Università degli Studi di Padova

DIPARTIMENTO MATEMATICA

Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Master's degree Thesis in Mathematics

The Chebotarev invariant of a direct product of non-abelian finite simple groups

Candidate

Jessica Anzanello

Matricola 2087680

Supervisor

Prof. Andrea Lucchini

Academic Year 2023-2024

19th July 2024

Acknowledgements

I would first and foremost like to thank my supervisor, Andrea Lucchini: thank you for sparking my interest in group theory since my undergraduate studies, for the immense knowledge and inspiration that you have imparted to me, and for all the precious advice that you have given me. Your guidance and help have been invaluable, and I am deeply grateful for the opportunity to work on this problem.

I thank my parents for always encouraging me to do what I love.

Thank you, Asia and Sofia, for being people I can always rely on.

Thank you, Francesca, Giorgia, Linda, Lisa and Nicole, for your long-lasting friendship.

Thank you, Anna, for helping me navigate both trivial issues and heavy challenges, and for your unending support throughout the writing of this thesis.

Contents

List of Tables

Notation

A_n	Alternating group of degree n
S_n	Symmetric group of degree n
$\mathrm{Sym}(\Omega)$	Symmetric group on the set Ω
$\mathbb{E}[\tau]$	Expected value of a random variable τ
$\mathbb{F}_q$	Finite field of q elements
$\mathbb{P}$	Probability function
$\mathrm{AGL}_n(p)$	The affine general linear group of degree n over $\mathbb{F}_p$
$G \circ H$	Central product of G and H
$G.H$	(Not necessarily split) extension of G by H
$G : H$ or $G \rtimes H$	Split extension of G by H
G'	Derived subgroup of G
$G \wr H$	Wreath product $G^n \rtimes H$, where $H \leq S_n$ permutes the coordinates of G^n
$d(G)$	Minimal number of generators for G
$\log a$	Base two logarithm of a
n	A natural number
p	A prime number
q	A prime power

0.1 Introduction

In this thesis, we are interested in *generation* and *invariable generation* of finite groups. While the first has a long and rich history in finite group theory, the latter is still quite new and unexplored. Invariable generation was firstly introduced in the early nineties, with motivation from computational Galois theory, by Dixon (see [Dix92]). Following his work, we say that a subset $\{g_1, \dots, g_t\}$ of a finite group G *invariably generates* G if $\{{g_1}^{x_1}, \dots, {g_t}^{x_t}\}$ generates G for every t-tuple $(x_1, \dots, x_t) \in G^t$.

The motivating question of the present work is the following:

Question 1. Let G be a direct product of k non-abelian finite simple groups. If we choose random elements from G independently, with replacement, and with the uniform distribution, how many should we expect to pick until the elements chosen generate G? And how many to invariably generate G?

We can formalise the quantities needed to answer the question above in the following way. Let G be a non-trivial finite group and let $x = (x_n)_{n\in\mathbb{N}}$ be a sequence of independent, uniformly distributed, G-valued random variables. We may define two random variables (two waiting times) by:

(i) $\tau_G := \min\{n \geq 1 : \langle x_1, \dots, x_n \rangle = G\} \in [1, +\infty]$;

(ii) $\tau_{I,G} := \min\{n \geq 1 : \{x_1, \dots, x_n\}$ invariably generates $G\} \in [1, +\infty]$.

We denote the expectations of τ_G and $\tau_{\mathrm{I},G}$ respectively with $e_1(G)$ and $C(G)$. The latter is known as the *Chebotarev invariant* of G, and was firstly introduced by Kowalski and Zywina in 2012 [KZ12], taking its name from its relation with the *Chebotarev density theorem*.

In this thesis we answer Question 1 by deriving upper bounds for $e_1(G)$ and for $C(G)$, where G is a direct product of k non-abelian finite simple groups. In both cases, we give a polynomial bound for these expectations in terms of the logarithm of the number of direct factors and we show that such logarithmic bounds are best possible.

Layout of the thesis

Chapter 1. In the first chapter we deal with the case of (classical) generation. For $n \in \mathbb{N}$, denote by $m_n(G)$ the number of maximal subgroups of G with index n. We are interested in the following quantity, which is roughly equal to $e_1(G)$:

$$\mathcal{M}(G) = \sup_{n\geq 2} \frac{\log m_n(G)}{\log n}.$$

Indeed, in [LM20], Lucchini and Moscatiello have proved that

$$\lceil \mathcal{M}(G) \rceil - 4 \leq e_1(G) \leq \lceil \mathcal{M}(G) \rceil + 3.$$

Using Goursat's lemma, we provide a description of the maximal subgroups of a direct product of groups, and then we prove the following upper bound for $\mathcal{M}(G)$.

Theorem (Theorem 1.10)**.** *Let $G = T_1 \times \cdots \times T_k$ be a direct product of k non-abelian finite simple groups. Then*

$$\mathcal{M}(G) \leq \max_{1 \leq i \leq k} \frac{3 \log k}{\log l(T_i)} + 8,$$

where $l(T_i)$ denotes the minimum index of a proper subgroup of T_i.

Finally, we show that this logarithmic bound is best possible, modulo improving the constants, at least when the direct factors are all isomorphic.

Chapter 2. The aim of this chapter is to outline some information about finite almost simple groups and, in particular, about their maximal subgroups, which will be used in Chapter 3 to deal with the Chebotarev invariant of a direct product of non-abelian finite simple groups. The proof of the main result of Chapter 3 heavily relies on the Classification of Finite Simple Groups, therefore a wide range of tools is required. Among the others, we discuss the powerful subgroup structure theorems for the maximal subgroups of the alternating and symmetric groups (O'Nan Scott theorem) and of the almost simple classical groups (Aschbacher theorem [Asc84]). We also provide a brief description of Shintani descent, equipped with several detailed examples.

Chapter 3. The third chapter investigates the case of invariable generation. Our main result reads as follows.

Theorem (Theorem 3.6)**.** *Let $G = T_1 \times \cdots \times T_k$ be a direct product of k non-abelian finite simple groups. Then there exists an absolute constant γ such that*

$$C(G) \leq \gamma \log k.$$

The strategy of the proof is discussed in Subsection 3.1.2. We conclude the chapter by proving that the bound obtained for the Chebotarev invariant is best possible, at least when the direct factors are all isomorphic, and, finally, we observe that although both $C(G)$ and $e_1(G)$ are $O(\log k)$, the difference between the two invariants can be arbitrarily large.

1

An upper bound for $\mathcal{M}(G)$

Let G be a non-trivial finite group and let $x = (x_n)_{n\in\mathbb{N}}$ be a sequence of independent, uniformly distributed, G-valued random variables. As mentioned in the introduction, in this chapter we are interested in the following waiting time:

$$\tau_G \coloneqq \min\{n \geq 1 \mid \langle x_1, \ldots, x_n\rangle = G\},$$

and we denote by $e_1(G)$ the expectation $\mathbb{E}[\tau_G]$ of this random variable. In other words, $e_1(G)$ is the expected number of elements of G which have to be picked at random, with replacement, before a generating set for G is found.

Note that $\tau_G > n$ if and only if $\langle x_1, \ldots, x_n\rangle \neq G$, so we have

$$\mathbb{P}(\tau_G > n) = 1 - \mathbb{P}_G(n),$$

where $\mathbb{P}_G(n)$ denotes the probability that n randomly chosen elements of G generate G, i.e.

$$\mathbb{P}_G(n) = \frac{|\{(g_1, \ldots, g_n) \in G^n \mid \langle g_1, \ldots, g_n\rangle = G\}|}{|G|^n}.$$

One may ask why should we be interested in probabilistic generation, i.e. in the study of the probability that a random d-tuple of elements of a group generate the group, rather than just in minimal generation, i.e. in the minimal d such that there exists such a d-tuple. The following example, taken from [Tra20], answers to this moral question.

Example 1.1. Let $d(G)$ denote the minimal number of generators for a group G and let us consider the group $G \coloneqq A_5^{19}$. Then:

- $d(G) = 2$ (moreover, it is a well-known result that A_5^{19} is the largest 2-generated direct power of A_5);

- but $\mathbb{P}_G(2) \approx 0.00000000001046624$ (this can be obtained using [[KL90a], Proposition 9]);
- on the other hand, $e_1(G) \approx 4.2969719$.

There are different approaches to the study of probabilistic generation. For example, in [Pak99], Pak defined the following invariant:

$$\mathcal{V}(G) := \min\left\{k \in \mathbb{N} \mid \mathbb{P}_G(k) \geq \frac{1}{e}\right\},$$

and he observed that $e_1(G)$ is related to $\mathcal{V}(G)$ in the following way (see [[Pak99], Theorem 2.5]):

$$\frac{1}{e}e_1(G) \leq \mathcal{V}(G) \leq \frac{e}{e-1}e_1(G).$$

Significant estimations for $\mathcal{V}(G)$ have been obtained by Lubotzky in [Lub03].

In this chapter, we are interested in another related invariant: for $n \in \mathbb{N}$, denote by $m_n(G)$ the number of maximal subgroups of G with index n and let

$$\mathcal{M}(G) = \sup_{n\geq 2} \frac{\log m_n(G)}{\log n}.$$

$\mathcal{M}(G)$ can be seen as the polynomial degree of the rate of growth of $m_n(G)$ and it is roughly equal to $\mathcal{V}(G)$, indeed we have (see [[Lub03], Proposition 1.2]):

$$\mathcal{M}(G) - 3.5 \leq \mathcal{V}(G) \leq \mathcal{M}(G) + 2.02.$$

Moreover, as already pointed out in the introduction, this rate is roughly equal to $e_1(G)$, and precisely we have ([[LM20], Theorem 1.1]):

$$\lceil \mathcal{M}(G) \rceil - 4 \leq e_1(G) \leq \lceil \mathcal{M}(G) \rceil + 3.$$

This invariant has been studied for finite and profinite groups by various authors, see for example [LM20], and the references therein.

The aim of this chapter is to give an estimate of $\mathcal{M}(G)$ for

$$G \cong \prod_{1\leq i\leq r} T_i^{k_i}, \tag{1.1}$$

with T_i a non-abelian simple group and $T_i \not\cong T_j$ for all $i \neq j$.

1.1 The maximal subgroups of G

In order to estimate $\mathcal{M}(G)$, first of all we need a description of the maximal subgroups of G. The key observation is the following.

Proposition 1.1.

(i) If G_1 and G_2 are two groups without common composition factors, then the maximal subgroups of $G = G_1 \times G_2$ are all and only of the form $M_1 \times G_2$, with $M_1 \underset{max}{<} G_1$, and $G_1 \times M_2$, with $M_2 \underset{max}{<} G_2$.

