UNIVERSITÀ DEGLI STUDI DI PADOVA

Sede amministrativa: Università degli studi di Padova
Dipartimento di Matematica Pura e Applicata

SCUOLA DI DOTTORATO DI RICERCA IN SCIENZE MATEMATICHE
INDIRIZZO MATEMATICA
CICLO XXIII

ON THE DIRICHLET POLYNOMIAL OF THE SIMPLE GROUPS OF LIE TYPE

by
Massimiliano Patassini

Direttore della Scuola: Ch.mo Prof. Paolo Dai Pra
Coordinatore d'indirizzo: Ch.mo Prof. Franco Cardin
Supervisore: Ch.mo Prof. Andrea Lucchini

Dottorando: Massimiliano Patassini

January 7, 2011

Contents

Abstract

In this thesis we discuss three problems concerning the Dirichlet polynomial $P_S(s)$ of a simple group of Lie type S.

The first problem is a conjecture of Kennet Brown: if G is a finite group, then the order complex of the coset poset of G is not contractible. We prove that the conjecture holds for a large class $\mathfrak{C}$ of classical groups and we show how to generalize this result to the groups whose components are in the class $\mathfrak{C}$, under some assumptions.

The second problem is to determine whether the Dirichlet polynomial of a simple group is reducible or not in the ring of Dirichlet polynomials. We give a complete answer for the Dirichlet polynomials of the simple groups of Lie type. This allows us to find the factorization into irreducible of the Dirichlet polynomial of a group whose non-abelian chief factors are simple groups of Lie type, under some assumptions on the rank of these last groups.

The third problem is a conjecture of Erika Damian and Andrea Lucchini: if S is a simple group and G is a finite group such that $P_S(s) = P_G(s)$, then $G/\mathrm{Frat}(G) \cong S$. We complete the proof of this conjecture. This conjecture was proved for S abelian, alternating and sporadic. Moreover, it was proved that if G_1 and G_2 are two non-isomorphic groups of Lie type defined over fields with the same characteristic, then $P_{G_1}(s) \neq P_{G_2}(s)$. We show that it is possible to recognize the characteristic of a group of Lie type form its Dirichlet polynomial. This is enough to complete the proof of the conjecture.

Sommario

In questa tesi discuteremo tre problemi riguardanti il polinomio di Dirichlet $P_S(s)$ di S, gruppo semplice di tipo Lie.

Il primo problema è una congettura di Kennet Brown: se G è un gruppo finito, allora il complesso simpliciale associato al coset poset di G non è contraibile. Dimostreremo che questa congettura vale per un'ampia classe $\mathfrak{C}$ di gruppi classici e mostreremo come generalizzare questo risultato a gruppi le cui componenti appartengono alla classe $\mathfrak{C}$, sotto certe condizioni.

Il secondo problema consiste nel determinare quando il polinomio di Dirichlet di un gruppo semplice è riducibile nell'anello dei polinomi di Dirichlet. Daremo una risposta completa al problema per i polinomi di Dirichlet di gruppi semplici di tipo Lie. Questo ci permette di trovare la fattorizzazione in irriducibili del polinomio di Dirichlet di un gruppo i cui fattori principali non abeliani sono gruppi semplici di tipo Lie, con alcune ipotesi sul rango di questi ultimi gruppi.

Il terzo problema è una congettura di Erika Damian e Andrea Lucchini: se S è un gruppo semplice e G è un gruppo finito tale che $P_S(s) = P_G(s)$, allora $G/\mathrm{Frat}(G) \cong S$. Completeremo la dimostrazione di questa congettura, che era stata già dimostrata per S gruppo abeliano, alterno e sporadico. Inoltre, era stato dimostrato che se G_1 e G_2 sono due gruppi di tipo Lie definiti su campi con la stessa caratteristica e non isomorfi, allora $P_{G_1}(s) \neq P_{G_2}(s)$. Per completare la dimostrazione della congettura, mostreremo che è possibile riconoscere la caratteristica di un gruppo di tipo Lie dal suo polinomio di Dirichlet.

Notation

0.1 General notation

Let a, k be two nonnegative integer number, let p be a prime number, let π be a set of prime numbers, let Y be a set, let G be a finite group and N a normal subgroup of G. Let $\mathbb{K}$ be a finite field.

List of symbols

$\varnothing$	empty set	
$a_k(G)$	k-th coefficient of the Dirichlet polynomial $P_G(s)$	p.8
$a_k(f(s))$	k-th coefficient of the Dirichlet polynomial $f(s)$	p.8
$a_k(G, N)$	k-th coefficient of the Dirichlet polynomial $P_{G,N}(s)$	p.8
$\mathrm{Aut}(G)$	group of automorphisms of G	
$\hat{a}_k$	largest Zsigmondy prime for $\langle a, k\rangle$	p.25
Alt_k	alternating group of degree k	
B	Borel subgroup of a simple group of Lie type	p.35
$C_G(H)$	centralizer in G of a subgroup H	
C_k	cyclic group of order k	
$d(G)$	minimal number of generators of G	
$f^{(\pi)}(s)$	π-Dirichlet polynomial of $f(s)$	p.9
$\mathbb{F}_q$	field with q elements	
$\mathrm{Frat}(G)$	Frattini subgroup of G	

G'	derived subgroup of G	
$\mathbb{N}$	natural numbers	
$\mathrm{M}_{n,k}(\mathbb{K})$	matrix $n \times k$ with coefficient in $\mathbb{K}$	
$N_G(H)$	normalizer in G of a subgroup H	
$\mathrm{Out}(G)$	group of outer automorphisms of G	
$O^r(G)$	smallest normal subgroup of G whose quotient is an r-group	
$P_G(s)$	Dirichlet polynomial of G	p.8
$P_{G,N}(s)$	Dirichlet polynomial of G given G/N	p.8
$P_G^{(\pi)}(s)$	π-Dirichlet polynomial of G	p.9
$P_{G,N}^{(\pi)}(s)$	π-Dirichlet polynomial of G given G/N	p.9
$\hat{q}_k^*$	product of the Zsigmondy prime for $\langle q, k\rangle$	p.26
$\mathcal{P}(Y)$	set of subsets of Y	
$\mathcal{R}$	ring of Dirichlet polynomials with integer coefficients	p.8
$\mathcal{R}_\pi$	subring of $\mathcal{R}$	p.8
$\mathcal{R}'$	subring of $\mathcal{R}$	p.23
$\mathcal{R}'_\pi$	subring of $\mathcal{R}'$	p.23
$\mathbb{R}$	real numbers	
$\mathrm{soc}(G)$	socle of G, i.e. product of the minimal normal subgroups of G	
$\mathrm{Stab}_G(Y)$	stabilizer of Y under the action of G	
Sym_k	symmetric group of degree k	
t	the number $\sqrt[\lvert\rho\rvert]{\lvert\mathbb{K}\rvert}$	p.29, 36
$v_p(k)$	p-adic valuation of k	p.26
X_π	set of commuting indeterminates $\{x_p : p \in \pi\}$	
$\mathbb{Z}$	integer numbers	
μ_G	Möbius function of the subgroup lattice of G	p.22
$\pi(k)$	set of prime divisors of k	
$\pi(G)$	set of prime divisors of $\lvert G\rvert$	
π'	set of prime numbers p such that $p \notin \pi$	p.8
ρ	symmetry of the Dynkin diagram	p.33

Φ	homomorphism of rings	p.9
Ψ	homomorphism of rings	p.24
$\lvert f(s)\rvert_p$	p-part of $f(s)$	p.28
$\lvert k\rvert_p$	p-part of k	p.26

0.2 Notation for Classical groups

For a better explanation, see also Subsection 3.1.1. The group $\mathrm{GL}(V, F)$ is the group of automorphisms of the vector space V over $\mathbb{F}_q$.

List of symbols

$A(V,\kappa), A$		p.32
$\mathcal{C}_1, ..., \mathcal{C}_8$	classes of geometric maximal subgroups	p.43
$\mathbf{f}$	bilinear form	p.31
$\bar{K}$	reduction modulo scalars (for $K \leq \Gamma(V,\kappa)$)	p.31
$I(V,\kappa), I$	subgroup of $\mathrm{GL}(V,\mathbb{F})$	p.31
$\mathbf{L}, \mathbf{S}, \mathbf{O}, \mathbf{U}$	types of Classical groups	p.31
$\mathbf{O}^\circ, \mathbf{O}^+, \mathbf{O}^-$	types of Classical groups	p.31
Q	quadratic form	p.31
$S(V,\kappa)$	subgroup of $\mathrm{GL}(V,\mathbb{F})$	p.32
$\mathcal{S}$	class of maximal subgroups	p.43
V	Vector space over $\mathbb{F}_q$	p.31
$\Gamma(V,\kappa), \Gamma$	κ-semisimilarity	p.31
κ	form defined on a vector space V	p.31
$\Omega(V,\kappa), \Omega$	subgroup of $\mathrm{GL}(V,\mathbb{F})$	p.32

0.3 Notation for root systems, Lie algebras, Dynkin diagrams

See Subsection 3.1.2 for a better explanation. In the sequel, let J be a subset of I, let u and w be two reflections.

List of symbols

$c_n(X, -(d-1))$		p.66
$\mathfrak{D}$	Dynkin diagram	p.33
$\mathfrak{D}'$	Dynkin diagram associated to $\mathcal{W}$	p.35
$\mathcal{D}_J, D_K$		p.35
$F_{\mathfrak{D}'}(t)$		p.36
I	set of ρ-orbits of Π	p.34
I_u	subset of I	p.64
I_u^c	complementary subset of I_u	p.64
$I_{u_1,...,u_l}$	intersection of $I_{u_1}, ..., I_{u_l}$	p.64
J^*	union of the elements of J	p.34
$\tilde{J}$	set of $N_X(B)$-orbits of J	p.41
$l(w)$	length of w	p.34
$l_{\mathcal{W}}^X$		p.66
$\mathfrak{L}$	simple Lie algebra	p.33
$o(J)$	size of $\tilde{J}$	p.41
P_J	parabolic subgroup over B, associated to the set of roots J	p.36
$\mathcal{P}^X(I)$	set of fixed point of $\mathcal{P}(I)$ under the action of $N_X(B)$	p.41
$\mathcal{S}_H(G)$	set of $L \leq G$ such that $L \geq H$	p.39
$\mathcal{S}_B^X(S)$	fixed point of $\mathcal{S}_B(S)$ under the action of $N_X(B)$	p.39
$T_{\mathcal{W}_J}(t)$		p.35
$\mathfrak{V}$	Cartan subalgebra of $\mathfrak{L}$	p.33

$\mathfrak{V}_K$	Subspace of $\mathfrak{V}$ spanned by K	p.34
W	Weyl group of Φ	p.34
W_K	Weyl group of Φ_K	p.34
$\mathcal{W}$	subgroup of W	p.35
$\mathcal{W}_i$		p.35
$\mathcal{W}_J$		p.35
w, w_r	reflection, element of W	p.34
Π, Σ	sets of fundamental roots	p.33
τ	isometry associated to ρ	p.34
$\tau^X_{\mathfrak{D}'}(i)$		p.69
Φ, Ψ	system of roots	p.33
Φ_K		p.34
Φ_i		p.35
Ψ^+	set of positive roots of Ψ w.r.t. a fundamental system Σ	p.34
Ψ^-	set of negative roots of Ψ w.r.t. a fundamental system Σ	p.34
ω_i	unique element of W_i such that $\omega_i(\Phi_i^+) = \Phi_i^-$	p.59
$(-,-)$	Killing form on $\mathfrak{L}$	p.33

0.4 Notation for Chapter 6

Let V be a vector space endowed with a form κ and let W be a subspace of V.

List of symbols

e_i, f_i, x, y, z	vectors of a basis of V	p.81
$H_{I^{(W)}}$		p.98
$I^{(W)}$	the group $I(W^\perp/W, \kappa_{W^\perp/W})$	p.93
L		p.107
$\mathcal{L}_H(X)$	set of $W \leq V$ such that $\mathrm{Stab}_{X\cap\overline{\Gamma}} \geq H \cap \overline{\Gamma}$	p.83
$\mathcal{L}_H^*(X)$	non-trivial totally singular elements of $\mathcal{L}_H(X)$	p.83
$\mathcal{L}_H^*(X)/\psi$	quotient set of $\mathcal{L}_H^*(X)$ under the action of $\psi \in \overline{A} - \overline{\Gamma}$	p.83
$\mathcal{L}_H^{(W)}$		p.93
$\mathcal{L}(+)$	$+$-reducible elements of $\mathcal{L} \subseteq \mathrm{Sub}(V)$	p.85
$\mathcal{L}(\cap)$	$\cap$-reducible elements of $\mathcal{L} \subseteq \mathrm{Sub}(V)$	p.85
$\mathcal{M}_H(X)$	maximal subgroups of X supplementing S and containing H	p.83
$\mathcal{P}$	property of a subset of $\mathrm{Sub}(V)$	p.85
$\mathrm{Sub}(V)$	set of all the vector subspaces of V	p.83
$\mathcal{U}_k$	set of totally singular subspaces of dimension k	p.84
$W^\perp$	orthogonal of W with respect to $\mathbf{f}$	p.81
$\beta(n)$		p.80
$\beta_p(X)$		p.58
$\tilde{\beta}_p(X)$		p.79
γ	homomorphism	p.84
κ_W	restriction of κ to W	p.81
$\kappa_{W^\perp/W}$	form induced by κ to $W^\perp/W$	p.93
$\phi_{l,h}$		p.82
$\phi^{(W)}$	element induced by ϕ in $I^{(W)}$	p.94
Ψ_H	map	p.84
(v, w)	$\mathbf{f}(v, w)$	p.81

0.5 Notation for Chapter 9

List of symbols

$\mathcal{G}_1$	family of groups	p.118
$\mathcal{G}_2$	family of groups	p.118
$\theta_1(X)$	number associated to the group X	p.119
$\theta_2(X)$	number associated to the group X	p.119

0.6 Notation for Part III

List of symbols

$h(n,q)$		p.140
$\mathcal{M}(A,k)$	maximal subgroups which order is divisible by k in a group A	p.141

0.7 Definitions

Introduction

Let G be a finite group and let N be a normal subgroup of G. The *Dirichlet polynomial* $P_{G,N}(s)$ *of* G *given* G/N is

$a_k(G,N)$

$$P_{G,N}(s) = \sum_{k\geq 1} \frac{a_k(G,N)}{k^s}, \text{ where } a_k(G,N) = \sum_{\substack{H \leq G,\, |G:H| = k,\\ NH = G,}} \mu_G(H).$$

Here μ_G is the Möbius function of the subgroup lattice of G, which is defined inductively by $\mu_G(G) = 1$ and $\mu_G(H) = -\sum_{K>H} \mu_G(K)$ if $H < G$. Moreover, *the Dirichlet* $P_G(s)$ *polynomial of* G is given by $P_G(s) = P_{G,G}(s)$ and $a_k(G) = a_k(G,G)$.

$a_k(G)$ The polynomials $P_G(s)$ and $P_{G,N}(s)$ are elements of the ring of Dirichlet finite $\mathcal{R}$ series (also called Dirichlet polynomials) with integer coefficients ,

$$\mathcal{R} = \left\{ \sum_{m\geq 1} \frac{a_m}{m^s} : a_m \in \mathbb{Z}, |\{m : a_m \neq 0\}| < \infty \right\}.$$

$a_k(f(s))$ Let $f(s) = \sum_{k\geq 1} \frac{a_k}{k^s}$ be an element of $\mathcal{R}$. We let $a_k(f(s)) = a_k$ be the k-th coefficient of $f(s)$.

π' Let π be a set of prime numbers and let π' be the set of prime number that do π-number not lie in π. We say that a positive number m is a π-*number* if each prime divisor of X_π m lies in π. Denote by X_π the set of commuting indeterminates $\{x_r : r \in \pi\}$. Let $\mathcal{R}_\pi$ $\mathcal{R}_\pi$ be the subring of $\mathcal{R}$ given by

$$\left\{ \sum_{m\geq 1} \frac{a_m}{m^s} \in \mathcal{R} : a_m \neq 0 \Rightarrow m \text{ is a } \pi'\text{-number} \right\}.$$

Note that both $\mathcal{R}$ and $\mathcal{R}_\pi$ are factorial domains (see [DLM04]). In fact there exists
Φ a ring isomorphism

$$\Phi : \ \mathcal{R}_\pi \ \rightarrow \ \mathbb{Z}[X_{\pi'}]$$

defined by $\Phi(r^{-s}) = x_r$ for each $r \in \pi'$.

Moreover, there is an interesting ring homomorphism between $\mathcal{R}$ and $\mathcal{R}_\pi$, given by $f^{(\pi)}(s)$

$$\begin{array}{ccc} \mathcal{R} & \rightarrow & \mathcal{R}_\pi \\ f(s) = \sum_{k\in\mathbb{N}} \frac{a_k}{k^s} & \mapsto & f^{(\pi)}(s) = \sum_{k\in\mathbb{N}} \frac{b_k}{k^s} \end{array}$$

where

$$b_k = \begin{cases} a_k & \text{if } k \text{ is a } \pi'\text{-number} \\ 0 & \text{otherwise.} \end{cases}$$

In particular, the polynomial $P^{(\pi)}_{G,N}(s)$ is called the *π-Dirichlet polynomial of G given N* and the polynomial $P^{(\pi)}_G(s)$ is called the *π-Dirichlet polynomial of G*. $P^{(\pi)}_{G,N}(s)$ $P^{(\pi)}_G(s)$

As noted in [Gas59], some values of the polynomials $P_G(s)$ and $P_{G,N}(s)$ have a probabilistic interpretation. In fact, for $n \geq d(G/N)$, the number $P_{G,N}(n)$ is the conditional probability that n randomly chosen elements $g_1, ..., g_n$ of G generate G, given that $Ng_1, ..., Ng_n$ generate G/N. Also the polynomial $P^{(r)}_G(s)$ has a probabilistic interpretation. In fact, if r is a prime number and P is a Sylow r-subgroup of G, then for each positive integer n the number $P^{(r)}_G(s)$ is the conditional probability that n randomly chosen elements of G generate G together with the elements of P, given that their product normalizes P (see [DL07b, Proposition 1]).

Chapter 1

History and motivations

The Dirichlet polynomial of a group has been studied by many authors. In the 1996, Mann introduced the Probabilistic Zeta function of a group, which is the counterpart of the Dirichlet polynomial (see [Man96]). In his article, he pointed out the possibility to define this object for a wide class of groups, namely the positively finitely generated groups. However, the study of the finite case is very important. For instance, if G is a profinite group and $\{N_i\}_{i\in I}$ is a set of normal open subgroups of G such that $\bigcap_i N_i = 1$, then $P_G(s) = \inf_i P_{G/N_i}(s)$.

In the same year, Boston proposed the study of this function and in particular of its irreducible factors (which are called the *generalized Euler factors*), in order to obtain a better understanding for a possible number theoretical interpretation (see [Bos96]). In fact, it was already known to Gaschütz (see [Gas59]) that

$$P_G(s) = P_{G/N}(s)P_{G,N}(s),$$

where N is a normal subgroup of G. So, if $1 = G_0 \trianglelefteq G_1 \trianglelefteq ...G_k = G$ is a chief series of G, then we have:

$$P_G(s) = \prod_{i=0}^{k-1} P_{G/G_i,G_{i+1}/G_i}(s). \quad (*)$$

The factorization $(*)$ is well understood, thanks to the work of Gaschütz (see [Gas59] and [Gas62]), Detomi and Lucchini (see [DL03b]) on the crowns. We need

some definitions in order to explain this factorization. Let N be a minimal normal subgroup of a group G, and let

$$L_N = \begin{cases} G/C_G(N) & \text{if } N \text{ is not abelian,} \\ G/C_G(N) \ltimes N & \text{otherwise.} \end{cases}$$

be the *monolithic primitive group associated with* N. Clearly N is (isomorphic to) the socle of L_N. Moreover, if $A = H/K$ is a chief factor of G, then A is a minimal normal subgroup of G/K and $L_A = L_{H/K}$. Define:

$$\tilde{P}_{L_N,1}(s) = P_{L_N,N}(s), \;\; \tilde{P}_{L_N,i}(s) = P_{L_N,N}(s) - \frac{(1 + q_N + ... + q_N^{i-2})\gamma_N}{|N|^s} \text{ for } i > 1,$$

where $\gamma_N = |C_{\mathrm{Aut}(N)}(L_N/N)|$ and $q_N = |\mathrm{End}_{L_N}(N)|$ if N is abelian, $q_N = 1$ otherwise. In particular, note that if N is abelian, then N is a direct product of isomorphic cyclic groups of prime order and

$$P_{L_N,N} = 1 - \frac{|Der(L_N/N, N)|}{|N|^s},$$

where $|Der(L_N/N, N)|$ is the number of complement of N in L_N.

Finally, let A_1 and A_2 be two chief factors of G. We say that A_1 is *G-equivalent* to A_2 if A_1 and A_2 are G-isomorphic to the minimal normal subgroups of a primitive epimorphic image of G (recall that this epimorphic image has one or two minimal normal subgroups and in the latter case they are not G-isomorphic). For a non-Frattini chief factor A of G, let $\delta_G(A)$ be the number of factors of G which are G-equivalent to A (it is independent on the choice of the chief series). Now we can state the main result of [DL03b].

Theorem 1.1 ([DL03b, Theorem 18])**.** *Let G be a finite group. Then*

$$P_G(s) = \prod_{A \in \mathcal{A}} \left(\prod_{1 \le i \le \delta_G(A)} \tilde{P}_{L_A,i}(s) \right),$$

where $\mathcal{A}$ is the set of representatives of the quotient set given by the G-equivalence relation on the set of chief factors of G, and L_A is the monolithic primitive group associated with A.

Because of this theorem, we have that the factorization $(*)$ is independent on the choice of the series and it is well understood in terms of Dirichlet polynomials of primitive monolithic groups. Since the knowledge of the primitive monolithic groups with abelian socle is complete, the Dirichlet polynomial of a soluble group is well known, as shown in the following result.

Theorem 1.2 ([DL03a, Theorem 5])**.** *Let G be a finite group. The following are equivalent:*

(1) G is soluble;

(2) the factors of $P_G(s)$ are of the form $\left(1-\frac{c}{q^s}\right)$ for some $c \in \mathbb{N}$ and q a prime power,

(3) the sequence $n \mapsto a_n(G)$ is multiplicative, i.e. $a_{nm}(G) = a_n(G)a_m(G)$ whenever $(m,n) = 1$.

We can say some more words on the Dirichlet polynomial of a monolithic primitive group L with non-abelian socle N. Assume that S is a simple component of L, define $X = N_L(S)/C_L(S)$ and $n = |L : N_L(S)|$. Since $S \cong \mathrm{soc}(X)$, assume that $S \leq X$. The following result shows a connection between the Dirichlet polynomials $P_{L,N}(s)$ and $P_{X,S}(s)$.

Theorem 1.3 (See [Ser08, Theorem 5])**.** *Under the above conditions we have that*

$$P^{(r)}_{L,N}(s) = P^{(r)}_{X,S}(ns - n + 1)$$

for each prime divisor r of the order of S.

1.1 The coset poset and the Dirichlet polynomial of a group

Let $\mathcal{C}(G)$ be the set of the proper cosets of G, i.e. $\mathcal{C}(G) = \{Hg : H < G, g \in G\}$. It is ordered by inclusion, so we refer to $\mathcal{C}(G)$ as *the coset poset of G.*

A natural object of investigation is the order complex $\Delta(\mathcal{C}(G))$ of $\mathcal{C}(G)$ (which is a simplicial complex). The elements of $\Delta(\mathcal{C}(G))$ are finite chains

$$H_1 g_1 < H_2 g_2 < ... < H_k g_k$$

of elements of $\mathcal{C}(G)$ (for references, see [Mun84] and [Spa66]). In particular, we can speak of the Euler characteristic $\chi(\mathcal{C}(G)) := \chi(\Delta(\mathcal{C}(G)))$ and the reduced Euler characteristic $\tilde{\chi}(\mathcal{C}(G)) := \chi(\mathcal{C}(G)) - 1$. In [Bro00], Brown pointed out a connection between the order complex $\Delta(\mathcal{C}(G))$ and the Dirichlet polynomial of G. In fact, it turns out that

$$P_G(-1) = -\tilde{\chi}(\mathcal{C}(G)).$$

Remind that if a complex is contractible, then the Euler characteristic equals one. Noting that $P_G(-1) \neq 0$ if G is a soluble group, Brown conjectured that $P_G(-1) \neq 0$ for all finite groups G.

In the soluble case, Brown proved the following result.

Proposition 1.4 ([Bro00, Proposition 8])**.** *Let G be a finite soluble group and let d be the number of non-Frattini chief factor of G. Then $\Delta(\mathcal{C}(G))$ has the homotopy type of a bouquet of $(d-1)$-spheres and the number of spheres is $|\tilde{\chi}(\mathcal{C}(G))| = |P_G(-1)|$.*

No such result is known for non-soluble groups, apart from some cases (e.g. $\Delta(\mathcal{C}(\mathrm{Alt}_5))$ is homotopy equivalent to a bouquet of 2-spheres, see [Bro00]).

In our thesis (see also [Pat09b]) we prove that $\Delta(\mathcal{C}(G))$ is not contractible for a wide class of classical groups. Our main result is the following.

Theorem 1.5. *Let G be a classical group which does not contain non-trivial graph automorphisms. Then $P_G(-1)$ does not vanish, hence the order complex $\Delta(\mathcal{C}(G))$ is not contractible.*

The proof of this theorem requires a careful work on the structure of the parabolic subgroups of G and their intersections (especially when the intersection of two maximal parabolic subgroups of G is not a parabolic subgroup) and a good knowledge

about the maximal subgroups of G (invoking also the classification of finite simple groups).

Using Theorem 1.3, we extend this result to the groups whose composition factors are classical simple groups (under certain technical conditions, see Theorem 7.1). Part I of the present thesis is devoted to the proof of this result.

The connection between the coset poset of the group G and the Dirichlet polynomial of G is strong. In fact, the coset poset of G completely determines $P_G(s)$, as shown in [Bro00, Section 9]. In particular, let $\mathcal{L}$ be the coset lattice of G, consisting of all cosets of G and the empty set. A Möbius function $\tilde{\mu}$ is defined on $\mathcal{L}$, setting $\tilde{\mu}(G) = 1$ and $\sum_{H \in \mathcal{L}, H \supset K} \tilde{\mu}(H) = 0$ if $K \in \mathcal{L}$ is properly contained in G. So we can construct a Dirichlet polynomial

$$P_{\mathcal{C}(G)}(s) = \sum_{K \in \mathcal{L} - \{\varnothing\}} \frac{\tilde{\mu}(K)}{(|G| : |K|)^s}.$$

It turns out that

$$P_{\mathcal{C}(G)}(s+1) = P_G(s),$$

so the coset poset completely determines $P_G(s)$. Moreover, note that

$$\tilde{\chi}(\Delta(\mathcal{C}(G))) = \tilde{\mu}(\varnothing) = -\sum_{H \in \mathcal{L}, H \supset \varnothing} \tilde{\mu}(H) = -P_{\mathcal{C}(G)}(0) = -P_G(-1).$$

1.2 Irreducibility of the Dirichlet polynomial of a group

As we have seen before, the ring of Dirichlet polynomials is a factorial domain. It is a natural question to ask when a Dirichlet polynomial of a group G is irreducible. An easy result is the following.

Lemma 1.6 ([DLM04, Corollary 7])**.** *If $P_G(s)$ is irreducible, then $G/\mathrm{Frat}(G)$ is a simple group.*

A more general result is the following.

Proposition 1.7. *Let G be a finite group such that* $\mathrm{Frat}(G) = 1$. *If $P_{G,\mathrm{soc}(G)}(s)$ is irreducible, then G is a primitive monolithic group.*

Proof. Let N be a minimal normal subgroup of G. By definition, we have that $N \leq \mathrm{soc}(G)$. It is straightforward to show that $P_{G,\mathrm{soc}(G)}(s) = P_{G,N}(s)P_{G/N,\mathrm{soc}(G)/N}(s)$. Since $P_{G,\mathrm{soc}(G)}(s)$ is irreducible we have that either $P_{G,N}(s) = 1$ or $P_{G/N,\mathrm{soc}(G)/N}(s) = 1$.

Since $\mathrm{Frat}(G) = 1$, by [Laf78, Lemma] we have that the chief factors below $\mathrm{soc}(G)$ are non-Frattini. By [DLM04, Lemma 6], if $K \trianglelefteq G$, then $P_{G,K}(s) = 1$ if and only if $K \leq \mathrm{Frat}(G)$. Assume that $P_{G,N}(s) = 1$. We get that $N \leq \mathrm{Frat}(G)$, against the hypothesis. Thus we have $P_{G/N,\mathrm{soc}(G)/N}(s) = 1$, so $\mathrm{soc}(G)/N \leq \mathrm{Frat}(G/N)$. Since the chief factors of G under $\mathrm{soc}(G)$ are non-Frattini we get $N = \mathrm{soc}(G)$.

Let M be a maximal subgroup of G which does not contain $\mathrm{soc}(G)$ (it exists since $\mathrm{Frat}(G) = 1$). Let

$$\mathrm{core}_G(M) = \bigcap_{g \in G} M^g$$

and note that $\mathrm{core}_G(M) \trianglelefteq G$. Clearly we have that $\mathrm{core}_G(M) = 1$, otherwise $\mathrm{soc}(G) \leq \mathrm{core}_G(M)$ but $\mathrm{soc}(G) \not\leq M$. Hence G is a primitive group. This completes the proof. □

As we have seen in the beginning of this chapter, the Dirichlet polynomial of a group G factorizes in correspondence to the chief factors of G. In particular, given a non-Frattini chief factor H/K of G we have that $P_{G/K,H/K}(s)$ divides $P_G(s)$. Unfortunately, the factor $P_{G/K,H/K}(s)$ is not always irreducible in $\mathcal{R}$. For instance, we have:

$$P_{\mathrm{PSL}_2(7)}(s) = (1 - 2/2^s)(1 + 2/2^s + 4/4^s - 14/7^s - 28/14^s - 28/28^s + 21/21^s + 42/42^s)$$

and

$$P_{\mathrm{Alt}_4,V}(s) = (1 - 4/4^s) = (1 - 2/2^s)(1 + 2/2^s),$$

where V is the subgroup of order 4 in Alt_4.

The results on the irreducibility of $P_G(s)$ are collect in the following theorem.

Theorem 1.8. *The following hold:*

- *If p is a prime number such that $p \geq 5$, then $P_{\mathrm{Alt}_p}(s)$ is irreducible ([DLM04, Theorem 12]).*
- *If p is a prime number such that $p \geq 5$, then $P_{\mathrm{PSL}_2(p)}(s)$ is reducible if and only if $\log_2(p+1) \equiv 3 \pmod 4$ ([DLM04, Proposition 14 and 15])*
- *If q is a power of a prime number and q is not a prime number, then $P_G(s)$ is irreducible for $G = \mathrm{PSL}_2(q), {}^2B_2(q)$ or ${}^2G_2(q)$ ([Pat09c, Proposition 15]).*

In this thesis (see also [Pat09a]) we prove the following.

Theorem 1.9. *Let G be a finite simple group of Lie type. The Dirichlet polynomial $P_G(s)$ is reducible if and only if $G \cong \mathrm{PSL}_2(p)$ and $\log_2(p+1) \equiv 3 \pmod 4$.*

In order to obtain this result, we study the irreducibility of the Dirichlet polynomial $P_G^{(p)}(s)$ (which is well understood) and we use some results on the irreducibility of a multivariate polynomial with coefficient in $\mathbb{Z}$ to extend the result to the polynomial $P_G(s)$. Again we invoke the classification of finite simple groups.

Moreover, thanks to Theorem 1.3, we extend the result to some polynomials of type $P_{G,N}(s)$, where G is a monolithic primitive group with socle N (see Theorem 8.1). Part II is dedicated to the proof of this result.

1.3 Recognition of properties of the group from its Dirichlet polynomial

Let G and H be two finite groups and assume that $P_G(s) = P_H(s)$. Suppose that we know the group G. What can we say about H? It is easy to see that we can not infer that $H \cong G$, since, for instance, $P_G(s) = P_{G/\mathrm{Frat}(G)}(s)$. Also $H/\mathrm{Frat}(H) \cong G/\mathrm{Frat}(G)$ is not true. For example, $P_{C_6 \times C_3}(s) = P_{\mathrm{Sym}_3 \times C_3}(s)$ and $P_{\mathrm{PGL}_2(9)}(s) = P_{M_{10}}(s)$ (use [GAP]). However, many properties of H can be recognized from the Dirichlet polynomial H. We summarize them in the following theorem.

Theorem 1.10. *Let p be a prime number. Let G and H be two finite groups and assume that $P_G(s) = P_H(s)$.*

- *If G is soluble, then H is soluble ([DL03c, Theorem 1], see also Theorem 1.2).*
- *If G is a p-group, then H is a p-group.*
- *If G is p-soluble, then H is p-soluble. In particular, G is p-soluble if and only if the sequence $\{a_n(G)\}_{n\in\mathbb{N}}$ is p-multiplicative ([DL07a, Theorem 1.2]).*
- *If G is perfect, then H is perfect ([DL03a, Proposition 7]). In particular, the following are equivalent:*
  - *$O^p(G) = G$.*
  - *p divides $a_p(G)$.*
- *If G is simple, then $H/\mathrm{Frat}(H)$ is simple ([DL07b, Theorem 7]). In particular, assume that the following hold:*
  (1) $P_H^{(2)}(s)$ has a simple zero in 1, i.e. $P_H^{(2)}(1) = 0$ and $\prod_{(n,2)=1} n^{\frac{a_n(G)}{n}} \neq 1$.
  (2) Let $m = \min\{k : a_k(H) \neq 0, k > 1\}$. If $a_k(H) \neq 0$, then k divides $m!$.
  (3) If $a_k(H) \neq 0$ and k is a power of a prime number, then k divides $a_k(H)$ and either $k = m$ or $(k, m) = (8, 7)$.

  Then $H/\mathrm{Frat}(H)$ is a non-abelian simple group ([DL07b], [Mas07]).

We can say something more when G is a simple group. In fact, we have the following.

Theorem 1.11. *Let G be a finite simple group and let H be a finite group such that $P_G(s) = P_H(s)$.*

- *If G is abelian, then $H/\mathrm{Frat}(H) \cong G$.*
- *If G is alternating, then $H/\mathrm{Frat}(H) \cong G$ ([DL04]).*

- *If G is sporadic, then $H/\mathrm{Frat}(H) \cong G$ ([DL06, Theorem 11]).*
- *If G and H are simple groups of Lie type defined over fields with the same characteristic, then $G \cong H$ ([DL06, Theorem 14]).*

In Part III of this thesis, we complete the prove of the following.

Theorem 1.12. *Let G be a finite simple group and let H be a finite group. If $P_G(s) = P_H(s)$, then $H/\mathrm{Frat}(H) \cong G$.*

In particular, we show that it is possible to recognize the characteristic of a simple group of Lie type from its Dirichlet polynomial (see Theorem 13.6 and Proposition 14.1). In most cases, it turns out that the characteristic of G is the "dominant prime" of $P_G(s)$ (i.e. a prime number p such that if r is a prime number and $\mathrm{po}(G) = \mathrm{lcm}\{n|a_n(G) \neq 0\}$, then $|\mathrm{po}(G)|_p \geq |\mathrm{po}(G)|_r$). In order to obtain the result we need to study some maximal subgroups of the groups of Lie type, so we invoke the classification of finite simple groups, which is also required to complete the proof of the main theorem.

In the past, some conjectures on $P_G(s)$ were proposed. A way to recognize a simple group is to know the order of the group. In fact, there are at most two non-isomorphic simple groups with the same order. In order to recognize the order of a simple group G from $P_G(s)$, it is natural to compare the number $\mathrm{po}(G) = \mathrm{lcm}\{n|a_n(G) \neq 0\}$ with $|G|$. It was conjectured that $|G| = \mathrm{po}(G)$ (see [DL03a, Conjecture 1], and [DL06]). This is false. In fact, if $G = \mathrm{PSL}_2(p)$ with p a prime number such that $p \equiv 17 \pmod{40}$ ([Pat09c]), then $\mathrm{po}(G) = |G|/2$. Moreover, $\mathrm{po}(\mathrm{PSU}_3(3)) = |\mathrm{PSU}_3(3)|/8$ (use [GAP]). However, a weaker result was conjectured in [DL06] and proved in [DL07a].

Theorem 1.13 ([DL07a, Theorem 1.3])**.** *Let G be a finite group. Then $\pi(|G/\mathrm{Frat}(G)|) = \pi(\mathrm{po}(G))$.*

This means that we can recover the prime divisors of $|G/\mathrm{Frat}(G)|$ from the Dirichlet polynomial of G. Moreover, if G is a primitive monolithic group, then

the prime divisors of the socle $\mathrm{soc}(G)$ are exactly the prime numbers r such that $P^{(r)}_{G,\mathrm{soc}(G)}(s) \neq P_{G,\mathrm{soc}(G)}(s)$.

Another interesting question is the following. Given a finite group G, is it possible to recognize the non-Frattini chief factors of G from its Dirichlet polynomial? As we have seen in Theorem 1.1, we can factorize the Dirichlet polynomial considering a chief series of G. Now we say some words on the contribution of the abelian chief factors of G. We define another Dirichlet polynomial:

$$Q_G(s) = \prod_{A \in \mathcal{A}'} \left(\prod_{1 \leq i \leq \delta_G(A)} \tilde{P}_{L_A,i}(s) \right),$$

where $\mathcal{A}' = \{A \in \mathcal{A} : A \text{ is abelian}\}$. As we have seen before, we have that

$$Q_G(s) = \prod_{A \in \mathcal{A}'} \left(\prod_{1 \leq i \leq \delta_G(A)} \left(1 - \frac{c(A,i)}{|A|^s}\right) \right),$$

where $c(A,i)$ is a positive integer. Now, a factorization of this type is unique, as the following Lemma shows.

Lemma 1.14 ([DL03a, Lemma 16])**.** *Suppose that*

$$\prod_{1 \leq i \leq k_1} \left(1 - \frac{c_i}{p^{n_i s}}\right) = \prod_{1 \leq j \leq k_2} \left(1 - \frac{d_j}{p^{m_j s}}\right),$$

where $c_1, ..., c_{k_1}, d_1, ..., d_{k_1}$ are positive integers. Then $k_1 = k_2$ and there exists $\sigma \in \mathrm{Sym}(k_1)$ such that $m_{\sigma(i)} = n_i$ and $d_{\sigma(i)} = c_i$ for $1 \leq i \leq k_1$.

So, if we know the polynomial $Q_G(s)$, we know the non-Frattini abelian chief factors of G. Of course, it is not immediate to recognize the polynomial $Q_G(s)$ from $P_G(s)$: this requires a careful study of the contribution of the non-abelian chief factors to $P_G(s)$.

As well, in order to understand the non-abelian chief factors from the knowledge of $P_G(s)$ we wish to prove two facts:

- the Dirichlet polynomial $P_{G,\mathrm{soc}(G)}(s)$ is irreducible for G a monolithic primitive group, with few exception. At the present date, the alternating case is open and it seems to require a certain amount of number theoretical knowledge.

- if $P_{G_1,\mathrm{soc}(G_1)}(s) = P_{G_2,\mathrm{soc}(G_2)}(s)$ for two monolithic primitive groups G_1 and G_2, then $\mathrm{soc}(G_1) \cong \mathrm{soc}(G_2)$. If G_1 is abelian, the result is known. Assume that G_1 is not abelian. To prove the claim, it is useful to understand the number $n = |G : N_G(S)|$, where S is a simple component of a monolithic primitive group G (note $\mathrm{soc}(G) \cong S^n$). We believe that

$$n = \max\{m \in \mathbb{N} : \forall k \in \mathbb{Z} \text{ if } a_k(G, \mathrm{soc}(G)) \neq 0 \text{ and } \pi(k) \neq \pi(S), \text{ then } k \in \mathbb{Z}^m\}.$$

  In this way, we can reduce the problem to the almost simple case: in fact, by Theorem 1.3, we have that

$$P^{(r)}_{G_i,\mathrm{soc}(G_i)}(s) = P^{(r)}_{X_i,S_i}(n_i s - n_i + 1)$$

  for each prime number $r \in \pi(\mathrm{soc}(G_1)) = \{r : P^{(r)}_{G_1,\mathrm{soc}(G_1)}(s) \neq P_{G_1,\mathrm{soc}(G_1)}(s)\}$ (see below Theorem 1.13), where S_i is a simple component of G_i, $X_i = N_{G_i}(S_i)/C_{G_i}(S_i)$ and n_i is defined as n above. So the problem is reduced to the following: if X_1 and X_2 are almost simple groups such that

$$P^{(r)}_{X_1,\mathrm{soc}(X_1)}(s) = P^{(r)}_{X_2,\mathrm{soc}(X_2)}(s)$$

  for each prime number $r \in \pi(\mathrm{soc}(X_1)) = \{r : P^{(r)}_{X_1,\mathrm{soc}(X_1)}(s) \neq P_{X_1,\mathrm{soc}(X_1)}(s)\}$ (see below Theorem 1.13), then $\mathrm{soc}(X_1) \cong \mathrm{soc}(X_2)$. This can be proved quite easily when $\mathrm{soc}(X_1)$ is an alternating or sporadic group (the proof should be similar to the simple case). The situation for a groups of Lie type of characteristic p is quite more complicated: as in the simple case, one can try to find the Artin invariants (see the proof of [DL06, Theorem 14]). However, it seems to be harder here since it is not always true that $|P^{(p)}_{X_1,\mathrm{soc}(X_1)}(0)| = |\mathrm{soc}(X_1)|_p$, and this was a key fact in the proof of the claim in the simple case.

Nevertheless, we believe this two facts to hold true, so we conjecture the following.

Conjecture 1.15. *Let G and H be two finite groups. If $P_G(s) = P_H(s)$, then G and H have the same non-Frattini chief factors.*

Chapter 2

Basic results

In this chapter we give some notation and some results on the objects of our study.

2.1 The Möbius function of the subgroup lattice and the ring of Dirichlet polynomials

A very important object of our analysis is the Möbius function of the subgroup lattice of a group. Let G be a finite group. The Möbius function of the subgroup lattice of G is defined by :

μ_G

$$\mu_G(H) = \begin{cases} 1 & \text{if } H = G \\ -\sum_{H<K\leq G} \mu_G(K) & \text{if } H < G. \end{cases}$$

This function has some nice properties that we collect in the following proposition.

Proposition 2.1. *Let G be a finite group and H a subgroup of G.*

(1) If $\mu_G(H) \neq 0$, then H is intersection of maximal subgroups of G (See [Hal36]).

(2) The index $|N_G(H) : H|$ divides $\mu_G(H)|G : HG'|$ ([HIz89, Theorem 4.5]).

Let N be a normal subgroup of G and let m be a positive integer. Recall that

$$a_m(G, N) = \sum_{\substack{H \leq G, |G:H| = m, \\ NH = G,}} \mu_G(H).$$

Very often, in our proofs we have to show that $a_m(G,N) \neq 0$. By definition of $a_m(G,N)$ we have the following result.

Lemma 2.2. *Let G be a finite group, let N be a normal subgroup of G and let m be a positive integer.*

(1) Assume that if H is a subgroup of G such that $HN = G$ and $|G:H| = m$, then H is maximal. We have that $a_m(G,N) \neq 0$.

(2) Assume that if H_1 and H_2 are subgroups of G such that $H_1N = H_1N = G$ and $|G:H_2| = |G:H_1| = m$, then H_1 and H_2 are conjugated in G. We have that $a_m(G,N) \neq 0$ if and only if $\mu_G(H_1) \neq 0$.

The second result stated in Proposition 2.1, has an interesting consequence. Indeed, if $N \leq G'$, then Proposition 2.1 implies that $|N_G(H) : H|$ divides $\mu_G(H)$ if $HN = G$. Now, we have that

$$a_m(G,N) = \sum_{H \in \mathcal{C}_m(G,N),} |G : N_G(H)|\mu_G(H),$$

where $\mathcal{C}_m(G,N)$ is a set of representatives of the conjugacy classes of subgroups H of G such that $HN = G$ and $|G:H| = m$. Thus we obtain the following.

Lemma 2.3. *Let G be group and let N be a normal subgroup of G such that $N \leq G'$. Then m divides $a_m(G,N)$ for each positive integer m.*

Assume that $N \leq G'$. By the above lemma, we get that $P_{G,N}(s)$ is an element of $\mathcal{R}'$

$$\mathcal{R}' = \left\{ \sum_{m \geq 1} \frac{a_m}{m^s} : a_m \in m\mathbb{Z}, |\{m : a_m \neq 0\}| < \infty \right\},$$

which is a subring of $\mathcal{R}$. Let π be a set of prime numbers. We have that $P^{(\pi)}_{G,N}(s)$ is an element of $\mathcal{R}'_\pi$

$$\mathcal{R}'_\pi = \left\{ \sum_{m \geq 1} \frac{a_m}{m^s} \in \mathcal{R}' : a_m \neq 0 \Rightarrow m \text{ is a } \pi' \text{ number} \right\}.$$

We define the map Ψ

$$\Psi : \mathcal{R}'_\pi \rightarrow \mathbb{Z}[X_{\pi'}]$$

given by $\Psi(p^{1-s}) = x_p$ for each $p \in \pi$. Clearly, Ψ is a ring isomorphism. In particular, since the groups we are studying satisfies the condition $N \leq G'$, we consider $P_{G,N}(s)$ as an element of $\mathcal{R}'_\pi$, for $\pi' = \pi(N)$.

EXAMPLE 1. Let $G = \mathrm{Alt}_5$. By [GAP], we have

$$P_G(s) = 1 - 5^{1-s} - 6^{1-s} - 10^{1-s} + 20^{1-s} + 2 \cdot 30^{1-s} - 60^{1-s},$$

hence

$$\Psi(P_G(s)) = 1 - x_5 - x_2x_3 - x_2x_5 + x_2^2x_5 + 2x_2x_3x_5 - x_2^2x_3x_5.$$

When we study the irreducibility of a Dirichlet polynomial we heavily use this correspondence between the ring of Dirichlet polynomials and the ring of polynomials with integer coefficients. Usually, in order to prove that a certain Dirichlet polynomial $f(s) = \sum_{m \geq 1} \frac{a_m}{m^s} \in \mathcal{R}'_\pi$ is irreducible in $\mathcal{R}$, we show that $\Psi(f(s))$ is irreducible in $\mathbb{Z}[X_{\pi'}]$. This is enough under the assumption $a_1(f(s)) = 1$, as shown in the below lemma.

Lemma 2.4. *Let π be a set of prime and let $f(s)$ be an element of ${\mathcal{R}'}_\pi$ such that $a_1(f(s)) = 1$. Then $f(s)$ is irreducible in $\mathcal{R}$ if and only if $\Psi(f(s))$ is irreducible in $\mathbb{Z}[X_{\pi'}]$.*

Proof. The map Ψ is an isomorphism of rings, hence $f(s)$ is irreducible in ${\mathcal{R}'}_\pi$ if and only if $\Psi(f(s))$ is irreducible in $\mathbb{Z}[X_{\pi'}]$. Since $a_1(f(s)) = 1$ we have that $f(s)$ is irreducible as an element of $\mathcal{R}'$ if and only if $f(s)$ is irreducible in $\mathcal{R}$. Indeed, assume that $f(s)$ is irreducible in $\mathcal{R}'$ and $f(s) = g(s)h(s)$ in $\mathcal{R}$. Thus there exists $m_1, m_2 \in \mathbb{Z}$ such that $m_1g(s)$ and $m_2h(s)$ are in $\mathcal{R}'$. So $m_1m_2f(s) = m_1g(s)m_2h(s)$, but $f(s)$ is prime in $\mathcal{R}'$, then $f(s)$ divides $m_1g(s)$ or $m_2h(s)$. Without loss of generality, assume that $mf(s) = m_2h(s)$ for some $m \in \mathbb{Z}$. We get $m_1m_2f(s) = m_1g(s)m_2h(s) = m_1g(s)mf(s)$, hence $m_2 = g(s)m$, so $g(s)$ is an integer. Since $f(s) = g(s)h(s)$, $a_1(f(s)) = 1$ and $g(s) \in \mathbb{Z}$, we have that $|g(s)| = 1$. Thus we get the claim. $\square$

Finally, Theorem 1.3 can be restated in the following way.

Theorem 2.5 (See [Ser08, Theorem 5]). *Let L be a monolithic primitive group with a simple component S. Let $X = N_L(S)/C_L(S)$ and let $n = |L : N_L(S)|$. Let $\Gamma : \mathbb{Z}[X_{\pi(S)'}] \to \mathbb{Z}[X_{\pi(S)'}]$ be the ring homomorphism defined by $\Gamma(x_r) = x_r^n$ for each $r \in \pi(S)'$. We have that*

$$\Psi(P^{(\pi)}_{L,\mathrm{soc}(L)}(s)) = \Gamma(\Psi(P^{(\pi)}_{X,\mathrm{soc}(S)}(s)))$$

for each $\pi \subseteq \pi(S)$.

