algebraic groups and simply connected groups. We refer the reader to [75, Definition 6.14 and Definition 9.14] for the definitions.

THEOREM 5.25 (Malle, Navarro, Robinson). *Let $\boldsymbol{G}$ be a reductive algebraic group such that $[\boldsymbol{G}, \boldsymbol{G}]$ is simply connected. Let F be an Frobenius morphism on $\mathbf{G}$ and let $\boldsymbol{T}$ be a maximal F-stable torus. Let π be a set of primes not containing the defining characteristic of $\boldsymbol{G}$. Then*

$$k_\pi(\boldsymbol{G}^F) = \frac{1}{|W|} \sum_{w \in W} |\boldsymbol{T}^{wF}|_\pi,$$

where $W = \mathbf{N}_{\boldsymbol{G}}(\boldsymbol{T})/\boldsymbol{T}$ is the Weyl group of $\boldsymbol{G}$ with respect to $\boldsymbol{T}$.

THEOREM 5.26. *Let S be a finite simple group of Lie type. Assume that $S = \boldsymbol{G}^F/\mathbf{Z}(\boldsymbol{G}^F)$ for a simple algebraic group $\boldsymbol{G}$ of simply connected type and a Frobenius morphism F on $\mathbf{G}$. Let $\pi = \{p, s\}$ with $p < s$ be a set of primes not containing the defining characteristic of S. Suppose that s divides $|\mathrm{Syl}_p(S)|$. Then*

$$\mathrm{d}_\pi(\boldsymbol{G}^F) \leqslant \frac{1}{p}.$$

In particular, if $|\mathbf{Z}(\boldsymbol{G}^F)|_\pi = 1$, then $\mathrm{d}_\pi(S) \leqslant \frac{1}{p}$.

PROOF. Let $G := \mathbf{G}^F$. We first claim that a Hall π-subgroup of G, if exists, cannot be abelian. Assume for contradiction that G does have such subgroup, say H. Then $\overline{H} := H\mathbf{Z}(G)/\mathbf{Z}(G)$ would be an abelian Hall π-subgroup of S, implying that $\mathbf{N}_S(P)$ contains $\overline{H}$, where P is a Sylow p-subgroup of S that is contained in $\overline{H}$. It follows that s does not divide $|S : \mathbf{N}_S(P)|$, violating the hypothesis.

Let $\mathbf{T}$ be an F-stable maximal torus of $\mathbf{G}$, and let $W = \mathbf{N}_{\mathbf{G}}(\mathbf{T})/\mathbf{T}$ be the Weyl group of $\mathbf{G}$ with respect to $\mathbf{T}$. Since π does not contain the defining characteristic of S, we have

$$k_\pi(G) = \frac{1}{|W|} \sum_{w \in W} |\mathbf{T}^{w^{-1}F}|_\pi$$

by Theorem 5.25. It follows that

$$\mathrm{d}_\pi(G) = \frac{1}{|W|} \sum_{w \in W} \frac{|\mathbf{T}^{w^{-1}F}|_\pi}{|G|_\pi}.$$

Now, if $|\mathbf{T}^{wF}|_\pi = |G|_\pi$ for some $w \in W$ then a Hall π-subgroup of $\mathbf{T}^{wF}$, which is abelian, would be a Hall π-subgroup of G, and this contradicts the above claim. Thus

$$\frac{|\mathbf{T}^{wF}|_\pi}{|G|_\pi} \leqslant 1/p$$

for every $w \in W$. It then follows that

$$\mathrm{d}_\pi(G) \leqslant \frac{1}{p},$$

proving the first part of the theorem.

For the second part, assume that $|\mathbf{Z}(G)|_\pi = 1$. By Lemma 5.24, we then have

$$\mathrm{d}_\pi(S) = \mathrm{d}_\pi(G/\mathbf{Z}(G)) = \mathrm{d}_\pi(G) \leqslant \frac{1}{p},$$

as stated. □

Theorem 5.26 already proves Theorem 5.18 in several cases, as seen in the next result. In what follows, to unify the notation, we use GL^ϵ, SL^ϵ and PSL^ϵ for linear groups when $\epsilon = +$, and for unitary groups when $\epsilon = -$. We also use E_6^+ for E_6 and E_6^- for ${}^2E_6$.

Remark 5.27. We recall that the unitary group $\mathrm{GL}^-(n,q)$ consists of elements of $\mathrm{GL}(n,q^2)$ that fix the canonical Hermitian form. If the form is the canonical one, then $U \in \mathrm{GL}(n,q^2)$ is unitary iff U^{-1} coincides with the transpose of $\overline{U}$, where $\overline{U}$ is the matrix obtained from U by raising the entries by their q-th power.

Theorem 5.28. *Let S be a simple group of Lie type and let π be a set of two odd primes not containing the defining characteristic of S. Let p be the smallest prime in π. Assume that we are not in one of the following situations:*

(i) $S = E_6^\epsilon(q)$ *and* $3 \in \pi$.

(ii) $S = \mathrm{PSL}^\epsilon(n,q)$ *with* $n \geqslant 3$ *and* $\gcd(n, q-\epsilon)_\pi \neq 1$.

Then $\mathrm{d}_\pi(S) \leqslant \frac{1}{p}$.

Proof. Let $\mathbf{G}$ and F be as in Theorem 5.26. According to [**75**, Table 24.12], if we are not in one of the stated situations, then $|\mathbf{Z}(\mathbf{G}^F)|_\pi = 1$. The result then follows from Theorem 5.26. □

Next we prove Theorem 5.18 for case (i) in Theorem 5.28.

Proposition 5.29. *Let $S = E_6^\epsilon(q)$ with $(3,q) = 1$ and let $P \in \mathrm{Syl}_3(S)$. Then $|P'| > 3$. In particular, Theorem 5.18 holds in the case $S = E_6^\epsilon(q)$ and $3 \in \pi$.*

Proof. Let $\mathbf{G}$ be a simple algebraic group of simply connected type and $F : \mathbf{G} \to \mathbf{G}$ a Frobenius morphism such that $S = \mathbf{G}^F/\mathbf{Z}(\mathbf{G}^F)$. By [**75**, Corollary 25.17], we know that every Sylow 3-subgroup of $\mathbf{G}^F$ lies in $\mathbf{N}_{\mathbf{G}^F}(\mathbf{T})$ for some maximal F-stable torus $\mathbf{T}$ of $\mathbf{G}$. Therefore Sylow 3-subgroups of $\mathbf{N}_{\mathbf{G}^F}(\mathbf{T})/\mathbf{T}^F = \mathrm{SO}(5,3)$ (the Weyl group of E_6) are homomorphic images of Sylow 3-subgroups of $S = \mathbf{G}^F/\mathbf{Z}(\mathbf{G}^F)$. Since the size of the derived subgroup of Sylow 3-subgroups of $\mathrm{SO}(5,3)$ is 9 (this can be calculated by GAP [**33**]), we deduce that $|P'| > 3$. □

In the remainder of this subsection, we will prove Theorem 5.18 for case (ii) in Theorem 5.28.

LEMMA 5.30. *Let p be an odd prime and let $S = \mathrm{PSL}^\epsilon(n,q)$. Assume that p divides $\gcd(n, q-\epsilon)$ and Sylow p-subgroups of S are abelian. Then $n = p = 3$. Furthermore, $q - \epsilon$ is divisible by 3 but not 9.*

PROOF. It is argued in Lemma 2.8 of [61] that if Sylow p-subgroups of S are abelian and $p \geqslant 5$ then p cannot divide $|\mathbf{Z}(\mathrm{SL}^\epsilon(n,q))| = \gcd(n, q-\epsilon)$. Therefore our hypotheses imply that $p = 3$.

We first prove that $n = 3$. The condition $p = 3$ divides $\gcd(n, q-\epsilon)$, implies that $n \geqslant 3$. Assume for contradiction that $n > 3$. Let w be an element of order 3 of $\mathbb{F}_{q^2}^\times$, and consider the element $g := \mathrm{diag}(I_{n-2}, w, w^{-1}) \in \mathrm{GL}(n, q^2)$.

We claim that $g \in \mathrm{GL}^\epsilon(n,q)$. Assume first that $\epsilon = +$. Then we have that 3 divides $q-1$ and hence $w \in \mathbb{F}_q \subseteq \mathbb{F}_{q^2}$. It follows that $g \in \mathrm{GL}(n,q) = \mathrm{GL}^\epsilon(n,q)$. Assume now that $\epsilon = -$. In this case, 3 divides $q+1$. It follows that $w^q = w^{-1}$ and hence $g^q = g^{-1}$. Thus, $g \in \mathrm{GL}^\epsilon(n,q)$ by Remark 5.27. The claim follows.

Now, we have

$$\mathbf{C}_{\mathrm{GL}^\epsilon(n,q)}(g) = \mathrm{GL}^\epsilon(n-2,q) \times \mathrm{GL}^\epsilon(1,q)^2,$$

and so

$$|\mathrm{GL}^\epsilon(n,q) : \mathbf{C}_{\mathrm{GL}^\epsilon(n,q)}(g)| = q^{2n-1}\frac{(q^n-\epsilon^n)(q^{n-1}-\epsilon^{n-1})}{(q-\epsilon)^2}.$$

Since 3 divides $\gcd(n, q-\epsilon)$, we have that 3 must divide $|\mathrm{GL}^\epsilon(n,q) : \mathbf{C}_{\mathrm{GL}^\epsilon(n,q)}(g)|$. In fact, we also have 3 divides $|\mathrm{SL}^\epsilon(n,q) : \mathbf{C}_{\mathrm{SL}^\epsilon(n,q)}(g)|$. On the other hand, as 1 is the only eigenvalue of g with multiplicity larger than 1 (recall that $n > 3$), it is easy to see that $\mathbf{C}_{\mathrm{SL}^\epsilon(n,q)}(g)$ is the full pre-image of $\mathbf{C}_{\mathrm{PSL}^\epsilon(n,q)}(\overline{g})$ under the natural projection from SL^ϵ to PSL^ϵ, where $\overline{g}$ is the image of g in $\mathrm{PSL}^\epsilon(n,q)$. In particular, $|\mathrm{SL}^\epsilon(n,q) : \mathbf{C}_{\mathrm{SL}^\epsilon(n,q)}(g)| = |\mathrm{PSL}^\epsilon(n,q) : \mathbf{C}_{\mathrm{PSL}^\epsilon(n,q)}(\overline{g})|$, and hence 3 divides $|\mathrm{PSL}^\epsilon(n,q) : \mathbf{C}_{\mathrm{PSL}^\epsilon(n,q)}(\overline{g})|$, implying that Sylow 3-subgroups of $S = \mathrm{PSL}^\epsilon(n,q)$ are not abelian. We have shown that $n = 3$.

Finally, assume that 9 divides $q - \epsilon$. Let λ be an element of order 9 in $\mathbb{F}_{q^2}^\times$ and consider $h := \mathrm{diag}(\lambda, \lambda^3, \lambda^5) \in \mathrm{SL}(3, q^2)$, also of order 9. Reasoning as before, we have that $h \in \mathrm{SL}^\epsilon(3,q)$. We then have $\mathbf{C}_{\mathrm{GL}^\epsilon(3,q)}(h) = \mathrm{GL}^\epsilon(1,q)^3$, so that $|\mathbf{C}_{\mathrm{SL}^\epsilon(3,q)}(h)| = (q-\epsilon)^2$. Moreover, as $\{\lambda, \lambda^3, \lambda^5\} = \{a\lambda, a\lambda^3, a\lambda^5\}$ if and only if $a = 1$, $\mathbf{C}_{\mathrm{SL}^\epsilon(3,q)}(h)$ is the full pre-image of $\mathbf{C}_{\mathrm{PSL}^\epsilon(3,q)}(\overline{h})$. We deduce that $|\mathbf{C}_{\mathrm{PSL}^\epsilon(3,q)}(\overline{h})| = (q-\epsilon)^2/3$. This is smaller than the 3-part of $|\mathrm{PSL}^\epsilon(3,q)|$, and thus Sylow 3-subgroups of $\mathrm{PSL}^\epsilon(3,q)$ are not abelian, violating the hypothesis. So 9 cannot divide $q - \epsilon$, as stated. □

THEOREM 5.31. *Let p be an odd prime, let $n \geqslant 4$, and let $(n,p) \neq (6,3)$. Let $G := \mathrm{SL}^\epsilon(n,q)$ defined in characteristic not equal to p, let $S = G/\mathbf{Z}(G) = \mathrm{PSL}^\epsilon(n,q)$, and let $P \in \mathrm{Syl}_p(S)$. Suppose that $P/\mathbf{Z}(P)$ is abelian. Then p does not divide $|\mathbf{Z}(G)|$.*

PROOF. Assume for contradiction that p divides $|\mathbf{Z}(G)| = \gcd(n, q-\epsilon)$. Lemma 5.30 already shows that P is non-abelian, but we need to work harder to force $P/\mathbf{Z}(P)$ to be non-abelian, which is the contradiction we are seeking. Let $\lambda \in \mathbb{F}_{q^2}^{\times}$ be an element of order p and consider the p-element

$$x := \mathrm{diag}(\lambda, \lambda^{-1}, I_{n-2}) \in \mathrm{SL}(n, q^2).$$

Reasoning as in Lemma 5.30, we have that $x \in G$. Let $V = \mathbb{F}_q^n$, respectively $\mathbb{F}_{q^2}^n$, denote the natural G-module for $\epsilon = +$, respectively $\epsilon = -$. Fix a basis $B = \{v_1, v_2, ..., v_n\}$ of V, and consider the permutation y on B defined by

$$y := \{v_1 \mapsto v_2, v_2 \mapsto v_3, ..., v_{p-1} \mapsto v_p, v_p \mapsto v_1, v_i \mapsto v_i \text{ for } p < i \leqslant n\},$$

which is well-defined as $p \leqslant n$. Note that, as $p > 2$, we have $y \in G$ and $o(y) = p$. Direct calculation shows that

$$[x, y] = \mathrm{diag}(\lambda^{-1}, \lambda^2, \lambda^{-1}, I_{n-3}) =: s.$$

Suppose that the p-part of $q - \epsilon$ is p^a and let C be the (unique) cyclic subgroup of order p^a of $\mathbb{F}_{q^2}^{\times}$. We define

$$D := G \cap \{\mathrm{diag}(\lambda_1, \ldots, \lambda_n) \mid \lambda_1, \ldots, \lambda_n \in C\}.$$

We observe that if $d = \mathrm{diag}(\lambda_1, \ldots, \lambda_n) \in D$, then

$$d^y = \mathrm{diag}(\lambda_p, \lambda_1, \lambda_2, \ldots, \lambda_p, \lambda_{p+1}, \ldots, \lambda_n) \in D.$$

It follows that $\langle y \rangle$ normalizes D and hence $D\langle y \rangle$ is a p-subgroup of G. Therefore, both x and y belong to a Sylow p-subgroup, say $\widehat{P}$, of G. We deduce that $s = [x, y] \in \widehat{P}'$, which implies that $s\mathbf{Z}(G) \in P'$, where $P \in \mathrm{Syl}_p(S)$ is the image of $\widehat{P}$ under the natural projection $\mathrm{SL}^{\epsilon} \to \mathrm{PSL}^{\epsilon}$.

We will show that $s\mathbf{Z}(G)$ does not belong to $\mathbf{Z}(P)$, which is enough to conclude that $P/\mathbf{Z}(P)$ is not abelian.

Let $\widetilde{G} := \mathrm{GL}^{\epsilon}(n, q)$. We have

$$\mathbf{C}_{\widetilde{G}}(s) = \begin{cases} \mathrm{GL}^{\epsilon}(3, q) \times \mathrm{GL}^{\epsilon}(n-3, q) & \text{if } p = 3 \\ \mathrm{GL}^{\epsilon}(1, q) \times \mathrm{GL}^{\epsilon}(2, q) \times \mathrm{GL}^{\epsilon}(n-3, q) & \text{if } p > 3. \end{cases}$$

It is easy to see that $|S : \mathbf{C}_S(s\mathbf{Z}(G))| = |G : \mathbf{C}_G(s)| = |\widetilde{G} : \mathbf{C}_{\widetilde{G}}(s)|$. Hence,

$$|S : \mathbf{C}_S(s\mathbf{Z}(G))| = \begin{cases} \dfrac{|\mathrm{GL}^{\epsilon}(n, q)|}{|\mathrm{GL}^{\epsilon}(3, q)||\mathrm{GL}^{\epsilon}(n-3, q)|} & \text{if } p = 3 \\ \dfrac{|\mathrm{GL}^{\epsilon}(n, q)|}{|\mathrm{GL}^{\epsilon}(1, q)||\mathrm{GL}^{\epsilon}(2, q)||\mathrm{GL}^{\epsilon}(n-3, q)|} & \text{if } p > 3. \end{cases}$$

It follows that, if ℓ is the defining characteristic of S, then

$$|S : \mathbf{C}_S(s\mathbf{Z}(G))|_{\ell'} = \begin{cases} \dfrac{(q^n-\epsilon^n)(q^{n-1}-\epsilon^{n-1})(q^{n-2}-\epsilon^{n-2})}{(q-\epsilon)(q^2-1)(q^3-\epsilon^3)} & \text{if } p=3 \\ \dfrac{(q^n-\epsilon^n)(q^{n-1}-\epsilon^{n-1})(q^{n-2}-\epsilon^{n-2})}{(q-\epsilon)^2(q^2-1)} & \text{if } p>3. \end{cases}$$

Using the condition $p \mid \gcd(n, q-\epsilon)$ and the assumption $(n,p) \neq (6,3)$, we see that this is divisible by p. It follows that $s\mathbf{Z}(G)$ does not belong to $\mathbf{Z}(P)$, and this finishes the proof. □

LEMMA 5.32. *Let $S = \mathrm{PSL}^\epsilon(n,q)$ with $n \geqslant 4$. If 3 divides $q-\epsilon$, then $\mathrm{d}_3(S) \leqslant \frac{1}{3}$. In particular, if 3 divides $q-\epsilon$ and $3 \in \pi$, then $\mathrm{d}_\pi(S) \leqslant \frac{1}{3}$.*

PROOF. Assume, to the contrary, that $\mathrm{d}_3(S) > 1/3$. Then $\mathrm{d}_3(P) > 1/3$, and thus $|P'| \leqslant 3$ by Theorem 4.14, where $P \in \mathrm{Syl}_3(S)$. The proof of Theorem 5.31 shows that P' contains two elements $s\mathbf{Z}(G)$ and $t\mathbf{Z}(G)$, where $s = \mathrm{diag}(\lambda^{-1}, \lambda^2, \lambda^{-1}, I_{n-3})$ and $t = \mathrm{diag}(1, \lambda^{-1}, \lambda^2, \lambda^{-1}, I_{n-4})$. Obviously, these elements generate a group of order greater than 3, a contradiction. □

LEMMA 5.33. *Let $S = \mathrm{PSL}^\epsilon(3,q)$ and let π a set of odd primes with $3 \in \pi$. Then $\mathrm{d}_\pi(S) \leqslant \frac{1}{3}$.*

PROOF. If 3 does not divide $q-\epsilon$, then the result follows by Proposition 5.26. We therefore assume that 3 divides $q-\epsilon$. In particular, 3 divides $q^2+\epsilon q+1$. Set $t = \frac{(q-\epsilon)_3}{3}$ and note that

$$|S|_3 = \frac{((q-\epsilon)^2(q+\epsilon)(q^2+\epsilon q+1))_3}{3} \geqslant (q-\epsilon)_3^2 = 9t^2.$$

On the other hand, counting the number of conjugacy classes of 3-elements in $\mathrm{PSL}^\epsilon(3,q)$ (see [**116**]) we have $k_3(S) = (t^2+t+2)/2 \leqslant 2t^2$. Therefore,

$$\mathrm{d}_\pi(S) \leqslant \mathrm{d}_3(S) = \frac{k_3(S)}{|S|_3} \leqslant \frac{2t^2}{9t^2} < \frac{1}{3},$$

as wanted. □

PROPOSITION 5.34. *Theorem 5.18 holds for $S = \mathrm{PSL}^\epsilon(n,q)$ with $n \geqslant 3$ and $\pi = \{p,s\}$ with $p < s$ odd primes such that q is not divisible by neither p nor s.*

PROOF. The result follows by Theorem 5.26 in the case $\gcd(n, q-\epsilon)_\pi = 1$. So assume that $\gcd(n, q-\epsilon)_\pi > 1$ and let$r \in \pi$ be a divisor of $\gcd(n, q-\epsilon)$. The case $n = 3$ is handled by Lemma 5.33. So we assume furthermore that $n \geqslant 4$.