(ii) If $G = S^t$ is a direct product of t isomorphic non-abelian simple groups, then the maximal subgroups M of G are of two types:

- *given $1 \le i \le t$ and $X \underset{max}{<} S$, $M = \{(s_1, \dots, s_t) \in S^t \mid s_i \in X\}$,*
- *given $1 \le i < j \le t$ and $\alpha \in \mathrm{Aut}(S)$, $M = \{(s_1, \dots, s_t) \in S^t \mid s_j = s_i^{\alpha}\}$.*

Proposition 1.1 is a consequence of a result of É. Goursat that dates back to 1889, known as Goursat's lemma [Gou89], that gives a description of the subgroups of a direct product $G \times H$, which involves isomorphisms between factor groups of subgroups of G and H.

We follow [Thé97] for the proof of Goursat's lemma and the subsequent Lemma 1.3 and Proposition 1.4, which correspond respectively to [[Thé97], Lemmas 1.1, 1.2 and 1.3].

Theorem 1.2 (Goursat's lemma)**.** *Let G and H be two groups. Then, the subgroups of $G \times H$ are in bijection with the set of 5-tuples $(\tilde{S}_1, S_1, \tilde{S}_2, S_2, \phi)$, where $S_1 \trianglelefteq \tilde{S}_1 \le G$, $S_2 \trianglelefteq \tilde{S}_2 \le H$ and $\phi : \tilde{S}_1/S_1 \longrightarrow \tilde{S}_2/S_2$ is an isomorphism. Specifically:*

(i) if S is a subgroup of $G \times H$, then $S = \{(s_1, s_2) \in \tilde{S}_1 \times \tilde{S}_2 \mid (S_1 s_1)^{\phi} = S_2 s_2\}$, where $\tilde{S}_1$ and $\tilde{S}_2$ are the projections of S onto the two factors G and H, S_1 and S_2 are the intersections of S with $G \times 1$ and $1 \times H$, and the map $\phi : S_1 g \mapsto S_2 h$, with $(g, h) \in S$ is a well-defined isomorphism.

(ii) Conversely, if $\phi : \tilde{S}_1/S_1 \longrightarrow \tilde{S}_2/S_2$ is an isomorphism between sections of G and H respectively, then $S = \{(s_1, s_2) \in \tilde{S}_1 \times \tilde{S}_2 \mid (S_1 s_1)^{\phi} = S_2 s_2\}$ is a subgroup of $G \times H$.

And the two constructions are inverse to each other.

Proof. If S is a subgroup of $G \times H$, we define $S_1 := S \cap (G \times 1)$, $S_2 := S \cap (1 \times H)$, $\tilde{S}_1 := \pi_1(S)$, $\tilde{S}_2 := \pi_2(S)$, where $\pi_1 : G \times H \longrightarrow G$ and $\pi_2 : G \times H \longrightarrow H$ are the canonical projections onto the two factors. We identify S_1 with a subgroup of G and so $S_1 \trianglelefteq \tilde{S}_1$. Indeed, if $s_1 \in S_1$ and $g \in \tilde{S}_1$, $(s_1, 1) \in S$ and $\exists h \in \tilde{S}_2$ such that $(g, h) \in S$. So, $(g, h)^{-1}(s_1, 1)(g, h) = (g^{-1} s_1 g, 1) \in S$ and therefore $g^{-1} s_1 g \in S_1$. Similarly, we identify S_2 with a subgroup of H and we have $S_2 \trianglelefteq \tilde{S}_2$.

Note that $S_1 \times S_2 \le S \le \tilde{S}_1 \times \tilde{S}_2$.

Now, for any $g \in \tilde{S}_1$, $\exists h \in \tilde{S}_2$ such that $(g,h) \in S$, and the class $S_2h \in \tilde{S}_2/S_2$ is uniquely determined by g, because if $(g,h),(g,h') \in S$, then $(g,h)^{-1}(g,h') = (1, h^{-1}h') \in S_2$, and thus $S_2h = S_2h'$. Moreover, if $g \in S_1$, then $(g,1) \in S$, and so $S_2h = S_2$. Therefore, the class S_2h only depends on the class $S_1g \in \tilde{S}_1/S_1$. This well defines a group homomorphism $\phi : \tilde{S}_1/S_1 \to \tilde{S}_2/S_2$ mapping S_1g to S_2h. Exchanging the role of the two factors of the product, we obtain similarly a group homomorphism ψ in the other direction and it follows easily that the two are inverse to each other.

Conversely, any isomorphism of sections $\phi : \tilde{S}_1/S_1 \to \tilde{S}_2/S_2$ determines uniquely a subgroup S of $G \times H$ by the above procedure and the two constructions are inverse to each other. □

Remark 1.1. If S is a subgroup of $G \times H$, and if S_1, S_2, $\tilde{S}_1$, $\tilde{S}_2$ and ϕ are as in point (i) of the previous theorem, then S coincides with the inverse image $\pi^{-1}(\Delta_\phi)$, where Δ_ϕ is the graph of the isomorphism ϕ, and $\pi : \tilde{S}_1 \times \tilde{S}_2 \to \tilde{S}_1/S_1 \times \tilde{S}_2/S_2$ is the quotient map.

To describe the maximal subgroups of $G \times H$, we shall need the following fact.

Lemma 1.3. *Let $\phi : G \to H$ be an isomorphism and Δ_ϕ be the graph of ϕ. Then the lattice of subgroups of $G \times H$ containing $\Delta\phi$ is isomorphic to the lattice of normal subgroups of G. In particular Δ_ϕ is maximal if and only if G is simple (and hence H too).*

Proof. If $\Delta_\phi \leqslant S \leqslant G \times H$, we define $N := S \cap (G \times 1)$, and we identify it with a subgroup of G. Then, $N \trianglelefteq G$, because if $n \in N$ and $g \in G$, then $(g^{-1}ng, 1) = (g, g^\phi)^{-1}(n,1)(g, g^\phi)$. This defines the required map $S \mapsto N$. If, conversely, $N \trianglelefteq G$, we set $S := N\Delta_\phi$ and it is easy to check that this defines the inverse map. □

We are ready for the description of the maximal subgroups of $G \times H$.

Proposition 1.4. *Let S be a maximal subgroup of $G \times H$. Then:*

(i) either S is a standard subgroup of $G \times H$, i.e. $S = S_1 \times H$ with $S_1 \underset{max}{<} G$ or $S = G \times S_2$ with $S_2 \underset{max}{<} H$,

(ii) or S corresponds, by the construction in Theorem 1.2, to an isomorphism $\phi : G/S_1 \to H/S_2$ of simple groups.

Proof. Let $S \underset{max}{<} G \times H$, corresponding to $\phi : \tilde{S}_1/S_1 \to \tilde{S}_2/S_2$, via the construction of Goursat's lemma. If $S_1 \neq G$, then $S \leq \tilde{S}_1 \times H < G \times H$, so $S = \tilde{S}_1 \times H$, and consequently S is standard, $S_1 = \tilde{S}_1$ and $S_1 \underset{max}{<} G$. Similarly, S is standard if $S_2 \neq H$.

Now, assume that $\tilde{S}_1 = G$ and $\tilde{S}_2 = H$. We claim that $G/S_1 (\cong H/S_2)$ is a simple group. Indeed, $S/(S_1 \times S_2)$ is equal to the graph of the isomorphism $\phi : G/S_1 \to G/S_2$ and therefore we can conclude by the previous Lemma 1.3. Namely, $S \underset{max}{<} G \times H$ implies that $\Delta_\phi = S/(S_1 \times S_2) \underset{max}{<} (G \times H)/(S_1 \times S_2)$ and thus, by Lemma 1.3, G/S_1 is simple. □

Now, we can prove proposition 1.1.

Proof. (i) If G_1 and G_2 don't have common composition factors, condition (ii) of Proposition 1.4 cannot occur. Therefore all the maximal subgroups of $G_1 \times G_2$ are standard.

(ii) For the second case, where $G \cong S^t$, with S a non-abelian simple group, we can assume $t = 2$. If $M \underset{max}{<} S \times S$, by Proposition 1.4, either $M = M_1 \times S$, with $M_1 \underset{max}{<} S$, or $M = S \times M_2$, with $M_2 \underset{max}{<} S$, or M corresponds to an isomorphism of simple groups $\phi : S \longrightarrow S$ and so, by Goursat's lemma, $M = \{(s_1, s_2) \in \tilde{S}_1 \times \tilde{S}_2 = S \times S \mid s_1^{\phi} = s_2\}$. The same reasoning works for $t \geq 3$ and so we have obtained description (ii). □

Observation 1.1. Thanks to Proposition 1.1, we have a complete description of the maximal subgroups of $G \cong \prod_{1 \leq i \leq r} T_i^{k_i}$, with T_i a non-abelian finite simple group and $T_i \not\cong T_j$ for all $i \neq j$. Let us ponder for a moment on this description.

Since $T_i^{k_i}$ and $T_j^{k_j}$ don't have common composition factors, the maximal subgroups M of G are all of the form:

$$M = T_1^{k_1} \times \cdots \times T_{i-1}^{k_i-1} \times M_i \times T_{i+1}^{k_i+1} \times \cdots \times T_r^{k_r},$$

for $i \in \{1 \ldots r\}$ and $M_i \underset{max}{<} T_i^{k_i}$.
Therefore we have two possibilities.

(i) $M_i = T_i \times \cdots \times \widetilde{M_i} \times \cdots \times T_i$, with $\widetilde{M_i} \underset{max}{<} T_i$. In this case, $|M_i| = |T_i|^{k_i - 1} |\widetilde{M_i}|$ and thus $[G : M] = [T_i^{k_i} : M_i] = [T_i : \widetilde{M_i}]$.

(ii) $M_i = \{(t_1, \cdots, t_j, \cdots, t_k, \cdots, t_{k_i}) \in T_i^{k_i} : t_k = t_j^{\phi}\}$, given $j < k$ and $\phi \in \mathrm{Aut}(T_i)$. In this case, $|M_i| = |T_i|^{k_i - 1}$ and thus $[G : M] = [T_i^{k_i} : M_i] = \frac{|T_i|^{k_i}}{|T_i|^{k_i - 1}} = |T_i|$.

1.2 Proof of the main result

Let us consider Out(G), the outer automorphism group of G. Recall that this is defined as the quotient Out(G)=Aut(G)/Inn(G), where Inn(G) is the subgroup of inner automorphisms, i.e. Inn(G)= $\{\sigma_g \mid g \in G\}$, with $\sigma_g(x) = x^g$. In the proof of the main result of this chapter we will need the following.

Lemma 1.5. *If S is a non-abelian finite simple group, then* $|\mathrm{Out}(S)| \leq \log |S|$.