Example 2. Let $L = M_{22}^n \rtimes C_n$ and $\pi = \{2\}$. In this case $\mathrm{soc}(L) \cong M_{22}^n$ and $X = \mathrm{soc}(S) = S$, so $P_{X,S}(s) = P_S(s)$, and we have (use [GAP]):

$$P^{(2)}_{X,S}(s) = P^{(2)}_S(s) = 1 - 77^{1-s} - 231^{1-s} + 1155^{1-s},$$

$$P^{(2)}_{L,\mathrm{soc}(L)}(s) = P^{(2)}_{X,S}(ns - n + 1) = 1 - 77^{n(1-s)} - 231^{n(1-s)} + 1155^{n(1-s)},$$

and

$$\Psi(P^{(2)}_S(s)) = 1 - x_7x_{11} - x_3x_7x_{11} + x_3x_5x_7x_{11},$$

$$\Psi(P^{(2)}_{L,\mathrm{soc}(L)}(s)) = 1 - x_7^nx_{11}^n - x_3^nx_7^nx_{11}^n + x_3^nx_5^nx_7^nx_{11}^n = \Gamma(\Psi(P^{(2)}_S(s))).$$

2.2 The Zsigmondy primes

We state some useful results on the primitive prime divisors.

Lemma 2.6 (see [Zsi92]). *Let $a, k \in \mathbb{N}$, $a, k \geq 2$. There exists a prime divisor r of $a^k - 1$ such that r does not divide $a^i - 1$ for all $0 < i < k$, except in the following cases:*

- *$k = 2, a = 2^s - 1$ with $s \geq 2$.*
- *$k = 6, a = 2$.*

*When this prime divisor exists, it is called a **Zsigmondy prime for** $\langle a, k\rangle$.*

Let a and k be two positive integers greater than 1. If there exists a Zsigmondy prime for $\langle a, n\rangle$ we let $\hat{a}_k$ be the greatest Zsigmondy prime for $\langle a, k\rangle$. $\hat{a}_k$

Lemma 2.7 (see [Fei88]). *Let $a, k \in \mathbb{N}, a, k \geq 2$. Let r be a Zsigmondy prime for $\langle a, k\rangle$. We have that:*

- *$r \equiv 1 \pmod{n}$, so $r \geq k+1$.*
- *If $k \geq 3$ and $(a,k) \notin \{(2,4),(2,6),(2,10),(2,12),(2,18),(3,4),(3,6),(5,6)\}$, and r is the largest Zsigmondy prime for $\langle a, k\rangle$, then $|a^k - 1|_r > k+1$ (i.e. r^2 divides $a^k - 1$ or $r \geq 2k+1$).*

Lemma 2.8 ([LPS90, p.38]). *Let $k \in \mathbb{N}, k \geq 3$ and let $q = p^f$ for some prime number p and $f \geq 1$, $(q,k) \neq (2,6)$. Let $\hat{q}_k^*$ denote the product of the Zsigmondy prime for $\langle q, k\rangle$. We have that:*

$\hat{q}_k^*$

- *If $\hat{q}_k^* = k+1$, then $(q,k) \in \{(2,4),(2,10),(2,12),(2,18),(3,4),(3,6),(5,6)\}$.*
- *If $\hat{q}_k^* = 2k+1$, then $(q,k) \in \{(2,3),(2,8),(2,20),(4,3),(4,6)\}$.*

2.3 The r-part of $q^n \pm 1$

Let p be a prime number and let k be an integer. We denote by $|k|_p$ the *p-part of k*, i.e. $|k|_p = p^i$ where p^i divides k but p^{i+1} does not divide k. We set $|0|_p = 0$. The *p-adic valuation of k* is the number $v_p(k)$ which is the smallest integer such that $p^{v_p(k)} = |k|_p$. We set $v_p(0) = -\infty$.

$|k|_p$

$v_p(k)$

Let r be another prime number and let q be a power of p. Let t be the smallest positive integer such that $q^t \equiv 1 \pmod{r}$. Moreover, let

$$h = \begin{cases} v_r(q^t - 1) & \text{if } r \neq 2 \\ \max\{h^+, h^-\} & \text{if } r = 2, \end{cases}$$

where $h^- = v_2(q-1)$ and $h^+ = v_2(q+1)$.

Lemma 2.9 ([HB82, Lemma 8.1]). *Let $q \geq 3$ be an odd natural number and let n be a positive integer. We have that*

$$|q^n - 1|_2 = \begin{cases} \max\{|q-1|_2, |q+1|_2\}|n|_2 & \text{if } 4|(q-1) \text{ or } n \text{ is even,} \\ 2 & \text{if } 4|(q+1) \text{ and } n \text{ is odd.} \end{cases}$$

$$|q^n+1|_2 = \begin{cases} 2 & \text{if } 4|(q-1) \text{ or } n \text{ is even,} \\ |q+1|_2 & \text{if } 4|(q+1) \text{ and } n \text{ is odd.} \end{cases}$$

Let $r \neq 2$ be a prime number, $q \geq 2$ a natural number; then we have:

$$|q^n-1|_r = \begin{cases} 1 & \text{if } t \nmid n, \\ |q^t-1|_r|n/t|_r & \text{if } t|n. \end{cases}$$

$$|q^n+1|_r = \begin{cases} 1 & \text{if } t \nmid 2n \text{ or } t|n, \\ |q^t-1|_r|2n/t|_r & \text{if } t|2n \text{ and } t \nmid n. \end{cases}$$

2.4 On the irreducibility of a polynomial

In the sequel, we give some results on the irreducibility of polynomials we shall use in Part II.

Lemma 2.10. *Let D be a commutative domain. Suppose that $a \in D$ and let $f(x) = 1 - ax^m \in D[x]$. We have that $f(x)$ is reducible in $D[x]$ if and only if one of the following holds:*

- *$a \in D^u$ for some prime number u such that u divides m;*
- *$-4a \in D^4$ and 4 divides m.*

Proof. Left to the reader: just apply [Lan02, Chap. VI, Theorem 9.1]. □

Since we deal with polynomials with integer coefficients, we have that D is a ring of polynomial with integer coefficients. Thus the above lemma has the following immediate consequence.

Corollary 2.11. *Let $D = \mathbb{Z}[x_1, ..., x_k]$. Suppose that $a \in D$ and let $f(x) = 1 - ax^m \in D[x]$. If $f(x)$ is reducible, then $a^2 \in D^{2u}$ for some prime divisor u of m.*

Another corollary of Lemma 2.10 is the following.

Corollary 2.12. *Let D be a factorial domain and suppose that $f(x) \in D[x]$ is an irreducible polynomial such that $f(0) \neq 0$. Let $k \geq 1$ and $m_1, ..., m_k \in \mathbb{N} - \{0\}$ such that $(m_1, ..., m_k) = 1$. The polynomial $f(x_1^{m_1} \cdot ... \cdot x_k^{m_k})$ is irreducible in $D[x_1, ..., x_k]$.*

Proof. Let F be the field of fraction of D and let $\overline{F}$ be the algebraic closure of F. An irreducible factor of $f(x)$ in $\overline{F}[x]$ is a polynomial $g(x) = x - a$ for some $a \in \overline{F} - \{0\}$, since $f(0) \neq 0$. By the previous Lemma, $g(x_1^{m_1} \cdot ... \cdot x_k^{m_k}) = x_1^{m_1} \cdot ... \cdot x_k^{m_k} - a$ is irreducible in $\overline{F}[x_1, ..., x_k]$. So an irreducible factor of $f(x_1^{m_1} \cdot ... \cdot x_k^{m_k})$ in $\overline{F}[x_1, ..., x_k]$ is a polynomial $g(x_1^{m_1} \cdot ... \cdot x_k^{m_k})$. This proves that if $f(x_1^{m_1} \cdot ... \cdot x_k^{m_k})$ is reducible in $D[x_1, ..., x_{m_k}]$, then $f(x)$ is reducible in $D[x]$. □

In order to state the next lemma, we need some definition. Let $f(s)$ be a Dirichlet
$|f(s)|_r$ polynomial in $\mathcal{R}$. We denote by $|f(s)|_r$ the *r-part of* $f(s)$, i.e. the least common multiple of the numbers $\{|k|_r : a_k(f(s)) \neq 0\}$.

Lemma 2.13. *Let $h(s) = \sum_{k=1}^{\infty} \frac{a_k}{k^s}$ be a Dirichlet polynomial and let m be the least common multiple of $\{k : a_k \neq 0\}$. Assume that the following hold:*

- *There exists a set of prime number π_0 such that $h^{(\pi_0)}(s)$ is irreducible.*
- *There exists a set $\varnothing \neq \pi \subseteq \pi(m)$ such that $|h^{(\pi_0)}(s)|_v = |m|_v$ for all $v \in \pi$.*

Then $h(s)$ is irreducible in $\mathcal{R}$ if and only if $(h(s), h^{(\pi)}(s)) = 1$.

Proof. Note that $h^{(\pi)}(s) \neq h(s)$, since $|h^{(\pi_0)}(s)|_v = |m|_v$ implies that there exists $k \in \mathbb{N}$ such that v divides k and $a_k \neq 0$. Thus, if $h(s)$ is irreducible, then $(h(s), h^{(\pi)}(s)) = 1$.

Assume that $(h(s), h^{(\pi)}(s)) = 1$. Let $f(s)$ and $g(s)$ be two Dirichlet polynomials such that $f(s)g(s) = h(s)$. Since $h^{(\pi_0)}(s)$ is irreducible and $f^{(\pi_0)}(s)g^{(\pi_0)}(s) = h^{(\pi_0)}(s)$, we may assume that $f^{(\pi_0)}(s) = h^{(\pi_0)}(s)$ and $g^{(\pi_0)}(s) = 1$. Let $v \in \pi$. Note that $|f(s)|_v \geq |f^{(\pi_0)}(s)|_v = |h^{(\pi_0)}(s)|_v = |m|_v$. Since $|m|_v = |h(s)|_v = |f(s)|_v |g(s)|_v$, we have that $|g(s)|_v = 1$, thus $g^{(v)}(s) = g(s)$. It follows that $g^{(\pi)}(s) = g(s)$. This implies that $g(s)$ divides $h^{(\pi)}(s)$. Since $g(s)$ divides also $h(s)$, by $(h(s), h^{(\pi)}(s)) = 1$ we have that $g(s) = 1$. □

Chapter 3

The simple groups of Lie type

3.1 Notation

A simple group of Lie type G is the subgroup X^F of fixed point under a Frobenius map F of a connected reductive algebraic group X defined over an algebraically closed field of characteristic $p > 0$.

The simple groups of Lie type can be classified in several ways. For instance, they split into two classes: the Chevalley groups and the Twisted groups (see [Car72]). These groups are completely determined by a simple Lie Algebra $\mathfrak{L}$ over $\mathbb{C}$, a finite field $\mathbb{K}$ and a symmetry of the Dynkin diagram of $\mathfrak{L}$.

In general, for the groups of Lie type, we use the notation of [Car72]. The group is denoted by ${}^kL_l(t^k)$, where $k \in \{1, 2, 3\}$ (if $k = 1$, then k is omitted), L varies over the letters $A, ..., G$, l is the Lie rank of the Lie algebra and t^k is a power of a prime number p. In particular, the group ${}^kL_l(t^k)$ is defined over a the field $\mathbb{F}_{t^k}$ of characteristic p (so we allow t to be irrational). Finally, we set $q = t$, with the exception given in Table 3.1. In Table 3.1 we record the various names we use for the groups of Lie type.

Another way to classify the groups of Lie type is to divide them into classical and exceptional groups.

Table 3.1: Simple groups of Lie type

Lie notation	Other notation	Conditions
$A_n(t)$	$\mathrm{PSL}_{n+1}(q)$	$n \geq 1, (n,t) \neq (1,2), (1,3)$
${}^2A_n(t^2)$	$\mathrm{PSU}_{n+1}(q)$	$n \geq 2, (n,t) \neq (2,2)$
$B_n(t)$	$\mathrm{P}\Omega_{2n+1}(q)$	$n \geq 3, t$ odd
${}^2B_2(t^2)$		$q = t^2 = 2^{2k+1}, k \geq 1$
$C_n(t)$	$\mathrm{PSp}_{2n}(q)$	$n \geq 2, (n,t) \neq (2,2)$
$D_n(t)$	$\mathrm{P}\Omega^+_{2n}(q)$	$n \geq 4$
${}^2D_n(t^2)$	$\mathrm{P}\Omega^-_{2n}(q)$	$n \geq 4$
${}^3D_4(t^3)$		
$E_6(t)$		
${}^2E_6(t^2)$		
$E_7(t)$		
$E_8(t)$		
$F_4(t)$		$t \geq 3$
${}^2F_4(t^2)$		$q = t^2 = 2^{2k+1}, k \geq 1$
$G_2(t)$		$t \geq 3$
${}^2G_2(t^2)$		$q = t^2 = 3^{2k+1}, k \geq 1$

3.1.1 The classical groups

Let p be a prime number, let f be a positive integer and let q be the number p^f. Moreover let n be an integer greater than or equal to 2. Denote by V a vector space of dimension n over $\mathbb{F} = \mathbb{F}_{q^u}$ where $u \in \{1, 2\}$. As in [KL90, §2.1], let κ be a form defined over the vector space V over $\mathbb{F}_{q^u}$ and let $\mathbf{f}$ be the bilinear form associated to κ. We consider four cases :

V κ $\mathbf{f}$

$\mathbf{L}, \mathbf{S}, \mathbf{O}, \mathbf{U}$

- Case **L**: $\kappa = \mathbf{f}$ is identically 0.
- Case **S**: $\kappa = \mathbf{f}$ is a non-degenerate symplectic form.
- Case **O**: $\kappa = Q$ is a non-degenerate quadratic form; moreover $\mathbf{f}(v, w) = Q(v + w) - Q(v) - Q(w)$. Q
- Case **U**: $\kappa = \mathbf{f}$ is a non-degenerate unitary form.

The number u is defined as follows

$$u = \begin{cases} 2 & \text{if case } \mathbf{U} \text{ holds,} \\ 1 & \text{otherwise.} \end{cases}$$

Moreover, when case **O**, we distinguish three cases (see [KL90, p.27-28]):

$\mathbf{O}^o, \mathbf{O}^+, \mathbf{O}^-$

- Case $\mathbf{O}^o$, if n is odd (in this case q is odd);
- Case $\mathbf{O}^+$, if (V, Q) is of Witt defect 0;
- Case $\mathbf{O}^-$, if (V, Q) is of Witt defect 1.

Denote by $\Gamma(V, \kappa)$ the group of the κ-semisimilarity . Moreover, let $\Gamma(V, \kappa)$ $I(V, \kappa)$

$$I(V, \kappa) = \{\phi \in GL(V, \mathbb{F}) : \kappa(\phi(v)) = \kappa(v), \text{ for all } v \in V^l\},$$

where $l = 1$ if κ is quadratic, $l = 2$ otherwise. With a little abuse of notation, we denote by $\mathbb{F}^*$ the group of scalar linear transformations. If K is a subgroup of $\Gamma(V, \kappa)$, denote by $\overline{K}$ the reduction modulo $\mathbb{F}^* \cap K$. For example, $\overline{\Gamma}(V, \kappa)$ is the factor group $\overline{K}$

$\Gamma(V,\kappa)/\mathbb{F}^*$. Let $S(V,\kappa) = I(V,\kappa) \cap \mathrm{SL}(V,\mathbb{F})$ and let $\Omega(V,\kappa)$ be the derived subgroup of $S(V,\kappa)$. In particular, note that $\overline{\Omega}(V,\kappa) = \overline{S}(V,\kappa)$ unless case **O** holds (see [KL90, p.14]). It turns out that: $S(V,\kappa)$ $\Omega(V,\kappa)$

$$\overline{\Omega}(V,\kappa) \cong \begin{cases} \mathrm{PSL}_n(q) & \text{if case } \mathbf{L} \text{ holds,} \\ \mathrm{PSU}_n(q) & \text{if case } \mathbf{U} \text{ holds,} \\ \mathrm{PSp}_n(q) & \text{if case } \mathbf{S} \text{ holds,} \\ \mathrm{P\Omega}_n(q) & \text{if case } \mathbf{O}^\circ \text{ holds,} \\ \mathrm{P\Omega}_n^+(q) & \text{if case } \mathbf{O}^+ \text{ holds,} \\ \mathrm{P\Omega}_n^-(q) & \text{if case } \mathbf{O}^- \text{ holds.} \end{cases}$$

$A(V,\kappa)$ Finally, define

$$A(V,\kappa) = \begin{cases} \Gamma(V,\kappa)\langle\iota\rangle & \text{in case } \mathbf{L} \text{ with } n \geq 3, \\ \Gamma(V,\kappa) & \text{otherwise.} \end{cases}$$

where ι is an inverse transpose automorphism (see [KL90, (2.2.4)]) of the group $S(V,\kappa) \cong \mathrm{SL}(V)$ when case **L** holds.

We recall the following.

Theorem 3.1 ([KL90, Theorem 2.1.4])**.** *Assume that $n \geq 2, 3, 4, 7$ in cases $\mathbf{L}, \mathbf{U}, \mathbf{S}$ and $\mathbf{O}$ respectively. If $\overline{\Omega}(V,\kappa)$ is non-abelian simple, then $\mathrm{Aut}(\overline{\Omega}(V,\kappa)) \cong \overline{\Gamma}(V,\kappa)$, except when one of the following holds:*

- *Case $\mathbf{L}$ and $n \geq 3$. In this case $\mathrm{Aut}(\overline{\Omega}(V,\kappa))$ has a subgroup of index 2 isomorphic to $\overline{\Gamma}$.*
- *Case $\mathbf{O}^+$ and $n = 8$.*
- *Case $\mathbf{S}$, $n = 4$ and q even.*

Following [KL90], we say that a group X is a *classical projective group* if

$$\overline{\Omega}(V,\kappa) \leq X \leq \overline{A}(V,\kappa)$$

for some V and κ as above.

When V and κ are clear from the contest, we omit them. For example, we shall write $\overline{\Gamma}$ instead of $\overline{\Gamma}(V,\kappa)$.

3.1.2 Lie algebras, system of roots and Dynkin diagrams

Let p be a prime number. Let $\mathbb{K}$ be a field of characteristic p. We denote by G a group of Lie type over the field $\mathbb{K}$. We have that G is either an untwisted or a twisted group of Lie type. In both cases, a simple Lie algebra $\mathfrak{L}$ over the field $\mathbb{K}$ is associated to G.

If G is an untwisted group of Lie type, then G is a Chevalley group $\mathfrak{L}(\mathbb{K})$, which is a certain group of automorphisms of $\mathfrak{L}$ over the field $\mathbb{K}$ (see [Car72, Proposition 4.4.3]).

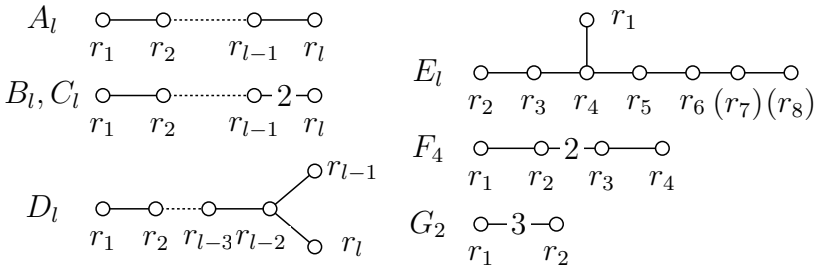
If G is a twisted group of Lie type, then G is a subgroup of a Chevalley group $\mathfrak{L}(\mathbb{K})$.

Now, let G be our group of Lie type. The following objects are associated to G.

- A Killing form $(-,-)$ on the simple Lie algebra $\mathfrak{L}$ over the field $\mathbb{K}$. $(-,-)$ $\mathfrak{L}$
- A system of roots Φ in a Cartan subalgebra $\mathfrak{V}$ of $\mathfrak{L}$ and a system of fundamental roots Π in Φ. Φ $\mathfrak{V}$ Π
- A Dynkin diagram $\mathfrak{D}$, that is a graph with elements of Π as vertices, such that $r \in \Pi$ and $s \in \Pi$ are joined by a bond of strength $\frac{4(r,s)^2}{(r,r)(s,s)}$ (see [Car72, §3.4]). $\mathfrak{D}$
- A symmetry ρ of the Dynkin diagram of $\mathfrak{L}$ (see [Car72, §13.1]). In particular the order of ρ is 1, 2 or 3 (see [Car72, §13.4]). ρ

In Figure 3.1, we report the Dynkin diagrams of a simple Lie algebra.

Figure 3.1: Dynkin diagrams



Now, we give some other definitions and remarks on the root systems.

Ψ^+, Ψ^-

- Given a system of roots Ψ and a fundamental system Σ in Ψ, let Ψ^+, Ψ^- be the sets of positive and negative roots with respect to the fundamental system Σ. We recall that a root in $r \in \Psi$ is a linear combination of roots of Σ with integer coefficients which are all non-negative if $r \in \Psi^+$ and all non-positive if $r \in \Psi^-$ (see [Car72, §2.1]).

w_r

- The vector space $\mathfrak{V}$ is spanned by Π in $\mathfrak{L}$. Let $r \in \mathfrak{V}$; a linear map $w_r : \mathfrak{V} \to \mathfrak{V}$, defined by
$$w_r(x) = x - \frac{2(r,x)}{(r,r)}r,$$
W is called a reflection. The Weyl group W of Φ is the subgroup of transformations of $\mathfrak{V}$ generated by the reflections $\{w_r : r \in \Phi\}$. Note that W is generated also by the so-called fundamental reflections $\{w_r : r \in \Pi\}$ (see [Car72, Proposition 2.1.8]). Let $l(w)$ be the length of $w \in W$, defined as the minimal n such that $w = w_{r_1}...w_{r_n}$ for $r_i \in \Pi, i \in \{1, ..., n\}$. Thus $l(1) = 0$. Moreover, $l(w) = |\Phi^+ \cap w^{-1}(\Phi^-)|$ (see [Car72, Theorem 2.2.2]).

$l(w)$

$\mathfrak{V}_K$ Φ_K

- For a subset K of Π, let $\mathfrak{V}_K$ be the subspace of $\mathfrak{V}$ spanned by K. Let $\Phi_K = \Phi \cap \mathfrak{V}_K$ and let W_K be the subgroup of W generated by the reflections $\{w_r : r \in \Phi_K\}$. Note that Φ_K is a system of roots in $\mathfrak{V}_K$, K is a fundamental system and the Weyl group of Φ_K is W_K ([Car72, Proposition 2.5.1]).

W_K

τ

- An isometry τ of $\mathfrak{V}$ is associated to the symmetry ρ in such a way that $\tau(r)$ is a positive multiple of $\rho(r)$ for each $r \in \Pi$ (see [Car72, §13.1]). The isometry τ is uniquely determined by ρ. In particular, observe that for every $w \in W$, the element $w^\tau = \tau^{-1}w\tau$ belongs to W. Finally, note that ρ and τ are non-trivial if and only if G is twisted.

I

- Let k be the number of the ρ-orbits of Π. Let $I = \{O_1, ..., O_k\}$ denote the set of ρ-orbits of Π. For each $J \subseteq I$, let $J^* = \cup_{K \in J} K$.

J^*

$\mathcal{W}$

- Let $\mathcal{W}$ denote the subgroup of the Weyl group W consisting of the $w \in W$ such that $w^\tau = w$ (see [Car72, §13.1]). For a subset J of I, let $\mathcal{W}_J = W_{J^*} \cap \mathcal{W}$. In particular, if $J = \{O_i\}$ for some $i \in \{1, ..., k\}$, then let $W_i = W_{J^*} = W_{O_i}$, $\mathcal{W}_i = \mathcal{W}_{J^*} = \mathcal{W}_{O_i}$ and $\Phi_i = \Phi_{J^*} = \Phi_{O_i}$. $\mathcal{W}_J$ W_i $\mathcal{W}_i$ Φ_i

- Let $\mathfrak{D}'$ be the Dynkin diagram of $\mathcal{W}$, that is a graph induced by the Dynkin diagram $\mathfrak{D}$, identifying the nodes in the same ρ-orbit (see [Car72, 13.3.8]). $\mathfrak{D}'$ is a graph with as nodes the elements of I, such that $K_1 \in I$ and $K_2 \in I$ are joined if there exists $r_1 \in K_1$ and $r_2 \in K_2$ such that r_1 and r_2 are joined in $\mathfrak{D}$. $\mathfrak{D}'$

- Let K be a subset of Π. We define D_K to be the set of elements w of W such that $w(r) \in \Phi^+$ for each $r \in K$. For a subset J of I, let $\mathcal{D}_J = D_{J^*} \cap \mathcal{W}$. D_K $\mathcal{D}_J$

- For $J \subseteq I$, let $T_{\mathcal{W}_J}(t)$

$$T_{\mathcal{W}_J}(t) = \sum_{w \in \mathcal{W}_J} t^{l(w)}.$$

3.2 The parabolic subgroups of a simple group of Lie type

Let G be a simple group of Lie type defined over a field of characteristic p. Denote by B a Borel subgroup of G. A *parabolic subgroup of* G is a subgroup of G containing a Borel subgroup. B

The parabolic subgroups are crucial in our study since they are the subgroups of G that contain a Sylow p-subgroup and that are intersection of maximal subgroups.

Lemma 3.2 ([DL06, Lemma 2])**.** *Let G be a simple group of Lie type of characteristic p. Let B be the Borel subgroup of G. We have that*

$$P_G^{(p)}(s) = \sum_{B \leq P \leq G} \frac{\mu_G(P)}{|G : P|^{s-1}}.$$

A large part of our study is focused on the analysis of the polynomial $P_G^{(p)}(s)$. Indeed, we know a big amount of informations on it, as we will see below.

There is a deep connection between the system of roots and the parabolic subgroups, as shown in the following proposition.

Proposition 3.3 ([Car72, Theorem 8.3.4, Section 8.6, Section 14.1])**.** *Let G be a simple group of Lie type over $\mathbb{K}$ and let B be a Borel subgroup of G. Assume that I is the set of ρ-orbits of Π. Let $\mathcal{S}_B(G) = \{H \leq G : H \geq B\}$. There is a bijection*

P_J

$$\begin{array}{rccc} \Theta: & \mathcal{P}(I) & \to & \mathcal{S}_B(G) \\ & J & \mapsto & P_J \end{array}$$

such that:

(1) $P_J \cap P_K = P_{J\cap K}$ for $J, K \subseteq I$ (so the map is a lattice isomorphism);

(2) $P_\varnothing = B$ and $P_I = G$;

(3) $\frac{|P_J|}{|P_I|} = T_{\mathcal{W}_J}(t)$, where $t = \sqrt[|\rho|]{|\mathbb{K}|}$.

Hence, combining Lemma 3.2 and Proposition 3.3, we have the following.

Proposition 3.4 (See [DL06, Theorem 3])**.** *Let G be a simple group of Lie type of characteristic p. We have that*

$$P_G^{(p)}(s) = (-1)^{|I|}\sum_{J\subseteq I}(-1)^{|J|}|S:P_J|^{1-s} = (-1)^{|I|}\sum_{J\subseteq I}(-1)^{|J|}\left(\frac{T_{\mathcal{W}_I}(t)}{T_{\mathcal{W}_J}(t)}\right)^{1-s}.$$

As we have seen in the previous subsection, the expression $T_{\mathcal{W}_J}(t)$ depends on the elements of J. However, there is another way to express $T_{\mathcal{W}_J}(t)$, as we will see below.

Let $t = \sqrt[|\rho|]{|\mathbb{K}|}$, where G is defined over the field $\mathbb{K}$. Recall that $\mathfrak{D}$ is the Dynkin diagram of the Lie algebra associated to G and $\mathfrak{D}'$ the Dynkin diagram induced by the action of ρ. Denote by $F_{\mathfrak{D}'}(t)$ the polynomial

$F_{\mathfrak{D}'}(t)$

$$\prod_{i=1}^{l}\frac{1-\epsilon_i t^{m_i+1}}{1-\epsilon_i t},$$

where m_i and ϵ_i are given in Table 3.2 (see [Car72, Proposition 10.2.5, Theorem 14.3.1]). By [Car72, Theorem 10.2.3, Theorem 14.2.1], we have that $T_{W_I}(t) = F_{\mathfrak{D}'}(t)$ if I is the set or ρ-orbits of Π associated to G.

Table 3.2: m_i and ϵ_i.

$\mathfrak{D}$	$m_1, ..., m_l$	$\mathfrak{D}'$	$\epsilon_1, ..., \epsilon_l$
A_l	$1, ..., l$	$\mathfrak{D}$	$1, ..., 1$
B_l, C_l	$1, 3, 5, ..., 2l-1$	${}^2A_l$	$1, -1, 1, ..., (-1)^{l+1}$
D_l	$1, 3, 5, ..., 2l-3, l-1$	${}^2B_2$	$1, -1$
E_6	$1, 4, 5, 7, 8, 11$	${}^2D_l$	$1, 1, ..., 1, -1$
E_7	$1, 5, 6, 9, 11, 13, 17$	${}^3D_4$	$1, 1, \omega, \omega^2$
E_8	$1, 7, 11, 13, 17, 19, 23, 29$	${}^2E_6$	$1, -1, 1, 1, -1, 1$
F_4	$1, 5, 7, 11$	${}^2F_4$	$1, 1, -1, -1$
G_2	$1, 5$	${}^2G_2$	$1, -1$

In Table 3.2, we set $\omega = e^{\frac{2\pi i}{3}}$. In particular, note that $\mathfrak{D} = \mathfrak{D}'$ if and only if S is untwisted. In this case, the ϵ_i's are all 1.

Suppose that $J \subseteq I$. Denote by J^* the set $\bigcup_{K \in J} K$. For $K \subseteq \Pi$, let $\mathfrak{D}_K$ be the subdiagram of $\mathfrak{D}$ corresponding to the set of roots K. Let $\mathfrak{D}'_J$ be the subdiagram of $\mathfrak{D}'$ corresponding to the set of nodes J. Let $\mathfrak{D}'_{J_1}, ..., \mathfrak{D}'_{J_k}$ be the connected components of $\mathfrak{D}'_J$. Clearly we have that $J = \bigcup_{i=1}^{k} J_i$ and the union is disjoint. Since J^* is a subset of Π, we have that $\mathfrak{D}_{J^*}$ is a subdiagram of $\mathfrak{D}$.

Suppose that $\mathfrak{D}'_J$ is connected. Then just one of the following holds:

- $\mathfrak{D}_{J^*}$ is connected and $\mathfrak{D}'_J$ is the Dynkin diagram $\mathfrak{D}''$ of a simple group of Lie type which is untwisted if and only if $\mathfrak{D}_{J^*}$ and $\mathfrak{D}'_J$ are isomorphic graphs. In this case define $F_{\mathfrak{D}'_J}(t) = F_{\mathfrak{D}''}(t)$.

- $\mathfrak{D}_{J^*}$ is not connected, it has $|\rho|$ components and each of its connected components is isomorphic to the Dynkin diagram $\mathfrak{D}''$ of an untwisted group. In this case define $F_{\mathfrak{D}'_J}(t) = F_{\mathfrak{D}''}(t^{|\rho|})$.

We are ready to state the following.

Proposition 3.5 (See [Car72, Theorem 10.2.3, Theorem 14.2.1]). *Under the above*

setting, for a subset J of I we have:

$$T_{\mathcal{W}_J}(t) = \prod_{i=1}^{k} F_{\mathfrak{D}'_{J_i}}(t).$$

EXAMPLE 1. Let $G = {}^2A_3(t^2)$. The Dynkin diagram $\mathfrak{D}$ of G is A_3 and $I = \{\{r_1, r_3\}, \{r_2\}\}$ (we refer to Figure 3.1).

- Since $\mathfrak{D}' = {}^2A_3$, we have
$$F_{\mathfrak{D}'}(t) = F_{{}^2A_3}(t) = \frac{1-t^2}{1-t}\frac{1+t^3}{1+t}\frac{1-t^4}{1-t} = (1+t)^2(1-t+t^2)(1+t^2).$$
- Let $J_1 = \{\{r_1, r_3\}\}$. Clearly, $\mathfrak{D}'_{J_1}$ is connected and the diagram $\mathfrak{D}'_{J_1^*}$ has 2 connected components isomorphic to A_1. So $F_{D'_{J_1}}(t) = F_{A_1}(t^2) = 1 + t^2$.
- Now, let $J_2 = \{\{r_2\}\}$. Clearly, $\mathcal{D}_{J_2^*}$ is the Dynkin diagram A_1. So $F_{D'_{J_2}}(t) = F_{A_1}(t) = 1 + t$.

By Proposition 3.4, we have:

$$P_G^{(p)}(s) = 1 - \big((1+t)^2(1-t+t^2)\big)^{1-s} - \big((1+t)(1+t^2)(1-t+t^2)\big)^{1-s} + \big((1+t)^2(1+t^2)(1-t+t^2)\big)^{1-s}.$$

3.2.1 The parabolic subgroups of an almost simple group of Lie type

Now we consider a more general setting. Let X be an almost simple group with socle S isomorphic to a simple group of Lie type.

Our aim is to give an explicit formula for $P_{X,S}^{(p)}(s)$. Note that we can generalize Lemma 3.2 in the following way.

Lemma 3.6. *Let r be a prime number, let G be a finite group and let N be a normal subgroup of G. Let R be a Sylow r-subgroup of G. Suppose that if M is maximal subgroup of G such that $MN = G$ and $R \leq M$, then M contains also $N_G(R)$. We have that*

$$P_{G,N}^{(r)}(s) = \sum_{\substack{R \leq H \leq G,\\ HN = G}} \frac{\mu_G(H)}{|G:H|^{s-1}}.$$

Proof. The proof is the same as in [DL06, Lemma 2], considering just the subgroups H such that $HN = G$. □

Let P be a Sylow p-subgroup of X. Thus $P \cap S$ is a Sylow p-subgroup of S and $B = N_S(P \cap S)$ is a Borel subgroup in S. Given a subgroup K of X, denote by $\mathcal{S}_K(X)$ the set of subgroups H of X such that $H \geq K$. $\mathcal{S}_K(X)$

Lemma 3.7 ([Car72, Theorem 8.3.3])**.** *Let H be a subgroup of S such that $H \geq B$. Then $N_S(H) = H$.*

Lemma 3.8. *Let P and B as above. We have that:*

(1) $N_X(B) = N_X(P \cap S)$ and $N_X(B)S = X$;

(2) if M is a maximal subgroup of X such that $M \geq P$ and $MS = X$, then $M \geq N_X(B)$.

Proof. Well known, see [KL90]. □

The last lemma implies that $\mathcal{S}_{N_X(B)}(X) = \{H \leq X : H \geq N_X(B), HS = X\}$. We say that the elements of the set $\mathcal{S}_{N_X(B)}(X)$ are the *parabolic subgroup of X over $N_X(B)$*. A *parabolic subgroup of X* is an element of $\mathcal{S}_{N_X(B)}(X)$ for some Borel subgroup B of S.

Since $P \cap S \trianglelefteq P$, we have that Lemma 3.8(1) implies that $N_X(P) \leq N_X(B)$. Hence, by Lemma 3.8(2) and Lemma 3.6 we get that

$$P^{(p)}_{X,S}(s) = \sum_{\substack{P \leq H \leq X,\\ HS = X}} \frac{\mu_X(H)}{|X:H|^{s-1}} = \sum_{H \in \mathcal{S}_{N_X(B)}(X)} \frac{\mu_X(H)}{|X:H|^{s-1}},$$

observing that if $P \leq H < N_X(B)$, then H is not an intersection of maximal subgroups (by Lemma 3.8(2)), hence $\mu_X(H) = 0$ by Proposition 2.1(1).

Now we want to give a better description of the elements of the set $\mathcal{S}_{N_X(B)}(X)$. Let $\mathcal{S}^X_B(S)$ denote the subset of $\mathcal{S}_B(S) = \{H \leq S : H \geq B\}$ given by $\mathcal{S}^X_B(S)$

$$\{H \in \mathcal{S}_B(S) : N_X(H) \geq N_X(B)\}.$$

We have the following.

Proposition 3.9. *The map $\eta : \mathcal{S}_{N_X(B)}(X) \to \mathcal{S}_B^X(S)$ given by $\eta(H) = H \cap S$ is well-defined. Moreover η is an isomorphism of posets, in particular $N_X(\eta(H)) = H$ for each $H \in \mathcal{S}_{N_X(B)}(X)$.*

Proof. We show that η is well defined. Let $H \in \mathcal{S}_{N_X(B)}(X)$. Clearly $H \cap S \geq N_X(B) \cap S = N_S(B) = B$. Since $H \cap S \trianglelefteq H$, we have that $N_X(H \cap S) \geq H \geq N_X(B)$. Hence $H \cap S \in \mathcal{S}_B^X(S)$.

We claim that η is surjective. Let $K \in \mathcal{S}_B^X(S)$. By definition $N_X(K) \geq N_X(B)$, so $N_X(K) \in \mathcal{S}_{N_X(B)}(X)$. Finally $\eta(N_X(K)) = N_X(K) \cap S = N_S(K) = K$ by Lemma 3.7.

We claim that η is injective. It is enough to prove that $N_X(\eta(H)) = H$ for each $H \in \mathcal{S}_{N_X(B)}(X)$. As above, we have that $N_X(H \cap S) \geq H$. Since $HS = X$, using Lemma 3.7, we get

$$|X : N_X(H \cap S)| = |S : N_X(H \cap S) \cap S| = |S : N_S(H \cap S)| = |S : H \cap S| = |X : H|,$$

thus $N_X(H \cap S) = H$.

Clearly the map η is an isomorphism of posets. □

Recall from Proposition 3.3, that the map:

$$\begin{array}{rccc} \Theta : & \mathcal{P}(I) & \to & \mathcal{S}_B(S) \\ & J & \mapsto & P_J \end{array}$$

is an isomorphism of lattices. Since that $N_X(B)$ acts by conjugation on $\mathcal{S}_B(S)$, in view the isomorphism Θ, the group $N_X(B)$ acts on $\mathcal{P}(I)$. In particular, the action is the following: if $J \subseteq I$ and $g \in N_X(B)$, then J^g is the unique subset of I such that $P_{J^g} = P_J^g$. Moreover, the group $N_X(B)$ acts on I: if $O \in I$ is a ρ-orbit, then $\{O^g\} = \{O\}^g$. Note that if S is twisted, then the action of $N_X(B)$ is trivial. Assume that S is untwisted. The action of $N_X(B)$ on I can be thought as an action of $N_X(B)$ on Π. So, any element g of $N_X(B)$ induces a symmetry ψ_g of the Dynkin diagram $\mathcal{D}$ of S. Since $X = SN_X(B)$, if $h \in X$, then $h = sg$ for some $s \in S$ and $g \in N_X(B)$. If ψ_g is not trivial, then we say that h is a *non-trivial graph automorphism of order*

$|\psi_g|$ in X (the definition does not depend on the choice of g, since the action does not depend on the choice of g).

Observe that $\mathcal{S}_B^X(S)$ is the set of fixed points of $\mathcal{S}_B(S)$ under the action of $N_X(B)$.

If X does not contain non-trivial graph automorphisms, then ψ_g is the trivial symmetry for each $g \in N_X(B)$. In this case, we have $\mathcal{S}_B^X(S) = \mathcal{S}_B(S)$.

If X contains a non-trivial graph automorphism, then S is untwisted and ρ is trivial.

Let $\mathcal{P}^X(I)$ be the subposet of $\mathcal{P}(I)$ consisting of the subsets of I which are union of $N_X(B)$-orbits of elements of I. Clearly $\mathcal{P}^X(I)$ is the set of fixed point of $\mathcal{P}(I)$ under the action of $N_X(B)$. The map Θ restricts to an isomorphism of posets between $\mathcal{P}^X(I)$ and $\mathcal{S}_B^X(S)$. Moreover, if $J \in \mathcal{P}^X(I)$, then let $\tilde{J}$ be the set of $N_X(B)$-orbits of J and denote by $o(J)$ the size of $\tilde{J}$. $\mathcal{P}^X(I)$ $\tilde{J}$ $o(J)$

Now we can prove the following generalization of Proposition 3.4 (see also [DL06, Theorem 3]).

Theorem 3.10. *Let X and S be as above. Then*

$$P_{X,S}^{(p)}(s) = (-1)^{o(I)} \sum_{J \in \mathcal{P}^X(I)} (-1)^{o(J)} |S : P_J|^{1-s} = (-1)^{o(I)} \sum_{J \in \mathcal{P}^X(I)} (-1)^{o(J)} \left(\frac{T_{\mathcal{W}_I}(t)}{T_{\mathcal{W}_J}(t)} \right)^{1-s}.$$

In particular, if X does not contain non-trivial graph automorphisms, then $P_{X,S}^{(p)}(s) = P_S^{(p)}(s)$.

Proof. By the above consideration, we obtain an isomorphism of posets $\tilde{\eta} : \mathcal{P}^X(I) \to \mathcal{S}_{N_X(B)}(X)$, given by $\tilde{\eta}(J) = N_X(P_J)$ for $J \in \mathcal{P}^X(I)$. In particular, we get $\mu_{\mathcal{P}^X(I)}(J) = \mu_X(N_X(P_J))$. Note that $\mu_{\mathcal{P}^X(I)}(J) = (-1)^{o(I)-o(J)}$. Indeed there is an isomorphism between the poset $\mathcal{P}^X(I)$ and the poset $\mathcal{P}(\tilde{I})$ of subsets of $\tilde{I}$, given by $J \mapsto \tilde{J}$. Thus $\mu_{\mathcal{P}^X(I)}(J) = \mu_{\mathcal{P}(\tilde{I})}(\tilde{J})$, and by [Sta97, 3.8.3], we get $\mu_{\mathcal{P}(\tilde{I})}(\tilde{J}) = (-1)^{o(I)-o(J)}$.

Since $N_X(P_J) \cap S = P_J$, we have that $|X : N_X(P_J)| = |S : P_J|$. By Lemma 3.6

and Lemma 3.8, we obtain:

$$\begin{aligned} P^{(p)}_{X,S}(s) &= \sum_{H\in\mathcal{S}_{N_X(B)}(X)} \frac{\mu_X(H)}{|X:H|^{s-1}} = \sum_{J\in\mathcal{P}^X(I)} \frac{\mu_X(N_X(P_J))}{|X:N_X(P_J)|^{s-1}} = \\ &= \sum_{J\in\mathcal{P}^X(I)} (-1)^{o(I)-o(J)}|S:P_J|^{1-s} = (-1)^{o(I)} \sum_{J\in\mathcal{P}^X(I)} (-1)^{o(J)}|S:P_J|^{1-s}. \end{aligned}$$

Apply Proposition 3.3 and the proof is complete. □

Now, we give an example of explicit computation of $P^{(p)}_{X,S}(s)$ (when we speak about Dynkin diagram, we refer to Figure 3.1).

EXAMPLE 2. Let X be an almost simple group with socle $S \cong A_3(t)$ and suppose that X contains a non-trivial graph automorphism. Here, the Dynkin diagram $\mathfrak{D} = \mathfrak{D}'$ is A_3, hence $I = \{\{r_1\},\{r_2\},\{r_3\}\}$. Since X contains a non-trivial automorphism, the set of $N_X(B)$-orbits of I is $\tilde{I} = \{\{\{r_1\},\{r_3\}\},\{\{r_2\}\}\}$.

- We have $F_{\mathfrak{D}'}(t) = F_{A_3}(t) = \frac{1-t^2}{1-t}\frac{1-t^3}{1-t}\frac{1-t^4}{1-t} = (1+t)^2(1+t+t^2)(1+t^2)$.
- Let $J_1 = \{\{r_1\},\{r_3\}\}$. The diagram $\mathfrak{D}_{J_1^*} = \mathfrak{D}_{\{r_1,r_3\}}$ has 2 connected components isomorphic to A_1. So $F_{\mathfrak{D}_{J_1}}(t) = F_{A_1}(t)^2 = (1+t)^2$.
- Now, let $J_2 = \{\{r_2\}\}$. Clearly, $\mathfrak{D}_{J_2^*}$ is the Dynkin diagram A_1. So $F_{\mathfrak{D}_{J_2}}(t) = F_{A_1}(t) = 1+t$.

By Theorem 3.10, we have:

$$P^{(p)}_{X,S}(s) = 1-\big((1+t^2)(1+t+t^2)\big)^{1-s}-\big((1+t)(1+t^2)(1+t+t^2)\big)^{1-s}+\big((1+t)^2(1+t^2)(1+t+t^2)\big)^{1-s}.$$

3.3 Maximal subgroups of a simple group of Lie type

3.3.1 Classical groups

Let X be an almost simple group with socle G a classical simple group. We assume that if $G \cong \mathrm{P}\Omega_8(q)$, then X does not contain graph automorphisms of order 3 and if $G \cong \mathrm{PSp}_4(q)$ is symplectic, then X does not contain graph automorphisms.

In this section we deal with the maximal subgroups M of X such that $MG = X$ and M does not contain a Sylow p-subgroup of X. By [KL90], the group $M \cap G$ is a member of one of the classes of geometric subgroups $\mathcal{C}_1, ..., \mathcal{C}_8$ or of the class $\mathcal{S}$ (see [KL90] for the notation). In [KL90], Kleidman and Liebeck showed the structure of the geometric maximal subgroup. We use the notation of [KL90]. In particular, we use its description of the collections $\mathcal{C}_i$ of the maximal subgroups of a classical group G. So, when we say that a subgroup M has a certain type in a certain class, we are referring to [KL90, Table 3.5.A-F].

$\mathcal{C}_1, ..., \mathcal{C}_8$
$\mathcal{S}$

Now we state a crucial theorem, due to Aschbacher, on the maximal subgroups of the classical groups.

Theorem 3.11 (see [Asc84], [KL90])**.** *Let G be a classical simple group. A maximal subgroups of G either lies in $\mathcal{C}_1 - \mathcal{C}_8$ or in the class $\mathcal{S}$. A subgroup H of G lies in $\mathcal{S}$ if and only if the following hold.*

a. *The socle S of H is a non-abelian simple group.*

b. *If L is the full covering group of S, and if $\rho : L \to \mathrm{GL}(V)$ is a representation of L such that $\overline{\rho(L)} = S$ (where $^-$ denotes the reduction modulo scalars), then ρ is absolutely irreducible.*

c. *$\rho(L)$ cannot be realized over a proper subfield of $\mathbb{F}$.*

d. *If $\rho(L)$ fixes a non-degenerate quadratic form on V, then $G \in \{\mathrm{P}\Omega_n(q), \mathrm{P}\Omega_n^+(q), \mathrm{P}\Omega_n^-(q)\}$.*

e. *If $\rho(L)$ fixes a non-degenerate symplectic form on V, but no non-degenerate quadratic form, then $G = \mathrm{PSp}_n(q)$.*

f. *If $\rho(L)$ fixes a non-degenerate unitary form on V, then $G = \mathrm{PSU}_n(q)$.*

g. *If $\rho(L)$ does not satisfy the conditions in (d), (e) of (f), then $G = \mathrm{PSL}_n(q)$.*

We say that a maximal subgroups of a classical group G is a *geometric maximal subgroup* if it lies in one of the class $\mathcal{C}_1 - \mathcal{C}_8$.

An interesting result on the elements of the class $\mathcal{S}$ is the following.

Theorem 3.12 ([LPS90, p.32])**.** *Let H be a member of $\mathcal{S}$ and let S be the socle of H. Then one of the following holds:*

- $|H| < q^{2n+4}$ *if G is not unitary,* $|H| < q^{4n+8}$ *if G is unitary;*
- $S \cong \mathrm{Alt}_c$ *for* $c \in \{n+1, n+2\}$.
- *S and G are in Table 3.3.*

Table 3.3: Class $\mathcal{S}$, some groups

S	G
$\mathrm{PSL}_d(q)$	$\mathrm{PSL}_{\frac{d(d-1)}{2}}(q)$
$\mathrm{P\Omega}^+_{10}(q)$	$\mathrm{PSL}_{16}(q)$
$\mathrm{E}_6(q)$	$\mathrm{PSL}_{27}(q)$
M_{24}	$\mathrm{PSL}_{11}(2)$
$\mathrm{E}_7(q)$	$\mathrm{PSp}_{56}(q), q$ *odd*
$\mathrm{P\Omega}_7(q)$	$\mathrm{P\Omega}^+_8(q)$
$\mathrm{P\Omega}_9(q)$	$\mathrm{P\Omega}^+_{16}(q)$
$\mathrm{E}_7(q)$	$\mathrm{P\Omega}^+_{56}(q), q$ *even*
Co_1	$\mathrm{P\Omega}^+_{24}(2)$

As reported in Table 3.4, for some groups of small Lie rank, the class $\mathcal{S}$ is completely determined or we can make a restriction on the possible members of this class.

Moreover, by [KL82, Theorem 5.7], we have that if H is a maximal subgroup in the class $\mathcal{S}$ of $\mathrm{PSU}_4(q)$, then $\mathrm{soc}(H)$ is $\mathrm{Alt}_7, \mathrm{PSL}_2(7), \mathrm{PSp}_4(3)$ or $\mathrm{PSL}_3(4)$.

