



Universidade de Brasília

**On pyramidal groups of prime power degree and
the number of cyclic subgroups**

Xiaofang Gao

Advisor: Dr. Martino Garonzi

Departamento de Matemática
Universidade de Brasília

Dissertação apresentada como requisito parcial para obtenção do grau de
Doutor(a) em Matemática

Brasília, 27 de Junho de 2024

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

On pyramidal groups of prime power degree and the number of cyclic subgroups

por

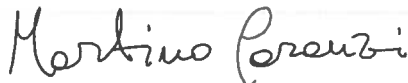
Xiaofang Gao*

Tese apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

DOUTOR EM MATEMÁTICA

Brasília, 27 de Junho de 2024.

Comissão examinadora:



Prof. Dr. Martino Garonzi – UnB (Orientador)



Prof. Dr. Igor dos Santos Lima – UnB (Membro)



Prof. Dr. Claude Marion - Universidade do Porto (Membro)

דן לוי

Prof. Dr. Dan Levy – Tel-Aviv Academic College (Membro)

*O autor foi bolsista da CAPES durante a elaboração desta tese.

Acknowledgements

Firstly, I would like to express my heartfelt gratitude to my supervisor, Professor Martino Garonzi, for his time, support, guidance, and patience. I sincerely appreciate the committee members for their careful reading and valuable suggestions for my thesis.

I am also thankful to the professors and postgraduate students of the Department of Mathematics at the University of Brasilia for their help and companionship.

Furthermore, I am deeply grateful to my family for their unwavering support and encouragement throughout my university studies.

Lastly, I am grateful for the financial support provided by CAPES.

Resumo

Seja G um grupo finito. Uma involução de G é um elemento de G de ordem 2. G é chamado de piramidal se todas as involuções de G forem conjugadas em G , e G é chamado de m -piramidal se for piramidal e tiver precisamente m involuções, onde m é um inteiro positivo. Os grupos piramidais podem ser interpretados como grupos específicos de automorfismos de certas estruturas combinatórias chamadas de sistemas triplos de Kirkman piramidais, que foram objeto de estudo em artigos recentes (veja [1, 2]). Mais especificamente, um grupo m -piramidal age como grupo de automorfismos de um sistema triplo de Kirkman piramidal, regularmente em todos os pontos exceto m pontos fixos. Obviamente, a ordem de um grupo m -piramidal G está fortemente relacionada ao número de vértices de um sistema triplo de Kirkman piramidal. Bonvicini, Buratti, Garonzi, Rinaldi e Traetta [2] forneceram algumas propriedades de grupos 3-piramidais e o conjunto de ordens para tais grupos. Nosso objetivo é provar que, se m é uma potência de um primo ímpar p^k onde $p \neq 7$, então todo grupo m -piramidal é solúvel se e somente se $m = 9$ ou k é ímpar. Também determinamos as ordens dos grupos m -piramidais quando $m \neq 7$ é um número primo. Além disso, obtemos uma classificação dos grupos 3-piramidais. Posteriormente, são discutidos os números de subgrupos cíclicos e subgrupos cíclicos maximais de G . Uma família de grupos é chamada (maximal) cyclic bounded ((M)CB) se, para cada número natural n , existem apenas um número finito de grupos na família com no máximo n subgrupos cíclicos (maximais). Neste tópico, provamos que a família de grupos de ordem de potência de primo é MCB. Provamos também que a família de grupos finitos sem fatores diretos coprimos cíclicos é CB. Como consequência, um número natural $n \geq 10$ é primo se, e somente se, houver apenas um número finito de grupos finitos com precisamente n subgrupos cíclicos. O conteúdo dessa tese consiste dos artigos [8, 9, 10]. O primeiro deles foi publicado no Journal of Algebra, os outros dois foram submetidos para publicação.

Palavras-chave: Grupos primitivo, Grupos finito, Grupos solúveis, Sistemas Triplos de Kirkman, Subgrupos cíclicos, Subgrupos cíclicos maximais.

Título em português: Sobre os grupos piramidais de grau potência de primo e o número de subgrupos cíclicos.

Abstract

Let G be a finite group. An involution of G is an element of G of order 2. G is called pyramidal if all involutions of G are conjugate in G , and G is called m -pyramidal if it is pyramidal and it has precisely m involutions, where m is a positive integer. Pyramidal groups can be interpreted as specific groups of automorphisms of certain combinatorial structures called pyramidal Kirkman triple systems, which were object of study in recent papers (see [1, 2]). More specifically, an m -pyramidal group acts as automorphism group of an m -pyramidal Kirkman triple system, regularly on all but m fixed points. Obviously, the order of an m -pyramidal group G is strongly related to the vertex size X of an m -pyramidal Kirkman triple system. Bonvicini, Buratti, Garonzi, Rinaldi and Traetta [2] provided some properties of 3-pyramidal groups and the set of orders for such groups. Our goal is to prove that, if m is an odd prime power p^k where $p \neq 7$, then every m -pyramidal group is solvable if and only if either $m = 9$ or k is odd. We also determine the orders of the m -pyramidal groups when $m \neq 7$ is a prime number. Moreover, we obtain a classification of 3-pyramidal groups. Subsequently, the numbers of cyclic and maximal cyclic subgroups of G are discussed. A family of groups is called (maximal) cyclic bounded ((M)CB) if, for every natural number n , there are only finitely many groups in the family with at most n (maximal) cyclic subgroups. In this topic we prove that the family of groups of prime power order is MCB. We also prove that the family of finite groups without cyclic coprime direct factors is CB. As a consequence, a natural number $n \geq 10$ is prime if and only if there are only finitely many finite groups with precisely n cyclic subgroups. The content of this thesis consists of the papers [8, 9, 10]. The first of them was published in the Journal of Algebra, the other two were submitted for publication.

Keywords: Primitive group, Finite group, Solvable group, Kirkman Triple System, Cyclic subgroup, Maximal cyclic subgroup.

Notation

Symbol	Meaning
$ G $	order of a group G
$o(g)$	order of an element g
a^g	the conjugate of a by g : $g^{-1}ag$
$[x, y]$	the commutator of x and y : $x^{-1}y^{-1}xy$
$[H, K]$	the commutator subgroup of H and K
$ G : K $	the index of K in G
G'	derived subgroup of G
$H \times K$	the direct product of H and K
$H : K$ or $H \rtimes K$	the semidirect product (or split extension) of H by K
$H.K$ or HK	an unspecified extension of H by K
$H \cdot K$	any case of $H.K$ which is not a split extension
$H \wr K$	the wreath product of H and K
$H \circ K$	the central product of H and K
$[n]$	an arbitrary group of order n
n or C_n	a cyclic group of order n
G^n	the direct product of n groups of structure G
p^n	the elementary abelian group of order p^n
p^{m+n}	the extension of an elementary abelian group of order p^m by an elementary abelian group of order p^n
p^{1+2n}	an extraspecial group of this order with centre of order p and central quotient elementary abelian of order p^{2n}
$A \setminus B$ or $A - B$	elements of A not in B
Q_{2^n}	quaternion group of order 2^n
D_{2n}	dihedral group with $2n$ elements
SD_{2n}	semidihedral group of order $2n$

Symbol	Meaning
$\Phi(G)$	Frattini subgroup of G
M_G	the normal core of M in G
(a, b)	the greatest common divisor of a and b
$\lfloor n \rfloor$	largest integer $\leq n$
\mathbb{F}_q	field with q elements
I_n	an $n \times n$ identity matrix
SmallGroup(n, i)	the i -th group of order n in the Small Group Library of GAP

Contents

Introduction	1
1 Preliminaries	11
1.1 General theory and results	11
1.2 Some properties of primitive and almost-simple groups	24
2 The solvability of pyramidal groups of prime degree	29
2.1 About pyramidal KTS and pyramidal groups	29
2.2 Preliminaries	30
2.3 The proof of Theorem A	41
3 The solvability of pyramidal groups of prime power degree	49
3.1 Preliminaries	50
3.2 The proof of Theorem B	51
4 Some properties of pyramidal groups	56
4.1 Preliminaries	56
4.2 The proof of Theorem C	59
4.3 The proof of Theorem D	61
5 The number of (maximal) cyclic subgroups.	63
5.1 Preliminaries	63

5.2	The proof of Theorem E	68
5.3	The proof of Theorem F	68
5.4	The proof of Theorem G	70
Appendix		72
A The classification of simple pyramidal groups		73
Bibliography		75

Introduction

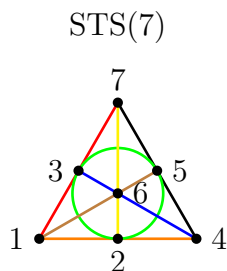
In Query 6 of the Lady's and Gentleman's Diary of 1850, T. P. Kirkman posed the following problem, known as *Kirkman's School-Girl Problem*: 15 young ladies in a school walk out 3 abreast for 7 days in succession: it is required to arrange them daily, so that no two shall walk twice abreast.

The Kirkman's School-Girl Problem can be generalized to v girls. On each of $(v-1)/2$ days, each girl is to be included in exactly one group of 3 and each pair of girls are to walk in the same group of girls exactly once. In 1971, D. K. Ray-Chaudhuri and R. M. Wilson proved that such a schedule exists if and only if $v \equiv 3 \pmod{6}$ (see [4]). A solution to this problem is an example of a Kirkman triple system, which is a Steiner triple system having a parallelism, that is, a partition of the blocks of the triple system into parallel classes which are themselves partitions of the points into disjoint blocks.

Now we introduce the definitions of Steiner triple system and Kirkman triple system. Sometimes, in order to save space, we write blocks in the form abc rather than $\{a, b, c\}$.

A *Steiner triple system* of order v , briefly STS(v), is a pair (V, B) where V is a set of v points and B is a set of 3-subsets (blocks) of V with the property that any two distinct points are contained in exactly one block, in other words, for any pair of points $x \neq y$, there exists a block containing both x and y .

For example:



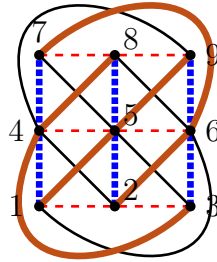
In the above Steiner triple system STS(7), we have $V = \{1, 2, \dots, 7\}$ and

$$B = \{124, 137, 457, 267, 165, 463, 235\}.$$

A *Kirkman triple system* of order v , briefly $\text{KTS}(v)$, is an $\text{STS}(v)$ together with a resolution R of its block set B , that is a partition of B into classes (parallel classes) each of which is, in its turn, a partition of the point-set V .

For example:

$\text{KTS}(9)$



In the above Kirkman triple system $\text{KTS}(9)$, we have $V = \{1, 2, \dots, 9\}$,

$$B = \{123, 456, 789, 147, 258, 369, 168, 249, 357, 159, 267, 348\},$$

and

$$R = \{\{123, 456, 789\}, \{147, 258, 369\}, \{168, 249, 357\}, \{159, 267, 348\}\}.$$

Moreover, we have the following 4 parallel classes:

$\{1, 2, 3\}$,	$\{4, 5, 6\}$,	$\{7, 8, 9\}$,
$\{1, 4, 7\}$,	$\{2, 5, 8\}$,	$\{3, 6, 9\}$,
$\{1, 6, 8\}$,	$\{2, 4, 9\}$,	$\{3, 5, 7\}$,
$\{1, 5, 9\}$,	$\{2, 6, 7\}$,	$\{3, 4, 8\}$.

Note that a $\text{STS}(v)$ has $\frac{1}{3}\binom{v}{2} = \frac{1}{6}v(v-1)$ blocks and a $\text{KTS}(v)$ has $\frac{1}{2}(v-1)$ parallel classes. It has been known since the mid-nineteenth century that a $\text{STS}(v)$ exists if and only if $v \equiv 1$ or $3 \pmod{6}$ [3]. The analogous result for KTSs has been instead obtained more than a century later [4]: a $\text{KTS}(v)$ exists if and only if $v \equiv 3 \pmod{6}$. These structures fall into the broader category of combinatorial designs.

An *automorphism of a Steiner triple system* is a permutation of its points leaving the block-set invariant. Analogously, an *automorphism of a Kirkman triple system* is an automorphism of the underlying Steiner triple system leaving the resolution invariant. Thus an automorphism of a KTS is automatically an automorphism of the underlying STS though the converse is not true in general. Of course, the automorphisms of a STS (resp. KTS) D form a group with composition, which we denote by $\text{Aut}(D)$. Steiner triple systems that possess an automorphism with a specified property or an automorphism

group with a specified action have attracted significant attention for a long time. For more information on this subject, see [1].

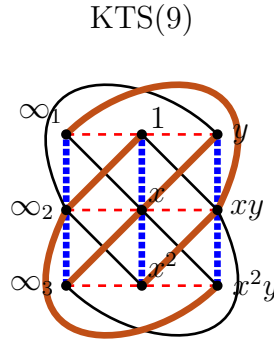
Recall that a group action of G on a set X is called regular if it is transitive and its point stabilizers are trivial. In this case, $|G| = |X|$.

A Steiner (resp. Kirkman) triple system D is called m -pyramidal if there exists a subgroup G of $\text{Aut}(D)$ fixing m points and acting regularly on the other points. If this happens, we say that the STS (resp. KTS) is m -pyramidal realized “under” G . Note that if this happens, then of course D has $|G| + m$ points.

Let us give an example. We construct a 3-pyramidal Kirkman triple system under $G = S_3$. $V = \{\text{vertices}\}$.

$$G = S_3 = \langle x, y : x^3 = y^2 = 1, yx = x^2y \rangle = \{1, x, x^2, y, xy, x^2y\}.$$

$$V = G \cup \{\infty_1, \infty_2, \infty_3\} = \{\infty_1, \infty_2, \infty_3, 1, x, x^2, y, xy, x^2y\}.$$



For the above Kirkman triple system KTS(9), we have 5 G -orbits of blocks and 4 parallel classes.

$\{\infty_1, \infty_2, \infty_3\}, \{1, x, x^2\}, \{y, xy, x^2y\},$		
$\{\infty_1, 1, y\},$	$\{\infty_2, x, xy\},$	$\{\infty_3, x^2, x^2y\},$
$\{\infty_1, x, x^2y\},$	$\{\infty_2, x^2, y\},$	$\{\infty_3, 1, xy\},$
$\{\infty_1, x^2, xy\},$	$\{\infty_2, 1, x^2y\},$	$\{\infty_3, x, y\}.$

Let D be a Steiner triple system, M. Buratti, G. Rinaldi and T. Traetta proved that if D is 3-pyramidal realized under G then G has precisely 3 involutions. Moreover, they proved the following result in [1]:

Theorem (M. Buratti, G. Rinaldi, T. Traetta, 2017). A 3-pyramidal Steiner triple system STS(v) exists if and only if $v \equiv 7, 9 \pmod{24}$ or $v \equiv 3, 19 \pmod{48}$.

In [2], the following theorem was proved for the 3-pyramidal Kirkman triple system $\text{KTS}(v)$, providing a necessary condition for its existence.

Theorem (S. Bonvicini, M. Buratti, M. Garonzi, G. Rinaldi, T. Traetta, 2021). A necessary condition for the existence of a 3-pyramidal Kirkman triple system $\text{KTS}(v)$ is that $v = 24n + 9$ or $v = 24n + 15$ or $v = 48n + 3$ for some n which, in the last case, must be of the form $4^e m$ with m odd. This condition is also sufficient in each of the following cases:

- (1) $v = 24n + 9$ and $4n + 1$ is a sum of two squares.
- (2) $v = 24n + 15$ and either $2n + 1 \equiv 0 \pmod{3}$ or the square-free part of $2n + 1$ does not have any prime $p \equiv 11 \pmod{12}$.
- (3) $v = 48n + 3$.

Moreover, they provided some difference methods to construct 3-pyramidal Kirkman triple systems and observed that each group having a 3-pyramidal action on a Kirkman triple system must have exactly three involutions, and these involutions are pairwise conjugate (see [2, Theorem 3.8]). We can prove the following result about an m -pyramidal Kirkman triple system using the same method as in [2].

Call ∞_i the fixed points, for $i = 1, \dots, m$. Clearly, we may identify the vertices of the KTS with

$$V = G \cup \{\infty_1, \dots, \infty_m\}.$$

G acts on V by right multiplication on the elements of G and by fixing the points ∞_i .

The following will be proved in section 2.1.

Proposition. Assume an m -pyramidal KTS can be realized under a nontrivial group G . Then G has precisely m involutions and the involutions of G are pairwise conjugate.

This motivates the following definition. In this thesis, all groups are assumed to be finite.

Definition (Pyramidal groups). A group G is called m -pyramidal if G has precisely m involutions, which are all conjugate to each other. G is called pyramidal if it is m -pyramidal for some m .

If G is a finite group with m involutions, and $m \geq 1$, then m is odd. In fact, by Lagrange's theorem $|G|$ is even. Note that the set $\{x \in G : x \neq x^{-1}\}$, on one hand, has even size, and on the other hand, is of size $|G| - 1 - m$. Therefore $|G|$ and $|G| - 1 - m$ are even, and so m is odd.

For example, if m is any odd integer larger than 1, then the dihedral group D_{2m} with $2m$ elements is a solvable m -pyramidal group. The alternating group A_5 of degree 5 is

a nonsolvable 15-pyramidal group. Moreover, if G is m -pyramidal and H is any group of odd order, then $G \times H$ is also m -pyramidal. Observe that an m -pyramidal group G is necessarily nonabelian of order divisible by $2m$. Indeed, the number m divides $|G|$ by the Orbit-Stabilizer theorem, which states that the length of the G -orbit of an element x equals the index of $Stab_G(x)$ in G (see Definition 1.1.1). On the other hand, G contains involutions, so $|G|$ is also divisible by 2.

There is literature about finite solvable pyramidal group see for example [5, Section 8 of Chapter IX]. The Sylow 2-subgroups of such groups were classified by D. L. Shaw [6], they are cyclic, generalized quaternion (in case there is only one involution), homocyclic (direct products of isomorphic cyclic groups) or Suzuki 2-groups, i.e. 2-groups P that admit a solvable subgroup of $\text{Aut}(P)$ whose action on the involutions of P is transitive. The pyramidal nonsolvable simple groups were classified in the proof of [7, Lemma 1]. It is natural to ask whether it is possible to determine all the values of the odd integer m such that every m -pyramidal group is solvable. In Chapter 2 we discuss the solvability of m -pyramidal groups where $m \neq 7$ is prime and we get the following Theorem A. It was proved in [9].

Theorem A (X. Gao, M. Garonzi). Let $m \neq 7$ be a prime number and let G be an m -pyramidal group. Then G is solvable.

After establishing the solvability of m -pyramidal groups where $m \neq 7$ is prime, we turned our attention to the case of prime power, conjecturing whether all p^k -pyramidal groups are solvable. Subsequently, we found counterexamples, such as if $q > 3$ is any odd prime power, then $\mathbb{F}_q^2 \rtimes \text{SL}(2, q)$ is a nonsolvable q^2 -pyramidal group (see Chapter 3). In Chapter 3 we discuss the values of prime powers m for which the m -pyramidal groups are all solvable and the following Theorem B was proved in [9].

Theorem B (X. Gao, M. Garonzi). Let m be a prime power p^k with $p \neq 7$ an odd prime. Then the following are equivalent.

- (1) Every m -pyramidal group is solvable.
- (2) k is odd or $m = 9$.

If G is a 1-pyramidal group, then a Sylow 2-subgroup P of G is either a cyclic or a generalized quaternion group since P has a unique subgroup of order 2 (see [11, Theorem 6.11]). If G is nonsolvable, then P is noncyclic because otherwise G would have a normal 2-complement N in G (see [11, Corollary 5.14]), and hence $G/N \cong P$, implying that G would be solvable because N and G/N are solvable by the Feit-Thompson theorem, a contradiction. What properties do we have about the m -pyramidal groups? In [2], the authors obtained some properties about 3-pyramidal groups, such as: if G is a 3-pyramidal group of order $|G| = 2^n \cdot d$ with d odd, then n must be even when $n > 1$. In Chapter 4, we give the following theorem C, which provides a classification of 3-pyramidal groups. It was proved in [8].

Theorem C (X. Gao, M. Garonzi). Let G be a finite group and $O(G)$ the largest normal subgroup of G of odd order. Let K be the subgroup generated by the involutions of G . Then G is 3-pyramidal if and only if one of the following holds.

- (1) G is isomorphic to $S_3 \times H$ where H is a group of odd order.
- (2) $O(G) \leq C_G(K)$ and $G/O(G)$ is isomorphic to $N \rtimes A$ where N is the Suzuki 2-group of order 64 and A is a subgroup of $\text{Aut}(N)$ of order 3 or 15.
- (3) $O(G) \leq C_G(K)$ and $G/O(G)$ is isomorphic to $(C_{2^n} \times C_{2^n}) \rtimes A$ where A is the cyclic group of order 3 generated by the automorphism $(a, b) \mapsto (b, (ab)^{-1})$.

In item (1) $K \cong S_3$ while in items (2), (3) $K \cong C_2 \times C_2$.

The following general question is interesting: if m is an odd positive integer, what are the values of v such that there exists an m -pyramidal Kirkman triple system KTS on v vertices? Of course, if an m -pyramidal Kirkman triple system is realized under a group G , then G is m -pyramidal. Moreover, the number of vertices is $|G| + m$. However it is important to observe that the converse is not true. For example, if n is any positive integer, then $G = S_3 \times C_{4n+3}$ is a 3-pyramidal group not associated to any 3-pyramidal STS (see [1, Theorem 3.4(iii)]: such a STS should have $|G| + 3 = 24n + 21$ vertices), and so in particular it is not associated to any 3-pyramidal KTS. Despite this, it is still interesting to study the orders of the m -pyramidal groups and also the values of the integers m such that there exist m -pyramidal groups with some prescribed property. In [2], the following theorem was proved:

Theorem (S. Bonvicini, M. Buratti, M. Garonzi, G. Rinaldi, T. Traetta, 2021). There exists a 3-pyramidal group of order n if and only if $n \equiv 6 \pmod{12}$ or $n = 4^\alpha m$ with $\alpha > 0$ and $m \equiv 3 \pmod{6}$.

Let m be an odd positive integer and let X_m be the set of orders of m -pyramidal groups. In the following Theorem D we generalize the above result and we concentrate on the case in which $m \neq 7$ is a prime number. The orders of the m -pyramidal groups, where $m \neq 7$ is a prime number, were determined in [9].

Theorem D (X. Gao, M. Garonzi). Let $m \neq 7$ be an odd prime number. If m has the form $2^n - 1$ for some integer n , set $Y_m = \{2^a \cdot m \cdot d : n|a, d \text{ odd}\}$, otherwise $Y_m = \emptyset$. Write $m - 1 = 2^t \cdot r$ with r odd and let $Z_m = \{2^a \cdot m \cdot d : 1 \leq a \leq t, d \text{ odd}\}$. Then $X_m = Y_m \cup Z_m$.

Groups and quantities are closely connected. Some important properties of a group can be determined by its order, such as the groups of order 15 being cyclic, the groups of order p^2 being abelian, and the groups of order 135 being nilpotent. The second topic of this thesis concerns the influence of quantity relations on properties of groups. Specifically, we

focus on the impact of the number of cyclic (resp. maximal cyclic) subgroups of a group on its structure. In fact, the influence of the number of cyclic (resp. maximal cyclic) subgroups is an active topic of research (e.g. [12, 13, 14, 15, 16, 17, 18, 19, 21, 22, 23]). In Chapter 5 we discuss the influence of the number of cyclic (resp. maximal cyclic) subgroups of finite groups on their structure.

If X is an arbitrary subset of a group G , define

$$c(X) := \sum_{x \in X} \frac{1}{\varphi(o(x))} \quad (1)$$

where $o(x)$ denotes the order of x and φ is Euler's totient function. Since a cyclic group of order n has $\varphi(n)$ generators, the number of cyclic subgroups of G is precisely equal to $c(G)$. More generally, if whenever $x \in X$ and k is an integer coprime to $o(x)$ we have $x^k \in X$, then $c(X)$ equals the size of the set $\{\langle x \rangle : x \in X\}$, where $\langle x \rangle$ is the cyclic subgroup generated by x .

It is easy to see that $c(G) = |G|$ if and only if G is an elementary abelian 2-group. M. Tărnăuceanu was inspired by this result, and in [13] he classified the finite groups with $c(G) = |G| - 1$. In the same article, he proposed the following open question:

Open question. Classify the groups G with $c(G) = n$ for a given n .

M. Garonzi and I. Lima [12] proved that for any $r > 0$ if G has exactly $|G| - r$ cyclic subgroups, then $|G| \leq 8r$, therefore the number of such G is finite. Moreover, we can use the computer program GAP [20] to find all G with exactly $|G| - r$ cyclic subgroups for small values of r .

E. Haghi and A. R. Ashrafi [24, 19] gave a classification of finite groups with n cyclic subgroups, where $2 \leq n \leq 10$, K. Sharma and A.S. Reddy [25] classified the finite groups with 11 cyclic subgroups (see Lemma 5.1.7). In particular, E. Haghi and A. R. Ashrafi [24] proved the following result:

Theorem (E. Haghi and A. R. Ashrafi, 2018). Let G be a finite group with $c(G) < 32$. Then G is solvable.

Another relevant quantity is the number of maximal cyclic subgroups, denoted by $\lambda(G)$ (introduced by J. R. Rogerio in [21]). A subgroup H of G is called a *maximal cyclic subgroup* of G if it is maximal, with respect to inclusion, in the family of the cyclic subgroups of G . In other words H is cyclic and it is not properly contained in any cyclic subgroup of G . Using the fact that every cyclic subgroup is contained in a maximal cyclic subgroup, it is easy to see that a finite group G is cyclic if and only if $\lambda(G) = 1$.

A *covering* of G is a family $\mathcal{H} = \{H_1, \dots, H_k\}$ of proper subgroups of G whose union is G . Note that G admits a covering if and only if G is noncyclic. The covering \mathcal{H} of G is called *irredundant* if $\mathcal{H} \setminus \{H_i\}$ is not a covering for all $i \in \{1, \dots, k\}$. In other words, \mathcal{H} is irredundant if and only if no proper subfamily of \mathcal{H} is a covering.

It is easy to see that, if G is noncyclic, then the maximal cyclic subgroups of G form an irredundant covering.

The study of coverings of a group by its subgroups dates back to 1926, when G. Scorza [26] proved that a group G admits an irredundant covering by 3 subgroups if and only if it has a normal subgroup N such that $G/N \cong C_2 \times C_2$. Since then, several authors have been working on problems involving group coverings in various settings. In [27], J. H. E. Cohn defined $\sigma(G)$ to be the minimal size of an irredundant covering of the noncyclic group G . A number of results were proved for solvable groups leading to the conjecture that if G is a noncyclic solvable group then $\sigma(G) = p^a + 1$, where p^a is the order of a particular chief factor of G . It was also conjectured that there is no group G for which $\sigma(G) = 7$. Both of these conjectures were later proved by M. Tomkinson in [28]. More recently, A. Abdollahi et al. [29] gave a complete classification of the groups with $\sigma(G) = 6$, while J. Zhang [30] proved the non-existence of finite groups with $\sigma(G) = 11, 13$ and showed that $\sigma(\text{PSL}(2, 7)) = 15$. Other papers that contributed to this theory of minimal coverings over the last decades are [31, 32, 33, 34] and [35].

In [36], R. Brodie considered a slightly different problem. He classified the groups G that have exactly one irredundant covering by proper subgroups (see also [37, 21] for more details). J. R. Rogério [21] first defined another extremal variant of the covering problem. For a group G , define the function $\lambda(G)$ as the maximal size of an irredundant covering of G . This function has received attention in recent years, see [21, 22, 23]. By [21, Proposition 4], if G is noncyclic, then the maximal size of an irredundant covering of G equals the number of maximal cyclic subgroups of G . In this thesis, if G is a cyclic group, we set $\lambda(G) = 1$, so that $\lambda(G)$ always coincides with the number of maximal cyclic subgroups of G .