Let $R \in \mathrm{Syl}_r(S)$. We have that $R/\mathbf{Z}(R)$ is abelian by hypothesis. This and the condition that r divides $\gcd(n, q-\epsilon)$ contradict Theorem 5.31 if $r \geqslant 5$. The remaining case $r = 3$ is handled by Lemma 5.32. □

We have completed the proof of Theorem 5.18, by combining Theorems 5.21, 5.22, 5.23, 5.28 and Propositions 5.29 and 5.34.

As mentioned before, Theorem H follows from Theorem 5.18 and Theorem 5.19, together with Theorem 5.8.

5.4. Examples and open problems

In this section we present examples related with the content of this section and we propose some conjectures related to them.

The following examples show that converses of parts (i) and (ii) of Theorem H are false and the bounds are generically sharp. Throughout this section, π will be a set of primes and p will be the smallest prime in π.

EXAMPLE 5.35. We show that the converse of part (i) of Theorem H when $p = 2$. Let $\pi = \{2\}$ (in general, we may take any set of primes π with $2 \in \pi$ and $3 \notin \pi$) and let $G = \mathsf{S}_4 \times A$ for an abelian group A. Then

$$\mathrm{d}_2(G) = \mathrm{d}_2(\mathsf{S}_4 \times A) = \mathrm{d}_2(\mathsf{S}_4)\,\mathrm{d}_2(A) = \mathrm{d}_2(\mathsf{S}_4) = \frac{1}{2}.$$

EXAMPLE 5.36. We show that the converse of part (i) of Theorem H when $p > 2$. Assume that $|\pi| \geqslant 3$ and $p > 2$. Let P be a finite p-group with $|P'| = p$. Let

$$G = P \times (\prod_{p \neq q \in \pi} \mathsf{C}_q).$$

In this case

$$\begin{aligned}\mathrm{d}_\pi(G) &\leqslant \Big(\frac{p^2+p-1}{p^3}\Big) \cdot \Big(\prod_{p \neq q \in \pi} \frac{q+1}{2q}\Big) \\ &\leqslant \Big(\frac{p^2+p-1}{p^3}\Big) \cdot \Big(\frac{p+1}{2p}\Big)^{|\pi|-1} \\ &\leqslant \Big(\frac{p^2+p-1}{p^3}\Big) \cdot \Big(\frac{p+1}{2p}\Big).\end{aligned}$$

Since $p \geqslant 3$, this is less than $\frac{5}{6p}$.

EXAMPLE 5.37. We show that the converse of part (ii) of Theorem H when $p = 2$. Let $\pi = \{2\}$ (as before, we may take any set of primes π with $2 \in \pi$ and $3 \notin \pi$) and let $G = \mathsf{A}_4 \times A$ for an abelian group A. Then

$$\mathrm{d}_2(G) = \mathrm{d}_2(\mathsf{A}_4 \times A) = \mathrm{d}_2(\mathsf{A}_4)\,\mathrm{d}_2(A) = \mathrm{d}_2(\mathsf{A}_4) = \frac{1}{2} < \frac{5}{8}.$$

EXAMPLE 5.38. We show that the converse of part (ii) of Theorem H when $p > 2$. Assume that $|\pi| \geqslant 3$ and $p > 2$. Let $C = \prod_{q \in \pi} \mathbf{C}_q$. Let $T = \mathsf{C}_{p-1} \times (\mathsf{C}_2)^{|\pi|-1}$

and set $G = C \rtimes T$. Then

$$\mathrm{d}_\pi(G) = \frac{2}{p} \cdot \prod_{p \neq q \in \pi} \frac{q+1}{2q}.$$

Since $|\pi| \geqslant 3$, $q \geqslant p+2$ and all primes q in π are odd, we get

$$\mathrm{d}_\pi(G) \leqslant \Big(\frac{2}{p}\Big) \cdot \Big(\frac{(p+2)+1}{2(p+2)}\Big) \cdot \Big(\frac{(p+4)+1}{2(p+4)}\Big) \leqslant \frac{24}{35p} < \frac{1}{p} \leqslant \frac{p^2+p-1}{p^3}.$$

The inequality $\mathrm{d}_\pi(G) > \frac{p^2+p-1}{p^3}$ in part (ii) of Theorem H is sharp for every set of primes π. To see this, take G to be the direct product of a non-abelian p-group P such that $P/\mathbf{Z}(P) \cong \mathsf{C}_p \times \mathsf{C}_p$ (such a p-group exists by Remark 4.10) with an abelian group. In this case $\mathrm{d}_\pi(G) = \Pr(G) = \frac{p^2+p-1}{p^3}$ and G does not contain an abelian Hall π-subgroup.

Now let us consider the inequality $\mathrm{d}_\pi(G) > 1/p$ of part (i) of Theorem H. This condition is best possible when $p = 2$ and $3 \in \pi$, for if G is the direct product of S_3 and an abelian group, then $\mathrm{d}_\pi(G) = 1/2$ and G does not contain a nilpotent Hall π-subgroup. However, the bound is certainly not best possible when p is odd. For example, if we take $\pi = \{3, 7\}$ and $G = \mathsf{C}_7 \rtimes \mathsf{C}_3$, then $\mathrm{d}_\pi(G) = \Pr(G) = 5/21 < 1/3$ and G does not possess a nilpotent Hall π-subgroup.

Theorem D provided the best possible bound $g_n(p)$ such that if $\Pr(G) > g_n(p)$ and $p > 2$ is the smallest prime dividing $|G|$, then G is nilpotent. We conjecture that the bound $g_n(p)$ used in Theorem D should also be good for $\mathrm{d}_\pi(G)$.

Conjecture 5.39. *Let π be a set of* odd *primes and let p be the smallest prime in π. Let G be a group. If $\mathrm{d}_\pi(G) > g_n(p)$, then G has a nilpotent Hall π-subgroup.*

Notice that the proposed bound in Conjecture 5.39 would be best possible. To see this, let $p > 2$ be any prime. Since Theorem D is sharp, we have that there exists a non-nilpotent group L_p such that the smaller prime divisor of $|L_p|$ is p and $\Pr(L_p) = g_n(p)$. Thus, if we take π as the set of prime divisors of $|L_p|$, then we have that $\mathrm{d}_\pi(L_p) = g_n(p)$ and L_p does not possess a nilpotent Hall π-subgroup.

Proving this conjecture would require significantly more effort, especially when dealing with simple groups of Lie type in the setting where π does not contain the characteristic of S. The biggest issue is that $g_n(p)$ depends on non-explicit functions defined on p.

CHAPTER 6

Commuting probability of π-elements

6.1. Introduction

In this chapter we study the existence of normal and abelian Hall π-subgroups in terms of the probability that two π-elements commute

DEFINITION. Let π be a set of primes and let G be a group. We define $\Pr_\pi(G)$ as the probability that two randomly chosen π-elements of G commute, that is

$$\Pr_\pi(G) = \frac{|\{(x,y) \in G_\pi \times G_\pi \mid xy = yx\}|}{|G_\pi|^2}.$$

In [16], Burness, Guralnick, Moretó and Navarro introduced $\Pr_p(G)$, where p is a prime, and they proved a version of the Gustafson–Joseph Theorem for $\Pr_p(G)$.

THEOREM 6.1 (Theorem A of [16]). *Let G be a group and let p be a prime. Then G possesses a normal and abelian Sylow p-subgroup if and only if $\Pr_p(G) > \frac{p^2+p-1}{p^3}$.*

In fact, this result was a direct consequence of the following result.

THEOREM 6.2 (Theorem C of [16]). *Let G be a group and let p be a prime. If $x \in G_p \backslash \mathbf{O}_p(G)$, then*

$$\frac{|\mathbf{C}_G(x)_p|}{|G_p|} \leqslant \frac{1}{p}.$$

Our goal is to extend these results for a general set of primes π.

THEOREM I. *Let G be a group, let π be a set of primes and let p be the smallest prime in π. If $x \in G_\pi \backslash \mathbf{O}_\pi(G)$, then*

$$\frac{|\mathbf{C}_G(x)_\pi|}{|G_\pi|} \leqslant \frac{1}{p}.$$

If $\mathbf{F}^*(G)$ is a π'-group, it is possible to replace $1/p$ by $1/q$, where q is the smallest prime dividing $o(x)$ (see Theorem 6.13 below). The proof of this fact is independent of Theorem I and its proof does not depend on *CFSG*. It remains an open

problem to determine whether or not we can replace $1/p$ by $1/q$ in Theorem I, where q is the largest prime dividing $o(x)$.

From Theorem I, we deduce a generalized version of [**16**, Theorem A] for a general set of primes π. Our main result is the following.

THEOREM J. *Let G be a group, let π be a set of primes and let p be the smallest member of π. Then G has a normal and abelian Hall π-subgroup if and only* $\mathrm{Pr}_\pi(G) > \frac{p^2+p-1}{p^3}$.

As noted in [**16**], we observe that [**16**, Theorem A] and Theorem J are best possible for every prime p. For $p = 2$ we have that $\mathrm{Pr}_2(\mathsf{S}_3) = \frac{5}{8}$ and S_3 does not possess a normal Sylow 2-subgroup. Moreover, $\mathrm{Pr}_3(\mathsf{A}_4) = \frac{11}{27}$ and A_4 does not possess a normal Sylow 3-subgroup. Finally, for every $p > 3$, the group $\mathrm{PSL}(2,p)$ is simple and $\mathrm{Pr}_p(\mathrm{PSL}(2,p)) = \frac{p^2+p-1}{p^3}$ (see [**16**, Theorem B]).

It is worth remarking that the proofs of Theorems I and J are a refinement of the proofs of the main results of [**16**]. In general, we will use similar arguments and techniques as the ones used in that paper. The biggest difference will appear while studying the symmetric and alternating groups. Moreover, the study of groups of Lie type will be more involved in this thesis than in [**16**].

6.2. Preliminary results

6.2.1. Normal subgroups and π-commuting probability. In this subsection, we relate $\mathrm{Pr}_\pi(G)$ with $\mathrm{Pr}_\pi(G/N)$ for a normal subgroup N of G.

From Lemmas 4.8 and 5.9, we have that the invariants $\mathrm{Pr}(G)$ and $\mathrm{d}_\pi(G)$ behave well with respect to subgroups and quotients. However, in the case of $\mathrm{Pr}_\pi(G)$, it is not true that $\mathrm{Pr}_\pi(G) \leqslant \mathrm{Pr}_\pi(G/N)$ for any normal subgroup N. The following example appeared in [**16**, Remark 2.2].

EXAMPLE 6.3. Let $\pi = \{2\}$ and let G be the group `SmallGroup`(420,30) in the `SmallGroup` database in GAP [**33**]. This group has a normal subgroup N with $|N| = 3$ and $G/N = \mathsf{D}_{10} \times \mathsf{D}_{14}$. Computing, we have that

$$\mathrm{Pr}_2(G) = \frac{211}{1296} > \frac{11}{72} = \mathrm{Pr}_2(G/N).$$

The best we can get is the following result, which relates $\mathrm{Pr}_\pi(G)$ with $\mathrm{Pr}_\pi(G/N)$ when N is a normal π-subgroup of G.

LEMMA 6.4. *Let π be a set of primes, let N be a normal π-subgroup of G and let $x \in G_\pi$. Then the following hold:*

(i) $\frac{|\mathbf{C}_G(x)_\pi|}{|G_\pi|} \leqslant \frac{|\mathbf{C}_{G/N}(xN)_\pi|}{|(G/N)_\pi|}$.

(ii) $\Pr_\pi(G) \leqslant \Pr_\pi(G/N)$.

PROOF. Let $\bar{\cdot}$ denote the quotient by N.

First, we express $\overline{G}_\pi$ in terms of G_π. Since N is a normal π-subgroup, we have that $\overline{x}$ is a π-element if and only if x is a π-element. Thus $\overline{G}_\pi = \overline{G_\pi}$. Since $\{xN \mid x \in G_\pi\}$ is a partition of G_π, we deduce that $|\overline{G}_\pi| = \frac{|G_\pi|}{|N|}$.

In order to prove (i), it suffices to show that $|\mathbf{C}_G(x)_\pi| \leqslant |N||\mathbf{C}_{\overline{G}}(\overline{x})_\pi|$. It is easy to see that if $y \in \mathbf{C}_G(x)_\pi$, then $\overline{y} \in \mathbf{C}_{\overline{G}}(\overline{x})_\pi$. It follows that

$$|\mathbf{C}_{\overline{G}}(\overline{x})_\pi| \geqslant |\{\overline{y} \mid y \in \mathbf{C}_G(x)_\pi\}| = \frac{|\{yt \mid y \in \mathbf{C}_G(x)_\pi, t \in N\}|}{|N|} \geqslant \frac{|\mathbf{C}_G(x)_\pi|}{|N|},$$

which gives (i).

Now, let us prove (ii). Applying (i) and the fact that $|G_\pi| = |N||\overline{G}_\pi|$, we obtain

$$\Pr_\pi(G) = \frac{1}{|G_\pi|} \sum_{x \in G_\pi} \frac{|\mathbf{C}_G(x)_\pi|}{|G_\pi|} \leqslant \frac{1}{|\overline{G}_\pi|} \cdot \frac{1}{|N|} \sum_{x \in G_\pi} \frac{|\mathbf{C}_{\overline{G}}(\overline{x})_\pi|}{|\overline{G}_\pi|}.$$

Now, we observe that

$$\sum_{x \in G_\pi} \frac{|\mathbf{C}_{\overline{G}}(\overline{x})_\pi|}{|\overline{G}_\pi|} = \sum_{\overline{y} \in \overline{G}_\pi} \sum_{n \in N} \frac{|\mathbf{C}_{\overline{G}}(\overline{y})_\pi|}{|\overline{G}_\pi|} = |N| \sum_{\overline{y} \in \overline{G}_\pi} \frac{|\mathbf{C}_{\overline{G}}(\overline{y})_\pi|}{|\overline{G}_\pi|}.$$

and thus we deduce that

$$\Pr_\pi(G) \leqslant \frac{1}{|\overline{G}_\pi|} \sum_{\overline{y} \in \overline{G}_\pi} \frac{|\mathbf{C}_{\overline{G}}(\overline{y})_\pi|}{|\overline{G}_\pi|} = \Pr_\pi(\overline{G}),$$

which gives (ii). □

Example 6.3 above shows that this result cannot be extended, even when N is a normal π'-subgroup.

6.2.2. Preliminary results on actions of groups. In this subsection we present some results on actions of groups that we will use throughout this section. We recall that the action of a group A on a group G is said to be coprime if $\gcd(|A|, |G|) = 1$.

LEMMA 6.5 (Lemma 2.3 of [16]). *Let P be a p-group acting coprimely on a group K and let L be a P-invariant subgroup of K. If*

$$\frac{|\mathbf{C}_K(P) : \mathbf{C}_L(P)|}{|K : L|} < 1,$$

then

$$\frac{|\mathbf{C}_K(P) : \mathbf{C}_L(P)|}{|K : L|} \leqslant \frac{1}{p+1}.$$

LEMMA 6.6 (Lemma 2.4 of [16]). *Let G be a group, let $x, y \in G$ and let $K \leqslant G$ such that both x and y normalize K, $Kx = Ky$ and $\gcd(|K|, o(x)o(y)) = 1$. Then, $x = y^k$ for some $k \in K$.*

COROLLARY 6.7. *Let G be a group and let π be a set of primes. If $y \in G$ is a π-element and $K \leqslant G$ is a π'-subgroup of G normalized by y, then $y^K = (Ky)_\pi$.*

PROOF. Clearly, y^K is contained in $(Ky)_\pi$. Now, let $z \in (Ky)_\pi$. We know that $Ky = Kz$ and, since K is a π'-group and y is a π-element, we have that $\gcd(|K|, o(y)) = 1 = \gcd(|K|, o(z))$. Thus, by Lemma 6.6, we deduce that z and y must be K-conjugate. □

Finally, we introduce the fixed point ratio, which will be the key for proving Theorem I.

DEFINITION. Let G be a group acting on a finite set Ω. Given $z \in G$, we define the **fixed point ratio** of z as the proportion of elements in Ω fixed by z. That is

$$\mathrm{fpr}(z, \Omega) = \frac{|\{\omega \in \Omega \mid \omega^z = \omega\}|}{|\Omega|}.$$

REMARK 6.8. Assume that the action of G on Ω is transitive. Let $z \in G$ and let H be the point stabilizer of some element in Ω. Then, [14, Lemma 1.2(iii)] gives

$$\mathrm{fpr}(z, \Omega) = \frac{|z^G \cap H|}{|z^G|}.$$

It is important to remark that given a π-element $x \in G$, the proportion

$$\frac{|\mathbf{C}_G(x)_\pi|}{|G_\pi|}$$

is exactly the fixed point ratio of x, where we consider the action of G on G_π by conjugation. We will need the following results from [15] on the fixed point ratios of primitive permutation groups.