Proof. This follows from the Classification of Finite Simple Groups. See, for example, [Koh03] for a proof. □

Remark 1.2. Here and throughout this thesis, the symbol log denotes the logarithm to the base 2.

Lemma 1.6. *If S is a non-abelian finite simple group, then* $|\mathrm{Aut}(S)| \leq |S| \log |S|$.

Proof. Let us consider Out(S)=Aut$(S)/$Inn(S). Since S is non-abelian simple, $|\mathrm{Inn}(S)|=|S|$ and, by Lemma 1.5, $|\mathrm{Out}(S)| \leq \log |S|$. Therefore, $|\mathrm{Aut}(S)| = |\mathrm{Inn}(S)||\mathrm{Out}(S)| \leq |S| \log |S|$. □

Finally, we will use these crucial results.

Theorem 1.7 ([Luc15])**.** *Let S be a finite non-abelian simple group. Then,*

$$e_1(S) \leq e_1(A_6) \approx 2.494$$

For convenience, we now restate the following result.

Theorem 1.8 ([LM20])**.** *Let G be a finite group. Then*

$$\lceil \mathcal{M}(G) \rceil - 4 \leq e_1(G) \leq \lceil \mathcal{M}(G) \rceil + 3.$$

Combining Theorems 1.7 and 1.8 we obtain

Corollary 1.9. *Let S be a finite non-abelian simple group. Then,*

$$\lceil \mathcal{M}(S) \rceil \leq 6.$$

We are ready for the main result of this chapter.

Theorem 1.10. *If G is a product of non-abelian finite simple groups as in (1.1) and $k := \sum_{i=1}^{r} k_i$, then*

$$\mathcal{M}(G) \leq \max_{1 \leq i \leq r} \frac{3 \log k}{\log l(T_i)} + 8, \tag{1.2}$$

where $l(T_i)$ denotes the minimum index of a proper subgroup of T_i.

Proof. Using the above description of Observation 1.1 for the maximal subgroups of G, we have

$$\begin{aligned} m_n(G) &= \sum_{i=1}^{r} k_i m_n(T_i) + \sum_{i,|T_i|=n} \binom{k_i}{2} |\mathrm{Aut}(T_i)| \\ &\leq k \max_{1 \leq i \leq r} m_n(T_i) + \binom{k}{2} n \log n, \end{aligned}$$

where we used Lemma 1.6 to say that $|\mathrm{Aut}(T_i)| \leq |T_i| \log |T_i| = n \log n$. Therefore

$$\frac{\log m_n(G)}{\log n} \leq \frac{\log \left(k \max_{1 \leq i \leq r} m_n(T_i) + \binom{k}{2} n \log n \right)}{\log n}.$$

We now estimate $\log\left(k \max_i m_n(T_i) + \binom{k}{2} n \log n\right)$. Note that it makes sense to assume $k \geq 2$ and therefore

$$\begin{aligned}
&\log\left(k \max_i m_n(T_i) + \binom{k}{2} n \log n\right) \\
&\leq \log(k \max_i m_n(T_i))\mathbb{1}_{\{\max_i m_n(T_i) \geq 1\}} + \log\left(\binom{k}{2} n \log n\right) \\
&\leq \max_i \log m_n(T_i)\mathbb{1}_{\{\max_i m_n(T_i) \geq 1\}} + 3\log k + 2\log n,
\end{aligned}$$

where we used: $\log\left(\binom{k}{2} n \log n\right) = \log\left(\frac{k^2-k}{2} n \log n\right) \leq 2\log k - 1 + 2\log n$. We obtain:

$$\begin{aligned}
\sup_{n\geq 2} \frac{\log m_n(G)}{\log n} &\leq \sup_{n\geq 2} \frac{3\log k}{\log n} + \max_i \sup_{n\geq 2} \frac{\log(m_n(T_i))}{\log n} + 2 \\
&= \sup_{n\geq 2} \frac{3\log k}{\log n} + \max_i \mathcal{M}(T_i) + 2.
\end{aligned}$$

Using Corollary 1.9, we have $\mathcal{M}(T_i) \leq 6$, thus

$$\mathcal{M}(G) \leq \sup_{n\geq 2} \frac{3\log k}{\log n} + 8. \tag{1.3}$$

To conclude, we can obtain a better estimate of the constant that multiplies $3\log k$. Note that $m_n(G) \neq 0$ if and only if there exist $i \in \{1, \ldots, r\}$ and $M_i \underset{max}{<} T_i$ such that $|T_i : M_i| = n$, or $|T_i| = n$, so we can replace $\sup_{n\geq 2} \frac{1}{\log n}$ with $\max_i \frac{1}{\log(l(T_i))}$, where $l(T_i)$ is the minimum index of a proper subgroup of T_i. □

Remark 1.3. The estimate of Theorem 1.10 is accurate and such logarithmic bound is best possible, at least when the direct factors are all isomorphic. Indeed, consider $G = A_5^k$. A_5 has:

- 5 maximal subgroups of index 5 (A_4);
- 6 maximal subgroups of index 6 (D_{10});
- 10 maximal subgroups of index 10 (twisted S_3 in A_5).

So, the non-zero values of $m_n(A_5^k)$ are:

- $m_5(A_5^k) = 5k$,
- $m_6(A_5^k) = 6k$,
- $m_{10}(A_5^k) = 10k$,
- $m_{60}(A_5^k) = \binom{k}{2}|\operatorname{Aut}(A_5)| = \binom{k}{2}5!$.

And thus we obtain:

$$\mathcal{M}(A_5^k) = \sup_{n\geq 2} \frac{\log m_n(A_5^k)}{\log n} = \max\left\{\frac{\log 5k}{\log 5}, \frac{\log\left(\binom{k}{2}5!\right)}{\log 60}\right\} = \frac{\log k}{\log 5} + 1.$$

2

The maximal subgroups of the finite almost simple groups

This chapter aims to briefly discuss some information about finite almost simple groups and, in particular, about their maximal subgroups, that we shall need in Chapter 3 to deal with the Chebotarev invariant of a direct product of non-abelian finite simple groups. The proof of our main result heavily relies on the Classification of the Finite Simple Groups (CFSG). Therefore, we start by recalling its statement.

Theorem 2.1 (CFSG, Gorenstein)**.** *Each finite non-abelian simple group is isomorphic to one of the following groups:*

(i) *an alternating group A_n, for $n \geq 5$,*

(ii) *a classical group,*

(iii) *an exceptional group of Lie type,*

(iv) *one of the 26 sporadic groups.*

Definition 2.1. A group G is called *almost simple* if there exists a simple group S such that $S \trianglelefteq G \leq \mathrm{Aut}(S)$.

Note that, in this case, $\mathrm{soc}(G) = S$.

Definition 2.2. A group G is called *quasisimple* if G is perfect, that is $G = G'$, and $G/Z(G)$ is simple.

The next easy lemma highlights the fact that, for a quasisimple group G, there is a natural $1 - 1$ correspondence between the maximal subgroups of G and the maximal subgroups of the simple quotient $G/Z(G)$.

Lemma 2.2. *Let G be perfect and let M be a maximal subgroup of G. Then:*

(i) M contains $Z(G)$;

(ii) $M/Z(G)$ is maximal in $G/Z(G)$;

(iii) the preimage in G of every maximal subgroup of $G/Z(G)$ is maximal in G.

Proof. (i) Assume that $Z := Z(G) \not\leq M$. Then, $M < ZM$ gives $ZM = G$, by maximality of M. Hence, $M \trianglelefteq G$ and $G/M \cong Z/(M \cap Z)$ is abelian. This implies that $G' \leq M$, contradicting the assumption $G' = G$.

(ii) and (iii) are straightforward. □

2.1 The symmetric and alternating groups

It was known to Galois that A_n is simple for $n \geq 5$. If $n \geq 7$, then the almost simple groups with alternating socle are only A_n and S_n, and this is a consequence of the fact that, for those n, $\mathrm{Aut}(A_n) \cong S_n$ (see [Wil09], Subsection 2.4.2 for a proof).

The maximal subgroups of A_n and S_n fall into three classes: the intransitive, the imprimitive and the primitive. The first two families of maximal subgroups are quite easy to classify, and the latter family is described by O'Nan Scott theorem, which we shall state later.

First of all, we recall the notions of transitivity and primitivity.

Definition 2.3 (Transitivity)**.** Let $G \leq \mathrm{Sym}(\Omega)$. We define an equivalence relation $\sim$ on Ω by the rule that $\alpha \sim \beta$ if and only if there is an element $g \in G$ with $\alpha^g = \beta$. The equivalence classes of $\sim$ are the *orbits* of G, and we say that G is *transitive* if there is just one orbit, and *intransitive* otherwise.

Definition 2.4 (k-transitivity)**.** Let $G \leq \mathrm{Sym}(\Omega)$ and let k be a positive integer less than $|\Omega|$. We say that G is *k-transitive* on Ω if it acts transitively on the set of all k-tuples of distinct elements of Ω, where the action is componentwise: $(\alpha_1, \dots, \alpha_k)^g = (\alpha_1^g, \dots, \alpha_k^g)$.

Note that if G is k-transitive on Ω, then $n(n-1)\cdots(n-k+1)$ divides $|G|$.

A non-empty subset Δ of Ω is a *block* for a permutation group $G \leq \mathrm{Sym}(\Omega)$ if for all $g \in G$ either $\Delta^g = \Delta$, or $\Delta^g \cap \Delta = \varnothing$. That is, each element of G either permutes the elements of Δ among themselves, or maps all of them outside Δ. If Δ is a block for G, it is easy to show that Δ^g is also a block, for all $g \in G$. The set of translates $\{\Delta^g \mid g \in G\}$ is called a *block system* for G. Observe that Ω is a block, and $\{\omega\}$ is a block for every $\omega \in \Omega$. The blocks Ω, $\{\omega\}$ are called *trivial blocks*.

Definition 2.5 (Primitivity)**.** If G is a transitive subgroup of $\mathrm{Sym}(\Omega)$ and there exists a non-trivial block for G, then G is *imprimitive*; all other transitive groups are *primitive*.

Let us assume that G is transitive. A partition of Ω is a family $\mathcal{P} = \{\Delta_1, \dots, \Delta_k\}$ of non-empty subsets of Ω such that $\Omega = \Delta_1 \cup \cdots \cup \Delta_k$ and $\Delta_i \cap \Delta_j = \varnothing$, whenever

$i \neq j$. We say that a group G *stabilises* the partition $\mathcal{P}$ if $\Delta_i^g \in \mathcal{P}$ for all $g \in G$ and for all $i \in \{1, \ldots, k\}$. If G stabilises a partition $\mathcal{P}$, since G is assumed to be transitive on Ω, it is clear that G acts on $\mathcal{P}$ by $(\Delta_i, g) \mapsto \Delta_i^g$, and that this action is transitive: if $\Delta_i, \Delta_j \in \mathcal{P}$, $\alpha \in \Delta_i$ and $\beta \in \Delta_j$, then there exists $g \in G$ such that $\alpha^g = \beta$, so $\Delta_i^g \cap \Delta_j \neq \varnothing$ and this implies that $\Delta_i^g = \Delta_j$. We deduce that all of the members of $\mathcal{P}$ have the same size, and that if Δ is one of them, then either $\Delta^g = \Delta$, or $\Delta^g \cap \Delta = \varnothing$. Therefore, the partitions stabilised by G correspond exactly to the block systems for G.