In [21, 22], J. R. Rogério, R. Bastos, and I. Lima classified the finite groups G with $\lambda(G) = 3, 4, 5, 6$. Furthermore, they [22] provided a solvability criterion for a group G in terms of the $\lambda(G)$ as follows:

Theorem (R. Bastos, I. Lima, J. R. Rogério, 2020). Let G be a group with $\lambda(G) \leq 30$. Then G is solvable.

We say that an element $x \in G$ is *primitive* if $\langle x \rangle$ is a maximal cyclic subgroup of G . Equivalently, the element $x \in G$ is primitive if whenever x is a power of an element $y \in G$, the element y is a power of x .

Let P be the set of primitive elements of G . It is easy to show that G has precisely $c(P)$ maximal cyclic subgroups, in other words $\lambda(G) = c(P)$. For example, if G is a p -group (for some prime number p) then $\lambda(G) = c(G) - c(G^p)$, where $G^p = \{g^p : g \in G\}$ is the set of non-primitive elements.

Assume A and B are groups of coprime orders. Then $c(A \times B) = c(A) \cdot c(B)$ and $\lambda(A \times B) = \lambda(A) \cdot \lambda(B)$. This can also be proved by using (1). Specifically, in the case of λ , an element $(a, b) \in A \times B$ is primitive in $A \times B$ if and only if a is primitive in A and b

is primitive in B (see Lemma 5.1.10).

We give some examples. If G is a cyclic p -group of order p^n (where p is a prime number), then $c(G) = n + 1$ and $\lambda(G) = 1$. As an easy but less trivial example, consider $G = D_{2n}$, the dihedral group of order $2n$. The maximal cyclic subgroups of G are the non-normal subgroups of order 2 and the unique cyclic subgroup of order n , so that $\lambda(G) = n + 1$. On the other hand $c(G) = n + d(n)$ where $d(n)$ is the number of positive divisors of n . If $m \geq 4$ is an integer, there exists a noncyclic (abelian) finite group G with $c(G) = m$. Indeed we can write $m - 2 = np$ for some prime p and some integer $n \geq 1$ and $c(C_p \times C_{p^n}) = np + 2 = m$ by Lemma 5.1.12.

A natural question is the following: what does $\lambda(G)$ bound? Using a result of L. Pyber [61] about noncommuting elements, we prove that the index of the center $|G : Z(G)|$ can be bounded above in terms of $\lambda(G)$ (see Proposition 5.1.5). In particular, the Fitting length and the derived length of a solvable group can be bounded above in terms of $\lambda(G)$. The same is true for the nilpotency class of a nilpotent group. Concerning the derived length, we prove the following in Section 5.2. It was proved in [10].

Theorem E (X. Gao, M. Garonzi). If G is any finite solvable group then the derived length of G is at most $2 + \frac{5}{2} \log_3(\lambda(G))$.

We say that a family of groups is *(maximal) cyclic bounded ((M)CB)* if, for every natural number n , there are only finitely many groups G in the family (up to isomorphism) with at most n (maximal) cyclic subgroups. In other words, a family \mathcal{F} of groups is CB (resp. MCB) if, for every natural number n , there are only finitely many groups G in \mathcal{F} (up to isomorphism) such that $c(G) \leq n$ (resp. $\lambda(G) \leq n$).

We give some examples:

- The family of dihedral groups is MCB since $\lambda(D_{2n}) = n + 1$.
- The family of all finite groups is not CB since $c(C_p) = 2$ for all prime p .
- The family of cyclic 2-groups is CB but not MCB since $\lambda(C_{2^n}) = 1$ and $c(C_{2^n}) = n + 1$.

In particular, not every CB family is MCB. On the other hand, since $\lambda(G) \leq c(G)$, every MCB family is CB.

In Section 5.3 we prove the following. It was proved in [10].

Theorem F (X. Gao, M. Garonzi). The following statements hold.

- (1) The family of noncyclic groups of prime power order is MCB. More precisely, if G is a noncyclic finite p -group and $t = \lambda(G)$ then $|G| \leq c^t \cdot t^{t^2}$ for some constant c .

- (2) The family of groups G such that every nontrivial Sylow subgroup of the center $Z(G)$ is noncyclic is MCB. In particular, the family of groups with trivial center is MCB.

Let \mathcal{B} be the set of positive integers n such that there are only finitely many finite noncyclic groups with precisely n cyclic subgroups. From the work of Ashrafi and Haghi [19, 24] (see also [18] and [17]) we immediately deduce that $3, 4, 5, 6, 7, 9 \in \mathcal{B}$ and $8, 10 \notin \mathcal{B}$. These papers have as objective to classify the groups with a given number of cyclic subgroups. It is interesting to observe that, in all known results, there are only finitely many noncyclic groups whose number of cyclic subgroups is a given prime number, in other words it seems that \mathcal{B} contains all the prime numbers. We confirm this in the following theorem, which was proved in Section 5.4. It was proved in [10].

Theorem G (X. Gao, M. Garonzi). $\mathcal{B} = \{1, 4, 6, 9\} \cup \mathcal{P}$ where \mathcal{P} is the set of prime numbers.

Chapter 1

Preliminaries

In the first chapter, we will introduce some fundamental concepts and results of group theory that are applied in this thesis.

1.1 General theory and results

Definition 1.1.1. Let Ω be a non-empty set, whose elements are called points. S_Ω denotes the symmetric group on Ω . The action of a group G on Ω , denoted by φ , refers to a homomorphism from G to S_Ω . Specifically, for every element $x \in G$, there is a corresponding transformation $\varphi(x) : \alpha \mapsto \alpha^x$ on Ω , satisfying the condition

$$(\alpha^x)^y = \alpha^{xy} \quad \text{for } x, y \in G, \alpha \in \Omega;$$

or

$$\varphi(xy) = \varphi(x)\varphi(y) \quad \text{for } x, y \in G.$$

The stabilizer of $\alpha \in \Omega$, also called point stabilizer, is

$$G_\alpha = \text{Stab}_G(\alpha) = \{g \in G : \alpha^g = \alpha\}.$$

The kernel of this action equals the intersection of all point stabilizers, namely,

$$\begin{aligned} \text{Ker}(\varphi) &= \{g \in G : \varphi(g) = 1_{S_\Omega}\} \\ &= \{g \in G : \alpha^g = \alpha, \quad \forall \alpha \in \Omega\} = \bigcap_{\alpha \in \Omega} G_\alpha. \end{aligned}$$

The action φ of G on Ω is said to be faithful if $\text{Ker}(\varphi) = \{1\}$. It is called trivial if $\text{Ker}(\varphi) = G$, and it is called transitive if for any two elements α, β of Ω , there exists $g \in G$ such that $\alpha^g = \beta$. For $\alpha \in \Omega$,

$$\alpha^G = \{\alpha^g : g \in G\}$$

is the orbit that contains α , it is called G -orbit of α . It is easy to get that

$$|\alpha^G| = |G : G_\alpha| \quad \text{for } \alpha \in \Omega.$$

In particular, the length $|\alpha^G|$ of the orbit α^G is a divisor of $|G|$.

Example 1.1.2. Let H be a subgroup of a group G and let Ω be the set of all right cosets of H in G . For each $x \in G$, we define an action φ of G on Ω as follows:

$$\varphi(x) : Hg \mapsto Hgx, \quad \forall Hg \in \Omega.$$

It is easy to see that G acts transitively on Ω because for any Hg_1, Hg_2 in Ω , there exists $g_1^{-1}g_2 \in G$ such that $Hg_1(g_1^{-1}g_2) = Hg_2$. The stabilizer of Hg is H^g , and the kernel of this action is

$$H_G = \bigcap_{g \in G} H^g.$$

H_G is called the normal core of H in G . In other words, it is the largest normal subgroup of G contained in H . We say that H is a core-free subgroup of G if $H_G = \{1\}$.

Definition 1.1.3. Let $G \leq S_\Omega$ and let k be a positive integer not greater than $|\Omega|$. We say that G is k -transitive on Ω if, for any two ordered k -tuples of elements in Ω , denoted as

$$(i_1, i_2, \dots, i_k) \quad \text{and} \quad (j_1, j_2, \dots, j_k),$$

there exists an element $g \in G$ such that $i_s^g = j_s$, where $s = 1, 2, \dots, k$.

Note that if $G \leq S_\Omega$ is k -transitive for some $k \geq 2$, then it is also $(k-1)$ -transitive. For example, the symmetric group S_n is n -transitive, and the alternating group A_n is an $(n-2)$ -transitive group.

Lemma 1.1.4. Assume G acts transitively on Ω and $1 < k \leq |\Omega|$. Then G is k -transitive on Ω if and only if the stabilizer G_α of α in G is $(k-1)$ -transitive on $\Omega \setminus \{\alpha\}$, where $\alpha \in \Omega$.

Proof. We first suppose that G is k -transitive on Ω . For any two ordered $(k-1)$ -tuples

$$(i_2, i_3, \dots, i_k) \quad \text{and} \quad (j_2, j_3, \dots, j_k)$$

of elements in $\Omega \setminus \{\alpha\}$. The element $g \in G_\alpha$ that transforms

$$(\alpha, i_2, i_3, \dots, i_k) \quad \text{to} \quad (\alpha, j_2, j_3, \dots, j_k)$$

naturally satisfies transforming (i_2, i_3, \dots, i_k) to (j_2, j_3, \dots, j_k) . Thus G_α is $(k-1)$ -transitive on $\Omega \setminus \{\alpha\}$.

Conversely, let

$$(i_1, i_2, \dots, i_k) \quad \text{and} \quad (j_1, j_2, \dots, j_k)$$

be two ordered k -tuples of elements in Ω . Since G acts transitively on Ω , there exists $h \in G$ such that $i_1^h = j_1$, and

$$i_2^h = j_2', \dots, i_k^h = j_k'.$$

Since G_{j_1} is $(k-1)$ transitive on $\Omega \setminus \{j_1\}$, there is $l \in G_{j_1}$ such that

$$(j_2')^l = j_2, \dots, (j_k')^l = j_k.$$

Write $g = hl$, then

$$i_1^g = j_1, i_2^g = j_2, \dots, i_k^g = j_k.$$

Therefore, G is k -transitive on Ω . □

Recall the *direct product*

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

with identity element $1_{G \times H} = (1_G, 1_H)$ and group operations

$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2),$$

$$(g, h)^{-1} = (g^{-1}, h^{-1}).$$

Recall also the *semidirect product* $G \rtimes H$ or $G :_{\phi} H$, where $\phi : H \rightarrow \text{Aut}(G)$ describes an action of H on G . We define

$$G \rtimes H = \{(g, h) : g \in G, h \in H\}$$

with identity element $1_{G \rtimes H} = (1_G, 1_H)$ and group operations

$$(g_1, h_1)(g_2, h_2) = (g_1g_2^{\phi(h_1^{-1})}, h_1h_2),$$

$$(g, h)^{-1} = ((g^{-1})^{\phi(h)}, h^{-1}).$$

The above Lemma 1.1.4 shows that if G acts transitively on Ω , then G is 2-transitive on Ω if and only if G_{α} is transitive on $\Omega \setminus \{\alpha\}$. Now we use this property to prove the following result:

Lemma 1.1.5. *Let $V = \mathbb{F}_p^n$ and let H be a subgroup of $\text{GL}(V)$. The semidirect product $G = V \rtimes H$ acts naturally (and transitively) on the right cosets of H in G . This action is 2-transitive if and only if H acts transitively on $V \setminus \{0\}$.*

Proof. Let

$$\Omega := \{Hv : v \in V\}$$

be the set on which G acts. Recall that the stabilizer $\text{Stab}_G(H)$ of H is H . In the light of Lemma 1.1.4, saying that this action is 2-transitive is equivalent to saying that there

exists $\alpha \in \Omega$ such that the action of $\text{Stab}_G(\alpha)$ on $\Omega \setminus \{\alpha\}$ is transitive. Equivalently, H acts transitively on $\Omega \setminus \{H\}$. In other words, for all $v, w \in V$ with $v \neq 0 \neq w$, there exists $h \in H$ such that $Hvh = Hw$. Equivalently, for every two nonzero vectors $v, w \in V$ there exists $h \in H$ such that $vhw^{-1} \in H$. This condition is equivalent to $h^{-1}vhw^{-1} \in H$ and, since $V \trianglelefteq G$ and $V \cap H = \{1\}$, $h^{-1}vhw^{-1} = \{1\}$, this is equivalent to saying that $v^h = w$. \square

For 2-transitive groups, we have the following results, which can be found in [41].

Theorem 1.1.6 (Theorem 4.3 of [41]). *Let N be a minimal normal subgroup of a finite 2-transitive group G acting on Ω . Then N is either elementary abelian or simple.*

Theorem 1.1.7 (Theorem 4.11 of [41]). *The finite 2-transitive groups are explicitly known. In particular, if $k \geq 6$ then the only finite k -transitive groups are symmetric group S_k and alternating group A_{k+2} , the only finite 5-transitive groups are symmetric group S_5 , alternating group A_7 , M_{12} and M_{24} , and the only finite 4-transitive groups are symmetric group S_4 and alternating groups A_6 and the Mathieu groups M_{11} , M_{12} , M_{23} and M_{24} .*

In fact, a finite 2-transitive group has a unique minimal normal subgroup. Moreover, the classification of finite 2-transitive groups can be found in [41, Tables 7.3 and 7.4]. Now, we provide Tables 7.3 and 7.4 from [41], which correspond to Tables 1.1 and 1.2 in this thesis.

Degree	$H = G_0$	Condition	No. of actions
q^d	$\text{SL}(d, q) \trianglelefteq H \leq \Gamma\text{L}(d, q)$		up to q if q even, $d = 2$ 2 if $(d, q) = (3, 2)$ up to q if q even
q^{2d}	$\text{Sp}(d, q) \trianglelefteq H$	$d \geq 2$	up to q if q even
q^6	$G_2(q) \trianglelefteq H$	q even	up to q
q	$(2^{1+2} \rtimes 3) = \text{SL}(2, 3) \trianglelefteq H$	$q = 5^2, 7^2, 11^2, 23^2$	1
q	$2^{1+4} \trianglelefteq H$	$q = 3^4$	1
q	$\text{SL}(2, 5) \trianglelefteq H$	$q = 11^2, 19^2, 29^2, 59^2$	1
2^4	A_6		2
2^4	A_7		1
2^6	$\text{PSU}(3, 3)$		2
3^6	$\text{SL}(2, 13)$		1

Table 1.1: Affine 2-transitive groups.

Remark: Table 1.1 lists the finite 2-transitive groups with elementary abelian socle. The order of the socle of such groups is equal to their degree n ($n = p^m$ and p is prime). The stabiliser $G_0 = H$ of the origin is a subgroup of $\text{GL}(m, p)$ and it acts transitively on $\text{soc}(G) \setminus \{0\}$. The meanings of remaining symbols in Table 1.1 and detailed information on the 2-transitive groups can be found in [41, Page 194].

n	Condition	N	$\max G/N $	No. of actions
n	$n \geq 5$	A_n	2	2 if $n = 6$ 1 otherwise
$(q^d - 1)/(q - 1)$	$d \geq 2$ $(d, q) \neq (2, 2), (2, 3)$	$\text{PSL}(d, q)$	$(d, q - 1)e$	2 if $d > 2$ 1 otherwise
$2^{2d-1} + 2^{d-1}$	$d \geq 3$	$\text{Sp}(2d, 2)$	1	1
$2^{2d-1} - 2^{d-1}$	$d \geq 3$	$\text{Sp}(2d, 2)$	1	1
$q^3 + 1$	$q \geq 3$	$\text{PSU}(3, q)$	$(3, q + 1)e$	1
$q^2 + 1$	$q = 2^{2d+1} > 2$	$Sz(q)$	$2d + 1$	1
$q^3 + 1$	$q = 3^{2d+1} > 3$	$R_1(q)$	$2d + 1$	1
11		$\text{PSL}(2, 11)$	1	2
11		M_{11}	1	1
12		M_{11}	1	1
12		M_{12}	1	2
15		A_7	1	2
22		M_{22}	2	1
23		M_{23}	1	1
24		M_{24}	1	1
28		$\text{PSL}(2, 8)$	3	1
176		Hs	1	2
276		Co_3	1	1

Table 1.2: Almost-simple 2-transitive groups.

Remark: Table 1.2 lists the finite 2-transitive groups G with simple socle N , n being the degree. The final column gives the number of non-isomorphic actions. (For example, for $\text{PSL}(d, q)$, $d > 2$, these actions are on the points and hyperplanes of the projective space.)

The primitive permutation groups play an important role in the proof of Theorem A. We would like to introduce the definition, classification, and important properties of primitive groups.

Definition 1.1.8 (Primitive group). *We say that a finite group G is primitive of degree n if it admits a maximal subgroup M of index n whose normal core M_G is trivial, i.e., $M_G = \{1\}$. In other words, M is a core-free maximal subgroup.*

Let M be a maximal subgroup of G , it is easy to see that M/M_G is a core-free maximal subgroup of the quotient group G/M_G because

$$(M/M_G)_{G/M_G} = \bigcap_{gM_G \in G/M_G} (M/M_G)^{gM_G} = \left(\bigcap_{g \in G} M^g \right) / M_G = M_G / M_G.$$

Thus G/M_G is a primitive group of degree $|G : M|$.

It is known that the concept of a primitive group has another equivalent definition. We refer the reader to [38] for more details. Let Ω be a non-empty set and $G \leq S_\Omega$. A block B of G is a subset of Ω such that either $Bg = B$ or $Bg \cap B = \emptyset$, for any $g \in G$. Observe that \emptyset , Ω and any subset with a single element $\{\omega\}$, for $\omega \in \Omega$ are blocks, which are called *trivial blocks*.

Definition 1.1.9. *A faithful transitive permutation representation of a group G is said to be primitive if it does not have non-trivial blocks. A primitive group is a group which possesses a primitive permutation representation.*

If H is a subgroup of G , a subgroup K of G is called a *supplement* of H in G if $G = HK$. In particular, we say that K is a *complement* of H in G if $G = HK$ and $H \cap K = \{1\}$.

The Schur-Zassenhaus theorem is a famous theorem related to complements. It states the following:

Theorem 1.1.10 (Schur-Zassenhaus). *Let G be a group and H a normal subgroup of G such that $(|H|, |G/H|) = 1$. Then*

- (1) H has a complement in G .
- (2) If H or G/H is solvable, then all such complements are conjugate in G .

Note that $(|H|, |G/H|) = 1$, so either $|H|$ or $|G/H|$ is odd. In the light of Feit-Thompson theorem, groups of odd order are necessarily solvable, thus the solvability condition in item (2) is always satisfied. H is a Hall π -subgroup of G , where π is the set of prime divisors of $|H|$. Moreover, all π -elements of G are contained in H because otherwise there would exist a π -element x of G such that $x \in G \setminus H$, and then xH would be a π -element of G/H since $o(xH)$ divides $o(x)$, contradicting the fact that $(|H|, |G/H|) = 1$. Therefore H is the unique subgroup of G of a given order $|H|$, so H is a characteristic subgroup of G .

A normal subgroup $N \neq \{1\}$ of G is a *minimal normal subgroup* of G if $\{1\}$ and N are the only normal subgroups of G that are contained in N . It is evident that every nontrivial finite group possesses minimal normal subgroups. Moreover, any nontrivial finite group is either simple or contains a proper minimal normal subgroup. It is well-known that a minimal normal subgroup N of a finite group is a direct product of mutually isomorphic simple groups (see [39, Theorem 5 of Chapter 4]). Thus, if N is solvable, then N is isomorphic to C_p^n , where p is a prime and n is an integer, and if N is nonsolvable, then N is isomorphic to S^n , where S is a nonabelian simple group and n is an integer.

Let M and N be two distinct minimal normal subgroups of G , then $M \cap N$ is also normal in G . By the minimality of M and N , we can get $M \cap N = \{1\}$. For any $m \in M$, $n \in N$, we have $m^{-1}n^{-1}mn \in M \cap N = \{1\}$ since M and N are normal subgroups of G . Therefore $mn = nm$, and hence $[M, N] = \{1\}$.

Recall that the *socle* of a finite group G , denoted by $\text{soc}(G)$, is the subgroup of G generated by the minimal normal subgroups of G . The following remarkable result, obtained by Baer, provides a classification for all primitive groups based on the structure of the socle of G (see [38]).

Theorem 1.1.11 (Baer). *(1) A group G is primitive if and only if there exists a subgroup M of G such that $G = MN$ for all minimal normal subgroups N of G .*

- (2) Let G be a primitive group. Assume that U is a core-free maximal subgroup of G and that N is a non-trivial normal subgroup of G . Write $C = C_G(N)$. Then $C \cap U = \{1\}$. Moreover, either $C = \{1\}$ or C is a minimal normal subgroup of G .
- (3) If G is a primitive group and U is a core-free maximal subgroup of G , then exactly one of the following statements holds:
- (a) $\text{soc}(G) = S$ is a self-centralising abelian minimal normal subgroup of G which is complemented by $U : G = US$ and $U \cap S = \{1\}$. In this case G is called affine or primitive of type I.
 - (b) $\text{soc}(G) = S$ is a nonabelian minimal normal subgroup of G which is supplemented by $U : G = US$. In this case $C_G(S) = \{1\}$ and G is called primitive of type II.
 - (c) $\text{soc}(G) = A \times B$, where A and B are the two unique minimal normal subgroups of G and both are complemented by $U : G = AU = BU$ and $A \cap U = B \cap U = A \cap B = \{1\}$. Moreover, $A = C_G(B)$, $B = C_G(A)$, and A , B and $AB \cap U$ are nonabelian isomorphic groups. In this case G is called primitive of type III.

Definition 1.1.12. A group G is called almost-simple if it admits a nonabelian simple normal subgroup S such that $C_G(S) = \{1\}$.

To say that G is an almost-simple group is equivalent to saying that there exists a nonabelian simple group S such that $S \leq G \leq \text{Aut}(S)$. Indeed, assume that G is an almost-simple group as described in Definition 1.1.12. Then the natural homomorphism $G \rightarrow \text{Aut}(S)$ has kernel equal to $C_G(S) = \{1\}$, hence $G \lesssim \text{Aut}(S)$, this implies that $S \leq G \lesssim \text{Aut}(S)$. Observe that $Z(S) = \{1\}$, so we can identify S with the inner automorphism group $\text{Inn}(S)$ and write $S \leq \text{Aut}(S)$. In particular, it is obvious that $\text{soc}(G) = S$ because otherwise there would exist a minimal normal subgroup L of G distinct from S , and then $L \leq C_G(S) = \{1\}$, a contradiction. Conversely, let G be a finite group admitting a nonabelian simple subgroup S such that $S \leq G \leq \text{Aut}(S)$. Since $\text{Aut}(S)$ acts faithfully on S , $C_G(S) \leq C_{\text{Aut}(S)}(S) = \{1\}$, and thus $C_G(S) = \{1\}$, this proves that G admits a nonabelian simple normal subgroup S such that $C_G(S) = \{1\}$. Therefore, G is an almost-simple group.

Let G be an almost-simple group with $\text{soc}(G) = S$, and let M be a maximal subgroup of G such that $S \not\leq M$. We claim that M is a core-free maximal subgroup of G . Suppose for a contradiction that $K := M_G$ is not trivial. Since S and K are normal subgroups of G , so is $K \cap S$. As S is the (unique) minimal normal subgroup of G , either $K \cap S = S$ or $K \cap S = \{1\}$. The former case does not hold, as otherwise $S \leq K$, contradicting $S \not\leq M$. Hence $K \cap S = \{1\}$. Thus $s^{-1}k^{-1}sk \in S \cap K = \{1\}$ for any $s \in S$, $k \in K$. It follows that $K \leq C_G(S) = \{1\}$, which is a contradiction. This establishes the claim. Therefore, G is a primitive group of type II.

Now suppose that H is a permutation group acting on $\Omega = \{1, \dots, n\}$. Define

$$G^n = G \times G \times \dots \times G = \{(g_1, \dots, g_n) : g_i \in G\},$$

the direct product of n copies of G , and let H act on G^n by permuting the n subscripts. That is $\phi : H \rightarrow \text{Aut}(G^n)$ is defined by

$$(g_1, \dots, g_n)^{\phi(h)} \mapsto (g_{1h^{-1}}, \dots, g_{nh^{-1}}), \quad \forall h \in H.$$

Then the *wreath product* $G \wr H$ is defined to be $G^n :_{\phi} H$. An element of $G \wr H$ can be written as

$$(g_1, \dots, g_n)h \text{ with } g_i \in G, h \in H$$

and the multiplication in $G \wr H$ is defined by

$$(g_1, \dots, g_n)h(g'_1, \dots, g'_n)h' = (g_1g'_{1h}, \dots, g_ng'_{nh})hh'.$$

Let G be a group, let A and B be subgroups of G , and $K = A \cap B$. G is called the *central product* of A and B with respect to K , denoted by $G = A \circ B$, if $G = AB$ and $[A, B] = \{1\}$. Obviously, A and B are normal subgroups of G and $K \leq Z(G)$. In particular, if $A \cap B = \{1\}$ then $A \circ B = A \times B$.

Let $H \leq G$ and $S \subseteq G$. Then S is a *transversal* of H in G (or *set of right coset representatives* for H in G) if S contains exactly one element of every right coset Hx , $x \in G$; and S is a *left transversal* of H in G if S contains exactly one element of every left coset of H in G .

The following two lemmas can be found in [40]. Lemma 1.1.13 is due to Frobenius. Lemma 1.1.14 is particularly important for the proof of Theorem A.

Lemma 1.1.13 (Embedding Argument). *Let H be a subgroup of the finite group G , let x_1, \dots, x_n be a right transversal for H in G , and let ξ be any homomorphism with domain H , say $\xi : H \rightarrow X$. Then the map*

$$f : G \rightarrow \xi(H) \wr S_n,$$

$$x \mapsto (\xi(x_1xx_{1\pi}^{-1}), \dots, \xi(x_nxx_{n\pi}^{-1}))\pi,$$

where $\pi \in S_n$ is the unique permutation that satisfies $x_i x \in Hx_{i\pi}$ for all $i = 1, \dots, n$, is a well-defined homomorphism with kernel equal to the normal core of $\text{Ker}(\xi)$ in G , in other words $\text{Ker}(f) = (\text{Ker}(\xi))_G$.

Lemma 1.1.14. *Let G be a finite primitive group of type II with socle S^m for some positive integer m and nonabelian simple group S . Then there exists an almost-simple group X with socle S and a transitive group $K \leq S_m$ such that G is isomorphic to a subgroup of $X \wr K$ containing S^m and the restriction of the natural projection $G \rightarrow K$ is surjective.*

Proof. Write

$$S^m = T_1 \times T_2 \times \dots \times T_m$$

for the direct product of m copies T_1, \dots, T_m of S . Denote by R the first factor, that is,

$$R := T_1 \times \{1\} \times \dots \times \{1\}.$$

Let $N := N_G(R)$ and $C := C_G(R)$. Note that R and C are normal subgroups of N , so $RC/C \trianglelefteq N/C$. Since R is a nonabelian simple group, $R \cap C = Z(R) = \{1\}$, so that

$$RC/C \cong R/R \cap C = R.$$

Suppose $nC \in C_{N/C}(RC/C)$ where $n \in N$. Then $nCrC = rCnC$ for any $r \in R$, implying that $nrC = rnC$, that is $n^{-1}r^{-1}nr \in C$. Observe that $n^{-1}r^{-1}nr \in R$ since $R \trianglelefteq N$. Therefore,

$$n^{-1}r^{-1}nr \in C \cap R = \{1\},$$

and so $nr = rn$ for any $r \in R$, this implies that $n \in C$. Thus $C_{N/C}(RC/C) = C$, this means that N/C admits a nonabelian simple normal subgroup RC/C such that $C_{N/C}(RC/C)$ is trivial. Hence $X := N/C$ is an almost-simple group with socle $RC/C \cong S$.