Recall the notation for $\hat{q}_e$ and $\hat{q}^*_e$. Let d be the dimension of the vector space associated to a classical group G (not unitary) defined over a field $\mathbb{F}_q$ (for example,

Table 3.4: Subgroups that (possibly) lie in the Class $\mathcal{S}$ for some groups of low Lie rank

G	H	Conditions	Reference
$\mathrm{PSL}_2(q)$	Alt_5	if $p \equiv \pm 1 \pmod 5$, then $q = p$, otherwise $q = p^2 \notin \{4, 25\}$	[Hup67]
$\mathrm{PSL}_3(q)$	$\mathrm{PSL}_2(7)$	$p \notin \{2, 7\}$; if $p^3 \equiv 1 \pmod 7$, then $q = p$, otherwise $q = p^2 \geq 25$	[Mit11], [Har26]
	Alt_6	if $p \equiv 1, 4 \pmod{15}$, then $q = p$, otherwise $q = p^2 \neq 9$	
	$\mathrm{Alt}_6.2$	$q = 25$	
	Alt_7	$q = 25$	
$\mathrm{PSL}_4(q), q$ even	Alt_7	$q = 2$	[Mwe76]
$\mathrm{PSL}_5(2)$			[CCN+85]
$\mathrm{PSU}_3(q)$	$\mathrm{PSL}_2(7)$	$p^3 \equiv -1 \pmod 7$ and $q = p \neq 5$	[Mit11], [Har26]
	Alt_6	$q = p \equiv 11, 14 \pmod{15}$	
	$\mathrm{Alt}_6.2$	$q = 5$	
	Alt_7	$q = 5$	
$\mathrm{PSp}_4(q), q$ odd	$\mathrm{PSL}_2(q)$	$p \geq 5$ and $q \geq 7$	[Mit14]
	Alt_6	$q = p \equiv \pm 5 \pmod{12}, q \neq 7$	
	$\mathrm{Alt}_6.2$	$q = p \equiv \pm 1 \pmod{12}$	

if $G = \mathrm{PSp}_{2n}(q)$, then $d = 2n$). Let e be as in Table 3.6-3.7. By [GPPS99, Example 2.6-2.9] we have that if H is a subgroup in the class $\mathcal{S}$ of G and $(\hat{q}_e^*, |G : H|) = 1$, then $S = \mathrm{soc}(H)$ appears in the last column of the Table 3.6-3.7. For example, let $G = \mathrm{P}\Omega_7(3)$ and $e = 4$. In this case $d = 7$. The socle of a maximal subgroup H in the class $\mathcal{S}$ of G, such that $\hat{3}_4^* = 5$ does not divide $|G : H|$, is Alt_8, Alt_9 or $\mathrm{PSp}_6(2)$.

Now, let us consider the group $G = \mathrm{PSU}_n(q)$, defined over the field $\mathbb{F}_{q^2}$. Let $d = n$ and let e be as in Table 3.8. By [GPPS99, Example 2.6-2.9] we have that if H is a subgroup in the class $\mathcal{S}$ of G and $(\hat{q}_e^*, |G : H|) = 1$, then $S = \mathrm{soc}(H)$ appears in the last column of the Table 3.8.

In Table 3.9-3.14 we report the maximal geometric subgroups H of G such that $(\hat{q}_e^*, |G : H|) = 1$, using the notation of [KL90] for the type and the class.

Recall the definition of the class $\mathcal{S}$. In particular, if M lies in $\mathcal{S}$, then there exists an absolutely irreducible representation $\rho : L \to \mathrm{GL}(V)$ such that $\overline{\rho(L)} = S$, where L is the full covering of S.

As in [KL90, §5.3], for a finite group S and a prime number r, let $R_r(S) = \min\{m : L \text{ has a nontrivial projective representation of degree } m \text{ in characteristic } r\}$. Moreover, let $R_{p'}(S) = \min\{R_r(S) : r \text{ is a prime number}, r \neq p\}$ and $R(S) = \min\{R_r(S) : r \text{ is a prime number}\}$. In particular, we are concerned with the simple groups S such that $R(S) \leq 12$. We report these groups in Table 3.15, 3.16 and 3.17, using [KL90, Proposition 5.3.7, Proposition 5.3.8, Theorem 5.3.9 and Proposition 5.4.13].

Assume that S is a group of Lie type of characteristic p over $\mathbb{F}_r$. Let $\overline{\mathbb{F}_p}$ denote the algebraic closure of $\mathbb{F}_p$. Since ρ is absolutely irreducible, we can think to V as an irreducible projective $\overline{\mathbb{F}_p}S$-module. Moreover, by definition of the class $\mathcal{S}$, we have that V cannot be realized over a proper subfield of $\mathbb{F}$. Under these assumptions, by [KL90, Proposition 5.4.6 and Remark 5.4.7], there exist an integer k and an irreducible projective $\overline{\mathbb{F}_p}S$-module of dimension t such that one of the following holds:

- $r = q^{uk}$ and $\dim(V) = n = t^k$;
- S is of type ${}^2A_l, {}^2D_2, {}^2E_6$, $r = q^{uk/2}$, k is odd and $n = t^k$;

- S is of type ${}^3D_4$, $r = q^{uk/3}$, $3 \nmid k$ and $n = t^k$;
- S is of type ${}^2B_2, {}^2G_2, {}^2F_4$, $r = q^{uk}$ and $n \geq t^k$.

In Table 3.18 we report the possibilities for S when $t \leq 12$.

3.3.2 Exceptional groups

Let X be an almost simple group with a socle S isomorphic to an exceptional group of Lie type.

The maximal subgroups of X are not completely known. However, they are completely determined for some groups, as reported in Table 3.5.

Table 3.5: Reference for the maximal subgroups of some exceptional groups

S	Reference
${}^2B_2(t^2)$	[Suz62], [Pat09c]
${}^3D_4(t^3)$	[Kle88b]
${}^2F_4(t^2)$	[Mal91]
$G_2(t)$	[Kle88a], [Coo81]
${}^2G_2(t^2)$	[Kle88a]

For the other groups, namely $F_4(t), E_6(t), E_7(t), E_8(t)$ and ${}^2E_6(t)$, the best result is the following.

Theorem 3.13 (See [ILS03, Theorem 9])**.** *Let M be a maximal subgroup of a finite exceptional group S over $\mathbb{F}_t$, where t is a power of p. Let*

$$k(S) = \begin{cases} 12\log_p(t)t^{56} & \text{if } S \cong E_8(q), \\ 4\log_p(t)t^{30} & \text{if } S \cong E_7(q), \\ 4\log_p(t)t^{28} & \text{if } S \cong E_6(q), \\ 4\log_p(t)t^{28} & \text{if } S \cong {}^2E_6(q), \\ 4\log_p(t)t^{20} & \text{if } S \cong F_4(q). \end{cases}$$

If $|M| \geq k(S)$, then M is known.

Table 3.6: Maximal subgroups H in the class $\mathcal{S}$ of a classical group (not unitary) of dimension d over $\mathbb{F}_q$ such that $(\hat{q}_e^*, |G:H|) = 1$, $(e,q) \neq (6,2)$.

e	d	q	$S = \mathrm{soc}(H)$
$d-4, d \geq 9$	10	3,5	$\mathrm{Alt}_{11}, \mathrm{Alt}_{12}$
	14	2	$\mathrm{Alt}_{15}, \mathrm{Alt}_{16}$
	16	2	$\mathrm{Alt}_{17}, \mathrm{Alt}_{18}$
	22	2	$\mathrm{Alt}_{23}, \mathrm{Alt}_{24}$
$d-3, d \geq 7$	7	2,3	$\mathrm{Alt}_8, \mathrm{Alt}_9$
	7	3	$\mathrm{PSp}_6(2)$
	9	3,5	$\mathrm{PSL}_2(8), \mathrm{Alt}_{10}, \mathrm{Alt}_{11}$
	9		$\mathrm{PSL}_3(q^2)$
	13	2	$\mathrm{Alt}_{14}, \mathrm{Alt}_{15}$
	15	2	$\mathrm{Alt}_{16}, \mathrm{Alt}_{17}$
	21	2	$\mathrm{Alt}_{22}, \mathrm{Alt}_{23}$
$d-2, d \geq 5$	6	2, 3	$\mathrm{Alt}_5, \mathrm{Alt}_7, \mathrm{Alt}_8, \mathrm{PSL}_2(11)$
	6	3	$\mathrm{PSL}_3(4), M_{12}$
	8	3, 5	$\mathrm{Alt}_8, \mathrm{Alt}_9, \mathrm{Alt}_{10}, \mathrm{PSL}_2(7), \mathrm{P}\Omega_8^+(2), \mathrm{Sp}_6(2), \mathrm{PSL}_2(8)$
	8	5	$\mathrm{Alt}_7, {}^2B_2(8), \mathrm{PSL}_3(4)$
	8		$\mathrm{PSL}_2(q^3), \mathrm{PSU}_3(q)$
	8		$\mathrm{P}\Omega_7(q)(q \text{ odd}), \mathrm{Sp}_6(q)(p=2)$
	12	2	$\mathrm{Alt}_{13}, \mathrm{Alt}_{14}, \mathrm{PSL}_2(11), \mathrm{PSL}_2(23)$
	14	2	$G_2(3), \mathrm{PSp}_6(3), \mathrm{PSL}_2(13),$ $\mathrm{PSL}_2(27), \mathrm{Alt}_{15}, \mathrm{Alt}_{16}$
	20	2	$\mathrm{Alt}_{21}, \mathrm{Alt}_{22}, J_1, \mathrm{PSL}_2(19)$
$d-1, d \geq 4$	4	2, 4	$\mathrm{Alt}_7, \mathrm{Alt}_8, \mathrm{PSL}_2(7)$
	5	2	$\mathrm{PSp}_4(3), \mathrm{PSL}_2(9)$
	5	2, 3	$\mathrm{Alt}_6, \mathrm{Alt}_7, \mathrm{PSL}_2(11)$
	5	3	M_{11}
	7	3, 5	$\mathrm{Alt}_8, \mathrm{Alt}_9, \mathrm{PSp}_6(2), \mathrm{PSL}_2(7), \mathrm{PSL}_2(8)$
	7	3, 4, 5, 17	$\mathrm{PSL}_2(13)$
	7	5	$\mathrm{PSU}_3(3)$
	7	$p=3$	$\mathrm{PSU}_3(q), {}^2G_2(q)$
	7	p odd	$G_2(q)$
	9	2	$\mathrm{PSL}_2(17)$
	11	2	$\mathrm{Alt}_{12}, \mathrm{Alt}_{13}, M_{23}, M_{24}, \mathrm{PSL}_2(23), \mathrm{PSL}_2(11)$
	13	2	$\mathrm{Alt}_{14}, \mathrm{Alt}_{15}, \mathrm{PSL}_3(3), \mathrm{PSp}_4(5),$ $\mathrm{PSp}_6(3), \mathrm{PSL}_2(25), \mathrm{PSL}_2(27), \mathrm{PSL}_2(13)$
	19	2	$\mathrm{Alt}_{20}, \mathrm{Alt}_{21}, \mathrm{PSL}_2(19)$
	19	2, 3	$\mathrm{PSL}_2(37)$
	21	2	$\mathrm{PSL}_2(41)$

Table 3.7: Maximal subgroups H in the class $\mathcal{S}$ of a classical group (not unitary) of dimension d over $\mathbb{F}_q$ such that $(\hat{q}_e^*, |G : H|) = 1$, $(e, q) \neq (6, 2)$.

e	d	q	$S = \mathrm{soc}(H)$
$d, d \geq 3$	3	2, 4	$\mathrm{PSL}_2(7)$
	4	2	$\mathrm{Alt}_7, \mathrm{Alt}_8, \mathrm{PSL}_2(9), \mathrm{PSp}_4(3)$
	4		${}^2B_2(q), p = 2$
	4	2, 3	$\mathrm{Alt}_5, \mathrm{Alt}_6$
	6	3	$\mathrm{PSL}_3(4)$
	6	3, 4, 5, 17	$\mathrm{PSL}_2(13)$
	6	3, 5	$\mathrm{Alt}_7, \mathrm{Alt}_8, \mathrm{PSL}_2(7)$
	6	5	$J_2, \mathrm{PSU}_3(3)$
	6		$G_2(q), p = 2$
	8	2	$\mathrm{PSL}_2(17)$
	10	2	$\mathrm{Alt}_{11}, \mathrm{Alt}_{12}, M_{11}, M_{12}, M_{22}, \mathrm{PSL}_2(11)$
	12	2	$\mathrm{Alt}_{13}, \mathrm{Alt}_{14}, \mathrm{PSL}_3(3), \mathrm{PSL}_2(13), \mathrm{PSL}_2(25), \mathrm{PSp}_4(5)$
	18	2	$\mathrm{Alt}_{19}, \mathrm{Alt}_{20}, \mathrm{PSL}_2(19)$
	18	2, 3	$\mathrm{PSL}_2(37)$
	20	2	$\mathrm{PSL}_2(41)$

Table 3.8: Subgroups H in the class $\mathcal{S}$ of $\mathrm{PSU}_d(q)$ such that $(\hat{q}_e^*, |G : H|) = 1$, $(e, q) \neq (6, 2)$.

e	d	q	$S = \mathrm{soc}(H)$
$2d - 8, d \geq 9$ odd	9	2	Alt_{11}
$2d - 6, d \geq 8$ even			
$2d - 4, d \geq 5$ odd	5	3,5	Alt_7
$2d - 2, d \geq 4$ even	4	3,5	$\mathrm{Alt}_7, \mathrm{PSL}_2(7)$
	4	3	$\mathrm{PSL}_3(4)$
	6	2	$\mathrm{PSL}_2(11), M_{22}$
	10	2	$\mathrm{PSL}_2(19)$
$2d, d \geq 3$ odd	3	3, 5	$\mathrm{PSL}_2(7)$
	3	5	Alt_7
	5	2	$\mathrm{PSL}_2(11)$
	9	2	$J_3, \mathrm{PSL}_2(19)$

Table 3.9: Geometric maximal subgroups H of $\mathrm{PSL}_n(q)$ such that $(\hat{q}_e^*, |G:H|) = 1$.

$\hat{q}_e$	H	Conditions
$\hat{q}_n$	$\mathrm{GL}_{n/r}(q^r)$ in $\mathcal{C}_3$	$r \mid n, r$ prime
$(q,n) \neq (2,6)$,	$\mathrm{Sp}_n(q)$ in $\mathcal{C}_8$	n even
$n \geq 3$	$O_n^-(q)$ in $\mathcal{C}_8$	n even, q odd
	$U_n(q^{1/2})$ in $\mathcal{C}_8$	n odd, $q = q_0^2$
$\hat{q}_{n-1}$	P_1 in $\mathcal{C}_1$	
$(q,n) \neq (2,7)$,	$\mathrm{GL}_1(q) \wr S_n$ in $\mathcal{C}_2$	$\hat{q}_{n-1}^* = n$
$n \geq 4$	$\mathrm{GL}_1(q^n)$ in $\mathcal{C}_3$	$\hat{q}_{n-1}^* = n$
	$O_n(q)$ in $\mathcal{C}_8$	nq odd
	$U_n(q^{1/2})$ in $\mathcal{C}_8$	n even, $q = q_0^2$
$\hat{q}_{n-2}$	P_1, P_2 in $\mathcal{C}_1$	
$(q,n) \neq (2,8)$,	$\mathrm{GL}_1(q) \wr S_n$ in $\mathcal{C}_2$	$\hat{q}_{n-2}^* = n-1$
$n \geq 5$	$\mathrm{Sp}_n(q)$ in $\mathcal{C}_8$	n even
	$O_n^\pm(q)$ in $\mathcal{C}_8$	q odd, n even
	$U_n(q^{1/2})$ in $\mathcal{C}_8$	n odd, $q = q_0^2$
$\hat{q}_{n-3}$	P_1, P_2, P_3 in $\mathcal{C}_1$	
$(q,n) \neq (2,9)$,	$\mathrm{GL}_1(q) \wr S_n$ in $\mathcal{C}_2$	$\hat{q}_{n-3}^* = n-2$
$n \geq 7$	$O_n(q)$ in $\mathcal{C}_8$	qn odd
	$U_n(q^{1/2})$ in $\mathcal{C}_8$	n even, $q = q_0^2$

Table 3.10: Geometric maximal subgroups H of $\mathrm{PSU}_n(q)$ such that $(\hat{q}_e^*, |G:H|) = 1$.

$\hat{q}_e$	H	Conditions
$\hat{q}_{2n}$ $(q,n) \neq (2,3)$ $n \geq 3, n$ odd	$\mathrm{GU}_{n/r}(q^r)$ in $\mathcal{C}_3$	$r \mid n, r \geq 3$ prime
$\hat{q}_{2n-2}$ $(q,n) \neq (2,4)$, $n \geq 4, n$ even	$\mathrm{GU}_1(q) \perp \mathrm{GU}_{n-1}(q)$ in $\mathcal{C}_1$	
$\hat{q}_{2n-4}$ $(q,n) \neq (2,5)$, $n \geq 5, n$ odd	P_1 in $\mathcal{C}_1$ $\mathrm{GU}_1(q) \perp \mathrm{GU}_{n-1}(q)$ in $\mathcal{C}_1$ $\mathrm{GU}_2(q) \perp \mathrm{GU}_{n-2}(q)$ in $\mathcal{C}_1$	
$\hat{q}_{2n-6}$ $n \geq 8, n$ even	P_1 in $\mathcal{C}_1$ $\mathrm{GU}_1(q) \perp \mathrm{GU}_{n-1}(q)$ in $\mathcal{C}_1$ $\mathrm{GU}_2(q) \perp \mathrm{GU}_{n-2}(q)$ in $\mathcal{C}_1$ $\mathrm{GU}_3(q) \perp \mathrm{GU}_{n-3}(q)$ in $\mathcal{C}_1$ $\mathrm{GU}_{n/3}(q^3)$ in $\mathcal{C}_3$	 $3 \mid n$
$\hat{q}_{2n-8}$ $n \geq 9, n$ odd	P_1, P_2 in $\mathcal{C}_1$ $\mathrm{GU}_1(q) \perp \mathrm{GU}_{n-1}(q)$ in $\mathcal{C}_1$ $\mathrm{GU}_2(q) \perp \mathrm{GU}_{n-2}(q)$ in $\mathcal{C}_1$ $\mathrm{GU}_3(q) \perp \mathrm{GU}_{n-3}(q)$ in $\mathcal{C}_1$ $\mathrm{GU}_4(q) \perp \mathrm{GU}_{n-4}(q)$ in $\mathcal{C}_1$	

Table 3.11: Geometric maximal subgroups H of $\mathrm{PSp}_{2n}(q)$ such that $(\hat{q}_e^*, |G:H|) = 1$.

$\hat{q}_e$	H	Conditions
$\hat{q}_{2n}$ $(q,n) \neq (2,3)$, $n \geq 2$	$\mathrm{GU}_n(q)$ in $\mathcal{C}_3$ $\mathrm{Sp}_{2n/r}(q^r)$ in $\mathcal{C}_3$ $2^{1+4}.O_4^-(2)$ in $\mathcal{C}_6$ $O_{2n}^-(q)$ in $\mathcal{C}_8$	nq odd $r \mid 2n, r$ prime, $2n/r$ even $(q,n) = (3,2)$ q even
$\hat{q}_{2n-2}$ $(q,n) \neq (2,4)$, $n \geq 3$	P_1 in $\mathcal{C}_1$ $\mathrm{Sp}_2(q) \perp \mathrm{Sp}_{2n-2}(q)$ in $\mathcal{C}_1$ $\mathrm{GU}_n(q)$ in $\mathcal{C}_3$ $O_{2n}^{\pm}(q)$ in $\mathcal{C}_8$	 $\hat{q}_{2n-2}^* = n$ n even, q odd q even

Table 3.12: Geometric maximal subgroups H of $\mathrm{P}\Omega_{2n+1}(q), q$ odd, such that $(\hat{q}_e^*, |G : H|) = 1$.

$\hat{q}_e$	H	Conditions
$\hat{q}_{2n}$	$O_1(q) \perp O_{2n}^-(q)$ in $\mathcal{C}_1$	
$n \geq 3$	$O_1(q) \wr S_{2n+1}$ in $\mathcal{C}_2$	$\hat{q}_{2n}^* = 2n+1$
$\hat{q}_{2n-2}$	P_1 in $\mathcal{C}_1$	
$n \geq 3$	$O_1(q) \perp O_{2n}^{\pm}(q)$ in $\mathcal{C}_1$	
	$O_3(q) \perp O_{2n-2}^-(q)$ in $\mathcal{C}_1$	
	$O_{2n-1}(q) \perp O_2^{\pm}(q)$ in $\mathcal{C}_1$	
	$O_1(q) \wr S_{2n+1}$ in $\mathcal{C}_2$	$\hat{q}_{2n-2}^* = 2n-1, q$ odd
	$O_{\frac{2n+1}{3}}(q^3)$ in $\mathcal{C}_3$	$3 \mid 2n+1$

Table 3.13: Geometric maximal subgroups H of $\mathrm{P}\Omega_{2n}^-(q)$ such that $(\hat{q}_e^*, |G : H|) = 1$.

$\hat{q}_e$	H	Conditions
$\hat{q}_{2n}$	$\mathrm{GU}_n(q)$ in $\mathcal{C}_3$	n odd
$n \geq 4$	$O_{2n/r}^-(q^r)$ in $\mathcal{C}_3$	$2n/r \geq 4$ even, $r \mid 2n, r$ prime
$\hat{q}_{2n-2}$	P_1 in $\mathcal{C}_1$	
$n \geq 4$	$O_1(q) \perp O_{2n-1}(q)$ in $\mathcal{C}_1$	q odd
$(q,n) \neq (2,4)$	$O_2^+(q) \perp O_{2n-2}^-(q)$ in $\mathcal{C}_1$	$q \geq 4$
	$\mathrm{Sp}_{2n-2}(q)$ in $\mathcal{C}_1$	q even
	$O_1(q) \wr S_{2n}$ in $\mathcal{C}_2$	$\hat{q}_{2n-2}^* = 2n-1, q$ odd
	$O_n(q^2)$ in $\mathcal{C}_3$	qn odd
$\hat{q}_{2n-4}$	P_1, P_2 in $\mathcal{C}_1$	
$n \geq 5$	$O_1(q) \perp O_{2n-1}(q)$ in $\mathcal{C}_1$	q odd
$(q,n) \neq (2,5)$	$O_3(q) \perp O_{2n-3}(q)$ in $\mathcal{C}_1$	q odd
	$O_2^+(q) \perp O_{2n-2}^-(q)$ in $\mathcal{C}_1$	$q \geq 4$
	$O_2^-(q) \perp O_{2n-2}^+(q)$ in $\mathcal{C}_1$	
	$O_4^+(q) \perp O_{2n-4}^-(q)$ in $\mathcal{C}_1$	
	$\mathrm{Sp}_{2n-2}(q)$ in $\mathcal{C}_1$	q even
	$O_1(q) \wr S_{2n}$ in $\mathcal{C}_2$	$\hat{q}_{2n-4}^* = 2n-3, q$ odd
	$\mathrm{GU}_n(q)$ in $\mathcal{C}_3$	n odd
	$O_n^-(q^2)$ in $\mathcal{C}_3$	n even

Table 3.14: Geometric maximal subgroups H of $\mathrm{P}\Omega^+_{2n}(q)$ such that $(\hat{q}^*_e, |G:H|) = 1$.

$\hat{q}_e$	H	Conditions
$\hat{q}_{2n-2}$	$O_1(q) \perp O_{2n-1}(q)$ in $\mathcal{C}_1$	q odd
$n \geq 4$	$O_2^-(q) \perp O_{2n-2}^-(q)$ in $\mathcal{C}_1$	
$(q,n) \neq (2,4)$	$\mathrm{Sp}_{2n-2}(q)$ in $\mathcal{C}_1$	q even
	$O_1(q) \wr S_{2n}$ in $\mathcal{C}_2$	$\hat{q}^*_{2n-2} = 2n-1, q$ odd
	$\mathrm{GU}_n(q)$ in $\mathcal{C}_3$	n even
	$O_n(q^2)$ in $\mathcal{C}_3$	qn odd
	$2^{1+6}O_6^+(2)$ in $\mathcal{C}_6$	$q \in \{3,5\}, n = 4$
$\hat{q}_{2n-4}$	P_1 in $\mathcal{C}_1$	
$n \geq 5$	$O_1(q) \perp O_{2n-1}(q)$ in $\mathcal{C}_1$	q odd
$(q,n) \neq (2,5)$	$O_3(q) \perp O_{2n-3}(q)$ in $\mathcal{C}_1$	q odd
	$O_2^+(q) \perp O_{2n-2}^+(q)$ in $\mathcal{C}_1$	$q \geq 4$
	$O_2^-(q) \perp O_{2n-2}^-(q)$ in $\mathcal{C}_1$	
	$O_4^-(q) \perp O_{2n-4}^-(q)$ in $\mathcal{C}_1$	
	$\mathrm{Sp}_{2n-2}(q)$ in $\mathcal{C}_1$	q even
	$O_1(q) \wr S_{2n}$ in $\mathcal{C}_2$	$\hat{q}^*_{2n-4} = 2n-3, q$ odd
	$O_n^+(q^2)$ in $\mathcal{C}_3$	n even

Table 3.15: Alternating and Sporadic simple groups with $R(S) \leq 12$

S	$R(S)$	S	$R(S)$
Alt_5	2	Alt_6	2
Alt_7	3	Alt_8	4
Alt_9	7	Alt_{10}	8
Alt_{11}	9	Alt_{12}	10
Alt_{13}	11	Alt_{14}	12
M_{11}	≥ 5	M_{12}	≥ 6
M_{22}	≥ 6	M_{23}	≥ 11
M_{24}	≥ 11	J_1	≥ 7
J_2	≥ 6	J_3	≥ 9
Suz	≥ 12		

Table 3.16: Simple groups of Lie type of characteristic r with $R_{r'}(S) \leq 12$, such that S does not appear in Table 3.15

S	$R_{r'}(S) \geq$	S	$R_{r'}(S) \geq$
$\mathrm{PSL}_3(2)$	2	$\mathrm{PSL}_2(7)$	3
$\mathrm{PSL}_3(4)$	4	$\mathrm{PSU}_4(2)$	4
$\mathrm{PSp}_4(3)$	4	$\mathrm{PSL}_2(11)$	5
$\mathrm{PSL}_2(13)$	6	$\mathrm{PSU}_3(3)$	6
$\mathrm{PSU}_4(3)$	6	$\mathrm{PSL}_2(8)$	7
$\mathrm{PSp}_6(2)$	7	$\mathrm{P}\Omega_8^+(2)$	8
${}^2B_2(8)$	8	$\mathrm{PSL}_2(17)$	8
$\mathrm{PSL}_3(3)$	8	$\mathrm{PSL}_2(19)$	9
$\mathrm{PSU}_5(2)$	10	$\mathrm{PSL}_2(23)$	11
$\mathrm{PSL}_2(25)$	12	$\mathrm{PSp}_4(5)$	12
$G_2(4)$	12		

Table 3.17: Simple groups of Lie type of characteristic p with $R_p(S) \leq 12$

S	$R_p(S)$	conditions
$\mathrm{PSL}_2(q)$	2	
$\mathrm{PSL}_l(q)$	l	$3 \leq l \leq 12$
$\mathrm{PSU}_l(q)$	l	$3 \leq l \leq 12$
$\mathrm{PSp}_4(q)$	4	
$\mathrm{PSp}_l(q)$	l	$l \in \{6, 8, 10, 12\}$
$\mathrm{P}\Omega_l(q)$	l	q odd, $l \in \{7, 9, 11\}$
$\mathrm{P}\Omega_8^+(q)$	8	
$\mathrm{P}\Omega_l^+(q)$	l	$l \in \{10, 12\}$
$\mathrm{P}\Omega_l^-(q)$	l	$l \in \{8, 10, 12\}$
${}^2B_2(q)$	4	$p = 2, f \geq 3, f$ odd
$G_2(q)$	$7 - \delta_{p,2}$	
${}^2G_2(q)$	7	$p = 3, f \geq 3, f$ odd
${}^3D_4(q)$	8	

Table 3.18: Dimension t of the irreducible projective $\overline{\mathbb{F}_p}S$ modules with $t \leq 12$, S group of Lie type of characteristic p

S	Values of t
$\mathrm{PSL}_2(q)$	some $t \geq 2$
$\mathrm{PSL}_3(q)$	3 and some $t \geq 6$
$\mathrm{PSL}_4(q)$	$4, 6$ and some $t \geq 10$
$\mathrm{PSL}_5(q)$	$5, 10$
$\mathrm{PSL}_l(q), 6 \leq l \leq 12$	l
$\mathrm{PSU}_3(q)$	3 and some $t \geq 6$
$\mathrm{PSU}_4(q)$	$4, 6$ and some $t \geq 10$
$\mathrm{PSU}_5(q)$	$5, 10$
$\mathrm{PSU}_l(q), 6 \leq l \leq 12$	l
$\mathrm{PSp}_4(q)$	$4, 5 - \delta_{p,2}$ and some $t \geq 9$
$\mathrm{PSp}_6(q)$	$6, 8(q$ even$)$
$\mathrm{PSp}_l(q), l \in \{8, 10, 12\}$	l
$\mathrm{P}\Omega_7(q)$	$7, 8$
$\mathrm{P}\Omega_l(q), l \in \{9, 11\}$	l
$\mathrm{P}\Omega_l^{\pm}(q), l \in \{8, 10, 12\}$	l
$G_2(q)$	$7 - \delta_{p,2}, 14 - 7\delta_{p,3}$
${}^2G_2(q)$	7
${}^3D_4(q)$	some $t \geq 8$
${}^2B_2(q)$	some $t \geq 4$

Part I

On the non contractibility of the order complex of the coset poset of a classical group.

Chapter 4

Introduction

In this part, our aim is to prove the following theorem.

Theorem 4.1. *Let G be a finite group whose chief factors are either abelian or classical projective groups. Then $P_{G,\mathrm{soc}(G)}(-1) \neq 0$, hence the order complex of the coset poset of G is not contractible.*

This theorem is a corollary of the more general Theorem 7.1 which requires more technical assumptions.

In the sequel we illustrate the strategy employed to prove the result. First, we state a more precise version of Theorem 1.3. We say that a maximal subgroup M of a monolithic group L is *non-trivial intersecting* if $1 < pr(M \cap \mathrm{soc}(L)) < S$, where $pr : \mathrm{soc}(L) \to S$ is the projection to a simple component S of $\mathrm{soc}(L)$.

non-trivial intersecting

Theorem 4.2 ([Ser08, Theorem 4 and 5])**.** *Let G be a monolithic primitive group with a non-abelian simple component S. Let $d' = |G : N_G(S)|$ and let $X = N_G(S)/C_G(S)$. We have that:*

$$P_{G,\mathrm{soc}(G)}(s) - \sum_{|S||m} \frac{a_m(G, \mathrm{soc}(G))}{m^s} = P_{X,S}(d's - d' + 1) - \sum_{|S||m^{d'}} \frac{a_m(X, S)}{m^{d's-d'+1}}.$$

Moreover, assuming that if M is a maximal subgroup of G, then M is non-trivial intersecting, we have that

$$P_{G,\mathrm{soc}(G)}(s) = P_{X,S}(d's - d' + 1).$$

Thus we get that

$$P_{G,\mathrm{soc}(G)}(-1) = \sum_{|S||m} a_m(G,\mathrm{soc}(G))m - \sum_{|S||m^{d'}} a_m(X,S)m^{2d'-1} + P_{X,S}(1-2d').$$

By Lemma 2.3 we have that

$$\left| \sum_{|S||m} a_m(G,\mathrm{soc}(G))m - \sum_{|S||m^{d'}} a_m(X,S)m^{2d'-1} \right|_p \geq |S|_p^2.$$

In our analysis, we find some conditions which assure that $|P_{X,S}(1-2d')|_p < |S|_p^2$. Now, we concentrate on the study of $|P_{X,S}(1-2d')|_p$. Let $d = 2d'$. Note that

$$P_{X,S}(1-d) = P_{X,S}^{(p)}(1-d) + \sum_{p|k} a_k(X,S)k^{d-1}.$$

By Lemma 2.3, we have

$$\left| \sum_{p|k} a_k(X,S)k^{d-1} \right|_p \geq q^{d\beta_p(X)},$$

$\beta_p(X)$ where

$$q^{\beta_p(X)} = \min\{|X:H|_p : H < X, |X:H|_p > 1, HS = X, \mu_X(H) \neq 0\}.$$

So, in order to show that $P_{G,\mathrm{soc}(G)}(-1) \neq 0$, it is enough to prove that

$$|P_{X,S}^{(p)}(1-d)|_p < \min\{q^{d\beta_p(X)}, |S|_p^2\}.$$

In Chapter 5, we study the value of $|P_{X,S}^{(p)}(1-d)|_p$. In Chapter 6, we give a lower bound for $\beta_p(X)$, computing the exact value for some groups. Finally, in Chapter 7, we prove the main theorem.

Chapter 5

Evaluating $|P^{(p)}_{X,S}(1-d)|_p$

5.1 Some results on root systems

Let S be a simple group of Lie type over the field $\mathbb{K}$. We use the notation introduced in Subsection 3.1.2. Moreover, we set $k = |I|$ for this section.

We denote by t the positive number $\sqrt[|\rho|]{|\mathbb{K}|}$. This definition is the most convenient, although it allows t to be irrational (see [Car72, §14.1]).

The following lemma is quite technical. We point out some important facts on root systems.

Lemma 5.1. *Using the notation introduced in Subsection 3.1.2, the followings hold.*

(1) The set $\{w(\Phi_i^+) : w \in \mathcal{W}, i \in \{1, ..., k\}\}$ *is a partition of* Φ.

(2) There exists a unique element $\omega \in W$ *such that* $\omega(\Phi^+) = \Phi^-$. *This element is an involution and* $l(\omega) = |\Phi^+|$. *In particular,* $\omega \in \mathcal{W}$.

(3) Let $K \subseteq \Pi$ *and let* $w \in W_K$. *The length* $l(w)$ *is the same whether* w *is regarded as an element of the Weyl group* W *or of the Weyl group* W_K.

(4) Let $i \in \{1, ..., k\}$. *There exists a unique element* $\omega_i \in W_i$ *such that* $\omega_i(\Phi_i^+) = \Phi_i^-$. *Moreover,* ω_i *generates* $\mathcal{W}_i$ *in* W *and* $\{\omega_i : i \in \{1, ..., k\}\}$ *generates* $\mathcal{W}$ *in* W. ω_i

(5) Let $i \in \{1, ..., k\}$ and let $w \in \mathcal{W}$ such that $w(r) \in \Phi^-$ for some $r \in O_i$. We have that $l(w\omega_i) = l(w) - l(\omega_i)$.

(6) Let $w \in \mathcal{W}$ and let $r, s \in O_i$ for some $i \in \{1, ..., k\}$. The roots $w(r)$ and $w(s)$ have the same sign, i.e. either $w(r), w(s) \in \Phi^+$ or $w(r), w(s) \in \Phi^-$.

(7) Let $w \in \mathcal{W}$ and let J be a subset of I. We have that $w = d_J w_J$ for uniquely determined $d_J \in \mathfrak{D}_J$ and $w_J \in \mathcal{W}_J$. Moreover, $l(w) = l(d_J) + l(w_J)$.

(8) Let $i, j \in \{1, ..., k\}$. Let w be an element of $\mathcal{W}$ such that $w(O_i) \subseteq \Phi_j^-$. We have that $\omega_i^w = w\omega_i w^{-1} = \omega_j$.

Proof.

(1) See [Car72, Lemma 13.2.1].

(2) See [Car72, Proposition 2.2.6]. It remains to show that $\omega \in \mathcal{W}$. Since τ preserves the sign of each root, we have that $\tau\omega\tau^{-1}(\Phi^+) = \Phi^-$. Hence $\tau\omega\tau^{-1} = \omega$, as required.

(3) This is [Car72, Lemma 9.4.1].

(4) This is [Car72, Proposition 13.1.2].

(5) This is inside the proof of [Car72, Proposition 13.1.2].

(6) This is clear since τ preserves the sign of each root.

(7) By [Car72, Theorem 2.5.8], we know that $w = d_{J^*} w_{J^*}$ for uniquely determined $d_{J^*} \in D_{J^*}$ and $w_{J^*} \in W_{J^*}$, and that $l(w) = l(d_{J^*}) + l(w_{J^*})$. So, it remains to prove that w can be expressed in the form $w = d_J w_J$ for $d_J \in \mathfrak{D}_J$ and $w_J \in \mathcal{W}_J$. Suppose $l(w) = 0$, we have that $w = 1$ and $w = 1.1$ is the required factorization. Now, assume $l(w) > 0$ and proceed by induction on $l(w)$. If $w \in \mathfrak{D}_J$, then $w = w.1$ is the required factorization. If $w \notin \mathfrak{D}_J$, then there exist $i \in \{1, ..., k\}$ and $r \in O_i$ such that $O_i \in J$ and $w(r) \in \Phi^-$. So, by part

(5), $l(ww_i) = l(w) - l(w_i) < l(w)$. Hence, by induction, $ww_i = d_J w'_J$ for some $d_J \in \mathfrak{D}_J$ and $w'_J \in \mathcal{W}_J$. Clearly $w_J = w'_J w_i$ is in $\mathcal{W}_J$, so $w = d_J w_J$ as required.

(8) Since W is generated by the fundamental reflections, we have $\omega_i = w_{r_1}...w_{r_n}$ for some $r_l \in O_i, l \in \{1, ..., n\}$. So, using the definition of reflection, we have

$$\omega_i^w = w_{r_1}^w ... w_{r_n}^w = w_{w(r_1)} ... w_{w(r_n)}.$$

Since $w(r_l) \in \Phi_j^- \subset \Phi_j$ for $l \in \{1, ..., n\}$, we have that ω_i^w is an element of W_{O_j}. But clearly $\omega_i^w \in \mathcal{W}$, hence $\omega_i^w \in \mathcal{W}_j$. Now, since $w(O_i) \subseteq \Phi_j^-$, then also $w(\Phi_i^+) \subseteq \Phi_j^-$. By definition, we have $\omega_j(\Phi_j^+) = \Phi_j^-$ so, by part (1) of the lemma, we get $w(\Phi_i^+) = \Phi_j^-$. Thus $\omega_i^w(\Phi_j^+) = w\omega_i w^{-1}(\Phi_j^+) = w\omega_i(\Phi_i^-) = w(\Phi_i^+) = \Phi_j^-$. Since $\omega_i^w(\Phi_j^+) = \Phi_j^-$ and $\omega_i^w \in \mathcal{W}_j$, part (4) yields $\omega_i^w = \omega_j$. □

We fix the notation ω_i for $i \in \{1, ..., k\}$, as in the previous lemma.

Now, we give an useful definition. Let $n \in \mathbb{N}$ and $i_j \in \{1, ..., k\}$ for $j \in \{1, ..., n\}$ and let $w \in \mathcal{W}$. An *ω-factorization of w* is an expression of w of the form

$$\omega_{i_1} ... \omega_{i_n},$$

and the integer n is called the *length of the ω-factorization.*

Lemma 5.2. *We have the following.*

(1) Let $w \in \mathcal{W}$. Let $n \in \mathbb{N}$, $i_j \in \{1, ..., k\}$ for $j \in \{1, ..., n\}$ and suppose that $w = \omega_{i_1} ... \omega_{i_n}$ is an ω-factorization of minimal length of w. We have that

$$l(w) = \sum_{j=1}^{n} l(\omega_{i_j}) = \sum_{j=1}^{n} |\Phi_{i_j}^+|.$$

(2) Let $i \in \{1, ..., k\}$ and let $w \in \mathcal{W}$ such that $w(r) \in \Phi^-$ for some $r \in O_i$. We have that ω_i appears in each ω-factorization of w of minimal length.

Proof.

(1) The argument is similar to the proof of [Car72, Theorem 2.2.2]. It is clear that for any $u, v \in W$, $l(u) \leq l(vu) + l(u)$. Hence we have

$$l(w) \leq l(w\omega_{i_n}) + l(\omega_{i_n}) \leq l(w\omega_{i_n}\omega_{i_{n-1}}) + l(\omega_{i_{n-1}}) + l(\omega_{i_n}) \leq ... \leq \sum_{j=1}^{n} l(\omega_{i_j}) = L'. \quad (\dagger)$$

Thus $l(w) \leq L'$. Now, by contradiction, assume that $l(w) < L'$. So, we have that at least one of the inequalities in (†) is strict, i.e. there exists $m \in \{1, ..., n\}$ such that

$$l(\omega_{i_1}...\omega_{i_m}) = l(w\omega_{i_n}...\omega_{i_{m+1}}) < l(w\omega_{i_n}...\omega_{i_m}) + l(\omega_{i_m}) = l(\omega_{i_1}...\omega_{i_{m-1}}) + l(\omega_{i_m}).$$

This implies that $\omega_{i_1}...\omega_{i_m}(O_{i_m}) \subseteq \Phi^+$. In fact, if $\omega_{i_1}...\omega_{i_m}(r) \in \Phi^-$ for some $r \in O_{i_m}$, then

$$l(\omega_{i_1}...\omega_{i_m}) = l(\omega_{i_1}...\omega_{i_{m-1}}) + l(\omega_{i_m}),$$

by part (5) of the previous lemma.

Now, $\omega_{i_m}(O_{i_m}) \subseteq \Phi^-$ and $\omega_{i_1}...\omega_{i_m}(O_{i_m}) \subseteq \Phi^+$ imply that there exists a $j \in \{1, ..., m\}$ such that $\omega_{i_j}...\omega_{i_m}(O_{i_m}) \subseteq \Phi^+$ and $\omega_{i_{j+1}}...\omega_{i_m}(O_{i_m}) \subseteq \Phi^-$. However, ω_j change the sign of all roots in Φ_j, but of none in $\Phi - \Phi_j$. Hence $\omega_{i_{j+1}}...\omega_{i_m}(O_{i_m}) \subseteq \Phi_j^-$. By part (8) of the previous lemma, we have that $\omega_{i_{j+1}}...\omega_{i_m}\omega_{i_m}\omega_{i_m}...\omega_{i_{j+1}} = \omega_{i_j}$. Hence $\omega_{i_j}...\omega_{i_{m-1}} = \omega_{i_{j+1}}...\omega_{i_m}$, so we get

$$\begin{aligned} w &= \omega_{i_1}...\omega_{i_j}...\omega_{i_{m-1}}...\omega_{i_n} = \omega_{i_1}...\omega_{i_{j-1}}\omega_{i_{j+1}}...\omega_{i_m}\omega_{i_m}...\omega_{i_n} \\ &= \omega_{i_1}...\omega_{i_{j-1}}\omega_{i_{j+1}}...\omega_{i_{m-1}}\omega_{i_{m+1}}...\omega_{i_n}. \end{aligned}$$

But this is an ω-factorization of w of length $n-2$, a contradiction.

(2) Suppose that ω_i does not appear in an ω-factorization of w of minimal length. We claim that $w(O_i) \subseteq \Phi^+$. If $l(w) = 0$, then $w = 1$ and the result is clear. Suppose that $l(w) > 0$ and prove the claim by induction on the length of an ω-factorization of w. If $w = \omega_j$ for some $i \in \{1, .., k\}$ with $j \neq i$ (by hypothesis), then $\omega_j(O_i) \subset \Phi^+$ by definition of ω_j. Now, suppose that $w = \omega_{i_1}...\omega_{i_n}$ for some $n \geq 2$, $i_j \in \{1, ..., k\} - \{i\}$ for all $j \in \{1, ..., n\}$. By induction, we have

that $\omega_{i_2}...\omega_{i_n}(O_i) \subseteq \Phi^+$. In particular, $\omega_{i_2}...\omega_{i_n}(\Phi_i^+) \subseteq \Phi^+$. By contradiction, assume that $\omega_{i_2}...\omega_{i_n}(\Phi_i^+) \cap \Phi_{i_1}^+ \neq \varnothing$. By part (1) of the previous lemma, we have that $\omega_{i_2}...\omega_{i_n}(\Phi_i^+) = \Phi_{i_1}^+$, hence $w(\Phi_i^+) = \Phi_{i_1}^-$. So, by part (8) of the previous lemma, we get $\omega_i^w = \omega_{i_1}$, therefore

$$\omega_i = \omega_{i_n}...\omega_{i_1}...\omega_{i_n}.$$

This means that ω_i is in the group generated by $\omega_{i_1}, ..., \omega_{i_n}$, so $\omega_i \in \langle W_{O_{i_1}}, ..., W_{O_{i_n}} \rangle = W_{O_{i_1} \cup ... \cup O_{i_n}}$ and $\omega_i \in W_{O_i}$ (see [Car72, Theorem 2.5.6]). But $W_{O_{i_1} \cup ... \cup O_{i_n}} \cap W_{O_i} = W_\emptyset = 1$, a contradiction. So we have $\omega_{i_2}...\omega_{i_n}(\Phi_i^+) \cap \Phi_{i_1}^+ = \varnothing$, hence $w(\Phi_i^+) \subseteq \Phi^+$ since ω_{i_1} does not change the sign of the roots in $\Phi - \Phi_{i_1}$. Hence $w(O_i) \subseteq \Phi^+$, as we claimed. $\square$

An useful lemma about trees.

Lemma 5.3. *Let $d \geq 2$ be a natural number. Let T be a finite graph and assume that T has l connected components which are trees. Let $p(T)$ be the set of d-uples $(V_1, ..., V_d)$ such that*

- *$\{V_1, ..., V_d\}$ is a partition of the set of vertices V of T (i.e. $\bigcup_{i=1}^d V_i = V$ and if $i \neq j$, then $V_i \cap V_j = \varnothing$; so some V_i can be empty),*
- *if $a, b \in V_i$ for some $i \in \{1, ...d\}$, then a and b are not joined in T.*

The size of $p(T)$ is $d^l(d-1)^{|V|-l}$.

Proof. First assume that $l = 1$. We prove the claim by induction on $k = |V|$. If $k = 1$, then the result is clear. Suppose that $k > 1$. Since T is a tree, there exists a vertex $v \in V$ which has a unique vertex u of T joined to it. Consider the tree T' obtained from T deleting the vertex v. Since T' has $k-1$ vertices, by induction, we have that $|p(T')| = d(d-1)^{k-2}$. Suppose that $(V_1', ..., V_d') \in d(T')$. Without loss of generality, we may assume that $u \in V_d'$. Clearly, the d-uples $(V_1' \cup \{v\}, V_2', ..., V_d')$, $(V_1', V_2' \cup \{v\}, V_3', ..., V_d')$, ..., $(V_1', V_2', ..., V_{d-1}' \cup \{v\}, V_d')$ are $d-1$ elements of $p(T)$.

Moreover, each element $(V_1, ..., V_d)$ of $p(T)$ such that $u \in V_d$ is obtained in this way. Thus we conclude that $p(T) = p(T')(d-1) = d(d-1)^{k-1}$.

Now, let $T_1, ..., T_l$ be the connected components of T, and assume that $V_1, ..., V_l$ are the corresponding set of vertices. It is clear that

$$p(T) = \prod_{i=1}^{l} p(T_i) = \prod_{i=1}^{l} d(d-1)^{|V_i|-1} = d^l (d-1)^{|V|-l}.$$

This completes the proof. □

5.2 On the value of $P_{X,S}^{(p)}(s)$ for $s = -(d-1)$

Let X be an almost simple group with socle S isomorphic to a simple group of Lie type. In the sequel, we consider the value of $P_{X,S}^{(p)}(s)$ for $s = -(d-1)$, where d is a positive integer greater than 1. Firstly, we obtain an easier expression for $P_{X,S}^{(p)}(s)$.

To do that, we introduce some more definitions. Let u be an element of $\mathcal{W}$. We
I_u denote by I_u the subset of I consisting of the orbits $K \in I$ such that $u(K) \subseteq \Phi^+$. By Lemma 5.1 (6), note that $K \in I_u$ if and only if there exists $r \in K$ such that
I_u^c $u(r) \in \Phi^+$. Moreover, let $I_u^c = I - I_u$. Finally, if $u_1, ..., u_l$ are elements of $\mathcal{W}$, then let
$I_{u_1,...,u_l}$

$$I_{u_1,...,u_l} = \bigcap_{i=1}^{l} I_{u_i}.$$

Mimicking the proof of [Car72, Proposition 9.4.5], we obtain the following

Lemma 5.4. *Under the above assuptions, we have that*

$$(-1)^{o(I)} P_{X,S}^{(p)}(-(d-1)) = \sum_{J \in \mathcal{P}^X(I)} (-1)^{o(J)} \left(\frac{P_{\mathcal{W}}(t)}{P_{\mathcal{W}_J}(t)} \right)^d = \sum_{\substack{u_1, ..., u_d \in \mathcal{W} \\ I^X_{u_1,...,u_d} = \varnothing}} t^{\sum_{i=1}^d l(u_i)}.$$

where $I^X_{u_1,...,u_d}$ is the largest $N_X(B)$-invariant subset of $I_{u_1,...,u_d}$.

Proof. Let J be a subset of I. By Lemma 5.1 (7), each element w of $\mathcal{W}$ has a unique expression in the form $w = d_J w_J$, where $d_J \in \mathfrak{D}_J$ and $w_J \in \mathcal{W}_J$. Moreover,

$l(w) = l(d_J) + l(w_J)$. It follows that

$$\begin{aligned} P_{\mathcal{W}}(t) &= \sum_{w\in\mathcal{W}} t^{l(w)} = \sum_{d_J\in\mathfrak{D}_J}\sum_{w_J\in\mathcal{W}_J} t^{l(d_J w_J)} = \sum_{d_J\in\mathfrak{D}_J}\sum_{w_J\in\mathcal{W}_J} t^{l(d_J)+l(w_J)} \\ &= \sum_{d_J\in D_J} t^{l(d_J)} \sum_{w_J\in\mathcal{W}_J} t^{l(w_J)} = \sum_{d_J\in\mathfrak{D}_J} t^{l(d_J)} P_{\mathcal{W}_J}(t). \end{aligned}$$

Hence, we have

$$\begin{aligned} \sum_{J\in\mathcal{P}^X(I)} (-1)^{o(J)} \left(\frac{P_{\mathcal{W}}(t)}{P_{\mathcal{W}_J}(t)}\right)^d &= \sum_{J\subseteq I}(-1)^{o(J)} \left(\sum_{d_J\in\mathfrak{D}_J} t^{l(d_J)}\right)^d = \\ &= \sum_{J\in\mathcal{P}^X(I)} (-1)^{o(J)} \sum_{u_1,\dots,u_d\in\mathfrak{D}_J} t^{\sum_{i=1}^d l(u_i)} = \\ &= \sum_{J\in\mathcal{P}^X(I)} (-1)^{o(J)} \sum_{\substack{u_1,\dots,u_d\in\mathcal{W} \\ u_i(J^*)\subseteq\Phi^+}} t^{\sum_{i=1}^d l(u_i)} = \\ &= \sum_{u_1,\dots,u_d\in\mathcal{W}} t^{\sum_{i=1}^d l(u_i)} \sum_{\substack{J\subseteq I_{u_1,\dots,u_d}, \\ J\in\mathcal{P}^X(I)}} (-1)^{o(J)}. \end{aligned}$$

The last equality holds since we have that $J \subseteq I_{u_1,\dots,u_d}$ if and only if $u_1(J^*),\dots,u_d(J^*) \subseteq \Phi^+$.