Note that, if Δ is a block for G, then $d := |\Delta|$ is a divisor of $n = |\Omega|$. In particular, if the block Δ is non trivial, then n cannot be a prime number.

Definition 2.6 (Wreath product)**.** If H and K are two groups and $K \leq S_n$, then $H \wr K$ denotes the *wreath product* between H and K, i.e., the semidirect product $H \rtimes K$, where K acts on H^n by permuting the coordinates, namely, $\pi \in K$ acts on H^n by

$$(x_1, \ldots, x_n)^\pi = \pi^{-1}(x_1, \ldots, x_n)\pi = (x_{1\pi^{-1}}, \ldots, x_{n\pi^{-1}}).$$

We are ready to describe the intransitive and imprimitive maximal subgroups of A_n and S_n.

2.1.1 Intransitive and imprimitive maximal subgroups

In order to prove the next proposition, we shall need the following results: the first is due to Jordan and the second to Frobenius. Proofs can be found for example in [[Gar21], Theorems 6.6 and 8.1].

Theorem 2.3 (Jordan)**.** *Assume that G is primitive on Ω and let G_Δ be the pointwise stabiliser of $\Delta \subseteq \Omega$ in G. If G_Δ is primitive on $\Gamma := \Omega \setminus \Delta$ and $1 < |\Gamma| = m < n = |\Omega|$, then G is $(n - m + 1)$-transitive.*

Theorem 2.4 (Embedding argument)**.** *Let H be a subgroup of a finite group G, let $x_1, \ldots, x_n$ be a right transversal for H in G and let φ be any homomorphism with domain H, say $\varphi : H \to X$. Then the map*

$$f : G \to \varphi(H) \wr S_n, \quad x \mapsto (\varphi(x_1 x x_{1\pi}^{-1}), \ldots, x_n x x_{n\pi}^{-1}))\pi,$$

where $\pi \in S_n$ is the unique permutation that satisfies $x_i x \in H_{x_{i\pi}}$ for all $i = 1, \ldots, n$, is a well-defined homomorphism with $\ker f = (\ker \varphi)_G$*, the normal core of* $\ker \varphi$ *in G.*

Proposition 2.5. *If X is A_n or S_n and M is any maximal subgroup of X, with $M \neq A_n$, then the following holds:*

(i) if M is intransitive, then $M = (S_k \times S_l) \cap X$, with $n = k + l$ and $k \neq l$;

(ii) if M is imprimitive, then $M = (S_k \wr S_l) \cap X$, with $n = kl$, $k > 1$ and $l > 1$.

Proof. We prove the proposition for $X = S_n$, the case $X = A_n$ being similar, and we follow the proofs of Garonzi contained in [[Gar21], Chapters 7 and 8].

Intransitive case. Let $\Omega = \{1, \dots, n\}$ and let $G \leq \mathrm{Sym}(\Omega) = S_n$ be an intransitive permutation group. Then, G has more than one orbit on Ω, and letting O be one of them, G is contained in $\mathrm{Stab}(O) = \{g \in S_n \mid O^g = O\}$. Note also that we have a natural isomorphism:

$$\mathrm{Stab}(O) \cong \mathrm{Sym}(O) \times \mathrm{Sym}(\Omega \setminus O),\ g \mapsto (g_{|_O}, g_{|_{\Omega\setminus O}}).$$

Thus, the maximal intransitive subgroups of S_n, i.e. maximal among the intransitive subgroups, are of the form $G = \mathrm{Stab}(O)$, where O is a non-empty proper subset of Ω. We have therefore obtained that these subgroups are of type $S_k \times S_l$, where $0 < k = |O| < n$ and $l = n - k = |\Omega \setminus O|$. Now, we want to prove that such subgroups are indeed maximal in S_n, unless $k = l$. Assume that $G = \mathrm{Stab}(O)$ is not a maximal subgroup of S_n, then, it is properly contained in some maximal subgroup $M \leq S_n$, which is therefore transitive on Ω. Let us first assume that M is primitive. Note that, since we can assume that $n \geq 3$, either O or $\Omega \setminus O$ has at least two elements, and therefore G (and thus M) contains a 2-cycle, interchanging those two elements. Now, Jordan theorem 2.3 implies that $M = S_n$, a contradiction. Indeed, let $\sigma = (ab)$ be the transposition contained in M, let $\Gamma = \{a, b\}$ and let $\Delta = \Omega \setminus \Gamma$. Note that M_Δ acts primitively on Γ, since $\sigma \in M_\Delta$ and $|\Gamma| = 2$ is prime. Therefore, using Jordan theorem, M is $(n-1)$-transitive and thus $n!$ divides $|M|$, implying that $M = S_n$.

So, we can assume that M is imprimitive, and let Δ be a non-trivial block for M. Then Δ is also a non trivial block for G, therefore $\Delta \cap O$ is either empty or a block for $G^O := \{g_{|_O} \mid g \in G\}$ and $\Delta \cap \bar{O}$ is either empty or a block for $G^{\bar{O}}$. Since $G^O \cong \mathrm{Sym}(O)$ is primitive on O and $G^{\bar{O}} \cong \mathrm{Sym}(\bar{O})$ is primitive on $\bar{O}$, we deduce that either $|\Delta \cap O| \leq 1$ or $\Delta \cap O = O$, and either $|\Delta \cap \bar{O}| \leq 1$ or $\Delta \cap \bar{O} = \bar{O}$. We investigate such cases.

- If $\Delta \cap O = \{\alpha\}$ and $\Delta \cap \bar{O} = \{\beta\}$, then $\Delta = \{\alpha, \beta\}$. If there exists $\gamma \in O \setminus \Delta$, then, since $G = \mathrm{Stab}(O)$, $g = (\alpha\gamma) \in G$ and $\Delta^g = \{\beta, \gamma\}$. This contradicts the fact that Δ is a block. Therefore $O \setminus \Delta = \varnothing$ and similarly $\bar{O} \setminus \Delta = \varnothing$, so $\Omega = \Delta$, contradicting the fact that Δ is a non-trivial block.

- If $\Delta \cap O = \{\alpha\}$ and $\Delta \supseteq \bar{O}$, then, $\Delta = \{\alpha\} \cup \bar{O}$. Since Δ is a non-trivial block, there exists $\beta \in \Omega \setminus \Delta$, hence there exists $g \in G$ such that $\alpha^g = \beta$, so $\Delta^g = \{\beta\} \cup \bar{O}$ is not disjoint from Δ and not equal to Δ, a contradicition.

- We are left with the case in which one of $\Delta \cap O$ and $\Delta \cap \bar{O}$ is empty, say $\Delta \cap O = \varnothing$, therefore $\Delta = \bar{O}$. Since M is transitive, there exists $m \in M$ that takes an element of $\bar{O}$ to an element of O, hence $\Delta^m \subseteq O$. But then $\Delta^m = \Delta^m \cap O$ is a block for $G^O = \mathrm{Sym}\, O$, of size at least 2, hence $\Delta^m = O$, and in particular $|\bar{O}| = |O|$.

This shows that if O is a proper subset of Ω and $G = \mathrm{Stab}(O)$ is not a maximal subgroup of S_n, then $n > 2$ and $|\bar{O}| = |O|$. So, G has type $S_k \times S_k$, with $2k = n$. Indeed, such a subgroup is not maximal if $n > 2$: it is contained in an imprimitive wreath product

$S_k \wr S_2$, the stabilizer of a partition with two parts of size k, which, as we are now going to see, is a maximal subgroup of S_n.

Imprimitive case Let $k, l > 1$ such that $kl = n$. Then, the wreath product $S_k \wr S_l$ embeds into S_n as an imprimitive group. To see this, it is enough to check that $S_k \wr S_l$ acts faithfully and imprimitively on the set $\{1, \ldots, k\} \times \{1, \ldots, l\}$, which is a set of size $kl = n$, by the rule:

$$(i, j)^{(x_1, \ldots, x_l)\sigma} := (i^{x_j}, j^{\sigma}).$$

It is straightforward to check that the above rule defines an action. This action is imprimitive, admitting $\Delta_j := \{1, \ldots, k\} \times \{j\}$ as a block system, $j = 1, \ldots, l$. Indeed,

$$\Delta_j^{(x_1, \ldots, x_l)\sigma} = \Delta_j^{\sigma} = \Delta_{j^{\sigma}}.$$

Finally, it is easy to see that this action is faithful: assume that $(i, j)^{(x_1, \cdots, x_l)\sigma} = (i, j)$ for all (i, j). Fix $j \in \{1, \ldots, l\}$, then $i^{x_j} = i$ for all $i \in \{1, \ldots, k\}$, and therefore $x_j = 1$ for all j. Moreover, $j^{\sigma} = j$ for all j and so $\sigma = 1$.

Actually, $S_k \wr S_l$ is a maximal imprimitive subgroup, meaning that it is no properly contained in any imprimitive subgroup of S_n. Moreover, every maximal imprimitive subgroup of S_n is of this type. This can be proved using the Embedding argument 2.4 as follows. Let $G \leq S_n$ be an imprimitive subgroup: this means that there is a non-trivial block $\Delta \subseteq \Omega$ for G; let $k := |\Delta|$ and let $H := \mathrm{Stab}_G(\Delta)$ be the setwise stabiliser of Δ in G. Since G acts transitively on the block system $\{\Delta^g \mid g \in G\}$, by the fundamental counting principle we have that $|\{\Delta^g \mid g \in G\}| = [G : H]$, call l this number. Since the translates of Δ partition $\{1, \ldots, n\}$, we have that $kl = n$. The action of H on Δ induces a homomorphism $\varphi : H \to \mathrm{Sym}(\Delta) \cong S_k$. By the Embedding argument, we obtain a homomorphism

$$f : G \to \varphi(H) \wr S_l \leq S_k \wr S_l,$$

with kernel the normal core of $\ker(\varphi)$ in G. Note that $h \in \ker(\varphi)$ if and only if h fixes Δ pointwise, and $h \in (\ker \varphi)^g$ if and only if h fixes Δ^g pointwise. Therefore, $\ker \varphi = 1$ and hence G embeds in the wreath product $S_k \wr S_l$.