We now apply the embedding argument to the natural homomorphism $\alpha : N \rightarrow \text{Aut}(R)$. Note that

$$\text{Ker}(\alpha) = \{n \in N : r^n = r, \forall r \in R\} = C_N(R) = N \cap C = C,$$

so $\alpha(N) \cong N/\text{Ker}(\alpha) = N/C = X$. Since S^m is a minimal normal subgroup of G , G acts transitively on the set of direct factors of S^m , this implies that $C^g = C_G(R^g)$ for any $g \in G$, thus the conjugates of C in G are precisely the centralizers of the direct factors of S^m , therefore an element belongs to the normal core $(\text{Ker}(\alpha))_G$ if and only if it centralizes all of the direct factors, in other words

$$(\text{Ker}(\alpha))_G = \bigcap_{g \in G} C^g = C_G(S^m) = \{1\}.$$

Let $\rho : G \rightarrow \text{Sym}(m)$ denote the conjugation action of G on

$$\Omega = \{R = R_1, R_2, \dots, R_m\},$$

where R_i is the i -th direct factor of S^m and $i \in \mathcal{I} = \{1, 2, \dots, m\}$. Since G acts transitively on Ω , it follows that

$$m = |R^G| = |G : \text{Stab}_G(R)| = |G : N|$$

and G also acts transitively on \mathcal{I} . By Lemma 1.1.13, G is isomorphic to a subgroup of $X \wr K$ where $K = \text{Im}(\rho)$ is a transitive subgroup of $\text{Sym}(m)$. Moreover, the kernel of the action ρ of G on Ω is

$$Y := \text{Ker}(\rho) = \bigcap_{i=1}^m N_G(R_i) = \bigcap_{g \in G} N^g.$$

Therefore, G/Y is isomorphic to a subgroup G^ρ of $\text{Sym}(m)$. In particular, $K = G^\rho$ and $R_{i^{x^\rho}} = R_i^x$ for $x \in G$ and $i \in \mathcal{I}$. Let M be a core-free maximal subgroup of G , then $G = MY$. This means that if τ is a permutation of \mathcal{I} in K , there exists an element $x \in M$ such that the conjugation by x permutes the R_i in the same way τ does: $R_{i^\tau} = R_i^x$, for all $i \in \mathcal{I}$. In other words, $x^\rho = \tau$. This is to say that the projection of M onto K is surjective. \square

Now we introduce the well-known O’Nan-Scott theorem, which gives us a classification of the maximal subgroups of the alternating and symmetric groups (see [42, Theorem 2.4]).

Theorem 1.1.15 (O’Nan-Scott Theorem). *If H is any proper subgroup of S_n other than A_n , then H is a subgroup of one or more of the following subgroups:*

- (1) *an intransitive group $S_k \times S_m$, where $n = k + m$.*
- (2) *an imprimitive group $S_k \wr S_m$, where $n = km$.*
- (3) *a primitive wreath product, $S_k \wr S_m$, where $n = k^m$.*
- (4) *an affine group $\text{AGL}(d, p) \cong p^d : \text{GL}(d, p)$, where $n = p^d$.*
- (5) *a group of shape $T^m \cdot (\text{Out}(T) \times S_m)$, where T is a nonabelian simple group, acting on the cosets of a subgroup $\text{Aut}(T) \times S_m$, where $n = |T|^{m-1}$.*
- (6) *an almost-simple group acting on the cosets of a core-free maximal subgroup of index n .*

The next result states a fact about the length of conjugacy class of finite simple group. It is Burnside’s Theorem (see [43, Theorem 31.3]).

Theorem 1.1.16 (Burnside Theorem). *Let p be a prime number and let r be an integer with $r \geq 1$. Suppose that G is a finite group with a conjugacy class of size p^r . Then G is not simple.*

Definition 1.1.17. *For any group G , we define the subgroups $Z_i(G)$ for $i = 0, 1, 2, \dots$ as follows (we abbreviate $Z_i(G) = Z_i$). Define $Z_0 = \{1\}$, and for $i > 0$, Z_i is the subgroup of G corresponding to $Z(G/Z_{i-1})$ by the Correspondence Theorem:*

$$Z_i/Z_{i-1} = Z(G/Z_{i-1}).$$

The sequence of subgroups

$$\{1\} = Z_0 \leq Z_1 \leq \dots \leq Z_n \leq \dots$$

is called the upper central series of G ; its i -th term Z_i is called the i -th center of G . A group G is said to be nilpotent if $Z_m(G) = G$ for some integer m ; in this case, the smallest integer c such that $Z_c(G) = G$ is called the nilpotent class of G .

Definition 1.1.18. *An abelian series of a group G is a normal series*

$$\{1\} \trianglelefteq G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G,$$

in which each factor G_{i+1}/G_i is abelian. If G has an abelian series, the length of the shortest abelian series in G is called the derived length of G .

Note that a group G is solvable if and only if it has an abelian series. In particular, a solvable group with derived length at most 2 is said to be *metabelian*. It is well-known that every nilpotent group is solvable, but a solvable group is not necessarily nilpotent.

If G is a finite group with a subgroup H such that $H \cap H^x = \{1\}$ for all x in $G \setminus H$, then

$$N = G - \bigcup_{g \in G} (H^g - \{1\})$$

is a normal subgroup of G such that $G = HN$ and $H \cap N = \{1\}$ (this is Frobenius' theorem, see 8.5.5 of [45]). A group G which has a proper nontrivial subgroup H with the above property is called a *Frobenius group*. H is called a *Frobenius complement* and N the *Frobenius kernel*.

Let $G = N \rtimes H$ be a Frobenius group with Frobenius kernel N . We know that the Frobenius kernel N is a nilpotent group, actually it is equal to the Fitting subgroup of G . This is a deep result that depends on Thompson's theorem about groups with fixed point free automorphisms of prime order, see 10.5.6 of [45]. Thus N is solvable. Moreover, the Frobenius complement H has the property that Sylow p -subgroups of H are cyclic when p is odd, and cyclic or generalized quaternion if $p = 2$.

We also need the following fact, which is Theorem 5.53 in [44].

Theorem 1.1.19 (I. N. Herstein). *Let G be a finite group admitting an abelian maximal subgroup H . Then G is solvable.*

Proof. Obviously, $H \leq N_G(H) \leq G$. If $H < N_G(H)$, then $N_G(H) = G$ by the maximality of H , it follows that H is a maximal normal subgroup of G . Thus G/H is isomorphic to a nonabelian simple group S or an abelian simple group C_p , where p is prime. Assume $G/H \cong S$. Since all nonabelian simple groups have nontrivial proper subgroups, there exists a subgroup M containing H such that

$$\{1\} \neq M/H < G/H \cong S$$

by the Correspondence Theorem, thus $H < M < G$, contradicting the maximality of H . Thus, $G/H \cong C_p$. Hence, H and G/H are both solvable, and so is G . Without loss of generality $N_G(H) = H$. If $H \cap H^x = \{1\}$ for all $x \in G \setminus H$, then G is a Frobenius group with H as its Frobenius complement. Let

$$N = G - \bigcup_{g \in G} (H^g - \{1\}),$$

then N is the normal kernel of G , and so $G/N \cong H$. Since N is nilpotent and H is abelian, G is solvable. Now we assume that there exists $x \in G \setminus H$ such that $B = H \cap H^x \neq \{1\}$. Then B is normal in both H and H^x because H and H^x are abelian subgroups, so that H and H^x are subgroups of $N_G(B)$, thus $H < N_G(B)$. Since H is a maximal subgroup of G , $N_G(B) = G$, and then $B \trianglelefteq G$. G/B contains the abelian maximal subgroup H/B , by induction on $|G|$, G/B is solvable, and B being solvable, so also is G . \square

Remark: If the hypothesis “ H abelian” is replaced by “ H nilpotent”, then the above Theorem 1.1.19 is not true in general. A deep result of J. G. Thompson allows one to establish solvability if the group admits a nilpotent maximal subgroup of odd order, the proof of this result can be found in [45, 10.4.2].

Let $a > 1$ be a natural number, and let n be an integer greater than 1. A *primitive prime divisor* of $a^n - 1$ is a prime number p such that $p \mid a^n - 1$ but $p \nmid a^i - 1$ for all $0 < i < n$.

Primitive prime divisors play an important role in group theory and number theory. Next, we will use Zsigmondy’s Theorem to prove Lemma 1.1.21, which is very helpful for this thesis.

Theorem 1.1.20 (Zsigmondy’s Theorem [47]). *Let a and n be integers greater than 1. Then there exists a prime divisor q of $a^n - 1$ such that q does not divide $a^j - 1$ for any $0 < j < n$, except exactly in the following cases:*

- (1) $n = 2$, $a = 2^s - 1$, where $s \geq 2$.
- (2) $n = 6$, $a = 2$.

A *Mersenne prime* is a prime number of the form $2^n - 1$ for some integer n . If n is a composite number then so is $2^n - 1$. Therefore, an equivalent definition of the Mersenne primes is that they are the prime numbers of the form $M_p = 2^p - 1$ for some prime p .

The following lemma shows, in particular, that prime powers of the form $2^n - 1$ are actually prime numbers.

Lemma 1.1.21. *If p is a prime number such that $p^k = a^n - 1$ for some integers $k \geq 1$ and $a, n > 1$, then one of the following holds.*

- (1) $(p, k, a, n) = (2, 3, 3, 2)$,
- (2) $a = 2$, $k = 1$ and n is a prime number.

Proof. Assume $n \notin \{2, 6\}$. Then Zsigmondy’s theorem 1.1.20 implies that $a^n - 1$ has a primitive prime divisor, which of course must be equal to p . It follows that p does not divide $a^j - 1$ for any j with $1 \leq j < n$. However, $p^k = a^n - 1$ is of course divisible by $a - 1$, so since p does not divide $a - 1$ we deduce that $a = 2$. Since if $n = 6$ then $a = 2$, this argument shows that either $a = 2$ or $n = 2$. If $n = 2$ then $p^k = (a - 1)(a + 1)$ implies that $(p, k, a, n) = (2, 3, 3, 2)$. Now assume that $a = 2$.

We have $p^k = 2^n - 1$ hence p is odd. We will prove that $k = 1$ and that n is a prime number. If $n = 2$ the claim is obvious, now assume $n \geq 3$. Since p is odd, it is congruent

to 1, 3, 5 or 7 modulo 8, so $p^2 \equiv 1 \pmod{8}$. On the other hand, $p^k = 2^n - 1 \equiv -1 \pmod{8}$ since $n \geq 3$. This implies that k is odd, hence we have a factorization

$$2^n = p^k + 1 = (p + 1)(p^{k-1} - p^{k-2} + \dots - p + 1)$$

The second factor is a sum of k odd integers, so it is odd. Since it divides 2^n , it must be equal to 1, so that $2^n = p + 1$ implying $k = 1$. We now prove that n is a prime number. Consider a factorization $n = rs$ with r, s positive integers and $s > 1$. We will prove that $r = 1$. Note that

$$p = 2^n - 1 = 2^{rs} - 1 = (2^r - 1)(1 + 2^r + \dots + 2^{r(s-1)})$$

implying that one of the two factors must equal 1. Since $s > 1$, the second factor is larger than 1, so $2^r - 1 = 1$, i.e. $r = 1$. \square

Definition 1.1.22. *A Fitting chain (or Fitting series or nilpotent series) for a group is a subnormal series*

$$\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \dots \trianglelefteq N_n = G$$

such that each factor N_{i+1}/N_i is nilpotent. The Fitting length or nilpotent length of a group is defined to be the smallest possible length of a Fitting chain, if one exists.

Note that the Fitting length (or nilpotent length) measures how far a solvable group is from being nilpotent.

As usual, we denote by $\Phi(G)$ the *Frattini subgroup* of G , which is the intersection of all the maximal subgroups of G . In particular, if $G = \{1\}$ then $\Phi(G) = \{1\}$. Moreover, the Frattini subgroup $\Phi(G)$ of a finite group G is nilpotent (see 5.2.5 of [52]), that is

$$\Phi(G) = P_1 \times P_2 \times \dots \times P_n,$$

where P_i is a Sylow p_i -subgroup of $\Phi(G)$ and $\{p_1, p_2, \dots, p_n\}$ is the set of all prime divisors of $|\Phi(G)|$. Thus P_i is a characteristic subgroup of $\Phi(G)$ for $i = 1, 2, \dots, n$. Moreover P_i is normal in G because $P_i \trianglelefteq_c \Phi(G) \trianglelefteq G$.

The following result can be found in [46].

Theorem 1.1.23 (Gaschütz's Theorem). *Let G be a finite group and $S_1(G)$ the product of all the abelian minimal normal subgroups of G . Then $\Phi(G) = 1$ if and only if G splits over $S_1(G)$.*

Now we introduce the following two frequently used results.

Theorem 1.1.24 (Theorem 6.11 of [11]). *Let P be a p -group containing at most one subgroup of order p . Then either P is cyclic, or else $p = 2$ and P is generalized quaternion.*

Let G be a finite group of even order and P a Sylow 2-subgroup of G . If P has a unique involution then P is a cyclic group or a generalized quaternion group by Theorem 1.1.24.

Theorem 1.1.25 (Corollary 5.14 of [11]). *Let P be a Sylow p -subgroup of G , where G is a finite group and p is the smallest prime divisor of $|G|$, and assume that P is cyclic. Then G has a normal p -complement.*

Theorem 1.1.25 shows that if G is a nonsolvable group then a Sylow 2-subgroup P of G is not a cyclic group. Indeed, assume that P is cyclic, then G has a normal 2-complement N by Theorem 1.1.25, it follows that $G \cong N \rtimes P$ and $|N|$ is odd. In the light of Feit-Thompson theorem N is solvable, thus G is solvable, a contradiction.

Lemma 1.1.26. *Let $G \cong C_p^n$ be an elementary abelian p -group where p is prime. Then $\text{Aut}(G) \cong \text{GL}(n, p)$.*

Proof. Note that C_p^n can be viewed as an n -dimensional vector space V over the finite field \mathbb{F}_p , and V is a group under addition. Since any \mathbb{F}_p -linear map is additive, $\text{GL}(n, p) \leq \text{Aut}(V)$. We now prove the other inclusion, in other words we prove that every automorphism of the additive group V is \mathbb{F}_p -linear. Let $\varphi \in \text{Aut}(V)$. If $a \in \mathbb{F}_p$ then we can write $a = 1 + 1 + \dots + 1$, so

$$\varphi(av) = \varphi((1 + 1 + \dots + 1)v) = \varphi(v + \dots + v) = a\varphi(v)$$

for any $v \in V$. Therefore, φ is a linear transformation on V , and then $\text{Aut}(V) \leq \text{GL}(n, p)$. \square

1.2 Some properties of primitive and almost-simple groups

Now we include some definitions and results about almost-simple groups that will be used in the proof of Theorem A. Definition 1.2.1 and Lemma 1.2.2, presented below, can be found in [8].

Definition 1.2.1. *Let G be an almost-simple group with socle S . The maximal subgroup H of S is G -ordinary if its G -class equals its S -class, in other words for any $g \in G$ there exists $s \in S$ such that $H^g = H^s$. We say that H is ordinary if it is $\text{Aut}(S)$ -ordinary.*

Note that, if $S \leq G \leq Y \leq \text{Aut}(S)$ and H is a Y -ordinary maximal subgroup of S , then H is also G -ordinary, so that ordinary maximal subgroup of S is G -ordinary for any almost-simple group G with socle S .

The $\text{Aut}(S)$ -class of H is a disjoint union of S -classes: there exist $\varphi_1, \dots, \varphi_c \in \text{Aut}(S)$ such that the subgroups $H^{\varphi_i} \leq S$ are pairwise not conjugate in S and for any $\varphi \in \text{Aut}(S)$

there exist $s \in S$, $i \in \{1, \dots, c\}$ such that $H^\varphi = H^{\varphi_i s}$. Let $C_i = \{H^{\varphi_i s} : s \in S\}$ be the S -class of H^{φ_i} , for $i = 1, \dots, c$. Then $\text{Aut}(S)$ acts transitively on the set $\{C_i : i = 1, \dots, c\}$ by sending (C_i, φ) to the S -class of $H^{\varphi_i \varphi}$. This corresponds to a homomorphism $\pi : \text{Aut}(S) \rightarrow \text{Sym}(c)$. Note that H is $\text{Aut}(S)$ -ordinary if and only if $c = 1$.

Lemma 1.2.2. *Let G be an almost-simple group with socle S , H a maximal subgroup of S , and π the map as defined in the previous paragraph.*

- (1) *If $G \leq \text{Ker}(\pi)$ then H is G -ordinary.*
- (2) *If G is normal in $\text{Aut}(S)$ and H is G -ordinary, then $G \leq \text{Ker}(\pi)$.*
- (3) *If $c = 2$ and G does not have C_2 as a quotient, then H is G -ordinary.*
- (4) *If H is G -ordinary, then $N_G(H)$ is a maximal subgroup of G and the intersection $N_G(H) \cap S$ is equal to H . Moreover, $|N_G(H)| = |G||H|/|S|$.*

Proof. Item 1. Assume $G \leq \text{Ker}(\pi)$ and let $g \in G$. Then H^g belongs to the S -class of H , so there is some $s \in S$ with $H^g = H^s$. This shows that H is G -ordinary.

Item 2. Assume that G is normal in $\text{Aut}(S)$, that H is G -ordinary and let $g \in G$. Then there is some $s \in S$ with $H^g = H^s$. If $i \in \{1, \dots, c\}$ then, since $\varphi_i g \varphi_i^{-1} \in G$, because $G \trianglelefteq \text{Aut}(S)$, there is some $s \in S$ with $H^{\varphi_i g \varphi_i^{-1}} = H^s$, therefore

$$H^{\varphi_i g} = H^{s \varphi_i} = H^{\varphi_i \varphi_i^{-1} s \varphi_i}$$

belongs to the S -class of H^{φ_i} since $S \trianglelefteq \text{Aut}(S)$.

Item 3. Let $N := \text{Ker}(\pi)$. Then

$$G/G \cap N \cong GN/N \leq \text{Aut}(S)/N \cong \text{Im}(\pi) \leq \text{Sym}(c).$$

In particular, if $c = 2$ then the index $|G : G \cap N|$ is 1 or 2. So if $c = 2$ and G does not have C_2 as a quotient then $|G : G \cap N| = 1$, i.e. $G \leq N = \text{Ker}(\pi)$. This implies that H is G -ordinary by item (1).

Item 4. Since H is G -ordinary, for every $g \in G$, there is $s \in S$ such that $H^g = H^s$, hence $H^{gs^{-1}} = H$, and hence $gs^{-1} \in N_G(H)$. Therefore $N_G(H)S = G$. Since H is not normal in G , G has a maximal subgroup M with $N_G(H) \leq M < G$, so that $MS = G$. Since $M \cap S \trianglelefteq M$ and $N_M(M \cap S) \leq N_G(M \cap S)$, the maximality of M in G implies that $N_G(M \cap S)$ is equal to one of M, G . Since

$$\{1\} \neq H \leq M \cap S < S$$

and S is a simple group, $M \cap S$ cannot be normal in G , so $N_G(M \cap S) = M$. Since $H \leq M \cap S < S$, the maximality of H in S implies that $M \cap S = H$. Therefore,

$$N_G(M \cap S) = N_G(H) = M$$

and

$$N_G(H) \cap S = M \cap S = H.$$

Finally, since $MS = G$, we have $|G| = |M||S|/|H|$, this implies that $|M| = |N_G(H)| = |G||H|/|S|$. \square

In fact, the ordinary maximal subgroups of the low-dimensional finite classical simple groups can be found in the tables provided in [48, Chapter 8]. For example: Table 1.3 and Table 1.4 correspond to Table 8.1 and Table 8.16 of [48], respectively. In those two tables, the definition of c is given above and the ordinary maximal subgroups of $\text{PSL}(2, q)$ and $\text{Sz}(q)$ are those groups corresponding to $c = 1$ in Tables 1.3 and 1.4. We will use these two tables to prove Lemma 1.2.7 and Theorem A.

\mathcal{C}_i	Subgp	Notes	c	Stab
\mathcal{C}_1	$E_q : (q-1)$		1	$\langle \delta, \phi \rangle$
\mathcal{C}_2	$Q_{2(q-1)}$	$q \neq 5, 7, 9, 11; q$ odd	1	$\langle \delta, \phi \rangle$
		$N1$ if $q = 7, 11$	1	$\langle \delta \rangle$
		$N2$ if $q = 9$	1	$\langle \delta, \phi \rangle$
\mathcal{C}_2	$D_{2(q-1)}$	q even	1	$\langle \phi \rangle$
\mathcal{C}_3	$Q_{2(q+1)}$	$q \neq 7, 9; q$ odd	1	$\langle \delta, \phi \rangle$
		$N1$ if $q = 7$	1	$\langle \delta \rangle$
		$N2$ if $q = 9$	1	$\langle \delta, \phi \rangle$
\mathcal{C}_3	$D_{2(q+1)}$	q even	1	$\langle \phi \rangle$
\mathcal{C}_5	$\text{SL}(2, q_0).2$	$q = q_0^2, q$ odd	2	$\langle \phi \rangle$
\mathcal{C}_5	$\text{SL}(2, q_0)$	$q = q_0^r, q$ odd, r odd prime	1	$\langle \delta, \phi \rangle$
\mathcal{C}_5	$\text{PSL}(2, q_0)$	$q = q_0^r, q$ even, $q_0 \neq 2, r$ prime	1	$\langle \phi \rangle$
\mathcal{C}_6	$2_-^{1+2}.S_3 \cong 2^- .S_4^-$	$q = p \equiv \pm 1 \pmod{8}$	2	1
	$2_-^{1+2} : 3 \cong 2^- .A_4$	$q = p \equiv \pm 3, 5, \pm 13 \pmod{40}$	1	$\langle \delta \rangle$
		$N1$ if $q = p \equiv \pm 11, \pm 19 \pmod{40}$	1	$\langle \delta \rangle$

$d := |Z(\text{SL}(2, q))| = (q-1, 2), |\delta| = d, |\phi| = e, q = p^e \geq 4.$

Table 1.3: The maximal subgroups of $\text{SL}(2, q)$ ($= \text{Sp}(2, q) \cong \text{SU}(2, q)$) of geometric type

\mathcal{C}_i	Suzuki	Subgp	Notes	c	Stab
\mathcal{C}_1	$H(q)$	$E_q^{1+1} : C_{q-1}$		1	$\langle \phi \rangle$
$\mathcal{C}_2/\mathcal{C}_1$	B_0	$D_{2(q-1)}$		1	$\langle \phi \rangle$
$\mathcal{C}_3/\mathcal{C}_8$	B_1 or B_2	$(q - \sqrt{2q} + 1) : 4$		1	$\langle \phi \rangle$
$\mathcal{C}_3/\mathcal{C}_8$	B_2 or B_1	$(q + \sqrt{2q} + 1) : 4$		1	$\langle \phi \rangle$
\mathcal{C}_5	$G(q_0)$	$\text{Sz}(q_0)$	$q = q_0^r, r$ prime, $q_0 \neq 2$	1	$\langle \phi \rangle$

$|Z(\text{Sz}(q))| = 1, |\phi| = e.$ Note that $\text{Sz}(2) \cong F_{20} \cong 5 : 4$ is soluble.

Table 1.4: The maximal subgroups of $\text{Sz}(q) < \text{Sp}(4, q), q = 2^e, e > 1$ odd.

Remark: The meaning of the notation in Tables 1.3 and 1.4 can be found in [48].

Recall that a nonabelian simple group is called a *minimal simple group* if its proper subgroups are solvable. J. G. Thompson [49] proved the following theorem.

Theorem 1.2.3 (J. G. Thompson). *Every minimal simple group is isomorphic to one of the following groups:*

- (1) $\text{PSL}(2, 2^r)$, r any prime.
- (2) $\text{PSL}(2, 3^r)$, r any odd prime.
- (3) $\text{PSL}(2, p)$, p any prime exceeding 3 such that $p^2 + 1 \equiv 0 \pmod{5}$.
- (4) $\text{Sz}(2^r)$, r any odd prime.
- (5) $\text{PSL}(3, 3)$.

D. Levy [50] provided the definition of a minimal almost-simple group that is analogous to minimal simple groups.

Definition 1.2.4. *A subgroup H of an almost-simple group G is called faithful if $\text{soc}(G)$ is not contained in H , it is called unfaithful if $\text{soc}(G)$ is contained in H . The almost-simple group G is called minimal almost-simple if every faithful subgroup of G is solvable. In other words, G is minimal almost-simple if and only if every subgroup of G not containing $\text{soc}(G)$ is solvable.*

For example, minimal simple groups are minimal almost-simple groups. A nonabelian simple group T is called “new” if it is not minimal simple but it is the socle of a minimal almost-simple group. D. Levy [50] provided the following classification of minimal almost-simple groups, which is very helpful in the proof of Theorem A (see [50, Theorem 1.20]).

Theorem 1.2.5 (D. Levy). *Let L be an almost-simple group. Then L is minimal almost-simple if and only if its socle T is isomorphic to one of the groups on the following list subject to the indicated conditions.*

- (1) $\text{PSL}(2, 2^r)$, r any prime. T is minimal simple, $\text{Out}(T) = \langle \phi \mid o(\phi) = r \rangle$.
- (2) $\text{PSL}(2, 3^r)$, r any odd prime. T is minimal simple, $\text{Out}(T) = \langle \delta, \phi \mid o(\delta) = 2, o(\phi) = r, [\delta, \phi] = 1 \rangle$.
- (3) $\text{PSL}(2, p)$, $p > 3$ a prime satisfying $p^2 + 1 \equiv 0 \pmod{5}$. T is minimal simple, $\text{Out}(T) = \langle \delta \mid o(\delta) = 2 \rangle$.
- (4) $\text{PSL}(2, p)$, $p \geq 11$ a prime satisfying $p \equiv \pm 1 \pmod{10}$ and $L = \text{Aut}(T)$. T is new, $\text{Out}(T) = \langle \delta \mid o(\delta) = 2 \rangle$.
- (5) $\text{PSL}(2, p^{2^m})$, $p \geq 3$ a prime, m a positive integer and $L/\text{Inn}(T) \not\leq \langle \phi \rangle$. T is new, $\text{Out}(T) = \langle \delta, \phi \mid o(\delta) = 2, o(\phi) = 2^m, [\delta, \phi] = 1 \rangle$.
- (6) $\text{Sz}(2^r)$, r any odd prime. T is minimal simple, $\text{Out}(T) = \langle \phi \mid o(\phi) = r \rangle$.
- (7) $\text{PSL}(3, 3)$. T is minimal simple, $\text{Out}(T) = \langle \gamma \mid o(\gamma) = 2 \rangle$.

For the following definition we refer the reader to [48, Definition 1.3.8].

Definition 1.2.6. *Let G be an almost-simple group with $\text{soc}(G) = S$. A maximal subgroup M of G is called a novel maximal subgroup (or, simply, a novelty) if $S \cap M$ is not a maximal subgroup of S .*

Recall that if L is any almost-simple group, then L is a primitive group of type II. Next, we prove the following result using Table 1.3, Table 1.4 and Theorem 1.2.5.