THEOREM 6.9 (Theorem 1 of [15]). *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with socle J and point stabilizer H. If $z \in G$ is an element of prime order p, then either*

$$\mathrm{fpr}(z, \Omega) \leqslant \frac{1}{p+1},$$

or one of the following holds:

(i) G is almost simple and one of the following holds:

a) $G \in \{\mathsf{S}_n, \mathsf{A}_n\}$ acting on k-element subsets of $\{1, \ldots, n\}$ with $1 \leqslant k < n/2$.

b) G *is classical in a subspace action and* $(G, H, z, \mathrm{fpr}(z, \Omega))$ *is listed in Table 6 of* [15].

c) $G = \mathsf{S}_n$, $H = \mathsf{S}_{n/2} \wr \mathsf{C}_2$ *and* z *is a transposition.*

d) $G = M_{22} \rtimes \mathsf{C}_2$, $H = \mathrm{PSL}(3,4) \rtimes (\mathsf{C}_2 \times \mathsf{C}_2)$ *and* z *is an involution in the class* $z = 2B$ *(in the ATLAS* [24] *notation).*

(ii) G *is an affine group,* $J = (\mathbf{C}_p)^d$, $z \in \mathrm{GL}_d(p)$ *is a transvection and* $\mathrm{fpr}(z, \Omega) = \frac{1}{p}$.

(iii) $G \leqslant A \wr \mathsf{S}_t$ *is a product type group with its product action on* $\Omega = \Gamma^t$ *and* $z \in A^t \cap G$, *where* $A \leqslant \mathrm{Sym}(\Gamma)$ *is one of the almost simple primitive groups in part (i).*

Corollary 6.10 (Corollary 3 of [15]). *Let* $G \leqslant \mathrm{Sym}(\Omega)$ *be a finite almost simple primitive permutation group with socle* J *and point stabilizer* H. *If* $z \in G$ *has prime order* p, *then either*

$$\mathrm{fpr}(z, \Omega) \leqslant \frac{1}{p},$$

or one of the following holds:

(i) $J = \mathsf{A}_n$ *and* Ω *is the set of* k*-element subsets of* $\{1, \ldots, n\}$ *with* $1 \leqslant k < n/2$.

(ii) G *is a classical group in a subspace action and* $(G, J, p, z, \mathrm{fpr}(z, \Omega))$ *is one of the possibilities recorded in Table 1 of* [15].

6.3. Proof of Theorem I

In this section we prove Theorem I. The general structure of the proof is organized as follows. We will begin by proving Theorem I when $\mathbf{F}^*(G)$ is a π'-subgroup. Then we will use the fixed point ratios to prove some weakened versions of Theorem I. Finally, we will use the previous cases to complete the proof. We remark that the structure of the proof of Theorem I follows the original proof of [16, Theorem A].

6.3.1. Special case. In this subsection we prove Theorem I when $\mathbf{F}^*(G)$ is a π'-subgroup. As we pointed in the introduction of this chapter, in this case, we will be able to prove an enhanced version. The proof of this case is based in coprime actions.

The following results give information on the proportion of π-elements which commute with a fixed π-element when the group possesses a normal and non-trivial π'-subgroup.

Proposition 6.11. *Let* G *be a group, let* π *be a set of primes and let* K *be a normal* π'*-subgroup of* G. *Assume that* $x \in G$ *is an element of order* $p \in \pi$,

such that $[x, K] = K$*. If* $y \in G$ *is a* π*-element which commutes with* x*, then the following hold:*

(i) If $[y, K] \neq 1$*, then*

$$\frac{|\{z \in (Ky)_\pi \mid [x, z] = 1\}|}{|(Ky)_\pi|} \leqslant \frac{1}{p+1}.$$

(ii) If $L = \langle K, x\rangle$*, then*

$$\frac{|\{z \in (Ly)_\pi \mid [x, z] = 1\}|}{|(Ly)_\pi|} \leqslant \frac{1}{p}.$$

Proof. We begin by proving (i). By Corollary 6.7, we have that $y^K = (Ky)_\pi$ and hence

$$\frac{|\{z \in (Ky)_\pi \mid [x, z] = 1\}|}{|(Ky)_\pi|} = \frac{|y^K \cap \mathbf{C}_G(x)|}{|y^K|}.$$

Now, $y^K \cap \mathbf{C}_G(x) = (Ky)_\pi \cap \mathbf{C}_G(x)$ and since $Ky \cap \mathbf{C}_G(x) = \mathbf{C}_K(x)y$, we deduce that $y^K \cap \mathbf{C}_G(x) = (\mathbf{C}_K(x)y)_\pi$. Now applying again Corollary 6.7 again, we see that $(\mathbf{C}_K(x)y)_\pi = y^{\mathbf{C}_K(x)}$. Since $\mathbf{C}_{\mathbf{C}_K(x)}(y) = \mathbf{C}_K(x) \cap \mathbf{C}_K(y)$, we deduce that

$$\frac{|y^K \cap \mathbf{C}_G(x)|}{|y^K|} = \frac{|\mathbf{C}_K(x) : (\mathbf{C}_K(x) \cap \mathbf{C}_K(y))|}{|K : \mathbf{C}_K(y)|}.$$

If this proportion is 1, then $[y, K] \subseteq \mathbf{C}_G(x)$ and hence, by the Three Subgroups Lemma (see [**54**, Lemma 4.9]), we have that $1 = [y, [x, K]] = [y, K]$, which is impossible. Thus, the proportion is strictly smaller than 1, and hence applying Lemma 6.5 with $P = \langle x\rangle$ and $L = \mathbf{C}_K(y)$, we deduce that this proportion is at most $\frac{1}{p+1}$ and the result follows.

Now, we prove (ii). For each $i \in \{0, 1, \ldots, p-1\}$ we define $a_i = |(Kx^iy)_\pi \cap \mathbf{C}_G(x)|$ and $b_i = |(Kx^iy)_\pi|$. Then

$$\frac{|\{z \in (Ly)_\pi \mid [x, z] = 1\}|}{|(Ly)_\pi|} = \frac{\sum_{i=0}^{p-1} a_i}{\sum_{i=0}^{p-1} b_i}.$$

Let $i \in \{0, 1, \ldots, p-1\}$. If $[x^iy, K] \neq 1$, then part (i) gives $a_i \leqslant \frac{b_i}{p+1}$. Thus, if $[x^iy, K] \neq 1$ for all $i \in \{0, 1, \ldots, p-1\}$, then

$$\frac{\sum_{i=0}^{p-1} a_i}{\sum_{i=0}^{p-1} b_i} \leqslant \frac{\frac{1}{p+1}\sum_{i=0}^{p-1} b_i}{\sum_{i=0}^{p-1} b_i} = \frac{1}{p+1} < \frac{1}{p}$$

and the result follows. Thus, we may assume that there exists $i \in \{0, 1, \ldots, p-1\}$ such that $[x^iy, K] = 1$. Without loss of generality, we may assume that $i = 0$, and hence $[y, K] = 1$. Thus, $y^K = \{y\}$ and hence $a_0 = b_0 = 1$. Now, since

$[y, K] = 1$ and $[x, K] = K$, we have that $[x^i y, K] \neq 1$ for all $i \in \{1, \dots, p-1\}$. Therefore, $a_i \leqslant \frac{b_i}{p+1}$ for all $i \in \{1, \dots, p-1\}$ and hence

$$\frac{1 + \sum_{i=1}^{p-1} a_i}{1 + \sum_{i=1}^{p-1} b_i} \leqslant \frac{1 + \frac{1}{p+1} \sum_{i=1}^{p-1} b_i}{1 + \sum_{i=1}^{p-1} b_i} = \frac{p}{(p+1)(1 + \sum_{i=1}^{p-1} b_i)} + \frac{1}{p+1}.$$

We also observe that $1 + \sum_{i=1}^{p-1} b_i = |(Ly)_\pi|$. Now, given $i \in \{1, \dots, p-1\}$ we note $x^i y \in (Kx^i y)_\pi$ and $x^i y$ commutes with x. Thus, $b_i \geqslant (p+1)a_i \geqslant p+1$ and hence $|(Ly)_\pi| \geqslant 1 + (p-1)(p+1) = p^2$. Therefore,

$$\frac{1 + \sum_{i=1}^{p-1} a_i}{1 + \sum_{i=1}^{p-1} b_i} \leqslant \frac{p}{(p+1)|(Ly)_\pi|} + \frac{1}{p+1} \leqslant \frac{p}{(p+1)p^2} + \frac{1}{p+1} = \frac{1}{p}$$

and the result follows. □

THEOREM 6.12. *Let π be a set of primes, let G be a group and let $x \in G$ be an element of order p, where $p \in \pi$. If there exists a normal π'-subgroup K of G such that $[x, K] \neq 1$, then*

$$\frac{|\mathbf{C}_G(x)_\pi|}{|G_\pi|} \leqslant \frac{1}{p}.$$

PROOF. Since $K\mathbf{C}_G(x)$ contains all elements in G commuting with x we may assume that $G = K\mathbf{C}_G(x)$. Since $\gcd(o(x), |K|) = 1$, we have that $[x, K] = [x, [x, K]]$ (see [**54**, Lemma 4.29]). Moreover, $[x, K]$ is normal in G and $[x, K]$ is a π'-subgroup (since $[x, K] \leqslant K$). Thus, we may replace K by $[x, K]$ and hence, we may assume that $K = [x, K]$. Let $L = \langle K, x \rangle$. It is easy to see that every π-element of G lies in Ly for some $y \in G_\pi$. Therefore, it suffices to prove that the proportion of π-elements in Ly commuting with x is at most $\frac{1}{p}$ for every $y \in G_\pi$. That is, we aim to prove that

$$\frac{|\{z \in (Ly)_\pi \mid [z, x] = 1\}|}{|(Ly)_\pi|} \leqslant \frac{1}{p} \tag{6.3.1}$$

for every $y \in G_\pi$.

If no π-element of Ly commutes with x, then the left-hand side of inequality (6.3.1) is 0 and hence inequality (6.3.1) holds trivially. Let us assume that there exists a π-element in Ly commuting with x. Thus, we may assume that $[x, y] = 1$ and hence, inequality (6.3.1) holds by Proposition 6.11(ii). □

Now, we prove an enhanced version of Theorem I when $\mathbf{F}^*(G)$ is a π'-group.

THEOREM 6.13. *Let π be a set of primes and let G be a group such that $\mathbf{F}^*(G)$ is a π'-group. If x is a non-trivial π-element of G, then*

$$\frac{|\mathbf{C}_G(x)_\pi|}{|G_\pi|} \leqslant \frac{1}{q}.$$

where q is the largest prime dividing $o(x)$.

PROOF. Since $\mathbf{C}_G(x) \leqslant \mathbf{C}_G(x^{\frac{o(x)}{q}})$, we may assume that x is an element of order q. The group $\mathbf{F}^*(G)$ is a normal subgroup of G with $\mathbf{C}_G(\mathbf{F}^*(G)) \leqslant \mathbf{F}^*(G)$ (see Theorem 1.11). By hypothesis, we have that $\gcd(o(x), |\mathbf{F}^*(G)|) = 1$, and hence $[x, \mathbf{F}^*(G)] \neq 1$. Thus, applying Theorem 6.12 with $K = \mathbf{F}^*(G)$, we get

$$\frac{|\mathbf{C}_G(x)_\pi|}{|G_\pi|} \leqslant \frac{1}{q}$$

and the result follows. □

6.3.2. General case. Now, we work towards a proof of Theorem I in the general setting. We remark that the proof of Theorem I relies on Theorem 6.9 and Corollary 6.10. Before beginning the proof, we have to prove some preliminary results, which provide information on the proportion of π-elements commuting with a fixed automorphism of order $p \in \pi$ of a central product of quasisimple groups.

PROPOSITION 6.14. *Let K be a central product of quasisimple groups with $\mathbf{O}_\pi(K) = 1$ and assume that the simple quotients of all components of K are isomorphic. Let $x, y \in \mathrm{Aut}(K)$ be non-trivial π-elements such that x acts non-trivially on the set of components of K. Then the proportion of elements in y^K commuting with x is at most $\frac{1}{p+1}$, where p is the smallest prime dividing $o(x)$.*

PROOF. If no element of y^K commutes with x, then the result holds trivially. Thus, we may assume that there exists an element in y^K commuting with x and hence, replacing y by an appropriate K-conjugate of y, we may assume that $[x, y] = 1$. Let $K_1, \ldots, K_t$ be the components of K and let L be the simple group such that $K_i/\mathbf{Z}(K_i) \cong L$ for all $i \in \{1, \ldots, t\}$. Since x acts non-trivially on the components, we have that $t \geqslant p > 1$. Set $J = K/\mathbf{Z}(K) \cong L^t$. We can view x and y as automorphisms of J and, in particular, they act in the set of components of J (which are just the copies of L in J). Since x acts non-trivially on the set of components, then there exists a non-trivial $\langle x, y\rangle$-orbit, say $\mathcal{O}$, on the set of components of J. Replacing J by the product of all copies in $\mathcal{O}$, we may assume that $\langle x, y\rangle$ acts transitively on the set of components of J. We define $G = \langle J, x, y\rangle \leqslant \mathrm{Aut}(J)$. Since $\langle x, y\rangle$ acts transitivelyon the set of components of J, we deduce that J is the unique minimal normal subgroup of G and hence J is the socle of J. The result will follow once we prove that the proportion of elements in y^J commuting with x (considered as automorphisms of J) is at most $\frac{1}{p+1}$.

It is not hard to see that for $z \in J$, $y^z \in \mathbf{C}_G(x)$ if and only if $x^{z^{-1}} \in \mathbf{C}_G(y)$. Therefore,

$$\frac{|y^J \cap \mathbf{C}_G(x)|}{|y^J|} = \frac{|x^J \cap \mathbf{C}_G(y)|}{|x^J|}.$$

Now, let H be a maximal subgroup of G containing $\mathbf{C}_G(y)$. We notice that H cannot contain J since $G = J\mathbf{C}_G(y)$. Since J is the socle of G, we deduce that H is a core-free maximal subgroup. Thus, G acts primitively on the set of cosets $\Omega = G/H$ and hence

$$\frac{|x^J \cap \mathbf{C}_G(y)|}{|x^J|} \leqslant \frac{|x^G \cap H|}{|x^G|} = \mathrm{fpr}(x, \Omega).$$

Thus, it suffices to prove that $\mathrm{fpr}(x, \Omega) \leqslant \frac{1}{p+1}$.

Assume first that $G \leqslant A \wr \mathsf{S}_t$ with its product action on $\Omega = \Gamma^t$, where A is an almost simple group with socle L and Γ is a set such that $A \leqslant \mathrm{Sym}(\Gamma)$. Thus, $x = nh$ where $n \in \mathrm{Aut}(L)^t$ and $h \in S_t$. Since x acts non-trivially on the set of components, we deduce that $h \neq 1$. Let $o(h) = r > 1$ (in particular, $r \geqslant p$). Then there exists a cycle of length r in the decomposition of $h \in \mathsf{S}_t$ as a product of disjoint cycles. In this situation, a straightforward computation with the product action shows that $|\{\omega \in \Omega \mid \omega^x = \omega\}| \leqslant |\Gamma|^{1-r}$ (a similar argument can be found in the proof of [**15**, Theorem 6.1]) and hence

$$\mathrm{fpr}(x, \Omega) \leqslant |\Gamma|^{1-r} \leqslant \frac{1}{r+1} \leqslant \frac{1}{p+1},$$

where the second inequality holds because $|\Gamma| \geqslant 5$. Thus, the result holds in this case.

Assume now that the action of G on Ω is not a product type action. We claim that (G, Ω) is none of the exceptions (i), (ii) or (iii) in Theorem 6.9. By our assumption, we are not in case (iii) of Theorem 6.9. Now, since the socle of G is $J \cong L^t$ with $t > 1$, we deduce that we have that G is not almost simple and hence we are not in case (i) of Theorem 6.9. Finally, since the socle of G is J, which is a non-solvable group, we have that we are not in case (ii) of Theorem 6.9. Thus, the claim follows.

Now, we observe that $x^{\frac{o(x)}{p}}$ is an element of order p in G. Therefore, since (G, Ω) is none of the exceptions (i), (ii) or (iii) in Theorem 6.9, we have

$$\mathrm{fpr}(x, \Omega) \leqslant \mathrm{fpr}(x^{\frac{o(x)}{p}}, \Omega) \leqslant \frac{1}{p+1}$$

and the result follows. □

Before continuing, we recall and prove some additional results that we will need.

PROPOSITION 6.15 (Lemma 3.9 of [**16**]). *Let G be an almost simple group with socle J and assume J is not isomorphic to an alternating group. Let p be a prime divisor of $|J|$ and suppose $x \in G$ has order p. Then there exists an element $y \in J$ of order p such that*

$$\frac{|y^G \cap \mathbf{C}_G(x)|}{|y^G|} \leqslant \frac{1}{p+1}.$$

The next result is a refinement of [**16**, Lemma 3.7].

LEMMA 6.16. *Let π be a set of primes, let G be a group, let $x \in G_\pi \backslash \mathbf{O}_\pi(G)$ and let*

$$D = \{y \in G \mid \langle y \rangle \text{ is } G\text{-conjugate to } \langle x \rangle\}.$$

Then $|D| \geqslant p^2 - 1$, where p is the smallest prime dividing $o(x)$.

PROOF. If x is a q-element for some prime $q \in \pi$, then the result follows from [**16**, Lemma 3.7]. Thus, we may assume that $o(x)$ is divisible by at least two different primes. Let us define

$$T = \{y \in \langle x \rangle \mid \langle y \rangle = \langle x \rangle\}.$$

It is easy to see that $T \subseteq D$ and $|T| = \varphi(o(x))$, where φ denotes again Euler's totient function. Thus, if $\varphi(o(x)) \geqslant p^2 - 1$, then the result holds.

Assume first that $p > 2$. If $o(x)$ has at least three prime divisors (counting multiplicities), then $\varphi(o(x)) \geqslant (p-1)^3 \geqslant p^2 - 1$. Thus, we may assume that $o(x)$ is divisible by at most two primes (counting multiplicities). Since x is not a q-element, we have that $o(x) = pt$, where $p < t$ are two odd primes (in particular, $t \geqslant p + 2$). Therefore, $\varphi(o(x)) = (p-1)(t-1) \geqslant (p-1)(p+1) = p^2 - 1$.