To conclude, we observe that $S_k \wr S_l$ is actually a maximal subgroup of S_n. Indeed, a subgroup properly containing it would be primitive and would contain a 2-cycle (moving two elements of a block), therefore, as observed in the proof of the intransitive case, such a subgroup would be equal to the whole group S_n.

□

2.1.2 Primitive maximal subgroups

The O'Nan–Scott Theorem constitutes one of the most influential results in permutation group theory. There are many different versions of this theorem, some giving much more details than others; the following formulation is taken from [LPS87].

Theorem 2.6. *If X is A_n or S_n and M is any primitive maximal subgroup of X, with $M \neq A_n$, then M satisfies one of the following:*

(i) $M = \mathrm{AGL}_k(p) \cap X$, *with* $n = p^k$ *and* p *prime (affine case);*

(ii) $M = (T^k.(\mathrm{Out}\,T \times S_k)) \cap X$, *with* T *a non-abelian simple group,* $k \geq 2$ *and* $n = |T|^{k-1}$ *(diagonal case);*

(iii) $M = (S_k \wr S_l) \cap X$, *with* $n = k^l$, $k \geq 5$ *and* $l \geq 2$, *excluding the case where* $X = A_n$ *and* M *is imprimitive on* Ω *(wreath case);*

(iv) $T \trianglelefteq M \leqslant \mathrm{Aut}\,T$, *with* T *a non-abelian simple group,* $T \neq A_n$ *and* M *acting primitively on* Ω *(almost simple case).*

Since we will not need to use the explicit structure of these subgroups later, we shall not give details of the structure of the groups in each of these cases, and we refer the reader, for example, to Cameron's textbook [Cam99] for more information. Note that this theorem does not say that the groups listed are maximal in X, but certainly every maximal subgroup of X is of one of the types listed. We mention that, in [LPS87], Liebeck, Praeger and Saxl investigated when the groups M in $(i) - (iv)$ are maximal in MA_n.

We conclude this section by stating the following two results, which will be useful in the next chapter.

Theorem 2.7 ([LMS05])**.** *The symmetric group* S_n *has* $n^{o(1)}$ *conjugacy classes of primitive maximal subgroups.*

Here, $o(1)$ denotes a number that tends to 0 as n tends to infinity.

Theorem 2.8 ([LP93])**.** *The fraction of elements of* S_n *that belong to a non-trivial transitive subgroup decreases with* n *as* $n^{-\alpha}$, *for some absolute constant* $\alpha > 0$.

2.2 The classical groups

We now provide a short introduction to classical groups. We commend the unfamiliar reader to the book of Kleidman and Liebeck [[KL90b], Chapter 2], which we will mostly follow, for a detailed introduction to the topic.

Preliminaries

Let us start with some preliminary definitions. Let V be a vector space over a field $\mathbb{F}$. A map $f : V \times V \longrightarrow \mathbb{F}$ is a *left-linear form* if for each $v \in V$, the map $V \longrightarrow \mathbb{F}$ given by $u \mapsto f(u,v)$ is a linear map. f is called *non-degenerate* if for each $v \in V \setminus \{0\}$, the maps $V \longrightarrow \mathbb{F}$ given by $u \mapsto f(u,v)$ and $u \mapsto f(v,u)$ are non-zero. We will mostly omit the symbol f by writing $(\cdot,\cdot)$ for $f(\cdot,\cdot)$.

If $(\cdot,\cdot)$ is bilinear, we say that $(\cdot,\cdot)$ is alternating when $(v,v) = 0$ for all $v \in V$.

Recall that a *quadratic form* on V is a map $Q : V \longrightarrow \mathbb{F}$ such that

$$Q(\lambda v) = \lambda^2 Q(v), \text{ for all } v \in V \text{ and } \lambda \in \mathbb{F},$$

endowed with an *associated bilinear form* $(\cdot,\cdot)_Q$ defined as

$$(u,v)_Q = Q(u+v) - Q(u) - Q(v).$$

Q is said to be *non-degenerate* if $(\cdot,\cdot)_Q$ is non-degenerate and Q is *non-singular* if

$$rad(Q) = \{u \in V \mid Q(u) = 0 \text{ and } (u,v)_Q = 0 \text{ for all } v \in V\} = 0.$$

Assume that $(V,\mathbb{F},\kappa)$ and $(V',\mathbb{F},\kappa')$ are two spaces of dimension n over $\mathbb{F}$, where κ and κ' are either both left-linear or both quadratic forms. Therefore, κ and κ' are maps from V^l to $\mathbb{F}$, where $l = 1$ if κ and κ' are both quadratic and $l = 2$ otherwise. An invertible element $g \in \mathrm{Hom}_{\mathbb{F}}(V,V')$ is

(i) an *isometry* if $\kappa'(vg) = \kappa(v)$, for all $v \in V^l$;

(ii) a *similarity* if there exists $\lambda \in \mathbb{F}^*$ such that $k'(vg) = \lambda\kappa(v)$, for all $v \in V^l$.

If there exists such an isometry or similarity, we say that $(V,\mathbb{F},\kappa)$ and $(V',\mathbb{F},\kappa')$ are *isometric* or *similar*. If $(V,\mathbb{F},\kappa)$=$(V',\mathbb{F},\kappa')$, the sets of isometries and similarities of such a form are groups under composition and we denote them with $I(V,\mathbb{F},\kappa)$ and $\Delta(V,\mathbb{F},\kappa)$ respectively.

Now, we recall that a map $g : V \longrightarrow V$ is called an $\mathbb{F}$-semilinear transformation of V if there is a field automorphism $\sigma(g) \in \mathrm{Aut}(\mathbb{F})$ such that for all $u,v \in V$ and $\lambda \in \mathbb{F}$,

$$(u+v)g = ug + vg \text{ and } (\lambda v)g = \lambda^{\sigma(g)}(vg).$$

If g is an $\mathbb{F}$-semilinear transformation, then g is *non-singular* if $\{v \in V \mid vg = 0\} = 0$. We define $\Gamma\mathrm{L}(V,\mathbb{F})$ as the set of all non-singular $\mathbb{F}$-semilinear transformations of V. It is straightforward to check that if $g,h \in \Gamma\mathrm{L}(V,\mathbb{F})$, then their composition gh also lies in $\Gamma\mathrm{L}(V,\mathbb{F})$ and $\sigma(gh) = \sigma(g)\sigma(h)$. Therefore, $\Gamma\mathrm{L}(V,\mathbb{F})$ forms a group, called the *general semilinear group* of V over $\mathbb{F}$.

Finally, an element $g \in \Gamma\mathrm{L}(V,\mathbb{F})$ is called a κ-*semisimilarity* if there exist $\lambda \in \mathbb{F}^*$ and $\alpha \in \mathrm{Aut}(\mathbb{F})$ such that

$$\kappa(vg) = \lambda\kappa(v)^\alpha,$$

for all $v \in V^l$. The set of κ-semisimilarities forms a group, which we denote by $\Gamma(V,\mathbb{F},\kappa)$. It is easy to verify that the element λ appearing in the definition of g is uniquely determined by g. Thus, there is a well-defined map

$$\tau : \Gamma(V,\mathbb{F},\kappa) \longrightarrow \mathbb{F}^*,\ g \mapsto \lambda,$$

whose restriction to $\Delta(V,\mathbb{F},\kappa)$ is a homomorphism with kernel $I(V,\mathbb{F},\kappa)$.

Classical forms

Let p be a prime number, let r be a positive integer and let q be the number p^r. Unless otherwise specified, from now on V is an n-dimensional vector space over a field $\mathbb{F}$ of characteristic $p > 0$, where $\mathbb{F} = \mathbb{F}_{q^u}$, with $u \in \{1,2\}$, or $\mathbb{F} = \overline{\mathbb{F}}_p$ is algebraically closed. Let κ be a a left-linear form f or a quadratic form Q defined over the vector space V. We consider four cases.

L: $\kappa = f$ is identically 0.

S: $\kappa = f$ is a symplectic form, that is, a non-degenerate bilinear alternating form.

O: $\kappa = Q$ is a non-degenerate quadratic form.

U: $\kappa = f$ is a unitary form over a *finite* field $\mathbb{F} = \mathbb{F}_{q^2}$, that is, f is linear in the first variable, additive in the second, non-degenerate and $f(v,w) = f(w,v)^\sigma$ for all $v, w \in V$, where σ is the (unique) field automorphism of $\mathbb{F}$ of order 2.

The above forms are known as the *classical forms*.

If κ is a classical form on V and W is a vector subspace, we may consider κ_W, the restriction of κ to W (this is a minor abuse of terminology, for strictly speaking, κ_W is the restriction to $W \times W$ in cases **L**, **U** and **S**). We will be concerned with the cases when W is *non-degenerate*, which means that κ_W is non-degenerate, and when W is *totally singular*, which means $\kappa_W = 0$.

We recall that a symplectic form exists on V if and only if $n = 2m$ is even. 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** holds and $\mathbb{F}$ is a finite field, we distinguish three cases, according to the parity of the dimension n of V and the *Witt index* of the quadratic form on V, namely, the dimension of a maximal totally singular subspace of V with respect to the form (see [[KL90b], §§2.5-2.8]). We have the following trifurcation:

$\mathbf{O}^\circ$, if $n = 2m + 1$ is odd (here q is assumed to be odd, see Remark 2.2);

$\mathbf{O}^+$, if $n = 2m$ and (Q, V) has Witt index m;

$\mathbf{O}^-$, if $n = 2m$, and (Q, V) has Witt index $m - 1$.

We will refer to these forms, as *zero*, *plus-type* and *minus-type* quadratic forms, respectively. Instead, when $\mathbb{F}$ is an algebraically closed field, all non-degenerate quadratic forms on a $2m$-dimensional vector space V have Witt index m, and therefore we will omit the superscripts $\circ$ and $+$.

Remark 2.1. We highlight uniqueness of the just defined forms up to isometry/similarity and we describe standard bases in each case. Proofs can be found in [KL90b], Propositions 2.3.1, 2.3.2, 2.4.1, 2.5.3 and 2.5.4.