Lemma 1.2.7. *Let L be a minimal almost-simple group with socle S . Assume that L/S is a cyclic m -group where m is an odd prime number. Let R be a maximal subgroup of L such that $RS = L$. Then $R \cap S$ is a maximal subgroup of S .*

Proof. If $L = S$ then there is nothing to prove, so we can assume that $S < L$, and, in this case $|L/S| = m^s$ for some integer $s \geq 1$. Note that $L/S \leq \text{Out}(S)$. Considering the list of minimal almost-simple groups in Theorem 1.2.5, we see that for cases (3), (4), (5) and (7) we have that $\text{Out}(S)$ is a nontrivial 2-group and hence they are eliminated as candidates for L . In case (1), $S \cong \text{PSL}(2, 2^r)$ where r is a prime, and $|\text{Out}(S)| = r$. So we have to consider $r = m \geq 3$ and $s = 1$. To prove the statement of the lemma we have to check that the maximal subgroups of L which do not contain S are not novelties (R is a novelty precisely when $R \cap S$ is not maximal in S). This can be done by consulting Table 1.3, where novelties are marked by the letter N followed by a serial number. One can check that $\text{PSL}(2, 2^r)$ do not have novelties. In case (2), $S \cong \text{PSL}(2, 3^r)$ where r is an odd prime, and $\text{Out}(S)$ has a unique cyclic subgroup of order r . Setting $r = m$ and $s = 1$, we can verify that the maximal subgroups in the relevant entries of Table 1.3 are not novelties. Finally, in case (6) of Theorem 1.2.5, $S \cong \text{Sz}(2^r)$ with r an odd prime and $|\text{Out}(S)| = r$, and again, consulting Table 1.4 we find that there are no novelties. \square

Chapter 2

The solvability of pyramidal groups of prime degree

Recall that a group G is called m -pyramidal if G has precisely m -involutions, which are all conjugate to each other. G is called pyramidal if it is m -pyramidal for some m . In particular, m must be an odd integer. In this Chapter, we study pyramidal groups and prove Theorem A, which we state again for convenience. This theorem was proved in [9].

Theorem A (X. Gao, M. Garonzi). Let $m \neq 7$ be a prime number and let G be an m -pyramidal group. Then G is solvable.

2.1 About pyramidal KTS and pyramidal groups

The following proposition was stated in the introduction and it motivates our interest in pyramidal groups. We will now prove it.

Proposition 2.1.1. *Assume an m -pyramidal KTS can be realized under a nontrivial group G . Then G has precisely m involutions and the involutions of G are pairwise conjugate.*

Proof. First, we prove that G has precisely m involutions. Note that for each $i \in \{1, \dots, m\}$ there exists a block B_i passing through 1 and ∞_i , call it $B_i = \{1, x_i, \infty_i\}$. We claim that $x_i \in G$. If it were not the case, then x_i would be a fixed point ∞_j with $j \neq i$, that is $B_i = \{1, \infty_j, \infty_i\}$. Thus $B_i g = \{g, \infty_j, \infty_i\}$ is a block for any $g \in G$. Since there is a unique block passing through ∞_j and ∞_i , $g = \{1\}$, and then $G = \{1\}$, a contradiction. Now, $B_i x_i^{-1} = \{x_i^{-1}, 1, \infty_i\}$ is a block by assumption, hence it is equal to B_i by uniqueness of the block passing through 1 and ∞_i . This implies that $x_i = x_i^{-1}$ hence x_i has order 2. This gives us m elements of order 2, namely x_1, \dots, x_m . Now assume $x \in G$ is any element of order 2 and let $B = \{1, x, y\}$ be the block through 1 and x . Then

$Bx = \{x, 1, yx\}$ and again, by uniqueness of the block through 1 and x , we have that $yx = y$. Since $x \neq 1$, we deduce that y is a fixed point ∞_i , therefore $x = x_i$. This proves that the involutions of G are precisely x_1, \dots, x_m .

Now we prove that x_1, \dots, x_m are pairwise conjugate in G . Let \mathcal{Q} be the parallel class containing the block $B = \{1, x_1, \infty_1\}$. Note that $Bx_1 = B$, therefore $B \in \mathcal{Q} \cap \mathcal{Q}x_1$, hence $\mathcal{Q}x_1 = \mathcal{Q}$. Now, let $B_i = \{\infty_i, g_i, h_i\}$ be the block of \mathcal{Q} through ∞_i , for a fixed $i \in \{1, \dots, m\}$. Since $B_ix_1 \in \mathcal{Q}x_1 = \mathcal{Q}$ and the unique block of \mathcal{Q} through ∞_i is B_i , we must have $B_ix_1 = B_i$, that is

$$\{\infty_i, g_ix_1, h_ix_1\} = \{\infty_i, g_i, h_i\}.$$

If $g_ix_1 = g_i$ and $h_ix_1 = h_i$, then there exist two integers $j, k \in \{1, \dots, m\}$ with $j \neq i \neq k$ such that $g_i = \infty_j$ and $h_i = \infty_k$, thus $B_i = \{\infty_i, \infty_j, \infty_k\}$. Note that the block B_i is fixed by all $g \in G$, so it belongs to all the parallel classes $\mathcal{Q}g$, $g \in G$, therefore $\mathcal{Q}g \cap \mathcal{Q} \neq \emptyset$ for any $g \in G$, thus $\mathcal{Q}g = \mathcal{Q}$ for any $g \in G$. Let $i \in \{2, \dots, m\}$ and let $Y = \{x_i, a_i, b_i\}$ be the block in \mathcal{Q} containing x_i . Obviously, $Yx_i = \{1, a_ix_i, b_ix_i\} \in \mathcal{Q}x_i = \mathcal{Q}$. This implies that

$$\{1, x_1, \infty_1\} = \{1, a_ix_i, b_ix_i\}$$

because \mathcal{Q} is a partition of the point set. But if $a_ix_i = \infty_1$ then $a_i = \infty_1$ is a contradiction, and if $b_ix_i = \infty_1$ then $b_i = \infty_1$ is a contradiction (\mathcal{Q} is a partition of the point set). Thus $g_ix_1 = h_i$ and $h_ix_1 = g_i$. Note that

$$B_ig_i^{-1} = \{\infty_i, 1, h_ig_i^{-1}\} = \{\infty_i, 1, g_ix_1g_i^{-1}\},$$

and this block must equal $\{1, x_i, \infty_i\}$ by uniqueness of the block through 1 and ∞_i . This proves that $g_ix_1g_i^{-1} = x_i$. \square

2.2 Preliminaries

In this section, we will prove some basic and important properties of pyramidal groups. The authors of [2] proved Lemma 2.2.1 about 3-pyramidal groups.

Lemma 2.2.1 (Lemma 4.4 and Theorem 4.6 of [2]). *Let G be a 3-pyramidal group and write $|G| = 2^n \cdot d$ with d odd. Let K be the subgroup of G generated by the 3 involutions. If $n \geq 2$ then n is even, K is isomorphic to the Klein group $C_2 \times C_2$ and $G/C_G(K) \cong A_3$.*

Definition 2.2.2. *We say that a finite group G of order $2^a d$ with d odd is of n -type if n divides a .*

Lemma 2.2.1 implies that if G is a 3-pyramidal group of order $2^n \cdot d$ where $n \geq 2$ and d odd then G is of 2-type. We will make use of the well-known Frattini's argument to prove Lemma 2.2.4. For Frattini's argument we refer the reader to [45, 5.2.14].

Lemma 2.2.3 (Frattini's argument). *If N is a normal subgroup of G and P is a Sylow p -subgroup of N , then $G = N_G(P)N$.*

Lemma 2.2.4. *Let $m \geq 1$ be an odd integer and let G be an m -pyramidal group. Write $|G| = 2^a \cdot d$ with d odd and let H be a subgroup of G . Denote by K the (characteristic) subgroup of G generated by all the involutions of G and define $C := C_G(K)$. Then*

- (1) *If H has even order and $HC = G$, then H is m -pyramidal.*
- (2) *If p is any prime divisor of $|G|$, Q is a Sylow p -subgroup of C and $H = N_G(Q)$, then H is m -pyramidal.*
- (3) *If m is a prime, and if H has even order and it contains a Sylow m -subgroup of G , then H is m -pyramidal.*
- (4) *Assume $H \trianglelefteq G$ and that $|H|$ is odd. Let ε be an involution in G and let ℓ be the number of elements $h \in H$ with the property that $h^\varepsilon = h^{-1}$. Then G/H is m/ℓ -pyramidal. In particular, if G is 1-pyramidal then so is G/H and, if the involutions of G commute pairwise, then G/H is m -pyramidal.*
- (5) *If m is a prime number and H is a normal 2-subgroup of G then $|H| \equiv 1 \pmod{m}$.*
- (6) *If $m = 3$ and $a = 1$ then $K \cong S_3$ and $G \cong C \times K$.*

Proof. Item 1. Assume G is m -pyramidal and let $H \leq G$ with $HC = G$ and $|H|$ even. If $h \in H$ is an involution and $g \in G$ then, writing $g = xc$ where $x \in H$, $c \in C$, we have $h^g = h^{xc} = h^x \in H$. This implies that all the involutions of G belong to H and that they are conjugate in H . We deduce that H is m -pyramidal.

Item 2. With the help of Lemma 2.2.3, we have that $HC = G$. Since $Q \leq C$, this implies that K centralizes Q , and hence $K \leq H$, so $|H|$ is even. By item (1), H is m -pyramidal.

Item 3. Since $|H|$ is even, H contains at least one involution. Note that $|G : C_G(x)| = m$ and $C \leq C_G(x)$ for any involution x of G . It follows that $|G/C|$ is a multiple of m , since

$$|G : C| = |G : C_G(x)| \cdot |C_G(x) : C| = m \cdot |C_G(x) : C|.$$

Hence there is no Sylow m -subgroup of G contained in C . Let S be a Sylow m -subgroup of G contained in H . Since m is a prime number and $|S| = m^z$ for some integer z , $|x^S| = |S : C_S(x)| = m$ or 1 for any involution x of G . If there exists an involution x of G such that $|x^S| = 1$ then $S = C_S(x) \leq C_G(x)$, thus $|G : C_G(x)|$ would not be divisible by m , a contradiction. This implies that $|x^S| = m$ for any involution x of G . Therefore, S acts transitively on the involutions. Recall that $S \leq H$ and H contains at least one involution ε , so $\varepsilon^s \in H$ for any $s \in S$, therefore all involutions of G are contained in H and H is m -pyramidal.

Item 4. If xH is an involution of G/H , then $x^2 \in H$, this implies that there exists $h \in H$ such that $x^2 = h$. Since $|H|$ is odd, $o(h) = t$ is also odd. It is obvious that $o(xH)$ divides $o(x)$, so $o(x)$ is even. Moreover,

$$t = o(h) = o(x^2) = \frac{o(x)}{(2, o(x))} = \frac{o(x)}{2}.$$

Hence $o(x) = 2t$ and x^t is an involution in G . Since Hx is an involution in G/H , we have $Hx = (Hx)^t = Hx^t$. Hence every involution of G/H has the form $H\varepsilon$ where ε is an involution of G . Let Hx and Hy be two distinct involutions of G/H , with $o(x) = o(y) = 2$, and there is an element $1 \neq g \in G$ such that $x^g = y$ because all involutions of G are conjugate, thus $(Hx)^{H^g} = Hx^g = Hy$. Therefore, Hx and Hy are conjugate in G/H . This implies that all involutions of G/H are conjugate. The involutions of G belonging to the coset $H\varepsilon$ have the form $h\varepsilon$ with $h \in H$ and $(h\varepsilon)^2 = 1$, equivalently $h^\varepsilon = h^{-1}$. Therefore $H\varepsilon$ contains $|I_\varepsilon|$ involutions, where

$$I_\varepsilon := \{h \in H : h^\varepsilon = h^{-1}\}.$$

Since all the involutions are conjugate, the size of I_ε does not depend on ε , let us call it ℓ . Since each coset of H corresponding to an involution of G/H contains ℓ involutions, G/H contains m/ℓ involutions. If $m = 1$ then of course $m/\ell = 1$, in other words, if G is 1-pyramidal, then G/H is 1-pyramidal. Assume that the involutions commute pairwise. If there exists an involution $h\varepsilon \in H\varepsilon$ with $h \neq 1$, then ε commutes with $h\varepsilon$, so $h = (h\varepsilon)\varepsilon$ is an involution, contradicting the fact that $|H|$ is odd. This implies that $\ell = 1$, so G/H is m -pyramidal.

Item 5. Since $|G : C_G(x)| = m$ for every involution x , we have that m divides $|G/C|$ so there is an element $g \in G$ of order a power of m which acts nontrivially on the set of involutions. Since m is a prime number, g does not fix any involution (either all the orbits have size 1 or there is only one orbit of size m). Since H is normal in G , the group $\langle g \rangle$ acts on H by conjugation. If $1 \neq h \in H$ with $o(h) = 2^a$ for some integer a , and h is fixed by g , then g also fixes the 2^{a-1} -th power of h , which is an involution, so no nontrivial element of H is fixed by g . Therefore any orbit of $\langle g \rangle$ acting on $H \setminus \{1\}$ has size a power of m larger than 1. Note that

$$H = C_1 \cup C_2 \cup \dots \cup C_s, \quad \text{where } C_1 = \{1\}$$

and

$$|H| = 1 + |C_2| + \dots + |C_s|,$$

where

$$C_i = h_i^{\langle g \rangle} = \{h_i^c : c \in \langle g \rangle\}, \quad \text{and } h_i \in H.$$

As we proved above $|C_i|$ is a power of m larger than 1 for $i = 2, 3, \dots, s$. Thus m divides $|H| - 1$.

Item 6. Assume $a = 1$ and i, j, k are the three involutions of G . Then $ij \neq ji$, because if it were not the case, $\langle i, j \rangle$ would be isomorphic to $C_2 \times C_2$, implying that $|G|$ would be

divisible by 4, a contradiction. So $i^j \neq i$ and of course $i^j \neq j$ since $i \neq j$, therefore $i^j = k$. The same argument shows that $j^i = k$, therefore

$$(ij)^3 = (iji)(jij) = k^2 = \{1\}.$$

Thus, ij has order 3. Note that K can be generated by two involutions i and j , so $K \cong S_3$. Obviously, the order of C is odd because otherwise these three involutions of G would commute pairwise, a contradiction. Observe that

$$N_G(K)/C = G/C \lesssim \text{Aut}(K) = S_3.$$

Since $|G|$ is even, $|C|$ is odd, and 3 divides $|G/C|$, $G/C \cong S_3$. Moreover, $C \cap K = Z(K) = \{1\}$, we have

$$|CK| = \frac{|C| \cdot |K|}{|C \cap K|} = |G|,$$

hence $CK = G$ and, since C, K are normal in G , it follows that $G \cong C \times K$. \square

Proposition 2.2.5. *Let N be a finite abelian group of odd order and let A be a subgroup of $\text{Aut}(N)$ containing the inversion map $\iota : N \rightarrow N, n \mapsto n^{-1}$ and with the property that ι is the unique element of order 2 in A . Then the semidirect product $N \rtimes A$ is $|N|$ -pyramidal.*

Proof. Write $G = NA$. If an element $na \in NA = G$ has order 2 where $n \in N$ and $a \in A$, then

$$1 = (na)^2 = nana = (n \cdot n^{a^{-1}}) \cdot a^2.$$

Thus

$$n \cdot n^{a^{-1}} = a^{-2} \in A \cap N = \{1\}.$$

Hence $a^2 = 1$ and $n^a = n^{-1}$. Since $|N|$ is odd, $n^a = n^{-1} \neq n$, therefore $a \neq 1$. This implies that a has order 2, so $a = \iota$. This proves that the involutions of G are precisely the elements of the form $n\iota$ with $n \in N$ arbitrary, so G has $|N|$ involutions. Moreover

$$\iota^n = n^{-1}\iota n = n^{-2}n\iota n = n^{-2}nn^{-1}\iota = n^{-2}\iota.$$

Since $|N|$ is odd, we deduce that all the involutions of G are conjugate to ι , hence G is $|N|$ -pyramidal. \square

Lemma 2.2.6. *Let G be a finite group whose Sylow 2-subgroups have only one element of order 2. Then G is pyramidal.*

Proof. Let x, y be two involutions of G . There exist two Sylow 2-subgroups P, Q of G with $x \in P$ and $y \in Q$. Let $g \in G$ be such that $g^{-1}Pg = Q$. Then Q contains y and $g^{-1}xg$. Since Q contains only one involution, it follows that $g^{-1}xg = y$. \square

Recall that a finite 2-group has a unique element of order 2 if and only if it is cyclic or generalized quaternion (see [11, Theorem 6.11]). As usual, we denote by $O(G)$ the maximal normal subgroup of odd order in G . In the following result, $Z^*(G)$ denotes the inverse image in G of the center of $G/O(G)$. For the proof of the following theorem, see Theorem 1, Lemma 2 of [51].

Theorem 2.2.7 (Glauberman's Z^* theorem). *Let G be a finite group. If T is a Sylow 2-subgroup of G containing an involution ε not conjugate in G to any other element of T , then $\varepsilon \in Z^*(G)$.*

Proposition 2.2.8. *Let G be a finite group containing precisely m involutions, call them x_1, \dots, x_m . If the following hold:*

- (1) $x_i x_j \neq x_j x_i$ for all $i \neq j$,
- (2) $G = \langle x_1, \dots, x_m \rangle$,

then G is m -pyramidal and $G' = O(G)$ where $O(G)$ is the unique largest odd order normal subgroup of G , and $G \cong G' \rtimes C_2$. In particular, G is solvable. Moreover, if m is a prime number, then G is a dihedral group of order $2m$.

Observe that, in the above proposition, the order of G' is not equal to m in general, an example of this is $\text{SmallGroup}(54,8) = C_3^2 : S_3$ with $m = 9$.

Proof. First, note that the involutions of G are all conjugate. Indeed, let P be a Sylow 2-subgroup of G , since the center $Z(P)$ of P is not trivial, there exists an element z of order 2 belonging to $Z(P)$, hence z commutes with all the involutions in P , so it is the only involution of P . By Lemma 2.2.6, G is m -pyramidal.

Let $O = O(G)$ be the largest normal subgroup of G of odd order and let $Z^*(G)$ be the inverse image in G of the center of G/O . Note that P has only one involution, call it ε , so ε is not conjugate in G to any other element of P . In the light of Theorem 2.2.7 we have $\varepsilon \in Z^*(G)$, i.e., $\varepsilon O \in Z(G/O)$. Therefore $O\langle\varepsilon\rangle$ is normal in G , and hence the involutions of G are all contained in $O\langle\varepsilon\rangle$. Since G is generated by the involutions, $G = O\langle\varepsilon\rangle$. Since $O \cap \langle\varepsilon\rangle = 1$, we have $G = O \rtimes \langle\varepsilon\rangle$ and hence G' is contained in O . If $a \in G$ is written as a product of involutions,

$$a = y_1 y_2 \dots y_{t-1} y_t$$

with $y_s \in \{x_1, \dots, x_m\}$ for all s , then $a \in G'$ if and only if t is even. Indeed, since the involutions are conjugate, for any two involutions x and y of G there exists $g \in G$ such that $y = x^g$, so that $xy = x^{-1}g^{-1}xg$, thus any product of two involutions is a commutator, and this implies that if t is even then $a \in G'$. Conversely, if $a \in G'$ then t must be even, since if t is odd then $y_t = y_{t-1} \dots y_1 a$ belongs to G' since $t-1$ is even, this implies that $|G'|$ is even, contradicting the fact that $G' \leq O$. Therefore, if $\varepsilon \in G$ is an involution, then

for every $g \in G \setminus G'$ we have $g\varepsilon \in G'$. This implies that $|G : G'| = 2$ hence $G' = O$. By the Feit-Thompson theorem, G' is solvable, so G is solvable.

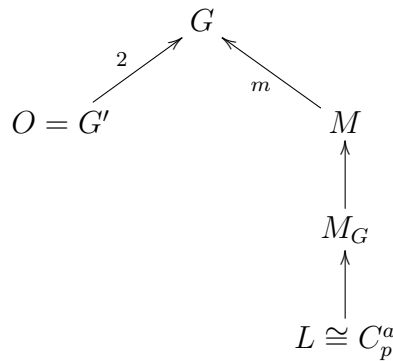
Now assume that m is a prime number. We will prove, by induction on $|G|$, that $G \cong D_{2m}$. We know that $G = G' \rtimes \langle \varepsilon \rangle$, $o(\varepsilon) = 2$. Let $M := C_G(\varepsilon)$. Since G is m -pyramidal, $|G : M| = m$, prime, so M is a maximal subgroup of G .

Suppose first that the normal core M_G of M in G is trivial. Then G is a primitive group of prime degree m . Since G is solvable, G is a primitive group of type I by Theorem 1.1.11, this implies that $G = V \rtimes M$ where $V \cong C_m$ is a minimal normal subgroup of G . On the other hand, since $C_G(V) = V$ we have

$$G/V \lesssim \text{Aut}(C_m) \cong C_{m-1}.$$

It follows that V contains G' and the minimality of V implies that $G' = V$. Therefore $G \cong C_m \rtimes C_2 \cong D_{2m}$.

We now show that M_G must in fact be trivial. Suppose for a contradiction that $M_G \neq \{1\}$ and let L be a minimal normal subgroup of G contained in M_G .



Since G is solvable, $L \cong C_p^a$ for some prime p and integer a . If $p = 2$, then $L \cong C_2$ since $G \cong G' \rtimes C_2$ and $|G'|$ is odd. Since L is normal in G , its single nontrivial element is a central involution of G . This contradicts the fact that the number of involutions m is prime, so $m > 1$, and the fact that all involutions are conjugate to each other. Thus $|L|$ is odd. Clearly, $L \neq G'$ since otherwise $G' = L \leq M < G$ and, being $|G : G'| = 2$, $G' = M$ and hence $m = 2$, a contradiction. By Lemma 2.2.4(4), G/L is 1-pyramidal or m -pyramidal. If G/L is 1-pyramidal, then $x_iL = x_jL$ for any two involutions x_i and x_j of G , this implies that $x_i x_j \in L$. Since every element of G' is a product of an even number of involutions, $G' \leq L$, and since $|G : G'| = 2$ we deduce that $G' = L$, contradicting the fact that $L \neq G'$. Therefore G/L is m -pyramidal. We now prove that any two distinct involutions of G/L do not commute. Let x be an involution of G with $x \neq \varepsilon$. If $x\varepsilon L = \varepsilon xL$ then $[x, \varepsilon] \in L \leq M = C_G(\varepsilon)$, so

$$x\varepsilon x = [x, \varepsilon]\varepsilon = \varepsilon[x, \varepsilon] = \varepsilon x \varepsilon x \varepsilon$$

hence ε commutes with $x\varepsilon x$, implying that $x\varepsilon x = \varepsilon$ (because two distinct involutions of G cannot commute), so that $x\varepsilon = \varepsilon x$, a contradiction. This implies that the quotient

group G/L satisfies all the conditions of the statement, so by induction we may assume that $G/L \cong D_{2m}$. If $g \in G$ then

$$L = L^g \leq M^g = C_G(\varepsilon^g).$$

Since the involutions are all conjugate and generate G , we must have $L \leq Z(G)$. Since any subgroup of L is normal in G , L is an abelian simple group by the minimality of L , that is, L has prime order p . Since $|G : L| = 2m$, we deduce that $|G| = 2mp$ and G' is abelian because $G'/L \cong C_m$ and $L \leq Z(G')$. Therefore, G' is isomorphic to one of:

$$C_m \times C_m, \quad C_{m^2} \quad \text{or} \quad C_m \times C_p \quad \text{where } m \neq p,$$

and then G is isomorphic to one of the following three groups:

$$(C_m \times C_p) \rtimes C_2, \quad (C_m \times C_m) \rtimes C_2 \quad \text{or} \quad C_{m^2} \rtimes C_2 \cong D_{2m^2}.$$

Since G is generated by m involutions and D_{2m^2} contains m^2 involutions, $G \cong (C_m \times C_p) \rtimes C_2$ or $(C_m \times C_m) \rtimes C_2$. Note that since $L \leq Z(G) \neq \{1\}$, we have $G \cong C_p \times D_{2m}$ or $C_m \times D_{2m}$, contradicting the fact that G is generated by involutions. \square

Now, we aim to study pyramidal groups in which the involutions commute pairwise. Before proving the following Lemma 2.2.9, we introduce the concepts of transvection and Frobenius automorphism.

Let F be a field and let V be a finite dimensional F -vector space with $\dim_F(V) = n$. A linear transformation τ of V is called a *transvection* if there exists a hyperplane U of V such that $u^\tau = u$ for all $u \in U$, and $u^\tau - u \in U$ for all $u \in V$. Equivalently, under a suitable base change, given two distinct $i, j \in \{1, 2, \dots, n\}$ and $b \in F$, a transvection is a matrix of the form

$$T_{ij}(b) = 1 + be_{ij},$$

where e_{ij} is the matrix whose sole nonzero entry is a 1 in the (i, j) -position. Obviously, $T_{ij}(b)$ belongs to $\text{SL}(V)$.

Let A be a unitary commutative ring whose characteristic is a prime number p . The *Frobenius endomorphism* φ is defined by

$$\varphi : A \rightarrow A, \quad \varphi(a) := a^p, \quad \forall a \in A.$$

It respects the multiplication of A :

$$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b),$$

and $\varphi(1) = 1^p = 1$ as well. Moreover, it also respects the addition of A :

$$\varphi(a + b) = (a + b)^p = \sum_{i=0}^p \binom{p}{i} a^i b^{p-i}.$$

Observe that, if $0 < i < p$, then the integer $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ is divisible by p , since p is a prime hence it is coprime to $i!(p-i)!$. Therefore all the summands, considered in A , are equal to zero, except those which correspond to $i = 0$ and $i = p$, that is, b^p and a^p . This proves that $(a + b)^p = a^p + b^p$ in A . Therefore, φ is a ring homomorphism. Moreover, if A is a domain then φ is injective because $\text{Ker}(\varphi) = \{0\}$ ($a^p = 0$ implies $a = 0$) and if A is finite then φ is also surjective by the pigeonhole principle. So if A is a finite field, its Frobenius endomorphism is an isomorphism, called the *Frobenius automorphism*.

Lemma 2.2.9. *Assume that $m \neq 7$ is a prime power, G is an m -pyramidal group and the subgroup K of G generated by the involutions is an elementary abelian 2-group of size 2^n , so that $2^n - 1 = m$. Then m is a prime number and $G/C_G(K)$ is isomorphic to one of C_m , $C_m \rtimes C_n$, where in the second case the action is given by the Frobenius automorphism of a field F of size 2^n acting naturally on $F \setminus \{0\}$.*

Proof. Lemma 1.1.21 implies that m and n are actually prime numbers and $n \neq 3$. Clearly, K is a minimal normal subgroup of G since $K \cong C_2^n \trianglelefteq G$ and all involutions of G are conjugate. Moreover we have a faithful action by conjugation of $N_G(K)/C_G(K) = G/C_G(K)$ on K , and hence $G/C_G(K)$ is isomorphic to a subgroup H of $\text{Aut}(K) \cong \text{GL}(n, 2)$ (see Lemma 1.1.26) and H is irreducible because the nontrivial elements of K are pairwise conjugate in G .

We have $K \cong \mathbb{F}_2^n$, $n \neq 3$ prime, $m = 2^n - 1 \neq 7$ prime. Since G is an m -pyramidal group, all elements of $K \setminus \{0\}$ form the single conjugacy class of involutions in G and H acts transitively on $K \setminus \{0\}$. Set

$$X := K \rtimes H,$$

where \rtimes is defined with respect to the action of $H \cong G/C_G(K)$. Since H acts transitively on $K \setminus \{0\}$, we have that X is a 2-transitive group, by Lemma 1.1.5. Let $kh \in C_X(K)$ where $k \in K$, $h \in H$, then $v^{kh} = v^h = v$ for any involution v of K . Since H acts transitively on $K \setminus \{0\}$, $h = 1$, it follows that $C_X(K) = K$. Obviously, K is a minimal normal subgroup of X . We claim that K is the unique minimal normal subgroup of X . Indeed, suppose that $L \neq K$ is a minimal normal subgroup of X , then $[L, K] = \{1\}$, and hence $L < C_X(K) = K$, contradicting the minimality of K . This proves that K is the unique minimal normal subgroup of X , i.e., $\text{soc}(X) = K$. Therefore, X is a 2-transitive affine group of degree 2^n . Consider Table 1.1, which is the classification of 2-transitive affine groups. Since n is prime, we are only concerned with the first line of the table, in which the degree q^d can be interpreted in two different ways: $q = 2^n$, $d = 1$ or $q = 2$, $d = n$. The second case gives $H = \text{GL}(n, 2)$. The first case gives

$$C_m \cong \text{GL}(1, 2^n) \leq H \leq \Gamma L(1, 2^n).$$

Since n is prime, there are only three possibilities for H : namely $\text{GL}(n, 2)$, C_m and $C_m \rtimes C_n$ where, in the third case, the action of C_n on C_m is precisely the natural action of the Frobenius automorphism of order n , that is $\phi : x \mapsto x^2$, on the set $F^* = F \setminus \{0\}$

where F is the finite field of size 2^n . In other words

$$C_m \rtimes C_n = F^* \rtimes \langle \phi \rangle.$$

Also, note that $\mathrm{GL}(n, 2)$ and $C_m \rtimes C_n$ are the same group if $n = 2$.