Assume now that $p = 2$. We may assume that $\varphi(o(x)) \leqslant 2$ and hence $o(x) \in \{2, 3, 4, 6\}$. Since we are assuming that x is not a q-element, we have that $o(x) = 6$. In this case, $\{2, 3\} \subseteq \pi$ and $T = \{x, x^5\}$. Assume that $x^g \in T$ for every $g \in G$. In this case, $\langle x \rangle$ is normal in G and hence $x \in \mathbf{O}_\pi(G)$, which is a contradiction. Thus, there exists $g \in G$ such that $x^g \notin T$. Then $\{x, x^5, x^g\} \subseteq D$ and hence $|D| \geqslant 3$. □

PROPOSITION 6.17. *Let K be a quasisimple group with $\mathbf{O}_\pi(K) = 1$. Let $J = K/\mathbf{Z}(K)$, and let $x \in \mathrm{Aut}(K)_\pi$ such that x has order $p \in \pi$. Assume that J is not an alternating group. If $y \in \mathrm{Aut}(K)$ is a π-element, then the proportion of elements in $(Ky)_\pi$ commuting with x is at most $\frac{1}{p}$.*

PROOF. Reasoning as in the proof of Proposition 6.14, we may assume that $[x, y] = 1$ and view x and y as automorphisms of J. Set $G = \langle J, x, y \rangle$. Notice that, since x commutes with all elements in $\langle x, y \rangle$, then $x^G = x^J$. We will divide the proof in different claims.

Claim 1: *If $(G, p) \neq (O^+(2n, 2), 2)$ and $z \in G \backslash \{1\}$, then the proportion of elements in z^K commuting with x is at most $1/p$.*

Assume first that (J, p) is not an exception in Corollary 6.10. Let H be any core-free maximal subgroup of G containing $\mathbf{C}_G(z)$. Since we are assuming that (J, p) is not an exception in Corollary 6.10, we deduce that

$$\frac{|z^J \cap \mathbf{C}_G(x)|}{|z^J|} = \frac{|x^J \cap \mathbf{C}_G(z)|}{|x^J|} \leqslant \frac{|x^G \cap H|}{|x^G|} = \mathrm{fpr}(x, G/H) \leqslant \frac{1}{p},$$

where the first inequality holds because $x^G = x^J$ and $\mathbf{C}_G(z) \leqslant H$. Reasoning as in Theorem 6.14, we deduce that the proportion of elements in z^K commuting with x is at most $\frac{1}{p}$.

Now assume that (J,p) is one of the exceptions of Corollary 6.10(ii). Let r be a prime and let $z \in G$ be an element of order r and let $(G,p,r) \neq (O^+(2n,2),2,2)$. By looking at [**15**, Table 1], we observe that either $p < r$, or one of the following holds:

(i) $r = p = 2$ and $G \neq O^+(2n,2)$.

(ii) $r < p = q-1$ and $J = \mathrm{PSL}(2,q)$.

(iii) $(G,p,r) = (\mathrm{PSp}(6,2),3,2)$.

Assume first that we are in cases (i), (ii) or (iii). Since $(G,p,r) \neq (O^+(2n,2),2,2)$ there exists some maximal subgroup H of G such that $\mathbf{C}_G(z)$ contains H and $\mathrm{fpr}(x,G/H) \leqslant 1/p$. Thus,

$$\frac{|z^J \cap \mathbf{C}_G(x)|}{|z^J|} = \frac{|x^J \cap \mathbf{C}_G(z)|}{|x^J|} \leqslant \frac{|x^G \cap H|}{|x^G|} = \mathrm{fpr}(x,G/H) \leqslant \frac{1}{p},$$

and Claim 1 holds in this case.

Assume now that $p < r$ and let T be a maximal subgroup of G containing $\mathbf{C}_G(x)$. Then $\mathrm{fpr}(z,G/T) \leqslant 1/r$ and hence

$$\frac{|z^J \cap \mathbf{C}_G(x)|}{|z^J|} \leqslant \frac{|z^G \cap T|}{|z^G|} = \mathrm{fpr}(z,G/T) \leqslant \frac{1}{r} < \frac{1}{p}.$$

This proves that Claim 1 holds when (J,p) is one of the exceptions and z is an element of prime order. Since $\mathbf{C}_G(z) \subseteq \mathbf{C}_G(z^m)$ and $\mathrm{fpr}(z,G/H) \leqslant \mathrm{fpr}(z^m,G/H)$, for all $z \in G\backslash\{1\}$ and for all $m \geqslant 1$, we have that Claim 1 holds for all $z \in G\backslash\{1\}$.

Claim 2: *If $(G,p) = (O^+(2n,2),2)$ and $z \in G\backslash\{1\}$ and it is not a 2-element, then the proportion of elements in z^K commuting with x is at most $1/3$.*

Reasoning as in the last paragraph of Claim 1, we may assume that $o(z) = r$, where r is the smallest prime dividing $o(z)$. In particular, r is an odd prime. Then, Claim 2 follows from the case "$p < r$" of Claim 1.

Claim 3: *There exists a normal subset D of $K_p\backslash\{1\}$ such that $|D| \geqslant p^2 - 1$ and the proportion of elements in D commuting with x is at most $1/(p+1)$.*

By Theorem 6.15, there exists w a non-trivial p-element of J such that

$$\frac{|w^J \cap \mathbf{C}_G(x)|}{|w^J|} \leqslant \frac{|w^G \cap \mathbf{C}_G(x)|}{|w^G|} \leqslant \frac{1}{p+1}.$$

Let us identify w with its pre-image on K. Thus, if we embed w in K and we set

$$D = \{z \in G \mid \langle z\rangle \text{ is conjugate to } \langle w\rangle \text{ in } K\},$$

then we have that D is a normal subset of p-elements. Therefore, $D = \bigcup_{i=1}^{r} z_i^K$, where each z_j is K-conjugate to some power of w and hence

$$\frac{|z_i^J \cap \mathbf{C}_G(x)|}{|z_i^J|} = \frac{|w^J \cap \mathbf{C}_G(x)|}{|w^J|} \leqslant \frac{1}{p+1}.$$

Thus, the proportion of elements in D commuting with x is at most $1/(p+1)$. Moreover, by Lemma 6.16, we know that $|D| \geqslant p^2 - 1$. This proves Claim 3.

We are now ready prove the proposition when $(G,p) \neq (O^+(2n,2),2)$. We have that $(Ky)_\pi = \bigcup_{i=1}^{t} y_i^K$, where each y_i^K is a π-element. Assume first that $Ky \neq K$. By Claim 1, the proportion of elements in y_i^K commuting with x is at most $1/p$ for each i and the result follows in this case. Assume now that $Ky = K$. Let D be the set defined in Claim 3. Since $D \subseteq K_\pi \backslash \{1\}$ and D is normal in G it follows that

$$(Ky)_\pi = K_\pi = \{1\} \cup D \cup (\bigcup_{i=1}^{s} y_i^K),$$

where each y_i^K is a non-trivial π-element. By Claim 1, the proportion of elements in y_i^K commuting with x is at most $1/p$ for all i. Therefore, it suffices to prove that

$$\frac{|D \cap \mathbf{C}_K(x)| + 1}{|D| + 1} \leqslant \frac{1}{p}.$$

Now, by the second claim, we have that $|D \cap \mathbf{C}_K(x)| \leqslant \frac{|D|}{p+1}$. Thus,

$$\frac{|D \cap \mathbf{C}_K(x)| + 1}{|D| + 1} \leqslant \frac{1 + \frac{1}{p+1}|D|}{|D| + 1} = \frac{p + 1 + |D|}{(p+1)(|D| + 1)} =$$

$$= \frac{p}{(p+1)(|D| + 1)} + \frac{1}{p+1} \leqslant \frac{1}{(p+1)p} + \frac{1}{p+1} = \frac{1}{p},$$

where the last inequality holds because $|D| \geqslant p^2 - 1$.

To complete the proof, we may assume that $(G,p) = (O^+(2n,2),2)$ (in particular, $2 \in \pi$). Assume first that Ky contains no 2-element. In this case $(Ky)_\pi = \bigcup_{i=1}^{t} y_i^K$, where each y_i is a π-element which is not a 2-element. Thus, applying Claim 2, we deduce that the proportion of elements in each y_i^K that commute with x is at most $1/3$. Therefore, the result holds in this case.

Assume now that Ky contains a 2-element. Replacing y by a 2-element in Ky, we may assume that y is a 2-element. Then $(Ky)_\pi = (Ky)_2 \cup (\bigcup_{i=1}^{t} y_i^K)$, where each y_i is a π-element which is not a 2-element. Reasoning as before, the proportion of elements in y_i^K which commute with x is at most $1/3$ for each i. Moreover, by [**16**, Proposition 3.10 (ii) b)], we have that the proportion of elements in $(Ky)_2$ commuting with x is at most $1/2$. Thus, the result follows in this case. □

Finally, we prove two results that will allow us to study the case when the group has alternating composition factors. We recall that, given $x \in \mathsf{S}_n$, the support of x is the set of elements in $\{1, \dots, n\}$, which are not fixed by x.

PROPOSITION 6.18. *Let p be a prime, let π be a set of primes containing p and let $n \geqslant 5$. If $x \in \mathsf{S}_n$ is an element of order p and x is not a transposition, then*

$$|(\mathsf{A}_n)_\pi| \geqslant p|\mathbf{C}_{\mathsf{A}_n}(x)_\pi|,$$

and

$$|(\mathsf{S}_n \backslash \mathsf{A}_n)_\pi| \geqslant p|(\mathbf{C}_{\mathsf{S}_n}(x) \backslash \mathsf{A}_n)_\pi|.$$

Equivalently, the proportion of π-elements in A_n and in $\mathsf{S}_n \backslash \mathsf{A}_n$ commuting with x is at most $\frac{1}{p}$.

PROOF. Let m be the size of the support of x. We notice that p divides m and that $\mathbf{C}_{\mathsf{S}_n}(x) = (\mathsf{C}_p \wr \mathsf{S}_{m/p}) \times \mathsf{S}_{n-m} \leqslant (\mathsf{S}_p \wr \mathsf{S}_{m/p}) \times \mathsf{S}_{n-m}$.

Assume first that $m = p$ and $p \geqslant 5$. In this case, $\mathbf{C}_{\mathsf{S}_n}(x) = \langle x \rangle \times \mathsf{S}_{n-m}$ and hence, $|(\mathbf{C}_{\mathsf{A}_n}(x))_\pi| = p|(\mathsf{A}_{n-p})_\pi|$ and $|(\mathbf{C}_{\mathsf{S}_n}(x) \backslash \mathsf{A}_n)_\pi| = p|(\mathsf{S}_{n-p} \backslash \mathsf{A}_{n-p})_\pi|$. On the other hand, we also have that $|(\mathsf{A}_n)_\pi| \geqslant |(\mathsf{A}_p)_\pi||(\mathsf{A}_{n-p})_\pi|$ and $|(\mathsf{S}_n \backslash \mathsf{A}_n)_\pi| \geqslant |(\mathsf{A}_p)_\pi||(\mathsf{S}_{n-p} \backslash \mathsf{A}_{n-p})_\pi|$. Since A_p does not possess a normal Sylow p-subgroup, we have that $|(\mathsf{A}_p)_p| \geqslant p^2$ and hence $|(\mathsf{A}_p)_\pi| \geqslant p^2$. Thus, both inequalities of the proposition hold.

Next assume that $m > p$ and $m \geqslant 5$. Since A_m does not possess a normal Sylow p-subgroup, we deduce that $|(\mathsf{A}_m)_\pi| \geqslant p^2$ and the following inequalities are satisfied

$$\begin{aligned} |\mathbf{C}_{\mathsf{A}_n}(x)_\pi| \leqslant\ & |((\mathsf{S}_p \wr \mathsf{S}_{m/p}) \cap \mathsf{A}_m)_\pi||(\mathsf{A}_{n-m})_\pi| + \\ & + |((\mathsf{S}_p \wr \mathsf{S}_{m/p}) \cap (\mathsf{S}_m \backslash \mathsf{A}_m))_\pi||(\mathsf{S}_{n-m} \backslash \mathsf{A}_{n-m})_\pi| \end{aligned}$$

and

$$\begin{aligned} |(\mathbf{C}_{\mathsf{S}_n}(x) \backslash \mathsf{A}_n)_\pi| \leqslant\ & |((\mathsf{S}_p \wr \mathsf{S}_{m/p}) \backslash \mathsf{A}_m)_\pi||(\mathsf{A}_{n-m})_\pi| + \\ & + |((\mathsf{S}_p \wr \mathsf{S}_{m/p}) \cap \mathsf{A}_m)_\pi||(\mathsf{S}_{n-m} \backslash \mathsf{A}_{n-m})_\pi|. \end{aligned}$$

Now, we claim that

$$|((\mathsf{S}_p \wr \mathsf{S}_{m/p}) \cap \mathsf{A}_m)_\pi| \leqslant \frac{|(\mathsf{A}_m)_\pi|}{p} \tag{6.3.2}$$

and

$$|((\mathsf{S}_p \wr \mathsf{S}_{m/p}) \backslash \mathsf{A}_m))_\pi| \leqslant \frac{|(\mathsf{S}_m \backslash \mathsf{A}_m)_\pi|}{p}. \tag{6.3.3}$$

Let us prove inequality (6.3.2) (the proof of inequality (6.3.3) is analogous). Let $(\mathsf{A}_m)_\pi = \{1\} \cup (\bigcup_{i=1}^t y_i^{\mathsf{A}_m})$, where each y_i is a non-trivial π-element of A_m.

Applying Theorem 6.9, we have that

$$\frac{|y_i^{\mathsf{A}_m} \cap (\mathsf{S}_p \wr \mathsf{S}_{m/p})|}{|y_i^{\mathsf{A}_m}|} \leqslant \frac{1}{p+1}$$

for all $i \in \{1, \dots, t\}$. Thus, we deduce that

$$\frac{|((\mathsf{S}_p \wr \mathsf{S}_{m/p}) \cap \mathsf{A}_m)_\pi|}{|(\mathsf{A}_m)_\pi|} = \frac{1 + \sum_{i=1}^t |y_i^{\mathsf{A}_m} \cap (\mathsf{S}_p \wr \mathsf{S}_{m/p})|}{1 + \sum_{i=1}^t |y_i^{\mathsf{A}_m}|} \leqslant$$

$$\leqslant \frac{p+1+\sum_{i=1}^t |y_i^{\mathsf{A}_m}|}{(p+1)(1+\sum_{i=1}^t |y_i^{\mathsf{A}_m}|)} = \frac{p}{(p+1)|(\mathsf{A}_m)_\pi|} + \frac{1}{p+1} \leqslant \frac{1}{p},$$

where the last inequality holds since $|(\mathsf{A}_m)_\pi| \geqslant p^2$. Therefore, inequality (6.3.2) holds.

Now, applying inequalities (6.3.2) and (6.3.3), we deduce that

$$|\mathbf{C}_{\mathsf{A}_n}(x)_\pi| \leqslant \frac{1}{p}(|(\mathsf{A}_m)_\pi||(\mathsf{A}_{n-m})_\pi| + |(\mathsf{S}_m \backslash \mathsf{A}_m)_\pi||(\mathsf{S}_{n-m} \backslash \mathsf{A}_{n-m})_\pi|) =$$
$$= \frac{1}{p}|(\mathsf{S}_m \times \mathsf{S}_{n-m})_\pi \cap \mathsf{A}_n| \leqslant \frac{|(\mathsf{A}_n)_\pi|}{p}$$

and

$$|(\mathbf{C}_{\mathsf{S}_n}(x) \backslash \mathsf{A}_n)_\pi| \leqslant \frac{1}{p}(|(\mathsf{S}_m \backslash \mathsf{A}_m)_\pi||(\mathsf{A}_{n-m})_\pi| + |(\mathsf{A}_m)_\pi||(\mathsf{S}_{n-m} \backslash \mathsf{A}_{n-m})_\pi|) =$$
$$= \frac{1}{p}|(\mathsf{S}_m \times \mathsf{S}_{n-m})_\pi \backslash \mathsf{A}_n| \leqslant \frac{|(\mathsf{S}_n \backslash \mathsf{A}_n)_\pi|}{p}$$

and the proposition holds.

To complete the proof, we may assume that $m \in \{3, 4\}$.

Suppose first that $m = 3$. Then $3 \in \pi$ and x is a 3-cycle. Without loss of generality, we may assume that $x = (1, 2, 3)$. In this case, we have that $\mathbf{C}_{\mathsf{S}_n}(x)_\pi = \langle (1, 2, 3) \rangle \times (\mathsf{S}_{n-3})_\pi$ and hence $|\mathbf{C}_{\mathsf{A}_n}(x)_\pi| = 3|(\mathsf{A}_{n-3})_\pi|$ and $|(\mathbf{C}_{\mathsf{S}_n}(x) \backslash \mathsf{A}_n)_\pi| = 3|(\mathsf{S}_{n-3} \backslash \mathsf{A}_{n-3})_\pi|$. Fix $i \in \{4, \dots, n\}$ and let $L(i)$ be the set of elements of the form $(1, 2, i)b$ or $(1, i, 2)b$, where $b \in (\mathsf{A}_n)_\pi$ fixes1,2 and i. Analogously, we define $T(i)$ as the set of elements of the form $(1, 2, i)b$ or $(1, i, 2)b$ for $b \in (\mathsf{S}_n \backslash \mathsf{A}_n)_\pi$ fixing 1,2 and i. Notice that the $L(i)$ are disjoint subsets of elements of $(\mathsf{A}_n)_\pi$ of size $2|(\mathsf{A}_{n-3})_\pi|$, whose elements do not commute with x. Adding the number of π-elements in A_n which commute with x, we have that $|(\mathsf{A}_n)_\pi| \geqslant (2n-3)|(\mathsf{A}_{n-3})_\pi|$. Replacing the $L(i)$ by $T(i)$ and reasoning analogously, we deduce that $|(\mathsf{S}_n \backslash \mathsf{A}_n)_\pi| \geqslant (2n-3)|(\mathsf{S}_{n-3} \backslash \mathsf{A}_{n-3})_\pi|$. Therefore,

$$\frac{|\mathbf{C}_{\mathsf{A}_n}(x)_\pi|}{|(\mathsf{A}_n)_\pi|} \leqslant \frac{3}{2n-3},$$

and we observe that $\frac{3}{2n-3}$ is smaller than $1/3$ for $n \geqslant 6$. For $n = 5$ we only have to compute this proportion for $\pi \in \{\{3\}, \{2,3\}, \{3,5\}, \{2,3,5\}\}$. Since $\mathbf{C}_{\mathsf{A}_5}(x) = \langle x \rangle$, we have that $|\mathbf{C}_{\mathsf{A}_5}(x)_\pi| = 3$ for any of the possible π. Moreover, $|(\mathsf{A}_5)_\pi| \geqslant |(\mathsf{A}_5)_3| = 21$. Thus, $\frac{|\mathbf{C}_{\mathsf{A}_5}(x)_\pi|}{|(\mathsf{A}_5)_\pi|} \leqslant \frac{3}{21} < \frac{1}{3}$ and the result follows in this case.