(i) Up to isometry, there is a unique symplectic form $(\cdot,\cdot)$ on a $2m$-dimensional vector space V and we consider the standard basis

$$\mathcal{B} = (e_1, f_1, \ldots, e_m, f_m)$$

and define the bilinear form $(\cdot,\cdot)$ as

$$(e_i, e_j) = (f_i, f_j) = 0, \quad (e_i, f_j) = \delta_{ij}.$$

(ii) A non-degenerate quadratic form $Q = Q^+$ of plus-type on a $2m$-dimensional vector space V is unique up to isometry and we fix the standard basis

$$\mathcal{B}^+ = (e_1, f_1, \dots, e_m, f_m)$$

and define the quadratic form Q^+, with associated bilinear form $(\cdot,\cdot) = (\cdot,\cdot)_{Q^+}$, as

$$Q^+(e_i) = Q^+(f_i) = 0,\ (e_i, e_j) = (f_i, f_j) = 0,\ (e_i, f_j) = \delta_{ij}.$$

(iii) The uniqueness of a non-degenerate quadratic form Q on a $(2m+1)$-dimensional vector space V is up to similarity. We fix the basis

$$\mathcal{B} = (e_1, f_1, \dots, e_m, f_m, x)$$

and define Q and $(\cdot,\cdot) = (\cdot,\cdot)_Q$ as

$$\begin{gathered} Q(e_i) = Q(f_i) = 0,\ Q(x) = 1, \\ (e_i, e_j) = (f_i, f_j) = (e_i, x) = (f_i, x) = 0,\ (e_i, f_j) = \delta_{ij}. \end{gathered}$$

(iv) Now, assume that $\mathbb{F} = \mathbb{F}_q$ and consider a non-degenerate quadratic form $Q = Q^-$ of minus type over a $2m$-dimensional vector space V, which is uniquely defined up to isometry. To be consistent with Subsection 2.2.10, we deviate from [KL90b] and we follow [GLS98]. We fix the basis

$$\mathcal{B}^- = (e_1, f_1, \dots, e_m, f_m, x_m, y_m)$$

and define Q^- and $(\cdot,\cdot) = (\cdot,\cdot)_{Q^-}$ as

$$\begin{gathered} Q^-(e_i) = Q^-(f_i) = 0,\ Q^-(x_m) = Q^-(y_m) = 1, \\ (e_i, e_j) = (f_i, f_j) = (e_i, x_m) = (f_i, x_m) = (e_i, y_m) = (f_i, y_m) = 0, \\ (e_i, f_j) = \delta_{ij},\ (x_m, y_m) = \zeta^2 + \zeta^{-2}, \end{gathered}$$

where $\zeta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ satisfies $\zeta^{q+1} = 1$.

(v) Finally, up to isometry, there is a unique unitary form $(\cdot,\cdot)$ on V and we may consider the standard basis

$$\mathcal{B} := \begin{cases} \{e_1, f_1, \dots, e_m, f_m\} & \text{if } n = 2m, \\ \{e_1, f_1, \dots, e_m, f_m, x\} & \text{if } n = 2m+1, \end{cases}$$

where

$$(e_i, e_j) = (f_i, f_j) = 0,\ (e_i, f_j) = \delta_{ij},\ (e_i, x) = (f_i, x) = 0,\ (x, x) = 1.$$

Let $\epsilon \in \{\circ, +, -\}$. We write

$$\mathrm{GU}_n(\mathbb{F}), \ \mathrm{Sp}_n(\mathbb{F}) \text{ and } \mathrm{O}_n^\epsilon(\mathbb{F})$$

for the isometry groups of a unitary, symplectic and quadratic form of ϵ-type on a $\mathbb{F}$-vector space V. We omit the superscript ϵ if $\mathbb{F} = \overline{\mathbb{F}}_p$, since there is no ambiguity. If $\mathbb{F} = \mathbb{F}_{q^u}$, we adopt the notation:

$$\mathrm{GL}_n(q), \ \mathrm{GU}_n(q), \ \mathrm{Sp}_n(q) \text{ and } \mathrm{O}_n^\epsilon(q).$$

Note in particular that with $\mathrm{GU}_n(q)$ we denote the isometry group of a unitary form on $\mathbb{F}^n_{q^2}$.

Remark 2.2. Although the uniqueness of a quadratic form Q on a $(2m+1)$- dimensional vector space V is only up to similarity, note that similar forms have isomorphic isometry groups, therefore it makes sense to write $\mathrm{O}^\circ_{2m+1}(\mathbb{F})$ for the isometry group of such a form. Moreover, in this case it is not restrictive to assume that p is odd, since when $p = 2$, then Q is degenerate and $\mathrm{O}_{2m+1}(\mathbb{F}) \cong \mathrm{Sp}_{2m}(\mathbb{F})$ (see [[Cam00], Theorem 6.1]).

If X is any subgroup of $\mathrm{GL}_n(\mathbb{F})$, then we write PX for the corresponding projective group $X/X \cap \mathbb{F}^*$. Moreover, let $S(V, \mathbb{F}, \kappa)$ denote the subgroup of $I(V, \mathbb{F}, \kappa)$ of determinant one maps.

As a matter of convenience we shall write

$$X = X(V, \mathbb{F}, \kappa),$$

where X ranges over the symbols S, I, Δ and Γ. Thus, we obtain a chain of groups:

$$S \leq I \leq \Delta \leq \Gamma. \tag{2.1}$$

We finally give the definition of *finite classical group*.

Definition of the finite classical groups

Let $\mathbb{F}$ be the finite field $\mathbb{F}_{q^u}$, as defined before, and let κ be a classical form on a finite-dimensional $\mathbb{F}$-vector space V. For each of the cases **L**, **S**, $\mathbf{O}^\epsilon$ and **U** we obtain the sequence of groups appearing in (2.1), and we define further groups $A = A(V, \mathbb{F}, \kappa)$ and $\Omega = \Omega(V, \mathbb{F}, \kappa)$ as follows. In case **L** with $n \geq 3$, the group $S = \mathrm{SL}(V, \mathbb{F})$ possesses an inverse-transpose automorphism ι ([see [KL90b], §2.1]), and in cases $\mathbf{O}^\epsilon$, the group S contains a certain subgroup of index 2 (see [[KL90b], §2.5]). We define

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

$$\Omega := \begin{cases} \text{this subgroup of index 2 in } S & \text{in cases } \mathbf{O}^\epsilon, \\ S & \text{otherwise.} \end{cases}$$

Thus, we obtain a chain of groups:

$$\Omega \leq S \leq I \leq \Delta \leq \Gamma \leq A. \tag{2.2}$$

This chain is A-invariant, that is, each group is normalized by A. Moreover $\mathbb{F}^* \trianglelefteq A$, and denoting by $\bar{\ }$ reduction modulo scalars, we obtain also a projective version of (2.2). The notation for the groups in chain (2.2) in the cases **L**, **S**, $\mathbf{O}^\epsilon$ and **U** is contained in Table 2.1.

Table 2.1: Notation for the finite classical groups

case	X	notation	terminology
L	$\Omega = S$	$\mathrm{SL}_n(q)$	linear groups
	$I = \Delta$	$\mathrm{GL}_n(q)$	
	Γ	$\Gamma\mathrm{L}_n(q)$	
	$A = \Gamma\langle\iota\rangle$		
U	$\Omega = S$	$\mathrm{SU}_n(q)$	unitary groups
	I	$\mathrm{GU}_n(q)$	
	Δ		
	$A = \Gamma$	$\Gamma\mathrm{U}_n(q)$	
S	$\Omega = S = I$	$\mathrm{Sp}_n(q)$	symplectic groups
	Δ	$\mathrm{GSp}_n(q)$	
	$A = \Gamma$	$\Gamma\mathrm{Sp}_n(q)$	
$\mathbf{O}^\epsilon$	Ω	$\Omega^\epsilon_n(q)$	orthogonal groups
	S	$\mathrm{SO}^\epsilon_n(q)$	
	I	$\mathrm{O}^\epsilon_n(q)$	
	Δ	$\mathrm{GO}^\epsilon_n(q)$	
	$A = \Gamma$	$\Gamma\mathrm{O}^\epsilon_n(q)$	

Definition 2.7. We define a *(finite) classical group* to be any group G satisfying

$$\Omega \leq G \leq A \text{ or } \overline{\Omega} \leq \overline{G} \leq \overline{A}, \tag{2.3}$$

in one of the cases **L**, **S**, $\mathbf{O}^\epsilon$ or **U**. If G is such a classical group, then G is called a *linear, symplectic, orthogonal* or *unitary group*, in the cases **L**, **S**, $\mathbf{O}^\epsilon$ or **U**, respectively. Moreover, the vector space V over which κ is defined is called the *natural module* for G.

Apart from a few special cases, the groups $\overline{\Omega}$ are non-abelian simple and comprise the *(finite) classical simple groups*, which are described in Table 2.2 (note that each excluded group is either not simple or coincides with another simple group [[KL90b], Theorem 2.1.3 and Proposition 2.9.1]). Furthermore, with only a few exceptions, $\overline{A} \cong \mathrm{Aut}(\overline{\Omega})$. We state with more precision some of these results, which correspond to Theorem 2.1.3 and Theorem 2.1.4 in [KL90b].

Theorem 2.9. *(i) Assume that $n = \dim_{\mathbb{F}}(V)$ is at least 2, 3, 4, 7 in cases* **L**, **U**, **S** *and* $\mathbf{O}^{\epsilon}$, *respectively. Then $\overline{\Omega}$ is non-abelian simple, except for* $\mathrm{PSL}_2(2)$, $\mathrm{PSL}_2(3)$, $\mathrm{PSU}_3(2)$ *and* $\mathrm{PSp}_4(2)$.

(ii) Assume that $\overline{\Omega}$ is simple and that n is as in (i). Then $\overline{A}$ = $\mathrm{Aut}(\overline{\Omega})$, *except when* $\Omega = \mathrm{Sp}_4(q)$ *with q even and when* $\Omega = \Omega_8^+(q)$.

Table 2.2: Finite simple classical groups

	$\mathrm{PSL}_n(q)$	$\mathrm{PSU}_n(q)$	$\mathrm{PSp}_n(q)$	$\mathrm{P}\Omega_n^{\epsilon}(q)$
lower bound on n	2	3	4	7
excluded (n, q)	(2,2),(2,3)	(3,2)	(4,2)	

2.2.0 Aschbacher theorem

A similar program to the O'Nan-Scott theorem for classifying the maximal subgroups of the classical groups began in 1984 with the publication of Aschbacher's paper on the subject [Asc84]. For an almost simple classical group G, Aschbacher introduces eight classes of natural, geometrically defined subgroups, labelled $\mathcal{C}_i$, for $1 \leq i \leq 8$, and shows that if M is a maximal subgroup of G not containing $\mathrm{soc}(G)$, then either M is contained in one of these natural subgroup collections, and we refer to it as a *geometric subgroup*, or it belongs to a family, denoted $\mathcal{S}$ or $\mathcal{C}_9$, of almost simple irreducible groups.