We are left to prove that $G/C \not\cong \mathrm{GL}(n, 2)$ for $n > 3$, where $C = C_G(K)$. We assume that G is a group of minimal order with the following three properties: G is m -pyramidal, the involutions of G commute pairwise and $G/C \cong \mathrm{GL}(n, 2)$. Assume that there exists a maximal subgroup M of G such that $C \not\leq M$, then $M < MC \leq G$, thus $MC = G$ by the maximality of M . Since

$$\mathrm{GL}(n, 2) \cong G/C = MC/C \cong M/(M \cap C)$$

we have that $|M|$ is even. Lemma 2.2.4(1) implies that M is m -pyramidal, that is $K \leq M$ and all involutions of M are conjugate. Note that

$$M/C_M(K) = M/(C \cap M) \cong G/C \cong \mathrm{GL}(n, 2)$$

and $|M| < |G|$, moreover the involutions of M commute pairwise because they are involutions in G . This contradicts the minimality of $|G|$. Therefore C is contained in every maximal subgroup of G , in other words $C \leq \Phi(G)$. Since $n > 3$,

$$G/C \cong \mathrm{GL}(n, 2) \cong \mathrm{PSL}(n, 2)$$

is a simple group, so C is a maximal normal subgroup of G and hence $C = \Phi(G)$. We claim that K is the unique minimal normal subgroup of G . Indeed, suppose that $L \neq K$ is a minimal normal subgroup of G , then L does not contain K , so it does not contain involutions, implying that $|L|$ is odd. Note that $L \leq C$ because otherwise $CL = G$ by maximality of C as a normal subgroup of G , and then

$$\mathrm{GL}(n, 2) \cong G/C \cong L/(L \cap C),$$

this contradicts the fact that $|L|$ is odd. In this case $\bar{K} \cong K$ is a minimal normal subgroup of \bar{G} where, for $R \leq G$, we define $\bar{R} := RL/L$. The fact that $L \cap K = \{1\}$ easily implies that $C_{\bar{G}}(\bar{K}) = \bar{C}$. Moreover,

$$\mathrm{GL}(n, 2) \cong G/C \cong \bar{G}/\bar{C}.$$

By Lemma 2.2.4(4), \bar{G} is an m -pyramidal group in which the involutions commute pairwise. Since $L \neq \{1\}$, this contradicts the minimality of $|G|$. This proves that K is the unique minimal normal subgroup of G , in particular $O(G) = \{1\}$. This implies that $\Phi(G) = C$ is a 2-group. Indeed, if it were not, then it would have a Sylow subgroup of odd order, which would be normal in G because $\Phi(G)$ is nilpotent, contradicting $O(G) = \{1\}$.

We are in the following situation: $G/C \cong \mathrm{GL}(n, 2)$, $n > 3$, $K = \langle x_1, \dots, x_m \rangle \cong \mathbb{F}_2^n$ is the unique minimal normal subgroup of G and $C = C_G(K) = \Phi(G)$ is a 2-group. Let

of order 7 acting transitively on the nonzero vectors of \mathbb{F}_2^3 . It is easy to check that $\rho_1 C, \rho_2 C, \dots, \rho_{(n-1)/2} C$ pairwise commute with each other. We construct the element

$$xC = \rho_1 \rho_2 \dots \rho_{(n-1)/2} C.$$

Note that $(\rho_i C)^{\tau C} = \rho_i^2 C$ for $i = 1, 2, 3, \dots, (n-3)/2$ and $(\rho_{(n-1)/2} C)^{\tau C} = \rho_{(n-1)/2} C$, hence $(xC)^{\tau C} = x^8 C$, and then $x^\tau \in \langle C, x \rangle$, thus there exists $c \in C$ such that $x^\tau = x^8 c$, this implies that $x^\tau \in \langle C, x \rangle$. Therefore, the element τ normalizes $\langle x, C \rangle$ (since C is normal in G). Obviously, $o(xC) = 21$ and $o(x) = 2^u \cdot 21$ for some u . Up to replacing x with x^{2^u} , we may assume that $o(x) = 21$. Moreover, $C_K(x) = \{1\}$ and

$$\gamma(xC) = \begin{pmatrix} 0 & 1 & & & & & & & \\ 1 & 1 & & & & & & & \\ & & \ddots & & & & & & \\ & & & 0 & 1 & & & & \\ & & & 1 & 1 & & & & \\ & & & & & 0 & 0 & 1 & \\ & & & & & 1 & 0 & 0 & \\ & & & & & 0 & 1 & 1 & \end{pmatrix}.$$

Now let $H := \langle C, x, \tau \rangle \leq G$, $S = \langle x \rangle$, $J := N_H(S)$. Since τ normalizes $\langle C, x \rangle$, we have $\langle C, x \rangle$ is normal in H and $H/\langle C, x \rangle$ is a 2-group. Moreover, the order of the quotient group $\langle C, x \rangle/C$ is 21, it follows that $\langle C, x \rangle$ is solvable since both C and $\langle C, x \rangle/C$ are solvable. Therefore, $H = \langle C, x \rangle \langle \tau \rangle$ is solvable. Since C is a 2-group, S is a Hall subgroup of the solvable group H , therefore if $h \in H$ then S^h is a Hall subgroup of $\langle C, x \rangle$. This is because $\langle C, x \rangle$ is normal in H , and S is contained in $\langle C, x \rangle$. Since $\langle C, x \rangle$ is solvable, there exists $y \in \langle C, x \rangle$ such that $S^h = S^y$, so $S^{hy^{-1}} = S$. Thus $hy^{-1} \in N_H(S) = J$, so that

$$H = J \langle C, x \rangle = CJ.$$

Note that $\tau \in H = CJ$, let $\tau = c\theta \in CJ$ where $c \in C$ and $\theta \in J$. Since $\tau \in G \setminus C$, we have $1 \neq \theta = c^{-1}\tau \in \tau C$. Therefore $\theta C = \tau C$, and we may change the definition of τ in the beginning of the argument by setting it to be equal to θ . There is no harm in doing this, because all that was used until now has to do only with the action of τ on K , so we have the freedom to change the representative in τC . Thus we can assume that $\tau \in J$. Since the involutions of G belong to K and τ does not centralize K , τ is not an involution. Since C is a 2-group, τ has order a power of 2, say $o(\tau) = 2^k$ with $k \geq 2$, and hence $t := \tau^{2^{k-1}}$ has order 2 so it belongs to K . Therefore $t \in K \cap J$. Since t normalizes S , we can write $x^t = x^r$ for some natural number r . Since $t \in K$,

$$x^{r-1} = x^r \cdot x^{-1} = x^t \cdot x^{-1} = t^{-1} x t x^{-1} = t^{-1} (x t x^{-1}) \in K$$

and since x has odd order this implies that $x^{r-1} = 1$, hence $x^t = x^r = x$, so $t \in C_K(x) = \{1\}$, which implies that $t = 1$, a contradiction. \square

Lemma 2.2.10. *Let G be an m -pyramidal group of order $2^a \cdot d$ where $m = 2^n - 1 \neq 7$ is prime and d is odd. If $K \cong C_2^n$, then n divides a .*

Proof. If $m = 3$, then $n = 2$ and $K \cong C_2 \times C_2$, this implies that $a \geq 2$, thus the claim follows from Lemma 2.2.1. Now assume that $m > 3$, so that $n > 2$. Note that $m = 2^n - 1 \neq 7$ is a prime number, so $n \neq 3$ is also a prime number by Lemma 1.1.21. Let $C := C_G(K)$. Since $K \cong C_2^n$, we have

$$G/C \cong C_m \quad \text{or} \quad C_m \rtimes C_n$$

by Lemma 2.2.9. Since n and m are odd prime numbers, G/C is a group of odd order. Let Q be a Sylow 2-subgroup of C , then Q is a Sylow 2-subgroup of G , so $|Q| = 2^a$. By Lemma 2.2.4(2), $N_G(Q)$ is an m -pyramidal group. Since Q is normal in $N_G(Q)$, Lemma 2.2.4(5) implies that

$$2^a = |Q| \equiv 1 \pmod{m}.$$

Since the prime number n is the order of 2 in the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^*$, we deduce that n divides a . \square

2.3 The proof of Theorem A

In this section we will prove that if $m \neq 7$ is prime then all m -pyramidal groups are solvable. As usual, K denotes the subgroup of G generated by its involutions. In the following proof, we will use several times Feit-Thompson theorem, that says that any finite group of odd order is solvable. Equivalently, any nonabelian simple group has even order.

Assume, by contradiction, that G is a nonsolvable m -pyramidal group of minimal order. Let $O = O(G)$ be the largest normal subgroup of G of odd order. Since m is prime, G/O is 1-pyramidal or m -pyramidal by Lemma 2.2.4(4). Set $C := C_G(K)$.

Assume that G/O is 1-pyramidal. Since $|O|$ is odd, a Sylow 2-subgroup of G is isomorphic to a Sylow 2-subgroup of G/O , it follows that a Sylow 2-subgroup of G is a generalized quaternion group or a cyclic group with the help of Theorem 1.1.24, and for any two involutions x_i, x_j of G we have $x_i x_j \neq x_j x_i$ because otherwise $\langle x_i, x_j \rangle \cong C_2 \times C_2$ and it would be contained in a Sylow 2-subgroup of G , contradicting the fact that a Sylow 2-subgroup of G has a unique involution. This implies that $C_G(x)$ contains the unique involution x for any involution x of G . Thus $|C|$ is odd since

$$C = \bigcap_{x \in T} C_G(x) = \bigcap_{g \in G} C_G(x^g) = \bigcap_{g \in G} (C_G(x))^g,$$

where T is the set of involutions of G . Therefore C is solvable. By Proposition 2.2.8 we have $K \cong D_{2m}$, hence

$$G/C \lesssim \text{Aut}(D_{2m}) \cong C_m \rtimes \text{Aut}(C_m) \cong C_m \rtimes C_{m-1}.$$

Since both C and G/C are solvable, we deduce that G is solvable, a contradiction.

We may assume, therefore, that G/O is m -pyramidal. Since O is solvable, the minimality of $|G|$ implies that $O = \{1\}$. Let N be a minimal normal subgroup of G , then

$$N \cong S^n \quad \text{or} \quad N \cong C_2^n$$

where $n \geq 1$ and S is a nonabelian simple group. In particular, all involutions of G are contained in N since they are all conjugate to each other in G .

Suppose first that $N \cong S^n$ where S is a nonabelian simple group. Let $i(X)$ denote the number of involutions of the group X . Then

$$m = i(N) = (i(S) + 1)^n - 1 = i(S) \cdot ((i(S) + 1)^{n-1} + \dots + 1).$$

Therefore m is divisible by $i(S)$, so $i(S) = m$ or $i(S) = 1$. If $i(S) = 1$, then S has a unique involution x , this implies that for any $s \in S$, we have $x^s = s^{-1}xs = x$ (since $o(x^s) = 2$), thus $x \in Z(S)$, contradicting the fact that $Z(S) = \{1\}$. Therefore, $i(S) = m$, and so $n = 1$. Let x_1, x_2, \dots, x_m be the m involutions. Since they are conjugate in G and $S \trianglelefteq G$, we have

$$|x_i^S| = \frac{|S|}{|C_G(x_i) \cap S|} = \frac{|S^g|}{|C_G(x_i^g) \cap S^g|} = \frac{|S|}{|C_G(x_i^g) \cap S|} = |(x_i^g)^S| = d,$$

where $g \in G$. This means that $|x_i^S| = |x_j^S| = d$ for every i, j . Since S has m involutions, this implies that d is a divisor of m . Since m is prime, $d = 1$ or m . If $d = 1$ then

$$\{x_1, x_2, \dots, x_m\} \subseteq Z(S),$$

contradicting $Z(S) = \{1\}$. Therefore $d = m$, and hence S has a conjugacy class of prime size m , contradicting Burnside's Theorem 1.1.16.

Suppose that $N \cong C_2^n$. Since N contains involutions, it follows that $K = N$. Since $2^n - 1 = m \neq 7$ is a prime number, $n \neq 3$ is prime by Lemma 1.1.21. By Lemma 2.2.9, G/C is isomorphic to one of $C_m \times C_n, C_m$.

Assume $G/C \cong C_m \times C_n$, so that there is a normal subgroup A of G containing C such that $A/C \cong C_m$ and $G/A \cong C_n$. Note that A has even order since $K \leq C < A$ and it contains a Sylow m -subgroup of G . Thus, Lemma 2.2.4(3) implies that A is m -pyramidal. The minimality of $|G|$ implies that A is solvable and hence G is solvable because $G/A \cong C_n$, giving a contradiction.

So from now on we can assume that $K = N \cong C_2^n$ and $G/C \cong C_{2^{n-1}} = C_m$. In particular, C is a maximal subgroup of G , because its index in G is the prime m . Note that both K and C are normal in G . We will use several times the following fact: if H is a proper subgroup of G such that $HC = G$ then H is solvable. When $|H|$ is odd, this follows from the Feit-Thompson theorem, and when $|H|$ is even, this follows from Lemma 2.2.4(1) and the minimality of $|G|$. Since $O(G) = \{1\}$, the minimal normal subgroups of G have even order, so they contain all the involutions of G . This implies that the unique minimal normal subgroup of G is K .

2.3.1 Step 1

We will prove that there exists a normal subgroup N of G with $\Phi(G) < N \leq C$ such that G/N is a cyclic m -group, $N/\Phi(G)$ is a nonabelian chief factor of G , isomorphic to S^t for some nonabelian simple group S , and $\Phi(G)$ is a 2-group containing K .

$$\{1\} \xrightarrow{2^a} \Phi(G) \xrightarrow{S^t} N \xrightarrow{m^b} C \xrightarrow{m} G$$

Proof. Let N be a normal subgroup of G such that G/N is cyclic and N is of minimal order with this property. If G/N is not an m -group, then there exists $L/N \trianglelefteq G/N$ such that $|G : L|$ is a prime distinct from m , so that $LC = G$ since $|G : C| = m$, so L is solvable. Since G/L is solvable, this contradicts the fact that G is nonsolvable. So G/N is a cyclic m -group. Moreover N is contained in C because otherwise $NC = G$ and then N would be solvable, so G would be solvable as well. Consider a normal subgroup R of G contained in N with the property that N/R is a minimal normal subgroup of G/R . We claim that $R = \Phi(G)$. First, if $\Phi(G) = \{1\}$ then, by Theorem 1.1.23 G has a subgroup H such that $G = S_1(G) \rtimes H$ where $S_1(G)$ denotes the product of all the abelian minimal normal subgroups of G . Since K is the unique minimal normal subgroup of G and it is abelian, $S_1(G) = K$. Note that all involutions of G are contained in K , so $|H|$ is odd, it follows that $G/K \cong H$ is solvable, so G is solvable, contradicting the nonsolvability of G . Moreover $\Phi(G)$ is a 2-group because otherwise there would exist a nontrivial Sylow subgroup P of $\Phi(G)$ of odd order, and since $P \trianglelefteq_c \Phi(G) \trianglelefteq G$, being $\Phi(G)$ nilpotent, P would be a nontrivial normal subgroup of G of odd order, contradicting $O(G) = \{1\}$. Therefore $\Phi(G)$ is a nontrivial 2-group. In particular $\Phi(G)$ contains involutions, so $K \leq \Phi(G)$. Observe that

$$\Phi(G)/\Phi(G) \cap N \cong \Phi(G)N/N \leq \Phi(G/N).$$

Since G/N is an m -group, the order of $\Phi(G/N)$ is odd, while $\Phi(G)/\Phi(G) \cap N$ is a 2-group. This forces $\Phi(G)/\Phi(G) \cap N = \{1\}$, thus $\Phi(G) \leq N$. By minimality of $|N|$, G/R is not a cyclic m -group, so if $x \in G$ is an m -element that generates G/C , then $R\langle x \rangle$ is a proper subgroup of G , moreover $R\langle x \rangle C = G$, so R is solvable. Since $R \leq N \leq C$, to prove that $R \leq \Phi(G)$ it is enough to prove that if M is a maximal subgroup of G distinct from C , then $R \leq M$. We have $MC = G$, so M is solvable hence $MR \neq G$ being G nonsolvable and M, R solvable. Therefore $R \leq M$, implying that $R \leq \Phi(G)$. Since G/N is an m -group and G is nonsolvable, we deduce that $\Phi(G) \neq N$, in other words $\Phi(G)$ is properly contained in N . Since $R \leq \Phi(G) < N$ and N/R is a minimal normal subgroup of G/R , we deduce that $R = \Phi(G)$. Since $\Phi(G)$ is nilpotent, the nonsolvability of G implies that $N/\Phi(G)$ is a nonabelian chief factor of G , isomorphic to a direct power S^t for some nonabelian simple group S . \square

2.3.2 Step 2

Let M be a maximal subgroup of G with $M \neq C$. Then the normal core M_G of M in G equals $\Phi(G)$ and consequently $G/\Phi(G)$ is a primitive group.

Proof. By Lemma 2.2.4(1), the maximal subgroups of G distinct from C are solvable by minimality of $|G|$, since they supplement C . If M_1 is a maximal subgroup of G such that $M_1 \neq C$ then $M_G \leq M_1$, since otherwise we would have $M_1 M_G = G$, contradicting the fact that G is nonsolvable, since M_1 and M_G are solvable. So every maximal subgroup of G different from C contains M_G , implying that $\Phi(G) = M_G \cap C$. To conclude the proof, we need to prove that $M_G \leq C$. If it were not the case, then $CM_G = G$. Note that

$$G/M_G = CM_G/M_G \cong C/M_G \cap C = C/\Phi(G)$$

has a subgroup $N/\Phi(G) \cong S^t$. In particular, every nonabelian simple group S has order divisible by 4 because otherwise S would have a nontrivial subgroup H of odd order such that $|S : H| = 2$, and then H would be a nontrivial normal subgroup of S , a contradiction. Since 4 divides $|S|$, a Sylow 2-subgroup of S contains a subgroup of order 4. This implies that the group S also contains a subgroup of order 4. Thus there exist two subgroups $A, B \leq G$ containing M_G such that $A \leq B$ and $|B : A| = |A : M_G| = 2$. Since A and B contain M_G , $AC = BC = G$, hence both A and B are m -pyramidal groups by Lemma 2.2.4(1). Write $|A| = 2^a \cdot d$ where d is odd, then $|B| = 2^{a+1} \cdot d$. Since

$$K \leq \Phi(G) \leq M_G \leq A \leq B$$

and $K \cong C_2^n$, Lemma 2.2.10 implies that n divides both a and $a + 1$, thus $n = 1$, contradicting the fact that $n \geq 2$. \square

2.3.3 Step 3

Let $W := G/\Phi(G)$. Then W is a primitive group whose socle is $N/\Phi(G) \cong S^t$, which is the unique minimal normal subgroup of W . Let T_1 be the first direct factor of $N/\Phi(G) \cong S^t$ and let

$$G_1 := N_W(T_1)/C_W(T_1).$$

Then G_1 is an almost-simple group with socle $T_1 C_W(T_1)/C_W(T_1) \cong S$ and we will identify G_1 with a subgroup of $\text{Aut}(S)$ containing S . Moreover, W is of n -type and, if U is a maximal subgroup of G_1 such that $US = G_1$, then U is a solvable group of n -type.

Proof. Write $|\Phi(G)| = 2^a$ and $|G| = 2^b \cdot d$, we have $|W| = 2^{b-a} \cdot d$. In the light of Lemma 2.2.4(5), $m = 2^n - 1$ divides $2^a - 1$, we deduce that n divides a . Moreover n divides b by Lemma 2.2.10, therefore n divides $b - a$, in other words W is of n -type. We refer to

[38, Chapter 1] for the general properties of primitive groups. Recall that W is a finite primitive group. Since W is not solvable, W is primitive of type II or III. Let M be a core-free maximal subgroup of W . We claim that W is a primitive group of type II. Indeed, assume that W is primitive of type III and A is a minimal normal subgroup of W distinct from B where $B := N/\Phi(G)$, then $W = B \rtimes M$ and $AB \cap M \cong B$ is a nonabelian group by Theorem 1.1.11, so $M \cong W/B \cong G/N$ is a cyclic group, implying that $AB \cap M \cong B$ is cyclic, contradicting the fact that B is a nonabelian group. This shows that W is a primitive group of type II and so has a unique minimal normal subgroup which must be $N/\Phi(G)$ by Step 1. Let $\rho : W \rightarrow \text{Sym}(t)$ denote the conjugation action of W on the set of direct factors of $N/\Phi(G) \cong S^t$. Obviously, $N/\Phi(G) \leq \text{Ker}(\rho)$ since $N/\Phi(G)$ is the unique minimal normal subgroup of W and $\text{Ker}(\rho)$ is not trivial. Set $P := W/\text{Ker}(\rho)$, then, by Lemma 1.1.14, we have an embedding of W in the standard wreath product $G_1 \wr P$. Since G/N is a cyclic m -group, the group P is a cyclic m -subgroup of $\text{Sym}(t)$ because it is a quotient group of G/N . As P acts transitively by conjugation on the t direct factors of the socle $N/\Phi(G)$, we have t is a power of m . See also Lemma 1.1.14.

Let U be a maximal subgroup of G_1 such that $US = G_1$ and let

$$V := (U \cap S)^t \leq S^t = \text{soc}(W).$$

We claim that $N_W(V) \text{soc}(W) = W$. Let $g \in W$. Identifying W with a subgroup of $G_1 \wr P$, we can write $g = (x_1, \dots, x_t)\gamma$ where $x_i \in G_1$ for all i and $\gamma \in P$. Since $US = G_1$, there exist $s_i \in S$, $u_i \in U$ such that $x_i = s_i u_i$ for all $i = 1, \dots, t$, and setting

$$n := (s_1, \dots, s_t) \in \text{soc}(W)$$

we have

$$h := (u_1, \dots, u_t)\gamma = (s_1^{-1}x_1, \dots, s_t^{-1}x_t)\gamma = n^{-1}g \in W,$$

therefore

$$V^h = ((U \cap S)^{u_1} \times \dots \times (U \cap S)^{u_t})^\gamma = V^\gamma = V$$

since $U \cap S$ is normal in U . We deduce that $h = n^{-1}g \in N_W(V)$ and since $n \in \text{soc}(W)$ the claim follows.

We claim that G_1/S is a cyclic m -group (perhaps trivial). Indeed, we have the following subgroup series:

$$\text{soc}(W) = N/\Phi(G) \leq T_1 C_W(T_1) \leq N_W(T_1) \leq W,$$

thus

$$\frac{G_1}{S} \cong \frac{N_W(T_1)}{T_1 C_W(T_1)} \cong \frac{N_W(T_1)/\text{soc}(W)}{T_1 C_W(T_1)/\text{soc}(W)} \lesssim \frac{W/\text{soc}(W)}{T_1 C_W(T_1)/\text{soc}(W)}.$$

It follows that G_1/S is isomorphic to a section of $W/\text{soc}(W) \cong G/N$, which is a cyclic m -group. So the claim follows.

We claim that $N_W(V) \neq W$. If it were not the case, then V would be normal in W and, since $N/\Phi(G)$ is a minimal normal subgroup of W and $U \cap S \neq S$, since $US = G_1$, the simplicity of S implies $U \cap S = \{1\}$ and $G_1/S \cong U$ is cyclic, therefore U is a cyclic maximal subgroup of the almost-simple group G_1 , contradicting Herstein's theorem, which says that a nonsolvable finite group cannot have abelian maximal subgroups (see Lemma 1.1.19). This is also a consequence of [48, Theorem 1.3.6]. So the claim follows.

Since $\Phi(G)$ is a nontrivial 2-group, the above three paragraphs imply that the preimage of $N_W(V)$ in G is a proper subgroup of G of even order and it is not contained in C because otherwise

$$W = N_W(V) \text{soc}(W) = N_W(V)(N/\Phi(G)) \leq N_W(V)(C/\Phi(G)) = C/\Phi(G) < W,$$

a contradiction. Therefore, the preimage of $N_W(V)$ is m -pyramidal by Lemma 2.2.4(1), and hence it is solvable by the minimality of $|G|$. So $U \cap S$ is solvable. Since

$$U/U \cap S \cong US/S = G_1/S$$

is a cyclic m -group, we deduce that U is solvable.

Summarizing, we have $N_W(V) \text{soc}(W) = W$, $N_W(V) \neq W$, G_1/S is a cyclic m -group, if $G_1 = S$ then G_1 is a minimal simple group, and if $G_1 \neq S$ then G_1 has only one nonsolvable maximal subgroup, which is the unique maximal subgroup containing S . By Lemma 1.2.7, $U \cap S$ is a maximal subgroup of S . Obviously, $U \cap S \leq N_S(U \cap S) < S$ by the simplicity of S . Therefore, $N_S(U \cap S) = U \cap S$, hence

$$N_W(V) \cap \text{soc}(W) = N_{\text{soc}(W)}(V) = N_{S^t}((U \cap S)^t) = (N_S(U \cap S))^t = V.$$

Since $N_W(V) \text{soc}(W) = W$ and

$$U/U \cap S \cong G_1/S \cong C_{m^s}$$

is a cyclic m -group for some integer s , writing $|U| = 2^d \cdot r$ with r odd and $W/\text{soc}(W) \cong C_{m^{b_1}}$ where $b_1 = b + 1$, we have

$$|N_W(V)| = |W : \text{soc}(W)| \cdot |N_W(V) \cap \text{soc}(W)| = m^{b_1} \cdot |U \cap S|^t = m^{b_1 - st} \cdot 2^{dt} \cdot r^t.$$

Since the preimage of $N_W(V)$ in G is m -pyramidal by Lemma 2.2.4(1), and $\Phi(G)$ is of n -type by Lemma 2.2.4(5), $N_W(V)$ is of n -type by Lemma 2.2.10, in other words dt is divisible by n . Since t is a power of m and m is coprime to n , we conclude that d is divisible by n . This means exactly that U is of n -type. \square

2.3.4 Step 4

$$G_1 = S.$$

Proof. Recall that, if X is an almost-simple group with socle S , which is nonabelian and simple, we say that a maximal subgroup H of S is *X-ordinary* if its X -class equals its S -class, in other words for every $x \in X$ there exists $s \in S$ such that $H^x = H^s$. If H is an X -ordinary maximal subgroup of S , then $N_X(H)$ is maximal in X with $N_X(H)S = X$, and

$$|N_X(H)| = |X||H|/|S|$$

by Lemma 1.2.2. Of course, if

$$S \leq X \leq Y \leq \text{Aut}(S)$$

and H is a Y -ordinary maximal subgroup of S , then H is also X -ordinary. Concerning our situation, we have $S \leq G_1 \leq \text{Aut}(S)$, G_1/S is a cyclic m -group and every maximal subgroup of G_1 not containing S is solvable. Assume by contradiction that $G_1 \neq S$. Since G_1/S is not a 2-group, $\text{Out}(S)$ is not a 2-group, so with the help of Theorem 1.2.5 we have S is isomorphic to one of the following groups:

$$\text{PSL}(2, 2^m), \text{PSL}(2, 3^m) \text{ or } \text{Sz}(2^m).$$

By Table 1.3, if $S \cong \text{PSL}(2, 2^m)$ or $\text{PSL}(2, 3^m)$ then S has a G_1 -ordinary maximal subgroup H of type $E_{2^m} : (2^m - 1)$ in the first case and $\text{PSL}(2, 3)$ in the second case when $m > 3$. Thus

$$|N_{G_1}(H)| = 2^m \cdot m \cdot (2^m - 1) \quad \text{or} \quad 2^2 \cdot 3 \cdot m$$

because $|G_1 : S| = m$, contradicting the fact that $N_{G_1}(H)$ is of n -type since m and n are distinct prime numbers, with n odd unless $(n, m) = (2, 3)$. If $m = 3$ and $S \cong \text{PSL}(2, 3^3)$ then G_1 has a maximal subgroup of type $C_{13} \rtimes C_6$, which is not of 2-type (see the second line of Table 1.3). If $S \cong \text{Sz}(2^m)$, by Table 1.4 S has a G_1 -ordinary maximal subgroup H of type $D_{2(2^m-1)}$. It is easy to deduce that

$$|N_{G_1}(H)| = 2 \cdot m \cdot (2^m - 1)$$

and $N_{G_1}(H)$ is not of n -type, a contradiction. \square

2.3.5 Step 5

Since W is a subgroup of $S \wr P$ containing $S^t = \text{soc}(W)$, with W projecting surjectively onto the transitive cyclic group $P \leq \text{Sym}(t)$, we deduce that W is isomorphic to the standard wreath product $S \wr P$, where P acts on S^t by permuting the coordinates. Consider

$$\Delta = \{(s, s, \dots, s) : s \in S\} \leq S^t, \quad H := N_W(\Delta).$$

It is clear that $P \leq H$, hence $\text{soc}(W)H = W$. Suppose $t = 1$. Then $P = \{1\}$ and $W = S$ is a nonabelian simple group, this contradicts the fact that W has a normal subgroup

$C/\Phi(G)$ of index m . Thus $t \geq 2$. Therefore Δ is not normal in W , since $\text{soc}(W)$ is a minimal normal subgroup of W , therefore $H \neq W$. Since $\Delta \cong S$ is nonsolvable and $\Delta \leq H$, we obtain that H is nonsolvable, thus the preimage of H in G is a nonsolvable proper subgroup of G , of even order and supplementing C , so it is m -pyramidal by Lemma 2.2.4(1). This contradicts the minimality of $|G|$.