Let $\tilde{I}^X_{u_1,\dots,u_d}$ be the set of $N_X(B)$-orbits of $I^X_{u_1,\dots,u_d}$. Note that the set $\{J\in\mathcal{P}^X(I) : J\subseteq I_{u_1,\dots,u_d}\}$ and the set $\mathcal{P}(\tilde{I}^X_{u_1,\dots,u_d})$ are isomorphic posets, an isomorphisms given by $J\mapsto\tilde{J}$, where J is the set of $N_X(B)$-orbits of J. Moreover, recall that $o(J) = |\tilde{J}|$. Finally, it is clear that

$$\sum_{\substack{J\subseteq I_{u_1,\dots,u_d}, \\ J\in\mathcal{P}^X(I)}} (-1)^{o(J)} = \sum_{\tilde{J}\subseteq\tilde{I}^X_{u_1,\dots,u_d}} (-1)^{|\tilde{J}|} = \begin{cases} 1 & \text{if } I^X_{u_1,\dots,u_d} = \varnothing, \\ 0 & \text{otherwise.} \end{cases}$$

since $I^X_{u_1,\dots,u_d} = \varnothing$ if and only if $\tilde{I}^X_{u_1,\dots,u_d} = \varnothing$. □

By the previous lemma, we can write

$$(-1)^{o(I)} P^{(p)}_{X,S}(-(d-1)) = \sum_{\substack{u_1,\dots,u_d\in\mathcal{W} \\ I^X_{u_1,\dots,u_d}=\varnothing}} t^{\sum_{i=1}^d l(u_i)} = \sum_{n\in\mathbb{N}} c_n(X,-(d-1)))t^n,$$

where

$$c_n(X,-(d-1)) = |\{(u_1,...,u_d) \in \mathcal{W}^d : I^X_{u_1,...,u_d} = \varnothing, \sum_{i=1}^{d} l(u_i) = n\}|.$$

REMARK. The elements of the set $\tilde{I}$ of $N_X(B)$-orbits in I are of the form $L = \{O_{i_1},...,O_{i_l}\}$ for some $l \in \{1,2,3\}$. In particular, we have that $|\Phi_{O_{i_{j_1}}}| = |\Phi_{O_{i_{j_2}}}|$, $|\Phi^+_{O_{i_{j_1}}}| = |\Phi^+_{O_{i_{j_2}}}|$ and $|\Phi^-_{O_{i_{j_1}}}| = |\Phi^-_{O_{i_{j_2}}}|$ for $j_1, j_2 \in \{1,..,l\}$. Thus, we can define

$l^X_{\mathcal{W}}$

$$l^X_{\mathcal{W}} = \sum_{L \in \tilde{I}} |\Phi^+_{O_L}|,$$

where O_L is an element of L, since the definition does not depend on the choice of O_L.

The following lemma shows that $c_n(X,-(d-1)) = 0$ for $n < l^X_{\mathcal{W}}$.

Lemma 5.5. *Let $u_1,...,u_d \in \mathcal{W}$. If $I^X_{u_1,...,u_d} = \varnothing$, then $\sum_{i=1}^{d} l(u_i) \geq l^X_{\mathcal{W}}$.*

Proof. Note that $I^X_{u_1,...,u_d} = \{K \in I : u_i(K^g) \subseteq \Phi^+ \forall i \in \{1,...,d\}, \forall g \in N_X(B)\}$. Assume that $I^X_{u_1,...,u_d} = \varnothing$ and let $L \in \tilde{I}$, i.e. L is a $N_X(B)$-orbit in I. Then there exists $i \in \{1,...,d\}$ and $O_L \in L$ such that $u_i(O_L) \subseteq \Phi^-$ and so $u_i(\Phi^+_{O_L}) \subseteq \Phi^-$. This implies that

$$\sum_{i=1}^{d} |\Phi^+_{O_L} \cap u_i^{-1}(\Phi^-)| \geq |\Phi^+_{O_L}|. \quad (\dagger_0)$$

Moreover we have

$$|\Phi^+ \cap u_i^{-1}(\Phi^-)| \geq \sum_{j=1}^{|I|} |\Phi^+_j \cap u_i^{-1}(\Phi^-)| \quad (\dagger_1)$$

for each $i \in \{1, ..., d\}$. Hence we get:

$$\begin{aligned}
\sum_{i=1}^{d} l(u_i) &= \sum_{i=1}^{d} |\Phi^+ \cap u_i^{-1}(\Phi^-)| \geq \\
&\geq \sum_{i=1}^{d} \sum_{j=1}^{|I|} |\Phi_j^+ \cap u_i^{-1}(\Phi^-)| = \\
&= \sum_{j=1}^{|I|} \sum_{i=1}^{d} |\Phi_j^+ \cap u_i^{-1}(\Phi^-)| = \\
&= \sum_{L \in \tilde{I}} \sum_{O \in L} \sum_{i=1}^{d} |\Phi_O^+ \cap u_i^{-1}(\Phi^-)| \geq \\
&\geq \sum_{L \in \tilde{I}} |\Phi_{O_L}^+| = l_{\mathcal{W}}^X.
\end{aligned}$$

This completes the proof. □

Proposition 5.6. *Let a be a positive integer. If $l_{\mathcal{W}}^X > a$, then $c_{l_{\mathcal{W}}^X + j}(X, -(d-1))$ is divisible by d for $j \in \{1, ..., a\}$.*

Proof. Let $U = \{(u_1, ..., u_d) \in \mathcal{W}^d : I^X_{u_1,...,u_d} = \varnothing \text{ and } \sum_{i=1}^{d} l(u_i) = l_{\mathcal{W}}^X + j\}$. Let ν be the permutation $(1...d)$. Let $\langle \nu \rangle$ be the subgroup of $\mathrm{Sym}_d = \mathrm{Sym}\{1, .., d\}$ generated by ν. Clearly $\langle \nu \rangle$ acts on U: if $\underline{u} = (u_1, ..., u_d) \in U$, then the action is given by $\underline{u}^\nu = (u_{\nu(1)}, ..., u_{\nu(d)})$. Fix $\underline{u} \in U$. In order to prove the lemma, we claim that the ν-orbit $[\underline{u}] = \{(u_{\nu^k(1)}, ..., u_{\nu^k(d)}) : k \in \mathbb{N}\}$ has d elements. Let σ be a permutation of the set $\{1, ..., d\}$ such that $u_i = u_{\sigma(i)}$ for each $i \in \{1, ..., d\}$ and $\sigma \in C_{\mathrm{Sym}_d}(\nu)$. Clearly $\mathrm{Stab}_{\langle \sigma \rangle}(i) = 1$, since if $\sigma(i) = i$, then $\sigma = 1$ because $\sigma \in C_{\mathrm{Sym}_d}(\nu)$. Hence the σ-orbit of i consists of $|\sigma|$ elements. Therefore, there exist $d/|\sigma|$ σ-orbits, and without loss of generality we may assume that the representatives of the orbits are $1, ..., d/|\sigma|$. So we have that $I^X_{u_1,...,u_{d/|\sigma|}} = I^X_{u_1,...,u_d} = \varnothing$. Hence, by definition of U and Lemma 5.5 we obtain

$$l_{\mathcal{W}}^X + j = \sum_{i=1}^{d} l(u_i) = \sum_{i=1}^{d/|\sigma|} |\sigma| l(u_i) = |\sigma| \sum_{i=1}^{d/|\sigma|} l(u_i) \geq |\sigma| l_{\mathcal{W}}^X.$$

Since $l_{\mathcal{W}}^X > a \geq j$, we have that $|\sigma| = 1$. This implies that the set $[\underline{u}] = \{(u_{\nu^k(1)}, ..., u_{\nu^k(d)}) : k \in \mathbb{N}\}$ consists of d elements and we get the claim. □

Proposition 5.7. *We have that*

$$c_{l^X_{\mathcal{W}}}(X, -(d-1)) = \sum_{i=1}^{o(I)} \tau^X_{\mathfrak{D}'}(i) d^i (d-1)^{o(I)-i},$$

where $\tau^X_{\mathfrak{D}'}(i)$ is defined in Step 3.

Proof. Let $u_1, ..., u_d \in \mathcal{W}$ such that $\sum_{i=1}^d l(u_i) = l^X_{\mathcal{W}}$ and $I^X_{u_1,...,u_d} = \varnothing$. As at the beginning of Lemma 5.5, for each $L \in \tilde{I}$ let $O_L \in L$ be such that there exists $i \in \{1, ..., d\}$ such that $u_i(\Phi^+_{O_L}) \subseteq \Phi^-$. Denote by $\hat{I}$ the set $\{O_L : L \in \tilde{I}\}$. Note that under our assumptions the last expression in the proof of the Lemma 5.5 holds with $=$ instead of $\geq$. This implies that the expressions $\dagger_0, \dagger_1$ become

$$\sum_{i=1}^{d} |\Phi^+_O \cap u_i^{-1}(\Phi^-)| = \begin{cases} |\Phi^+_{O_L}| & \text{if } O = O_L \\ 0 & \text{otherwise} \end{cases} \qquad (\dagger^*_0)$$

for each $L \in \tilde{I}$, and

$$|\Phi^+ \cap u_i^{-1}(\Phi^-)| = \sum_{j=1}^{k} |\Phi^+_j \cap u_i^{-1}(\Phi^-)| \quad (\dagger^*_1)$$

for each $i \in \{1, ..., d\}$.

We divide the proof in some steps.

Step 1. *The set $\{I^c_{u_1}, ..., I^c_{u_d}\}$ is a partition of $\hat{I} = \{O_L : L \in \tilde{I}\}$.*

Let $L \in \tilde{I}$. We have that there exists $i \in \{1, ...d\}$ such that $u_i(O_L) \subseteq \Phi^-$. By $(\dagger^*_0)$ there exists at most one $i \in \{1, ..., d\}$ such that $u_i(O_L) \subseteq \Phi^-$. So for each $L \in \tilde{I}$ there exists exactly one $i \in \{1, ..., d\}$ such that $u_i(O_L) \subseteq \Phi^-$.

Moreover, let $O \in L$ such that $O \neq O_L$. By $(\dagger^*_0)$ we have that $u_i(O) \subseteq \Phi^+$, hence $O \in I_{u_i}$ for each $i \in \{1, ..., d\}$. Thus we have the claim.

Step 2. *Let $u \in \{u_1, ..., u_d\}$. Let $i, j \in \{1, ..., |I|\}, i \neq j$. If $O_i, O_j \in I^c_u$, then O_i and O_j are not joined in the Dynkin diagram $\mathfrak{D}'$ of $\mathcal{W}$.*

By $(\dagger^*_1)$ we have that

$$\Phi^+ \cap u^{-1}(\Phi^-) = \cup_{j=1}^{|I|} (\Phi^+_j \cap u^{-1}(\Phi^-)).$$

Assume that $O_i, O_j \in I_u^c$. By contradiction, suppose that O_i and O_j are joined in $\mathfrak{D}'$. So, there exist $r \in O_i$ and $s \in O_j$ such that $4\frac{(r,s)^2}{(r,r)(s,s)} \neq 0$. In particular, this implies that $\frac{2(r,s)}{(r,r)} = -n$ for some $n \in \mathbb{N} - \{0\}$, such that $s, r+s, ..., nr+s \in \Phi$ (see [Car72, §3.3 and 3.4]). Now, by hypothesis, we have that $u(r) \in \Phi^-$ and $u(s) \in \Phi^-$, so $u(r+s) \in \Phi^-$. Hence, $r+s \in \Phi^+ \cap u^{-1}(\Phi^-) = \cup_{i=1}^{|I|}(\Phi_i^+ \cap u^{-1}(\Phi^+))$, thus $r+s \in \Phi_l^+$ for some $l \in \{1, ..., |I|\}$, a contradiction with $i \neq j$.

We need some more definition. Let J be a subset of I. Denote by $\mathfrak{D}'_J$ the subgraph of $\mathfrak{D}'$ obtained considering just the set of vertices J. Note that since $\mathfrak{D}'$ is a tree, then the connected components of $\mathfrak{D}'_J$ are trees. We say that a d-uples $(J_1, ..., J_d)$ is a *good d-partition of J* if the following hold:

- $\{J_1, ..., J_d\}$ is a partition of J,
- if $K_1 \in J_{i_1}, K_2 \in J_{i_2}$ and there is an edge between K_1 and K_2, then $i_1 = i_2$.

Let $\mathrm{par}(J)$ denote the set of good d-partitions of J. Finally, we say that $J \subseteq I$ is *well intersected* (briefly *w.i.*) if $|J \cap L| = 1$ for each $L \in \tilde{I}$

Note that by Step 1 and Step 2, we have that $(I_{u_1}^c, ..., I_{u_d}^c)$ is a good d-partition of $\hat{I}$. Moreover the set $\hat{I}$ is well intersected.

Step 3. *The set*

$$\mathrm{Par}^X(I) = \bigcup_{J \text{ } w.i.} \mathrm{par}(J)$$

has

$$\sum_{i=1}^{o(I)} \tau_{\mathfrak{D}'}^X(i) d^i (d-1)^{o(I)-i}$$

elements, where $\tau_{\mathfrak{D}'}^X(i)$ is the number of well intersected subset J of I such that $\mathfrak{D}'_J$ has i connected components. $\tau_{\mathfrak{D}'}^X(i)$

By Lemma 5.3, we have that $|\mathrm{par(J)}| = p(\mathfrak{D}'_J) = d^i(d-1)^{|J|-i}$, where i is the number of connected components of $\mathfrak{D}'_J$. If J is well intersected, then $|J| = |\tilde{I}| = o(I)$. The result follows.

STEP 4. *Let $u \in \{u_1, ..., u_d\}$. Denote by $\mathcal{I}_u$ the set of $i \in \{1, ..., |I|\}$ such that ω_i appears in each ω-factorization of u of minimal length. Let $\bar{\mathcal{I}}_u = \{j \in \{1, ..., |I|\} : O_j \in I_u^c\}$. We have that $\mathcal{I}_u = \bar{\mathcal{I}}_u$. Moreover, if $i \in \mathcal{I}_u$, then the factor w_i appears with multiplicity one in an ω-factorization of u of minimal length.*

Let $j \in \bar{\mathcal{I}}_u$, so $O_j \in I_u^c$. By Lemma 5.2 (2), we have that ω_j appears in each ω-factorization of u of minimal length. So $j \in \mathcal{I}_u$ and $\bar{\mathcal{I}}_u \subseteq \mathcal{I}_u$. Recall that $u(O_j) \subseteq \Phi^-$ if and only if $u(\Phi_j^+) \subseteq \Phi^-$. Hence, by $(\dagger_1^*)$, we have

$$l(u) = |\Phi^+ \cap u^{-1}(\Phi^-)| = \sum_{j \in \bar{\mathcal{I}}_u} |\Phi_j^+| \leq \sum_{j \in \mathcal{I}_u} |\Phi_j^+|.$$

Thus, to prove that $\bar{\mathcal{I}}_u \supseteq \mathcal{I}_u$ it is enough to show that

$$l(u) \geq \sum_{i \in \mathcal{I}_u} |\Phi_i^+|,$$

but this is clear by Lemma 5.2 (1). Moreover, we get $l(u) = \sum_{i \in \mathcal{I}_u} |\Phi_i^+|$. Hence, if $i \in \mathcal{I}_u$, then the factor w_i appears exactly once in an ω-factorization of u of minimal length.

STEP 5. *Let $u \in \{u_1, ..., u_d\}$. Let $i, j \in \mathcal{I}_u$. We have that ω_i and ω_j commute.*

Let $r \in O_i$ and $s \in O_j$. By Step 2, since $O_i, O_j \in I_u^c$, we have that O_i and O_j are not joined. So, in particular, $(r, s) = 0$. Thus w_r and w_s commutes. Since $\omega_i \in W_{O_i}$ and $\omega_j \in W_{O_j}$, we have $\omega_i \omega_j = \omega_j \omega_i$, as claimed.

Now we finish the proof of the proposition. Let U be the set of $(v_1, ..., v_d) \in \mathcal{W}^d$ such that $I^X_{v_1,...,v_d} = \varnothing$ and $\sum_{i=1}^d l(v_i) = l^X_{\mathcal{W}}$. Let $f : U \to \mathrm{Par}^X(I)$ be the map defined by $f(v_1, ..., v_d) = (I^c_{v_1}, ..., I^c_{v_d})$. By Step 3, in order to prove the proposition, it is enough to show that f is a bijection.

We claim that f is surjective. Let J be a well intersected subset of I and let $(J_1, ..., J_d)$ be a good d-partition of J. Since $J \subseteq I = \{O_1, ..., O_k\}$, where $k = |I|$, we let $i(J_l) = \{i \in \{1, ..., k\} : O_i \in J_l\}$ for $l \in \{1, ..., d\}$. Note that if $i, j \in i(J_l)$, then ω_i and ω_j commute, since O_i and O_j are not joined, being in the same member of a

good d-partition. So we let $v_l = \prod_{i \in i(J_l)} \omega_i$ and it is easy to see that $f(v_1, ..., v_d) = (J_1, ..., J_d)$, hence we have the claim.

Let us prove that f is injective. Let $(u_1, ...u_d), (v_1, ..., v_d) \in U$ and assume that $(I^c_{u_1}, ..., I^c_{u_d}) = (I^c_{v_1}, ..., I^c_{v_d})$. By Step 4, we have that $\mathcal{I}_{u_i} = \mathcal{I}_{v_i}$ for $i \in \{1, ...d\}$. So we have that an ω-factorization of minimal length of u_i has the same factors as an ω-factorization of minimal length of v_i, and each factor has multiplicity one in both the factorizations. By Step 5, these factors commutes, hence $u_i = v_i$ for $i \in \{1, ...d\}$. This ends the proof. □

5.2.1 The value of $l^X_{\mathcal{W}}$ and $\tau^X_{\mathfrak{D}'}(i)$ for an almost simple group X

In this section we calculate the explicit value of $l^X_{\mathcal{W}}$ and $\tau^X_{\mathfrak{D}'}(i)$ for the almost simple group X with socle S isomorphic to a simple group of Lie type. This values are given in the Table 5.1 and 5.2. In these tables we use the convention that $\binom{n}{k} = 0$ if $k < 0$ or $k > n$.

If S is an untwisted group, then ρ is trivial. Hence, the unique element of a ρ-orbit is a fundamental root. Thus, for each $i \in \{1, ..., k\}$, we have that $O_i = \{r_i\}$ where $\Pi = \{r_1, ..., r_k\}$. So, $\Phi^+_i = \Phi^+_{O_i} = \{r_i\}$.

Assume that the action of $N_X(B)$ on I is trivial (i.e. X does not contain non-trivial graph automorphisms). We have that $\tilde{I}$ is isomorphic to I as posets. Hence we get:

$$l^X_{\mathcal{W}} = \sum_{L \in \tilde{I}} |\Phi^+_{O_L}| = \sum_{i=1}^{|I|} |\Phi^+_i| = |I| = |\Pi|.$$

Moreover, I is the unique well intersected subset of $\tilde{I}$, so we obtain

$$\tau^X_{\mathfrak{D}'}(i) = \begin{cases} 1 & \text{if } i = 1, \\ 0 & \text{otherwise,} \end{cases}$$

since $\mathfrak{D}' = \mathfrak{D}'_I$ is connected. Hence we get

$$c_{l^X_{\mathcal{W}}}(X, -(d-1)) = d(d-1)^{|I|-1}.$$

Suppose that the action of $N_X(B)$ on I is not trivial (i.e. X does contains a non-trivial graph automorphism). Since Π is isomorphic to I as posets we have that $|\Phi^+_{O_L}| = 1$, hence we get:

$$l^X_{\mathcal{W}} = \sum_{L \in \tilde{I}} |\Phi^+_{O_L}| = |\tilde{I}| = o(I).$$

In order to compute $\tau^X_{\mathfrak{D}'}(i)$ we need some more attention. Note that $\mathfrak{D} = \mathfrak{D}'$.

For example, assume that $\mathfrak{D} = A_{2l}$ for some $l \geq 1$. In this case there exists a graph automorphism of order 2. We have to count the number of well intersected subsets J of I such that $\mathfrak{D}_J$ has i connected components. Note that each element $L \in \tilde{I}$ is of the form $L = \{\{r_j\}, \{r_{2l-j+1}\}\}$ where $j \in \{1, ..., l\}$. Moreover, the vertices r_i and r_j are joined in $\mathfrak{D}$ if and only if $|i - j| = 1$. An easy combinatoric argument shows that

$$\tau^X_{\mathfrak{D}'}(i) = 2\binom{l-1}{i-1}$$

for $1 \leq i \leq l$. The same result holds if $\mathfrak{D} = A_{2l+1}$ for some $l \geq 1$. Hence we get

$$c_{l^X_{\mathcal{W}}}(X, -(d-1)) = \sum_{i=1}^{l} \tau^X_{\mathfrak{D}'}(i) d^i (d-1)^{l-i} = \sum_{i=1}^{l} 2\binom{l-1}{i-1} d^i (d-1)^{l-i} = 2d(2d-1)^{l-1}.$$

Now, suppose S is a twisted group of Lie type. In this case the action of $N_X(B)$ on I is always trivial. Hence I and $\tilde{I}$ are isomorphic as posets, so we obtain

$$\tau^X_{\mathfrak{D}'}(i) = \begin{cases} 1 & \text{if } i = 1, \\ 0 & \text{otherwise,} \end{cases}$$

as above. Thus we get

$$c_{l^X_{\mathcal{W}}}(X, -(d-1)) = d(d-1)^{|I|-1}.$$

To get the value of $l^X_{\mathcal{W}}$, note that $\tilde{I}$ is isomorphic to I as posets. Hence we get:

$$l^X_{\mathcal{W}} = \sum_{L \in \tilde{I}} |\Phi^+_{O_L}| = \sum_{i=1}^{|I|} |\Phi^+_i|.$$

We need the following result.

Lemma 5.8 (See [Car72, §3.4 and 3.6]). *Let $r, s \in \Pi$ be two fundamental roots. Let $n_r = \frac{2(r,s)}{(r,r)}$, $n_s = \frac{2(s,r)}{(s,s)}$ and $n_{r,s} = n_r n_s$. Suppose that $n_r \leq n_s$. Exactly one of the following occurs.*

- *$n_{r,s} = 0$. We have that $n_r = n_s = 0$ and $\Phi^+_{\{r,s\}} = \{r, s\}$. In this case the roots are not joined in the Dynkin diagram $\mathfrak{D}$.*
- *$n_{r,s} = 1$. We have that $n_r = n_s = -1$ and $\Phi^+_{\{r,s\}} = \{r, s, r+s\}$.*
- *$n_{r,s} = 2$. We have that $n_r = -2, n_s = -1$ and $\Phi^+_{\{r,s\}} = \{r, s, r+s, 2r+s\}$.*
- *$n_{r,s} = 3$. We have that $n_r = -3, n_s = -1$ and $\Phi^+_{\{r,s\}} = \{r, s, r+s, 2r+s, 3r+s, 3r+2s\}$.*
- *$n_{r,s} = 4$. We have that $r = s$ and $\Phi^+_{\{r\}} = \{r\}$.*

We give some examples of the calculation of the value of $l^X_{\mathcal{W}}$. Let $\Pi = \{r_1, ..., r_l\}$. In the sequel, when we say that two roots are joined, we refer to Figure 5.1-5.4.

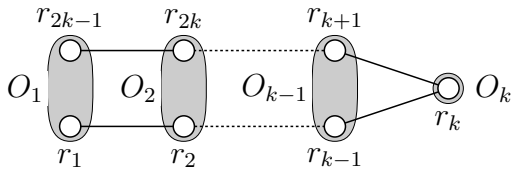
Case ${}^2A_l$.

We divide this case into two subcases, l odd and l even.

Suppose that l is odd. Thus the orbits are $O_i = \{r_i, r_{2k-i}\}$ for $i \in \{1, ..., k\}$, so that $l = 2k - 1$. Now, if $i < k$, then O_i consists of two roots which are not joined in $\mathfrak{D}$. So $O_i = \Phi^+_i$ for $i < k$. Moreover, $O_k = \{r_k\} = \Phi^+_k$. Hence, we have

$$l^X_{\mathcal{W}} = \sum_{i=1}^{k} |\Phi^+_i| = \sum_{i=1}^{k} |O_i| = 2k - 1 = l.$$

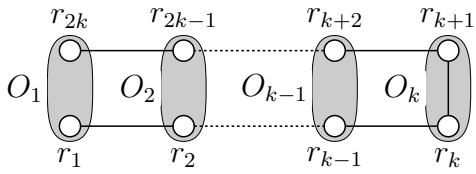
Figure 5.1: Dynkin diagram of A_{2k-1}



Suppose that l is even. Thus the orbits are $O_i = \{r_i, r_{2k+1-i}\}$ for $i \in \{1, ..., k\}$, so that $l = 2k$. As above, if $i < k$, then $O_i = \Phi_i$. Now, consider $O_k = \{r_k, r_{k+1}\}$. By [Car72, §3.6], we have that $n_{r_k, r_{k+1}} = 1$. Hence, by Lemma 5.8, $\Phi_k^+ = \{r_k, r_{k+1}, r_k + r_{k+1}\}$. Thus, we get

$$l_{\mathcal{W}}^X = \sum_{i=1}^{k} |\Phi_i^+| = \sum_{i=1}^{k-1} |O_i| + |\Phi_k^+| = 2(k-1) + 3 = l + 1.$$

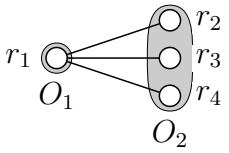
Figure 5.2: Dynkin diagram of A_{2k}



Case ${}^3D_4$**.**

In this case $k = 2$ and $O_1 = \{r_1\}$, $O_2 = \{r_2, r_3, r_4\}$. Clearly, $\Phi_1^+ = O_1$. Since r_2, r_3, r_4 are pairwise not joined in the Dynkin diagram $\mathfrak{D}$, we have that $\Phi_2^+ = O_2$. Thus, $l_{\mathcal{W}}^X = 4$.

Figure 5.3: Dynkin diagram of D_4



Case ${}^2G_2$**.**

In this case $k = 1$ and $O_1 = \{r_1, r_2\}$. Moreover, by [Car72, §3.6], we have $n_{r_1, r_2} = 3$. Thus, by Lemma 5.8, $\Phi_k^+ = \{r_1, r_2, r_1 + r_2, 2r_1 + r_2, 3r_1 + r_2, 3r_2 + 2r_2\}$. So, we get $l_{\mathcal{W}}^X = 6$.

Figure 5.4: Dynkin diagram of G_2

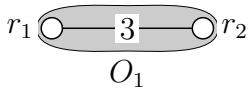


Table 5.1: Dynkin diagrams, fundamental roots and value of $l^X_{\mathcal{W}}$ when X does not contain non-trivial graph automorphisms

Untwisted				Twisted				
S	$\mathfrak{D} = \mathfrak{D}'$	$\lvert I\rvert$	$l^X_{\mathcal{W}}$	S	$\mathfrak{D}$	$\mathfrak{D}'$	$\lvert I\rvert$	$l^X_{\mathcal{W}}$
$A_k(t)$	A_k	k	k	${}^2A_{2k}(t^2)$	A_{2k}	B_k	k	$2k+1$
$B_k(t)$	B_k	k	k	${}^2A_{2k-1}(t^2)$	A_{2k-1}	C_k	k	$2k-1$
$C_k(t)$	C_k	k	k	${}^2B_2(t^2)$	B_2	A_1	1	4
$D_k(t)$	D_k	k	k	${}^2D_k(t^2)$	D_k	B_{k-1}	$k-1$	k
$E_6(t)$	E_6	6	6	${}^3D_4(t^3)$	D_4	G_2	2	4
$E_7(t)$	E_7	7	7	${}^2E_6(t^2)$	E_6	F_4	4	6
$E_8(t)$	E_8	8	8	${}^2F_4(t^2)$	F_4		2	6
$F_4(t)$	F_4	4	4	${}^2G_2(t^2)$	G_2	A_1	1	6
$G_2(t)$	G_2	2	2					

Table 5.2: Dynkin diagrams, values of $l^X_{\mathcal{W}}, \tau^X_{\mathfrak{D}'}$ and $c_{l^X_{\mathcal{W}}}(X, -(d-1))$ when X contains a non-trivial graph automorphism ρ.

S	$\lvert\rho\rvert$	$\mathfrak{D} = \mathfrak{D}'$	$l^X_{\mathcal{W}}$	$\tau^X_{\mathfrak{D}'}(i)$	$c_{l^X_{\mathcal{W}}}(X, -(d-1))$
$A_{2k}(t)$	2	A_{2k}	k	$2\binom{k-1}{i-1}$	$2d(2d-1)^{k-1}$
$A_{2k+1}(t)$	2	A_{2k+1}	$k+1$	$2\binom{k-1}{i-1}$	$2d(2d-1)^{k-1}$
$B_2(t)$	2	B_2	1	$2\binom{0}{i-1}$	$2d$
D_k	2	D_k	$k-1$	$2\binom{0}{i-1}$	$2d(d-1)^{k-2}$
$D_4(t)$	3	D_4	2	$3\binom{0}{i-1}$	$3d(d-1)$
$E_6(t)$	2	E_6	4	$2\binom{1}{i-1}$	$2d(d-1)^2(2d-1)$
$F_4(t)$	2	F_4	2	$2\binom{1}{i-1}$	$2d(2d-1)$
$G_2(t)$	2	G_2	1	$2\binom{0}{i-1}$	$2d$

5.2.2 The main result

Now, we can prove the main theorem.

Theorem 5.9. *Let X be an almost simple group with socle isomorphic to a simple group of Lie type of characteristic p over $\mathbb{K}$. We have that*

$$P^{(p)}_{X,S}(-(d-1)) = (-1)^{o(I)} \sum_{n\in\mathbb{N}} c_n(X, -(d-1))t^n$$

where $c_n(X,-(d-1)) = |\{(u_1,...,u_d) \in \mathcal{W}^d : I^X_{u_1,...,u_d} = \varnothing, \sum_{i=1}^d l(u_i) = n\}|$. In particular,

(1) if $n < l^X_{\mathcal{W}}$ or $n > d|\Phi^+|$, then $c_n(X,-(d-1)) = 0$,

(2) if X does not contain non-trivial graph automorphisms, then we have that

$$c_{l^X_{\mathcal{W}}}(X,-(d-1)) = d(d-1)^{|I|-1}.$$

If X contains a non-trivial graph automorphism, then $c_{l^X_{\mathcal{W}}}(X,-(d-1))$ is as in Table 5.2.

(3) $c_{l^X_{\mathcal{W}}+j}(X,-(d-1))$ is divisible by d for each positive integer $j < l^X_{\mathcal{W}}$.

Proof. The first assertion is Lemma 5.4.

Let $(u_1,...,u_d) \in \mathcal{W}^d$ such that $I^X_{u_1,...,u_d} = \varnothing$. Note that, if $w \in \mathcal{W}$, then $l(w) \leq |\Phi^+|$.

(1) By Lemma 5.5, if $n < l^X_{\mathcal{W}}$, then $c_n(X,-(d-1)) = 0$. Furthermore, $\sum_{i=1}^d l(u_i) \leq d|\Phi^+|$. Hence if $n > d|\Phi^+|$, then $c_n(X,-(d-1)) = 0$.

(2) This is Proposition 5.7 combined with the result of Subsection 5.2.1.

(3) This is Proposition 5.6.

This ends the proof. □

Proposition 5.10. *Let X be an almost simple group with socle S isomorphic to a simple group of Lie type of characteristic p over $\mathbb{K}$. If $N_G(X)$ acts transitively on I (i.e. $o(I) = 1$), then $|P^{(p)}_{X,S}(-(d-1))(t)|_p = |d|_p|\rho|_p t^{l^X_W}$, where ρ is a graph automorphism of largest order in X (see p.41 for the definition of graph automorphism).*

Proof. By Theorem 3.10 and Proposition 3.5, we have that

$$P^{(p)}_{X,S}(-(d-1))(t) = 1 - (1 + f(t))^d$$

for some function $f(t)$ such that $|f(t)|_p = |\rho|_p t^{l^X_{\mathcal{W}}}$. A direct computation shows that if $p = 2$, then $|f(t)|_2 \geq 4$. By Lemma 2.9, we have:

$$|P^{(p)}_{X,S}(-(d-1))(t)|_p = |d|_p|f(t)|_p = |d|_p|\rho|_p t^{l^X_W}$$

for each prime p. □

Proposition 5.11. *Let X be an almost simple group with socle S isomorphic to a simple group of Lie type of characteristic p over $\mathbb{K}$. Let $d > 1$ be a positive integer and suppose that $t|d|_p > |c_{l^X_{\mathcal{W}}}(X, -(d-1))|_p$ and $t^{l^X_{\mathcal{W}}-1} \geq |d|_p$. We have that*

$$|P^{(p)}_{X,S}(-(d-1))|_p = t^{l^X_{\mathcal{W}}}|c_{l^X_{\mathcal{W}}}(X, -(d-1))|_p.$$

Proof. If $l^X_{\mathcal{W}} > 1$, then applying Theorem 5.9 we get:

$$|P^{(p)}_{X,S}(-(d-1))|_p = \left|\sum_{n\in\mathbb{N}} c_n(X, -(d-1))t^n\right|_p = \left|\sum_{n=l^X_{\mathcal{W}}}^{d|\Phi^+|} c_n(X, -(d-1))t^n\right|_p =$$

$$= t^{l^X_{\mathcal{W}}}\left|c_{l^X_{\mathcal{W}}}(X, -(d-1)) + \sum_{n=l^X_{\mathcal{W}}+1}^{2l^X_{\mathcal{W}}-1} c_n(X, -(d-1))t^{n-l^X_{\mathcal{W}}} + \sum_{n=2l^X_{\mathcal{W}}}^{d|\Phi^+|} c_n(X, -(d-1))t^{n-l^X_{\mathcal{W}}}\right|_p.$$

By Theorem 5.9 we have that d divides $c_n(X, -(d-1))$ if $n \leq 2l^X_{\mathcal{W}} - 1$, hence $|c_n(X, -(d-1))t^{n-l^X_{\mathcal{W}}}|_p \geq t|d|_p > |c_{l^X_{\mathcal{W}}}(X, -(d-1))|_p$ for $n \leq 2l^X_{\mathcal{W}} - 1$ (by assumptions). Moreover, if $n \geq 2l^X_{\mathcal{W}}$, then $|c_n(X, -(d-1))t^{n-l^X_{\mathcal{W}}}|_p \geq t^{l^X_{\mathcal{W}}} \geq t|d|_p > |c_{l^X_{\mathcal{W}}}(X, -(d-1))|_p$ (by assumptions). Thus we get the claim.

Assume that $l^X_{\mathcal{W}} = 1$. In this case we have that $o(I) = 1$, so we can apply Proposition 5.10. $\square$

The condition $t|d|_p > |c_{l^X_{\mathcal{W}}}(X, -(d-1))|_p$ in the previous proposition is sufficient but not necessary. As we have seen in Proposition 5.10, we can drop the condition when $o(I) = 1$. However, it is not always true that $|P^{(p)}_{X,S}(-(d-1))|_p = t^{l^X_{\mathcal{W}}}|c_{l^X_{\mathcal{W}}}(X, -(d-1))|_p$. For example take $X = S = A_2(4)$: we have that $P^{(2)}_S(-(d-1)) = 1 - 2 \cdot 21^d + 105^d$ and $c_{l^S_{\mathcal{W}}}(S, -(d_i - 1)) = d(d-1)$.

Chapter 6

On some subgroups of X which do not contain a Sylow p-subgroup

In this chapter, let X be a classical projective group, as defined at p.32. Let S be the socle of X. Here we deal with the subgroups of X which do not contain a Sylow p-subgroup and which are intersection of maximal subgroups.

Recall that

$$\beta_p(X) = \log_q \min\{|X : H|_p : H < X, |X : H|_p > 1, HS = X, \mu_X(H) \neq 0\}.$$

We shall prove the following theorem.

Theorem 6.1. *Let X be a classical projective group of characteristic p and let S be its socle. Let $\tilde{\beta}_p(X)$ be as in Table 6.1 with the following exceptions:* $\tilde{\beta}_p(X)$

- *for $S = \mathrm{PSL}_2(q)$ we have $\tilde{\beta}_p(X) = \log_q p$;*
- *for $S = \mathrm{PSL}_3(q_0^2)$ we have $\tilde{\beta}_p(X) = 1.5$;*
- *for $S \in \{\mathrm{PSU}_4(q), \mathrm{PSL}_4(q)\}$, we have $\tilde{\beta}_p(X) = 2$.*

We have that $\beta_p(X) \geq \tilde{\beta}_p(X)$.

Table 6.1: Values of $\tilde{\beta}_p(X)$, given the socle S of X

S	$\tilde{\beta}_p(X)$
$\mathrm{PSL}_n(q)$	$n-1$
$\mathrm{PSU}_n(q)$	$n-1$
$\mathrm{PSp}_n(q)$	$\frac{n}{2} - \log_q \lvert 2\rvert_p$
$\mathrm{P}\Omega_n(q)$	$\frac{n-1}{2}$
$\mathrm{P}\Omega_n^{\pm}(q)$	$\frac{n-2}{2}$

The proof of this theorem is given in Theorem 6.2 and Proposition 6.18.

We divide the chapter into two sections. In the first section, we consider the subgroups which are intersection of maximal parabolic subgroups of X. In the second section we consider the maximal subgroups of X which are supplemented by S and which do not contain a Sylow p-subgroup of X.

6.1 On the intersection of maximal subgroups which contain a Sylow p-subgroup of X

The aim of this section is to prove the following.

Theorem 6.2. *Let X be a classical projective group with socle S and let H be a subgroup of X such that:*

- *$HS = X$,*
- *if M is a maximal subgroup of X and $M \geq H$, then M contains a Sylow p-subgroup of X.*
- *H does not contain a Sylow p-subgroup of X.*

$\beta(n)$ *Then $\mu_X(H) = 0$ or $|X : H|_p \geq q^{\beta(n)}$, where*

$$\beta(n) = \begin{cases} n-1 & \text{if case } \mathbf{L} \text{ or } \mathbf{U} \text{ hold,} \\ \frac{n}{2} - \log_q |2|_p & \text{if case } \mathbf{S} \text{ holds,} \\ \frac{n-1}{2} & \text{if case } \mathbf{O}^{\circ} \text{ holds,} \\ \frac{n-2}{2} & \text{if case } \mathbf{O}^{+} \text{ or } \mathbf{O}^{-} \text{ hold.} \end{cases}$$

In order to prove the above theorem, we investigate the structure of maximal subgroup in the class $\mathcal{C}_1(X)$, as described in [KL90]. In particular, we are interested to the maximal subgroups which contain a Sylow p-subgroup of X. In most cases, these subgroups are stabilizers of totally singular subspaces of V.

We recall some definition about the geometry of classical groups (see [KL90, p.16]). Let W be a subspace of V. We say that W is *totally singular* if the restriction κ_W of κ to W is equal to 0. We say that W is *non-degenerate* if κ_W is non-degenerate. Writing (v, w) instead of $\mathbf{f}(v, w)$, we denote by $W^{\perp}$ the set of $v \in V$ such that $(v, w) = 0$ for all $w \in W$.

κ_W

(v, w)

$W^{\perp}$

We need some preliminary technical lemmas.

Lemma 6.3 (See [KL90, Proposition 2.3.2, Proposition 2.4.1 and Proposition 2.5.3])**.** *The space (V, κ) has a basis :*

e_i, f_i, x, y, z

- $\{e_1, ...e_m\}$ *if* $n = m$ *and case* $\mathbf{L}$ *holds,*
- $\{e_1, ...e_m, f_1, ..., f_m\}$ *if* $n = 2m$ *and cases* $\mathbf{U}, \mathbf{O}^{+}$ *or* $\mathbf{S}$ *hold,*
- $\{e_1, ...e_m, f_1, ..., f_m, x\}$ *if* $n = 2m + 1$ *and cases* $\mathbf{U}$ *or* $\mathbf{O}^{\circ}$ *hold,*
- $\{e_1, ...e_m, f_1, ..., f_m, y, z\}$ *if* $n = 2m + 2$ *and case* $\mathbf{O}^{-}$ *holds.*

In all these cases we have $(e_i, e_j) = (f_i, f_j) = (e_i, x) = (f_i, x) = (e_i, y) = (f_i, y) = (e_i, z) = (f_i, z) = 0$ *and* $(e_i, f_j) = \delta_{ij}$ *for all* i, j*. Moreover,*

- *if case* $\mathbf{O}$ *holds, then* $Q(e_i) = Q(f_i) = 0$*,*
- *if case* $\mathbf{U}$ *holds, then* $(x, x) = 1$*,*
- *if case* $\mathbf{O}^{\circ}$ *holds, then* x *is non-singular,*

- *if case* $\mathbf{O}^-$ *holds, then* $Q(y) = 1, Q(z) = \zeta$ *and* $(y, z) = 1$*, where the polynomial* $X^2 + X + \zeta$ *is irreducible over* $\mathbb{F}$*.*

Lemma 6.4. *Let* m *as in the above lemma. Let* l *and* h *be two distinct integer numbers such that* $1 \leq l, h \leq m$*. There exists an element* $\phi_{l,h} \in S$ *such that:* $\phi_{l,h}$

(1) each subspace of $\langle e_1, ..., e_{l-1} \rangle$ *is stabilized by* $\phi_{l,h}$*,*

(2) each totally singular subspace of V *containing* $\langle e_h \rangle$ *is stabilized by* $\phi_{l,h}$*,*

(3) $\phi_{l,h}$ *does not stabilize a subspace of* V *containing* $\langle e_l \rangle$ *and not containing* $\langle e_h \rangle$*.*

Proof. Define a linear map $\phi = \phi_{l,h} : V \to V$ as follows:

- $\phi(e_l) = e_l + e_h$ and $\phi(e_i) = e_i$ for $i \neq l$,
- $\phi(f_h) = f_h - f_l$ and $\phi(f_i) = f_i$ for $i \neq h$,
- $\phi(x) = x, \phi(y) = y$ and $\phi(z) = z$ (when they occur).

Note that $\det(\phi) = 1$ and $\kappa(\phi(v)) = \kappa(v)$ for $v \in V^e$, where $e = 1$ if case **O** holds, $e = 2$ otherwise. Thus $(S(V, \kappa) \cap \mathbb{F}^*)\phi$ is an element of $\overline{S}(V, \kappa)$. Moreover, if case **O** holds, then it is easy to see that $(S(V, \kappa) \cap \mathbb{F}^*)\phi$ is a commutator in $\overline{S}(V, \kappa)$. Thus we let $\phi_{l,h} = (S(V, \kappa) \cap \mathbb{F}^*)\phi \in S$. Clearly (1) and (3) hold, so we prove only (2). Let U be a totally singular subspace of V such that $e_h \in U$. Let w be an element of U. Thus $w = \sum_{i=1}^{m} \alpha_i e_i + \sum_{i=1}^{m} \beta_i f_i + \gamma_x x + \gamma_y y + \gamma_z z$, for some $\alpha_i, \beta_i, \gamma_x, \gamma_y, \gamma_z \in \mathbb{F}_q$. Since U is totally singular, we have that $(w, e_h) = 0$, thus $\beta_h = 0$. Hence $\phi_{l,h}(w) = \alpha_l e_h + w$, so $\phi_{l,h}(w) \in U$ since $e_h \in U$. □

The following well-known facts about the spaces with forms will be use often without mention.

Lemma 6.5. *Let* κ *be a non-degenerate form and let* W *and* U *be two subspaces of* V*.*

(1) $W \leq U$ *if and only if* $U^\perp \leq W^\perp$*.*

(2) $(W+U)^\perp = W^\perp \cap U^\perp$.

(3) If W *is totally singular, then* $W \leq W^\perp$.

(4) If W *is totally singular and* $U \leq W^\perp$*, then* $U+W$ *is totally singular.*

(5) W *is non-degenerate if and only if* $W \cap W^\perp = 0$.

We introduce some definition and notation. Assume that H is as in Theorem 6.2. Let $\mathcal{M}_H(X)$ be the set of maximal subgroups M of X containing H and such that $MS = X$. We denote by $\mathcal{L}_H(X)$ the set $\mathcal{M}_H(X)$ $\mathcal{L}_H(X)$

$$\{W \leq V : \mathrm{Stab}_{X\cap\overline{\Gamma}}(W) \geq H \cap \overline{\Gamma}\}$$

and we let $\mathcal{L}_H^*(X) = \{W \in \mathcal{L}_H(X) : W \text{ is totally singular and } W \notin \{0, V\}\}$. It is $\mathcal{L}_H^*(X)$ clear that $\mathcal{L}_H^*(X) \subseteq \mathcal{L}_{S\cap H}^*(S)$ and $\mathcal{L}_{H\cap\overline{\Gamma}}^*(X \cap \overline{\Gamma}) = \mathcal{L}_H^*(X)$. Moreover, we have the following.

Proposition 6.6 (See [KL90, §4.1])**.** *Suppose that case* $\mathbf{O}^+$ *does not hold. Moreover, if case* $\mathbf{L}$ *holds, then assume* $X \leq \overline{\Gamma}$*. The map*

$$\mathrm{Stab}_X : \mathcal{L}_H^*(X) \to \mathcal{M}_H(X)$$

gives a one-to-one correspondence between $\mathcal{L}_H^*(X)$ *and* $\mathcal{M}_H(X)$*.*

We want to understand what happens in the case $\mathbf{L}$ and $X \not\leq \overline{\Gamma}$. Let ψ be an element of $\overline{A}-\overline{\Gamma}$. We have that ψ acts on the set $\mathrm{Sub}(V)$ of proper non-zero subspaces $\mathrm{Sub}(V)$ of V in the following way. Let $W \in \mathrm{Sub}(V)$, and note that $\mathrm{Stab}_S(W)^\psi$ is a maximal subgroup of S in the class $\mathcal{C}_1(S)$. Thus there exists a unique $U \in \mathrm{Sub}(V)$ such that $\mathrm{Stab}_S(U) = \mathrm{Stab}_S(W)^\psi$, so define $W^\psi = U$.

Suppose that H is as in the Theorem 6.2. Note that $H \cap (\overline{A} - \overline{\Gamma}) \neq \varnothing$, since otherwise $X = HG \leq \overline{\Gamma}$. Thus, we may assume that $\psi \in H \cap (\overline{A} - \overline{\Gamma})$. Note that if $W \in \mathcal{L}_H^*(X)$, then $W^\psi \in \mathcal{L}_H^*(X)$. Let $\mathcal{L}_H^*(X)/\psi$ be the set of equivalence classes of $\mathcal{L}_H^*(X)$ given the relation on $\mathcal{L}_H^*(X)$ such that W and U are equivalent if $W^\psi = U$. $\mathcal{L}_H^*(X)/\psi$

With the above notation, we obtain the following.

Proposition 6.7 (See [KL90, Proposition 4.1.23]). *Suppose that case* **L** *holds and* Ψ_H $X \not\leq \overline{\Gamma}$. *There is a one to one correspondence*

$$\Psi_H : \mathcal{L}_H^*(X)/\psi \to \mathcal{M}_H(X)$$

defined by $\Psi_H([W]) = N_X(\mathrm{Stab}_{X\cap\overline{\Gamma}}(W) \cap \mathrm{Stab}_{X\cap\overline{\Gamma}}(W^\psi))$ *where* $[W] = \{W, W^\psi\}$ *is the equivalence class of* $W \in \mathcal{L}_H^*(X)$. *Moreover*

$$\Psi_H([W]) \cap X \cap \overline{\Gamma} = \mathrm{Stab}_{X\cap\overline{\Gamma}}(W) \cap \mathrm{Stab}_{X\cap\overline{\Gamma}}(W^\psi).$$

$\mathcal{U}_k$ Now we turn to the case $\mathbf{O}^+$. As in [KL90, p.30], let $\mathcal{U}_k$ be the set of totally singular subspace of V of dimension k. Let $\sim$ be the relation on $\mathcal{U}_m$ defined by $W \sim U$ if $m - \dim(W \cap U)$ is even. This relation defines a partition $\{\mathcal{U}_m^1, \mathcal{U}_m^2\}$ of $\mathcal{U}_m$ γ and gives an homomorphism $\gamma : \overline{\Gamma} \to \mathrm{Sym}\{\mathcal{U}_m^1, \mathcal{U}_m^2\}$. In particular, $\mathcal{U}_m^1$ and $\mathcal{U}_m^2$ are the two S-orbits on $\mathcal{U}_m$.

We have the following.

Proposition 6.8 (See [KL90, Proposition 4.1.20 and Lemma 2.5.8]). *Suppose that case* $\mathbf{O}^+$ *holds. Let* $k = m - 1$ *if* $X \leq \ker(\gamma)$, *let* $k = m$ *otherwise. The map*

$$\mathrm{Stab}_X : \mathcal{L}_H^*(X) - \mathcal{U}_k \to \mathcal{M}_H(X)$$

is a one to one correspondence.