To complete the proof of the case $m = 3$, we may assume that $2 \in \pi$ (otherwise, $(\mathbf{C}_{\mathsf{S}_n}(x) \backslash \mathsf{A}_n)_\pi = \varnothing$ and there is nothing to prove). Reasoning as above, we have that

$$\frac{|(\mathbf{C}_{\mathsf{S}_n}(x) \backslash \mathsf{A}_n)_\pi|}{|(\mathsf{S}_n \backslash \mathsf{A}_n)_\pi|} \leqslant \frac{3}{2n-3},$$

which is smaller than $1/3$ for $n \geqslant 6$. For $n = 5$ we have $\pi \in \{\{2,3\}, \{2,3,5\}\}$ and here we get $|(\mathbf{C}_{\mathsf{S}_5}(x) \backslash \mathsf{A}_5)_{\{2,3,5\}}| = |(\mathbf{C}_{\mathsf{S}_5}(x) \backslash \mathsf{A}_5)_{\{2,3\}}| = 3$. It follows that

$$\frac{|(\mathbf{C}_{\mathsf{S}_5}(x) \backslash \mathsf{A}_5)_\pi|}{|(\mathsf{S}_5 \backslash \mathsf{A}_5)_\pi|} \leqslant \frac{3}{30} < \frac{1}{3}$$

and the proposition holds for $m = 3$.

Finally, assume that $m = 4$. In this case we may assume that $x = (1,2)(3,4)$ and hence $\mathbf{C}_{\mathsf{S}_n}(x) = \mathbf{C}_{\mathsf{S}_4}(x) \times \mathsf{S}_{n-4}$ and hence

$$|\mathbf{C}_{\mathsf{A}_n}(x)_\pi| = |(\mathbf{C}_{\mathsf{S}_n}(x) \backslash \mathsf{A}_n)_\pi| = 4|(\mathsf{S}_{n-4})_\pi|.$$

For $5 \leqslant i < j \leqslant n$, let $Z(i,j)$ be the set of elements of S_n of the form uv, where u is a double transposition on $\{1,2,i,j\}$, different from $(1,2)(i,j)$, and v is a π-element fixing each element of $\{1,2,i,j\}$. Analogously, we define $W(i,j)$ in the same way, but replacing u by a 4-cycle on $\{1,2,i,j\}$, different from $(1,2,i,j)$. Thus, $W(i,j)$ and $Z(i,j)$ are sets of π-elements not commuting with x such that $|W(i,j)| = 2|(\mathsf{S}_{n-4})_\pi|$ and $|Z(i,j)| = 2|(\mathsf{S}_{n-4})_\pi|$. Thus, for each choice of $\{i,j\}$, we obtain at least $2|(\mathsf{S}_{n-4})_\pi|$ different π-elements in A_n or in $\mathsf{S}_n \backslash \mathsf{A}_n$ not commuting with x. This implies

$$\min\{|(\mathsf{A}_n)_\pi|, |(\mathsf{S}_n \backslash \mathsf{A}_n)_\pi|\} \geqslant (4 + (n-4)(n-5))|(\mathsf{S}_{n-4})_\pi|.$$

For $n \geqslant 7$ we have that $\frac{4}{4+(n-4)(n-5)} \leqslant \frac{1}{2}$ and the proposition holds. Finally, suppose that $n \in \{5,6\}$. Let π be a set of primes such that $\{2\} \subseteq \pi \subseteq \{2,3,5\}$. Then $\mathbf{C}_{\mathsf{S}_n}(x)_\pi = \mathbf{C}_{\mathsf{S}_n}(x)_2$ and hence

$$\frac{|\mathbf{C}_{\mathsf{A}_n}(x)_\pi|}{|(\mathsf{A}_n)_\pi|} \leqslant \frac{|\mathbf{C}_{\mathsf{A}_n}(x)_2|}{|(\mathsf{A}_n)_2|} \leqslant \frac{1}{2}$$

and

$$\frac{|(\mathbf{C}_{\mathsf{S}_n}(x) \backslash \mathsf{A}_n)_\pi|}{|(\mathsf{S}_n \backslash \mathsf{A}_n)_\pi|} \leqslant \frac{|(\mathbf{C}_{\mathsf{S}_n}(x) \backslash \mathsf{A}_n)_2|}{|(\mathsf{S}_n \backslash \mathsf{A}_n)_2|} \leqslant \frac{1}{2}.$$

Thus, the result holds when $m = 4$. □

PROPOSITION 6.19. *Let $n \geqslant 5$ and let π be a set of primes containing 2. If $x \in \mathsf{S}_n$ is a transposition, then*

$$\frac{|\mathbf{C}_{\mathsf{S}_n}(x)_\pi|}{|(\mathsf{S}_n)_\pi|} < \frac{1}{2}.$$

PROOF. We may assume that $x = (1,2)$. We know that $\mathbf{C}_{\mathsf{S}_n}(x) = \langle (1,2) \rangle \times \mathsf{S}_{n-2}$ and hence $|\mathbf{C}_{\mathsf{S}_n}(x)_\pi| = 2|(\mathsf{S}_{n-2})_\pi|$. Given $j \in \{3, \dots, n\}$ we define

$$Z_j = \{\tau \in (\mathsf{S}_n)_\pi \mid \tau(1) = j, \tau(j) = 1\}$$

noting that Z_j is a set of π-elements of S_n that do not commute with x. In addition, we see that $Z_i \cap Z_j = \varnothing$ if $i \neq j$. Thus, counting the π-elements centralizing x, we get $|(\mathsf{S}_n)_\pi| \geqslant n|(\mathsf{S}_{n-2})_\pi|$. Therefore,

$$\frac{|\mathbf{C}_{\mathsf{S}_n}(x)_\pi|}{|(\mathsf{S}_n)_\pi|} \leqslant \frac{2|(\mathsf{S}_{n-2})_\pi|}{n|(\mathsf{S}_{n-2})_\pi|} = \frac{2}{n} \leqslant \frac{2}{5} < \frac{1}{2}$$

and the result follows. □

Now, we restate and prove Theorem I.

THEOREM 6.20. *Let G be a group and let π be a set of primes. If $x \in G_\pi \backslash \mathbf{O}_\pi(G)$, then*

$$\frac{|\mathbf{C}_G(x)_\pi|}{|G_\pi|} \leqslant \frac{1}{p},$$

where p is the smallest prime in π.

PROOF. By Lemma 6.4, we may assume that $\mathbf{O}_\pi(G) = 1$. Let q be the smallest prime dividing $o(x)$. Thus, $q \in \pi$ and hence $p \leqslant q$. Since $\mathbf{C}_G(x) \subseteq \mathbf{C}_G(x^{\frac{o(x)}{q}})$, we may assume that $o(x) = q$. We also have that $x \notin \mathbf{F}(G)$.

If x does not centralize $\mathbf{O}_{\pi'}(G)$, then the result follows by Theorem 6.12. Therefore, we may assume that x centralizes $\mathbf{O}_{\pi'}(G)$, and hence $x \in \mathbf{C}_G(\mathbf{F}(G)) \backslash \mathbf{F}(G)$. In particular, G is non-solvable by Theorem 1.9.

Let $K = \mathbf{E}(G)$ be the layer of G (see Section 1.3 for the definition of $\mathbf{E}(G)$). Since x has prime order, the action of $\langle x \rangle$ on K (by conjugation) is either trivial or faithful. If the action is trivial, then x centralizes both $\mathbf{F}(G)$ and K, and thus it centralizes $\mathbf{F}(G)K = \mathbf{F}^*(G)$, which is impossible since $\mathbf{C}_G(\mathbf{F}^*(G)) \leqslant \mathbf{F}^*(G)$ by Theorem 1.11. It follows that $\langle x \rangle$ acts faithfully on K.

Since $\mathbf{C}_G(x)_\pi \subseteq K\mathbf{C}_G(x)$, we may replace G by the subgroup $K\mathbf{C}_G(x)$. Replacing K by the central product of all components in a $\mathbf{C}_G(x)$-orbit in its action on the set of component, we may also assume that $\mathbf{C}_G(x)$ acts transitively on the components of K. In particular, the simple quotients of all components of K are isomorphic. Thus, we have two possibilities:

(a) x acts non-trivially on the set of components of K.

(b) x normalizes each component of K.

We notice that x is allowed to normalize some of the components in in case a). We observe that the result will follow once we prove that

$$\frac{|(Ky)_\pi \cap \mathbf{C}_G(x)|}{|(Ky)_\pi|} \leqslant \frac{1}{p}$$

for every non-trivial $y \in \mathbf{C}_G(x)_\pi$. We may also assume that $G = \langle K, x, y\rangle$ and that $\langle x, y\rangle$ acts transitively on the components of K.

Suppose first that we are in case a). Let $z \in (Ky)_\pi$ with $z \neq 1$. By Proposition 6.14, we have that

$$\frac{|z^K \cap \mathbf{C}_G(x)|}{|z^K|} \leqslant \frac{1}{q+1} \leqslant \frac{1}{p+1}.$$

Thus, if $Ky \neq K$, then by expressing $(Ky)_\pi$ as a union of conjugacy classes, we see that the proportion of π-elements in Ky which commute with x is at most $\frac{1}{p+1}$. Therefore, we may assume that $y \in K$ and hence, if we set

$$D = \{z \in K \mid \langle z\rangle \text{ is } G\text{-conjugate to } \langle y\rangle\},$$

then Lemma 6.16 gives $|D| \geqslant p^2 - 1$. Since $D \subseteq K_\pi$, we have that $|K_\pi| \geqslant p^2$. Now, expressing K_π as union of K-conjugacy classes and reasoning as in the proof of Proposition 6.11, we deduce that the proportion of π-elements in K commuting with x is at most $1/p$.

Suppose now that we are in case b). It follows that y must act transitively on the set of components of K. If K has at least components, then we can reduce the problem to the previous case (exchanging x and y). Thus, we may assume that K is quasisimple. By Propositions 6.17 and 6.18, the result holds unless $K/\mathbf{Z}(K) = \mathsf{A}_n$ and that x acts as a transposition. Thus, if we set $L = \langle K, x\rangle$, then, by Proposition 6.19, we deduce that the proportion of π-elements in the coset Ly commuting with x is at most $1/2$. Thus, the same holds for the coset Ky and the result follows. □

6.4. Results on $\mathrm{Pr}_\pi(G)$

In this section, we use Theorem I to prove Theorem J. If G possesses a normal and abelian Hall π-subgroup, then every pair of π-elements of G commute and hence $\mathrm{Pr}_\pi(G) = 1 > \frac{p^2+p-1}{p^3}$. Thus, we will only prove the converse assertion of Theorem J. We recall one elementary result that we will need.

Lemma 6.21. *Let G be a group and let π be a set of primes such that G does not possess a normal Hall π-subgroup. Then $|G_\pi| \geqslant p^2$, where p is the smallest prime in π.*

Proof. Since G does not possess a normal Hall π-subgroup, there exists $q \in \pi$ such that G does not possess a normal Sylow q-subgroup.

Let Q be a Sylow q-subgroup of G. If $|Q| \geqslant q^2$, then $|G_\pi| \geqslant |Q| \geqslant q^2 \geqslant p^2$ and the result follows. Assume now that $|Q| = q$. Then all Sylow q-subgroups intersect trivially and, by Sylow Theorems, we have that G possesses at least $q+1$ Sylow q-subgroups. Thus, $|G_\pi| \geqslant |G_q| \geqslant q^2 \geqslant p^2$ and the result follows. □

Now, we proceed to restate and prove Theorem J.

THEOREM 6.22. *Let G be a group, let π be a set of primes and let p be the smallest prime in π. If $\mathrm{Pr}_\pi(G) > \frac{p^2+p-1}{p^3}$, then G has a normal and abelian Hall π-subgroup.*

PROOF. First, we prove that G has a normal Hall π-subgroup by induction on $|G|$.

Suppose first that $\mathbf{O}_\pi(G) > 1$. By Lemma 6.4, $\mathrm{Pr}_\pi(G/\mathbf{O}_\pi(G)) \geqslant \mathrm{Pr}_\pi(G)$, and $|G/\mathbf{O}_\pi(G)| < |G|$. Thus, by induction, $G/\mathbf{O}_\pi(G)$ has a normal Hall π-subgroup and hence G has a normal Hall π-subgroup.

Thus, we may assume that $\mathbf{O}_\pi(G) = 1$. Then,

$$|\{(x,y) \in G_\pi \times G_\pi \mid xy = yx\}| = |\{(x,y) \in G \times G \mid x \in G_\pi, y \in \mathbf{C}_G(x)_\pi\}| = \\ = |G_\pi| + \sum_{x \in G_\pi \setminus \{1\}} |\mathbf{C}_G(x)_\pi|.$$

For every $x \in G_\pi \setminus \{1\}$ we have that $x \notin \mathbf{O}_\pi(G)$, so Theorem I gives

$$\frac{|\mathbf{C}_G(x)_\pi|}{|G_\pi|} \leqslant \frac{1}{p},$$

and hence

$$\mathrm{Pr}_\pi(G) = \frac{1}{|G_\pi|}\Big(1 + \sum_{x \in G_\pi \setminus \{1\}} \frac{|\mathbf{C}_G(x)_\pi|}{|G_\pi|}\Big) \leqslant \frac{1}{|G_\pi|}\Big(1 + \frac{|G_\pi| - 1}{p}\Big).$$

So, if we consider the function

$$f_p(x) = \frac{1}{x}\Big(1 + (x-1)\frac{1}{p}\Big) = \frac{1}{x}\Big(1 - \frac{1}{p}\Big) + \frac{1}{p},$$

then we have that $\mathrm{Pr}_\pi(G) \leqslant f_p(|G_\pi|)$. We observe that $f_p(x)$ is a decreasing function in x.

Suppose G does not have a normal Hall π-subgroup. By Lemma 6.21, we have that $|G_\pi| \geqslant p^2$ and hence

$$\mathrm{Pr}_\pi(G) \leqslant f_p(|G_\pi|) \leqslant f_p(p^2) = \frac{1}{p^2}\Big(1 - \frac{1}{p}\Big) + \frac{1}{p} = \frac{p^2+p-1}{p^3},$$

which is a contradiction.

Thus, G possesses a normal Hall π-subgroup, or equivalently, $\mathbf{O}_\pi(G)$ is a Hall π-subgroup of G and $\mathbf{O}_\pi(G) = G_\pi$. Then

$$\Pr(\mathbf{O}_\pi(G)) = \frac{|\{(x,y) \in G_\pi \times G_\pi \mid xy = yx\}|}{|G_\pi|^2} = \Pr_\pi(G) > \frac{p^2+p-1}{p^3}$$

and thus $\mathbf{O}_\pi(G)$ is abelian by Proposition 4.9. □

6.5. Open problems

We conclude by briefly discussing some open problems concerning the invariant $\Pr_\pi(G)$.

As we mentioned in the introduction of this chapter, it remains an open problem to determine whether or not p in the upper bound presented in Theorem I can be replaced by q, where q is the largest prime dividing $o(x)$.

Conjecture 6.23. *Let G be a group and let π be a set of primes. If $x \in G_\pi \backslash \mathbf{O}_\pi(G)$, then*

$$\frac{|\mathbf{C}_G(x)_\pi|}{|G_\pi|} \leqslant \frac{1}{q},$$

where q is the largest prime dividing $o(x)$.

It is not hard to see that Conjecture 6.23 cannot be proved by arguing as in the proof of Theorem I. And although the above conjecture is not relevant for obtaining results on $\Pr_\pi(G)$, we think it is a problem of independent interest.

We recall that the Itô–Michler Theorem [**57, 85**] asserts that a group G has a normal and abelian Sylow p-subgroup if and p does not divide the degree of any irreducible character of G. On the other hand, [**16**, Theorem A] provides a character-free condition for the existence of a normal and abelian Sylow p-subgroup.

The Brauer's Height Zero Conjecture [**11**] was proved for the principal block in [**71**]. The solution of this case of the conjecture provides a character-theoretical criterion for deciding the existence of abelian Sylow p-subgroups. On the other hand, [**35**, Theorem A] provides a character-theoretical criterion for the existence of a normal Sylow p-subgroup.

Thus, it is natural to ask whether we can use $\Pr_p(G)$ to obtain independent information on the normality and the commutativity of Sylow p-subgroups.

As we pointed out in the introduction of this chapter, for every prime p, there exists a group G such that $\Pr_p(G) = \frac{p^2+p-1}{p^3}$ and G does not possess a normal Sylow p-subgroup. Thus, we do not expect to obtain (much) information on the normality of a Sylow since for $p \geqslant 5$, the group $\mathrm{PSL}(2,p)$ is a simple and

$\Pr_p(G) = \frac{p^2+p-1}{p^3}$ (see [**16**, Theorem B]). However, we expect to obtain information on the commutativity of Sylow p-subgroups. In this direction, we expect the following conjecture to be true.

CONJECTURE 6.24 (Moretó). *Let G be a group, let p be a prime and let $P \in \mathrm{Syl}_p(G)$. Then*

$$\Pr_p(G) \leqslant \Pr(P).$$

Conjecture 6.24, if true, would allow us to apply the bounds in Proposition 4.14 or Theorems D and E to $\Pr_p(G)$ in order to restrict the structure of a Sylow p-subgroup.

We also think that the commuting probability of a Sylow p-subgroup could control the probability that p-elements in different Sylow p-subgroups commute. More precisely, we propose following conjecture.

CONJECTURE 6.25. *Let G be a group, let p be a prime and let $P, Q \in \mathrm{Syl}_p(G)$. Then*

$$\frac{|\{(x,y) \in P \times Q \mid xy = yx\}|}{|P|^2} \leqslant \Pr(P).$$

We suspect that Conjectures 6.24 and 6.25 are related to each other. However, we have find no connection among them yet.

Appendix A: Graphs, coverings and characters

A.1. Coverings and graph theory

In this section, we discuss the connection between the commuting probability, the coverings of groups and the study of graphs defined on groups.

Definition. Let π be a set of primes and let G be a group. We define the **non-commuting π-graph** of G as the graph whose vertices are labelled by the π-elements in G and two π-elements are joined if they do not commute. We will write $\Gamma_\pi(G)$ to denote it.

If $\pi = \pi(G)$, we will just write $\Gamma(G)$. The graph Γ is known as the non-commuting graph of G.

Our definition of non-commuting (π-)graph is not completely standard. In many papers, it is defined over the set of non-central (π-)elements. This difference is made to avoid the existence of isolated points in the graph.