This concludes the proof of the fact that, if $m \neq 7$ is a prime number, then any m -pyramidal group is solvable.

Chapter 3

The solvability of pyramidal groups of prime power degree

In this chapter, we discuss the solvability of pyramidal groups of prime power degree and prove Theorem B, which we state again for convenience. This theorem was proved in [9].

Theorem B (X. Gao, M. Garonzi). Let m be a prime power p^k with $p \neq 7$ an odd prime. Then the following are equivalent.

- (1) Every m -pyramidal group is solvable.
- (2) k is odd or $m = 9$.

As follows, we construct a family of nonsolvable p^k -pyramidal groups for an even integer k and a prime number p . However, when k is odd, we cannot use the same method to construct a nonsolvable p^k -pyramidal group.

Let q be an odd prime power and let $V = \mathbb{F}_q^2$. It is clear that $\mathrm{SL}(2, q)$ has a unique element ι of order 2 and ι acts on V by inversion. Thus the group

$$G = V \rtimes \mathrm{SL}(2, q)$$

is a q^2 -pyramidal group by Proposition 2.2.5. This shows that, if p is an odd prime number and k is an even positive integer, with $p^k \neq 9$, then there exists a nonsolvable p^k -pyramidal group. More generally, if there exist N and A as in Proposition 2.2.5, with A nonsolvable, then we can construct a nonsolvable $|N|$ -pyramidal group.

On the other hand, if there exists a nonsolvable subgroup H of $\mathrm{GL}(k, q)$ with k odd and -1 is the unique involution of H then the above argument shows that there exists

a nonsolvable q^k -pyramidal group. However, this H does not exist, because assuming it exists, defining

$$U := H \cap \mathrm{SL}(k, q),$$

the order $|U|$ is odd because H contains -1 as the unique involution and, since k is odd, $(-1)^k = -1$, thus $-1 \notin \mathrm{SL}(k, q)$. Therefore U is solvable and H/U is abelian because

$$H/U = H/H \cap \mathrm{SL}(k, q) \cong \mathrm{SL}(k, q)H/\mathrm{SL}(k, q) \leq \mathrm{GL}(k, q)/\mathrm{SL}(k, q) \cong \mathbb{F}_q^*,$$

so H is solvable.

3.1 Preliminaries

To prove Theorem B, we need the following results. In the following two results, we denote by $O(G)$ the largest normal subgroup of G of odd order.

Lemma 3.1.1 (Theorem 2 of [54]). *Let G be a finite group whose 2-Sylow subgroup is a generalized quaternion group. Then $G/O(G)$ has a center of order 2.*

Lemma 3.1.2 (Theorem 1 of [55]). *Let G be a finite group with dihedral Sylow 2-subgroups. Then $G/O(G)$ is isomorphic to one of the following.*

- (1) *A subgroup of $\mathrm{PFL}(2, q)$ containing $\mathrm{PSL}(2, q)$, q odd.*
- (2) *The alternating group A_7 .*
- (3) *A Sylow 2-subgroup of G .*

The following theorem was proved in [56].

Theorem 3.1.3. *Let G be a nonabelian simple group with $H < G$ and $|G : H| = p^a$, p prime. One of the following holds.*

- (1) *$G = A_n$ and $H \cong A_{n-1}$ with $n = p^a$.*
- (2) *$G = \mathrm{PSL}(n, q)$ and H is the stabilizer of a line or hyperplane. Then $|G : H| = (q^n - 1)/(q - 1) = p^a$. (Note n must be prime.)*
- (3) *$G = \mathrm{PSL}(2, 11)$ and $H \cong A_5$ with $11 = p^a$.*
- (4) *$G = M_{23}$ and $H \cong M_{22}$ with $23 = p^a$ or $G = M_{11}$ and $H \cong M_{10}$ with $11 = p^a$.*
- (5) *$G = \mathrm{PSU}(4, 2) \cong \mathrm{PSp}(4, 3)$ and H is the parabolic subgroup of index 27.*

3.2 The proof of Theorem B

If k is even and $m \neq 9$ then, choosing $q = p^{k/2}$, the group $\mathbb{F}_q^2 \rtimes \mathrm{SL}(2, q)$ is m -pyramidal and nonsolvable. This proves that (1) implies (2). The proof of the other implication is the content of the following two propositions. We will use the notation $i(G)$ to denote the number of involutions of G .

Proposition 3.2.1. *Any 9-pyramidal group is solvable.*

Proof. We prove the result by contradiction. Assume G is a nonsolvable 9-pyramidal group of minimal order. Let $O(G)$ be the maximal normal subgroup of G with odd order. Then $G/O(G)$ is a 1, 3 or 9-pyramidal group. Obviously, the quotient group $G/O(G)$ is not a 3-pyramidal group because otherwise $G/O(G)$ would be solvable by Theorem A and then G would be solvable as well, a contradiction.

Suppose $G/O(G)$ is a 9-pyramidal group. The minimality of $|G|$ implies that $O(G) = \{1\}$. Let N be a minimal normal subgroup of G , then

$$N \cong C_2^n \quad \text{or} \quad N \cong S^n$$

where $n \geq 1$ and S is a nonabelian simple group. Since all involutions of G are conjugate,

$$2^n - 1 = 9 \quad \text{or} \quad i(N) = (i(S) + 1)^n - 1 = 9,$$

this implies that $n = 1$ and $N \cong S$. Recall that $O(G) = \{1\}$ and all involutions are conjugate in G , so S is the unique minimal normal subgroup of G . We claim that $C_G(S) = \{1\}$. If it were not the case, then there would be a minimal normal subgroup of G distinct from S that is contained in $C_G(S)$ since

$$S \cap C_G(S) = Z(S) = \{1\},$$

a contradiction. This proves that $C_G(S) = \{1\}$. Thus G is an almost-simple group with socle S . Let $x_1, x_2, \dots, x_9 \in S$ be the 9 involutions of G . Since they are conjugate in G , the conjugacy classes x_i^S , $i = 1, \dots, 9$ all have the same size d . This implies that $d \in \{3, 9\}$ because $Z(S) = \{1\}$, contradicting Theorem 1.1.16 again.

Finally, we assume that $G/O(G)$ is 1-pyramidal. Then a Sylow 2-subgroup of $G/O(G)$ has a unique involution, thus it is a generalized quaternion group or a cyclic group by Theorem 1.1.24. Since $O(G)$ is solvable and G is nonsolvable, the quotient group $G/O(G)$ is nonsolvable and a Sylow 2-subgroup of $G/O(G)$ is a generalized quaternion group by Theorem 1.1.25. Since the group $O(G)$ is of odd order, this implies that a Sylow 2-subgroup of G is also a generalized quaternion group. Hence a Sylow 2-subgroup of G has a unique involution. This implies that, if x, y are two arbitrary distinct involutions of G , we have $xy \neq yx$. It follows that $|C_G(K)|$ is odd, and a Sylow 2-subgroup of

$$J := G/C_G(K)$$

is also a generalized quaternion group. On the other hand, G acts transitively on the 9 involutions of G by conjugation action, namely, we have the following homomorphism:

$$\alpha : G \rightarrow S_9 : \{x_1, x_2, \dots, x_9\} \rightarrow \{x_1, x_2, \dots, x_9\}.$$

Obviously,

$$\text{Ker}(\alpha) = \bigcap_{i=1}^9 C_G(x_i) = C_G(K)$$

and $G/\text{Ker}(\alpha) \lesssim S_9$. Therefore, J is isomorphic to a transitive subgroup of S_9 . Since the Sylow 2-subgroups of S_9 and A_9 are $(D_8 \times D_8) \times C_2$ and $C_2 \wr C_2^2$, respectively, as determined using GAP [20], and these are not generalized quaternion groups, it follows that J does not contain A_9 . By Theorem 1.1.15 the maximal imprimitive subgroups of S_9 are isomorphic to the wreath product $S_3 \wr S_3$, which is solvable, therefore J is primitive of degree 9. The nonsolvable primitive groups of degree 9 do not have generalized quaternion Sylow 2-subgroups, as can be seen using the AllPrimitiveGroups function in [20]. We have reached a contradiction. \square

Proposition 3.2.2. *Let G be a p^k -pyramidal group, where $p \neq 7$ and k is odd. Then G is solvable.*

Proof. We prove the result by contradiction. Assume G is a nonsolvable pyramidal group with a number of involutions that is a prime power with odd exponent, and assume G has minimal order with these properties. Write $m = p^k$ with k odd. Let $O := O(G)$ be the largest normal subgroup of G with odd order then, by Lemma 2.2.4(4) G/O is a p^a -pyramidal group, where $0 \leq a \leq k$. Let N/O be a minimal normal subgroup of G/O , then

$$N/O \cong S^n \quad \text{or} \quad N/O \cong C_2^m,$$

where $n \geq 1$ and S is a nonabelian simple group. First, if $N/O \cong S^n$ then

$$i(G/O) = (i(S) + 1)^n - 1 = p^a.$$

Since $i(S) > 1$ and p is odd, Lemma 1.1.21 implies that $n = 1$ and $N/O \cong S$. Since all involutions of G/O are conjugate and G/O does not have normal subgroup of odd order, the quotient group G/O has a unique minimal normal subgroup N/O , this implies that $C_{G/O}(N/O)$ is trivial. Hence G/O is an almost-simple group with socle S and $i(S) = p^a$. Since the involutions are all conjugate in G , they all belong to S and their conjugacy classes in S all have the same size. This implies that the conjugacy class size of an involution in S is a prime power, contradicting Theorem 1.1.16.

In the rest of the proof we will assume that $N/O \cong C_2^m$. In particular $2^n - 1 = p^a$ hence $a \in \{0, 1\}$ by Lemma 1.1.21, that is, G/O is p -pyramidal or 1-pyramidal. If G/O is p -pyramidal then, by Theorem A, G/O is solvable, and hence G is solvable, a contradiction. In the rest of the proof we will assume that G/O is 1-pyramidal, so that the Sylow

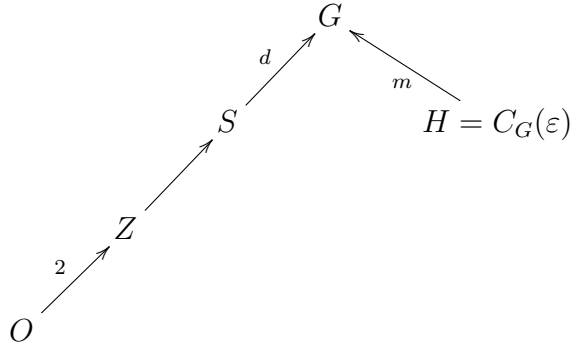
2-subgroups of G/O are generalized quaternion groups. This implies that the Sylow 2-subgroups of G are also generalized quaternion, hence if x, y are two arbitrary involutions of G then $xy \neq yx$. By Lemma 3.1.1, the center Z/O of G/O has order 2. Then the Sylow 2-subgroups of G/Z are dihedral, hence G/Z satisfies one of the items of Lemma 3.1.2. If

$$\frac{G}{Z} \cong \frac{G/O}{Z/O}$$

is a 2-group, then G/O would be solvable because Z/O is an abelian group. Therefore, by the Feit-Thompson theorem, G would be solvable, a contradiction. Thus either $G/Z \cong A_7$ or G/Z has a simple normal subgroup S/Z such that

$$\text{PSL}(2, q) \cong S/Z \trianglelefteq G/Z \leq \text{P}\Gamma\text{L}(2, q),$$

where $q = r^f$, r an odd prime. In the second case G/Z is an extension of S/Z by a subgroup of $\text{Out}(\text{PSL}(2, q)) \cong C_2 \times C_f$. Observe that the centralizer $H := C_G(\varepsilon)$ has ε as unique involution because any two involutions of G do not commute, and hence the order of $C = C_G(K)$ is odd and C is contained in O . Obviously, $|G : H| = m = p^k$. Now we have the following graph:



where $d = 1$ or d is a divisor of $2f$. Note that

$$|G : HS| \cdot |HS : H| = |G : H| = p^k,$$

so $|HS : H|$ divides p^k . Moreover,

$$|S : HZ \cap S| = |HZS : HZ| = |HS : HZ| = \frac{|HS : H|}{|HZ : H|}$$

hence $HZ \cap S$ has prime power index in S , say p^b with $b \leq k$.

We claim that H is nonsolvable. If $HZ \cap S = S$, i.e., $S \leq HZ$, then

$$S/Z \leq HZ/Z \cong H/H \cap Z$$

and $H/H \cap Z$ is nonsolvable since it contains a nonsolvable subgroup S/Z , so H is nonsolvable. If $HZ \cap S \neq S$, then the nonabelian simple group S/Z has a proper subgroup $(HZ \cap S)/Z$ such that

$$\frac{|S/Z|}{|(HZ \cap S)/Z|} = \frac{|S|}{|HZ \cap S|}$$

is a prime power. In the light of Theorem 3.1.3, either $HZ \cap S$ has index $r^f + 1 = p^b$ in S , contradicting the fact that both r and p are odd primes, or $S/Z \cong A_7$ with $p^b = 7$, or $S/Z \cong \text{PSL}(2, 11)$ with $p^b = 11$. The following quotient group is isomorphic to A_6 or A_5 , respectively.

$$\frac{HZ \cap S}{Z} = \frac{Z(S \cap H)}{Z} \cong \frac{S \cap H}{S \cap H \cap Z} = \frac{S \cap H}{Z \cap H}.$$

It follows that H is nonsolvable.

Let R be a minimal normal subgroup of G contained in O . Note that R is an elementary abelian group because R is solvable. Let

$$I_\varepsilon := \{n \in R : n^\varepsilon = n^{-1}\} \leq R.$$

Lemma 2.2.4(4) implies that G/R is m/ℓ -pyramidal where $\ell = |I_\varepsilon|$. Recall that m is a power of p , so ℓ must also be a power of p . Write $\ell = |I_\varepsilon| = p^t$. By the minimality of $|G|$ we have that $k - t$ is even, thus t is odd. I_ε is normalized by H because, if $h \in H$ and $n \in I_\varepsilon$, then $h\varepsilon = \varepsilon h$ hence

$$(n^h)^\varepsilon = n^{h\varepsilon} = n^{\varepsilon h} = (n^{-1})^h = (n^h)^{-1}.$$

We can see R as a finite dimensional \mathbb{F}_p -vector space acted upon by the linear transformation ε . Since $\varepsilon^2 = 1$ and p is odd, ε is diagonalizable over \mathbb{F}_p and its unique eigenvalues are 1 and -1 . Observe that I_ε is precisely the eigenspace of -1 in R and $H \cap R$ is the eigenspace of 1, so

$$\dim(I_\varepsilon) + \dim(H \cap R) = \dim(R),$$

thus

$$\ell = p^t = |I_\varepsilon| = |R : H \cap R| = |HR : H|.$$

Since $|G : H|$ is odd, $|G : HR|$ is also odd. This implies that any Sylow 2-subgroup of HR is a Sylow 2-subgroup of G , hence a Sylow 2-subgroup of HR is a generalized quaternion group, thus HR is a pyramidal group by Lemma 2.2.6. Note that

$$|HR : C_{HR}(\varepsilon)| = |HR : C_G(\varepsilon) \cap HR| = |HR : H|,$$

so HR is a p^t -pyramidal group. Since H is nonsolvable, using the minimality of $|G|$ again, we have $HR = G$ and $t = k$. Observe that R is an abelian minimal normal subgroup of G , thus $H \cap R$ is normal in H and in R . Since $HR = G$, we deduce that $H \cap R$ is normal in G hence $H \cap R = \{1\}$ by the minimality of R . It follows that $G = R \rtimes H$, $R \cong \mathbb{F}_p^k$ and ε acts on R as the inversion map $x \mapsto -x$. Let $\bar{H} := H/C_H(R)$. Since ε is the only involution of H and it does not centralize R , the centralizer $C_H(R)$ has odd

order, therefore \overline{H} is 1-pyramidal by Lemma 2.2.4(4). We can identify \overline{H} with a subgroup of $\mathrm{GL}(k, p)$ because

$$N_G(R)/C_G(R) \cong H/C_H(R) \lesssim \mathrm{Aut}(R) \cong \mathrm{GL}(k, p).$$

Let $U := \overline{H} \cap \mathrm{SL}(k, p)$. Suppose $|U|$ is odd. Then U is solvable. Observe that $\overline{H}/U \cong \overline{H}\mathrm{SL}(k, p)/\mathrm{SL}(k, p)$ is abelian because it is isomorphic to a subgroup of $\mathrm{GL}(k, p)/\mathrm{SL}(k, p) \cong C_{p-1}$, so \overline{H} is solvable, this implies that H is also solvable, a contradiction. Therefore $|U|$ is even, hence U contains an involution. Since $\overline{\varepsilon} = \varepsilon C_H(R)$ is the only involution of \overline{H} , we have $\overline{\varepsilon} \in U$, so that $\det(\overline{\varepsilon}) = 1$. Since $\overline{\varepsilon}$ is the inversion map, we deduce that $(-1)^k = \det(\overline{\varepsilon}) = 1$ contradicting the fact that k is odd. \square

Chapter 4

Some properties of pyramidal groups

We proved that if $m \neq 7$ is a prime number then all m -pyramidal groups are solvable. The natural question arises: what is the structure of an m -pyramidal group? and what is the order of an m -pyramidal group? In section 4.2 we discuss the structure of 3-pyramidal groups and give their classification. In section 4.3 we discuss the set of orders of m -pyramidal groups.

4.1 Preliminaries

We introduce some properties related to p -length, homocyclic groups, and Suzuki-2 groups.

Definition 4.1.1. *We say that G is a p -solvable group if it admits a series of normal subgroups*

$$\{1\} = V_0 < V_2 < \dots < V_n = G$$

such that each factor V_{i+1}/V_i is either a p -group or a p' -group, the p -length of G is the length l of the upper p -series

$$\{1\} = P_0 \leq N_0 < P_1 < N_1 < P_2 < \dots < P_l \leq N_l = G$$

where N_k/P_k is the largest normal p' -subgroup of G/P_k and P_{k+1}/N_k the largest normal p -subgroup of G/N_k , for $k = 0, \dots, l - 1$.

Definition 4.1.2. *A group G is called homocyclic if it is a direct product of isomorphic cyclic groups.*

Definition 4.1.3. *A Suzuki 2-group is a group G which has the following properties.*

- (1) G is a nonabelian 2-group.

- (2) G has more than one involution.
- (3) There exists a soluble subgroup of automorphism group of G which permutes the set of involutions in G transitively.

Lemma 4.1.4 (Theorem 7.9 of [5]). *Let G be a Suzuki 2-group. Then*

$$G' = \Phi(G) = Z(G) = \{x \in G : x^2 = 1\}.$$

Obviously, the center subgroup $Z(G)$ of a Suzuki 2-group G is an elementary abelian 2-group because the exponent of $Z(G)$ is 2. Note that if G is a finite p -group, then $\Phi(G) = G'G^p$, where $G^p = \langle g^p : g \in G \rangle$ (see [45, 5.3.2]). It follows that $G/\Phi(G)$ is isomorphic to an elementary abelian p -group. Therefore, the Suzuki 2-group G is of exponent 4 and class 2. In particular, it was proved in [57] that if G is a Suzuki 2-group and $Z(G) = q$ then $|G| = q^2$ or q^3 . The additional details about the Suzuki 2-groups can be found in [5] and [57].

Since m -pyramidal groups are solvable where $m \neq 7$ is a prime number. Thompson's result [5, Theorem 8.6 of Chapter IX] is now very useful for us. It states the following.

Theorem 4.1.5 (Thompson). *Suppose that G is a solvable group of even order and that a Sylow 2-subgroup of G contains more than one involution. Suppose that all the involutions in G are conjugate. Then the 2-length of G is 1 and the Sylow 2-subgroups of G are either homocyclic or Suzuki 2-groups.*

Lemma 4.1.6. *Let $G = N \rtimes A$ where $|N|$ and $|A|$ are coprime. Then $C_G(N) = Z(N) \times C_A(N)$.*

Proof. Since $C_G(N)$ and N are normal subgroups of G , so is $C_G(N) \cap N = Z(N)$. In particular, $C_G(N) \cap A = C_A(N)$ is normal in A . Let $g = na \in G$, where $n \in N$ and $a \in A$, we have

$$C_A(N)^g = C_A(N)^{na} = C_A(N),$$

thus $C_A(N)$ is normal in G . Note that $(|Z(N)|, |C_A(N)|) = 1$, so

$$Z(N) \cap C_A(N) = \{1\}.$$

It follows that the extension of $Z(N)$ by $C_A(N)$ is $Z(N) \times C_A(N)$, which is a subgroup of $C_G(N)$. Conversely, let $g = na \in C_G(N)$ where $n \in N$ and $a \in A$, then

$$n^g = n^{na} = n^a = n,$$

thus $na = an$. Moreover, $ag = ana = ga$, so that $ga^{-1} = a^{-1}g$. Since $(|N|, |A|) = 1$, there exist $u, v \in \mathbb{Z}$ such that $u|N| + v|A| = 1$, thus

$$g = (na)^{u|N|+v|A|} = n^{v|A|} \cdot a^{u|N|}.$$

Observe that

$$n^{v|A|} = (ga^{-1})^{v|A|} = g^{v|A|} \in C_G(N) \cap N = Z(N)$$

and

$$a^{u|N|} = (n^{-1}g)^{u|N|} = g^{u|N|} \in C_G(N) \cap A = C_A(N).$$

Thus

$$g = n^{v|A|} \cdot a^{u|N|} \in Z(N) \times C_A(N).$$

This implies that

$$C_G(N) \leq Z(N) \times C_A(N).$$

Therefore, $C_G(N) = Z(N) \times C_A(N)$. □

Singer cycle plays an important role in Section 4.3.

Definition 4.1.7. Assume $\mathbb{F} = \mathbb{F}_p^n$ is a finite field of size q . Let V be the underlying vector space of $\text{GL}(n, p)$ and let x be a generator for the multiplicative group of the finite field \mathbb{F} . Then identifying V with \mathbb{F} , given $v \in V$, the map

$$\varphi : V \rightarrow V, \quad \varphi(v) := vx$$

is called *Singer cycle*.

Note that $\varphi \in \text{Aut}(V) \cong \text{GL}(n, p)$. In fact, for any two vectors u and v of V , we have

$$\varphi(u + v) = (u + v)x = ux + vx = \varphi(u) + \varphi(v)$$

since V is a vector space over \mathbb{F} . Obviously,

$$\text{Ker}(\varphi) = \{v \in V : vx = 0\} = 0$$

and for any $v \in V$ there exist $vx^{-1} \in V$ such that $\varphi(vx^{-1}) = v$, thus φ is a bijective homomorphism from V to itself.

Moreover, it is easy to see that $o(\varphi) = q - 1$ and $\langle \varphi \rangle$ acts regularly on non-zero vectors of the vector space V . To see this, given two nonzero vectors v and w , we see that $v(v^{-1}w) = w$ and $vx = v$ if and only if $x = 1$, thus $\langle \varphi \rangle$ acts transitively on $V \setminus \{0\}$ and the kernel of this action is trivial.

In fact, if q is a power of a prime, then $\text{GL}(n, q)$ contains Singer cycles for all n and q , and we call the subgroup generated by a Singer cycle a *Singer subgroup*. In particular, all Singer subgroups of $\text{GL}(n, q)$ are conjugate (see [58, Page 187]).

4.2 The proof of Theorem C

In this section, we provide the proof of Theorem C, which we restate here once more for the benefit of the reader. It was proved in [8]

Theorem C (X. Gao, M. Garonzi). Let G be a finite group and $O(G)$ the largest normal subgroup of G of odd order. Let K be the subgroup generated by the involutions of G . Then G is 3-pyramidal if and only if one of the following holds.

- (1) G is isomorphic to $S_3 \times H$ where H is a group of odd order.
- (2) $O(G) \leq C_G(K)$ and $G/O(G)$ is isomorphic to $N \rtimes A$ where N is the Suzuki 2-group of order 64 and A is a subgroup of $\text{Aut}(N)$ of order 3 or 15.
- (3) $O(G) \leq C_G(K)$ and $G/O(G)$ is isomorphic to $(C_{2^n} \times C_{2^n}) \rtimes A$ where A is the cyclic group of order 3 generated by the automorphism $(a, b) \mapsto (b, (ab)^{-1})$.

In item (1) $K \cong S_3$ while in items (2), (3) $K \cong C_2 \times C_2$.