Now, we focus our attention to the set $\mathcal{L}_H(X)$. Observe that $\mathcal{L}_H(X)$ is a sublattice of the lattice of subspaces of V. In fact if U and W are subspaces of V, then $\mathrm{Stab}_{X\cap\overline{\Gamma}}(U) \cap \mathrm{Stab}_{X\cap\overline{\Gamma}}(W) \leq \mathrm{Stab}_{X\cap\overline{\Gamma}}(U + W) \cap \mathrm{Stab}_{X\cap\overline{\Gamma}}(U \cap W)$.

In general, the set $\mathcal{L}_H^*(X)$ is not a lattice. However, if $Z_1, Z_2 \in \mathcal{L}_H^*(X)$, then

- $Z_1 \cap Z_2 \in \mathcal{L}_H^*(X)$ if and only if $Z_1 \cap Z_2 > 0$;
- $Z_1 + Z_2 \in \mathcal{L}_H^*(X)$ if and only if there exists a totally singular proper subspace T of V such that $Z_1, Z_2 \leq T$.

Let $\mathcal{L}$ be a subset be of the set of vector subspaces of V.

$\mathcal{L}(+)$

- We denote by $\mathcal{L}(+)$ the subset of $\mathcal{L}$ consisting of the elements W such that there exist $Z_1, Z_2 \in \mathcal{L}$, with $Z_1 \neq W \neq Z_2$ and $W = Z_1 + Z_2$. Similarly, define $\mathcal{L}(\cap)$ as the subset of $\mathcal{L}$ consisting of the elements W such that there exist $Z_1, Z_2 \in \mathcal{L}$, with $Z_1 \neq W \neq Z_2$ and $W = Z_1 \cap Z_2$. $\mathcal{L}(\cap)$

- An element W of $\mathcal{L}$ is said to be **redundant in** $\mathcal{L}$ if for any $M \subseteq \mathcal{L}$ such that $W \in M$ and
$$\bigcap_{U \in M} \mathrm{Stab}_{X \cap \overline{\Gamma}}(U) = \bigcap_{U \in \mathcal{L}} \mathrm{Stab}_{X \cap \overline{\Gamma}}(U)$$
we have that
$$\bigcap_{U \in M - \{W\}} \mathrm{Stab}_{X \cap \overline{\Gamma}}(U) = \bigcap_{U \in \mathcal{L}} \mathrm{Stab}_{X \cap \overline{\Gamma}}(U).$$

- We say that $\mathcal{L}$ **fulfills the property** $\mathcal{P}$ if there exists $W \in \mathcal{L}$ such that for each $Z \in \mathcal{L}$ we have $W \leq Z$ or $W \geq Z$. In this case, W is said to be a $\mathcal{P}$**-element** of $\mathcal{L}$. $\mathcal{P}$ $\mathcal{P}$-element

We divide the rest of the section into two parts: $\mathcal{L}_H^*(X)$ fulfills the property $\mathcal{P}$ and $\mathcal{L}_H^*(X)$ does not fulfill the property $\mathcal{P}$.

6.1.1 $\mathcal{L}_H^*(X)$ fulfills the property $\mathcal{P}$

We consider the case when $\mathcal{L}_H^* = \mathcal{L}_H^*(X)$ fulfills the property $\mathcal{P}$. Our aim is to prove the following.

Proposition 6.9. *Let H be as in Theorem 6.2. Suppose that $\mathcal{L}_H^*$ fulfills the property $\mathcal{P}$. Then $\mu_X(H) = 0$.*

The proof of this proposition requires some preliminary results.

Proposition 6.10. *Let H be as in Theorem 6.2 and assume that H is an intersection of maximal subgroups of X. Suppose that W is a $\mathcal{P}$-element of $\mathcal{L}_H^*$ such that $W \in \mathcal{L}_H^*(+) \cup \mathcal{L}_H^*(\cap)$. Then W is redundant in $\mathcal{L}_H^*$.*

Proof. Since $\mathcal{L}^*_{H\cap\overline{\Gamma}}(X \cap \overline{\Gamma}) = \mathcal{L}^*_H(X)$, without loss of generality, we may assume that $X \leq \overline{\Gamma}$.

Suppose that M is a subset of $\mathcal{L}^*_H$ such that $W \in M$ and

$$\bigcap_{U\in M} \mathrm{Stab}_X(U) = \bigcap_{U\in\mathcal{L}^*_H} \mathrm{Stab}_X(U).$$

Note that

$$\bigcap_{U\in\mathcal{L}^*_H} \mathrm{Stab}_X(U) = H$$

by Proposition 6.6, 6.7 and 6.8.

For a contradiction, assume that

$$K = \bigcap_{U\in M-\{W\}} \mathrm{Stab}_X(U) > H.$$

Note that $M \subseteq \mathcal{L}^*_K \subset \mathcal{L}^*_H$ and W does not lie in $\mathcal{L}^*_K$. Moreover, W does not lie in the lattice $\mathcal{L}_K$.

We are going to consider two cases, namely $W \in \mathcal{L}^*_H(+)$ and $\mathcal{L}^*_H(+)$ does not contain $\mathcal{P}$-elements of $\mathcal{L}^*_H$.

Assume $W \in \mathcal{L}^*_H(+)$**.** Let T be the sum of the elements of $\mathcal{L}^*_K$ which are contained in W, i.e.

$$T = \sum_{U\in\mathcal{L}^*_K, U\leq W} U$$

(if for each $U \in \mathcal{L}^*_K$ we have $U \geq W$, then let $T = 0$). Clearly $T \leq W$ and since $W \notin \mathcal{L}^*_K$, then $T < W$. Since W is a $\mathcal{P}$-element, note that

$$\text{if } U \in \mathcal{L}^*_K, \text{ then } U \leq T \text{ or } U > W. \qquad (\dagger^1)$$

We claim that there exists an element

$$Y \text{ in } \mathcal{L}^*_H - \mathcal{L}^*_K, \text{ such that } Y < W \text{ and } Y \not\leq T. \qquad (\dagger^2)$$

Since $W \in \mathcal{L}^*_H(+)$, there exist $Z_1, Z_2 \in \mathcal{L}^*_H$ such that $Z_1 \neq W \neq Z_2$ and $Z_1 + Z_2 = W$. Since $W \notin \mathcal{L}_K$, we have that $Z_1 \notin \mathcal{L}^*_K$ or $Z_2 \notin \mathcal{L}^*_K$. Suppose that $Z_1, Z_2 \notin \mathcal{L}^*_K$. We

have that $T \ngeq Z_1$ or $T \ngeq Z_2$, otherwise $T \geq Z_1 + Z_2 = W$. So, in the case that $Z_1, Z_2 \notin \mathcal{L}_K^*$, let $Y \in \{Z_1, Z_2\}$ be such that $Y \nleq T$. Now, suppose that $Z_i \in \mathcal{L}_K^*$. Thus $Z_{2-i} \notin \mathcal{L}_K^*$ and so $T \ngeq Z_{2-i}$, otherwise $T = T + Z_i \geq Z_{2-i} + Z_i = W$. Hence, in the case that $Z_i \in \mathcal{L}_K^*$, set $Y = Z_{2-i}$.

Since W is totally singular, by Witt's Lemma ([KL90, Proposition 2.1.6]) we may assume that there exists $k \geq 2$ such that W has a basis $e_1, ..., e_k$ which is part of the standard basis given in Lemma 6.3. Moreover, by $(\dagger^2)$ and $T < W$, we may assume that there exist $0 \leq h \leq l < r \leq k$ such that $T \cap Y = \langle e_1, ..., e_h \rangle$, $T = \langle e_1, ..., e_l \rangle$, $Y = T \cap Y \oplus \langle e_{l+1}, ..., e_r \rangle$ and $k - r + l - h \geq 1$. Define an element $\phi \in S$ as follows (see Lemma 6.4):

- if $l > h$ (i.e. $T \cap Y < T$), then let $\phi = \phi_{l+1,l}$;
- if $l = h$ (i.e. $T \leq Y$, so $Y = T + Y < W$), then let $\phi = \phi_{l+1,r+1}$.

By Lemma 6.4, $(\dagger^1)$ and $(\dagger^2)$, we have that

$$\phi \in \bigcap_{U \in \mathcal{L}_K^*} \mathrm{Stab}_X(U) \cap \mathrm{Stab}_X(W) = H$$

and $\phi \notin \mathrm{Stab}_X(Y)$. This is in contradiction with $Y \in \mathcal{L}_H^*$.

Assume that $\mathcal{L}_H^*(+)$ does not contain $\mathcal{P}$-elements of $\mathcal{L}_H^*$. This implies that $W \in \mathcal{L}_H^*(\cap)$. If case **L** holds, then the proof is just the dual of the above case. So we assume that case **L** does not hold, so κ is a non-degenerate form.

Since $\mathcal{L}_H^*(+)$ does not contain $\mathcal{P}$-elements, we have that the elements of the set $\mathcal{N} = \{U \leq W : U \in \mathcal{L}_H^*\}$ form a chain of subspaces of V. In fact, for a contradiction suppose that the set $\mathcal{N}$ is not a chain. Thus there exists two elements $U_1, U_2 \in \mathcal{N}$ such that $U_1 \nleq U_2$ and $U_2 \nleq U_1$. Since $U_1, U_2 \leq W$, we get that $U_1 + U_2$ is totally singular, hence $U_1 + U_2 \in \mathcal{N}$. So $\mathcal{N}(+) \neq \varnothing$. Let A be a maximal element in $\mathcal{N}(+)$. It is straightforward to see that A is a $\mathcal{P}$-element of $\mathcal{N}$, hence it is a $\mathcal{P}$-element of $\mathcal{L}_H^*$, a contradiction. So, we have that $\mathcal{N} = \{U \leq W : U \in \mathcal{L}_H^*\}$ forms a chain of subspaces of V.

Note that if the elements of $\mathcal{L}_K^*$ form a chain of subspaces of V, then

$$\bigcap_{U \in \mathcal{L}_K^* \cup \{W\}} \mathrm{Stab}_S(U) = H \cap S$$

contains a Sylow p-subgroup of S (see [KL90, Corollary 4.1.15]). Hence H contains a Sylow p-subgroup of X, against the assumptions. We deduce that the set $\{U \geq W : U \in \mathcal{L}_K^*\}$ is not empty and it is not a chain. Let T be the intersection of the elements of $\mathcal{L}_K^*$ which contain W, i.e.

$$T = \bigcap_{U \in \mathcal{L}_K^*, U \geq W} U.$$

We have that $T \geq W$ and since $W \notin \mathcal{L}_K^*$, then $T > W$. Moreover, since W is a $\mathcal{P}$-element,

$$\text{if } U \in \mathcal{L}_K^*, \text{ then } U \geq T \text{ or } U < W. \qquad (\dagger^3)$$

Arguing as for $(\dagger^2)$, there exists an element

$$Y \text{ in } \mathcal{L}_H^* - \mathcal{L}_K^*, \text{ such that } Y > W \text{ and } Y \ngeq T. \qquad (\dagger^4)$$

We divide the rest of the proof in three cases, namely case $Y \cap T > W$, case $Y \cap T = W$ and $Y \cap T^\perp \nleq T$, case $Y \cap T = W$ and $Y \cap T^\perp \leq T$.

Suppose that $Y \cap T > W$. As above, since T is totally singular, we may assume that there exists $k \geq 2$ such that T has a basis $e_1, ..., e_k$ which is part of the standard basis given in Lemma 6.3. Moreover, by $(\dagger^4)$ we may assume that there exist $0 < h < l < k$ such that $W = \langle e_1, ..., e_h \rangle$ and $Y \cap T = \langle e_1, ..., e_l \rangle$. Let $\phi = \phi_{h+1,l+1}$ as in the Lemma 6.4. By Lemma 6.4, $(\dagger^3)$ and $(\dagger^4)$, we have that

$$\phi \in \bigcap_{U \in \mathcal{L}_K^*} \mathrm{Stab}_X(U) \cap \mathrm{Stab}_X(W) = H$$

and $\phi \notin \mathrm{Stab}_X(Y)$. This is in contradiction with $Y \in \mathcal{L}_H^*$.

Suppose that $Y \cap T = W$ *and* $Y \cap T^\perp \nleq T$. Thus pick an element v in $Y \cap T^\perp - T$. Clearly, we have that $T + \langle v \rangle$ is a totally singular subspace of V. As above, we may assume that there exists $k \geq 2$ such that T has a basis $e_1, ..., e_{k-1}$ and $v = e_k$.

Moreover, by $(\dagger^4)$ and $T > W$, we may assume that there exists $0 < l < k-1$ such that $W = \langle e_1, ..., e_l \rangle$. Let $\phi = \phi_{k,k-1}$ as in the Lemma 6.4. By Lemma 6.4, $(\dagger^3)$ and $(\dagger^4)$, we have that

$$\phi \in \bigcap_{U \in \mathcal{L}_K^*} \mathrm{Stab}_X(U) \cap \mathrm{Stab}_X(W) = H$$

and $\phi \notin \mathrm{Stab}_X(Y)$. This is in contradiction with $Y \in \mathcal{L}_H^*$.

Finally, assume that $Y \cap T = W$ *and* $Y \cap T^\perp \leq T$. Since in this case $Y \not\leq T^\perp$, we have that $T \not\leq Y^\perp$, so $T \cap Y^\perp < T$. Since $T \cap Y^\perp \in \mathcal{L}_H^* - \mathcal{L}_K^*$, if $T \cap Y^\perp > W$, then we argue as in the case $Y < T$ with $Y = T \cap Y^\perp$. Thus we can assume that $T \cap Y^\perp = W$. Now, since κ is non-degenerate, $T \cap Y^\perp = W$ implies $T^\perp + Y = W^\perp$. Let M be a maximal totally singular subspace of V containing T. Since $\mathcal{L}_K^*$ is not a chain, then $M > T$. Since M is totally singular, we may assume that M has a basis $e_1, ..., e_m$ which is part of the standard basis given in Lemma 6.3. Moreover, we may assume that there exists $0 < l < k < m$ such that $W = \langle e_1, ..., e_l \rangle$ and $T = \langle e_1, ..., e_k \rangle$. Let $\phi = \phi_{m,k}$ as in the Lemma 6.4. Clearly, by Lemma 6.4 and $(\dagger^3)$, we have that

$$\phi \in \bigcap_{U \in \mathcal{L}_K^*} \mathrm{Stab}_X(U) \cap \mathrm{Stab}_X(W) = H.$$

Since $Y \in \mathcal{L}_H^*$, we have that ϕ stabilizes Y. Note that $f_k \in W^\perp = T^\perp + Y$ and $(v, e_k) = 0$ for each $v \in T^\perp$. Thus there exist $v_1 \in Y$ and $v_2 \in T^\perp$ such that $v_1 + v_2 = f_k$, with $v_1 = \sum_{i=1}^m \alpha_i e_i + \sum_{i=1}^m \beta_i f_i + \gamma_x x + \gamma_y y + \gamma_z z$ and $\beta_k \neq 0$. This yields $\phi(v_1) - v_1 = \alpha_m e_k - \beta_k f_m$. Thus we have $\alpha_m e_k - \beta_k f_m \in Y \cap T^\perp \leq T$, a contradiction since $\beta_k \neq 0$. Hence we obtain $\phi \notin \mathrm{Stab}_X(Y)$, a contradiction. □

In the following lemma we show that if $\mathcal{L}^*$ is not a chain and $\mathcal{L}^*$ fulfills the property $\mathcal{P}$, then the assumptions of the previous proposition are satisfied.

Lemma 6.11. *Assume that the elements of* $\mathcal{L}^* = \mathcal{L}_H^*(X)$ *do not form a chain of subspaces of* V. *Suppose that* $\mathcal{L}^*$ *fulfills the property* $\mathcal{P}$. *Then there exists a redundant element in* $\mathcal{L}^*$.

Proof. Let T be a $\mathcal{P}$-element in $\mathcal{L}^*$. Since $\mathcal{L}^*$ is not a chain, there exist $U_1, U_2 \in \mathcal{L}^*$

such that $U_1 \not\leq U_2$ and $U_1 \not\geq U_2$. Hence there are elements of $\mathcal{L}^*$ which are not $\mathcal{P}$-elements.

Assume that U_1 is contained in T. Let C be the sum of the elements of $\mathcal{L}^*$ which are properly contained in T and which are not $\mathcal{P}$-elements in $\mathcal{L}^*$ (this set is not empty, since it contains U_1). By definition we have that $C \in \mathcal{L}^*$. We want to prove that C is a $\mathcal{P}$-element in $\mathcal{L}^*$. Let $Z \in \mathcal{L}^*$. Since T is a $\mathcal{P}$-element, we have $Z \leq T$ or $Z \geq T$. If $Z \geq T$, then $Z \geq T \geq C$. Assume that $Z < T$. If Z is a $\mathcal{P}$-element in $\mathcal{L}^*$, then $C \leq Z$ or $C \geq Z$. If Z is not a $\mathcal{P}$-element in $\mathcal{L}^*$, then $C \geq Z$ by definition of C. Thus C is a $\mathcal{P}$-element in $\mathcal{L}^*$. This implies also that $C \in \mathcal{L}^*(+)$ (using the definition of C). So we apply Proposition 6.10 and we obtain the claim.

If U_1 contains T, the proof is just the dual (take C to be the intersection of the elements of $\mathcal{L}^*$ which properly contain T and which are not $\mathcal{P}$-elements in $\mathcal{L}^*$). $\square$

Now we are ready to prove Proposition 6.9 in the case $X \leq \overline{\Gamma}$.

Proof of Proposition 6.9 (Case $X \leq \overline{\Gamma}$). If H is not an intersection of maximal subgroups of X, then $\mu_X(H) = 0$. So suppose H is an intersection of maximal subgroups. The elements of $\mathcal{L}^*$ do not form a chain of subspaces of V (i.e., a flag) since H does not contain a Sylow p-subgroup of X (see [KL90, Corollary 4.1.15(i)]). So we may apply Lemma 6.11.

By Lemma 6.11, there exists an element $T \in \mathcal{L}^*$ such that T is a redundant element. Let $\mathcal{M} = \{\mathrm{Stab}_X(W) : W \in \mathcal{L}^*\}$. By Proposition 6.6 and 6.8, we have that $\mathcal{M} \supseteq \mathcal{M}_H(X)$. Define

$$\overline{\mathcal{Y}} = \{J \subseteq \mathcal{M} : \bigcap_{M \in J} M = H\}.$$

By [Sta97, Corollary 3.9.4], we have that

$$\mu_S(H) = \sum_{K \in \overline{\mathcal{Y}}} (-1)^{|K|}.$$

Now, let

$$\mathcal{Y} = \{K \subseteq \mathcal{L}^* : \bigcap_{W \in K} \mathrm{Stab}_S(W) = H\},$$
$$\mathcal{Y}_T = \{K \subseteq \mathcal{L}^* : \bigcap_{W \in K} \mathrm{Stab}_S(W) = H, T \in K\} \quad \text{and}$$
$$\mathcal{Y}'_T = \{K \subseteq \mathcal{L}^* : \bigcap_{W \in K} \mathrm{Stab}_S(W) = H, T \notin K\}.$$

Since T is a redundant element we have $\mathcal{Y}'_T = \{K - \{T\} : K \in \mathcal{Y}_T\}$. Since the map

$$\mathrm{Stab}_X : \mathcal{L}^* \to \mathcal{M}$$

is a bijection, the map $\Theta : \mathcal{Y} \to \overline{\mathcal{Y}}$ defined by $\Theta(K) = \{\mathrm{Stab}_X(W) : W \in K\}$ is a bijection and $|K| = |\Theta(K)|$. Thus, we obtain

$$\begin{aligned}
\mu_X(H) &= \sum_{J \in \overline{\mathcal{Y}}} (-1)^{|J|} = \sum_{K \in \mathcal{Y}} (-1)^{|K|} = \\
&= \sum_{K \in \mathcal{Y}_T} (-1)^{|K|} + \sum_{K \in \mathcal{Y}'_T} (-1)^{|K|} = \\
&= \sum_{K \in \mathcal{Y}_T} (-1)^{|K|} + \sum_{K \in \mathcal{Y}_T} (-1)^{|K|-1} = \\
&= \sum_{K \in \mathcal{Y}_T} (-1)^{|K|} - \sum_{K \in \mathcal{Y}_T} (-1)^{|K|} = 0.
\end{aligned}$$

So the proof is complete. □

Now, we assume that $X \not\leq \overline{\Gamma}$. So, we are in the case **L**. We need the following lemma. Recall that the action of ψ on $\mathrm{Sub}(V)$ is defined before Proposition 6.7.

Lemma 6.12. *Let W and Z be two elements of $\mathrm{Sub}(V)$ and let $\psi \in \overline{A} - \overline{\Gamma}$. We have that $(Z \cap W)^\psi = Z^\psi + W^\psi$ and $(Z + W)^\psi = Z^\psi \cap W^\psi$.*

Proof. The result is clear if ψ is the inverse transpose map ι (as described, for example, in [KL90, (2.2.4)]). Since $\iota^2 = 1$ and $\langle \overline{\Gamma}, \iota \rangle = \overline{A}$, if $\psi \in \overline{A} - \overline{\Gamma}$, then $\psi = g\iota$ for some $g \in \overline{\Gamma}$. Clearly g acts on $\mathrm{Sub}(V)$, and we have that $(Z \cap W)^g = Z^g \cap W^g$ and $(Z + W)^g = Z^g + W^g$. This concludes the prove. □

Now we are ready to complete the proof of Proposition 6.9.

Proof of Proposition 6.9 (Case $X \not\leq \overline{\Gamma}$). Denote by $\mathcal{L}$ the set $\mathcal{L}_H(X)$, let $\mathcal{L}^* = \mathcal{L}^*_H(X)$ and $\mathcal{L}^*/\psi = \mathcal{L}^*_H(X)/\psi$.

As in the previous proof, we may assume that H is an intersection of maximal subgroups and the elements of $\mathcal{L}$ do not form a chain. So we may apply Lemma 6.11. In particular, there exists a $\mathcal{P}$-element T in $\mathcal{L}^*$ such that $T \in \mathcal{L}(+) \cup \mathcal{L}(\cap)$. Using Lemma 6.12, we have that ψ induces an isomorphism of lattices between $(\mathcal{L}^*, +, \cap)$ and $(\mathcal{L}^*, \cap, +)$. Thus we have that T^ψ is a $\mathcal{P}$-element in $\mathcal{L}^*$ and $T^\psi \in \mathcal{L}(+) \cup \mathcal{L}(\cap)$.

Suppose that $M \subseteq \mathcal{L}^*/\psi$, $[T] = \{T, T^\psi\} \in M$ and

$$\bigcap_{[U]\in M} \Psi_H([U]) = \bigcap_{U\in\mathcal{L}^*/\psi} \Psi_H([U]) = H.$$

We claim that

$$\bigcap_{[U]\in M-\{[T]\}} \Psi_H([U]) = H.$$

Clearly we have that

$$\bigcap_{[U]\in M} \Psi_H([U]) \cap X \cap \overline{\Gamma} = \bigcap_{[U]\in M} \mathrm{Stab}_{X\cap\overline{\Gamma}}(U) \cap \mathrm{Stab}_{X\cap\overline{\Gamma}}(U^\psi) = H \cap \overline{\Gamma}.$$

Now, since by Proposition 6.10 we have that T and T^ψ are redundant elements, we obtain

$$\bigcap_{[U]\in M-\{[T]\}} \mathrm{Stab}_{X\cap\overline{\Gamma}}(U) \cap \mathrm{Stab}_{X\cap\overline{\Gamma}}(U^\psi) = H \cap \overline{\Gamma},$$

i.e.

$$\bigcap_{[U]\in M-\{[T]\}} \Psi_H([U]) \cap X \cap \overline{\Gamma} = H \cap \overline{\Gamma}. \quad (\dagger)$$

Let $K = \bigcap_{[U]\in M-\{[T]\}} \Psi_H([U])$. Thus $(\dagger)$ means $K \cap \overline{\Gamma} = H \cap \overline{\Gamma}$. Clearly $K \geq H$, so $\overline{\Gamma}K = X$ and thus $|K : K \cap X \cap \overline{\Gamma}| = |K : H \cap \overline{\Gamma}| = 2$. Moreover, $|H : H \cap \overline{\Gamma}| = 2$. Hence we conclude that $K = H$ and we have the claim.

Arguing as in the proof of Proposition 6.9 (case $X \not\leq \overline{\Gamma}$), we obtain that $\mu_X(H) = 0$. $\square$

6.1.2 $\mathcal{L}_H^*(X)$ does not fulfill the property $\mathcal{P}$

Now, we consider the case when $\mathcal{L}_H^* = \mathcal{L}_H^*(X)$ does not fulfill the property $\mathcal{P}$. Thanks to the following lemma, we can restrict our attention to $\mathcal{L}_{H\cap S}^*(S)$.

Lemma 6.13. *Suppose that $\mathcal{L}_H^*(X)$ is not empty and $\mathcal{L}_H^*(X)$ does not fulfill the property $\mathcal{P}$. Then also $\mathcal{L}_{H\cap S}^*(S)$ is not empty and $\mathcal{L}_{H\cap S}^*(S)$ does not fulfill the property $\mathcal{P}$.*

Remind that $\mathcal{L}_H^*(X) \subseteq \mathcal{L}_{H\cap S}^*(S)$. For a contradiction, assume that there exists a $\mathcal{P}$-element Z in $\mathcal{L}_{H\cap S}^*(S)$. Since $\mathcal{L}_H^*(X)$ does not fulfill the property $\mathcal{P}$, there exists T_1 and T_2 distinct maximal elements of $\mathcal{L}_H^*(X)$. If Z contains T_1 and T_2, then $Z \geq T_1 + T_2$, a contradiction since Z is totally singular and $T_1 + T_2 \notin \mathcal{L}_H^*(X)$. So suppose that Z does not contain T_1. Since Z is a $\mathcal{P}$-element in $\mathcal{L}_{H\cap S}^*(S)$, we have that $Z \leq T_1$. So the set consisting of the elements U of $\mathcal{L}_H^*(X)$ such that $U \geq Z$ is not empty. Thus define

$$B = \bigcap_{U\in\mathcal{L}_H^*(X), U\geq Z} U.$$

We claim that B is a $\mathcal{P}$-element in $\mathcal{L}_H^*(X)$. Let $W \in \mathcal{L}_H^*(X)$. If $W \leq Z$, then $W \leq B$ by definition of B. If $W \geq Z$, then $W \geq B$ again by definition of B. Thus B is a $\mathcal{P}$-element in $\mathcal{L}_H^*(X)$, a contradiction. □

Recall that $I = I(V,\kappa) = \{\phi \in \mathrm{GL}(V) : \kappa(\phi(v)) = \kappa(v) \text{ for all } v \in V^l\}$ where $l = 1$ if κ is quadratic, $l = 2$ otherwise. Clearly S is a section of I.

Suppose that W is a totally singular subspace of V. The form κ induces a form $\kappa_{W^\perp/W}$ on $W^\perp/W$. Moreover, $\kappa_{W^\perp/W}$ is a zero, unitary, symplectic or orthogonal form according to whether κ is zero, unitary, symplectic or orthogonal (see [KL90, p.17-18]). $\kappa_{W^\perp/W}$

We introduce some useful definitions.

- Denote by $I^{(W)}$ the group $I(W^\perp/W, \kappa_{W^\perp/W})$. $I^{(W)}$
- If $W \in \mathcal{L}_H^*(X) \cup \{0\}$, then denote by $\mathcal{L}_H^{(W)}$ the set of element $U \in \mathcal{L}_H^*(X)$ $\mathcal{L}_H^{(W)}$

such that $W < U < W^\perp$. Note that $\mathcal{L}_H^{(0)} = \mathcal{L}_H^*$. Moreover, if $U \in \mathcal{L}_H^{(W)}$, then U/W is a totally singular subspace of $W^\perp/W$ (with respect to the induced form $\kappa_{W^\perp/W}$).

Let $W \in \mathcal{L}_H^*(X)$. Suppose that ϕ is an element of $\mathrm{Stab}_I(W)$. Thus ϕ induces an
$\phi^{(W)}$ element $\phi^{(W)}$ of $I^{(W)}$, defined by $\phi^{(W)}(v+W) = \phi(v) + W$ for $v \in W^\perp$.

Now, assume that ϕ is an element of

$$\bigcap_{U \in \mathcal{L}_H^*(X)} \mathrm{Stab}_I(U).$$

This yields $\phi^{(W)}$ is an element of

$$\bigcap_{U \in \mathcal{L}_H^{(W)}} \mathrm{Stab}_{I^{(W)}}(U/W).$$

Now we give a more concrete representation of ϕ using the matrices. The case **L** is trivial, so we assume that case **L** does not hold. Since W is totally singular, by Witt's Lemma ([KL90, Proposition 2.1.6]) we may assume that there exists $k \geq 1$ such that $W = \langle e_1, ..., e_k \rangle$ (see Lemma 6.3 for the notation). The matrix of a generic element of I in the basis $\mathcal{B}$ obtained juxtaposing the bases $\mathcal{B}_1 = (e_1, ..., e_k)$, $\mathcal{B}_2 = (e_{k+1}, ..., e_m)$, $\mathcal{B}_3 = (f_{k+1}, ..., f_m)$, $\mathcal{B}_4 = (x, y, z)$ and $\mathcal{B}_5 = (f_1, ..., f_k)$ is

$$M = \begin{pmatrix} M_{11} & M_{12} & M_{13} & M_{14} & M_{15} \\ M_{21} & M_{22} & M_{23} & M_{24} & M_{25} \\ M_{31} & M_{32} & M_{33} & M_{34} & M_{35} \\ M_{41} & M_{42} & M_{43} & M_{44} & M_{45} \\ M_{51} & M_{52} & M_{53} & M_{54} & M_{55} \end{pmatrix}$$

where M_{ij} is a matrix with respect to the basis $\mathcal{B}_i$ and $\mathcal{B}_j$ with coefficient in $\mathbb{F} = \mathbb{F}_{q^u}$. Consider an element $\phi \in \mathrm{Stab}_I(W)$, and let M be its matrix. It is clear that $M_{21} =$

$M_{31} = M_{41} = M_{51} = M_{52} = M_{53} = M_{54} = 0$. Let

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

be the matrix of the form $\mathbf{f}$ associated to κ, where D is a suitable matrix with coefficients in $\mathbb{F}$ and $a = 1$ if case $\mathbf{S}$ holds, $a = 0$ otherwise. . Since $\phi \in I$, we have that $MFM^{\alpha t} = F$, where α is the automorphism of $\mathbb{F}_{q^u}$ defined by $\lambda^\alpha = \lambda^q$ (see [KL90, Lemma 2.1.8]). Moreover, if $\kappa = Q$ is quadratic, then we require that $Q(\phi(v)) = Q(v)$ for all $v \in V$. This yields the following facts:

(1) The element $\phi^{(W)}$ of $I^{(W)}$ has matrix

$$M' = \begin{pmatrix} M_{22} & M_{23} & M_{24} \\ M_{32} & M_{33} & M_{34} \\ M_{42} & M_{43} & M_{44} \end{pmatrix}$$

with respect to the basis obtained juxtaposing the bases $(e_{k+1} + W, ..., e_m + W), (f_{k+1} + W, ..., f_m + W)$ and $(x + W, y + W, z + W)$. In particular, M' is invertible.

(2) $M_{55} = M_{11}^{-\alpha t}$.

(3)

$$\begin{pmatrix} M_{25} \\ M_{35} \\ M_{45} \end{pmatrix} = - \begin{pmatrix} (-1)^a M_{22} & M_{23} & M_{24} \\ (-1)^a M_{32} & M_{33} & M_{34} \\ M_{42} & M_{43} & M_{44} \end{pmatrix} \begin{pmatrix} M_{13}^{\alpha t} \\ M_{12}^{\alpha t} \\ D^{\alpha t} M_{14}^{\alpha t} \end{pmatrix} M_{11}^{-\alpha t}.$$

(4) $M_{15} M_{11}^{\alpha t} + (-1)^a M_{11} M_{15}^{\alpha t} = -M_{13} M_{12}^{\alpha t} - (-1)^a M_{12} M_{13}^{\alpha t} - M_{14} D M_{14}^{\alpha t}$.

(5) If case $\mathbf{O}^+$ or $\mathbf{O}^-$ hold, then by $Q(\phi(f_i)) = Q(f_i) = 0$ for $i \in \{1, ..., k\}$, we obtain

$$M_{15}^t M_{55}(i,i) = -(M_{25}^t M_{35}(i,i) + M_{45}(1,i) M_{45}(2,i) + M_{45}(1,i)^2 + \zeta M_{45}(2,i)^2)$$

We summarize the above discussion in the following lemma.

Lemma 6.14. *Let $\mathcal{B}$ be the base of V and let M be the matrix defined above. An element ϕ of $\mathrm{Stab}_I(W)$ is completely determined if we give:*

- *an element ψ of $I^{(W)}$, which has a matrix M' as above;*
- *the matrices $M_{11} \in \mathrm{GL}_k(\mathbb{F}_{q^u}), M_{12} \in \mathrm{M}_{k,m-k}(\mathbb{F}_{q^u}), M_{13} \in \mathrm{M}_{k,m-k}(\mathbb{F}_{q^u})$ and $M_{14} \in \mathrm{M}_{k,n-2m}(\mathbb{F}_{q^u})$;*
- *the elements $B(i,j) \in \mathbb{F}_{q^u}$ for $1 \leq i \leq j \leq k$, which are components of the matrix $B = M_{11}^{-1}M_{15}$. The element $B(i,i)$ satisfies $B(i,i)^\alpha + (-1)^a B(i,i) = b$ for some b determined by $M_{11}, M_{12}, M_{13}, M_{14}$ for $i \in \{1,...,k\}$. Moreover, if case $\mathbf{O}^+$ or $\mathbf{O}^-$ hold, then $B(i,i)$ is determined by $M', M_{11}, M_{12}, M_{13}, M_{14}$ for $i \in \{1,...,k\}$.*

Proof. As we have seen in the above discussion, if we give $M', M_{11}, M_{12}, M_{13}, M_{14}$ and M_{15}, then ϕ is completely determined. By (4) above we get:

$$\begin{aligned} B + (-1)^a B^{\alpha t} &= M_{11}^{-1}M_{15} + (-1)^a M_{15}^{\alpha t} M_{11}^{-\alpha t} = \\ &= -M_{11}^{-1}(M_{12}M_{13}^{\alpha t} + (-1)^a M_{13}M_{12}^{\alpha t} + M_{14}D^{\alpha t}M_{14}^{\alpha t})M_{11}^{-\alpha t}. \end{aligned}$$

Note that $B + (-1)^a B^{\alpha t}$ is completely determined by $M_{11}, M_{12}, M_{13}, M_{14}$. So it is enough to prove that if we give $B + (-1)^a B^{\alpha t}$ and $B(i,j)$ for $1 \leq i \leq j \leq k$, then B is completely determined. Assume that $B + (-1)^a B^{\alpha t}$ is given. Thus $B(j,i) + (-1)^a B(i,j)^\alpha = b_{i,j}$ for some $b_{i,j}$ fixed, with $1 \leq i \leq j \leq k$. Clearly, we have that $B(j,i) = b_{i,j} - (-1)^a B(i,j)^\alpha$ is determined.

Note that for $i \in \{1,...,k\}$ the element $B(i,i)$ satisfies the equation $B(i,i) + (-1)^a B(i,i)^\alpha = b_{i,i}$. Assume that case $\mathbf{O}^+$ or $\mathbf{O}^-$ hold. Therefore $\alpha = 1$, so by (5) above we have

$$B(i,i) = M_{11}^{-1}M_{15}(i,i) = M_{55}^t M_{15}(i,i) = M_{15}^t M_{55}(i,i).$$

Thus $B(i,i)$ is completely determined by the knowledge of $M', M_{11}, M_{12}, M_{13}$ and M_{14}. $\square$

Proposition 6.15. *Let W be an element of $\mathcal{L}_H^*(X)$. Suppose that $\mathcal{L}_H^{(W)} \neq \varnothing$ and $\mathcal{L}_H^{(W)}$ does not fulfill the property $\mathcal{P}$. Then one of the following holds:*

(1) There exist U and T in $\mathcal{L}_H^*$ such that $U + T = W^\perp$ and $U \cap T = W$.

(2) There exists $U \in \mathcal{L}_H - \{W, W^\perp\}$ such that $U^\perp + U = W^\perp$ and $U^\perp \cap U = W$.

(3) There exist $T \in \mathcal{L}_H^{(W)}$ and $U \in \mathcal{L}_H^{(W)}$ such that $U \cap T = W$, $\mathcal{L}_H^{(T)} \neq \varnothing$ and $\mathcal{L}_H^{(T)}$ does not fulfill the property $\mathcal{P}$.

Proof. Since $\mathcal{L}_H^{(W)} \neq \varnothing$ and $\mathcal{L}_H^{(W)}$ does not fulfill the property $\mathcal{P}$, there exist M_1 and M_2 distinct maximal elements in $\mathcal{L}_H^{(W)}$. Note that $\mathcal{L}_H^{(M_1 \cap M_2)}$ is non empty. We claim that $\mathcal{L}_H^{(M_1 \cap M_2)}$ does not fulfill $\mathcal{P}$. By contradiction, if Z is a $\mathcal{P}$-element in $\mathcal{L}_H^{(M_1 \cap M_2)}$, since M_1 and M_2 are maximal, then $Z \leq M_1$ and $Z \leq M_2$. So $Z \leq M_1 \cap M_2$, a contradiction with $Z \in \mathcal{L}_H^{(M_1 \cap M_2)}$.

Assume $M_1 \cap M_2 > W$. Consider the set

$$\mathcal{M} = \{Z \in \mathcal{L}_H^{(W)} : Z \leq M_1 \cap M_2, \mathcal{L}_H^{(Z)} \text{ does not fulfill } \mathcal{P}\}.$$

Let T be a minimal element in $\mathcal{M}$. Since $\mathcal{L}_H^{(M_1 \cap M_2)}$ is non empty, also $\mathcal{L}_H^{(T)}$ is not empty. Since $T \in \mathcal{L}_H^{(W)}$ and $\mathcal{L}_H^{(W)}$ does not fulfill the property $\mathcal{P}$, there exists $U \in \mathcal{L}_H^{(W)}$ such that $U \cap T < T$. For a contradiction, assume that $U \cap T > W$. Then $U \cap T \in \mathcal{L}_H^{(W)}$ and we have that $\mathcal{L}_H^{(U \cap T)}$ is not empty. Since $U \cap T < T$ and T is minimal in $\mathcal{M}$, we have that $\mathcal{L}_H^{(U \cap T)}$ fulfills $\mathcal{P}$. Thus there exists a $\mathcal{P}$-element Z in $\mathcal{L}_H^{(U \cap T)}$. Since $\mathcal{L}_H^{(T)} \subseteq \mathcal{L}_H^{(U \cap T)}$ and $\mathcal{L}_H^{(T)}$ does not fulfill $\mathcal{P}$, we have that $Z \leq T$. If $Z \leq U$, then $Z \leq U \cap T$, a contradiction with $Z \in \mathcal{L}_H^{(U \cap T)}$. If $Z \geq U$, then $U \leq T$, a contradiction. So we obtain $U \cap T = W$ and (3) holds.

Assume $M_1 \cap M_2 = W$. Suppose that $M_1 + M_2 = W^\perp$. Then (1) holds with $U = M_1$ and $T = M_2$. Now, suppose that $U = M_1 + M_2 < W^\perp$. Clearly case **L** does not hold. The subspace $U \cap U^\perp$ is a totally singular element of $\mathcal{L}_H$. We claim that $U \cap U^\perp = W$. For a contradiction, suppose that $U \cap U^\perp > W$. Without loss of generality, we may assume that $M_1 \not\geq U \cap U^\perp$. Now, $U \cap U^\perp \leq M_1^\perp$, so

$M_1 + U \cap U^\perp$ is an element of $\mathcal{L}_H^{(W)}$. This contradicts the maximality of M_1. Thus we have $U \cap U^\perp = W$, so $U^\perp + U = W^\perp$. Hence (2) holds. □

Let W be an element of $\mathcal{L}_H^* \cup \{0\}$. Suppose that $d = \dim W^\perp/W$. Recall that
$H_{I^{(W)}}$ $I^{(W)} = I(W^\perp/W, \kappa_{W^\perp/W})$. Let

$$H_{I^{(W)}} = \bigcap_{U \in \mathcal{L}_H^{(W)}} \mathrm{Stab}_{I^{(W)}}(U).$$

We have the following.

Proposition 6.16. *If $\mathcal{L}_H^{(W)}$ is not empty and $\mathcal{L}_H^{(W)}$ does not fulfill the property $\mathcal{P}$, then*

$$|I^{(W)} : H_{I^{(W)}}|_p \geq q^{\beta'(d)},$$

where

$$\beta'(d) = \begin{cases} d-1 & \text{if case } \mathbf{L} \text{ or } \mathbf{U} \text{ hold,} \\ \frac{d}{2} - \log_q |2|_p & \text{if case } \mathbf{S} \text{ holds,} \\ \frac{d-1}{2} & \text{if case } \mathbf{O}^\circ \text{ holds,} \\ \frac{d-2}{2} + \log_q |2|_p & \text{if case } \mathbf{O}^+ \text{ or } \mathbf{O}^- \text{ hold.} \end{cases}$$

Proof. Without loss of generality, we assume that $W = 0$. Let $I = I^{(0)}$ and $H_I = H_{I^{(0)}}$. Recall that n is the dimension of V. Since $\mathcal{L}_H^*$ is not empty, then $n \geq 2$ and Proposition 6.15 applies. In Table 6.2 we report the p-part of the order of I (see [KL90, p.19]).

Table 6.2: p-part of the order of I

Case	$\log_q \lvert I \rvert_p$	Conditions
$\mathbf{L}, \mathbf{U}$	$\frac{n(n-1)}{2}$	
$\mathbf{S}$	$\frac{n^2}{4}$	n even
$\mathbf{O}^\circ$	$\frac{(n-1)^2}{4}$	qn odd
$\mathbf{O}^\pm$	$\frac{n(n-2)}{4} + \log_q \lvert 2 \rvert_p$	n even

In order to prove the proposition, we argue by induction on n.

Case (1). *Assume that there exist U and T in $\mathcal{L}_H^*$ such that $U+T=V$ and $U\cap T=0$.* If case **L** holds, then $\mathrm{Stab}_I(T)\cap\mathrm{Stab}_I(U)$ is isomorphic to $\mathrm{GL}_{n_1}(q)\times\mathrm{GL}_{n_2}(q)$, where $n_1=\dim T$ and $n_2=\dim U$, and so

$$\log_q|I:H_I|_p\geq\frac{n(n-1)}{2}-\left(\frac{n_1(n_1-1)}{2}+\frac{n_2(n_2-1)}{2}\right)\geq n-1.$$

If case **L** does not hold, then T and U are maximal totally singular subspaces of V, so $\dim T=\dim U=n/2$. In particular n is even. By Witt's Lemma ([KL90, Proposition 2.1.6]) we may assume that $T=\langle e_1,...,e_m\rangle$ and $U=\langle f_1,...,f_m\rangle$ (see Lemma 6.3 for the notation). By [KL90, Lemma 4.1.9], we have that $\mathrm{Stab}_I(T)\cap\mathrm{Stab}_I(U)$ is isomorphic to $\mathrm{GL}_{n/2}(q^u)$. Thus we have that

$$\log_q|I:H_I|_p\geq\log_q|I|_p-\frac{nu(n-2)}{8}\geq\beta'(n)$$

for $n\geq 2$.

Case (2). *Assume that there exists $U\in\mathcal{L}_H-\{0,V\}$ such that $U^\perp+U=V$ and $U^\perp\cap U=0$.* Clearly, case **L** does not hold. So κ is non-degenerate, and thus U is non-degenerate. Let $k=\dim U$. By [KL90, §4.1], we obtain Table 6.3. Thus it is easy to see that

$$\log_q|I:H_I|_p\geq\log_q|I:\mathrm{Stab}_I(U)|_p\geq\beta'(n)$$

for $n\geq 2$ and $n>k$.

Table 6.3: p-part of the order $M=\mathrm{Stab}_I(U)$, where U is a non-degenerate proper subspace of V and $\dim U=k$

Case	Type of M	$\log_q\lvert M\rvert_p$	Conditions
U	$\mathrm{GU}_k(q)\perp\mathrm{GU}_{n-k}(q)$	$\frac{k(k-1)+(n-k)(n-k-1)}{2}$	
S	$\mathrm{Sp}_k(q)\perp\mathrm{Sp}_{n-k}(q)$	$\frac{k^2+(n-k)^2}{4}$	k even
$\mathbf{O}^\circ$	$\mathrm{O}^\circ_k(q)\perp\mathrm{O}^\pm_{n-k}(q)$	$\frac{(k-1)^2+(n-k)(n-k-2)}{4}$	k odd
$\mathbf{O}^\pm$	$\mathrm{O}^\pm_k(q)\perp\mathrm{O}^\pm_{n-k}(q)$	$\frac{k(k-2)+(n-k)(n-k-2)}{4}+\log_q\lvert 2\rvert_p$	k even
$\mathbf{O}^\pm$	$\mathrm{O}^o_k(q)\perp\mathrm{O}^o_{n-k}(q)$	$\frac{(k-1)^2+(n-k-1)^2}{4}$	k odd, q odd

Assume that **Case (1)** *and* **Case (2)** *do not hold.* By Proposition 6.15, there exist $T \in \mathcal{L}_H^*$ and $U \in \mathcal{L}_H^*$ such that $U \cap T = 0$, $\mathcal{L}_H^{(T)} \neq \varnothing$ and $\mathcal{L}_H^{(T)}$ does not fulfill the property $\mathcal{P}$.

Assume case **L** holds. Let $T = \langle e_1, ..., e_k \rangle$ and $U = \langle e_{k+1}, ..., e_h \rangle$, for some $k+1 \leq h \leq m = n$. In the basis $e_1, ..., e_n$ the generic matrix of an element of H_I is of the form

$$\begin{pmatrix} \mathrm{GL}(T) & \mathbb{O} & \mathrm{M}_{k\times(n-h)}(\mathbb{F}_q) \\ \mathbb{O} & & H_{I^{(T)}} \\ \mathbb{O} & & \end{pmatrix}.$$

Thus we have that

$$\log_q |H_I|_p \leq \log_q \left(|H_{I^{(T)}}|_p |\mathrm{M}_{k\times(n-h)}(\mathbb{F}_q)|_p |\mathrm{GL}(T)|_p \right) \leq \log_q |H_{I^{(T)}}|_p + k(n-h) + \frac{k(k-1)}{2}$$

This yields

$$\log_q |I : H_I|_p \geq \log_q |I : I^{(T)}|_p + \log_q |I^{(T)} : H_{I^{(T)}}|_p - k(n-h) - \frac{k(k-1)}{2}.$$

Since $\dim V/T < n$, by induction we have that

$$\log_q |I^{(T)} : H_{I^{(T)}}|_p \geq \beta'(\dim V/T) = \beta'(n-k) = n-k-1,$$

so we obtain

$$\begin{aligned} \log_q |I : H_I|_p &\geq \frac{n(n-1)}{2} - \frac{(n-k)(n-k-1)}{2} + n - k - 1 - k(n-h) - \frac{k(k-1)}{2} \\ &\geq n - 1 + k(h-k-1) \\ &\geq n - 1. \end{aligned}$$

The last inequality holds since $k \geq 1$ and $h \geq k+1$.

Assume case **L** does not hold. Assume that $U \cap T^\perp > 0$. Thus there exists $v \in U$ such that $v \in T^\perp$. By Witt's Lemma ([KL90, Proposition 2.1.6]) we may assume that $T = \langle e_1, ..., e_k \rangle$ and $v = e_{k+1}$. Let ϕ be an element of H_I. We have that $\phi(e_{k+1}) = \phi(v) \notin T$ since $U \cap T = 0$. Using the notation of Lemma 6.14, we have that the first column of M_{12} consists of zeros. By Lemma 6.14, to completely determine ϕ it is enough to give:

- $M_{11} \in \mathrm{GL}_k(q^u)$ ($q^{\frac{uk(k-1)}{2}} \prod_{i=1}^{k}(q^{ui}-1)$ choices);
- $M_{12} \in \mathrm{M}_{k,m-k}(\mathbb{F}_{q^u})$ with the first column filled with zeros ($q^{uk(m-k-1)}$ choices);
- $M_{13} \in \mathrm{M}_{k,m-k}(\mathbb{F}_{q^u})$ ($q^{uk(m-k)}$ choices for M_{13});
- $M_{14} \in \mathrm{M}_{k,n-2m}(\mathbb{F}_{q^u})$ ($q^{uk(n-2m)}$ choices for M_{14});
- $B(i,j) \in \mathbb{F}_{q^u}$ for $1 \leq i < j \leq k$ ($q^{\frac{uk(k-1)}{2}}$ choices);
- $B(i,i) \in \mathbb{F}_q$ for $i \in \{1,...,k\}$ and we have $q^{\lambda k}$ choices, where

$$\lambda = \begin{cases} 1 & \text{if } u = 2 \text{ or case } \mathbf{S} \text{ holds,} \\ 0 & \text{otherwise;} \end{cases}$$

- an element ψ of $H_{I^{(T)}}$, ($|H_{I^{(T)}}|$ choices).