The book of Kleidman and Liebeck [KL90b] contains a definitive investigation of Aschbacher theorem, establishing the structure, conjugacy and, when $n \geq 13$, maximality of each geometric subgroup of each almost simple classical group. More precisely, they classify the conjugacy classes of maximal groups $\overline{H}$ of those almost simple groups $\overline{G}$ for which $\overline{\Omega} := \mathrm{soc}(G) = \Omega/Z(\Omega)$ for some classical quasisimple group Ω, with $\overline{H} \cap \overline{\Omega} = K/Z(\Omega)$ for a subgroup K of Ω of geometric type. If $n \leq 12$, then complete information on the maximal subgroups of almost simple classical groups is given in [BHR13]. We adopt Kleidman and Liebeck's formulation of the theorem (see [[KL90b], §3.1]) and, in particular, when we talk of Aschbacher class $\mathcal{C}_i$, we refer to the definition given in [[KL90b], §4.i], which differ slightly from Aschbacher's original definition. We roughly describe Aschbacher classes in Table 2.3 and we give a brief discussion of each class in the next paragraphs, closely following the presentation given by Bray, Roney-Dougal and Holt in [BHR13]. Sometimes, we also follow the book of Burness and Giudici [[BG16], subsections 2.6.2.1-2.6.2.8].

Theorem 2.10 (Aschbacher)**.** *Let G be an almost simple classical group and let M be a maximal subgroup of G not containing* $\mathrm{soc}(G)$. *Then M belongs to one of Aschbacher classes $\mathcal{C}_1, \ldots, \mathcal{C}_8$ or to the residual subgroup collection $\mathcal{C}_9$.*

Table 2.3: Aschbacher classes

	structure stabilised	rough descrpition in $\mathrm{GL}_n(q)$
$\mathcal{C}_1$	tot. sing. or non-sing. subspace	maximal parabolic
$\mathcal{C}_2$	$V = \bigoplus_{i=1}^t V_i,\ \dim(V_i) = a$	$\mathrm{GL}_a(q) \wr S_t$, with $n = at$
$\mathcal{C}_3$	Ext. fields of $\mathbb{F}_q$ of prime index b	$\mathrm{GL}_a(q^b).b,\ n = ab$
$\mathcal{C}_4$	Tensor product $V = V_1 \otimes V_2$	$\mathrm{GL}_a(q) \circ \mathrm{GL}_b(q),\ n = ab$
$\mathcal{C}_5$	Subfields of $\mathbb{F}_q$ of prime index b	$\mathrm{GL}_n(q_0),\ q = q_0^b$
$\mathcal{C}_6$	symplectic-type r-groups	$(C_{q-1} \circ r^{1+2a}).\,\mathrm{Sp}_{2a}(r),\ n = r^a$
$\mathcal{C}_7$	$V = \bigotimes_{i=1}^t V_i,\ \dim(V_i) = a$	$(\mathrm{GL}_a(q) \circ \cdots \circ \mathrm{GL}_a(q)).S_t,\ n = a^t$
$\mathcal{C}_8$	non-degenerate classical form	$\mathrm{GSp}_n(q), \mathrm{GO}_n^\epsilon(q), \mathrm{GU}_n(q^{1/2}) \circ C_{q-1}$

Remark 2.3. Note that maximality among the members of each class is described in [[KL90b], §7 and §8].

Before starting discussing Aschbacher classes, we recall the following notions from representation theory, following [[KL90b], §2.10].

Let G be any subgroup of $\mathrm{GL}(V, \mathbb{F})$. G is *irreducible* in $\mathrm{GL}(V, \mathbb{F})$ if G stabilises no proper non-zero subspace of $\mathbb{F}^n$, and is *reducible* otherwise. Let $\mathbb{F} \leq \mathbb{K}$ be a field extension. If $\{v_1, \dots, v_n\}$ are linearly independent vectors of $\mathbb{F}^n$, then they remain linearly independent in $\mathbb{K}^n$. We can extend the n-dimensional $\mathbb{F}$-vector space V to an n-dimensional vector space over $\mathbb{K}$, by considering the tensor product $V \otimes_{\mathbb{F}} \mathbb{K}$. Moreover, G acts on $V \otimes_{\mathbb{F}} \mathbb{K}$ via

$$(v \otimes \lambda)g = vg \otimes \lambda, \text{ for } v \in V, \lambda \in \mathbb{K} \text{ and } g \in G, h$$

and thus we may view $G \leq \mathrm{GL}(V \otimes_{\mathbb{F}} \mathbb{K}, \mathbb{K})$. In general, if G is irreducible in $\mathrm{GL}(V, \mathbb{F})$, this does not imply that G is irreducible in $\mathrm{GL}(V \otimes_{\mathbb{F}} \mathbb{K}, \mathbb{K})$.

Definition 2.8. We say that G is *absolutely irreducible* in $\mathrm{GL}(V, \mathbb{F})$ if G remains irreducible in $\mathrm{GL}(V \otimes_{\mathbb{F}} \mathbb{K}, \mathbb{K})$ for all field extensions $\mathbb{K}$ of $\mathbb{F}$.

It is straightforward to see that if $\mathbb{F} \leq \mathbb{K}_1 \leq \mathbb{K}_2$ and G is irreducible in $\mathrm{GL}(V \otimes_{\mathbb{F}} \mathbb{K}_2, \mathbb{K}_2)$, then G is irreducible in $\mathrm{GL}(V \otimes_{\mathbb{F}} \mathbb{K}_1, \mathbb{K}_1)$. Therefore G is absolutely irreducible if and only if G is irreducible in $\mathrm{GL}(V \otimes_{\mathbb{F}} \overline{\mathbb{F}}, \overline{\mathbb{F}})$, where $\overline{\mathbb{F}}$ is the algebraic closure of $\mathbb{F}$.

2.2.1 Aschbacher class $\mathcal{C}_1$: subspace stabilisers

All members of class $\mathcal{C}_1$ are reducible groups. More in detail, the following holds.

Definition 2.9. Let G be a group such that $\Omega \trianglelefteq G \leq A$ as in series (2.3), and let $K \leq G$.

(i) If $G \leq \Gamma$, then K lies in class $\mathcal{C}_1$ if $K = N_G(W) := \{g \in G \mid W^g = W\}$ or $K = N_G(U,W) := N_G(U) \cap N_G(W)$ for certain non-degenerate, totally-singular or non-singular subspaces U and W of V, as in [[KL90b], Table 4.1.A].

(ii) Otherwise, K lies in Aschbacher class $\mathcal{C}_1$ if $K = N_A(H) \cap G$, where H is a $\mathcal{C}_1$-subgroup of Γ.

Example 2.1. Fixing a basis $\{e_1, \cdots, e_n\}$ for $V = \mathbb{F}_{q^n}$ such that $W = \langle e_1, \ldots, e_m \rangle$, in $\mathrm{GL}_n(q)$, the stabiliser of the subspace W takes the forms of a block matrix:

$$\begin{pmatrix} A & B \\ O & C \end{pmatrix},$$

with $A \in \mathrm{GL}_m(q)$, $C \in \mathrm{GL}_{n-m}(q)$ and $B \in M_{m,n-m}(q)$.

Further information on the groups in this class can be found in [[KL90b], §4.1].

2.2.2 Aschbacher class $\mathcal{C}_2$: imprimitive subgroups

Let $n = at$, where $1 \leq a < n$, and consider a decomposition of the n-dimensional vector space V as a direct sum:

$$V = V_1 \oplus \cdots \oplus V_t, \tag{2.4}$$

where $\dim V_i = a$, for all $i = 1, \ldots, t$. We refer to such a decomposition as an a-decomposition of V.

Definition 2.10. A subgroup H of $\Gamma\mathrm{L}(V, \mathbb{F})$ is *imprimitive* if H stabilises an a-decomposition of V, for some $a \mid n$, i.e. H permutes the spaces V_i among themselves.

Roughly speaking, class $\mathcal{C}_2$ consists of imprimitive subgroups. More specifically, the following holds.

Definition 2.11. Let G be a group such that $\Omega \trianglelefteq G \leq A$ as in series (2.2), and let $K \leq G$.

(i) If $G \leq \Gamma$ then K lies in class $\mathcal{C}_2$ if K is the stabiliser in G of an a-decomposition, where the V_i are either all non-degenerate or totally singular, as described in [[KL90b],Table 4.2.A].

(ii) Otherwise, K lies in $\mathcal{C}_2$ if $K = N_A(H) \cap G$, where H is a $\mathcal{C}_2$-subgroup of Γ.

Example 2.2. The stabiliser of the decomposition (2.4) in $\mathrm{GL}_n(q)$ is

$$\mathrm{GL}_a(q) \wr S_t.$$

More details on the $\mathcal{C}_2$-subgroups can be found in [[KL90b], §4.2].

2.2.3 Aschbacher class $\mathcal{C}_3$: extension field stabilisers

The subgroups in class $\mathcal{C}_3$ arise as stabilisers of prime degree field extensions of $\mathbb{F}$. As usual, let V be an n-dimensional vector space over $\mathbb{F}_{q^u}$. Let b be a positive integer such that $b \mid n$ and let $\mathbb{F}_\#$ be a field extension of $\mathbb{F}$ of degree b, so that $\mathbb{F}_\# \cong \mathbb{F}_{(q^u)^b}$. Then V acquires the structure of an $\mathbb{F}_\#$-vector space in a natural way. Namely, let $V_\#$ be an $\frac{n}{b}$-dimensional vector space over $\mathbb{F}_\#$. Since $\mathbb{F}$ is a subfield of $\mathbb{F}_\#$, we may view $V_\#$ as an n-dimensional vector space over $\mathbb{F}$, and we may therefore identify it with V. (In the following, we write $V_\#$ for V regarded as a vector space over $\mathbb{F}_\#$). Moreover, since any $\mathbb{F}_\#$-linear map of V must also be $\mathbb{F}$-linear, we obtain an embedding

$$\mathrm{GL}_{n/b}(q^b) \cong \mathrm{GL}(V_\#, \mathbb{F}_\#) \leq \mathrm{GL}(V, \mathbb{F}) \cong \mathrm{GL}_n(q).$$

Suppose now that case **S** holds, so that κ is symplectic. Furthermore suppose that $\kappa_\#$ is a symplectic form on $(V_\#, \mathbb{F}_\#)$. Writing $T = T_{\mathbb{F}}^{\mathbb{F}_\#}$ (the trace map from $\mathbb{F}_\#$ to $\mathbb{F}$), it easy to see that $T\kappa_\#$ is a non-degenerate symplectic form on $(V, \mathbb{F})$. Consequently

$$\mathrm{Sp}_{n/b}(q^b) \cong I(V_\#, \mathbb{F}_\#, \kappa_\#) \leq I(V, \mathbb{F}, T_{\kappa_\#}) \cong \mathrm{Sp}_n(q).$$

Since, as already stated, all symplectic forms over an n-dimensional $\mathbb{F}$-vector space are isometric, without loss of generality we may take $\kappa = T\kappa_\#$, and hence we obtain an embedding $I_\# = I(V_\#, \mathbb{F}_\#, \kappa_\#) \leq I$. In a similar fashion we obtain various other embeddings in the cases **U** and $\mathbf{O}^\epsilon$ of an isometry group $I_\# = I(V_\#, \mathbb{F}_\#, \kappa_\#)$ in the isometry group of $I = I(V, \mathbb{F}, \kappa)$ (see [[KL90b], §4.3]).