The non-commuting π-graph is closely related with the π-commuting probability. It is easy to see that the proportion (or density) of vertices in $\Gamma_\pi(G)$ coincides with $1 - \Pr_\pi(G)$. We recall that the clique number of a graph is the size of its largest complete subgraph. We will write $n_\pi(G)$ to denote the clique number of $\Gamma_\pi(G)$. By definition, $n_\pi(G)$ is the size of the largest subset of pairwise non-commuting π-elements in G. Sets of pairwise non-commuting elements are usually called **independent sets** (see, for example, Section 1 of [**104**]). We will write $n(G)$ when $\pi = \pi(G)$.

Our aim is to relate $n_\pi(G)$ with $\Pr_\pi(G)$. To do so, we introduce a classical result of Turán [**125**].

Lemma A.1 (Turán). *Let Γ be an undirected graph with n vertices, which does not contain a clique of size $r+1$-vertex clique. Then the number of edges in Γ is at most*

$$(1 - \frac{1}{r})\frac{n^2}{2}.$$

Proposition A.2. *Let G be a group and π be a set of primes. Then*

$$n_\pi(G) \geqslant \frac{1}{\Pr_\pi(G)}.$$

PROOF. On the one hand, we have that the number of edges of $\Gamma_\pi(G)$ is given by

$$\frac{|\{(x,y) \in G_\pi \times G_\pi \mid xy \neq yx\}|}{2} = (1 - \Pr_\pi(G))\frac{|G_\pi|^2}{2}.$$

On the other hand, the largest clique in $\Gamma_\pi(G)$ has size $n_\pi(G)$. Thus, by Turán's Theorem we deduce that

$$(1 - \Pr_\pi(G))\frac{|G_\pi|^2}{2} \leqslant (1 - \frac{1}{n_\pi(G)})\frac{|G_\pi|^2}{2}$$

and thus $n_\pi(G) \geqslant \frac{1}{\Pr_\pi(G)}$. □

The first consequence of Proposition A.11 is that we can improve a classical result of L. Pyber. Pyber [**104**, p. 294] proved that if S is a non-abelian finite simple group, then $|S| \leqslant (3n(S))^3$.

PROPOSITION A.3. *Let G be a group. Then the following hold:*

(i) $|G| \leqslant n(G)^2 \cdot k(\mathbf{F}(G))$.

(ii) $|G : \mathbf{F}(G)| \leqslant n(G)^2 \cdot \Pr(\mathbf{F}(G)) \leqslant n(G)^2$.

(iii) $n(G) \geqslant \operatorname{acd}(G)^2$.

(iv) If G is solvable of derived length $d \geqslant 4$, then $n(G) \geqslant \frac{2^{d+1}}{4d-7}$.

(v) If S is a non-abelian simple group, then $|S| \leqslant n(S)^c$, where $c = 1/0.59 \approx 1.6949$.

PROOF. Let G be a group. Proposition A.2 gives

$$n(G) \geqslant \frac{1}{\Pr(G)} = \frac{|G|}{k(G)}.$$

To prove (i) it suffices to apply the bound $k(G) \leqslant |G|^{1/2}k(\mathbf{F}(G))^{1/2}$ due to Guralnick and Robinson [**41**, Theorem 10]. Part (ii) follows dividing (i) by $|\mathbf{F}(G)|$. Now, (iii) follows from the following inequality (see Section 4.1)

$$\frac{1}{\Pr(G)} \geqslant (\frac{\sum_{\chi \in \operatorname{Irr}(G)} \chi(1)}{|\operatorname{Irr}(G)|})^2.$$

Part (iv) follows from the bound given by part a) of [**41**, Theorem 12] and arguing as in (i). By the results in [**31**], we have that $k(S) \leqslant |S|^{0.41}$. Thus, we deduce that $|S|^{0.59} \leqslant n(S)$ and (v) follows. □

We recall the following conjecture, which was stated at the end of [**16**].

CONJECTURE A.4. *Let p be a prime and let G be a group generated by p-elements with $\mathbf{O}_p(G) = 1$. Then $\Pr_p(G)$ tends to 0 as $|G|$ tends to infinity.*

PROPOSITION A.5. *Let p be a prime and assume that Conjecture A.4 holds for p. Then $|G|$ is bounded in terms of $n_p(G)$.*

PROOF. By Proposition A.2, we have that

$$n_p(G) \geqslant \frac{1}{\mathrm{Pr}_p(G)}$$

and by hypothesis $\frac{1}{\mathrm{Pr}_p(G)}$ tends to infinity as $|G|$ increases. Thus, $n_p(G)$ also tends to infinity as $|G|$ increases, and hence $|G|$ is bounded in terms of $n_p(G)$. □

Let $m, n \geqslant 1$ be two integers and let π be a set of primes. Following [**40**], we will say that $G \in C_\pi(m,n)$ if for any two subsets $S_1, S_2 \subseteq G_\pi$ with $|S_1| = m$, $|S_2| = n$, there exist $x \in S_1, y \in S_2$ such that $xy = yx$. The next result is a local version of [**1**, Theorem 1.1].

THEOREM A.6 (Theorem H of [**40**]). *There exists a real-valued function $g(m,n)$ such that if π is a set of primes, $G \in C_\pi(m,n)$ and $|G|_\pi > g(m,n)$, then G possesses abelian Hall π-subgroups.*

The proof of Theorem A.6 reduces to proving the following result.

PROPOSITION A.7. *For each prime p, we have $n_p(S)$ tends to infinity as $|S|$ increases, where S runs through all non-abelian simple groups with p dividing $|S|$.*

By Proposition A.5, we see that Proposition A.7 holds if Conjecture A.4 holds. However, in [**40**] we provided a direct proof of Proposition A.7, which does not depend on Conjecture A.4. We will briefly sketch the proof of Proposition A.7. To do this, we need to introduce some new notation and terminology.

DEFINITION. Let G be a group. If G is non-cyclic group, then we define the **covering number** of G as the smallest integer k such that there exists $H_1, \ldots, H_k < G$ with

$$G = H_1 \cup \ldots \cup H_k.$$

If G is cyclic, then we define the covering number of G as $+\infty$. We will write $\sigma(G)$ to denote the covering number of G.

There are many results on $\sigma(G)$. For example, an elementary result of Scorza [**114**] asserts that $\sigma(G) > 2$ for any group G. Moreover, applying Cayley's Theorem, it is easy to prove that $\sigma(S) \to \infty$ when S is simple and $|S| \to \infty$.

Using Scorza's Theorem, we have that $G \neq \mathbf{C}_G(x_1) \cup \mathbf{C}_G(x_2)$ for all $x_1, x_2 \in G \backslash \mathbf{Z}(G)$. Thus, there exists $y \in G \backslash (\mathbf{C}_G(x_1) \cup \mathbf{C}_G(x_2))$. It follows that the induced subgraph by the non-commuting graph of G on $G \backslash \mathbf{Z}(G)$ has diameter at most 2.

Inspired by $\sigma(G)$, the p-covering number of G was defined in [78] as follows.

DEFINITION. Let G be a group and let p be a prime. If G is not a cyclic p-group, then we define the p-covering number of G as the smallest integer k such that there exists $H_1, \ldots, H_k < G$ with

$$G_p \subseteq H_1 \cup \ldots \cup H_k.$$

If G is a cyclic p-group, then we define the p-covering number of G as $+\infty$. We will write $\sigma_p(G)$ to denote the p-covering number of G.

Let G be a group. Write $k = n_p(G)$ and let $\{x_1, \ldots, x_k\} \subseteq G_p$ be a pairwise non-commuting subset of G_p of maximal size. Then

$$G_p \subseteq \bigcup_{i=1}^{k} \mathbf{C}_G(x_i)$$

and hence $\sigma_p(G) \leqslant n_p(G)$.

Combining [40, Theorem G] with the inequality $\sigma_p(G) \leqslant n_p(G)$, we deduce that Proposition A.7 holds. Thus, Theorem A.6 holds by the comments after its statement.

Finally, we close this section by discussing the connectivity and the diameter of non-commuting p-graph. By [40, Theorem F], we have that $\sigma_p(G) \geqslant p + 1$ for any group G generated by its p-elements. We remark that this result does not depend on *CFSG*. Using it, we have the following.

PROPOSITION A.8. *Let p be a prime and let G be a group generated by its p-elements. Let $x_1, \ldots, x_p \in G \backslash \mathbf{Z}(G)$. Then there exists $y \in G_p$ such that y is joined to $x_1, \ldots, x_p$ in the non-commuting p-graph. In particular, the induced subgraph by the non-commuting graph of G on $G_p \backslash \mathbf{Z}(G)$ has diameter at most 2.*

PROOF. Since each x_i is non-central, we have that each $\mathbf{C}_G(x_i)$ is a proper subgroup in G. Thus, there exists $y \in G_p \backslash (\mathbf{C}_G(x_1) \cup \cdots \cup \mathbf{C}_G(x_p))$ by [40, Theorem F]. The result follows. □

We also present an alternative version, which is valid also for groups that are not generated by its p-elements. The following theorem is a consequence of [15, Theorems C and D].

THEOREM A.9. *Let p be a prime and let G be a group generated by its p-elements. If $x_1, \ldots, x_p \in G_p \backslash \mathbf{Z}(\mathbf{O}_p(G))$, then $G_p \nsubseteq \mathbf{C}_G(x_1) \cup \cdots \cup \mathbf{C}_G(x_p)$.*

PROOF. By [15, Theorems C and D], we have that

$$|\mathbf{C}_G(x_i)_p| \leqslant \frac{|G_\pi|}{p}$$

for any $1 \leqslant i \leqslant p$. Therefore,

$$|\mathbf{C}_G(x_1)_p \cup \cdots \cup \mathbf{C}_G(x_p)_p| \leqslant \sum_{i=1}^{p} |\mathbf{C}_G(x_i)_p| < |G_p|$$

and the result follows. □

As a consequence, we obtain the following result.

COROLLARY A.10. *Let G be a group generated by its p-elements and let Δ be the induced subgraph of non-commuting graph of G on $G_p \backslash \mathbf{Z}(\mathbf{O}_p(G))$. Then for any $x_1, \ldots, x_p \in G_p \backslash \mathbf{Z}(\mathbf{O}_p(G))$ there exists $y \in G_p \backslash \mathbf{Z}(\mathbf{O}_p(G))$ such that y is joined to x_i for every i. In particular, Δ is connected with diameter at most 2.*

PROOF. There exists $y \in G_p \backslash (\mathbf{C}_G(x_1) \cup \cdots \cup \mathbf{C}_G(x_p))$ by Theorem A.9. The result follows. □

A.2. Redundant Sylows and picky elements

In the previous section, we considered the coverings of G_p by proper subgroups. However, there is another version of the problem that seems very natural: covering G_p by Sylow p-subgroups. Since every p-element $x \in G$ belongs to some Sylow p-subgroup, it follows that G_p is the union of all the Sylow p-subgroups of G. This motivates the following question.

Do we need all the Sylow p-subgroups of G to cover G_p?

Although this question does not have an affirmative answer in general, the work in [77] indicates that the answer is yes more often than one could perhaps expect. This leads to the following definition, introduced in [77].

DEFINITION. Let G be a group and let p be a prime. We say that G has (or possesses) a **redundant** Sylow p-subgroup if G_p has a cover which is a proper subset of $\mathrm{Syl}_p(G)$.

Calculations in GAP [33] suggest that perhaps surprisingly, groups with a redundant Sylow p-subgroup are rare. Among the groups of order at most 2000 in the `SmallGroup` database in GAP [33], there are only examples of groups with a redundant Sylow p-subgroup when $p = 2$. The smallest of them have order 108, namely `SmallGroup`(108,17) and `SmallGroup`(108,40). Moreover, A_9 has a redundant Sylow 2-subgroup. This is the smallest example of symmetric or alternating group with a redundant Sylow p-subgroup that we found. Finally,

we also discovered that $\mathrm{PSL}(3,7)$ is an example of group with a redundat Sylow 3-subgroup.

These examples lead to a number of interesting questions, such as: Are there groups with a redundant Sylow p-subgroup for any odd prime? Which groups have a redundant Sylow p-subgroup? Which p-groups can appear as Sylow subgroups of groups having a redundant Sylow p-subgroup?

The following fundamental result allows us to interpret the concept of redundant Sylow p-subgroups in a convenient way.

LEMMA A.11. *Let G be a finite group and let p be a prime. Then G does not have a redundant Sylow p-subgroup if and only if there exists $x \in G_p$ such that x belongs to a unique Sylow p-subgroup.*

PROOF. Let $\mathrm{Syl}_p(G) = \{P_1, P_2, \ldots, P_n\}$ with $n = |\mathrm{Syl}_p(G)|$. The result is clear for $n = 1$. Assume that $n > 1$. The group G has a redundant Sylow p-subgroup if and only if $G_p = \bigcup_{i \neq j} P_i$ for some j. This happens if and only if $P_j \subseteq \bigcup_{i \neq j} P_i$, which is equivalent to saying that every element of P_j lies in more than one Sylow p-subgroup. □

This result motivates the following definition introduced by Moretó and Rizo [**93**].

DEFINITION. Let G be a group and let p be a prime. We say that $x \in G_p$ is a **picky** element if there exists a unique Sylow p-subgroup of G containing x.

We observe that if G possesses cyclic Sylow p-subgroups and $x \in G_p$ generates a Sylow p-subgroup, then x is a picky element. Thus, groups with cyclic Sylow subgroups do not possesses a redundant Sylow subgroup, by Lemma A.11. On the other hand, if G has TI-Sylow p-subgroups (that is, $P \cap Q = 1$ for any two different Sylow p-subgroups P and Q), then every non-trivial p-element is picky and hence, G does not possess a redundant Sylow p-subgroup. A classification of the finite simple groups possessing TI-Sylow p-subgroups can be found in [**10**, Proposition 1.3].

It is worth noting that there exist several papers dealing with picky elements. For instance, Thompson (see [**45**, Conjecture B]) stated a conjecture involving p-subgroups which are contained in a unique Sylow p-subgroup.

CONJECTURE A.12 (Thompson). *For each prime p there exists a non-decreasing function $f_p : \mathbb{N} \to \mathbb{N}$ satisfying the following property. If G is a p-solvable group and there exists a p-subgroup H of G lying in a unique Sylow p-subgroup of G, then the p-length of G is at most $f_p(|H|)$.*

Rae [106] proved that Thompson's Conjecture holds under the assumption that H is cyclic. In this case, H is generated by a picky element. More precisely, the following result is [106, Theorem B].

THEOREM A.13 (Rae). *Let G be a p-solvable group and assume that $x \in G$ is a picky element of order p^k. Then the p-length of G is at most $2k$.*

In addition, Herzog [47] studied the involutions of simple groups lying in a unique Sylow 2-subgroup. Picky elements in simple groups also arise in the main results of the papers [49, 50] by Ho and Völklein.

The paper [77] is devoted to studying the existence of picky elements in some families of groups. The first main result of that paper is [77, Theorem A]. This result asserts that, given p a prime and P a non-cyclic finite p-group of exponent p, then there exists a solvable group G such that $P \in \mathrm{Syl}_p(G)$ and G has a redundant Sylow p-subgroup. This result was improved by B. Sambale [113, Theorem 1] by removing the condition $\exp(P) = p$. Moreover, the proof of [113, Theorem 1] is constructive, in contrast to the proof of [77, Theorem A]. More precisely, Sambale proved the following.

THEOREM A.14 (Sambale). *Let p be a prime and let P be a non-cyclic p-group. For every prime $q \neq p$ there exists a q-elementary abelian group N such that P acts on N and $G := N \rtimes P$ has the following properties:*

(i) G has a redundant Sylow p-subgroup.

(ii) G_p can be covered by $\frac{1}{q^{p-1}}|\mathrm{Syl}_p(G)|$ Sylow p-subgroups of G.

We notice that property (ii) in Theorem A.14 shows that if we can cover G_p by $|\mathrm{Syl}_p(G)| - 1$ different Sylow p-subgroups, then G_p can be covered by using few Sylow p-subgroups. This provides a negative answer to [77, Question 8.7].

Examples of non-solvable groups with redundant Sylow p-subgroups are given in [77, Theorem E]. More precisely, we have the following result.

THEOREM A.15. *Let p be an odd prime and let q be a prime such that p divides $q-1$, but p^2 does not divide $q-1$. Then $\mathrm{GL}(p,q)$ has a redundant Sylow p-subgroup.*

For symmetric groups, it is possible to determine the picky elements. Let $n = \sum_{k=0}^{f} a_k p^k$ be the p-adic expansion of n. We say that $x \in \mathsf{S}_n$ is a **p-adic element** if the expression of x as product of disjoint cycles has a_k cycles of length p^k for every $k \geqslant 0$. We remark that the p-adic elements of S_n appeared in [35] (see [35, Theorem 3.16]). In addition, given $x \in \mathsf{S}_n$, we write $\mathrm{fix}(x)$ to denote the number of fixed points of x in the natural action of S_n on $\{1, \ldots, n\}$. The following result follows from the results in Section 4 of [77].

PROPOSITION A.16. *Let p be a prime and let $n \geqslant 1$ be an integer. Then $x \in \mathsf{S}_n$ is a picky p-element if and only one of the following holds:*

Type I: x is a p-adic element of S_n.

Type II: $p = 2$, $n \geqslant 6$ is even, $\mathrm{fix}(x) = 2$ and x is a 2-adic element of S_{n-2}.

Moreover, it was proved in [77], that if $n \geqslant 6$ and $x \in \mathsf{A}_n$ is a p-element, then x is picky in A_n if and only if x is picky in S_n. Thus, the following result follows from Proposition A.16.

COROLLARY A.17. *Let p be a prime and let G be A_n or S_n with $n \geqslant \max\{6, p\}$. Then G has a redundant Sylow p-subgroup if and only if $p = 2$ and $G = \mathsf{A}_n$ with $n = \sum_{i=r}^{k} a_i 2^i$, where $a_r, a_{r+1}, \ldots, a_k \in \{0, 1\}$, $a_r = a_k = 1$ and the following conditions are satisfied:*

- $\sum_{i=1}^{k} a_i \equiv 1 \pmod 2$ *if n is odd.*
- *$r \geqslant 2$ is even and $\sum_{i=r}^{k} a_i \equiv 1 \pmod 2$ if n is even.*

Corollary A.17 implies that A_9 and A_{16} are the first alternating groups possessing a redundant Sylow 2-subgroup.

Now, we consider groups of Lie type. We first consider the case when p is the characteristic of the group. Let G be a group of Lie type in characteristic p. Then every p-element is unipotent. During the preparation of [77], T. Weigel pointed out to us that if $x \in G_p$ is a regular unipotent element, then x belongs to a unique Borel subgroup (see Chapter V of [19]). It follows that x is a picky element of G. Moreover, groups of Lie type always possess regular unipotent elements. The following result of Malle is [70, Theorem 3.2] and it asserts that, for a quasisimple group of Lie type in characteristic p, "almost all" picky p-elements are regular unipotent.