So we get that

$$\log_q |H_I|_p \leq uk(n-2-k) + \lambda k + \log_q |H_{I^{(T)}}|_p.$$

This yields

$$\log_q |I : H_I|_p \geq \log_q |I : I^{(T)}|_p + \log_q |I^{(T)} : H_{I^{(T)}}|_p - uk(n-2-k) - \lambda k. \quad (*)$$

Since $\dim T^\perp/T < n$, by induction we have that

$$\log_q |I^{(T)} : H_{I^{(T)}}|_p \geq \beta'(\dim(T^\perp/T)) = \beta'(n-2k),$$

so it is easy to see that

$$\log_q |I : H_I|_p \geq \log_q |I : I^{(T)}|_p + \beta'(n-2k) - uk(n-2-k) - \lambda k = \beta'(n).$$

In the rest of the proof we show that we can always reduce to the case $U \cap T^\perp > 0$.

Assume that $U \cap T^\perp = 0$. Let $R = (U+T) \cap (U+T)^\perp = (U+T) \cap U^\perp \cap T^\perp$. We claim that $R \in \mathcal{L}_H^*$. By contradiction, suppose that $R \notin \mathcal{L}_H^*$. Since $R = (U+T) \cap (U+T)^\perp$

is totally singular and $R \notin \mathcal{L}_H^*$, we must have that $R = 0$. But this is a contradiction since **Case (2)** does not hold. So we have the claim. In particular, $R > 0$.

Assume that $R \cap T > 0$. Thus $R \cap T \in \mathcal{L}_H^*$. Since $\mathcal{L}_H^{(T)} \subseteq \mathcal{L}_H^{(R\cap T)}$, the set $\mathcal{L}_H^{(R\cap T)}$ is not empty. We claim that $\mathcal{L}_H^{(R\cap T)}$ does not fulfill the property $\mathcal{P}$. For a contradiction, assume that Z is a $\mathcal{P}$-element in $\mathcal{L}_H^{(R\cap T)}$. If $Z \geq T$, then $Z \in \mathcal{L}_H^{(T)}$, but $\mathcal{L}_H^{(T)}$ does not contain $\mathcal{P}$-elements. So $Z < T$. Since $R \leq U^\perp$, then $R + U \in \mathcal{L}_H^{(R\cap T)}$. Since $R + U \not\leq T$ and Z is a $\mathcal{P}$-element such that $Z < T$, then $Z < R + U$. So $Z \leq (R+U) \cap T \leq U^\perp \cap T \leq R \cap T$, a a contradiction. Since $R \cap T \in \mathcal{L}_H^*$, $U \in \mathcal{L}_H^*$, $U \leq (R \cap T)^\perp$, $U \cap R = 0$, $\mathcal{L}_H^{(R)}$ is not empty and $\mathcal{L}_H^{(R)}$ does not fulfill $\mathcal{P}$, without loss of generality we may assume that $R \cap T = T$ and argue as in the case $U \cap T^\perp > 0$.

Assume that $R \cap T = 0$. Since $R, T \in \mathcal{L}_H^*$, $R \leq T^\perp$, $R \cap T = 0$, $\mathcal{L}_H^{(T)}$ is not empty and $\mathcal{L}_H^{(T)}$ does not fulfill $\mathcal{P}$, without loss of generality we may assume that $R = U$ and argue as in the case $U \cap T^\perp > 0$.

The proof is finished. □

Theorem 6.17. *Let H be as in the Theorem 6.2. Suppose that $\mathcal{L}_H^*(X)$ is not empty and $\mathcal{L}_H^*(X)$ does not fulfill the property $\mathcal{P}$. Thus $|X : H|_p \geq q^{\beta(n)}$.*

Proof. Since $HG = X$, we have that $|X : H|_p = |S : H \cap S|_p$. By the previous proposition, we know that $|I : H_I|_p \geq q^{\beta'(d)}$, where $I = I(V, \kappa)$. Note that $F^* \leq H_I$, since a scalar matrix stabilizes each subspace. Let $R = S(V, \kappa)$. By [KL90, Table 2.1.C], we have that $|I : S|_p = 1$. Thus $|R : H_I \cap R|_p = |I : H_I|_p$. Now, $|\mathbb{F}^*|_p = 1$, so

$$\left|\overline{R} : \overline{R \cap H_I}\right|_p = |R : R \cap H_I|_p.$$

If case **O** does not hold, then $S = \overline{R}$. Since in this case $S \cap H = \overline{R \cap H_I}$, we have the claim. If case **O** holds, then $|\overline{R} : S| = 2$, so we have that $2|S : H \cap S|_p \geq |R : R \cap H_I|_p \geq q^{\beta'(n)}$. Thus $|S : H \cap S|_p \geq q^{\beta'(n) - \log_q |2|_p} = q^{\beta(n)}$. □

6.2 Indexes of subgroups of X which are contained in a maximal subgroup that does not contain a Sylow p-subgroup of X

The main task of this section is to prove the following.

Proposition 6.18. *Let X be a classical projective group. Let M be maximal subgroup of X such that $MS = X$ and M does not contain a Sylow p-subgroup of X. Then $\log_q |X : M|_p \geq \tilde{\beta}_p(X)$, where $\tilde{\beta}_p(X)$ is as in Theorem 6.1.*

Proof. If Case $\mathbf{L}, n = 2$ holds, then the result follows by [Hup67, p. 213].

Suppose that M is as in the statement. Suppose that M is a member of one of the classes $\mathcal{C}_1(X), ..., \mathcal{C}_8(X)$. By [KL90, Proposition 3.1.3], the group $M \cap S$ is a member of the classes $\mathcal{C}_1(S), ..., \mathcal{C}_8(S)$, or $X \not\leq \overline{\Gamma}$ (so that case $\mathbf{L}$ holds) and one of the following holds:

- $M \cap S$ is isomorphic to a subgroup of $C_2 \times S_n$, n is even and $q = 2$,
- $M \cap S$ is isomorphic to a subgroup of Alt_4 and $(n, q) = (5, 2)$,
- $M \cap S$ is isomorphic to a subgroup of $3^2.Q_8$ and $(n, q) = (3, 4)$,
- $M \cap S$ is isomorphic to a subgroup of $2^3.S_4.S_3$ and $(n, q) = (4, 3)$.

Using the results of [KL90] on the geometric subgroups a direct calculations show that if M is a member of one of the classes $\mathcal{C}_1(X), ..., \mathcal{C}_8(X)$, then the proposition holds.

If M does not lie in one of the classes $\mathcal{C}_1(X), ..., \mathcal{C}_8(X)$, then M is a member of the class $\mathcal{S}(X)$ (by Theorem 3.11). Let R be the socle of M. Since M lies in $\mathcal{S}$, the group R is non-abelian simple. We claim that $R \leq S$. In fact, $R \cap S$ is a normal subgroup of R. Hence $R \cap S = 1$ or $R \leq S$. For a contradiction, suppose that $R \cap S = 1$. Thus R is isomorphic to a subgroup of X/S, a contradiction, since X/S is soluble. So we

obtain the claim. In particular, if M is a member of the class $\mathcal{S}(X)$, then $M \cap S$ is a member of the class $\mathcal{S}(S)$.

By Theorem 3.12, we get that either R is in Table 3.3 or $|M| < q^{u(2n+4)}$. Assume that n is at least $8, 13, 12$ and 13 in the cases **L**, **U**, **S** and **O** respectively. An easy check shows that the proposition holds.

Assume that $n = 3$ and case **L** or **U** hold. By Table 3.4, it is straightforward to see that the proposition holds.

Throughout the rest of the proof, assume that if case **L** or **U** hold, then $n \geq 4$. Using [CCN$^+$85], it is easy to see that the proposition holds in the following cases:

- Case **L**, $(n, q) \in \{(4, 2), (5, 2)\}$.
- Case **U**, $(n, q) \in \{(4, 2), (5, 2)\}$.
- Case **S**, $(n, q) \in \{(4, 3), (4, 4), (6, 2), (8, 2)\}$.
- Case **O**, $(n, q) = (7, 3)$.
- Case **O**$^+$, $(n, q) = (8, 2)$.
- Case **O**$^-$, $(n, q) = (8, 2)$.

Recall the definition of the class $\mathcal{S}$ (see Theorem 3.11). In particular, if M lies in $\mathcal{S}$, then there exists an absolutely irreducible representation $\rho : L \to \mathrm{GL}(V)$ such that $\overline{\rho(L)} = R$, where L is the full covering of S.

Suppose that R is not a group of Lie type of characteristic p.

Using Tables 3.15 and 3.16, we find a lower bound of $|X : M|_p$, (the ratio $|G|_p/|\mathrm{Aut}(S)|_p$). It turns out that this lower bound is smaller than $q^{\tilde{\beta}_p(X)}$ in the following cases:

- Case **L**, $(n, q) \in \{(4, 2), (5, 2)\}$.
- Case **U**, $(n, q) \in \{(4, 2), (5, 2)\}$.
- Case **S**, $(n, q) \in \{(4, 4), (6, 2)\}$.

- Case $\mathbf{O}^{\pm}$, $(n, q) \in \{(8, 2)\}$.

Note that the cases above have been already considered.

Assume that R is a group of Lie type of characteristic p over $\mathbb{F}_r$. Again, using Tables 3.17 and 3.18, we find that the lower bound of $|X : M|_p$ (the ratio $|G|_p/|\mathrm{Aut}(S)|_p$) is greater that or equal to $q^{\tilde{\beta}_p(X)}$. In particular, when case $\mathbf{O}^{\mathrm{o}}$ holds for $n = 7$ we have that there can be a maximal subgroup M in $\mathcal{S}$ with socle isomorphic to $G_2(q)$, but it turns out that $M \cong G_2(q)$ (see [Kle87]), hence the result holds. Similarly, when case $\mathbf{O}^{\pm}$ holds for $n = 8$, we have that there can be a maximal subgroup M in $\mathcal{S}$ with socle R isomorphic to $\mathrm{PSp}_6(q)$ or $\mathrm{P}\Omega_7(q)$, but it turns out that $M = R$ (see [LPS90, p. 32, Table $\mathcal{G}$] and [Kle87]) hence the result holds. The proof is finished. $\square$

Chapter 7

Proof of the Main Theorem

This chapter is devoted to the proof of the main theorem of the present part. The following statement is the most general result we were able to obtain, so in order to state it we need a lot of assumptions. However, note that if G is a classical group which does not contain non-trivial graph automorphisms, then the assumptions are fulfilled.

Theorem 7.1. *Let G be a finite group. Let $\mathcal{A}$ be the set of representatives of the G-equivalence classes of chief factors of G. Let $A \in \mathcal{A}$ and denote by L_A the monolithic primitive group associated with A. Assume that for each $A \in \mathcal{A}$ exactly one of the following holds:*

- *A is abelian;*
- *$X_A = N_{L_A}(A)/C_{L_A}(A)$ is a projective classical group over the field $\mathbb{F}_q$ (for some q prime power) and $q^{L-1} > |d|_p$, $q > |\rho|_p|\eta d - 1|_p^{|I|-1}$ where $d = 2|L_A : N_{L_A}(A)|$, the number $|\rho|$ is the maximum order of a graph automorphism in X_A (see p.41 for the definition) and*

$$\eta = \begin{cases} 2 & \text{if } |\rho| = 2 \text{ and } \mathrm{soc}(X_A) \text{ is of type } \mathbf{L}, \\ 1 & \text{otherwise.} \end{cases}$$

Moreover, if there is a maximal subgroup of L_A which is not non-trivial intersecting, then assume that $|\rho|_p|d|_p|\eta d - 1|_p^{|I|-1} < |S|_p^2$, where $S = \mathrm{soc}(X_A)$;

- $\mathrm{soc}(X_A) \cong \mathrm{PSL}_2(49)$ *and* $X_A > \mathrm{soc}(X_A)$. *If there is a maximal subgroup of* L_A *which is not non-trivial intersecting, then assume that* $|d|_5 < 25$*;*
- $\mathrm{soc}(X_A) \cong \mathrm{PSL}_2(8)$. *In this case assume that* $|d|_7 = 1$*;*
- $A \cong \mathrm{PSL}_2(9), \mathrm{PSL}_4(2), \mathrm{PSU}_4(2), \mathrm{PSp}_6(2), \mathrm{PSL}_2(49)$.

Then $P_G(-1) \neq 0$*, hence the order complex of the coset poset of* G *is not contractible.*

The proof of the above result is in the end of the present chapter.

In Table 7.1 we fix the values of the number L, we shall use during the proof of the following results. L

Table 7.1: Value of L for the classical simple groups

Case	S	L	$\lvert I\rvert$
L	$\mathrm{PSL}_n(q)$	$n-1$	$n-1$
U	$\mathrm{PSU}_n(q)$	$2\left[\frac{n-1}{2}\right]+1$	$\left[\frac{n}{2}\right]$
S	$\mathrm{PSp}_n(q)$	$\frac{n}{2}$	$\frac{n}{2}$
$\mathbf{O}^\circ$	$\mathrm{P}\Omega_n(q)$	$\frac{n-1}{2}$	$\frac{n-1}{2}$
$\mathbf{O}^+$	$\mathrm{P}\Omega_n^+(q)$	$\frac{n}{2}$	$\frac{n}{2}$
$\mathbf{O}^-$	$\mathrm{P}\Omega_n^-(q)$	$\frac{n}{2}$	$\frac{n}{2}-1$

7.1 General case

Proposition 7.2. *Let* X *be a projective classical group with socle* S *of characteristic* p*. Let* d *be an even positive number, such that*

$$|P^{(p)}_{X,S}(1-d)|_p = |d(d-1)^{|I|-1}|_p q^L,$$

where $|I|$ *is the number or* ρ*-orbits of* S*. Moreover assume that*

- X *does not contain a non-trivial graph automorphism;*
- *if case* **L** *holds, then* $n \geq 3$ *and* $(n,q) \neq (4,2)$*;*

- *if case* **U** *holds, then* $(n, q) \neq (4, 2)$*;*
- *if case* **S** *holds, then* $(n, q) \neq (6, 2)$.

Then $|P_{X,S}(1-d)|_p = |d(d-1)^{|I|-1}|_p q^L$.

Proof. In order to prove the proposition, it is enough to show that

$$|d(d-1)^{|I|-1}|_p q^L < q^{d\beta_p(X)},$$

as we have seen in Chapter 4. Recall that $\beta_p(X) \geq \tilde{\beta}_p(X)$, which is given in Theorem 6.1. An easy computation shows that

$$|2|_p q^L < q^{2\tilde{\beta}_p(X)} \leq q^{2\beta_p(X)}, \quad (*)$$

hence for $d = 2$ the result holds. By $(*)$ we get:

$$|4|_p|(4-1)^{|I|-1}|_p q^L < |4|_p|3|_p^L q^L \leq (|2|_p q^L)^2 < q^{4\beta_p(X)},$$

hence for $d = 4$ we have the claim. Arguing in a similar way, we obtain the result for $d \leq 14$. Let $d = 2d'$ and assume that $d' \geq 8$. By $(*)$ we get:

$$|d(d-1)^{|I|-1}|_p q^L \leq |2|_p q^L |d'|_p |2d'-1|_p^L < q^{2\beta_p(X)} d'(2d'-1)^L \leq$$

$$\leq q^{2\beta_p(X)} 2^{L(d'-1)} \leq q^{2\beta_p(X)} (|2|_p q^L)^{d'-1} < q^{2d'\beta_p(X)},$$

since for $d' \geq 8$ we have that $d'(2d'-1) \leq 2^{d'-1}$. Thus the proof is complete. □

Proposition 7.3. *Let* X *be a projective classical group with socle* S *of characteristic* p*. Assume that*

- X *contains a graph automorphism of order 2 (i.e. case* **L** *or case* $\mathbf{O}^+$ *holds);*
- *if case* **L** *holds then* $(n, q) \neq (4, 2)$*; moreover we assume that* $|P_{X,S}^{(p)}(1-d)|_p = |2d(2d-1)^{\left[\frac{n}{2}\right]-1}|_p q^{\left[\frac{n-1}{2}\right]}$*;*
- *if case* $\mathbf{O}^+$ *holds we assume that* $|P_{X,S}^{(p)}(1-d)|_p = |2d(d-1)^{\frac{n}{2}-2}|_p q^{\frac{n}{2}-1}$.

Then $|P_{X,S}(1-d)|_p = |P^{(p)}_{X,S}(1-d)|_p$.

Proof. As in the previous proposition, it is enough to show that

$$|P^{(p)}_{X,S}(1-d)|_p < q^{d\beta_p(X)},$$

as we have seen in Chapter 4. Assume that case **L** holds. As in the previous proof, we have that

$$|d(d-1)^{n-1}|_p q^{n-1} < q^{d\beta_p(X)}.$$

Hence we get:

$$|4(4-1)^{\left[\frac{n}{2}\right]-1}|_p q^{\left[\frac{n-1}{2}\right]} \leq |4|_p q^{n-2} < q^{2\beta_p(X)},$$

thus we have the claim for $d = 2$. Similarly we get the result for $d = 4$. Assume that $d \geq 6$. Since $2d(2d-1)^{\left[\frac{n}{2}\right]-1} \leq d(d-1)^{n-1}$ for $d \geq 6$, we have that:

$$|2d(2d-1)^{\left[\frac{n}{2}\right]-1}|_p q^{\left[\frac{n-1}{2}\right]} \leq |d(d-1)^{n-1}|_p q^{n-1} < q^{d\beta_p(X)},$$

hence we obtain the claim.

Assume that case $\mathbf{O}^+$ holds. By the proof of the previous proposition, we have that

$$|d(d-1)^{\frac{n}{2}-1}|_p q^{\frac{n}{2}-1} < q^{d\beta_p(X)}.$$

Thus we get:

$$|2d(d-1)^{\frac{n}{2}-2}|_p q^{\frac{n}{2}-1} \leq |d(d-1)^{\frac{n}{2}-1}|_p q^{\frac{n}{2}-1} < q^{d\beta_p(X)}.$$

This completes the proof. □

7.2 The projective linear groups $\mathrm{PSL}_2(q)$

For a prime number r we let

$$b_r(X) = \min\{|X:H|_r, H < X, |X:H|_r > 1, HS = X, \mu_X(H) \neq 0\}.$$

For some almost simple groups X there exists a prime number $r > 2$ such that $b_r(X)$ and $P^{(r)}_{X,S}(1-d)$ are easy to compute (using [GAP]). In particular, for the groups X in Table 7.2 (except for $\mathrm{PSL}_2(8)$ and $\mathrm{P\Gamma L}_2(8)$), we have that $P^{(r)}_{X,S}(1-d) = 1-(a+1)^d$ where $|a|_r = r$, hence $|P^{(r)}_{X,S}(1-d)|_r = r|d|_r$ (see the proof of Proposition 5.10). If $S = \mathrm{PSL}_2(8)$, then $P^{(7)}_{X,S}(1-d) = 1 - 9^d - 36^d + 72^d$. It is easy to see that if $|d|_7 = 1$, then $|1 - 9^d - 36^d + 72^d|_7 = 7$.

Table 7.2: r for some $\mathrm{PSL}_2(q) \leq X \leq \mathrm{P\Gamma L}_2(q)$, with $q \leq 11$

X	r	X	r
$\mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5)$	5	M_{10}	5
$\mathrm{PGL}_2(5) \cong \mathrm{P\Gamma L}_2(4)$	5	$\mathrm{P\Gamma L}_2(9)$	5
$\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$	7	$\mathrm{PGL}_2(9)$	5
$\mathrm{PGL}_2(7) \cong \mathrm{P\Gamma L}_3(2)$	7	$\mathrm{PSL}_2(11)$	11
$\mathrm{PSL}_2(8)$	7	$\mathrm{PGL}_2(11)$	11
$\mathrm{P\Gamma L}_2(8)$	7		

Proposition 7.4. *Assume $n = 2$ and case* **L** *holds. Assume that $q \geq 13$. Let d be an even positive integer. The following hold.*

(1) If $q = p$, then $|P^{(p)}_{X,S}(1-d)|_p = p|d|_p$ and $b_p(X) = p$.

(2) If $q \neq p$ and $q \neq 49$, then $|P^{(t)}_{X,S}(1-d)|_t = |S|_t|d|_t$ and $b_t(X) \geq |S|_t^{1/2}$.

(3) If $q = 49$ and $X > S$, then $|P^{(5)}_{X,S}(1-d)|_t = 25|d|_5$ and $b_5(X) = 5^2$.

Proof. Let $\delta = (q-1, 2)$ and $q = p^f$.

We prove (1). In this case we have $f = 1$. Let P be a Sylow p-subgroup of X. Let M be a maximal subgroup of X such that M contains P and $MS = X$. By Lemma 3.8, we have $N_X(P) \leq M$, so we can apply Lemma 3.6. By [KL90, Proposition 4.1.16], we have that $M = N_X(M \cap S)$ and $M \cap S$ is a maximal subgroup of S. Since $M \cap S = N_S(P \cap S)$ we have that $\mathcal{M}_{P\cap S}(S) = \{M \cap S\}$ and so $\mathcal{M}_P(X) = \{M\}$. Applying Lemma 3.6, we deduce that

$$P^{(p)}_S(s) = 1 - \frac{1}{|S : M \cap S|^{s-1}} = 1 - \frac{1}{|X : M|^{s-1}} = P^{(p)}_{X,S}(s).$$

Hence we get:

$$P^{(p)}_{X,S}(s) = 1 - \frac{p+1}{(p+1)^s},$$

so we have $|P^{(p)}_{X,S}(-(d-1))|_p = |d|_p p$ (see Proposition 5.10), thus we obtain the claim.

Now, we prove (2). So assume $f \geq 2$ and $q \neq 49$. As in [Pat09c], case $m = 1$ of the proof of Proposition 16, let $t = \hat{p}_{2f}$ be a Zsigmondy prime for $\langle p, 2f \rangle$. In particular, for $f = 2$,

if 5^3 divides $p^2 + 1$, let $t = 5$;

otherwise, let $t = \hat{p}_4$ be a Zsigmondy prime for $\langle p, 4 \rangle$ distinct from 5.

Let T be a Sylow t-subgroup of X. By [Pat09c], case $m = 1$ of the proof of Proposition 16, we have:

(a) $P_S(s) = 1 - \frac{q(q-1)/2}{[q(q-1)/2]^s} + \sum_{t|k} \frac{a_k(S)}{k^s}$.

(b) Let K be a maximal subgroup of S. We have that $|S : K|$ is divisible by t if and only if K is not isomorphic to $D_{2(q+1)/\delta}$. In particular, if K is not isomorphic to $D_{2(q+1)/\delta}$, we have $v_t(|S : K|) > v_t(|S|)/2$, where $v_t : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is the t-adic valuation map.

(c) Let K_1 and K_2 be two distinct maximal subgroups isomorphic to $D_{2(q+1)/\delta}$. We have that $v_t(|S : K_1 \cap K_2|) > v_t(|S|)/2$.

(d) The group $N_S(T \cap S)$ is a maximal subgroup of S isomorphic to $D_{2(q+1)/\delta}$.

Moreover, by [Giu07], we have that

if M is a maximal subgroup of X and $M \cap S$ is a isomorphic to a subgroup of $D_{2(q+1)/\delta}$, then $M \cap S$ is isomorphic to $D_{2(q+1)/\delta}$. $(*)$

In particular, if M is in $\mathcal{M}_T(X)$, by (d) we have that $M \cap S = N_S(T \cap S)$ and $M = N_X(N_S(T \cap S))$. So we obtain $N_X(T \cap S) \leq N_X(N_S(T \cap S)) = M$ and since $N_X(T) \leq N_X(T \cap S)$, we get $N_X(T) \leq M$. Moreover, by (b), (d) and $M = N_X(M \cap S)$,

we have that $\mathcal{M}_{T\cap S}(S) = \{M \cap S\}$ and so $\mathcal{M}_T(X) = \{M\}$. Using (a) and applying Lemma 3.6, we deduce that

$$P_S^{(t)}(s) = 1 - \frac{1}{[q(q-1)/2]^{s-1}} = 1 - \frac{1}{|S : M \cap S|^{s-1}} = 1 - \frac{1}{|X : M|^{s-1}} = P_{X,S}^{(t)}(s).$$

Thus $|P_{X,S}^{(t)}(1-d)|_t = |S|_t|d|_t$ (argue as in Proposition 5.10).

Now, let H be a subgroup of X such that $HS = X$ and M does not contain a Sylow t-subgroup of X. We have that $|X : H| = |S : H \cap S|$. Suppose that M is a maximal subgroup of X containing H. By $(*)$ we have that $M \cap S$ is not isomorphic to a subgroup of $D_{2(q+1)/\delta}$. Thus, by (b) and (c), we obtain $v_t(|X : H|) > v_t(|S|)/2$. So we get that $b_t(X) \geq |S|_t^{1/2}$.

Finally, we prove (3). Assume that $q = 49$ and $X > S$. We show that $r = 5$ fulfills the requirements of the proposition. Let M be a maximal subgroup of X such that $MS = X$ and $|X : M|_5 = 1$. By [Giu07, Theorem 1.3, 1.4, 1.5 and 3.5], we have that M is conjugated to $N_X(D_{50})$. Let M_1 and M_2 be two distinct maximal subgroups of X such that $M_1S = M_2S = X$ and $|X : M_1|_5 = |X : M_2|_5 = 1$. We claim that $|X : M_1 \cap M_2|_5 > 1$. For a contradiction, suppose that $M_1 \cap M_2$ contains a Sylow 5-subgroup of X. Since M_1 and M_2 are conjugated to $N_X(D_{50})$, they contain a cyclic normal subgroup C of order 25. Thus $C \trianglelefteq X$, a contradiction. Hence we get

$$P_{X,S}^{(5)}(s) = 1 - 1176^{1-s},$$

so $|P_{X,S}^{(5)}(1-d)|_5 = 25|d|_5$ (argue as in Proposition 5.10). Now, if M is a maximal subgroup of X such that $MS = X$ and $|X : M|_5 > 1$, then we have that $|X : M|_5 = 5^2$ (see [Giu07, Theorem 1.3, 1.4, 1.5 and 3.5]). So we obtain the claim. □

7.3 Proof of Theorem 7.1

Note that there are some groups missing: $\mathrm{PSL}_2(9), \mathrm{PSL}_4(2), \mathrm{PSU}_4(2), \mathrm{PSp}_6(2)$ and their automorphism groups. Using [GAP], one can see that $P_{X,S}(-1) \neq 0$. Also $P_{\mathrm{PSL}_2(49)}(-1) \neq 0$.

Now we can prove Theorem 7.1.

Proof. By Theorem 1.1, we have that:

$$P_G(s) = \prod_{A \in \mathcal{A}} \left(\prod_{1 \leq i \leq \delta_G(A)} \tilde{P}_{L_A,i}(s) \right),$$

where

$$\tilde{P}_{L_A,1}(s) = P_{L_A,A}(s), \;\; \tilde{P}_{L_A,i}(s) = P_{L_A,A}(s) - \frac{c_{A,i}}{|A|^s} \text{ for } i > 1,$$

for some $c_{A,i} \in \mathbb{N}$ such that $|A|$ divides $c_{A,i}$ if A is not abelian. As it was pointed out before Theorem 1.1, if A is abelian, then $\tilde{P}_{L_A,i}(-1) \neq 0$ (indeed, this is a result of [Bro00]).

Now, assume that $X = N_{L_A}(A)/C_{L_A}(A)$ is a classical projective group. As we have see in Chapter 4, in order to show that $P_{L_A,i}(-1) \neq 0$, it is enough to prove that

$$|P^{(p)}_{X,A}(1-d)|_p < \min\{q^{d\beta_p(X)}, |S|_p^2\},$$

and if each maximal subgroup of L_A is non-trivial intersecting, then it is enough to show that

$$|P^{(p)}_{X,A}(1-d)|_r < q^{d\beta_p(X)}.$$

In particular, note that $q^{\beta_p(X)} \leq |S|_p$, hence $q^{d\beta_p(X)} \leq |S|_p^d = |A|_p^2$.

Since we assume that $q^{L-1} > |d|_p$, $q > |\rho|_p |\eta d - 1|_p^{|I|-1}$, by Proposition 5.10 and 5.11, we have that $|P^{(r)}_{X,A}(1-d)|_p = |\rho|_p |\eta d - 1|_p^{|I|-1}$. From Proposition 7.2, 7.3 and 7.4 the result follows.

In a similar way, the result holds in the other cases. □

Part II

On the irreducibility of the Dirichlet polynomial of a simple group of Lie type.

Chapter 8

Introduction

The aim of this part is to prove the following theorem.

Theorem 8.1. *Let G be a primitive monolithic group with a simple component S isomorphic to a simple group of Lie type. Let $X = N_G(S)/C_G(S)$. Let k be the maximum of the orders of the graph automorphisms in $X \lesssim \mathrm{Aut}(S)$. Assume that*

- *the Lie rank of S is greater than k;*
- *S is not isomorphic to one of the following groups: $A_2(2)$, $A_2(3)$, ${}^2A_3(3^2)$, ${}^2A_4(2^2)$, ${}^2A_5(2^2)$, $C_2(p)$ for p a Mersenne prime.*

The Dirichlet polynomial $P_{G,\mathrm{soc}(G)}(s)$ is irreducible in the ring of finite Dirichlet series.

In particular, if $G = S$, then we obtain a complete answer to the irreducibility problem.

Theorem 8.2. *Let S be a simple group of Lie type. Then $P_S(s)$ is reducible in the ring of Dirichlet finite series if and only if $S \cong A_1(p)$ for some Mersenne prime p such that $\log_2(p+1) \equiv 3 \pmod 4$.*

In order to prove such theorems, we first show that the Dirichlet polynomial $P^{(p)}_{G,\mathrm{soc}(G)}(s)$ is irreducible in most of cases. Next, we apply Lemma 2.13 with $h(s) =$

$P_{G,\mathrm{soc}(G)}(s)$, $\pi_0 = \{p\}$ and a suitable set of prime numbers π (usually consisting of some Zsigmondy primes).

With the same proof of Theorem 8.1, we obtain the following theorem, which gives a bijective correspondence between the set of chief factors of a group H and the set of irreducible factors of $P_H(s)$, under some assumptions.

Theorem 8.3. *Let H be a finite group. Let $1 = H_0 \trianglelefteq H_1 \trianglelefteq ... \trianglelefteq H_k = H$ be a chief series of H and assume that the chief factors of H are non-abelian. Let L_{K_i} be the monolithic primitive group associated with $K_i = H_{i+1}/H_i$, defined by $L_{K_i} = H_i/C_{H_i}(K_i)$. Suppose that L_{K_i} satisfies the assumptions of Theorem 8.1 for each $i \in \{0, ..., k-1\}$. Then*

$$P_H(s) = \prod_{i=0}^{k-1} P_{H_i,K_i}(s)$$

is a factorization into irreducible elements of $\mathcal{R}$.

Moreover, in a slightly more general situation, we are able to determine the number of non-Frattini chief factors of H. In fact, thanks to [DL03a, Lemma 16], as a corollary of Theorem 8.3, we have the following.

Theorem 8.4. *Let H be a finite group as above. Suppose that L_{K_i} satisfies the assumptions of Theorem 8.1 whenever K_i is a non-abelian chief factor of H. Let $k_1, k_2 \in \mathbb{N}$ such that*

$$P_H(s) = \prod_{i=1}^{k_1} \left(1 - \frac{c_i}{p_i^{a_i s}}\right) \prod_{j=1}^{k_2} f_j(s)$$

where $a_i, c_i \in \mathbb{N} - \{0\}$, p_i is a prime number for all $i \in \{1, ..., k_1\}$ and $f_j(s)$ is an irreducible Dirichlet polynomial not equal to $\pm(1 - \frac{c}{p^{as}})$ for any $a, c \in \mathbb{N} - \{0\}$ and p prime, for each $j \in \{1, ..., k_2\}$. Then k_1 is the number of non-Frattini abelian chief factors of H and k_2 is the number of non-abelian chief factors of H.

Chapter 9

The irreducibility of the Dirichlet polynomial $P^{(p)}_{G,\mathrm{SOC}(G)}(s)$

Let G be a primitive monolithic group with socle $\mathrm{soc}(G)$, the group S is a simple component of G and $X = N_G(S)/C_G(S)$. Moreover, let S be a simple group of Lie type of characteristic p and $S \cong \mathrm{soc}(X)$. The aim of the present section is to prove that the Dirichlet polynomial $P^{(p)}_{G,\mathrm{soc}(G)}(s)$ is irreducible when the Lie rank of S is greater than the order of each graph automorphisms of X (see Proposition 9.3).

9.1 Some preliminary results

Lemma 9.1. *Assume that S is a simple group of Lie type such that S is not isomorphic to one of the following groups: $A_1(p)$ with p a Mersenne prime, ${}^2A_3(2^2)$, $A_5(2)$, $C_3(2)$, $D_4(2)$. Define the number $\zeta(S)$ as in Table 9.1.*

Let r be the prime number $\hat{t}_{\zeta(S)}$ (i.e. the greatest Zsigmondy prime for $\langle t, \zeta(S)\rangle$). If H is a proper parabolic subgroup of S, then $|S : H|_r = |S|_r$.

Proof. Let H be a proper parabolic subgroup of S. By the discussion after Proposition 3.4, using the definition of Zsigmondy prime, if $|S : H|_r > 1$, then $|S : H|_r = |S|_r$. □

Table 9.1: $\zeta(S)$ for S a simple group of Lie type

S	$\zeta(S)$	S	$\zeta(S)$
$A_l(t)$	$l+1$	${}^2A_l(t^2), l$ odd	$2l$
$B_l(t), C_l(t)$	$2l$	${}^2A_l(t^2), l$ even	$2l+2$
$D_l(t)$	$2l-2$	${}^2D_l(t^2)$	$2l$
$E_6(t)$	12	${}^3D_4(t^3)$	12
$E_7(t)$	18	${}^2E_6(t^2)$	18
$E_8(t)$	30	${}^2B_2(t^2)$	4
$F_4(t)$	12	${}^2F_4(t^2)$	24
$G_2(t)$	6	${}^2G_2(t^2)$	6

$\mathcal{G}_1$ We denote by $\mathcal{G}_1$ the set of groups X such that X does not contain a non-trivial graph automorphism and S is isomorphic to one of the following groups:

- $A_l(t)$ for $l \geq 2$ and $(l,t) \notin \{(2,p) : p \text{ is a Mersenne prime}\} \cup \{(5,2)\}$;
- ${}^2A_l(t^2)$ for $l \geq 3$ and $(l,t) \notin \{(3,2)\}$;
- $B_l(t)$ for $l \geq 3$;
- $C_l(t)$ for $l \geq 2$ and $(l,t) \notin \{(2,p) : p \text{ is a Mersenne prime}\} \cup \{(3,2)\}$;
- $D_l(t)$ for $l \geq 4$ and $(l,t) \notin \{(4,2)\}$;
- ${}^2D_l(t^2)$, $E_l(t)$, ${}^2E_6(t^2)$.

$\mathcal{G}_2$ We define $\mathcal{G}_2$ to be the set consisting of the groups X such that the maximum of the order of a graph automorphism in X is 2 and S is isomorphic to one of the following groups:

- $A_l(t)$ for $l \geq 3$ and $(l,t) \notin \{(3,p) : p \text{ is a Mersenne prime}\} \cup \{5,2\}$;
- $D_l(t)$ for $l \geq 4$ and $(l,t) \notin \{(4,2)\}$;
- $E_6(t)$.

$\theta_1(X)$, $\theta_2(X)$

THE NUMBERS $\theta_1(X)$ AND $\theta_2(X)$. Let $k \in \{1,2\}$. Let X be an element of $\mathcal{G}_k$. The numbers $\theta_k(X)$ for $k \in \{1,2\}$ are defined in the following way:

- if $S \cong A_6(2)$, then $\theta_1(X) = \theta_2(X) = 5$;
- if $S \cong A_7(2)$, then $\theta_1(X) = 7$ and $\theta_2(X) = 5$;
- if $S \cong {}^2A_4(2^2)$, then $\theta_1(X) = 4$;
- if $S \cong C_4(2)$, then $\theta_1(X) = 3$;
- if $S \cong D_5(2)$, then $\theta_1(X) = \theta_2(X) = 3$;
- if $S \cong {}^2D_5(2^2)$, then $\theta_1(X) = 3$;
- otherwise let $\theta_k(X)$ be as in Table 9.2.

Table 9.2: $\theta_k(X)$ for X almost simple group of Lie type with socle S

S	$\theta_1(X)$	$\theta_2(X)$	S	$\theta_1(X)$
$A_l(t)$	l	$l-1$	${}^2A_3(t^2), {}^2A_5(t^2)$	4
$B_l(t), C_l(t)$	$2l-2$		${}^2A_l(t^2), l > 5$ odd	$2l-4$
$D_l(t), l \geq 5$	$2l-4$	$2l-4$	${}^2A_l(t^2), l \geq 4$ even	$2l-2$
$D_4(t)$	3	3	${}^2D_4(t^2)$	3
$E_6(t)$	8	5	${}^2D_l(t^2), l > 4$	$2l-4$
$E_7(t)$	12		${}^2E_6(t^2)$	10
$E_8(t)$	18			

We have the following.

Proposition 9.2. *Let $k \in \{1,2\}$. Assume that $X \in \mathcal{G}_k$. Let $v = \hat{t}_{\theta_k(X)}$. If H is a proper parabolic subgroup of S such that $|S:H|_v > 1$, then $|S:H|_v = |S|_v$. In particular, for $H = B$, we have $|S:H|_v = |S:B|_v = |S|_v$. Moreover, there exists $J \in \mathcal{P}^X(I)$ such that $|S:P_J|_v = 1$.*

Proof. Let H be a proper parabolic subgroup of S. By the discussion after Proposition 3.4 and the definition of Zsigmondy prime, it is not difficult to see that if $|S:H|_v > 1$, then $|S:H|_v = |S|_v$. It remains to prove there exists $J \in \mathcal{P}^X(I)$ such that $|S:P_J|_v = 1$.

Assume that $k = 1$. Using the labeling of Figure 3.1, define $K \subset \Pi$ as follows:

$$K = \begin{cases} \{r_1, r_3\} & \text{if } S \cong {}^2A_3(t^2), \\ \{r_1, r_4\} & \text{if } S \cong {}^2A_4(2^2), \\ \{r_2, ..., r_{l-1}\} & \text{if } S \cong {}^2A_l(t^2), l \geq 4, (l,t) \neq (4,2), \\ \{r_1, r_2\} & \text{if } S \cong {}^2D_4(t^2), \\ \{r_1, ..., r_{l-1}\} & \text{if } S \cong E_l(t) \\ \{r_2, ..., r_l\} & \text{otherwise.} \end{cases}$$

Assume that $k = 2$. Using the labeling of Figure 3.1, define $K \subset \Pi$ as follows:

$$K = \begin{cases} \{r_2, ..., r_{l-1}\} & \text{if } S \cong A_l(t), \\ \{r_2, ..., r_l\} & \text{if } S \cong D_l(t), \\ \{r_2, ..., r_6\} & \text{if } S \cong E_6(t). \end{cases}$$

In both cases, K is union of ρ-orbits. Let J be the set of these orbits. By definition of K, it is clear that $J \in \mathcal{P}^X(I)$. Moreover, it is easy to see that J satisfies the requirements. □

9.2 Proof of the irreducibility of $P^{(p)}_{G,\mathrm{soc}(G)}(s)$

Now, we can prove the following result on the irreducibility of $P^{(p)}_{G,\mathrm{soc}(G)}(s)$.

Proposition 9.3. *Let G be a primitive monolithic group with non-abelian socle $\mathrm{soc}(G)$ and let S be a simple component of G. Let $X = N_G(S)/C_G(S)$ and let k be the maximum of the orders of the graph automorphisms of X. Further, assume that S is a group of Lie type of Lie rank greater than k. The Dirichlet polynomial $P^{(p)}_{G,\mathrm{soc}(G)}(s)$ is irreducible in the ring of finite Dirichlet series.*

Proof. By Theorem 1.3, we have that $P^{(p)}_{G,\mathrm{soc}(G)}(s) = P^{(p)}_{X,S}(n(s-1)+1)$.

A direct inspection shows that the proposition holds if S is isomorphic to one of the following groups: $A_5(2), {}^2A_3(2^2), C_3(2), D_4(2)$. So, assume that S is not isomorphic to one of the following groups: $A_5(2), {}^2A_3(2^2), C_3(2), D_4(2)$.

Let $r = \hat{t}_{\zeta(S)}$ and let $x = x_r$ be the indeterminate corresponding to r, i.e. $\Psi(r^{(1-s)}) = x$. Let $D = \mathbb{Z}[X_{\pi(S)-\{r\}}]$.

Assume that $k \in \{1,2\}$ and X is in $\mathcal{G}_k$. Let $v = \hat{t}_{\theta_k(S)}$. Let $y = x_v$ be the indeterminate corresponding to v, i.e. $\Psi(v^{(1-s)}) = y$. Let $g(x,y) = \Psi(P^{(p)}_{G,\mathrm{soc}(G)}(s))$, considered as a polynomial in $E[x,y]$, where $E = \mathbb{Z}[X_{\pi(S)-\{r,v\}}]$. By Theorem 3.10, Lemma 9.1 and Proposition 9.2, we have that $g(x,y) = 1 - x^{m_1}(b + cy^{m_2})$ for some $b, c \in E - \{0\}$ and $m_1, m_2 \in \mathbb{N}, m_1, m_2 \geq 1$. Let $f(x)$ be the polynomial $g(x,y)$ in $D[x]$. For a contradiction, assume that $f(x)$ is irreducible in $D[x]$. By Lemma 2.10, we have that $b + cy^{m_2}$ or $-(b + cy^{m_2})$ is a non-trivial power in D. However, it is clear that $b + cy^{m_2}$ and $-(b + cy^{m_2})$ are not non-trivial power in $D = E[y]$.

Assume that $k \in \{1,2\}$ and $X \notin \mathcal{G}_k$. In this case, by Lemma 9.1, we have that

$$f(x) = \Psi(P^{(p)}_{G,\mathrm{soc}(G)}(s)) = 1 - ax^m$$

for some $m \in \mathbb{N}$ and $a \in D$. By Lemma 2.10, if $f(x)$ is reducible, then a or $-a$ is a non-trivial power in D. A direct inspection shows that this does not happen.

Assume that $k = 3$, i.e. S is isomorphic to $D_4(t)$ and that X contains a graph automorphism of order 3. Let $y = y_{\hat{t}_3} = \Psi(\hat{t}_3^{1-s})$ be the indeterminate corresponding to $\hat{t}_3$. We have that $f(y) = \Psi(P^{(p)}_{G,\mathrm{soc}(G)}(s)) = 1 - ay^m$ for some $m \in \mathbb{N}$ and $a \in D$. As above, by Lemma 2.10, if $f(x)$ is reducible, then a or $-a$ is a non-trivial power in D. A direct inspection shows that this does not happen. $\square$

Chapter 10

Proof of the main theorem.

In this section we prove Theorem 8.1. Recall that X is an almost simple group with socle a simple group of Lie type S, and B is a Borel subgroup of S.

A key role in the proof of Theorem 8.1 is played by the following proposition, which proves that, under some assumptions, $P_{X,S}^{(\Omega)}(s) = 1$ for $\Omega = \pi(S) - \pi(B)$.

Proposition 10.1. *Let S be a simple group of Lie type of characteristic p and assume that the Lie rank of S is at least 2. Moreover, assume that $S \notin \{A_2(2), A_3(2), {}^2A_3(3^2), {}^2A_4(2^2), {}^2A_5(2^2)\} \cup \{A_2(p), C_2(p)\}$ for p a Mersenne prime. Let B be a Borel subgroup of S and let $\Omega = \pi(S) - \pi(B)$. If H is a subgroup of S such that $|S|_r = |H|_r$ for all $r \in \Omega$, then $H = S$.*

Proof. Let H and S be as in the statement. For a contradiction, assume that $H < S$. Without loss of generality, we may assume that H is a maximal subgroup of S. By hypothesis, we have that

$$b(S) = \prod_{r \in \Omega} |S|_r = \frac{|S : B|}{\prod_{r||B|} |S : B|_r} \text{ divides } |H|.$$

Let π be a set of prime numbers. We denote by $M_\pi(S)$ the set of representatives of the isomorphism classes of maximal subgroups M of S such that r does not divide $|S : M|$ for all $r \in \pi$.

Table 10.1: $|S : B|_r$ when r divides $|B|$.

S	$\|S : B\|_2$	$\|S : B\|_3$	$\|S : B\|_5$	$\|S : B\|_7$	$\|S : B\|_r, r \geq 11$
$G_2(t)$	$\|t+1\|_2^2$	3	1	1	1
$E_6(t)$	$2^3\|t+1\|_2^4$	3^4	5	1	1
${}^2E_6(t^2), r\|t-1$	$2^3\|t+1\|_2^4$	3^2	1	1	1
${}^2E_6(t^2), r\|t+1$	$2^3\|t+1\|_2^4$	$3^4\|t+1\|_3^4$	$5\|t+1\|_5^4$	$\|t+1\|_7^4$	$\|t+1\|_r^4$
$E_7(t)$	$2^3\|t+1\|_2^7$	3^4	5	7	1
$E_8(t)$	$2^6\|t+1\|_2^8$	3^5	5^2	7	1
$F_4(t)$	$2^3\|t+1\|_2^4$	3^2	1	1	1

For the exceptional groups, we adopt the following strategy. We find a subset π of Ω such that if $H \in M_\pi(S)$, then $|H| < b(S)$. This is enough to prove the claim. In Table 10.1, we report the numbers $|S : B|_r$ with $r \in \pi(B)$ and $r \neq p$ for some exceptional group S.

Case $S = {}^3D_4(t^3)$**.** By [Kle88b], we have that $M_{\{\hat{t}_3,\hat{t}_{12}\}}(S) = \varnothing$.

Case $S = G_2(t)$**.** In this case we have $t \geq 4$ and the maximal subgroup of S are known (see [Kle88a] and [Coo81]). If $t = 4$, then $M_{\{5,7,13\}}(S) = \varnothing$. If $t \leq 7$ and $t \neq 4$, then $M_{\{\hat{t}_3,\hat{t}_6\}}(S) = \varnothing$. Suppose that $t \geq 9$. We have that $M_{\{\hat{t}_3,\hat{t}_6\}}(S) \subseteq \{A_1(13)\}$, but $b(S) > |A_1(13)|$.

Case $S = {}^2F_4(t^2)$**.** In this case, $t^2 = 2^{2k+1}$ and $k \geq 1$. The maximal subgroup of S are known (see [Mal91]). Note that $\Phi_{12}(t^2) = t^8 - t^4 + 1$ divides the order of S and a prime divisor of $\Phi_{12}(t^2)$ is a prime divisor of $b(S)$. Moreover, we have that $t^8 - t^4 + 1 = (t^4 - \sqrt{2}t^3 + t^2 - \sqrt{2}t + 1)(t^4 + \sqrt{2}t^3 + t^2 + \sqrt{2}t + 1)$ and $(t^4 - \sqrt{2}t^3 + t^2 - \sqrt{2}t + 1, t^4 + \sqrt{2}t^3 + t^2 + \sqrt{2}t + 1) = 1$. Thus let r_+ be a prime divisor of $t^4 + \sqrt{2}t^3 + t^2 + \sqrt{2}t + 1$ and r_- be a prime divisor of $t^4 - \sqrt{2}t^3 + t^2 - \sqrt{2}t + 1$. We have that $M_{\{r_+,r_-\}}(S) = \varnothing$.

Case $S \in \{E_6(t), {}^2E_6(t^2), E_7(t), E_8(t)\}$**.** By [ILS03, Theorem 9], the maximal subgroups H of S such that $|H| \geq \gamma(S)$ are known (the values of $\gamma(S)$ are given in Table 10.2). By direct inspection, it is easy to see that if $H \in M_{\pi_1(S)}(S)$, then $|H| < \gamma(S)$ (see Table 10.2 for the values of $\pi_1(S)$). Moreover, we have that $b(S) > \gamma(S)$

except for ${}^2E_6(t^2)$ and $t \in \{2,4,5\}$. Assume that $S = {}^2E_6(t^2)$ and $t \in \{2,4,5\}$. By [ILS03, Theorem 8], a direct inspection shows that if $H \in M_{\pi_1(S)}(S)$, then $|H| < b(S)$.

Table 10.2: Values of $\gamma(S)$ and $\pi_1(S)$ for some groups

S	$\gamma(S)$	$\pi_1(S)$
${}^kE_6(t^k), k \in \{1,2\}$	$4\log_p(t)t^{28}$	$\hat{t}_{12}, \hat{t}_{9k}$
$E_7(t)$	$4\log_p(t)t^{30}$	$\hat{t}_{18}, \hat{t}_{14}$
$E_8(t)$	$12\log_p(t)t^{56}$	$\hat{t}_{30}, \hat{t}_{24}$

Case $S = F_4(t)$. By [ILS03, Theorem 8], a direct inspection shows that if $H \in M_{\{\hat{t}_{12},\hat{t}_8\}}(S)$, then $|H| < b(S)$.