Proof. Let G be a 3-pyramidal group and write $|G| = 2^n \cdot d$, where d is odd. Let K be the subgroup of G generated by the three involutions i, j, k and let $C := C_G(K)$. Suppose first that $n = 1$. Then $K \cong S_3$ and $G \cong C_G(K) \times K$ by Lemma 2.2.4(6). Since G has exactly 3 involutions, and all of them are contained in K , $|C_G(K)|$ is odd. Now assume that $n \geq 2$. Lemma 2.2.1 implies that n is even, $K \cong C_2 \times C_2$ and $G/C \cong A_3$. Since K and $O(G)$ are normal subgroups of G of coprime orders, $K \cap O(G) = \{1\}$ hence $O(G) \leq C$. By Lemma 2.2.4(4) we may assume that $O(G) = \{1\}$. By Theorem A, G is solvable and Theorem 4.1.5 applies, so the 2-length of G is 1, namely, G has an upper 2-series

$$\{1\} = P_0 \leq N_0 < P_1 \leq N_1 = G,$$

where N_0 and N_1/P_1 are the largest normal 2'-subgroups of G and G/P_1 , respectively, and P_1/N_0 is the largest normal 2-subgroup of G/N_0 . Note that $|G/P_1|$ and $|N_0|$ are odd. Since $O(G) = \{1\}$, $N_0 = \{1\}$, this means that P_1 is a Sylow 2-subgroup of G and it is normal in G . In particular P_1 is the unique Sylow 2-subgroup of G . Write $N := P_1$. Hence, N has a complement A in G by the Schur-Zassenhaus theorem 1.1.10, i.e., $G = N \rtimes A$. Observe that $|A|$ is odd and

$$N_G(N)/C_G(N) = G/C_G(N) \lesssim \text{Aut}(N).$$

We claim that $C_G(N) = Z(N)$ is a 2-group. Indeed, Lemma 4.1.6 implies that

$$C_G(N) = Z(N) \times C_A(N).$$

Since $|C_A(N)|$ and $|Z(N)|$ are coprime, we have that $C_A(N)$ is a characteristic subgroup of $C_G(N)$, and hence $C_A(N)$ is normal in G . Note that, since $|A|$ is odd and so, as $O(G) = \{1\}$, $C_A(N) = \{1\}$. Thus

$$C_G(N) = Z(N) \times C_A(N) = Z(N).$$

Therefore $G/Z(N) \lesssim \text{Aut}(N)$ and A is isomorphic to a subgroup of $\text{Aut}(N)$. In the light of Theorem 4.1.5, N is either homocyclic or a Suzuki 2-group.

Assume that N is a homocyclic group, i.e. a direct product of pairwise isomorphic cyclic groups. Since N has three involutions, $N \cong C_{2^m} \times C_{2^m}$ for some positive integer m . It is easy to see that $\text{Aut}(N)$ is isomorphic to the group of 2×2 matrices with coefficients in $\mathbb{Z}/2^m\mathbb{Z}$ and invertible determinant, therefore $|\text{Aut}(N)| = 3 \cdot 2^{4m-3}$. Since A is isomorphic to a subgroup of $\text{Aut}(N)$ with odd order, $A \cong C_3$ and it is a Sylow 3-subgroup of $\text{Aut}(N)$. Note that all Sylow 3-subgroups of $\text{Aut}(N)$ are conjugate by Sylow's theorem, A is conjugate in $\text{Aut}(N)$ to $\langle \gamma \rangle$ where $\gamma : N \rightarrow N$ is defined by

$$(a, b) \mapsto (b, (ab)^{-1}).$$

Therefore $G \cong N \rtimes \langle \gamma \rangle$.

We next assume that N is a Suzuki 2-group. Since N has three involutions, we have

$$\Phi(N) = N' = Z(N) \cong C_2^2$$

by Lemma 4.1.4. A simple inspection using GAP [20] shows that no group of order 16 has these properties, therefore [57] implies that $|N| = 64$ and N is the unique Suzuki 2-group of order 64, $\text{SmallGroup}(64, 245) = C_2^2.C_2^4$, $|\text{Aut}(N)| = 3 \cdot 5 \cdot 2^{10}$ and G is isomorphic to $N \rtimes A$ where A is a subgroup of $\text{Aut}(N)$ of order 3 or 15. Since the subgroups of $\text{Aut}(N)$ of order 3 or 15 are Hall subgroups and $\text{Aut}(N)$ is solvable (by GAP [20]), they form a unique conjugacy class of subgroups, so G is determined completely up to isomorphism.

Conversely, it is not difficult to see that G is 3-pyramidal if $G \cong S_3 \times H$ where H is a group of odd order. Assume now that 4 divides $|G|$, let $O := O(G)$ and assume that O centralizes all involutions of G and that G/O is one of the groups in cases (2) and (3). Since 4 divides $|G/O|$ and G/O is 3-pyramidal, it has exactly 3 involutions iO , jO and kO . Let $zO \in G/O$ with $o(zO) \geq 3$ then $o(z) \geq 3$ since $o(zO)$ divides $o(z)$. Thus the union $iO \cup jO \cup kO$ contains all involutions of G . Since $|O|$ is odd, by the Schur-Zassenhaus theorem 1.1.10, we have $O\langle i \rangle \cong O \rtimes C_2$ and it contains an element of order 2, which can be denoted by i . Note that iO contains a unique involution because otherwise there would exist $\{1\} \neq y \in O$ such that $o(iy) = 2$. Since O is a group of odd order that centralizes all involutions of G , $iyiy = y^2 = 1$, implying that y would be an involution of O , a contradiction. Similarly, we can get that each of jO , kO contains a unique involution, therefore G has precisely three involutions, which we may assume to be i, j, k . Since iO, jO and kO are conjugate in G/O , there exists $g \in G$ such that

$$i^gO = (iO)^{gO} = jO,$$

and it follows that $i^g \in jO$. Since $o(i^g) = 2$ and j is the unique involution in jO , we obtain that $i^g = j$. The same argument shows that j and k are conjugate in G , so G is 3-pyramidal. \square

By the Feit-Thompson theorem, all finite groups of odd order are solvable. Therefore, the above Theorem C implies that all 3-pyramidal groups are solvable. The quotients $G/O(G)$ in item (2) are $\text{SmallGroup}(192,1025) = (C_2^2.C_2^4) : C_3$, $\text{SmallGroup}(960, 5748) = ((C_2^2.C_2^4) : C_5) : C_3$.

We can construct infinite families of 3-pyramidal groups as follows: let Y be a group of odd order with a normal subgroup X of index 3 and let $N := C_{2^n} \times C_{2^n}$. The group Y acts on N as an automorphism of order 3 as in item (3) of the statement of Theorem C, by composition

$$Y \rightarrow Y/X \cong C_3 \rightarrow \text{Aut}(N).$$

The semidirect product $G := N \rtimes Y$ is 3-pyramidal and $O(G) = X$. Also, note that there exist 3-pyramidal groups whose Sylow 2-subgroups are not normal. An example is $\text{SmallGroup}(1296,2705) = ((C_3 \times ((C_3 \times C_3) : C_4)) : C_4) : C_3$.

4.3 The proof of Theorem D

Let m be an odd integer and let X_m be the set of orders of m -pyramidal groups. In this section we will prove Theorem D, which we now state again for convenience. This theorem was proved in [9].

Theorem D (X. Gao, M. Garonzi). Let $m \neq 7$ be an odd prime number. If m has the form $2^n - 1$ for some integer n , set $Y_m = \{2^a \cdot m \cdot d : n|a, d \text{ odd}\}$, otherwise $Y_m = \emptyset$. Write $m - 1 = 2^t \cdot r$ with r odd and let $Z_m = \{2^a \cdot m \cdot d : 1 \leq a \leq t, d \text{ odd}\}$. Then $X_m = Y_m \cup Z_m$.

Proof. If P is any nontrivial 2-subgroup of $\text{Aut}(C_m) \cong C_{m-1}$ then, by Proposition 2.2.5, $C_m \rtimes P$ is m -pyramidal of order $m \cdot 2^a$ with $1 \leq a \leq t$, and if d is any odd positive integer then $C_d \times (C_m \rtimes P)$ is m -pyramidal of order $2^a \cdot m \cdot d$, therefore $Z_m \subseteq X_m$. If m has the form $2^n - 1$ then the multiplicative group of the finite field $F = \mathbb{F}_{2^n}$ is cyclic generated by an element x of order m . The multiplication by x induces an automorphism ψ of the additive group F , also of order m , and $\langle \psi \rangle$ acts transitively on $F \setminus \{0\}$. This automorphism ψ is usually called Singer cycle (see Definition 4.1.7). Consider a homocyclic group $H_{l,n} = (\mathbb{Z}/2^l\mathbb{Z})^n$. Its Frattini subgroup Φ is isomorphic to $H_{l-1,n}$. We denote by $\text{GL}(n, \mathbb{Z}/2^l\mathbb{Z})$ the group of $n \times n$ matrices with coefficients in $\mathbb{Z}/2^l\mathbb{Z}$ and invertible determinant. The natural map

$$\alpha : \text{GL}(n, \mathbb{Z}/2^l\mathbb{Z}) \rightarrow \text{GL}(n, \mathbb{Z}/2\mathbb{Z})$$

given by componentwise reduction modulo 2, is surjective and its kernel has size $2^{n^2(l-1)}$, so there exists $\tau \in \text{Aut}(H_{l,n})$ inducing the Singer cycle automorphism ψ on

$$H_{l,n}/\Phi \cong H_{1,n} = (\mathbb{Z}/2\mathbb{Z})^n.$$

Note that the order of ψ is m , that is, the order of $\alpha(\tau)$ is m . Thus

$$1 = (\alpha(\tau))^m = \alpha(\tau^m),$$

it follows that τ^m is an element of the kernel of α . Since $\text{Ker}(\alpha)$ is a 2-group, the order of τ is m multiplied by a power of 2. Raising τ to a suitable power of 2 gives an automorphism of $H_{l,n}$ of order m , call it γ . Observe that the only fixed point of γ in its action on $H_{l,n}/\Phi$ is the trivial element. Let $K \cong C_2^n$ be the subgroup of $H_{l,n}$ generated by the involutions, and let $\varepsilon \in K$ be an involution. Then there exists $a \in H_{l,n}$ such that $\varepsilon = a^{2^{l-1}}$. If γ fixes ε , then

$$(\gamma(a) \cdot a^{-1})^{2^{l-1}} = \gamma(a^{2^{l-1}}) \cdot (a^{2^{l-1}})^{-1} = \gamma(\varepsilon) \cdot \varepsilon^{-1} = 1,$$

therefore $\gamma(a)a^{-1} \in \Phi$, in other words $\gamma(a)\Phi = a\Phi$. This is a contradiction, since we know that γ acts fixed point freely on $H_{l,n}/\Phi$ and $a\Phi \neq \Phi$ since $a^{2^{l-1}} = \varepsilon \neq 1$. Therefore the action of γ on K is nontrivial, and since m is a prime number, this implies that $\langle \gamma \rangle$ acts transitively on $K \setminus \{1\}$. So $H_{l,n} \rtimes \langle \gamma \rangle$ is m -pyramidal of order $2^{nl} \cdot m$. If d is any odd positive integer, the direct product

$$C_d \times (H_{l,n} \rtimes \langle \gamma \rangle)$$

is m -pyramidal of order $2^{nd} \cdot m \cdot d$. This proves that $Y_m \subseteq X_m$.

We are left to prove that $X_m \subseteq Y_m \cup Z_m$. Let G be an m -pyramidal group where $m \neq 7$. Since m is the index of the centralizer of an involution, we can write

$$|G| = 2^a \cdot m \cdot d$$

with d odd. We will prove that $|G| \in Y_m \cup Z_m$ by induction on $|G|$ (for fixed m). Let N be a minimal normal subgroup of G . If $|N|$ is even, then, by the solvability of G , N is an elementary abelian 2-group $N \cong C_2^n$ and $m = 2^n - 1$. Lemma 2.2.10 implies that n divides a . Thus $|G| \in Y_m$. Now assume $|N|$ is odd. We know that G/N is 1-pyramidal or m -pyramidal (because m is prime). If G/N is m -pyramidal then, by induction, we have $|G/N| \in X_m \cup Y_m$, thus $|G| \in X_m \cup Y_m$ since $|N|$ is odd. So now assume that G/N is 1-pyramidal. Since $|N|$ is odd, the Sylow 2-subgroups of G/N are isomorphic to the Sylow 2-subgroups of G , which are either cyclic or generalized quaternion. Therefore $xy \neq yx$ for every two involutions x, y of G . If ε is an involution of G , then εN is the unique involution of G/N hence the subgroup $N\langle \varepsilon \rangle$ of G is normal in G and it contains all involutions of G , hence the subgroup of G generated by the involutions is

$$K = N\langle \varepsilon \rangle \cong D_{2m}$$

by Proposition 2.2.8, therefore $N \cong C_m$. This also implies that $|C_G(N)|$ is odd. Since $G/C_G(N)$ is isomorphic to a subgroup of $\text{Aut}(N) \cong C_{m-1}$, it follows that $a \leq t$. Thus $|G| \in Z_m$. \square

Chapter 5

The number of (maximal) cyclic subgroups.

Recall that given a finite group G , a subgroup H of G is called a maximal cyclic subgroup of G if H is cyclic and it is not properly contained in any cyclic subgroup of G . The number of cyclic subgroups and the number of maximal cyclic subgroups are interesting topics that have been studied by many researchers in recent years. In this chapter, we discuss the influence of the number of cyclic (resp. maximal cyclic) subgroups of finite groups on their structure. Let $c(G)$ denote the number of cyclic subgroups of G and $\lambda(G)$ the number of maximal cyclic subgroups of G .

5.1 Preliminaries

In this section, we introduce some results used to discuss the number of maximal cyclic subgroups and of cyclic subgroups.

Definition 5.1.1. *The norm $N(G)$ of a group G is the set of elements $x \in G$ such that $xT = Tx$ for every subgroup T of G . Therefore, the norm is the intersection of the normalizers of all its subgroups, and it is a characteristic subgroup of G .*

The following result was proved in [59]:

Lemma 5.1.2. *The norm of a group is in the second center of the group; the centralizer of the norm contains the commutator subgroup of the group.*

The following result can be found in [60].

Lemma 5.1.3. *Every solvable subgroup of S_n has its derived length $\ell(G)$ bounded by $\lfloor b \log n \rfloor$ where $b = 5/(2 \log 3) = 2.27559 \dots$. Moreover this bound is best possible whenever n is a power of 9.*

Let G be a finite group containing at most n pairwise non-commuting elements, L. Pyber [61] gave an upper bound on $|G : Z(G)|$ in terms of n . He proved the following:

Lemma 5.1.4. *If the group G contains at most n pairwise non-commuting elements, then $|G : Z(G)| \leq \alpha^n$ for some constant α .*

Let n be the maximal size of a set of pairwise non-commuting elements of a group G . We claim that $n \leq \lambda(G)$. To see this, let $S = \{x_1, \dots, x_n\}$ be a set of pairwise non-commuting elements of maximal size. Then, G has an element y_i such that $x_i \in \langle y_i \rangle$, and $\langle y_i \rangle$ is a maximal cyclic subgroup of G for any i . We claim that the $\langle y_i \rangle$'s are pairwise distinct. Indeed, assume that $C = \langle y_i \rangle = \langle y_j \rangle$ for some $i \neq j$. Then the two distinct elements x_i, x_j belong to the same cyclic subgroup C , hence they commute, a contradiction.

Lemma 5.1.4 implies that

$$|G : Z(G)| \leq \alpha^n \leq \alpha^{\lambda(G)}.$$

In other words, we have the following.

Proposition 5.1.5. *There exists a constant α such that $|G : Z(G)| \leq \alpha^{\lambda(G)}$ for every finite group G .*

Lemma 5.1.6 (Theorem 4.10 of Chapter 5 in [62]). *The following statements hold.*

- (1) *If P is a p -group with no noncyclic abelian normal subgroups, then either P is cyclic or $p = 2$ and P is isomorphic to D_{2^m} , $m \geq 4$, Q_{2^m} , $m \geq 3$, or SD_{2^m} , $m \geq 4$.*
- (2) *If P is a p -group with no noncyclic abelian subgroups, then either P is cyclic or $p = 2$ and P is isomorphic to Q_{2^m} , $m \geq 3$.*

Now we collect some results on the classification of the finite groups with n cyclic subgroups, where $2 \leq n \leq 11$.

Lemma 5.1.7. *Let G be a finite group. Then we have the following statements:*

- (1) *$c(G) = 2$ if and only if $G \cong C_p$ (see [24, Theorem 2.2]);*
- (2) *$c(G) = 3$ if and only if $G \cong C_{p^2}$ (see [24, Theorem 2.2]);*
- (3) *$c(G) = 4$ if and only if $G \cong C_{p^3}$, C_{pq} or $C_2 \times C_2$ (see [24, Theorem 2.2]);*
- (4) *$c(G) = 5$ if and only if $G \cong C_{p^4}$, $C_3 \times C_3$, Q_8 or S_3 (see [24, Theorem 2.2]);*
- (5) *$c(G) = 6$ if and only if $G \cong C_{p^5}$, C_{p^2q} or $C_2 \times C_4$ (see [24, Theorem 2.3]);*

- (6) $c(G) = 7$ if and only if $G \cong C_{p^6}, C_5 \times C_5, D_8, D_{10}$ or $\text{SmallGroup}(12, 1) = C_3 : C_4$ (see [24, Theorem 2.4]);
- (7) $c(G) = 8$ if and only if G is isomorphic to one of the following: $C_{p^7}, C_{pqr}, C_{p^3q}, C_2^3, C_2 \times C_8, C_3 \times C_9, C_2 \times C_{2p}, A_4, Q_{16}, \text{SmallGroup}(16, 6) = C_8 : C_2$ or $\text{SmallGroup}(27, 4) = C_9 : C_3$ (see [24, Theorem 2.5]);
- (8) $c(G) = 9$ if and only if G is isomorphic to $C_{p^8}, C_{p^2q^2}, C_7 \times C_7, \text{SmallGroup}(20, 1) = C_5 : C_4, D_{14}, \text{SmallGroup}(21, 1) = C_7 : C_3$ or $\text{SmallGroup}(24, 1) = C_3 : C_8$ (see [19, Theorem 2.4]);
- (9) $c(G) = 10$ if and only if G is isomorphic to $C_{p^9}, C_{p^4q}, C_p \times S_3, C_3 \times C_{3p}, C_p \times Q_8, C_2 \times C_{16}, C_4 \times C_4, SD_{16}, D_{12}, \text{SmallGroup}(16, 4) = C_4 : C_4$ or $\text{SmallGroup}(32, 17) = C_{16} : C_2$ (see [19, Theorem 2.4]);
- (10) $c(G) = 11$ if and only if $G \cong C_{p^{10}}, C_{27} \times C_3, C_3 \times S_3, \text{SmallGroup}(28, 1) = C_7 : C_4, \text{SmallGroup}(40, 1) = C_5 : C_8, \text{SmallGroup}(48, 1) = C_3 : C_{16}, \text{SmallGroup}(63, 1) = C_7 : C_9$ or $\text{SmallGroup}(81, 6) = C_{27} : C_3$ (see [25, Theorem 1.1]),

where p, q and r are distinct primes.

Moreover, A. R. Ashrafi and E. Haghi [19] provided a characterization for the simple group $\text{PSL}(2, 7)$ by using the number of cyclic subgroups. It is stated as follows:

Lemma 5.1.8 (Theorem 2.5 of [19]). *A finite simple group G satisfies $c(G) = 79$ if and only if $G \cong \text{PSL}(2, 7)$.*

J. R. Rogério [21] proved that the number of maximal cyclic subgroups of G equals the maximal size of an irredundant covering of G . Now we use this result to prove the following proposition.

Proposition 5.1.9. *If $H \leq G$ and $N \trianglelefteq G$ then $\lambda(H) \leq \lambda(G)$ and $\lambda(G/N) \leq \lambda(G)$.*

Proof. Let $\langle h_i \rangle, i = 1, \dots, n$, be the maximal cyclic subgroups of H , where $n = \lambda(H)$, and let $\langle x_i \rangle, i = 1, \dots, n$, be maximal cyclic subgroups of G such that $\langle h_i \rangle \leq \langle x_i \rangle$ for all i . To prove that $\lambda(H) \leq \lambda(G)$ it is enough to prove that, if $\langle x_i \rangle = \langle x_j \rangle$, then $\langle h_i \rangle = \langle h_j \rangle$. We can write $h_i = x^a$ and $h_j = x^b$ for some positive integers a, b , where $x = x_i$. Letting d be the greatest common divisor of a, b , we can then $dr = a$ and $ds = b$ with $r, s \in \mathbb{N}$. Moreover $ua + vb = d$ for some integers u, v and hence

$$y = x^d = (x^a)^u (x^b)^v \in H.$$

Since $y^r = h_i$ and $y^s = h_j$, we deduce that both $\langle h_i \rangle$ and $\langle h_j \rangle$ are contained in $\langle y \rangle$. Since they are maximal cyclic subgroups of H and $y \in H$, we deduce that they are both equal to $\langle y \rangle$. Therefore $\langle h_i \rangle = \langle y \rangle = \langle h_j \rangle$.

Let $N \trianglelefteq G$. We need to prove that $\lambda(G/N) \leq \lambda(G)$. If G/N is cyclic then $\lambda(G/N) = 1$ and there is nothing to prove, so now assume that G/N is noncyclic, so that G is noncyclic as well. If

$$\{H_1/N, \dots, H_k/N\}$$

is an irredundant covering of G/N of size $k = \lambda(G/N)$, then $\{H_1, \dots, H_k\}$ is an irredundant covering of G of size k . Therefore $\lambda(G/N) \leq \lambda(G)$. \square

Recall that an element $g \in G$ is called primitive if $\langle g \rangle$ is a maximal cyclic subgroup of G . Equivalently, an element $x \in G$ is primitive if whenever x is a power of an element $y \in G$, the element y is a power of x . We have the following result.

Lemma 5.1.10. *Let A, B be groups of coprime orders and let $G = A \times B$. An element $(a, b) \in G$ is primitive in G if and only if a is primitive in A and b is primitive in B . As a consequence, $\lambda(G) = \lambda(A) \cdot \lambda(B)$.*

Proof. Assume $(a, b) \in G$ is primitive. We prove that a is primitive. Suppose $a = x^k$ for some $x \in A$, $k \in \mathbb{Z}$. We need to prove that x is a power of a . Let d be the greatest common divisor of k and $|B|$. Since k/d is coprime to $|B|$, we can write $b = y^{k/d}$ for a suitable $y \in \langle b \rangle$, hence $(a, b) = (x^d, y)^{k/d}$. Since (a, b) is primitive, there exists $r \in \mathbb{Z}$ such that

$$(x^d, y) = (a, b)^r = (a^r, b^r),$$

hence $x^d = a^r$. Since d is coprime to $|A|$, this implies that x is a power of a . This proves that a is primitive and, similarly, b is primitive too. Conversely, assume a is primitive in A and b is primitive in B . Assume

$$(a, b) = (x, y)^k = (x^k, y^k),$$

then $a = x^k$ and $b = y^k$. Since a, b are primitive, there exist $l, m \in \mathbb{Z}$ such that $x = a^l$ and $y = b^m$. By the Chinese Remainder theorem, there exists $r \in \mathbb{Z}$ such that $r \equiv l \pmod{|A|}$ and $r \equiv m \pmod{|B|}$, therefore

$$(a, b)^r = (a^r, b^r) = (a^l, b^m) = (x, y).$$

This proves that (a, b) is primitive. \square

Lemma 5.1.11. *Let p be a prime number, let A, B be nontrivial finite p -groups with A cyclic and let $G := A \times B$. Then $A \times \{1\}$ is a maximal cyclic subgroup of G .*

Proof. If this is not true, then writing $A = \langle a \rangle$, there exists an element $(a^i, b) \in G$ such that $\langle (a, 1) \rangle$ is properly contained in $\langle (a^i, b) \rangle$. This means that $b \neq 1$ and there exists an integer m such that $a^{im} = a$, $b^m = 1$. The fact that $a^{im} = a$ implies that $o(a)$, which is a power of p different from 1 (as A is a nontrivial p -group), divides $im - 1$, implying that p does not divide m . Since $b^m = 1$ and B is a p -group, we deduce that $b = 1$, a contradiction. \square

Lemma 5.1.12. *Let p be a prime number, let P be a finite nontrivial p -group and let c be the number of cyclic subgroups of P , let λ be the number of maximal cyclic subgroups of P . If $G = P \times C_p$, then*

$$\begin{aligned} c(G) &= p(c-1) + 2, \\ \lambda(G) &= (p-1)(c-1) + \lambda + 1. \end{aligned}$$

In particular, $c(C_{p^a} \times C_p) = ap + 2$ and $\lambda(C_{p^a} \times C_p) = ap - a + 2$.

Proof. For every $b \in \mathbb{N}$, let c_b be the number of elements of order p^b in P . If $b \geq 2$, then G has $p \cdot c_b$ elements of order p^b . Moreover, G has $p \cdot c_1 + p - 1$ elements of order p and of course one element of order 1. Write $|P| = p^a$. It follows that

$$c(G) = 1 + \frac{p \cdot c_1 + p - 1}{\varphi(p)} + \sum_{b=2}^a \frac{p \cdot c_b}{\varphi(p^b)} = p \cdot \sum_{b=1}^a \frac{c_b}{\varphi(p^b)} + 2 = p(c-1) + 2.$$

Now, the $c - \lambda$ non-maximal cyclic subgroups of P are not maximal cyclic subgroups of G , therefore

$$\lambda(G) = p(c-1) + 2 - (c - \lambda) = (p-1)c - p + 2 + \lambda.$$

This is because, if $K = \langle x \rangle$ is any cyclic subgroup of G , then $x^p \in P \times \{1\}$, therefore all the subgroups of G properly contained in K are subgroups of $P \times \{1\}$. Therefore all the cyclic subgroups of G not contained in $P \times \{1\}$ are maximal cyclic. \square

Lemma 5.1.13. *Let p be a prime number, let P be a finite nontrivial p -group and let c be the number of cyclic subgroups of P , let c_b be the number of elements of order p^b in P . Then*

$$c(P \times C_{p^a}) = (a+1) + p^a(c-1) + \sum_{i=1}^{a-1} (a-i)c_i - \sum_{j=1}^{a-1} (p^{a-j} + p^{a-j-1} + \dots + p^2 + p)c_j.$$

Proof. The number of elements of order p^i (where $i \leq a$) is $c_i p^i + (1 + c_1 + c_2 + \dots + c_{i-1})\varphi(p^i)$, and there are $c_b p^a$ elements of order p^b for $b > a$. Thus

$$\begin{aligned} c(P \times C_{p^a}) &= 1 + \frac{c_1 p + \varphi(p)}{\varphi(p)} + \frac{c_2 p^2 + (1 + c_1)\varphi(p^2)}{\varphi(p^2)} + \frac{c_3 p^3 + (1 + c_1 + c_2)\varphi(p^3)}{\varphi(p^3)} \\ &\quad + \dots + \frac{c_a p^a + (1 + c_1 + \dots + c_{a-1})\varphi(p^a)}{\varphi(p^a)} + \sum_{b>a} \frac{c_b p^a}{\varphi(p^b)} \\ &= 1 + 1 + \frac{c_1 p}{\varphi(p)} + (1 + c_1) + \frac{c_2 p^2}{\varphi(p^2)} + (1 + c_1 + c_2) + \frac{c_3 p^3}{\varphi(p^3)} + \dots \\ &\quad + (1 + c_1 + c_2 + \dots + c_{a-1}) + \frac{c_a p^a}{\varphi(p^a)} + \sum_{b>a} \frac{c_b p^a}{\varphi(p^b)} \\ &= a + 1 + p^a(c-1) + \sum_{i=1}^{a-1} (a-i)c_i - \sum_{j=1}^{a-1} (p^{a-j} + p^{a-j-1} + \dots + p^2 + p)c_j \end{aligned}$$

\square

5.2 The proof of Theorem E

In this section, we will prove Theorem E, which we state again for convenience. It was proved in [10].

Theorem E (X. Gao, M. Garonzi). If G is any finite solvable group then the derived length of G is at most $2 + \frac{5}{2} \log_3(\lambda(G))$.

Proof. Let \mathcal{C} be the family of all maximal cyclic subgroups of G , so that $|\mathcal{C}| = \lambda = \lambda(G)$. Of course G acts on \mathcal{C} by conjugation. The kernel N of this action is the intersection of the normalizers of all maximal cyclic subgroups of G . It is clear that G/N is isomorphic to a subgroup of $\text{Sym}(\lambda)$.