THEOREM A.18 (Malle). *Let G be a quasi-simple group of Lie type over a field of $q = p^r$ elements. A unipotent element $x \in G$ is picky if and only if one of the following holds:*

(i) x is regular unipotent.

(ii) $G = \mathrm{SU}(2n + 1, q)$ with $n \geqslant 1$ and x has Jordan block sizes $(2n, 1)$.

(iii) $G = {}^2B_2(2^{2f+1})$ with $f \geqslant 1$.

(iv) $G = {}^2G_2(2^{2f+1})$ with $f \geqslant 1$.

(v) $G = {}^2F_4(2^{2f+1})$ with $f \geqslant 1$ and $|\mathbf{C}_G(x)| = 2q^6$ for $q^2 = 2^{2f+1}$.

Malle [70] is working towards a classification of the picky elements of groups of Lie type in non-defining characteristic.

The existence of redundant Sylow subgroups in sporadic groups was studied in Section 7 of [77]. For example, the Monster group possesses a redundant Sylow 7-subgroup. However, this study was not exhaustive, and there were sporadic groups for which it was not known whether they have a redundant Sylow p-subgroup. Recently, in e-mail correspondence with Moretó and Rizo, Breuer [13] determined all picky elements of sporadic simple groups.

A.3. Subnormalizers

Carter [18] defined the subnormalizer of $H \leqslant G$ as the largest subgroup of G that contains H as a subnormal subgroup, if it exists (see Section 1.3 for a definition of subnormal subgroup). Unfortunately, such a group does not always exists. For this reason, Lennox and Stonehewer [64] introduced the following set

$$S_G(H) = \{g \in G \mid H \trianglelefteq\trianglelefteq \langle H, g\rangle\}.$$

We will refer to this set as the **subnormalizer subset**. It follows from a theorem of Wielandt that $S_G(H)$ is a subgroup if and only if the subnormalizer of H exists, in the sense of Carter (and in this case, they coincide). In this case, they coincide.

More recently, Moretó and Rizo [93] defined the following set

$$\mathbf{Sub}_G(H) = \langle S_G(H)\rangle.$$

Following [93], we will refer to this set as the subnormalizer subset. It follows from a theorem of Wielandt that $\mathbf{Sub}_G(H)$ is a subgroup if and only if the subnormalizer in the sense of Carter exists. In this case, they coincide. Moreover, Moretó and Rizo defined the **subnormalizer subgroup of** H as

$$\mathbf{Sub}_G(H) = \langle S_G(H)\rangle.$$

For $x \in G$, we will write $S_G(x) := S_G(\langle x\rangle)$ and $\mathbf{Sub}_G(x) := \mathbf{Sub}_G(\langle x\rangle)$

Calculating $\mathbf{Sub}_G(x)$ for a general element can be very hard. However, the situation becomes easier when x is a p-element for a prime p. In a series of papers, Casolo [20, 21, 22] studied the properties of $S_G(H)$ for $H \leqslant G$ a p-subgroup. One of the most important theorem of these papers is the main result of [21], which is stated as follows.

THEOREM A.19 (Casolo). *Let p be a prime and let $H \leqslant G$ be a p-subgroup. If $P \in \mathrm{Syl}_p(G)$ contains H, then*

$$|S_G(H)| = \lambda_G(H)|\mathbf{N}_G(P)|,$$

where $\lambda_G(H)$ denotes the number of Sylow p-subgroups containing H.

We would like to remark that the proof of Theorem A.19 involves the use of simplicial complexes. The definition of the simplicial complex is not related to finite group theory, but it has been used before in character theory (see, for

example [**60**]). Theorem A.19 allows us to understand the picky elements by using the subnormalizers.

COROLLARY A.20. *Let p be a prime and let G be a group. Assume that $P \in \mathrm{Syl}_p(G)$ and $x \in P$. Then x is picky if and only if $\mathbf{Sub}_G(x) = S_G(x) = \mathbf{N}_G(P)$.*

PROOF. We have that x is picky if and only if $\lambda_G(\langle x \rangle) = 1$. By Theorem A.19, this happens if and only if $|S_G(x)| = |\mathbf{N}_G(P)|$. Since $\mathbf{N}_G(P) \subseteq S_G(x)$, the result follows. □

We remark that Moretó and Rizo [**93**] have a more elementary proof of Corollary A.20, which does not require Theorem A.19 (see also [**70**, Corollary 2.7]).

It is easy to see that, if $x \in P$ for $P \in \mathrm{Syl}_p(G)$, then $\mathbf{N}_G(P) \subseteq \mathbf{Sub}_G(x)$. Moreover, the following result of Malle (see [**70**, Proposition 2.6]) shows that much more is true. This result provides a tool for computing the subnormalizers of p-elements.

PROPOSITION A.21 (Malle). *Let p be a prime and let G be a group. Given $x \in G_p$, we have*

$$\mathbf{Sub}_G(x) = \langle \mathbf{N}_G(P) \mid P \in \mathrm{Syl}_p(G), x \in P \rangle.$$

If $x \in G$ is a p-element, then $\mathbf{Sub}_G(x) = G$ relatively often. One of the very challenging open problems concerning subnormalizers is to find conditions to ensure that $\mathbf{Sub}_G(x) < G$. Proposition A.21 suggests that $|\mathbf{Sub}_G(x)|$ tends to be larger when x lies in more subgroups. Using Proposition $\mathbf{Sub}_G(x)$, Malle [**70**] is working towards a classification of the p-elements of groups of Lie type with proper subnormalizers.

The study of the subnormalizers of the p-elements of the symmetric group is being developed in [**83**]. We expect to complete the classification of the 2-elements of S_n with proper subnormalizers in the next months. For $p > 2$, the study of the subnormalizers of the p-elements of S_n seems to be more involved. For example, we have the following result.

LEMMA A.22. *Let $k \geqslant 3$ be an integer and let $x \in \mathsf{S}_{2^k}$ be a 2-element. Then $\mathbf{Sub}_{\mathsf{S}_{2^k}}(x) < \mathsf{S}_{2^k}$ if and only if one of the following holds:*

(i) x is a 2^k-cycle.

(ii) $o(x) = 2^{k-1}$ and $\mathrm{fix}(x) > 0$.

Moreover, in case (ii), $\mathbf{Sub}_{\mathsf{S}_{2^k}}(x) = \mathbf{Sub}_{\mathsf{S}_{2^{k-1}}}(y) \wr \mathsf{S}_2$, where y is the product of all cycles of length smaller than 2^{k-1} in the expression of x as a product of disjoint cycles.

A.4. Picky and Subnormalizer Conjectures

In this section we present several conjectures concerning picky elements and the subnormalizers of p-elements. It is important to remark that many of the results of this section are being developed at the moment of writing this thesis. Thus, we are unable to state definitive results at the current stage.

As we saw in Section A.2, the picky elements have appeared several times in group-theoretical contexts. However, during the preparation of [77], Moretó realized that the picky elements have good properties from the point of view of character theory. For example, next result is [77, Corollary 2.4].

THEOREM A.23. *Let G be a group without a redundant Sylow p-subgroup. Then there exists $x \in G_p$ such that $\chi(x) = 0$ for every $\chi \in \mathrm{Irr}(G)$ that does not belong to a p-block of full defect.*

This motivated Moretó and Rizo to consider local-global problems involving picky elements and zeros of characters. Given a group G and a prime p, we write

$$\mathrm{Irr}_{p'}(G) = \{\chi \in \mathrm{Irr}(G) \mid \gcd(p, \chi(1)) = 1\}.$$

One of the most famous local-global conjectures is McKay Conjecture. After many efforts, this conjecture was finally proved in [17]. We remark that the case $p = 2$ had been previously proved by Malle and Späth [74].

THEOREM A.24 (McKay Conjecture). *Let G be a group, let p be a prime and let $P \in \mathrm{Syl}_p(G)$. Then*

$$|\mathrm{Irr}_{p'}(G)| = |\mathrm{Irr}_{p'}(\mathbf{N}_G(P))|.$$

Given $x \in G$, we write

$$\mathrm{Irr}^x(G) = \{\chi \in \mathrm{Irr}(G) \mid \chi(x) \neq 0\}.$$

Analogously, if $\mathcal{P} \subseteq G$, we write

$$\mathrm{Irr}^{\mathcal{P}}(G) = \{\chi \in \mathrm{Irr}(G) \mid \chi(x) \neq 0 \text{ for some } x \in \mathcal{P}\}.$$

For the remainder, given a prime p and a group G, we will write

$$\mathcal{P} = \{x \in P \mid x \text{ is picky in } G\},$$

where $P \in \mathrm{Syl}_p(G)$. Moretó and Rizo [93] have put forward the following conjecture.

CONJECTURE A.25 (Global Picky Conjecture). *Let p be a prime, let G be a group and let $P \in \mathrm{Syl}_p(G)$. Then there exists a bijection*

$$\Gamma : \mathrm{Irr}^{\mathcal{P}}(G) \to \mathrm{Irr}^{\mathcal{P}}(\mathbf{N}_G(P))$$

satisfying the following properties:

(I) $\Gamma(\chi)(1)_p = \chi(1)_p$ for every $\chi \in \mathrm{Irr}^{\mathcal{P}}(G)$.

(II) $\mathbb{Q}(\Gamma(\chi)(x)) = \mathbb{Q}(\chi(x))$ for every $\chi \in \mathrm{Irr}^{\mathcal{P}}(G)$ and every $x \in \mathcal{P}$.

(III) $\Gamma(\mathrm{Irr}^x(G)) = \mathrm{Irr}^x(\mathbf{N}_G(P))$ for every $x \in \mathcal{P}$.

They observed that $\Gamma(\chi)(x)_p = \chi(x)_p$ when $\chi(x)$ is rational. Malle [**70**] suggested that $\chi(x)_p$ makes sense even when $\chi(x)$ is not rational and after checking examples in groups of Lie type asked whether this could hold in general. This is also expected to hold for all other variations of the Global Picky Conjecture that we will present in this section. We will not mention it explicitly when presenting them.

Moretó and Rizo [**93**] have also observed that it is very often the case (but not always) that there exists a bijection satisfying $\Gamma(\chi)(x) = \pm\chi(x)$ for every $\chi \in \mathrm{Irr}^{\mathcal{P}}(G)$ and every $x \in \mathcal{P}$. In such a case, we will say that G satisfies the **Strong Global Picky Conjecture**. There exists a weaker version of the Global Picky Conjecture.

Conjecture A.26 (Picky Conjecture). *Let p be a prime, let G be a group and let $P \in \mathrm{Syl}_p(G)$. If $x \in P$ is a picky element, then there exists a bijection*

$$\Gamma : \mathrm{Irr}^x(G) \to \mathrm{Irr}^x(\mathbf{N}_G(P))$$

satisfying the following properties:

(I) $\Gamma(\chi)(1)_p = \chi(1)_p$ for every $\chi \in \mathrm{Irr}^x(G)$.

(II) $\mathbb{Q}(\Gamma(\chi)(x)) = \mathbb{Q}(\chi(x))$ for every $\chi \in \mathrm{Irr}^x(G)$.

We observe that if $\chi \in \mathrm{Irr}_{p'}(G)$ and $x \in G_p$, then $\chi(x) \neq 0$ by [**99**, Corollary 4.20]. Therefore, $\mathrm{Irr}_{p'}(G) \subseteq \mathrm{Irr}^x(G)$. Thus, if $x \in G$ is a picky p-element and the Picky Conjecture holds for (G, x), then the McKay Conjecture holds for G.

Given a picky p-element $x \in G$, we say that the **Strong Picky Conjecture** holds for (G, x) if there exists a bijection Γ satisfying $\Gamma(\chi)(x) = \pm\chi(x)$ for every $\chi \in \mathrm{Irr}^x(G)$. The main families of counterexamples to the Strong Picky Conjecture are the simple groups with non-abelian TI-Sylow p-subgroups.

Let $P \in \mathrm{Syl}_p(G)$ and let $x \in P$ be a picky p-element. By [**77**, Lemma 2.7], we have that $\mathbf{C}_G(x) = \mathbf{C}_{\mathbf{N}_G(P)}(x)$. Thus, applying the second orthogonality relation to x in G and in $\mathbf{N}_G(P)$, we have that

$$\sum_{\chi \in \mathrm{Irr}^x(G)} |\chi(x)|^2 = |\mathbf{C}_G(x)| = |\mathbf{C}_{\mathbf{N}_G(P)}(x)| = \sum_{\psi \in \mathrm{Irr}^x(\mathbf{N}_G(P))} |\psi(x)|^2.$$

Thus, if (G, x) satisfies the Strong Picky Conjecture, then the summands appearing in both sides are the same.

By Corollary A.20, we have that a p-element $x \in G$ is picky if and only if $\mathbf{Sub}_G(x) = \mathbf{N}_G(P)$ for $P \in \mathrm{Syl}_p(G)$ with $x \in P$. Moretó and Rizo [**93**] noticed

that the Picky Conjecture can be extended to arbitrary p-elements replacing the Sylow normalizer by the subnormalizer.

CONJECTURE A.27 (Subnormalizer Conjecture). *Let p be a prime, let G be a group and let $x \in G$ be a p-element. Then there exists a bijection*

$$\Gamma : \mathrm{Irr}^x(G) \to \mathrm{Irr}^x(\mathbf{Sub}_G(x))$$

satisfying the following properties:

(I) $\Gamma(\chi)(1)_p = \chi(1)_p$ for every $\chi \in \mathrm{Irr}^x(G)$.

(II) $\mathbb{Q}(\Gamma(\chi)(x)) = \mathbb{Q}(\chi(x))$ for every $\chi \in \mathrm{Irr}^x(G)$.

As before, given a p-element $x \in G$, we will say that (G, x) satisfies the **Strong Subnormalizer Conjecture** if there exists a bijection such that $\Gamma(\chi)(x) = \pm\chi(x)$.

We refer to [**70, 93**] for some of the cases where these conjectures are proved. There is much ongoing work in this direction.

A.5. Picky and Subnormalizer Conjectures in simple groups

Much is known about the Picky Conjecture for simple groups. Using the aforementioned classification of picky elements in sporadic groups, Breuer [**13**] proved the Strong Picky Conjecture for sporadic groups. It is worth mentioning that the character tables of normalizers of Sylow subgroups in sporadic groups are not completely known. Thus, the proof of the following result depends on some *ad hoc* arguments and heavily computational methods.

THEOREM A.28 (Breuer). *Let S be a sporadic simple group. Then the Global Picky Conjecture holds for S for any prime p.*

On the other hand, [**83**] studies these conjectures for symmetric groups. One of the main results there shows that the Strong Picky Conjecture holds for symmetric groups.

THEOREM A.29. *The Strong Global Picky conjecture holds for S_n for every prime p.*

Let n be an integer, let p be a prime and let $P \in \mathrm{Syl}_p(\mathsf{S}_n)$. Assume first that either $p > 2$ or $p = 2$ and n is odd. In this case, Proposition A.16, together with some calculations prove that $\mathrm{Irr}^{\mathcal{P}}(\mathsf{S}_n) = \mathrm{Irr}^x(\mathsf{S}_n)$ for $x \in P$ a picky element of type I. It is also possible to prove that $\mathrm{Irr}^x(\mathsf{S}_n) = \mathrm{Irr}_{p'}(\mathsf{S}_n)$. Assume now that $p = 2$ and n is even. In this case, it is possible to prove that $\mathrm{Irr}^{\mathcal{P}}(\mathsf{S}_n) = \mathrm{Irr}^y(\mathsf{S}_n)$ for $y \in P$ a picky element of type II. It is not hard to see that $\mathrm{Irr}^y(\mathsf{S}_n)$ contains even degree characters for $n \equiv 0 \pmod 8$. Following the proof of Theorem

A.29, it is possible to compute $\chi(g)$ for any picky p-element $g \in \mathsf{S}_n$ and any $\chi \in \mathrm{Irr}^g(\mathsf{S}_n)$. In the case, when $p = 2$, n is even and $y \in \mathsf{S}_n$ is of type II, then $\chi(y) = \pm 1$ for $\chi \in \mathrm{Irr}_{2'}(\mathsf{S}_n)$ and $\chi(y) = \pm 2$ for $\chi \in \mathrm{Irr}^y(\mathsf{S}_n) \setminus \mathrm{Irr}_{2'}(\mathsf{S}_n)$. If moreover $n = 2^k$ for $k \geqslant 3$, then

$$\{\chi(1)_2 \mid \chi \in \mathrm{Irr}^y(\mathsf{S}_{2^k})\} = \{1, 2, \ldots, 2^{k-2}\}.$$

This regularity contrasts with the behavior of $\{\chi(1)_2 \mid \chi \in \mathrm{Irr}(\mathsf{S}_{2^k})\}$, which has some gaps. For example, $\{\chi(1)_2 \mid \chi \in \mathrm{Irr}(\mathsf{S}_8)\} = \{1, 2, 4, 8, 64\}$. In [**83**], there are results studying the Subnormalizer Conjecture for symmetric groups.

THEOREM A.30. *Let $k \geqslant 3$ be an integer and let $x \in \mathsf{S}_{2^k}$ be a 2-element The Strong Subnormalizer Conjecture holds for (S_{2^k}, x).*

On the other hand, Malle [**70**] provides a systematic study of the Picky Conjecture and the Subnormalizer Conjecture for groups of Lie type. Just to show an example, for unipotent elements, we have the following result.

THEOREM A.31 (Malle). *Let $G = B_2(q), G_2(q), {}^3D_4(q)$ or ${}^2F_4(q)$. If $x \in G$ is unipotent, then the Subnormalizer Conjecture holds for (G, x).*

Malle [**70**] is working towards proving the Picky and Subnormalizer Conjectures in the case when p is not equal to the characteristic of the group.

It is expected that these conjectures will continue to motivate a much deeper analysis of [**77**]. For instance, it would be desirable to classify picky elements of arbitrary groups. This will possibly be an enormous task. As pointed out in [**77**], we expect that it should be possible to study the picky p-elements from the point of view of fusion systems, which is an approach that would be interesting to study in future work.

Bibliography

[1] A. Abdollahi, A. Azad, A. Hassanabadi, M. Zarrin, B. H. Neumann's question on ensuring commutativity of finite groups, *Bull. Austral. Math. Soc.* **74** (2006), 121–132.

[2] T. M. Apostol *Introduction to analytic number theory*, Undergrad. Texts Math., Springer-Verlag, New York-Heidelberg, 1976.

[3] A. Bächle, Integral group rings of solvable groups with trivial central units, *Forum Math.* **30(4)** (2018), 845–855.

[4] A. Bächle, M. Caicedo, E. Jespers, S. Maheshwary, Global and local properties of finite groups with only finitely many central units in their integral group ring, *J. Group Theory* **24** (2021), 1163–1188.