Table 10.3: Classical groups, geometric case

S	$\pi_{\mathcal{G}}(S)$	(l,t)	S	$\pi(S)$	(l,t)
$A_l(t)$	$5,7,31$	$(5,2)$	$C_l(t)$	$5,7,17$	$(4,2)$
	$31,127$	$(6,2)$		$5,7$	$(3,2)$
	$\hat{t}_2, \hat{t}_3$	$l=2$	$D_l(t)$	$5,7$	$(4,2)$
	$\hat{t}_{l-1}, \hat{t}_l, \hat{t}_{l+1}$	$(4,2),(10,2),(12,2),$		$17,31$	$(5,2)$
		$(4,3),(6,3),(6,5)$		$7,11,17$	$(6,2)$
$C_l(t)$	$7,11,13$	$(6,2)$	${}^2D_l(t^2)$	$7,17$	$(4,2)$

Case S a classical group. A maximal subgroup of S is either geometric or a nearly simple group in the class $\mathcal{S}$ (see [KL90] for a better explanation). The geometric maximal subgroups of S are known (see [KL90]). If S does not appear in

the Table 10.3, then let

$$\pi_{\mathcal{G}}(S) = \begin{cases} \{\hat{t}_{l+1}, \hat{t}_l\} & \text{if } S = A_l(t), \\ \{\hat{t}_{2l}, \hat{t}_{l+1}\} & \text{if } S = {}^2A_l(t), l \text{ odd}, \\ \{\hat{t}_{2l+2}, \hat{t}_{2l-2}\} & \text{if } S = {}^2A_l(t), l \text{ even}, \\ \{\hat{t}_{2l}, \hat{t}_l\} & \text{if } S = B_l(t), \\ \{\hat{t}_{2l}, \hat{t}_{2l-2}, \hat{t}_l\} & \text{if } S = C_l(t), \\ \{\hat{t}_{2l-2}, \hat{t}_{2l-4}, \hat{t}_l\} & \text{if } S = D_l(t), \\ \{\hat{t}_{2l}, \hat{t}_{2l-2}\} & \text{if } S = {}^2D_l(t). \end{cases}$$

By Subsection 3.3.1 (also see [KL90]), if $H \in M_{\pi_{\mathcal{G}}(S)}$, then H is not a geometric maximal subgroup.

By [CCN$^+$85], we have that if $S \cong A_5(2)$ or ${}^2A_3(2^2)$, then the class $\mathcal{S}$ is empty, so we let $\pi_{\mathcal{S}}(S) = \varnothing$.

Table 10.4: Classical groups, class $\mathcal{S}$

S	$\pi_{\mathcal{S}}(S)$	(l,t)	S	$\pi_{\mathcal{S}}(S)$	(l,t)
$A_l(t)$	$\hat{t}_{l+1}, \hat{t}_l$	$(2,4),(5,t),$	$C_l(t)$	$\hat{t}_4, \hat{t}_2$	$l \in \{2,3\}, t > 2$ even
		$(7,2),(17,3),(19,2)$		5	$(3,2)$
		and $(3,2^k), k \geq 2$		$5, 13$	$(3,3)$
	$19, 127$	$(8,2)$		31	$(3,5)$
	13	$(3,3)$		$7, 17$	$(4,2)$
	73	$(9,2)$		$\hat{t}_{2l-2}$	$(5,2),(9,2)$
	89	$(11,2)$		17	$(6,2)$
	131071	$(17,2)$		$19, 41$	$(10,2)$
${}^2A_l(t^2)$	$7, 13$	$(3,5)$	$D_l(t)$	$\hat{t}_{2l-4}$	$(4,2),(4,5),(6,2),(10,2)$
	43	$(8,2)$		$13, 5$	$(4,3)$
	17	$(9,2)$		127	$(7,2)$
$B_l(t)$	$\hat{t}_{2l}, \hat{t}_{2l-2}$	$(9,3),$		$\hat{t}_6, \hat{t}_4$	$l = 4,\ t \notin \{2,3,5\}$
		$(3,t)$ with $t > 5$	${}^2D_l(t^2)$	$\hat{t}_{2l}, \hat{t}_{2l-2}$	$(9,2),(9,3),(10,2)$
	$\hat{t}_4, \hat{t}_3$	$(3,3),(3,5)$		17	$(5,2),(6,2)$
				$5, 17$	$(4,2)$

If S is not in the Table 10.4, then let

$$\pi_{\mathcal{S}}(S) = \begin{cases} \{\hat{t}_{l+1}\} & \text{if } S = A_l(t), \\ \{\hat{t}_{2l}\} & \text{if } S = {}^2A_l(t^2), l \text{ odd, or } S \in \{B_l(t), C_l(t), {}^2D_l(t^2)\}, \\ \{\hat{t}_{2l+2}\} & \text{if } S = {}^2A_l(t^2), l \text{ even}, \\ \{\hat{t}_{2l-2}\} & \text{if } S = D_l(t). \end{cases}$$

Using [CCN+85] for $S \in \{C_3(2), D_4(2)\}$ and Subsection 3.3.1 in the other cases, we have that if $H \in M_{\pi_S(S)}$, then H is not a maximal subgroup in the class $\mathcal{S}$ of S.

So, if $\pi(S) = \pi_{\mathcal{G}}(S) \cup \pi_{\mathcal{S}}(S)$, then $M_{\pi(S)} = \varnothing$. □

10.1 The proof

We are ready to prove the main theorem.

Proof of Theorem 8.1. In order to prove the claim, we apply Lemma 2.13.

Assume that $S \cong A_3(2)$. Using [GAP], and applying Lemma 2.13 with $\pi_0 = \{2\}$ and $\pi = \{5, 7\}$, we obtain the claim.

Assume that $S \cong A_2(t)$ *for some* $t = p = 2^u - 1, u \geq 3$. In this case X does not contain a non-trivial graph automorphism. Let $\pi_1 = \pi(t-1) - \{2\}$. Clearly, π_1 is not empty.

We claim that $P^{(\pi_1)}_{G,\mathrm{soc}G}(s)$ is irreducible. Note that we have $P^{(\pi_1 \cup \{p\})}_{X,S}(s) = P^{(p)}_{X,S}(s)$ (see Section 3.2). Take $h(s) = P^{(\pi_1)}_{G,\mathrm{soc}(G)}(s)$ and $\pi_0 = \{p\}$. By Proposition 9.3 we have that $h^{(p)}(s) = P^{(p)}_{G,\mathrm{soc}(G)}(s)$ is irreducible. Let $\pi = \{t_3\}$. It is easy to see that $|P^{(p)}_{X,S}(s)|_{t_3} = |S|_{t_3}$, so using Theorem 1.3, we get $|h^{(p)}(s)|_{t_3} = |P^{(p)}_{G,\mathrm{soc}G}(s)|_{t_3} = |S|^n_{t_3}$. Now, we have that $|S|_{t_3} > 7$. In fact, otherwise we get that $t^2 + t + 1$ divides 21, a contradiction. By [Mit11], we have that $P^{(\pi_1 \cup \pi_2)}_{X,S}(s) = 1$, hence $h^{(\pi_2)}(s) = 1$. Applying Lemma 2.13, we obtain the claim.

Now, we claim that $|P^{(\pi_1)}_{G,\mathrm{soc}(G)}(s)|_t = |S|^n_t$. In order to show this, it is enough to prove that $a_k(X, S) \neq 0$ where $k = \frac{t^3(t+1)(t^2+t+1)}{3}$. Let H be a subgroup of X such that $HS = X$, H is intersection of maximal subgroups of X and $|X : H| = k$. By [KL90] and [Mit11], if M is a maximal subgroup of X such that $MS = X$ and $|X : M|$ is a

π_1' number, then $|X : M| = k$ or $M \cap S$ is a parabolic subgroup of S. It is easy to see that the index of the intersection of two distinct parabolic subgroups (not necessarily containing the same Borel subgroup) of S can not be k. Thus H must be a maximal subgroup of X, hence $a_k(X, S) \neq 0$.

Finally, we claim that $P_{G,\mathrm{soc}(G)}(s)$ is irreducible. Take $h(s) = P_{G,\mathrm{soc}(G)}(s)$. As we have seen above, $h^{(\pi_1)}(s)$ is irreducible. Let $\pi = \{p, t_3\}$. As before, we have that $|h^{(\pi_1)}(s)|_v = |S|_v^n$ for each $v \in \pi$. Moreover, by Section 3.2, we have that $h^{(\pi)}(s) = 1$. Thus, applying Lemma 2.13, we obtain the claim.

Assume that $S \ncong A_3(2)$ and $S \ncong A_2(p)$ for each $p = 2^u - 1, u \geq 3$. We verify that the conditions of Lemma 2.13 are fulfilled. Take $h(s) = P_{G,\mathrm{soc}(G)}(s)$ and $\pi_0 = \{p\}$. By Proposition 9.3 we have that $P^{(p)}_{G,\mathrm{soc}(G)}(s)$ is irreducible. As in Proposition 10.1, let B be a Borel subgroup of S and let $\pi = \pi(S) - \pi(B)$. By Proposition 3.10 and Theorem 1.3, we get that $|P^{(p)}_{G,\mathrm{soc}(G)}(s)|_v = |S|_v^n$ for each $v \in \pi$. Moreover, by Theorem 1.3 and Proposition 10.1, we have that $P^{(\pi)}_{G,\mathrm{soc}(G)}(s) = P^{(\pi)}_{X,S}(n(s-1)+1) = 1$. So we can apply Lemma 2.13. □

10.2 Proof in some other cases

Using a slightly different strategy, Theorem 8.1 can be proved also for some S of low rank. For example, we have the following.

Proposition 10.2. *Let G be a monolithic primitive group with a simple component isomorphic to $S = {}^2A_2(t^2)$ and assume that there exists a prime divisor of $t+1$ greater than 3. We have that $P_{G,\mathrm{soc}(G)}(s)$ is irreducible.*

We recall that $|S| = \frac{t^3(t-1)(t+1)^2(t^2-t+1)}{(t+1,3)}$. Let p be the characteristic of S. Let $t = p^f$ for some $f \in \mathbb{N}, f \geq 1$. Let r be the greatest prime divisor of $t+1$ greater than 3. Recall that $S \cong \mathrm{PSU}(V)$, where V is a vector space of dimension 3 over $\mathbb{F}_{t^2}$, endowed with a unitary form. Suppose that M is a maximal subgroup of X such that $MS = X$ and $|X : M|_r = 1$. By [Mit11] and [Har26], we have that $M \cap S$ is isomorphic to one of the following groups:

- $\mathrm{Stab}_S(v)$, a stabilizer of a non-degenerate vector $v \in V$. This group has order $t(t+1)(t^2-1)/\delta$.
- $C_{(t+1)^2/\delta}.S_3$.

Let $r_1 = t_6$. Note that:

(1) If M is a maximal subgroup of X such that $MS = X$ and $|X : M|_r = 1$, then $|X : M|_{r_1} = |S|_{r_1}$.

(2) If $a_k(X, S) \neq 0$ and p divides k, then $|k|_p \geq t^2$.

(3) $a_{t^2(t^2-t+1)}(X, S) \neq 0$.

(4) $a_{\frac{t^3(t-1)(t^2-t+1)}{6}}(X, S) \neq 0$.

The first and the third statements are clear. We prove (2). Let K be a maximal subgroup of X such that $KS = X$. By [KL90], [Mit11] and [Har26], if $|X : K|_p \neq 1$, then $|X : K|_p \geq t^2$. Moreover, if $|X : K|_p = 1$, then $K \cap S = B$ is a Borel subgroup of S, i.e. the stabilizer of a totally singular vector of V. Assume that H is the intersection of two distinct Borel subgroups, i.e. $H = \mathrm{Stab}_S(v_1) \cap \mathrm{Stab}_S(v_2)$ for some $v_1, v_2 \in V$ totally singular vectors. Note that $\langle v_1, v_2 \rangle$ is non-degenerate, so H is contained in $\mathrm{Stab}_S(\langle v_1, v_2 \rangle)$, a maximal subgroup of index $t^2(t^2 - t + 1)$. Thus (2) is established.

In order to prove (4), we claim that if $H \in \mathcal{A}_{\frac{t^3(t-1)(t^2-t+1)}{6}}(X, S)$, then H is a maximal subgroup of X isomorphic to $C_{(t+1)^2/\delta}.S_3$. In fact, let $H \cap S$ be the intersection of two distinct maximal subgroups $\mathrm{Stab}_S(v_1)$ and $\mathrm{Stab}_S(v_2)$ for some v_1 and v_2 non-degenerate vectors. If $\langle v_1, v_2 \rangle$ is non-degenerate, then $|H \cap S| = \frac{(t+1)^2}{\delta}$, hence $K \notin \mathcal{A}_{\frac{t^3(t-1)(t^2-t+1)}{6}}(X, S)$ for each subgroup K of H. If $\langle v_1, v_2 \rangle$ is degenerate, then there exists $0 \neq v \in \langle v_1, v_2 \rangle$ such that v is totally singular. Thus $H \cap S$ is contained in the Borel subgroup $\mathrm{Stab}_S(v)$, so $q+1$ divides $|X : H|$, hence $H \notin \mathcal{A}_{\frac{t^3(t-1)(t^2-t+1)}{6}}(X, S)$.

Now, let $x = \Psi(r_1)$, $y = \Psi(p)$ and $D = \mathbb{Z}[X_{\pi(S)-\{r_1,p\}}]$. By the above consideration, we have that:

$$\Psi(P^{(r)}_{G,\mathrm{soc}(G)}(s)) = 1 - a(y)x^{nm},$$

where $m \in \mathbb{N} - \{0\}$ and $a(y) \in D[y]$ is the following polynomial:

$$a(y) = b + \sum_{i=0}^{nf} c_i y^{2nf+i},$$

with $b, c_0, c_{nf} \in D - \{0\}$ and $c_i \in E$ for $i \in \{2, ..., nf-1\}$. We claim that $P^{(r)}_{G,\mathrm{soc}(G)}(s)$ is irreducible. For a contradiction, suppose that $P^{(r)}_{G,\mathrm{soc}(G)}(s)$ is reducible. By Lemma 2.10, we have that $a(y)$ or $-a(y)$ is a non-trivial power in $D[y]$. Clearly this does not happen since b, c_0 and c_{nf} are not zero. Thus we have a contradiction and $P^{(r)}_{G,\mathrm{soc}(G)}(s)$ is irreducible.

Finally, we use Lemma 2.13. Let $h(s) = P_{G,\mathrm{soc}(G)}(s)$, $\pi_0 = \{r\}$ and $\pi = \{p, r_1\}$. By Section 3.2, we have that $h^{(\pi)}(s) = P^{(\pi)}_{G,\mathrm{soc}(G)}(s) = 1$. Hence we are done. $\square$

Chapter 11

On the irreducibility of the Dirichlet polynomial of a simple group of Lie type

In this section we deal with the case $G = S$ a simple group of Lie type. Our aim is to complete the proof of Theorem 8.2.

11.1 Preliminary results

We need some preliminary results.

Lemma 11.1. *Let n, m be two positive integers and let p be a prime number. If $p^n + 1 = m^k$ for some integer $k \geq 2$, then $n = 1$ and p is a Mersenne prime or $(p, n, m, k) = (2, 3, 3, 2)$.*

Proof. Assume that $k > 1$ and that (p, n, m, k) is a solution of $p^n + 1 = m^k$. Suppose that $n = 1$. Thus $p = m^k - 1$. Since $m - 1$ divides $m^k - 1$, it must be $m = 2$, so p is a Mersenne prime. Suppose that $n > 1$. Since $p^n = m^k - 1$, there is no Zsigmondy prime for $\langle m, k \rangle$. By Lemma 2.6, we have two cases:

- $m = 2^u - 1$ for some u and $k = 2$. In this case, we have that $p^n = 2^{u+1}(2^{u-1} - 1)$ and this yields $(p, n, m, k) = (2, 3, 3, 2)$.
- $m = 2$ and $k = 6$. In this case, $2^6 - 1 = 63$ is not a power of a prime.

This concludes the proof. □

Lemma 11.2. *Let t be a power of a prime number p. Assume that $t+1 = |t+1|_2|t+1|_3$. The number $\frac{t^3(t-1)(t+1)^2}{3}$ is a non trivial power of an integer if and only if $t = 17$.*

Proof. The result is clear for $t \leq 5$. So we assume that $t > 5$ and that $\frac{t^3(t-1)(t+1)^2}{3}$ is a non trivial power of an integer.

Suppose that $|t+1|_3 = 1$. Thus $t + 1 = 2^k$ for some $k \geq 3$ and it turns out that $\frac{(2^{k-1}-1)}{3}$ must be a non-trivial power. Since 3 divides $2^{k-1} - 1$ we have that $k - 1$ is even. If $\frac{k-1}{2}$ is odd, then $2^{\frac{k-1}{2}} - 1$ is a non-trivial power, otherwise $2^{\frac{k-1}{2}} + 1$ is a non-trivial power. Using Lemma 2.6, we get that $k = 7$, so $t = 2^7 - 1 = 127$. However, for $t = 127$, the number $\frac{t^3(t-1)(t+1)^2}{3}$ is not a non-trivial power.

Suppose that $t + 1 = 3^h 2^k$ for some $h \geq 1, k \geq 1$. First assume $k = 1$. We have that $t + 1 = 2 \cdot 3^h$. By Lemma 2.6, this yields $t = p$. So if $\frac{t^3(t-1)(t+1)^2}{3}$ is a non-trivial power, it must be a cube. Hence we have that $\frac{3^h-1}{|3^h-1|_2} = m^3$ for some $m \in \mathbb{N}$. Let $|3^h - 1|_2 = 2^l$ for some $l \in \mathbb{N}$. Since $t > 5$ then $h \geq 2$, hence $2^l m^3 + 1$ is divisible by 9. Now, the cubes modulo 9 are $0, 1$ and -1. Clearly m is not divisible by 3, so we have $2^l \equiv \pm 1 \pmod 9$. This implies that 3 divides l, hence $3^h - 1$ is a cube. Using Lemma 2.6, we get that $h = 2$, so $t = 17$. Moreover, for $t = 17$, the number $\frac{t^3(t-1)(t+1)^2}{3}$ is a cube.

Second assume that $k \geq 2$. We get that $3^h 2^{k-1} - 1$ is a non-trivial power. Using Lemma 2.6, we get $k = 1$, against the assumptions.

Finally, suppose that $k = 0$. Thus $t = 3^h - 1$. Using Lemma 2.6, we get $t = 8$. However, for $t = 8$, the number $\frac{t^3(t-1)(t+1)^2}{3}$ is not a non-trivial power. □

Proposition 11.3. *Let S be a simple group of Lie type of characteristic p. The Dirichlet polynomial $P_S^{(p)}(s)$ is reducible if and only if $S \cong A_1(p), p$ a Mersenne prime or $S \cong A_1(8)$.*

Proof. By Proposition 9.3, the result is true if the Lie rank of S is greater than 1. Assume that the Lie rank of S is 1, thus $P_S^{(p)}(s) = 1 - a^{1-s}$ for some $a \in \mathbb{N}$ (see Section 3.2). By [DL03a], Theorem 3, we have that $P_S^{(p)}(0) = -|S|_p = -p^n$ for some $n \in \mathbb{N} - \{0\}$. Thus $p^n + 1 = a$. Suppose that $P_S^{(p)}(s)$ is reducible. By Lemma 2.10, the number $p^n + 1$ is a non-trivial power of an integer. By Lemma 11.1, we have that either p is a Mersenne prime and $n = 1$, or $(p, n) = (2, 3)$. This implies that $S \cong A_1(p)$ where p is a Mersenne prime, or $S \cong A_1(8)$. Clearly, we have that $P_{A_1(p)}^{(p)}(s) = 1 - 2^{u(1-s)}$ for a Mersenne prime $p = 2^u - 1$ and $P_{A_1(8)}^{(2)}(s) = 1 - 9^{1-s}$ which are reducible polynomials. □

11.2 Proof of Theorem 8.2

Now we can complete the proof of Theorem 8.2.

Proof of Theorem 8.2. Here we deal with the cases which were not considered in Theorem 8.1 and Proposition 10.2. The result is already known for $S \cong A_1(t), {}^2B_2(t^2)$ and ${}^2G_2(t^2)$ (see [Pat09c]). Moreover, using [GAP], we obtain the claim for S isomorphic to one of the following groups: $A_2(3)$, ${}^2A_2(3) \cong C_2(3)$, ${}^2A_2(5)$, ${}^2A_3(2)$ and ${}^2A_4(2)$.

We want to apply Lemma 2.13, so we let $h(s) = P_S(s)$. Let $\pi_0 = \{p\}$. By Proposition 11.3, the polynomial $h^{(\pi_0)}(s) = P_S^{(p)}(s)$ is irreducible. We want to find a set of prime numbers π such that for each $r \in \pi$ we have $|h^{(\pi_0)}(s)|_r = |S|_r$. Finally, we prove that $(h(s), h^{(\pi_0)}(s)) = 1$. The rest of the proof is divided in three cases.

Assume that $S \cong {}^2A_5(2)$. Remind that $|S| = 2^{15} \cdot 3^6 \cdot 5 \cdot 7 \cdot 11$. Let $\pi = \{5, 7, 11\}$. We claim that

$$\Psi(P_S^{(\pi)}(s)) = 1 - 3x_2^8 x_3^4.$$

Let M be a maximal subgroup of S. By [CCN+85], if $|S : M|_r = 1$ for each $r \in \pi$, then M is isomorphic to M_{22} and there are 3 conjugacy classes of such subgroups. Moreover, if M_1 and M_2 are two distinct maximal subgroups of S isomorphic to M_{22}, then there exists a prime number $r \in \pi$ such that $|S : M_1 \cap M_2|_r = r$. In fact, there

is no maximal subgroup H of M_{22} such that $|M_{22} : H|_r = 1$ for each $r \in \pi$. Thus we obtain the claim.

Clearly $h^{(\pi)}(s) = P_S^{(\pi)}(s)$ is irreducible. In order to apply Lemma 2.13, it remains to show that $(h(s), h^{(\pi)}(s)) = 1$. For a contradiction, assume that $(h(s), h^{(\pi)}(s)) \neq 1$. Since $h^{(\pi)}(s)$ is irreducible, we have that $(h(s), h^{(\pi)}(s)) = h^{(\pi)}(s)$, so $h(s) = h^{(\pi)}(s)f(s)$ for some $f(s) \in \mathcal{R}'$. Now, $h^{(p)}(s) = h^{(\{\pi,p\})}(s)f^{(p)}(s) = f^{(p)}(s)$. We have that:

$$|h(s)|_3 = |h^{(\pi)}(s)|_3|f(s)|_3 \geq |h^{(\pi)}(s)|_3|h^{(p)}(s)|_3 = 3^8 > |S|_3.$$

This is a contradiction, so we get $(h(s), h^{(\pi)}(s)) = 1$.

Assume that $S \cong {}^2A_2(t^2)$ *with* $t \notin \{3, 5\}$ *and* $t + 1 = |t + 1|_2|t + 1|_3$. We recall that $|S| = \frac{t^3(t-1)(t+1)^2(t^2-t+1)}{(t+1,3)}$, where $t = p^f$ for some $f \in \mathbb{N} - \{0\}$. Let

$$\pi = \begin{cases} \{7\} & \text{if } t = 17, \\ \{\hat{t}_6\} & \text{otherwise.} \end{cases}$$

Clearly $|P_S^{(p)}(s)|_{t_6} = |S|_{\hat{t}_6}$. We claim that

$$P_S^{(\hat{t}_6)}(s) = 1 - \left(\frac{t^3(t-1)(t+1)^2}{3}\right)^{1-s}.$$

In fact, by Lemma 2.7 and the assumptions, we have that $|S|_{\hat{t}_6} > 7$. Thus, by [Mit11] and [Har26], if M is a maximal subgroup of S such that $|S : M|_{\hat{t}_6} = 1$, then M is isomorphic to $C_{\frac{t^2-t+1}{(t+1,3)}}.3$ and there is a unique conjugacy class of these subgroups. Furthermore, if M_1 and M_2 are two distinct maximal subgroups of S both isomorphic to $C_{\frac{t^2-t+1}{(t+1,3)}}.3$, then t_6 divides $|S : M_1 \cap M_2|$. Indeed, for a contradiction, suppose that $|S : M_1 \cap M_2|_{t_6} = 1$. Then $M_1 \cap M_2$ contains a cyclic subgroup C of order t_6. Clearly C is normal in M_1 and M_2, so C is normal in S, a contradiction. Thus we obtain the claim.

Now, we claim that $P_S^{(\pi)}(s)$ is irreducible. First, assume that $t \neq 17$. For a contradiction, assume that $P_S^{(\pi)}(s)$ is reducible. Thus $\Psi(P_S^{(t_6)}(s)) = 1 - ax_p^{3f}$ for

$$a = \Psi\left(\frac{(t-1)(t+1)^2}{3}\right)$$

(note that $p \neq 3$ by hypothesis). By Lemma 2.10 we have that a or $-a$ is a non-trivial power of exponent that divides $3f$, hence $\frac{t^3(t-1)(t+1)^2}{3}$ is a non-trivial power in $\mathbb{Z}$. Since $t+1 = |t+1|_2|t+1|_3$, using Lemma 11.2 we have that $t = 17$, against the assumptions. So $h^{(t_6)}(s) = P_S^{(t_6)}(s)$ is irreducible. Now, let $t = 17$. By [Mit11], if M is a maximal subgroups of S such that $|S:M|_7 = 1$, then M is isomorphic to $C_{91}.3$ or to $\mathrm{PSL}_2(7)$. Hence $|S:M|_{17} = |S|_{17}$. Thus, we obtain

$$\Psi(P_S^{(7)}(s)) = 1 - x_{17}^3(a + bx_{13})$$

for some $a, b \in \mathbb{Z}[x_2, x_3] - \{0\}$. Hence, by Lemma 2.10, $P_S^{(7)}(s)$ is irreducible.

In order to apply Lemma 2.13, it remains to show that $(h(s), h^{(\pi)}(s)) = 1$. For a contradiction, assume that $(h(s), h^{(\pi)}(s)) \neq 1$. Since $h^{(\pi)}(s)$ is irreducible, we have that $(h(s), h^{(\pi)}(s)) = h^{(\pi)}(s)$, so $h(s) = h^{(\pi)}(s)f(s)$ for some $f(s) \in \mathcal{R}'$. Now, $h^{(p)}(s) = h^{(\{\pi,p\})}(s)f^{(p)}(s) = f^{(p)}(s)$. Let r be a prime divisor of $t+1$. We have that:

$$|h(s)|_r = |h^{(\pi)}(s)|_r|f(s)|_r \geq |h^{(\pi)}(s)|_r|h^{(p)}(s)|_r \geq \frac{|t-1|_r|t+1|_r^2}{|3|_r}|t+1|_r|t^2-t+1|_r > |S|_r$$

since $|t+1|_r > 1$. This is a contradiction, so we get $(h(s), h^{(\pi)}(s)) = 1$.

Assume that $S \cong C_2(p)$ with $p > 3$ a Mersenne prime. We recall that $|S| = \frac{p^4(p-1)^2(p+1)^2(p^2+1)}{2}$.

Let π be the set of odd prime divisors of p^2+1. Clearly $|P_S^{(p)}(s)|_r = |S|_r$ for each $r \in \pi$. Note that $p_4 \in \pi$.

We claim that

$$P_S^{(\pi)}(s) = 1 - \left(\frac{p^2(p^2-1)}{2}\right)^{1-s} + a\left(\frac{p^4(p^2-1)^2}{4}\right)^{1-s} + b\left(\frac{p^4(p^2-1)^2}{2}\right)^{1-s} + c\left(p^4(p^2-1)^2\right)^{1-s},$$

for some $a, b, c \in \mathbb{Z}$. In fact, by Lemma 2.7 and the assumptions, we have that $|S|_{p_4} > 5$. Thus, by [Mit13], if M is a maximal subgroup of S such that $|S:M|_r = 1$ for each $r \in \pi$, then M is isomorphic to $\mathrm{PSL}_2(p^2).2$ and there is a unique conjugacy class of these subgroups. Now, let M be a maximal subgroup of S isomorphic to $\mathrm{PSL}_2(q^2).2$, and let H be the intersection of some subgroups conjugated to M. Assume that N is the subgroup of M of index 2. If $H \geq N$, then $H = N$, so H is normal

in two distinct maximal subgroups, a contradiction. So $H \not\geq N$, hence $H \cap N$ is a proper subgroup of N. Since the maximal subgroups of $N \cong \mathrm{PSL}_2(p^2)$ are known (see [Hup67, p. 213]) and $|p^2+1|_{\hat{p}_4} > 5$, we have that if $|N : N \cap H|_r = 1$ for each $r \in \pi$, then $N \cap H$ is isomorphic to the dihedral group D_{p^2+1} or to the cyclic group $C_{\frac{p^2+1}{2}}$. This proves the claim.

Now, we claim that if $g(s) \in \mathcal{R}$ is an irreducible factor of $P_S^{(\pi)}(s)$, then $|g(s)|_2 \geq |p+1|_2 = 2^m$. Let $y = \Psi(2^{1-s}), D = \mathbb{Z}[y]$ and let $Y = \Psi\left(\left(\frac{p^2(p-1)}{2}\right)^{1-s}\right)$. Note that $\frac{p^2(p-1)}{2}$ is not a non-trivial power of an integer (use Lemma 2.6 and the fact that p is a Mersenne prime greater than 3). We have that

$$f(Y) = \Psi(P_S^{(\pi)}(s)) = 1 - x_2^m Y + x_2^{2m}(a + bx_2 + cx_2^2)Y^2$$

is a polynomial in $D[Y]$. By Corollary 2.12, since Y is not a non-trivial power in D, we have that each irreducible factor of $f(Y)$ in $\mathbb{Z}[X_{\pi(S)}]$ is an element of $D[Y]$. If $a = b = c = 0$, then $\Psi(P_S^{(\pi)}(s))$ is clearly irreducible. Now, suppose that $a \neq 0$ or $b \neq 0$ or $c \neq 0$. Thus $f(Y)$ is a polynomial of degree 2 in Y. In this case, it is easy to see that the degree of the indeterminate x_2 in an irreducible factor of $f(Y)$ is at least m.

In order to apply Lemma 2.13, it remains to show that $(h(s), h^{(\pi)}(s)) = 1$. For a contradiction, assume that $(h(s), h^{(\pi)}(s)) \neq 1$. Let $g(s) = (h(s), h^{(\pi)}(s))$ and $h(s) = g(s)f(s)$ for some $f(s) \in \mathcal{R}'$. Now, $h^{(p)}(s) = g^{(p)}(s)f^{(p)}(s) = f^{(p)}(s)$, since $h^{(\pi \cup \{p\})}(s) = 1$ and $g(s)$ divides $h^{(\pi)}(s)$. We have that:

$$|h(s)|_2 = |g(s)|_2 |f(s)|_2 \geq |p+1|_2 |h^{(p)}(s)|_2 = 2|p+1|_2 |p+1|_2^2 > |S|_r$$

since $|p+1|_2 > 2$. This is a contradiction, so we get $(h(s), h^{(\pi)}(s)) = 1$. $\square$

Part III

Recognition of the characteristic of a simple group of Lie type from its Probabilistic Zeta function.

Chapter 12

Introduction

Let G be a simple group of Lie type. Because of the isomorphisms $\mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5)$, $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$, $\mathrm{PSL}_2(8) \cong {}^2G_2(3)'$, $\mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3)$ and $\mathrm{PSU}_3(3) \cong G_2(2)'$ some groups have more than one characteristic. Let π_G be the set of these characteristics. We say that *the characteristic of* G is the prime number $p \in \pi_G$ such that $|G|_p \geq |G|_r$ for all $r \in \pi_G$. So, for example, we have that the characteristic of $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$ is 2. characteristic

The aim of this part is to prove the following theorem.

Theorem 12.1. *Let G be a simple group and let H be a finite group. If $P_G(s) = P_H(s)$, then $H/\mathrm{Frat}(H) \cong G$.*

As we can see from Theorem 1.11, in order to prove Theorem 12.1, it suffices to recognize the characteristic of a group of Lie type from its Dirichlet polynomial. As in [KLST90, Definition 3.1], if $k > 1$, then we say that a prime p is the *dominant prime in* k if $|k|_p \geq |k|_r$ for all prime numbers r. In particular, we say that p is *the dominant prime of* G if p is the dominant prime in $|G|$. Note that if p is the characteristic of a group of Lie type G, then p is the dominant prime of G (with few exception). In fact we have the following. dominant prime

Theorem 12.2 ([KLST90, Theorem 3.3])**.** *Let G be a simple group of Lie type and let p be the characteristic of G. Then p is the dominant prime in $|G|$ except in the*

following cases:

- $G = \mathrm{PSL}_2(p)$ *and* p *is a Mersenne prime,* $p > 7$*. Here* 2 *is the dominant prime and* $p \neq 2$*.*
- $G = \mathrm{PSL}_2(r-1)$ *and* r *is a Fermat prime,* $r > 5$*. Here* r *is the dominant prime and* $p \neq r$*.*

If $f(s)$ is a Dirichlet polynomial and $|f(s)| > 1$, then we say that a prime p is the *dominant prime of* $f(s)$ if $|f(s)|_p \geq |f(s)|_r$ for all prime numbers r.

In most of cases, the dominant prime of G is also the dominant prime of $P_G(s)$. However, this is not true in general: for instance, if $G = \mathrm{PSU}_3(3) \cong G_2(2)'$, then $|G| = 2^5 \cdot 3^3 \cdot 7$ and $|P_G(s)| = 2^2 \cdot 3^3 \cdot 7$ (use [GAP]). So, for some cases, we need an alternative strategy. We have the following result.

Theorem 12.3 ([DL06, Theorem 3])**.** *Let* G *be a simple group of Lie type of characteristic* p*. Then* $|P_G^{(p)}(0)| = |G|_p$*.*

It turns out that if the dominant prime r of G is not the characteristic of G, then $|P_G^{(r)}(0)|$ is not a power of r (with at most six exceptions). In particular, we obtain the following.

Theorem 12.4. *Let* G *be a simple group of Lie type. Suppose that* G *is not isomorphic to one of the following groups:* $\mathrm{PSU}_3(3)$*,* $\mathrm{PSU}_6(2)$*,* $\mathrm{PSp}_4(8)$*,* $\mathrm{PSp}_4(9)$*,* $\mathrm{PSp}_8(3)$ *and* $\mathrm{P}\Omega_8^+(3)$*. Let* π *be the set of prime numbers* r *such that* $P_G^{(r)}(0)$ *is a power of* r*. The characteristic of* G *is the prime number* $p \in \pi$ *such that* $|P_G(s)|_p \geq |P_G(s)|_r$ *for all prime numbers* $r \in \pi$*.*

In order to prove our claim, we consider a classical group G of characteristic p and we prove that $a_k(G) \neq 0$ for some $k \in \mathbb{N}$ such that $|k|_p$ is large enough, i.e. sufficient to prove that, with some exceptions, p is the dominant prime of $P_G(s)$. The same strategy is applied to the exceptional groups.

Chapter 13

The analysis for the classical groups

13.1 Some preliminary result

Here prove two useful lemmas.

Lemma 13.1. *Let K be a finite group, let N be a subnormal subgroup of K and let H be a subgroup of K. We have that $|H||N|$ divides $|K||H \cap N|$.*

Proof. We claim that $|NH|$ divides $|K|$. Arguing by induction on the subnormal defect, it suffices to prove that if $N \trianglelefteq L$ and $L \leq K$, then $|NH|$ divides $|LH|$. Clearly,

$$LH = \bigcup_{k \in R} NkH$$

for some $R \subseteq L$ such that the union is disjoint. Since $N \trianglelefteq L$, if $k \in L$, then $NkH = kNH$, so $|NH| = |kNH| = |NkH|$ for all $k \in L$. Hence $|LH| = |R||NH|$ and we have the claim.

Now, since $|H||N| = |NH||H \cap N|$ and $|NH|$ divides $|K|$, we have that $|H||N|$ divides $|K||H \cap N|$. □

Corollary 13.2. *Let K be a finite group and let H_1, H_2 and H be three subgroups of K. Assume that H_1 is normal in H_2 and H_2 is subnormal in K. If $H_1(H \cap H_2) < H_2$, then $L = \frac{H_1(H \cap H_2)}{H_1}$ is a proper subgroup of H_2/H_1 such that $\frac{|H||H_2|}{|H_1|}$ divides $|K||L|$.*

Proof. Just apply Lemma 13.1, observing that $\frac{|H\cap H_2|}{|H_1|}$ divides $\frac{|H_1(H\cap H_2)|}{|H_1|} = \frac{|H\cap H_2|}{|H\cap H_1|}$.
□

Table 13.1: $h(n,q)$ for a classical simple group G

Case	G	Conditions	$h(n,q)$
L1	$\mathrm{PSL}_n(q)$	$n \in \{3,5\}, (n,q) \neq (3,4)$	$\frac{n(q^n-1)}{(q-1,n)(q-1)}$
L2	$\mathrm{PSL}_4(q)$	$q \geq 4$	$\frac{2q^2(q^4-1)(q+1)}{(q-1,4)}$
L3	$\mathrm{PSL}_n(q)$	$n \geq 6$	$\frac{q^{\frac{(n-2)(n-3)}{2}}(q-1)}{(q-1,n)}\prod_{i=1}^{n-2}(q^i-1)$
U1	$\mathrm{PSU}_n(q)$	$n \in \{3,5,7\}$, $q \geq 7$ if $n=3$, $q \geq 3$ if $n=5$	$\frac{n(q^n+1)}{(q+1,n)(q+1)}$
U2	$\mathrm{PSU}_4(q)$	$q \geq 4$	$\frac{2q^2(q-1)^2(q+1)^3}{(q+1,4)}$
U3	$\mathrm{PSU}_6(q)$	$q \geq 3$	$\frac{3q^3(q^3+1)(q^6-1)}{(q+1,6)(q+1)}$
U4	$\mathrm{PSU}_n(q)$	$n \geq 8$	$\frac{q^{\frac{(n-3)(n-4)+6}{2}}(q+1)(q^2-1)(q^3+1)}{(q+1,n)}\prod_{i=2}^{n-3}(q^i-(-1)^i)$
S	$\mathrm{PSp}_{2n}(q)$	$n \geq 2, (n,q) \neq (3,2)$	$\frac{dq^{n^2/d}}{(q-1,2)}\prod_{i=1}^{n/d}(q^{2id}-1)$
O	$\mathrm{P}\Omega_{2n+1}(q)$	$n \geq 3, (n,q) \neq (3,3)$	$q^{n^2-3n+3}(q^2-1)(q^{n-1}+1)\prod_{i=1}^{n-2}(q^{2i}-1)$
O^+1	$\mathrm{P}\Omega^+_{2n}(q)$	$q \geq 4$	$2^{\alpha_+}q^{(n-1)(n-2)}(q+1)(q^{n-1}+1)\prod_{i=1}^{n-2}(q^{2i}-1)$
O^+2	$\mathrm{P}\Omega^+_{2n}(q)$	$q \leq 3, n \geq 5, (n,q) \neq (5,2)$	$2^{\alpha_+}q^{n^2-5n+8}(q^4-1)(q^{n-2}+1)\prod_{i=1}^{n-3}(q^{2i}-1)$
O^-1	$\mathrm{P}\Omega^-_{2n}(q)$	$q \geq 4$	$2^{\alpha_-}q^{(n-1)(n-2)}(q-1)(q^{n-1}+1)\prod_{i=1}^{n-2}(q^{2i}-1)$
O^-2	$\mathrm{P}\Omega^-_{2n}(q)$	$q \leq 3, n \geq 5, (n,q) \neq (5,2)$	$\frac{2q^{n^2-5n+8}(q^2-1)^2(q^{n-2}+1)}{(q-1,2)}\prod_{i=1}^{n-3}(q^{2i}-1)$

In Table 13.1, we have that

$$\alpha_+ = \begin{cases} -1 & \text{if } q \text{ is odd and } n \text{ is even,} \\ 0 & \text{if } qn \text{ is odd,} \\ 1 & \text{if } q \text{ is even.} \end{cases}$$

$$\alpha_- = \begin{cases} -1 & \text{if } q \text{ is odd and } n\frac{q-1}{2} \text{ is even,} \\ 0 & \text{if } q \text{ is odd and } n\frac{q-1}{2} \text{ is odd,} \\ 1 & \text{if } q \text{ is even.} \end{cases}$$

and d is the smallest prime divisor of n.

Theorem 13.3. *Let G and $h(n,q)$ be as in Table 13.1, under the Conditions given in Table 13.1. Each subgroup of G of order $h(n,q)$ is a maximal subgroup, except if case L3 holds. In general, we have that $a_{|G|/h(n,q)}(G) \neq 0$.*

Proof. In this proof, we use the results of Subsection 3.3.1. In the cases L1, L2, U1, U2 and U3, it is easy to see that if a subgroup of G has order $h(n,q)$, then it is a maximal subgroup.

We introduce a notation. Given a group A and a positive rational number k, let $\mathcal{M}(A,k)$ be the set of representatives of the conjugacy classes of the maximal subgroups of A whose order is divisible by k, i.e. $\mathcal{M}(A,k)$

$$\mathcal{M}(A,k) = \left\{ M \in \mathcal{M}(A) : \frac{|M|}{k} \in \mathbb{Z} \right\}$$

where $\mathcal{M}(A)$ is the set of representatives of the conjugacy classes of the maximal subgroups of A. When we describe the elements of this set we write the type and the class of each maximal subgroup (using the notation of [KL90], Table 2.5 A-F).

First, we consider the case L3.

$$\text{Case L3: } G = \mathrm{PSL}_n(q),\ n \geq 6.$$

We have that the elements of $\mathcal{M}(G, h(n,q))$ are:

M_1: P_1 in $\mathcal{C}_1$.

M_2: P_2 in $\mathcal{C}_1$.

Let H be a subgroup of G of order $h(n,q)$. We claim that $\mu_G(H) = 2$.

Let V be a vector space of dimension n over $\mathbb{F}_q$. Assume that $V = \langle e_1, ..., e_n \rangle$. We may identify $G = \mathrm{PSL}_n(q)$ with $\mathrm{PSL}(V)$. A maximal subgroup of type P_i in $\mathrm{PSL}(V)$ is the group $\mathrm{Stab}_G(W_i)$ or $\mathrm{Stab}_G(W_i^*)$, where W_i is a subspace of V of dimension i and W_i^* is a complement of W_i in V. Moreover Stab_G yields a 1-1 correspondence

between the set of proper non-zero subspace of V and the set of maximal subgroups of G in the class $\mathcal{C}_1$.

As we have seen above, we have that if $H \leq M$ for a maximal subgroup M of G, then M is of type P_i, $i \in \{1,2\}$. Let $K_j = \mathrm{Stab}_G(\langle e_j \rangle)$ and $K_j^* = \mathrm{Stab}_G(\langle e_j \rangle^*)$ for $j \in \{1,2\}$, $J = \mathrm{Stab}_G(\langle e_1, e_2 \rangle)$ and $J^* = \mathrm{Stab}_G(\langle e_1 \rangle^* \cap \langle e_2 \rangle^*)$. Clearly, a maximal subgroup of type P_1 is conjugate in G to K_1 or K_1^*, and a maximal subgroup of type P_2 is conjugate in G to J or J^*. Since $|H| = h(n,q)$, without loss of generality, we may assume that $H = K_1 \cap K_2 \cap K_1^* \cap K_2^* \cap J \cap J^*$. In particular, we have that the set of maximal subgroups of G which contain H is $\mathcal{M}_H = \{K_1, K_2, K_1^*, K_2^*, J, J^*\}$. Set $\mathcal{Y} = \{Y \subseteq \mathcal{M}_H : \bigcap_{M \in Y} M = H\}$. By [Sta97, Corollary 3.9.4], we have that

$$\mu_G(H) = \sum_{Y \in \mathcal{Y}} (-1)^{|Y|}.$$

An easy computation shows that $\mu_G(H) = 2$. This completes the proof of Case L3.

Now, we deal with the remaining cases. We want to show that if a H is a subgroup of G and $|H| = h(n,q)$, then H is a maximal subgroup. The structure of the proof is almost the same in all the cases. We find the elements of $\mathcal{M}(G, h(n,q))$ (using the results of Subsection 3.3.1) and we denote them by $M_0, ..., M_k$, for some $k \in \mathbb{N}$. The first element (M_0) is a maximal subgroup such that $|M_0| = h(n,q)$. The order of the other elements of $\mathcal{M}(G, h(n,q))$ is different from $h(n,q)$ (except in case S, $n = 2$).

Let $M \in \mathcal{M}(G, h(n,q))$ such that $|M| \neq |M_0|$. We claim that

(†) the group M does not properly contain H.

We argue by contradiction, so we assume that $H < M$.

There exists a simple group $S = H_2/H_1$ where H_1 and H_2 are two subgroups of M such that $H_1 \trianglelefteq H_2$ and the group H_2 is subnormal in M. Here $|S|$ does not divide $h(n,q)$, hence $H_1(H \cap H_2) < H_2$. We let $h'(n,q) = \frac{|S|}{|M|} h(n,q)$, we find the elements of $\mathcal{M}(S, h'(n,q))$ and we denote them by $N_1, ..., N_j$.

We claim that $\mathcal{M}(S, h'(n,q)) \neq \varnothing$. Since $H < M$ and $H_1(H \cap H_2) < H_2$, by Corollary 13.2 with $K = M$, we have that there exists a (maximal) subgroup N of

S such that $|H||S| = |M|h'(n,q)$ divides $|M||N|$, i.e. the ratio $\frac{|N|}{h'(n,q)}$ is an integer number. So we have that $\mathcal{M}(S, h'(n,q)) \neq \varnothing$, in particular $N \in \mathcal{M}(S, h'(n,q))$. As before, there exists a simple group $T = \tilde{H}_2/\tilde{H}_1$ where $\tilde{H}_1$ and $\tilde{H}_2$ are two subgroups of N such that $\tilde{H}_1 \trianglelefteq \tilde{H}_2$ and the group $\tilde{H}_2$ is subnormal in N. Again, $|T|$ does not divide $h(n,q)$. We let $h''(n,q) = \frac{|T|}{|N|}h'(n,q)$, we find the elements of $\mathcal{M}(T, h''(n,q))$ and we denote them by $L_1, ..., L_m$.

Let $\tilde{H} = \frac{H_1(H \cap H_2)}{H_1}$, which is a subgroup of S. By Corollary 13.2, the number $\frac{|\tilde{H}|}{h'(n,q)}$ is an integer, hence we may assume that $\tilde{H} < N$ (clearly $\tilde{H} \neq N$ since $|T|$ does not divide $h(n,q)$.) We claim that $\mathcal{M}(T, h''(n,q)) \neq \varnothing$. Since $\tilde{H} < N$, by Corollary 13.2, there exists a (maximal) subgroup L of T such that $|\tilde{H}||T|$ divides $|N||L|$ (note that $\tilde{H}_1(\tilde{H} \cap \tilde{H}_2) < \tilde{H}_2$ since $|T|$ does not divide $h(n,q)$). Hence the ratio $\frac{|L|}{h''(n,q)}$ is an integer number. This contradicts $\mathcal{M}(T, h''(n,q)) = \varnothing$ and we obtain the claim. So, we have $\mathcal{M}(T, h''(n,q)) \neq \varnothing$, in particular $L \in \mathcal{M}(T, h''(n,q))$. There exists a simple group $U = \hat{H}_2/\hat{H}_1$ where $\hat{H}_1$ and $\hat{H}_2$ are two subgroups of L such that $\hat{H}_1 \trianglelefteq \hat{H}_2$ and the group $\hat{H}_2$ is subnormal in L. Moreover, $|U|$ does not divide $h(n,q)$. We define $h'''(n,q) = \frac{|U|}{|L|}h''(n,q)$.

Let $\hat{H} = \frac{\tilde{H}_1(\tilde{H} \cap \tilde{H}_2)}{\tilde{H}_1}$, which is a subgroup of T. By Corollary 13.2, the number $\frac{|\hat{H}|}{h''(n,q)}$ is an integer, hence we may assume that $\hat{H} < L$ (clearly $\hat{H} \neq L$ since $|U|$ does not divide $h(n,q)$.) By Corollary 13.2, there exists a subgroup Y of U such that $|\hat{H}||U|$ divides $|L||Y|$ (note that $\hat{H}_1(\hat{H} \cap \hat{H}_2) < \hat{H}_2$ since $|U|$ does not divide $h(n,q)$). Hence the ratio $\frac{|Y|}{h'''(n,q)}$ is an integer number, so $\mathcal{M}(U, h'''(n,q)) \neq \varnothing$.

However, in our analysis we prove that at least one of the sets $\mathcal{M}(S, h'(n,q))$, $\mathcal{M}(T, h''(n,q))$ and $\mathcal{M}(U, h'''(n,q))$ is empty, hence we have a contradiction and (†) holds. We conclude that a subgroup of G of order $h(n,q)$ is a maximal subgroup isomorphic to M_0.

EXAMPLE. Let $G = \mathrm{P}\Omega^+_{10}(2)$. By [CCN+85], the maximal subgroups of G are known. We want to prove that if H is a subgroup of G and $h = |H| = 3110400$, then H is a maximal subgroup. The elements of $\mathcal{M}(G, h)$ are:

M_0: $O_4^-(2) \times O_6^-(2)$ in $\mathcal{C}_1$. Here $|M_0| = h$.

M_1: $\mathrm{Sp}_8(2)$ in $\mathcal{C}_1$. We have that $M_1 \cong \mathrm{PSp}_8(2)$ and we let $S = \mathrm{PSp}_8(2)$, $h' = h$. Note that $|S|$ does not divide h. By [CCN$^+$85], the maximal subgroups of $\mathrm{PSp}_8(2)$ are known, so the unique element of $\mathcal{M}(S, h')$ is:

N_1: $O_8^+(2)$ in $\mathcal{C}_8$. We have that $N_1 \cong \mathrm{P}\Omega_8^+(2) : 2$, we let $T = \mathrm{P}\Omega_8^+(2)$ and $h'' = h'/2$. Note that $|T|$ does not divide h. By [CCN$^+$85], the maximal subgroups of $\mathrm{P}\Omega_8^+(2)$ are known and we have that $\mathcal{M}(T, h'') = \varnothing$. By Corollary 13.2, since $\mathcal{M}(T, h'') = \varnothing$, we have that $M_1 \cong S$ does not contain a subgroup of order h.