We claim that N is actually equal to the set of elements of G that normalize every subgroup of G . To see this, let $g \in G$ be an element that normalizes every maximal cyclic subgroup of G . If H is any subgroup of G and $h \in H$, then there exists a maximal cyclic subgroup $\langle x \rangle$ of G containing $\langle h \rangle$, and by assumption $x^g = x^k$ for some integer k . Since $h \in \langle x \rangle$, there is some integer t such that $h = x^t$, so that

$$h^g = (x^t)^g = (x^g)^t = (x^k)^t = (x^t)^k = h^k \in \langle h \rangle \leq H,$$

this proves that g normalizes H . This proves the claim.

The above claim implies that N is equal to the norm of G . By Lemma 5.1.2, we deduce that N is contained in the second term of the upper central series, $N \leq Z_2(G)$. Since $Z(G) = Z_1(G) \leq Z_2(G)$, $Z_1(G)$ is contained in the center subgroup of $Z_2(G)$. Observe that $Z_2(G)/Z_1(G)$ is abelian, so $Z_2(G)$ is nilpotent, and then N is nilpotent of class at most 2. In particular, $N' \leq [Z_2(G), G] \leq Z_1(G)$ and, since $Z_1(G)$ is abelian, we have $N'' = \{1\}$.

Since G/N is isomorphic to a subgroup of $\text{Sym}(\lambda)$, we deduce that, if G is solvable, then the Fitting length of G is at most $1 + \lambda!$. Since $N'' = \{1\}$, the derived length of G is at most $2 + \lambda!$. We can do much better than this: Lemma 5.1.3 says that the derived length of a solvable permutation group of degree n is at most $\frac{5}{2} \log_3(\lambda)$. This proves Theorem E. \square

5.3 The proof of Theorem F

Recall that a family \mathcal{F} of groups is said to be MCB if, for every natural number n , there are only finitely many groups G in \mathcal{F} (up to isomorphism) such that $\lambda(G) \leq n$. In this section, we prove Theorem F, which we restate here once more for the benefit of the reader. It was proved in [10].

Theorem F (X. Gao, M. Garonzi). The following statements hold.

- (1) The family of noncyclic groups of prime power order is MCB. More precisely, if G is a noncyclic finite p -group and $t = \lambda(G)$ then $|G| \leq c^t \cdot t^{t^2}$ for some constant c .
- (2) The family of groups G such that every nontrivial Sylow subgroup of the center $Z(G)$ is noncyclic is MCB. In particular, the family of groups with trivial center is MCB.

Proof. Item (1). Let G be a noncyclic finite p -group, where p is a fixed prime number. If G is abelian then we can write

$$G = \prod_{i=1}^k C_{p^{a_i}} = \prod_{i=1}^k \langle g_i \rangle$$

with $k \geq 2$. Since the $\langle g_i \rangle$ are maximal cyclic subgroups of G by Lemma 5.1.11, we have $k \leq \lambda(G)$, so we are left to bound the a_i 's. Note that for any $i \in \{1, \dots, k\}$, G has a subgroup

$$A_i := C_{p^{a_i}} \times C_p.$$

Since $\lambda(H) \leq \lambda(G)$ for $H \leq G$ by Proposition 5.1.9, we have $\lambda(A_i) \leq \lambda(G)$ hence, by Lemma 5.1.12,

$$\lambda(G) \geq \lambda(A_i) = a_i p - a_i + 2 \geq a_i$$

and similarly $\lambda(G) \geq p$, therefore $|G| \leq t^{t^2}$ where $t = \lambda(G)$.

Now assume G is nonabelian. By Proposition 5.1.5, the index $|G : Z(G)|$ is bounded by a function of $\lambda(G)$. If H is a noncyclic abelian subgroup of G then $K = \langle H, Z(G) \rangle$ is a noncyclic abelian subgroup of G hence, by the abelian case, $|K|$ is bounded in terms of $\lambda(K) \leq \lambda(G)$, so since $Z(G)$ is contained in K , the order of $Z(G)$ is bounded in terms of $\lambda(G)$. We are left to analyze the case in which all abelian subgroups of G are cyclic. The class of p -groups all of whose abelian subgroups are cyclic is known: such a group is either cyclic or a generalized quaternion group by Lemma 5.1.6. Since G is noncyclic, it must be a generalized quaternion group Q_{2^n} , therefore $|Z(G)| = 2$ and we are done.

We now prove item (2). Let G be a finite group such that every nontrivial Sylow subgroup of $Z(G)$ is noncyclic. Write

$$Z(G) = P_1 \times P_2 \times \dots \times P_k$$

where P_i is a nontrivial Sylow subgroup of $Z(G)$ for $i = 1, 2, \dots, k$. Let

$$z := \min\{\lambda(P_1), \lambda(P_2), \dots, \lambda(P_k)\}.$$

Since P_i is noncyclic for all i , we have $z \geq 2$. By Proposition 5.1.9 and Lemma 5.1.10,

$$z^k \leq \lambda(P_1) \cdot \dots \cdot \lambda(P_k) = \lambda(Z(G)) \leq \lambda(G),$$

it follows that $k \leq \log_z(\lambda(G))$. By the item (1) of Theorem F, the family of noncyclic groups of prime power order is MCB, so by Proposition 5.1.9 we can bound the order of P_i in terms of $\lambda(G)$, thus $|Z(G)|$ is bounded by a function of $\lambda(G)$. Therefore $|G| = |G : Z(G)| \cdot |Z(G)|$ is also bounded by a function of $\lambda(G)$ by Proposition 5.1.5. \square

5.4 The proof of Theorem G

Recall that a family \mathcal{F} of groups is said to be CB if, for every natural number n , there are only finitely many groups G in \mathcal{F} (up to isomorphism) such that $c(G) \leq n$. Since $\lambda(G) \leq c(G)$, item (1) of Theorem F implies that the family of noncyclic groups of prime power order is CB. More precisely, we have the following.

Proposition 5.4.1. *If G is a noncyclic finite p -group and $t = c(G)$ then $|G| \leq t^t$.*

Proof. Let G be a noncyclic group of order p^n where p is a prime, we need to bound p and n in terms of $t = c(G)$. If $p = 2$ then $p < t$ since G is a noncyclic group (see Theorem 5.1.7). If $p \geq 3$, then by Lemma 5.1.6, G has a subgroup isomorphic to $C_p \times C_p$, which has $p + 2$ cyclic subgroups, therefore $p \leq t$. If p^m is the exponent of G and $g \in G$ has order p^m , then $\langle g \rangle$ has $m + 1$ cyclic subgroups, therefore $m \leq t - 1$ and $\exp(G) \leq t^{t-1}$. Since each cyclic subgroup of G has at most $\varphi(p^m) = p^{m-1}(p - 1)$ generators, G has at least $\frac{p^n - 1}{p^{m-1}(p-1)}$ cyclic subgroups, therefore

$$t \geq \frac{p^n - 1}{p^{m-1}(p-1)} = \frac{p^{n-1} + p^{n-2} + \dots + p + 1}{p^{m-1}} \geq \frac{p^{n-1}}{p^{m-1}} = p^{n-m}.$$

Thus $p^{n-m} \leq t$ hence $|G| = p^n = p^m \cdot p^{n-m} \leq t^{t-1} \cdot t = t^t$. \square

Before proving Theorem G, we need the following theorem.

Theorem 5.4.2. *Let G be a finite group with $c(G) = t$. Then $G \cong A \times B$ where A is cyclic, $|A|, |B|$ are coprime, the Sylow subgroups of the center of B have order at most t^t and $|B| \leq \alpha^t \cdot t^{t^2}$ where α is the constant in Lemma 5.1.4.*

Proof. We prove, by induction on $|G|$, that $G \cong A \times B$ where A is cyclic, $|A|, |B|$ are coprime, the Sylow subgroups of the center of B have order at most t^t and $|B| \leq \alpha^t \cdot t^{t^2}$. Proposition 5.4.1 implies that every noncyclic p -subgroup of G has order at most t^t . By Cauchy's theorem, for every prime p dividing $|G|$, there exists a cyclic subgroup of G of order p , therefore $|G|$ has at most t prime divisors. So if $Z(G)$ has no Sylow subgroup of order larger than t^t then $|Z(G)| \leq t^{t^2}$. Proposition 5.1.5 now implies that $|G| \leq \alpha^t \cdot t^{t^2}$ and hence we can choose $A = \{1\}$. Now assume that $Z(G)$ has a Sylow subgroup P with the property that $|P| > t^t$. In particular, P is cyclic and of course $P \trianglelefteq G$.

Let Q be a Sylow p -subgroup of G containing P and write $|Q| = p^k$. If Q is noncyclic, then $|P| \leq |Q| \leq t^t$, a contradiction. So Q is cyclic, hence Q has $k + 1$ cyclic subgroups. It follows that $k + 1 \leq c(G) = t$. If Q is not normal in G , then $1 < n_p(G) \equiv 1 \pmod{p}$ by Sylow's theorem, hence $p < n_p(G) \leq t$, therefore

$$|P| \leq |Q| = p^k \leq t^{t-1} < t^t,$$

a contradiction. We deduce that Q is cyclic and normal in G , so that $G = Q \rtimes K$ for a suitable K , by the Schur-Zassenhaus theorem. If this is not a direct product, then K is not normal in G , so Q is not contained in $N_G(K)$. Therefore Q cannot normalize all cyclic subgroups of K , in other words there is some $u \in K$ such that Q is not contained in $N_G(\langle u \rangle)$. It follows that p divides the index $|G : N_G(\langle u \rangle)|$, which equals the number of conjugates of $\langle u \rangle$ in G , hence $p \leq c(G) = t$. We deduce that

$$|P| \leq |Q| = p^k \leq t^{t-1} < t^t,$$

a contradiction. This implies that G is a direct product $Q \times K$ where Q is a cyclic p -group and p does not divide $|K|$. By induction, the result holds for K (since K is a proper subgroup of G), in other words, $K \cong K_1 \times B$ where K_1 is cyclic, $(|K_1|, |B|) = 1$, the Sylow subgroups of the center of B have order at most t^t and $|B| \leq \alpha^t \cdot t^{t^2}$. Note that

$$G = Q \times K = Q \times K_1 \times B,$$

where $|Q|$, $|K_1|$ and $|B|$ are pairwise coprime, so G can be written as $G = A \times B$ where $A = Q \times K_1$ is cyclic, $|A|$ and $|B|$ are coprime, the Sylow subgroups of the center of B have order at most t^t and $|B| \leq \alpha^t \cdot t^{t^2}$. Therefore, the result holds for G and we are done. \square

Observe that if $c(G)$ is replaced by $\lambda(G)$, then the Theorem 5.4.2 is not true. As an example of this, consider $G = G_k = C_3 \rtimes C_{2^k}$ with the action given by inversion. Then G is not isomorphic to a direct product of two nontrivial groups and $\lambda(G) = 4$. Indeed, writing $G = \langle a, b : a^3 = b^{2^k} = 1, a^b = a^{-1} \rangle$, since $a^{b^2} = a$, we have $N := \langle a, b^2 \rangle = \langle a \rangle \times \langle b^2 \rangle \cong C_{3 \cdot 2^{k-1}}$. The subgroup N is maximal cyclic and $\langle x \rangle$ is maximal cyclic for every $x \in G - N$, since $o(x) = 2^k$. Therefore

$$\begin{aligned} \lambda(G) &= 1 + c(G - N) = 1 + |G - N|/\varphi(2^k) = 4, \\ c(G) &= c(N) + c(G - N) = c(C_3) \cdot c(C_{2^{k-1}}) + |G - N|/\varphi(2^k) = 2k + 3. \end{aligned}$$

It follows that $|G|$ cannot be bounded in terms of $\lambda(G)$. This also shows that the family of groups $\{G_k : k \geq 1\}$ is CB but not MCB.

Call \mathcal{B} the set of positive integers n such that there are only finitely many noncyclic groups G with $c(G) = n$, up to isomorphism. We now prove Theorem G, which we restate here for convenience. This theorem was proved in [10].

Theorem G (X. Gao, M. Garonzi). $\mathcal{B} = \{1, 4, 6, 9\} \cup \mathcal{P}$ where \mathcal{P} is the set of prime numbers.

Proof. From the work of Ashrafi and Haghi [19, 24] (see also [18] and [17]) we immediately deduce that $3, 4, 5, 6, 7, 9 \in \mathcal{B}$ and $8, 10 \notin \mathcal{B}$. We need to show that an integer $n \geq 10$ is prime if and only if there are only finitely many noncyclic finite groups with precisely n cyclic subgroups. By Theorem 5.4.2, there exists a function f such that, if G is any

noncyclic finite group with $c(G) = n$, we have $G \cong A \times B$ with $|A|, |B|$ coprime, A cyclic and $|B| \leq f(n)$. In particular $c(G) = c(A) \cdot c(B)$ so, if n is prime, the fact that A is cyclic and G is noncyclic implies that $A = \{1\}$, so $G = B$ and $|G| \leq f(n)$. Conversely, assume n is not a prime number and write $n = ab$ with $a, b > 1$. Since $n \geq 10$ we may assume without loss of generality that $b \geq 4$. Then we can write $b - 2 = kq$ for some prime number q and some integer $k \geq 1$, so that $c(C_{q^k} \times C_q) = qk + 2 = b$ by Lemma 5.1.12 and, if r is any prime number distinct from q , the noncyclic group $C_{r^{a-1}} \times C_{q^k} \times C_q$ has $ab = n$ cyclic subgroups. Since there are infinitely many such primes r , we obtain the result. \square

Appendix A

The classification of simple pyramidal groups

In [7], H. Yamaki gave a classification of the pyramidal nonabelian simple groups. Let S be a finite simple group and $C_S(t)$ the centralizer of the involution t in S , and let t^S denote the conjugacy class of t in S . Tables A.1, A.2, A.3, and A.4, which correspond to Tables 1-4 of [7], provide information on all pyramidal simple groups, the order of centralizers of involutions in S , and compute the number of involutions in all pyramidal simple groups.

S	$ C_S(t) $	$ S $	$ t^S $
PSL(2, q), $q \equiv 1 \pmod{4}$	$q - 1$	$q(q^2 - 1)/2$	$q(q + 1)/2$
PSL(2, q), $q \equiv -1 \pmod{4}$	$q + 1$	$q(q^2 - 1)/2$	$q(q - 1)/2$
PSL(3, q)	$(q - 1)^2 q(q + 1)(3, q - 1)^{-1}$	$q^3(q^2 - 1)(q^3 - 1)(3, q - 1)^{-1}$	$q^2(q^2 + q + 1)$
PSL(4, q), $q \equiv 5 \pmod{8}$	$(q - 1)^3 q^2 (q + 1)^2 / 2$	$q^6 \prod_{i=1}^3 (q^{i+1} - 1) / 4$	$q^4 (q^2 + q + 1)(q^2 + 1) / 2$
$G_2(q)$	$q^2 (q^2 - 1)^2$	$q^6 (q^6 - 1)(q^2 - 1)$	$q^4 (q^2 + q + 1)(q^2 - q + 1)$
${}^2G_2(q)$, $q = 3^{2k+1}$, $k \geq 2$	$q(q^2 - 1)$	$q^3 (q^3 + 1)(q - 1)$	$q^2 (q^2 - q + 1)$
PSU(3, q)	$q(q + 1)(q^2 - 1)(3, q + 1)^{-1}$	$(q^3 + 1)q^3 (q^2 - 1)(3, q + 1)^{-1}$	$q^2 (q^2 - q + 1)$
PSU(4, q), $q \equiv 3 \pmod{8}$	$(q - 1)^2 q^2 (q + 1)^3 / 2$	$q^6 \prod_{i=1}^3 (q^{i+1} - (-1)^{i+1}) / 4$	$q^4 (q^2 - q + 1)(q^2 + 1) / 2$
${}^3D_4(q^3)$	$q^4 (q^2 - 1)(q^6 - 1)$	$q^{12} (q^8 + q^4 + 1)(q^6 - 1)(q^2 - 1)$	$q^8 (q^8 + q^4 + 1)$

Table A.1: Groups of Lie type over a field of odd characteristic.

S	$ C_S(t) $	$ S $	$ t^S $
$\text{PSL}(2, q)$	q	$(q+1)q(q-1)$	$(q+1)(q-1)$
$\text{PSL}(3, q)$	$q^3(q-1)(3, q-1)^{-1}$	$(q^3-1)(q^2-1)q^3(3, q-1)^{-1}$	$(q^3-1)(q+1)$
$\text{PSU}(3, q)$	$q^3(q+1)(3, q+1)^{-1}$	$(q^3+1)q^3(q^2-1)(3, q+1)^{-1}$	$(q^3+1)(q-1)$
$\text{Sz}(q), q = 2^{2k+1}, k \geq 1$	q^2	$(q^2+1)q^2(q-1)$	$(q^2+1)(q-1)$

Table A.2: Groups of Lie type over a field of even characteristic.

S	$ C_S(t) $	$ S $	$ t^S $
M_{11}	$2^4 \cdot 3$	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	$3 \cdot 5 \cdot 11$
J_1	$2^3 \cdot 3 \cdot 5$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	$7 \cdot 11 \cdot 19$
M_{22}	$2^7 \cdot 3$	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	$3 \cdot 5 \cdot 7 \cdot 11$
M_{23}	$2^7 \cdot 3 \cdot 7$	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	$3 \cdot 5 \cdot 11 \cdot 23$
J_3	$2^7 \cdot 3 \cdot 5$	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$	$3^4 \cdot 17 \cdot 19$
McL	$2^7 \cdot 3^2 \cdot 5 \cdot 7$	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	$3^4 \cdot 5^2 \cdot 11$
ON	$2^9 \cdot 3^2 \cdot 5 \cdot 7$	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$	$3^2 \cdot 7^2 \cdot 11 \cdot 19 \cdot 31$
Ly	$2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11$	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$	$3^3 \cdot 5^4 \cdot 31 \cdot 37 \cdot 67$
Th	$2^{15} \cdot 3^4 \cdot 5 \cdot 7$	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$	$3^6 \cdot 5^2 \cdot 7 \cdot 13 \cdot 19 \cdot 31$

Table A.3: Sporadic simple groups.

S	$ C_S(t) $	$ S $	$ t^S $
$A_5 = \text{PSL}(2, 4)$	2^2	$60 = 2^2 \cdot 3 \cdot 5$	$3 \cdot 5 = 15$
$A_6 = \text{PSL}(2, 3^2)$	2^3	$360 = 2^3 \cdot 3^2 \cdot 5$	$3^2 \cdot 5 = 45$
A_7	$2^3 \cdot 3$	$2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$	$3 \cdot 5 \cdot 7 = 105$

Table A.4: Alternating Groups.

Bibliography

- [1] M. Buratti, G. Rinaldi and T. Traetta. *3-pyramidal Steiner triple systems*. *Ars Mathematica Contemporanea*, 13:95-106, 2017.
- [2] S. Bonvicini, M. Buratti, M. Garonzi, G. Rinaldi and T. Traetta. *The first families of highly symmetric Kirkman Triple Systems whose orders fill a congruence class*. *Designs, Codes and Cryptography*, 89(12):2725-2757, 2021.
- [3] T. P. Kirkman. *On a problem in combinations*. *Cambridge and Dublin Mathematical Journal*, 2:191-204, 1847.
- [4] D. K. Ray-Chaudhuri and R. M. Wilson. *Solution of Kirkman's Schoolgirl Problem*. *Proceedings of Symposia in Pure Mathematics*, 19:187-203, 1971.
- [5] B. Huppert and N. Blackburn. *Finite Groups II, volume 242*. Springer, Berlin, Heidelberg, 1982.
- [6] D. L. Shaw. *The Sylow 2-subgroups of finite, soluble groups with a single class of involutions*. *Journal of Algebra*, 16:14-26, 1970.
- [7] H. Yamaki. *The order of a group of even order*. *Proceedings of the American Mathematical Society*, 136(2):397-402, 2008.
- [8] X. Gao and M. Garonzi. *The structure of 3-pyramidal groups*. *Journal of Algebra*, 636:75-87, 2023.
- [9] X. Gao and M. Garonzi. *On pyramidal groups whose number of involutions is a prime power*. Preprint. <https://arxiv.org/abs/2311.16690>.
- [10] X. Gao and M. Garonzi. *Bounds in terms of the number of cyclic subgroups*. Preprint. <https://arxiv.org/abs/2405.12160>
- [11] I. M. Isaacs. *Finite Group Theory. Graduate Studies in Mathematics, 92*. American Mathematical Society, 2008.
- [12] M. Garonzi and I. Lima. *On the number of cyclic subgroups of a finite group*. *Bulletin of the Brazilian Mathematical Society. New Series. Boletim da Sociedade Brasileira de Matemática*, 49(3):515-530, 2018.

- [13] M. Tărnăuceanu. *Finite groups with a certain number of cyclic subgroups*. The American Mathematical Monthly, 122(3):275-276, 2015.
- [14] M. Tărnăuceanu. *Finite groups with a certain number of cyclic subgroups II*. Acta Universitatis Sapientiae, Mathematica, 10(2):375-377, 2018.
- [15] R. Belshoff, J. Dillstrom and L. Reid. *Finite groups with a prescribed number of cyclic subgroups*. Communications in Algebra, 47(3):1043-1056, 2019.
- [16] R. Belshoff, J. Dillstrom and L. Reid. *Addendum to "Finite groups with a prescribed number of cyclic subgroups"*. Communications in Algebra, 47(10):3939-3940, 2019.
- [17] W. Zhou. *Finite groups with small number of cyclic subgroups*. <http://arxiv.org/abs/1606.02431v>.
- [18] H. Kalra. *Finite groups with specific number of cyclic subgroups*. Proceedings of the Indian National Science Academy, 129(52):1-10, 2019.
- [19] A. R. Ashrafi and E. Haghi. *On n -cyclic groups*. Bulletin of the Malaysian Mathematical Sciences Society, 42:3233-3246, 2019.
- [20] *The GAP Group*. GAP-Groups, Algorithms, and Programming, Version 4.12.2, 2022.
- [21] J. R. Rogério. *A note on maximal coverings of groups*. Communications in Algebra, 42(10):4498-4508, 2014.
- [22] R. Bastos, I. Lima and J. R. Rogério. *Maximal covers of finite groups*. Communications in Algebra, 48(2), 691-701, 2020.
- [23] A. Lucchini and M. Garonzi. *Irredundant and minimal covers of finite groups*. Communications in Algebra, 44(4):1722-1727, 2016.
- [24] E. Haghi and A. R. Ashrafi. *On the number of cyclic subgroups in a finite group*. Southeast Asian Bulletin of Mathematics, 42: 865-873, 2018.
- [25] K. Sharma and A. S. Reddy. *Groups having 11 cyclic subgroups*. International Journal of Group Theory, 13(2): 203-214, 2024.
- [26] G. Scorza. *Gruppi che possono pensarsi come somma di tre sottogruppi*. Bollettino della Unione Matematica Italiana, 5:216-218, 1926.
- [27] J. H. E. Cohn. *On n -sum groups*. Mathematica Scandinavica, 75:44-58, 1994.
- [28] M. J. Tomkinson. *Groups as the union of proper subgroups*. Mathematica Scandinavica, 81:189-198, 1997.
- [29] A. Abdollahi, M. J. Ataei, S. M. Amari and A. M. Hassanabadi. *Groups with a maximal irredundant 6-cover*. Communications in Algebra, 33:3225-3238, 2005.

- [30] J. Zhang. *Finite groups as the union of proper subgroups*. Serdica Mathematical Journal, 32:259–268, 2006.
- [31] A. Abdollahi and S. M. Jafarian Amiri. *On groups with an irredundant 7-cover*. Journal of Pure and Applied Algebra, 209:291–300, 2007.
- [32] A. Abdollahi and S. M. Jafarian Amiri. *Minimal coverings of completely reducible groups*. Publicationes Mathematicae Debrecen, 72:167–172, 2008.
- [33] R. A. Bryce, V. Fedri and L. Serena. *Covering groups with subgroups*. Bulletin Australian Mathematical Society, 55:469–476, 1997.
- [34] R. A. Bryce and L. Serena. *A note on minimal coverings of groups by subgroups*. Special issue on group theory, Journal of Australian Mathematical Society, 71:159–168, 2001.
- [35] A. Maróti. *Covering the symmetric groups with proper subgroups*. Journal of Combinatorial Theory, Series A, 110:97–111, 2005.
- [36] M. A. Brodie. *Uniquely covered groups*. Algebra Colloquium, 10:101–108, 2003.
- [37] S. O. Juriaans and J. R. Rogério. *On groups whose maximal cyclic subgroups are maximal*. Algebra Colloquium, 17:223–227, 2010.
- [38] A. Ballester-Bolinches and L. M. Ezquerro. *Classes of Finite Groups*. Springer, 2006.
- [39] J. L. Alperin and R. B. Bell. *Groups and Representations, volume 162*. Springer, 1995.
- [40] M. Garonzi. *The maximal subgroups of the symmetric group*. Ensaios Matemáticos (Mathematical Surveys), 36:1-51, 2021.
- [41] P. J. Cameron. *Permutation Groups*. Cambridge University Press, 2010.
- [42] R. A. Wilson. *The Finite Simple Groups*. Springer, 2009.
- [43] G. James and M. Liebeck. *Representations and Characters of Groups*. Cambridge University Press, 2001.
- [44] A. Machì. *Groups: An Introduction to Ideas and Methods of the Theory of Groups*. Springer, 2012.
- [45] D. J. S. Robinson. *A Course in the Theory of Groups, volume 80*. Springer Science & Business Media, 2012.
- [46] J. S. Rose. *A Course on Group Theory*. Cambridge University Press, 1978.
- [47] K. Zsigmondy. *Zur Theorie der Potenzreste*. Monatshefte für Mathematik und Physik, 3:265-284, 1892.

-
- [48] J. N. Bray, D. F. Holt and C. M. Roney-Dougal. *The Maximal Subgroups of the Low-dimensional Finite Classical Groups, volume 407*. Cambridge university press, 2013.
- [49] J. G. Thompson. *Nonsolvable finite groups all of whose local subgroups are solvable*. Bulletin of the American Mathematical Society, 74:383–437, 1968.
- [50] D. Levy. *Characterization of the solvable radical by Sylow multiplicities*. Journal of Algebra, 635:23-84, 2023.
- [51] G. Glauberman. *Central elements in core-free groups*. Journal of Algebra, 4(3):403-420, 1966.
- [52] H. Kurzweil and B. Stellmacher. *The Theory of Finite Groups: An Introduction*. Springer, 2004.
- [53] U. Dempwolff. *On the second cohomology of $GL(n, 2)$* . Journal of the Australian Mathematical Society, 16(2):207-209, 1973.
- [54] R. Brauer and M. Suzuki. *On finite groups of even order whose 2-Sylow group is a quaternion group*. Proceedings of the National Academy of Sciences of the United States of America, 45(12):1757-1759, 1959.
- [55] D. Gorenstein and J. H. Walter. *The characterization of finite groups with dihedral Sylow 2-subgroups. I*. Journal of Algebra, 2(1):85-151, 1965.
- [56] R. M. Guralnick. *Subgroups of prime power index in a simple group*. Journal of Algebra, 81:304-311, 1983.
- [57] G. Higman. *Suzuki 2-groups*. Illinois journal of mathematics, 7(1):79-96, 1963.
- [58] B. Huppert. *Endliche Gruppen, volume 1*. Springer Berlin-Heidelberg-New York, 1967.
- [59] E. Schenkman. *On the norm of a group*. Illinois Journal of Mathematics, 41(1):150–152, 1960.
- [60] J. D. Dixon, B. Mortimer. *Permutation Groups*. Springer, New York, 1996.
- [61] L. Pyber. *The number of pairwise noncommuting elements and the index of the centre in a finite group*. Journal of the London Mathematical Society, s2- 35(2):287–295, 1987.
- [62] D. Gorenstein. *Finite Groups*. AMS Chelsea Publishing, New York, 1968.