[5] F. Barry, D. MacHale, À. Ni Shé, Some supersolvability conditions for finite groups, *Math. Proc. R. Ir. Acad.* **106A(2)** (2006), 163–177.

[6] B. Baumeister, A. Maróti, H. P. Tong-Viet, Finite groups have more conjugacy classes, *Forum Math.* **29** (2017), 259–275.

[7] A. Beltrán, M. J. Felipe, G. Malle, A. Moretó, G. Navarro, L. Sanus, R. Solomon, P. H. Tiep, Nilpotent and abelian Hall subgroups in finite groups, *Trans. Amer. Math. Soc.* **368** (2016), 2497–2513.

[8] H. Bender, A group theoretic proof of the p^aq^b-theorem, *Math. Z.* **126(4)** (1972), 327–338.

[9] E. A. Bertram, Lower bounds for the number of conjugacy classes in finite groups. Ischia Group Theory 2004, *Contemp. Math.* **402** (2006), 95-117.

[10] H. I. Blau, G. O. Michler, Modular representation theory of finite groups with T.I. Sylow p-subgroups, *Trans. Amer. Math. Soc.* **319** (1990), no. 2, 417–468.

[11] R. Brauer, *Number theoretical investigations on groups of finite order*, in Proceedings of the International Symposium on Algebraic Number Theory, Tokyo and Nikko, 1955, 55–62, Science Council of Japan, Tokyo, 1956.

[12] R. Brauer, *Representations of Finite Groups*, Lectures on Modern Mathematics, Vol. I. Wiley, New York, 1963.

[13] T. Breuer, Private communication.

[14] T. C. Burness, Simple groups, fixed point ratios and applications, in: Local representation theory and simple groups, in EMS Series of Lectures in Mathematics 2018, 267–322, EMS, Zürich.

[15] T. C. Burness, R. M. Guralnick, Fixed point ratios for finite primitive groups and applications, *Adv. Math.* **411** (2022), Paper No. 108778.

[16] T. C. Burness, R. M. Guralnick, A. Moretó, G. Navarro, The probability that two p-elements commute, *Alg. Number Th.* **17** (2023), 1209–1229.

[17] M. Cabanes, B. Späth, The McKay Conjecture on character degrees, *Ann. of Math.* https://arxiv.org/abs/2410.20392.

[18] R. W. Carter, Nilpotent self-normalizing subgroups and system normalizers, *Proc. London Math. Soc. (3)* **12** (1962), 535–563.

[19] R. W. Carter, *Finite groups of Lie type. Conjugacy classes and complex characters*, Pure Appl. Math., Wiley and Sons, New York, 1985.
[20] C. Casolo, Subnormalizers in finite groups, *Comm. Algebra* **18(11)** (1990), 3791–3818.
[21] C. Casolo, On the subnormalizer of a p-subgroup, *J. Pure Appl. Algebra* **77** (1992), 231–238.
[22] C. Casolo, U. Dardano, Subnormality in the join of two subgroups, *J. Group Theory* **7** (2004), 507–520.
[23] D. Chillag, S. Dolfi, Semi-rational solvable groups, *J. Group Theory* **13(4)** (2010), 535–548.
[24] J. H. Conway, R. T. Curtis, S. P. Norton, and R. A. Parker, *Atlas of finite groups*, Clarendon Press, Oxford, 1985.
[25] D. A. Craven, Symmetric group character degrees and hook numbers, *Proc. London Math. Soc.* **96(3)** (2008), 26–50.
[26] L. Dornhoff, *Group Representation Theory. Part A: Ordinary representation theory*, Pure Appl. Math., 7. Marcel Dekker, Inc., New York, 1971.
[27] S. Eberhard, Commuting probabilities of finite groups, *Bull. London Math. Soc.* **47** (2015), 796–808.
[28] P. Erdös, P. Turán, On some problems of a statistical group-theory, IV, *Acta Math. Acad. Sci. Hung.* **19** (1968), 413–435.
[29] E. Farias e Soares, Big primes and character values for solvable groups, *J. Algebra* **100** (1986), 305–324.
[30] W. Feit, J. G. Thompson, Solvability of groups of odd order, *Pacific J. Math.* **13** (2022), 775–1029.
[31] J. Fulman, R. M. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, *Trans. Amer. Math. Soc.* **364** (2012), 3023–3070.
[32] P. X. Gallagher, The number of conjugacy classes in a finite group, *Math. Z.* **118** (1970), 175–179.
[33] The GAP Group, GAP Groups, algorithms, and programming, version 4.12.1, 2022, http://www.gap-system.org.
[34] M. Geck, *An Introduction to Algebraic Geometry and Algebraic Groups*, Oxf. Grad. Texts Math., 20. Oxford University Press, Oxford, 2003.
[35] E. Giannelli, S. Law, J. Long, C. Vallejo, Sylow branching coefficients and a conjecture of Malle and Navarro, *Bull. Lond. Math. Soc.* **54(2)** (2022), 552–567.
[36] M. Giudici, L. Morgan, C. E. Praeger, Finite simple groups have many classes of p-elements, *Pacific J. Math.* https://arxiv.org/abs/2411.18863.
[37] D. M. Goldschmidt, A group theoretic proof of the p^aq^b-theorem for odd primes, *Math. Z.* **113(5)** (1970), 373–375.
[38] D. Gorenstein, Finite groups. 2nd ed., Chelsea Publishing Co., 301. American Mathematical Society, New York, 1980.
[39] R. Gow, Groups whose characters are rational-valued, *J. Algebra* **40** (1976), 280–299.
[40] R. M. Guralnick, A. Maróti, J. Martínez Madrid, A. Moretó, N. Rizo Fixed point ratios, Sylow Numbers and coverings of p-elements in finite groups, *J. London Math. Soc.* https://arxiv.org/abs/2407.20355.
[41] R. M. Guralnick, G. R. Robinson, On the commuting probability in finite groups, *J. Algebra* **300** (2006), 509–528.
[42] W. H. Gustafson, What is the probability that two elements commute?, *Amer. Math. Monthly* **80** (1973), 1031–1034.
[43] P. Hall, Theorems like Sylow's, *Proc. Lond. Math. Soc.* **3** (1956), 286–304.

[44] P. Hall, G. Higman, On the p-length of p-soluble groups and reduction theorems for Burnside's problem, *Proc. Lond. Math. Soc.* **s3-6** (1956), 1–42.
[45] B. Hartley, Sylow p-subgroups and local p-solubility, *J. Algebra* **23** (1971), 347–369.
[46] D. R. Heath-Brown, Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression, *Proc. Lond. Math. Soc.* **s3-64(2)** (1992), 265–338.
[47] M. Herzog, On 2-Sylow intersections, *Israel J. Math.* **11** (1972), 326–327.
[48] L. Héthelyi, B. Külshammer, Elements of prime power order and their conjugacy classes in finite groups, *J. Aust. Math. Soc.* **78** (2005), 291–295.
[49] C. Y. Ho, H. Völklein, A criterion for an element to belong to a given Sylow p-subgroup I, *J. Algebra* **132** (1990), 113–122.
[50] C. Y. Ho, H. Völklein, A criterion for an element to belong to a given Sylow p-subgroup II, *Geom. Dedicata* **28** (1988), 363–368.
[51] N. N. Hung, A. Maróti, J. Martínez, Conjugacy classes of π-elements and nilpotent/abelian Hall π-subgroups, *Pacific J. Math.* **323** (2023), 185–204.
[52] B. Huppert, *Endliche gruppen*, Die Grundlehren der mathematischen Wissenschaften, 134. Springer Berlin, Heidelberg, 1967.
[53] I. M. Isaacs, *Character Theory of Finite Groups*, Dover Publications, New York, 1976.
[54] I. M. Isaacs, *Finite Group Theory*, Grad. Stud. Math., 92. American Mathematical Society, Providence, Rhode Island, 2008.
[55] I. M. Isaacs, *Characters of solvable groups*, Grad. Stud. Math., 189. American Mathematical Society, Providence, Rhode Island, 2018.
[56] I. M. Isaacs, M. Loukaki, A. Moretó, The average degree of an irreducible character of a finite group, *Isr. J. Math.* **197** (2013), 55–67.
[57] N. Itô, Some studies on group characters, *Nagoya Math. J.* **2** (1951) 17–28.
[58] K. S. Joseph, *Commutativity in non-abelian groups*, *Dissertation*, UCLA, (1969).
[59] T. M. Keller, Finite groups have even more conjugacy classes, *Israel J. Math.* **181** (2011), 433–444.
[60] R. Knörr, G. R. Robinson, Some remarks on a conjecture of Alperin, *J. London Math. Soc.* **39(2)** (1989), no. 1, 48–60.
[61] S. Koshitani, T. Sakurai, The principal p-blocks with four irreducible characters, *Bull. London Math. Soc.* **53** (2021), 1124–1138.
[62] E. Landau, Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante, *Math. Ann.* **56** (1903), 671–676.
[63] Y. Lazmouri, X. Li, K. Soundararajan, Conditional bounds for the least quadratic non-residue and related problems, *Math. Comp.* **84(295)** (2015), 2391–2412.
[64] J. C. Lennox, S. E. Stonehewer, *Subnormal Subgroups of Groups*, Claredon Press, Oxford, 1987.
[65] P. Lescot, Sur certains groupes finis, *Recv. Math. Spéciales* **8** (1987), 267–277.
[66] P. Lescot, Central extensions and commutativity degree, *Comm. Algebra* **29** (2001), 4451–4460.
[67] P. Lescot, H. N. Nguyen, Y. Yang, On the commuting probability and supersolvability of finite groups, *Monatsh. Math.* **174** (2014), 567–576.
[68] Y. Linnik, On the least prime in an arithmetic progression II. The Deuring-Heilbronn phenomenon, *Rec. Math.* **15(57)** (1944), 347–368.
[69] F. Lübeck, Numbers of conjugacy classes in finite groups of Lie type, available at http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/nrclasses/nrclasses.html?LANG=en.
[70] G. Malle, Picky elements, subnormalisers, and character correspondences, https://arxiv.org/abs/2503.10425.

[71] G. Malle, G. Navarro, Brauer's Height Zero Conjecture for principal blocks, *J. reine angew. Math.* **778** (2021), 119–125.
[72] G. Malle, G. Navarro, G. R. Robinson, Conjugacy class numbers and π-subgroups, *Pacific J. Math.* **311** (2021), 135–164.
[73] G. Malle, G. Navarro, A. A. Schaefer Fry, P. H. Tiep, Brauer's Height Zero Conjecture, *Ann. of Math.* **200** (2024), no. 2, 557–608.
[74] G. Malle, B. Späth, Characters of odd degree, *Ann. of Math.* **184** (2016), 869–908
[75] G. Malle, D. Testerman, *Linear algebraic groups and finite groups of Lie type*, Cambridge Stud. Adv. Math., 133. Cambridge University Press, Cambridge, 2011.
[76] A. Maróti and H. N. Nguyen, On the number of conjugacy classes of π-elements in finite groups, *Arch. Math.* **102** (2014), 101–108.
[77] A. Maróti, J. Martínez, A. Moretó, Covering the set of p-elements in finite groups by Sylow p-subgroups, *J. Algebra* **638** (2024), 840–861.
[78] A. Maróti, J. Martínez, A. Moretó, Covering the set of p-elements in finite groups by proper subgroups, *J. Comb. Theory Ser. A* **210** (2025), 105954.
[79] J. Martínez, Groups with small multiplicities of fields of values of irreducible characters, *J. Pure Appl. Algebra* **227(7)** (2023), 107343.
[80] J. Martínez, On the commuting probability of π-elements in finite groups, *Math. Nachr.* **297** (2024), 2287–2301.
[81] J. Martínez, Supersolvability and nilpotency in terms of the commuting probability and the average character degree, *Ann. Mat. Pura Appl.* **203** (2024), 765–778.
[82] J. Martínez Madrid, The Baby Monster is the largest group with at most 2 irreducible characters with the same degree, *Bull. Lond. Math. Soc.* https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/blms.70040.
[83] J. Martínez Madrid, In preparation.
[84] J. Martínez Madrid, M. Vergani, Multiplicities of fields of values of conjugacy classes in finite groups, In preparation.
[85] G. O. Michler, *Brauer's Conjectures and the Classification of Finite Simple Groups*, Lecture Notes in Math., vol. 1178, Springer, Berlin, 1986.
[86] A. Moretó, Complex group algebras of finite groups: Brauer's Problem 1, *Adv. Math.* **208(1)** (2007), 236–248.
[87] A. Moretó, Sylow numbers and nilpotent Hall subgroups, *J. Algebra* **379** (2013), 80–84.
[88] A. Moretó, Multiplicities of fields of values of irreducible characters of finite groups, *Proc. Amer. Math. Soc.* **149** (2021), 4109–4116.
[89] A. Moretó, Fields of values of cut groups and k-rational groups, *J. Algebra* **591** (2022), 111–116.
[90] A. Moretó, Methods and questions in character degrees of finite groups, *Vietnam J. Math.* **51** (2023), 685–701.
[91] A. Moretó, The average character degree of finite groups and Gluck's conjecture, *J. Group Theory* **26** (2023), 803–815.
[92] A. Moretó, H. N. Nguyen, On the average character degree of finite groups, *Bull. Lond. Math. Soc.* **46** (2014), 55–67.
[93] A. Moretó, N. Rizo, In preparation. https://www.uv.es/jomimar8/valenciaslides/moreto.pdf.
[94] A. Moretó, A. Sáez, Prime divisors of orders of products, *Proc. Roy. Soc. Edinburgh Sect. A* **149** (2019), no. 5, 1153–1162.
[95] A. Moretó, J. Sangroniz, A. Turull, Sylow subgroups and the number of conjugacy classes of p-elements, *J. Algebra* **275** (2004), 668–674.
[96] H. Nagao, On a conjecture of Brauer for p-solvable groups, *J. Math. Osaka City Univ.* **13** (1962) 35–38.

[97] G. Navarro, *Characters and blocks of finite groups*, London Math. Soc. Lecture Note Ser., 250. Cambridge University Press, Cambridge, 1998.
[98] G. Navarro, Quadratic characters in groups of odd order, *J. Algebra* **322 (7)** (2009), 2586–2589.
[99] G. Navarro, *Character theory and the McKay conjecture*, Cambridge Stud. Adv. Math., 175. Cambridge University Press, Cambridge, 2018.
[100] G. Navarro, P. H. Tiep, Rational irreducible characters and rational conjugacy classes in finite groups, *Trans. Amer. Math. Soc.* **360** (2008), 2443–2465.
[101] P. M. Neumann, A lemma that is not Burnside', *Math. Sci.* **4** (1979), 133–141.
[102] P. M. Neumann, Two combinatorial problems in group theory, *Bull. London Math. Soc.* **21** (1989), 456–458.
[103] N. N. Hung, A. A. Schaeffer Fry, H. P. Tong-Viet, C. Vinroot, On the number of irreducible real-valued characters of a finite group, *J. Algebra* **555** (2020), 275–288.
[104] L. Pyber, The number of pairwise noncommuting elements and the index of the centre in a finite group, *J. London Math. Soc.* **35(2)** (1987), 287–295.
[105] L. Pyber, Finite groups have many conjugacy classes, *J. Lond. Math. Soc.* **s2-46(2)** (1992), 239–249.
[106] A. Rae, Sylow p-subgroups of finite p-soluble groups, *J. London Math. Soc.* **7(2)**(1973), 117–123.
[107] D. J. S. Robinson, *A course in the theory of groups*, 2nd ed., Grad. Texts in Math., 80. Springer-Verlag, Inc., New York, 1996.
[108] D. J. S. Robinson, J. S. Wilson, Soluble groups with many polycyclic quotients, *Proc. Lond. Math. Soc.* **s3-48(2)** (1984), 193–229.
[109] J. J. Rotman, *An Introduction to the Theory of Groups*, 4th ed., Grad. Texts in Math. 148. Springer, New York, 1995.
[110] D. Rossi, *Fields of Values in Finite Groups: Characters and Conjugacy Classes*, PhD Thesis, University of Arizona, Tucson, 2018.
[111] J. Sangroniz, *Restrictions of Brauer characters and π-partial characters*, in Ischia group theory 2008, 236–242, World Sci. Publ., Hackensack, NJ.
[112] J. Sangroniz, A. Vera-Lopez, The finite groups with thirteen and fourteen conjugacy classes, *Math. Nachr.* **280** (2007), no 5-6, 676–694.
[113] B. Sambale, On redundant Sylow subgroups, *J. Algebra* **650** (2024), 1–9.
[114] G. Scorza, I gruppi che possono pensarsi come somme di tre loro sottogruppi, *Bol. Un. Mat. Ital.* **5** (1926), 216–218.
[115] C. A. Schroeder, Finite groups with many p-regular conjugacy classes, *J. Algebra* **641** (2024), 716–734.
[116] W. A. Simpson and J. S. Frame, The character tables of $\mathrm{SL}(3,q)$, $\mathrm{SU}(3,q^2)$, $\mathrm{PSL}(3,q)$, $\mathrm{PSU}(3,q^2)$, *Canad. J. Math.* **25** (1973), 486–494.
[117] J. Singer. A theorem in finite projective geometry and some applications to number theory, *Trans. Am. Math. Soc.*, **43(3)** (1938), 377–385.
[118] G. A. L. Souza, On groups with at most five irrational conjugacy classes, (2024) https://arxiv.org/abs/2409.03539.
[119] G. A. L. Souza, In preparation.
[120] J. F. Tent, Quadratic rational solvable groups, *J. Algebra* **363** (2012), 73–82.
[121] J. G. Thompson, Composition factors of rational finite groups, *J. Algebra* **319** (2005), 558–594.
[122] M. C. H. Tointon, Commuting probabilities of infinite groups, *J. Lond. Math. Soc.* **101(3)** (2020), 1280–1297.
[123] H. P. Tong-Viet, Conjugacy classes of p-elements and normal p-complements, *Pacific J. Math.* **308** (2020), 207–222.
[124] S. Trefethen, Non-Abelian composition factors of m-rational groups, *J. Algebra* **485** (2017), 288–309.

[125] P. Turán, On an extremal problem in graph theory, *Mat. Fiz. Lapok* **48** (1941), 436–452.

[126] A. Vera-López, J. Vera-López, Classification of finite groups according to the number of conjugacy classes I, *Israel J. Math.* **51** (1985), 305–338.

[127] A. Vera-López, J. Vera-López, Classification of finite groups according to the number of conjugacy classes II, *Israel J. Math.* **56** (1986), 188–221.

[128] H. Wielandt, Zum Satz von Sylow, *Math. Z.* **60** (1954), 407–408.

[129] T. Xylouris, *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression*, PhD Thesis, Universität Bonn, (2011).

[130] K. Zsigmondy, Zur theorie der potenzreste, *Monatsch. Math. Phys.* **3** (1892), 265–284.