M_2: P_1 in $\mathcal{C}_1$. We have that $M_2 \cong 2^8 : \mathrm{P}\Omega_8^+(2)$ and we let $S = \mathrm{P}\Omega_8^+(2)$, so $h' = h/2^8$. Note that $|S|$ does not divide h. By [CCN$^+$85], the maximal subgroups of $\mathrm{P}\Omega_8^+(2)$ are known and we have that $\mathcal{M}(S, h') = \varnothing$. By Corollary 13.2, since $\mathcal{M}(S, h') = \varnothing$, we have that M_2 does not contain a subgroup of order h.

So the claim is proved.

Case U4: $G = \mathrm{PSU}_n(q)$, $n \geq 8$.

The elements of $\mathcal{M}(G, h(n, q))$ are:

M_0: $\mathrm{GU}_3(q) \perp \mathrm{GU}_{n-3}(q)$ in $\mathcal{C}_1$.

M_1: $\mathrm{GU}_1(q) \perp \mathrm{GU}_{n-1}(q)$ in $\mathcal{C}_1$. Here $S = \mathrm{PSU}_{n-1}(q)$ and we have that the unique element of $\mathcal{M}(S, h'(n, q))$ is:

N_1: $\mathrm{GU}_1(q) \perp \mathrm{GU}_{n-2}(q)$ in $\mathcal{C}_1$. Here $T = \mathrm{PSU}_{n-2}(q)$ and we have that $\mathcal{M}(T, h''(n, q)) = \varnothing$.

M_2: $\mathrm{GU}_2(q) \perp \mathrm{GU}_{n-2}(q)$ in $\mathcal{C}_1$. Here $S = \mathrm{PSU}_{n-2}(q)$ and we have that $\mathcal{M}(S, h'(n, q)) = \varnothing$.

M_3: P_1 in $\mathcal{C}_1$. Here $S = \mathrm{PSU}_{n-2}(q)$ and we have that $\mathcal{M}(S, h'(n, q)) = \varnothing$.

CASE S: $G = \mathrm{PSp}_{2n}(q)$, $n \geq 2$, $(n,q) \neq (3,2)$.

The elements of $\mathcal{M}(G, h(n,q))$ are:

M_0: $\mathrm{Sp}_{2n/d}(q^d)$ in $\mathcal{C}_3$.

M_1: $O^-_{2n}(q), q$ even in $\mathcal{C}_8$. If $n = 2$, then $M_1 \cong M_0$. Assume that $n \geq 3$. In this case $S = \mathrm{P}\Omega^-_{2n}(q)$ and we have that $\mathcal{M}(S, h'(n,q)) = \varnothing$.

M_2: $G_2(q)$ in $\mathcal{S}$, q even and $n = 3$. Here $S = G_2(q)$ and we have that $\mathcal{M}(S, h'(n,q)) = \varnothing$ (see [Kle88a]).

CASE O: $G = \mathrm{P}\Omega_{2n+1}(q)$, $n \geq 3$, $(n,q) \neq (3,3)$.

The elements of $\mathcal{M}(G, h(n,q))$ are:

M_0: $O_3(q) \perp O^-_{2n-2}(q)$ in $\mathcal{C}_1$.

M_1: P_1 in $\mathcal{C}_1$, $n \geq 4$. Here $S = \mathrm{P}\Omega_{2n-1}(q)$ and we have that $\mathcal{M}(S, h'(n,q)) = \varnothing$.

M_2: $O_{2n-1}(q) \perp O^{\pm}_2(q)$ in $\mathcal{C}_1$. Here $S = \mathrm{P}\Omega_{2n-1}(q)$ and we have that $\mathcal{M}(S, h'(n,q)) = \varnothing$.

M_3: $O_1(q) \perp O^{\pm}_{2n}(q)$ in $\mathcal{C}_1$. Here $S = \mathrm{P}\Omega^{\pm}_{2n}(q)$ (note that if $n = 3$, then $S = \mathrm{PSL}_4(q)$ or $\mathrm{PSU}_4(q)$) and the elements of $\mathcal{M}(S, h'(n,q))$ are:

- N_1: $O_1(q) \perp O_{2n-1}(q)$ in $\mathcal{C}_1$. Here $T = \mathrm{P}\Omega_{2n-1}(q)$ (note that if $n = 3$, then $T = \mathrm{PSp}_4(q)$) and we have that $\mathcal{M}(T, h''(n,q)) = \varnothing$.
- N_2: $\mathrm{P}\Omega_7(q)$ in $\mathcal{S}$, $n = 4$. Here $S = \mathrm{P}\Omega_7(q)$ and we have that $\mathcal{M}(T, h''(n,q)) = \varnothing$.

CASE O$^+$1: $G = \mathrm{P}\Omega^+_{2n}(q)$, $n \geq 4$, $q \geq 4$.

The elements of $\mathcal{M}(G, h(n,q))$ are:

M_0: $O_2^-(q) \perp O_{2n-2}^-(q)$ in $\mathcal{C}_1$.

M_1: $O_1(q) \perp O_{2n-1}(q)$, in $\mathcal{C}_1$, q odd. Here $S = \mathrm{P}\Omega_{2n-1}(q)$ and we have that $\mathcal{M}(S, h'(n,q)) = \varnothing$.

M_2: $\mathrm{Sp}_{2n-2}(q)$ in $\mathcal{C}_1$, q even. Here $S = \mathrm{PSp}_{2n-2}(q)$ and we have that $\mathcal{M}(S, h'(n,q)) = \varnothing$.

CASE $\mathrm{O}^\varepsilon 2$, $\varepsilon \in \{+,-\}$: $G = \mathrm{P}\Omega_{2n}^\varepsilon(q)$, $n \geq 5$, $q \leq 3$, $(n,q) \neq (5,2)$, .

The elements of $\mathcal{M}(G, h(n,q))$ are:

M_0: $O_4^{-\varepsilon}(q) \perp O_{2n-4}^-(q)$ in $\mathcal{C}_1$.

M_1: P_1 in $\mathcal{C}_1$. Here $S = \mathrm{P}\Omega_{2n-2}^\varepsilon(q)$ and the elements of $\mathcal{M}(S, h'(n,q))$ are:

- N_1: $O_1(3) \perp O_{2n-3}(3)$ in $\mathcal{C}_1$, $q = 3$. Here $T = \mathrm{P}\Omega_{2n-3}(3)$ and we have that $\mathcal{M}(T, h''(n,3)) = \varnothing$.
- N_2: $\mathrm{Sp}_{2n-4}(2)$ in $\mathcal{C}_1$, $q = 2$. Here $S = \mathrm{PSp}_{2n-4}(2)$ and we have that $\mathcal{M}(T, h''(n,2)) = \varnothing$.

M_2: $O_1(3) \perp O_{2n-1}(3)$, in $\mathcal{C}_1$, $q = 3$. Here $S = \mathrm{P}\Omega_{2n-1}(3)$ and the elements of $\mathcal{M}(S, h'(n,q))$ are:

- N_1: P_1 in $\mathcal{C}_1$. Here $T = \mathrm{P}\Omega_{2n-3}(3)$ and that $\mathcal{M}(T, h''(n,3)) = \varnothing$.
- N_2: $O_1(3) \perp O_{2n-2}^\pm(3)$ in $\mathcal{C}_1$. Here $T = \mathrm{P}\Omega_{2n-2}^\pm(3)$ and we have that the unique element of $\mathcal{M}(T, h''(n,q))$ is:
  - L_1: $O_1(3) \perp O_{2n-3}(3)$ in $\mathcal{C}_1$. Here $U = \mathrm{P}\Omega_{2n-3}(3)$ and we have that $\mathcal{M}(U, h'''(n,3)) = \varnothing$.
- N_3: $O_{2n-3}(3) \perp O_2^\pm(3)$ in $\mathcal{C}_1$. Here $T = \mathrm{P}\Omega_{2n-3}(3)$ and that $\mathcal{M}(T, h''(n,3)) = \varnothing$.

M_3: $O_3(3) \perp O_{2n-3}(3)$, in $\mathcal{C}_1$, $q = 3$. Here $S = \mathrm{P}\Omega_{2n-3}(3)$ and we have that $\mathcal{M}(S, h'(n,q)) = \varnothing$.

M_4: $O_2^-(q) \perp O_{2n-2}^{-\varepsilon}(q)$, in $\mathcal{C}_1$. Here $S = \mathrm{P}\Omega_{2n-2}^-(q)$ and the elements of $\mathcal{M}(S, h'(n,q))$ are:

N_1: $O_1(3) \perp O_{2n-3}(3)$ in $\mathcal{C}_1$, $q = 3$. Here $T = \mathrm{P}\Omega_{2n-3}(3)$ and we have that $\mathcal{M}(T, h''(n,3)) = \varnothing$.

N_2: $\mathrm{Sp}_{2n-4}(2)$ in $\mathcal{C}_1$, $q = 2$. Here $T = \mathrm{PSp}_{2n-4}(2)$ and we have that $\mathcal{M}(T, h''(n,2)) = \varnothing$.

M_5: $\mathrm{Sp}_{2n-2}(2)$ in $\mathcal{C}_1$, $q = 2$. Here $S = \mathrm{PSp}_{2n-2}(2)$ and the elements of $\mathcal{M}(S, h'(n,q))$ are:

N_1: P_1 in $\mathcal{C}_1$. Here $T = \mathrm{PSp}_{2n-4}(2)$ and we have that $\mathcal{M}(T, h''(n,3)) = \varnothing$.

N_2: $\mathrm{Sp}_2(2) \perp \mathrm{Sp}_{2n-4}(2)$ in $\mathcal{C}_1$. Here $S = \mathrm{PSp}_{2n-4}(2)$ and we have that $\mathcal{M}(T, h''(n,2)) = \varnothing$.

N_3: $O_{2n-2}^{\pm}(2)$ in $\mathcal{C}_1$. Here $S = \mathrm{P}\Omega_{2n-2}^{\pm}(2)$. Assume that $S = \mathrm{P}\Omega_{2n-2}^{+}(2)$. The unique element of $\mathcal{M}(S, h'(n,q))$ is:

L_1: $\mathrm{Sp}_{2n-4}(2)$ in $\mathcal{C}_1$, $q = 2$. Here $U = \mathrm{PSp}_{2n-4}(2)$ and we have that $\mathcal{M}(U, h''(n,2)) = \varnothing$.

Assume that $S = \mathrm{P}\Omega_{2n-2}^-(2)$. The unique element of $\mathcal{M}(S, h'(n,q))$ is:

L_1: $\mathrm{Sp}_{2n-4}(2)$ in $\mathcal{C}_1$, $q = 2$. Here $U = \mathrm{PSp}_{2n-4}(2)$ and we have that $\mathcal{M}(U, h''(n,2)) = \varnothing$.

Case O$^-$1: $G = \mathrm{P}\Omega_{2n}^-(q)$, $n \geq 4$, $q \geq 4$.

The elements of $\mathcal{M}(G, h(n,q))$ are:

M_0: $O_2^+(q) \perp O_{2n-2}^-(q)$ in $\mathcal{C}_1$.

M_1: P_1 in $\mathcal{C}_1$. Here $S = \mathrm{P}\Omega^-_{2n}(q)$ and we have that $\mathcal{M}(S, h'(n,q)) = \varnothing$.

M_2: $O_1(q) \perp O_{2n-1}(q)$ in $\mathcal{C}_1$, q odd. Here $S = \mathrm{P}\Omega_{2n-1}(q)$ and we have that $\mathcal{M}(S, h'(n,q)) = \varnothing$.

M_3: $\mathrm{Sp}_{2n-2}(q)$ in $\mathcal{C}_1$, q even. Here $S = \mathrm{PSp}_{2n-2}(q)$ and we have that $\mathcal{M}(S, h'(n,q)) = \varnothing$.

M_4: $\mathrm{P}\Omega_7(q)$ in $\mathcal{S}$, $n = 4$. Here $S = \mathrm{P}\Omega_7(q)$ and we have that $\mathcal{M}(S, h'(n,q)) = \varnothing$.

M_5: $\mathrm{PSp}_6(q)$ in $\mathcal{S}$, $n = 4$. Here $S = \mathrm{PSp}_6(q)$ and we have that $\mathcal{M}(S, h'(n,q)) = \varnothing$.

13.2 Recognition of the characteristic of a Classical group

Recall the definition of the characteristic of G given in the introduction (p.137). In particular note that the characteristic of $\mathrm{PSL}_2(7)$ and $\mathrm{PSU}_3(3)$ is 2, the characteristic of $\mathrm{PSL}_2(8)$ and $\mathrm{PSU}_4(2)$ is 3 and the characteristic of $\mathrm{PSL}_2(4)$ is 5.

Proposition 13.4. *Let G be a classical simple group of characteristic p, let r be a prime number different from p and assume that the following cases do not occur:*

- $G = \mathrm{PSL}_2(q)$, $q > 7$ *Mersenne prime and* $r = 2$;
- $G = \mathrm{PSL}_2(q)$, $q + 1$ *Fermat prime and* $r = q + 1$;
- $G = \mathrm{PSU}_n(q)$, $(n, q, r) \in \{(3,3,3), (6,2,3)\}$;
- $G = \mathrm{PSp}_8(3)$ *and* $r = 2$;
- $G = \mathrm{PSp}_4(q)$, q *Fermat prime and* $r = 2$;
- $G = \mathrm{PSp}_4(9)$ *and* $r = 2$;

- $G = \mathrm{PSp}_4(q)$, $q > 5$, $q-1$ *Mersenne prime and* $r = q-1$*;*
- $G = \mathrm{PSp}_4(q)$, $q > 5$, q *Mersenne prime and* $r = 2$*;*
- $G = \mathrm{PSp}_4(q)$, $q > 5$, $q+1$ *Fermat prime and* $r = q+1$*;*
- $G = \mathrm{PSp}_4(8)$ *and* $r = 3$*;*
- $G = \mathrm{PSp}_4(q)$, $q > 5$, q^2+1 *Fermat prime and* $r = q^2+1$*;*
- $G = \mathrm{P}\Omega_8^+(2)$ *and* $r = 3$.

Then $|P_G(s)|_p > |G|_r \geq |P_G(s)|_r$.

Proof. Let $G = \mathrm{PSL}_2(q)$. By [Pat09c, Section 7], we have that $|P_G(s)|_p = q$. Thus the result holds.

Assume that $G \neq \mathrm{PSL}_2(q)$. Using [GAP] we get Table 13.3. Moreover, Table 13.4 is obtained from Theorem 13.3 and Table 13.3. Using [CCN$^+$85] and arguing as in the proof of Theorem 13.3, we have that:

- $a_{28431}(\mathrm{P}\Omega_7(3)) \neq 0$, so $|P_{\mathrm{P}\Omega_7(3)}|_3 \geq 3^7$;
- $a_{1120}(\mathrm{P}\Omega_8^+(2)) \neq 0$, so $|P_{\mathrm{P}\Omega_8^+(2)}|_2 \geq 2^5$;
- $a_{24192}(\mathrm{P}\Omega_8^-(2)) \neq 0$, so $|P_{\mathrm{P}\Omega_8^-(2)}|_2 \geq 2^7$;
- $a_{9552816}(\mathrm{P}\Omega_8^+(3)) \neq 0$, so $|P_{\mathrm{P}\Omega_8^+(3)}|_3 \geq 3^8$;
- $a_{8159697}(\mathrm{P}\Omega_8^-(3)) \neq 0$, so $|P_{\mathrm{P}\Omega_8^-(3)}|_3 \geq 3^7$;
- $a_{7555072}(\mathrm{P}\Omega_{10}^+(2)) \neq 0$, so $|P_{\mathrm{P}\Omega_{10}^+(2)}(s)|_2 \geq 2^{11}$;
- $a_{104448}(\mathrm{P}\Omega_{10}^-(2)) \neq 0$, so $|P_{\mathrm{P}\Omega_{10}^-(2)}(s)|_2 \geq 2^{11}$.

Comparing Table 13.3 and Table 13.4 with Table 13.2 we obtain the claim. Note that Table 13.2 is obtained using Lemma 2.9. □

Table 13.2: r-part of the order of a classical simple group G, for a prime divisor r of the order of G, $r \neq p$.

G	r	conditions	$\lvert G\rvert_r \lvert\delta(G)\rvert_r$
$\mathrm{PSL}_n(q)$	2	$t=1, \lvert q-1\rvert_2 > \lvert q+1\rvert_2$	$\lvert q-1\rvert_2^{n-1}\lvert n!\rvert_2$
		$t=1, \lvert q-1\rvert_2 < \lvert q+1\rvert_2$	$2^{\left[\frac{n-1}{2}\right]}\lvert q+1\rvert_2^{\left[\frac{n}{2}\right]}\lvert n!\rvert_2$
	$\neq 2$	$t=1$	$\lvert q-1\rvert_r^{n-1}\lvert n!\rvert_r$
		$t>1$	$\lvert q^t-1\rvert_r^{\left[\frac{n}{t}\right]}\lvert \left[\frac{n}{t}\right]!\rvert_r$
$\mathrm{P}\Omega_{2n+1}(q)$ and $\mathrm{PSp}_{2n}(q)$	2	$t=1, \lvert q-1\rvert_2 > \lvert q+1\rvert_2$	$2^n\lvert q-1\rvert_2^n\lvert n!\rvert_2$
		$t=1, \lvert q-1\rvert_2 < \lvert q+1\rvert_2$	$2^n\lvert q+1\rvert_2^n\lvert n!\rvert_2$
	$\neq 2$	t odd	$\lvert q^t-1\rvert_r^{\left[\frac{n}{t}\right]}\lvert \left[\frac{n}{t}\right]!\rvert_r$
		$t=2t_0$, $t_0\geq 1$	$\lvert q^{t_0}+1\rvert_r^{\left[\frac{n}{t_0}\right]}\lvert \left[\frac{n}{t_0}\right]!\rvert_r$
$\mathrm{P}\Omega_{2n}^+(q)$	2	$t=1, \lvert q-1\rvert_2 > \lvert q+1\rvert_2$	$2^{n-1}\lvert q-1\rvert_2^n\lvert n!\rvert_2$
		$t=1, \lvert q-1\rvert_2 < \lvert q+1\rvert_2$	$2^{n-1}\lvert q+1\rvert_2^n\lvert n!\rvert_2$
	$\neq 2$	t odd	$\lvert q^t-1\rvert_r^{\left[\frac{n}{t}\right]}\lvert \left[\frac{n}{t}\right]!\rvert_r$
		$t=2t_0$, $t_0\geq 1, t\mid n$	$\lvert q^{t_0}+1\rvert_r^{\left[\frac{n}{t_0}\right]}\lvert \left[\frac{n}{t_0}\right]!\rvert_r$
		$t=2t_0$, $t_0\geq 1, t\nmid n$	$\lvert q^{t_0}+1\rvert_r^{\left[\frac{n-1}{t_0}\right]}\lvert \left[\frac{n-1}{t_0}\right]!\rvert_r$
$\mathrm{PSU}_n(q)$	2	$t=1, \lvert q-1\rvert_2 > \lvert q+1\rvert_2$	$2^{n-1}\lvert q-1\rvert_2^{\left[\frac{n}{2}\right]}\lvert \left[\frac{n}{2}\right]!\rvert_2$
		$t=1, \lvert q-1\rvert_2 < \lvert q+1\rvert_2$	$2^{\left[\frac{n}{2}\right]}\lvert q+1\rvert_2^{n-1}\lvert \left[\frac{n}{2}\right]!\rvert_2$
	$\neq 2$	t odd or $t=4t_0$	$\lvert q^t-1\rvert_r^{\left[\frac{n}{2t}\right]}\lvert \left[\frac{n}{2t}\right]!\rvert_r$
		$t=2$	$\lvert q+1\rvert_r^{n-1}\lvert n!\rvert_r$
		$t=2t_0$, $t_0\geq 3$ odd	$\lvert q^{t_0}+1\rvert_r^{\left[\frac{n}{t_0}\right]}\lvert \left[\frac{n}{t_0}\right]!\rvert_r$
$\mathrm{P}\Omega_{2n}^-(q)$	2	$t=1, \lvert q-1\rvert_2 > \lvert q+1\rvert_2$	$2^n\lvert q-1\rvert_2^{n-1}\lvert (n-1)!\rvert_2$
		$t=1, \lvert q-1\rvert_2 < \lvert q+1\rvert_2$, n even	$2^n\lvert q+1\rvert_2^{n-1}\lvert (n-2)!\rvert_2$
		$t=1, \lvert q-1\rvert_2 < \lvert q+1\rvert_2$, n odd	$2^{n-1}\lvert q+1\rvert_2^n\lvert (n-1)!\rvert_2$
	$\neq 2$	t odd	$\lvert q^t-1\rvert_r^{\left[\frac{n-1}{t}\right]}\lvert \left[\frac{n-1}{t}\right]!\rvert_r$
		$t=2t_0$, $t_0\geq 1, t\mid n$	$\lvert q^{t_0}+1\rvert_r^{\left[\frac{n-1}{t_0}\right]}\lvert \left[\frac{n-1}{t_0}\right]!\rvert_r$
		$t=2t_0$, $t_0\geq 1, t\nmid n$	$\lvert q^{t_0}+1\rvert_r^{\left[\frac{n}{t_0}\right]}\lvert \left[\frac{n}{t_0}\right]!\rvert_r$

Table 13.3: Some values of $|P_G(s)|_p$

G	$\lvert P_G(s)\rvert_p$	G	$\lvert P_G(s)\rvert_p$
$\mathrm{PSL}_3(3)$	3^3	$\mathrm{PSU}_3(5)$	5^3
$\mathrm{PSL}_3(4)$	2^3	$\mathrm{PSp}_4(3) \cong \mathrm{PSU}_4(2)$	3^4
$\mathrm{PSL}_4(2)$	2^6	$\mathrm{PSU}_4(3)$	3^6
$\mathrm{PSL}_4(3)$	3^6	$\mathrm{PSU}_5(2)$	2^{10}
$G_2(2)' \cong \mathrm{PSU}_3(3)$	2^2	$\mathrm{PSp}_6(2)$	2^9
$\mathrm{PSU}_3(4)$	2^6	$\mathrm{PSp}_4(q), q \in \{3,4,5\}$	q^4

Table 13.4: Lower bounds for $|P_G(s)|_p$

G	Conditions	lower bound for $\lvert P_G(s)\rvert_p$
$\mathrm{PSL}_n(q)$	$n \in \{3,5\}$	$\frac{q^{\frac{n(n-1)}{2}}}{\lvert n\rvert_p}$
	$n = 4$	$\frac{q^4}{\lvert 2\rvert_p}$
	$n \geq 6$	q^{2n-3}
$\mathrm{PSU}_n(q)$	$n \in \{3,5,7\}$	$\frac{q^{\frac{n(n-1)}{2}}}{\lvert n\rvert_p}$
	$n = 4$	$\frac{q^4}{\lvert 2\rvert_p}$
	$n = 6, q \neq 2$	$\frac{q^{12}}{\lvert 3\rvert_p}$
	$n \geq 8$	q^{3n-9}
$\mathrm{PSp}_{2n}(q)$	d smallest prime divisor of n	$\frac{q^{\frac{n^2(d-1)}{d}}}{\lvert d\rvert_p}$
$\mathrm{P}\Omega_{2n+1}(q)$	$(n,q) \neq (3,3)$	q^{3n-3}
$\mathrm{P}\Omega^+_{2n}(q)$,	$q \geq 4$	$\frac{q^{2n-2}}{\lvert 2\rvert_p}$
$\mathrm{P}\Omega^-_{2n}(q)$	$q \leq 3, n \geq 5, (q,n) \neq (2,5)$	$\frac{q^{4n-8}}{\lvert 2\rvert_p}$

Proposition 13.5. *Let $G = \mathrm{PSp}_4(q)$ and assume that $q \geq 7$. Moreover, let $r \neq p$ be a prime number.*

(1) Let $q = p$ be a Mersenne prime or a Fermat prime. Then $P_G^{(2)}(0) = -\frac{(q^2-1)(q^2+2)}{2}$ or $|P_G(s)|_p \geq q^3$. In the latter case, $|P_G(s)|_p > |G|_r$.

(2) Let $q+1$ be a Fermat prime. Then $P_G^{(q+1)}(0) = -(q^4+q^2-1)$ or $|P_G(s)|_2 \geq q^3/4$. In the latter case, $|P_G(s)|_2 > |G|_r$.

(3) Let q^2+1 be a Fermat prime. Then $P_G^{(q^2+1)}(0) = -(q^4-q^2-1)$ or $|P_G(s)|_2 \geq q^4/4$. In the latter case, $|P_G(s)|_2 > |G|_r$.

(4) Let $q-1$ be a Mersenne prime. Then $P_G^{(q-1)}(0)$ is even.

Proof. By [Mit14] and [KL82], the maximal subgroups of G are known. Let

$$\mathcal{A}_r(G) = \{H \leq G : |G:H|_r = 1, \mu_G(H) \neq 0\}$$

and

$$\mathcal{M}_r(G) = \{H \in \mathcal{A}_r(G) : H \text{ is maximal in } G\}.$$

(1) If $M \in \mathcal{M}_2(G)$, i.e. M is a maximal subgroup of G such that $|G:M|_2 = 1$, then M is conjugated to a maximal subgroup of type $\mathrm{SL}_2(q) \wr S_2$ in the class $\mathcal{C}_2$, so $M \cong \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q).2.2$.

We claim that if $H \in \mathcal{A}_2(G) - \mathcal{M}_2(G)$, then $|G:H|_p \geq q^3$. Assume that $H \in \mathcal{A}_2(G) - \mathcal{M}_2(G)$. Then H is a proper subgroup of M such that $|M:H|_2 = 1$. Let $K = \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q) \leq M$, $K = K_1 \times K_2$ with $K_1 \cong K_2 \cong \mathrm{PSL}_2(q)$ and $K_1, K_2 \leq K$. Clearly, $H \cap K$ is a proper subgroup of K. Without loss of generality, we may assume that $H \cap K_1 < K_1$. Since $|M:H|_2 = 1$, then $|K_1 : H \cap K_1|_2 = 1$, hence $H \cap K_1$ is a subgroup of odd index of $\mathrm{PSL}_2(q)$ (the subgroups of $\mathrm{PSL}_2(q)$ are well known, see [Hup67]). In particular, we have that $|K_1 : H \cap K_1|_p \geq q$, hence also $|M:H|_p \geq q$, thus $|G:H|_p \geq q^3$.

Assume that $|P_G(s)|_p < q^3$. Then also $|P_G^{(2)}(s)|_p < q^3$, hence if $a_k(G) \neq 0$ and $k > 1$ is odd, then $|k|_p < q^3$ and so k is the index of a maximal subgroup, as we have seen above. So we have that

$$P_G^{(2)}(s) = 1 - \left(\frac{q^2(q^2+1)}{2}\right)^{1-s}$$

and the proof is finished.

(2) If $M \in \mathcal{M}_{q+1}(G)$, i.e. M is a maximal subgroup of G such that $|G : M|_{q+1} = 1$, then M is conjugated to a maximal subgroup of type $\mathrm{SL}_2(q) \wr S_2$ in the class $\mathcal{C}_2$ or M is conjugated to a maximal subgroup of type $O_4^+(q)$ in the class $\mathcal{C}_8$. In both cases, $M \cong \mathrm{PSL}_2(q) \times \mathrm{PSL}_2(q).2.2$.

We claim that if $H \in \mathcal{A}_{q+1}(G) - \mathcal{M}_{q+1}(G)$, then $|G : H|_2 \geq q^3/2$. Let K, K_1 and K_2 be as in (1). Note that $H \cap K < K$. In fact, if H contains K, then H is normal in M. Since $\mu_G(H) \neq 0$, then H is intersection of maximal subgroups isomorphic to M. Now, H is normal in each of these subgroups, a contradiction (G is simple). So $H \cap K < K$. Without loss of generality, we may assume that $H \cap K_1 < K_1$. Since $|M : H|_{q+1} = 1$, then $|K_1 : H \cap K_1|_{q+1} = 1$. The subgroups of $\mathrm{PSL}_2(q)$ are well known, so we have that $|K_1 : H \cap K_1|_2 \geq q/2$, hence also $|M : H|_2 \geq q/2$, thus $|G : H|_2 \geq q^3/4$.

Assume that $|P_G(s)|_2 < q^3/4$. Arguing as in (1), we have that

$$P_G^{(q+1)}(s) = 1 - 2\left(\frac{q^2(q^2+1)}{2}\right)^{1-s}$$

and the proof is complete.

(3) If $M \in \mathcal{M}_{q^2+1}(G)$, i.e. M is a maximal subgroup of G such that $|G : M|_{q^2+1} = 1$, then M is conjugated to a maximal subgroup of type $\mathrm{SL}_2(q^2)$ in the class $\mathcal{C}_3$ or M is conjugated to a maximal subgroup of type $O_4^-(q)$ in the class $\mathcal{C}_8$. In both cases, $M \cong \mathrm{PSL}_2(q^2).2$.

We claim that if $H \in \mathcal{A}_{q^2+1}(G) - \mathcal{M}_{q^2+1}(G)$, then $|G : H|_p \geq q^3/2$. Assume that $H \in \mathcal{A}_{q^2+1}(G) - \mathcal{M}_{q^2+1}(G)$. Then H is a proper subgroup of M such that

$|M : H|_{q^2+1} = 1$. Note that $H \cap \mathrm{PSL}_2(q^2)$ is a proper subgroup of $\mathrm{PSL}_2(q^2)$. In fact, if H contains $\mathrm{PSL}_2(q^2)$, then H is normal in M. Since $\mu_G(H) \neq 0$, then H is intersection of maximal subgroups isomorphic to M. Now, H is normal in each of these subgroups, a contradiction (G is simple). So $H \cap \mathrm{PSL}_2(q^2) < \mathrm{PSL}_2(q^2)$. Since $|M : H|_{q^2+1} = 1$, then $|\mathrm{PSL}_2(q^2) : H \cap \mathrm{PSL}_2(q^2)|_{q^2+1} = 1$. The subgroups of $\mathrm{PSL}_2(q)$ are well known, so we have that $|\mathrm{PSL}_2(q^2) : H \cap \mathrm{PSL}_2(q^2)|_2 \geq q^2/2$, hence also $|M : H|_2 \geq q^2/2$, thus $|G : H|_2 \geq q^4/4$.

Assume that $|P_G(s)|_2 < q^4/4$. Arguing as in (1), we have that

$$P_G^{(q^2+1)}(s) = 1 - 2\left(\frac{q^2(q^2-1)}{2}\right)^{1-s}$$

and we are done.

(4) By [DL06], Theorem 3, we know that $|P_G^{(2)}(0)| = |G|_2$. Moreover, if $H \in \mathcal{A}_2(G)$, then H contains the Borel subgroup of G (since H is an intersection of parabolic maximal subgroups of G). Now, the index of the Borel subgroup of G is $(q^2+1)(q+1)^2$, hence it is not divisible by $q-1$. Thus $\mathcal{A}_2(G) \subseteq \mathcal{A}_{q-1}(G)$, hence

$$P_G^{(q-1)}(s) = P_G^{(2)}(s) + \sum_{k \in \mathbb{N}, k \text{ even}} \frac{a_k(G)}{k^s}.$$

By Lemma 2.3, we have that k divides $a_k(G)$, hence we conclude that $P_G^{(q-1)}(0)$ is even. □

Theorem 13.6. *Let G be a classical simple group and assume that G is not isomorphic to one of the following group:* $\mathrm{PSU}_3(3)$, $\mathrm{PSU}_6(2)$, $\mathrm{PSp}_4(8)$, $\mathrm{PSp}_4(9)$, $\mathrm{PSp}_8(3)$ *and* $\mathrm{P}\Omega_8^+(2)$. *Let* pr *be the set of prime numbers r such that $P_G^{(r)}(0)$ is a power of r. The characteristic of G is the prime $p \in \pi$ such that $|P_G(s)|_p \geq |P_G(s)|_r$ for all $r \in \pi$.*

Proof. By Theorem 12.3, we have that $p \in \pi$. If G is not isomorphic to one of the group listed in the statement of Proposition 13.4, the result is clear.

Assume that $G = \mathrm{PSL}_2(q)$. By [Pat09c, Proposition 8], we have that if $q \notin \{4, 5, 7, 8, 9\}$, then $P_G^{(r)}(0)$ is a power of r if and only if $r = p$, hence $\pi = \{p\}$.

Clearly, the claim of the present theorem holds also if $q \in \{4, 5, 7, 9\}$ (remind that $\mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5)$ and $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$, so these groups have 2 characteristics).

Assume that $G = \mathrm{PSp}_4(q)$. By Proposition 13.4 and Proposition 13.5, the result holds if $q \notin \{8, 9\}$. $\square$

Chapter 14

Recognition of the characteristic of an Exceptional group

In Table 14.1, we report the r-part of the order of the classical simple groups, when r is a prime divisor of $|G|$ and r is not p. To obtain Table 14.1 we used Lemma 2.9 (see it for the notation).

Proposition 14.1. *Let G be an exceptional group of Lie type of characteristic p. Then $|P_G(s)|_p > |G|_r \geq |P_G(s)|_r$ for all prime number $r \neq p$.*

Proof. Let G and M be as in Table 14.2, under the given conditions. By [Suz62] (for $G = {}^2B_2(q)$), [Kle88a] (for $G = {}^2G_2(q)$), [LS86, Table 1] (for $G = {}^3D_4(q)$, $E_6(q)$, ${}^2E_6(q)$, $E_7(q)$, $E_8(q)$ or $F_4(q)$), [Mal91] (for $G = {}^2F_4(q)$) and [CCN$^+$85] (for $G = G_2(3)$, ${}^3D_4(2)$ or ${}^2F_4(2)'$) we have that if a subgroup H of G is isomorphic to M, then H is a maximal subgroup of G. Hence $a_{|G:M|}(G) \neq 0$, and we obtain a lower bound for $|P_G(s)|_p$, as described in Table 14.2. A direct computation, using Table 14.1, proves the claim. □

Table 14.1: Exceptional groups of Lie type

G	r	t	$v_r(G\delta(G))$
$E_6(q)$	2	$1, h^+ > h^-$	$4h+9$
		$1, h^+ < h^-$	$6h+7$
	$\neq 2$	1	$6h+4v_r(3)+v_r(5)$
		2	$4h+2v_r(3)$
		3	$3h$
		$4,6$	$2h$
		$5,8,9,12$	h
$E_7(q)$	2	1	$7h+10$
	$\neq 2$	$1,2$	$7h+4v_r(3)+v_r(5)+v_r(7)$
		$3,6$	$3h$
		4	$2h$
		$5,7,8,9,10,12,14,18$	h
$E_8(q)$	2	1	$8h+14$
	$\neq 2$	$1,2$	$8h+5v_r(3)+2v_r(5)+v_r(7)$
		$3,4$	$4h+v_r(5)$
		6	$4h$
		$5,8,10,12$	$2h$
		$7,9,14,15,20,24,30$	h
$F_4(q)$	2	1	$4h+7$
	$\neq 2$	$1,2$	$4h+2v_r(3)$
		$3,4,6$	$2h$
		$8,12$	h
$G_2(q)$	2	1	$2h+2$
	$\neq 2$	$1,2$	$2h+v_r(3)$
		$3,6$	h
${}^2B_2(q)$	$\neq 2$	$1,4$	h
${}^3D_4(q)$	2	1	$2h+2$
	3	$1,2$	$2h+2$
	$\notin \{2,3\}$	$1,2,3,6$	$2h$
		12	h
${}^2E_6(q)$	2	$1, h^- > h^+$	$4h+9$
		$1, h^- < h^+$	$6h+7$
	$\neq 2$	1	$4h+2v_r(3)$
		2	$6h+4v_r(3)+v_r(5)$
		$3,4,6$	$2h$
		$8,10,12,18$	h
${}^2F_4(q)$	$\neq 2$	1	$2h$
		2	$2h+v_r(3)$
		$4,6,12$	h
${}^2G_2(q)$	2	1	$h+1$
	$\neq 2$	$1,2,6$	h

Table 14.2:

G	Conditions	M	Lower bound for $\lvert P_G(s)\rvert_p$
${}^2B_2(q)$		$C_{q+\sqrt{2q}+1} \rtimes C_4$	$q^2/2$
${}^3D_4(2)$		$(C_7 \times \mathrm{PSL}_2(7)).2$	2^8
${}^3D_4(q)$	$q \geq 3$	$G_2(q)$	q^6
$E_6(q)$		$F_4(q)$	q^{12}
${}^2E_6(q)$		$(\mathrm{P}\Omega^-_{10}(q) \circ \frac{q+1}{(q+1,3)}).(q+1,4)$	q^{16}
$E_7(q)$		$({}^2E_6(q) \circ \frac{q+1}{(q-1,2)}).(q+1,3).2$	q^{27}
$E_8(q)$		$(\mathrm{SL}_2(q) \circ E_7(q)).(q-1,2)$	q^{56}
$F_4(q)$		${}^3D_4(q).3$	$q^{12}/\lvert 3\rvert_p$
${}^2F_4(2)'$		$\mathrm{PSL}_3(3).2$	2^6
${}^2F_4(q)$	$q = 2^{2k+1}, k \geq 1$	$C_{q^2+q\sqrt{2q}+q+\sqrt{2q}+1} : 12$	$q^{12}/4$
$G_2(3)$		$\mathrm{PSL}_2(13)$	3^5
$G_2(q)$	$q \geq 4$	$\mathrm{SU}_3(q).2$	$q^3/\lvert 2\rvert_p$
${}^2G_2(q)$		$C_{q+\sqrt{3q}+1} \rtimes C_4$	$q^3/3$

Chapter 15

Proof of the main theorem

Theorem 15.1. *Let G be a simple group of Lie type and let H be a finite group. Assume that $P_H(s) = P_G(s)$. Then $H/\mathrm{Frat}(H) \cong G$.*

Proof. Without loss of generality, we assume that $\mathrm{Frat}(H) = 1$.

First, we claim that H is a simple group. There are two ways to see that H is a simple group. The first one is by [DL07b, Theorem 7]. The second one is the following: we know that if G is a simple group of Lie type, then the Dirichlet polynomial $P_G(s)$ is reducible if and only if $G \cong \mathrm{PSL}_2(p)$ with $p = 2^e - 1$ and $e \equiv 3 \pmod 4$ (see [Pat09a]). Clearly, if $P_G(s)$ irreducible, then G is simple (see, for example, [DLM04, Corollary 7]). Moreover, if $G \cong \mathrm{PSL}_2(p)$ for some $p = 2^e - 1$ and $e \equiv 3 \pmod 4$, then H is simple by [DLM04, Proposition 16]. Finally we have that H is not cyclic. In fact, if H is cyclic, then $P_H(1) \neq 0$ (since $P_H(1)$ is the probability that a randomly chosen element of H generates H). But $P_G(1) = 0$, since G is non-abelian.

Second, we claim that H is a group of Lie type. By [DL04, Theorem 3], if H is an alternating group, then $H \cong G$. By [DL06, Theorem 11], if H is a sporadic group, then $H \cong G$. By the classification of finite simple groups, we may assume that H is a group of Lie type.

Now, we want to prove that if $P_G(s) = P_H(s)$, then H and G have the same characteristic. Let us consider some particular cases. For a group A let $m(A)$ be the

minimal index of a proper subgroup of A. Clearly $a_{m(A)}(A) \neq 0$. Since $P_H(s) = P_G(s)$, we have that $m = m(G) = m(H)$. Assume that $m = 28$. By Table 15.1, we have that $\{H, G\} \subseteq \{\mathrm{PSp}_6(2), \mathrm{PSU}_3(3), \mathrm{PSL}_2(27)\}$. Clearly $H, G \ncong \mathrm{Alt}_{28}$, since H and G are groups of Lie type. Moreover, $|P^{(2)}_{\mathrm{PSp}_6(2)}(0)| = 2^9$ (by Theorem 12.3), $|P^{(2)}_{\mathrm{PSU}_3(3)}(0)| = 2^6$ and $|P^{(2)}_{\mathrm{PSL}_2(27)}(0)| = 1288$ (use [GAP]). Thus $G \cong H$. Assume that m is one of the minimal indexes in Table 15.1 and $m \neq 28$. Since G and H are groups of Lie type, we see that they have the same characteristic. Finally, assume that m is not one of the values of Table 15.1. Let π be the set of prime numbers r such that $P^{(r)}_G(0)$ is a power of r. By Theorem 12.3, if p is the characteristic of G, then $p \in \pi$. Moreover, by Theorem 13.6 and Proposition 14.1, we have that the characteristic of G is the prime p such that $p \in \pi$ and $|P_G(s)|_p \geq |P_G(s)|_r$ for all $r \in \pi$. Thus we conclude that H and G have the same characteristic.

In order to complete the proof, we apply Theorem 1.11: if G and H are simple groups of Lie type defined over fields with the same characteristics and $P_G(s) = P_H(s)$, then $G \cong H$. $\square$

Table 15.1: Simple groups with a certain minimal index (obtained with [GAP] and [DL03a, Table 1])

Minimal index	Groups
28	$\mathrm{PSp}_6(2)$, $\mathrm{PSU}_3(3), \mathrm{PSL}_2(27)$ and Alt_{28}
120	$\mathrm{PSp}_8(2)$, $\mathrm{P}\Omega^+_8(2)$, and Alt_{120}
672	$\mathrm{PSU}_6(2)$ and Alt_{672}
585	$\mathrm{PSp}_4(8), \mathrm{PSL}_4(8)$ and Alt_{585}
820	$\mathrm{PSp}_4(9), \mathrm{PSL}_4(9)$ and Alt_{820}
3280	$\mathrm{PSp}_8(3), \mathrm{PSL}_8(3)$ and Alt_{3280}

Bibliography

[Asc84] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math.*, 76:469–514, 1984.

[Bos96] N. Boston. A probabilistic generalization of the Riemann zeta function. *Analytic Number Theory*, 1:155–162, 1996.

[Bro00] K. S. Brown. The coset poset and the probabilistic zeta function of a finite group. *J. Algebra*, 225:989–1012, 2000.

[Car72] R. W. Carter. *Simple Groups Of Lie Type*. John Wiley & Sons, 1972.

[CCN+85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, 1985.

[Coo81] B. N. Cooperstein. Maximal subgroups of $G_2(2^n)$. *J. Algebra*, 70:23–36, 1981.

[DL03a] E. Damian and A. Lucchini. The Dirichlet polynomial of a finite group and the subgroups of prime power index. *Advances in Group Theory 2002, Aracne, Rome*, pages 209–221, 2003.

[DL03b] E. Detomi and A. Lucchini. Crowns and factorization of the probabilistic zeta function of a finite group. *J. Algebra*, 265:651–668, 2003.

[DL03c] E. Detomi and A. Lucchini. Recognizing soluble groups from their Probabilistic Zeta function. *Bull. London Math. Soc.*, 35:659–664, 2003.

[DL04] E. Damian and A. Lucchini. Recognizing the Alternating groups from their Probabilistic Zeta function. *Glasgow Math. J.*, 46:569–599, 2004.

[DL06] E. Damian and A. Lucchini. On the Dirichlet polynomial of finite groups of Lie type. *Rendiconti del Seminario Matematico della Università di Padova*, 115:51–69, 2006.

[DL07a] E. Damian and A. Lucchini. Finite groups with p-multiplicative probabilistic zeta function. *Comm. Algebra*, 35(11):3451–3472, 2007.

[DL07b] E. Damian and A. Lucchini. The Probabilistic Zeta function of finite simple group. *Journal of Algebra*, 313:957–971, 2007.

[DLM04] E. Damian, A. Lucchini, and F. Morini. Some properties of the Probabilistic Zeta function of finite simple groups. *Pacific J. Math.*, 215:3–14, 2004.

[Fei88] W. Feit. On large Zsigmondy primes. *Proc. Amer. Math. Soc.*, 102:29–36, 1988.

[GAP] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.12*.

[Gas59] W. Gaschütz. Die Eulersche Funktion endlicher auflösbarer Gruppen. *Illinois J. Math.*, 3:469–476, 1959.

[Gas62] W. Gaschütz. Praefrattinigruppen. *Arch. Math.*, 13:418–426, 1962.

[Giu07] M. Giudici. Maximal subgroups of almost simple groups with socle $\mathrm{PSL}(2, q)$. *ArXiv Mathematics e-prints*, 2007.

[GPPS99] R. Guralnick, T. Penttila, C. E. Praeger, and J. Saxl. Linear groups with orders having certain large prime divisor. *Proc. London Math. Soc.*, 78:167–214, 1999.

[Hal36] P. Hall. The Eulerian Functions of a group. *Quart. J. Math.*, 7:134–151, 1936.

[Har26] R. W. Hartley. Determination of the ternary linear collineation groups whose coefficients lie in the $GF(2^n)$. *Ann. Math.*, 27:140–158, 1926.

[HB82] B. Huppert and N. Blackburn. *Finite Groups II.* Springen-Verlag, Berlin, 1982.

[HIz89] T. Hawkes, M. Isaacs, and M. Özaydin. On the Möbius function of a finite group. *Rocky Mountain Journal*, 19:1003–1034, 1989.

[Hup67] B. Huppert. *Endliche Gruppen.* Springen-Verlag, Berlin, 1967.

[ILS03] A. A. Ivanov, M. W. Liebeck, and J. Saxl. *A survey of maximal subgroups of exceptional groups of Lie type. In: Groups, combinatorics and geometry: Durham, 2001.* World scientific, Providence, Rhode Island, USA, 2003.

[KL82] W. M. Kantor and R. A. Liebler. The rank 3 permutation representations of the finite classical groups. *Trans. Amer. Math. Soc.*, 271:1–71, 1982.

[KL90] P. Kleidman and M. Liebeck. *The Subgroup Structure of the Finite Classical Groups.* Cambridge University Press, Cambridge, 1990.

[Kle87] P. B. Kleidman. The maximal subgroups of the finite 8-dimensional orthogonal groups $\mathrm{P}\Omega_8^+(q)$ and of their automorphism groups. *J. Algebra*, 110:173–242, 1987.

[Kle88a] P. B. Kleidman. The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, the Ree groups ${}^2G_2(q)$, and their automorphism groups. *J. Algebra*, 117:30–71, 1988.

[Kle88b] P. B. Kleidman. The maximal subgroups of the Steinberg triality groups ${}^3D_4(q)$ and their automorphism groups. *J. Algebra*, 115:182–199, 1988.

[KLST90] Wolfgang Kimmerle, Richard Lyons, Robert Sandling, and David N. Teague. Composition Factors from the Group Ring and Artin's Theorem on Orders of Simple Groups. *Proc. London Math. Soc.*, s3-60(1):89–122, 1990.

[Laf78] J. Lafuente. Homomorphs and formation of given derived class. *Math. Proc. Camb. Phil. Soc.*, 84:437–441, 1978.

[Lan02] S. Lang. *Algebra*, volume 211. Graduate Texts in Mathematics, New York, 2002.

[LPS90] M. Liebeck, C. Praeger, and J. Saxl. *The maximal factorization of the finite simple groups and their automorphism groups.* AMS, Providence, Rhode Island, USA, 1990.

[LS86] M. W. Liebeck and J. Saxl. On the orders of maximal subgroup of finite exceptional groups of Lie type. *Proc. Lond. Math. Soc.*, 55:299–330, 1986.

[Mal91] G. Malle. The maximal subgroups of ${}^2F_4(q^2)$. *Journal of Algebra*, 139:52–69, 1991.

[Man96] A. Mann. Positively finitely generated groups. *Forum Math.*, 8:429–459, 1996.

[Mas07] M. Massa. *The probabilistic zeta function of the Alternating and Symmetric group.* PhD thesis, Università degli studi di Milano - Bicocca, 2007.

[Mit11] H. H. Mitchell. Determination of the ordinary and modular ternary groups. *Trans. Amer. Math. Soc.*, 12:207–242, 1911.

[Mit13] H. H. Mitchell. Determination of the finite quaternary linear groups. *Trans. Amer. Math. Soc.*, 14:123–142, 1913.

[Mit14] H. H. Mitchell. The subgroups of the quaternary abelian linear group. *Trans. Amer. Math. Soc.*, 15:379–396, 1914.

[Mun84] J. R. Munkres. *Elements of Algebraic Topology.* Addison-Wesley, Menlo Park, CA, 1984.

[Mwe76] B. Mwene. On the subgroups of the group $\mathrm{PSL}_4(2^m)$. *J. Algebra*, 41:79–107, 1976.

[Pat09a] M. Patassini. On the irreducibility of the Dirichlet polynomial of a simple group of Lie type. Accepted by Israel J. Math, 2009.

[Pat09b] M. Patassini. On the (non) contractibility of the order complex of the coset poset of a classical group. Submitted to J. Algebra, 2009.

[Pat09c] M. Patassini. The Probabilistic Zeta function of $\mathrm{PSL}_2(q)$, of the Suzuki groups ${}^2\mathrm{B}_2(q)$ and of the Ree groups ${}^2\mathrm{G}_2(q)$. *Pacific J. Math*, 240:185–200, 2009.

[Ser08] P. Jiménez Seral. Coefficient of the Probabilistic Zeta function of a monolithic group. *Glasgow J. Math*, 50:75–81, 2008.

[Spa66] E. H. Spainer. *Algebraic Topology.* McGraw-Hill, New York, 1966.

[Sta97] R. P. Stanley. *Enumerative Combinatorics, Vol. 1.* Cambridge University Press, Cambridge, 1997.

[Suz62] M. Suzuki. On a class of doubly transitive groups. *Annals of Mathematics*, 75:105–145, 1962.

[Zsi92] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3:256–284, 1892.