Now, let $I_\# \leq I$ be an embedding as in [[KL90b], Table 4.3.A], let $\Gamma_\# = \Gamma(V_\#, \mathbb{F}_\#, \kappa_\#)$ and put $\tau_\# = \tau_{V_\#, \mathbb{F}_\#, \kappa_\#}$, where we recall that τ is the map that we have defined in the Preliminaries of this section. Define

$$\Gamma_{\#,\mathbb{F}} = \{g \in \Gamma_\# \mid \tau_\#(g) \in \mathbb{F}\}.$$

Then one checks that $\Gamma_{\#,\mathbb{F}} \leq \Gamma$.

Definition 2.12. If G is a subgroup such that $\Omega \leq G \leq A$, as in chain (2.3), a subgroup $K \leq G$ is a member of $\mathcal{C}_3$ if the following holds.

(i) If $G \leq \Gamma$, then $K = \Gamma_{\#,\mathbb{F}} \cap G$, with $b = [\mathbb{F}_\# : \mathbb{F}]$ prime, which arise with κ and $\kappa_\#$ as in [[KL90b], Table 4.3.A].

(ii) Otherwise, $K = N_A(H) \cap G$, where H is a $\mathcal{C}_3$-subgroup of Γ.

Example 2.3. If $G = \mathrm{GL}_n(q)$, then $\kappa = \kappa_\# = 0$ and $K = \mathrm{GL}_{n/b}(q^b) \rtimes \langle \varphi_q \rangle$, where φ_q is the standard q-Frobenius endomorphism. If $G = \mathrm{Sp}_n(q)$, then $k_\#$ is symplectic, $k = T\kappa_\#$ and $K = \mathrm{Sp}_{n/b}(q^b) \rtimes \langle \varphi_q \rangle$. Similarly, if $G = Y_n(q)$, where Y ranges over the symbol U or SO^ϵ, then $K = Y_{n/b}(q^b).b$, where K denotes the semidirect product of $Y_{n/b}(q^b)$ with the cyclic group of order b generated by a (generalised) Frobenius endomorphism. The generators of these cyclic groups are described in detail in Example 2.8 . We note that all the subgroups that we exemplified are indeed maximal, and we will use them in Chapter 3, Lemma 3.9.

For more information about the $\mathcal{C}_3$-subgroups, we refer the reader to [[KL90b], §4.3].

2.2.4 Aschbacher class $\mathcal{C}_4$: tensor product stabilisers, I

Definition 2.13. A group $G \leq \Gamma\mathrm{L}(V)$ *preserves* a tensor product decomposition $V = V_1 \otimes V_2$ if for all $g \in G$ there exist $g_1 \in \Gamma\mathrm{L}(V_1)$ and $g_2 \in \Gamma\mathrm{L}(V_2)$ such that for all $v_1 \in V_1$ and $v_2 \in V_2$

$$(v_1 \otimes v_2)g = v_1 g_1 \otimes v_2 g_2.$$

Aschbacher class $\mathcal{C}_4$ consists of groups which preserve appropriate tensor product decompositions $V = V_1 \otimes V_2$. More in detail, this subgroup collection is defined as follows.

Definition 2.14. Let G be a group such that $\Omega \trianglelefteq G \leq A$, as in series (2.3), and let $K \leq G$. Then the following holds.

(i) If $G \leq \Gamma$ then K lies in Aschbacher class $\mathcal{C}_4$ if K is the stabiliser in G of a tensor product decomposition $V_1 \otimes V_2$, where V_1 and V_2 are equipped with zero or non-degenerate forms f_i (i=1,2), as described in [[KL90b], Table 4.4.A], such that (V_1, f_1) is not similar to (V_2, f_2).

(ii) Otherwise, K lies in $\mathcal{C}_4$ if $K = N_A(H) \cap G$, where H is a $\mathcal{C}_4$-subgroup of Γ.

Example 2.4. If $G = \mathrm{GL}_n(q)$, the stabiliser of the tensor product $V = V_1 \otimes V_2$, where $\dim V_1 = n_1$ and $\dim V_2 = n_2$ is

$$\mathrm{GL}_{n_1}(q) \otimes \mathrm{GL}_{n_2}(q) \cong \mathrm{GL}_{n_1}(q) \circ \mathrm{GL}_{n_2}(q).$$

See [[KL90b], §4.4] for more details on this class.

2.2.5 Aschbacher class $\mathcal{C}_5$: subfield stabilisers

Definition 2.15. A subgroup H of $\mathrm{GL}_n(q)$ is a *subfield group* if H is absolutely irreducible and there exists a proper subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$ and an element $g \in \mathrm{GL}_n(q)$ such that

$$H^g \leq \langle Z(\mathrm{GL}_n(q)), \mathrm{GL}_n(q_0)\rangle,$$

i.e., up to scalars, H is conjugate to a group over a proper subfield of $\mathbb{F}_q$.

The members of Aschbacher class $\mathcal{C}_5$ can be described as subfield groups. More in detail, let $\mathbb{F}_\#$ be a subfield of index b in $\mathbb{F}$, so that $\mathbb{F}_\# \cong \mathbb{F}_{q^{u/b}}$. Let $\beta = \{v_1, \dots, v_n\}$ be a $\mathbb{F}$-basis of V and define $V_\#$ to be the $\mathbb{F}_\#$-span of β. Then $V_\#$ is an n-dimensional $\mathbb{F}_\#$-space isomorphic to $\mathbb{F}^n_{q^{u/b}}$. If $v = \sum_{i=1}^n \lambda_i v_i$, with $\lambda_i \in \mathbb{F}$, is an arbitrary element of V and $g \in \mathrm{GL}(V_\#, \mathbb{F}_\#)$ such that $v_i g := w_i$, then $\mathrm{GL}(V_\#, \mathbb{F}_\#)$ acts naturally on V by setting $vg = \sum_{i=1}^n \lambda_i w_i$. This action is faithful and hence there is a natural inclusion:

$$\mathrm{GL}_n(q^{u/b}) \cong \mathrm{GL}(V_\#, \mathbb{F}_\#) \leq \mathrm{GL}(V, \mathbb{F}) \cong \mathrm{GL}_n(q^u),$$

which extends to $\Gamma\mathrm{L}_n(q^{u/b}) \leq \Gamma\mathrm{L}_n(q^u)$.

In the following definition, for $G \leq \Gamma$, let $N_G(V_\#)$ denote the set of elements that fix $V_\#$ and in addition, if $V_\#$ is equipped with a form, act as semi-similarities of $V_\#$.

Definition 2.16. Let G be a group such that $\Omega \trianglelefteq G \leq A$, as in chain (2.3), and let $K \leq G$.

(i) If $G \leq \Gamma$, then K lies in class $\mathcal{C}_5$ if $K = N_G(V_\#)(Z(\mathrm{GL}_n(q^u)) \cap G)$, for some $\mathbb{F}_\#$-vector space $V_\#$ equipped with a form $\kappa_\# = \kappa_{V_\#}$ as in [[KL90b], Table 4.5.A], and where $b = [\mathbb{F} : \mathbb{F}_\#]$ is prime.

(ii) Otherwise, K lies in class $\mathcal{C}_5$ if $K = N_A(H) \cap G$, where H is a $\mathcal{C}_5$-subgroup of Γ.

Example 2.5. If $G = \mathrm{GL}_n(q)$, then $K = \mathrm{GL}_n(q^{1/b}) \circ C_{q-1}$.

Further information about the groups in this class can be found in [[KL90b], §4.5].

2.2.6 Aschbacher class $\mathcal{C}_6$: symplectic-type group stabilisers

We start the discussion of this class by recalling the following notions.

Definition 2.17. Let R be an r-group for some prime r.

(i) R is called *special* if $Z(R) = R' = \mathrm{Frat}(R)$.

(ii) A special group is said *extraspecial* if also $|Z(R)| = r$.

(iii) R is said to be of *symplectic-type* if every characteristic abelian subgroup of R is cyclic.

The description of the structure of extraspecial groups dates back to an old result of P. Hall. See [[Suz82], p.69] for a proof. The structure of symplectic-type r-groups is also well-understood, and is closely linked to that of extraspecial groups. More precisely, R is the central product of an extraspecial r-group and a group that is either cyclic, dihedral, semidihedral or quaternion (see [[Suz82], pp.75-76]). For the definition of the members of this Aschbacher class, we are only interested in those symplectic-type r-groups of minimal exponent: this is r, if r is odd and it is 2 or 4, if $r = 2$.

Definition 2.18. Let G be a group such that $\Omega \trianglelefteq G \leq A$, as in Series 2.3, and let $K \leq G$. Then K is a member of class $\mathcal{C}_6$ if $K = N_G(R)$, where $R \leq \Delta$ is a symplectic-type r-group of minimal exponent, for r a prime, $r \neq p$, as described in [[KL90b], Table 4.6.A], which acts absolutely irreducibly on the vector space V. To ensure that K is not contained in a $\mathcal{C}_5$-subgroup of G, it is required the condition $\mathbb{F} = \mathbb{F}_{p^e}$, where e is the smallest integer for which $p^e \equiv 1 \pmod{|Z(R)|}$.

These are rather restrictive conditions, and class $\mathcal{C}_6$ is empty for "most" classical groups. More details on this subgroup collection are contained in [[KL90b], §4.6].

2.2.7 Aschbacher class $\mathcal{C}_7$: tensor product stabilisers, II

While Aschbacher class $\mathcal{C}_4$ considers the stabilisers of a tensor product where the factors (V_i, κ_i) are not similar, the case when the tensor product factors are all similar is covered by class $\mathcal{C}_7$. These subgroups are sometimes referred as *wreathed* tensor product stabilisers, as their structure is, indeed, a wreath product.

Definition 2.19. (i) A group $G \leq \Gamma\mathrm{L}(V)$ *preserves* a tensor induced decomposition $V = V_1 \otimes V_2 \otimes \cdots \otimes V_t$ if for all $g \in G$ there exist $g_i \in \Gamma\mathrm{L}(V_i)$ and $\sigma \in S_t$ such that, for all $v_i \in V_i$:

$$(v_1 \otimes \cdots \otimes v_t)g = v_{1\sigma}g_{1\sigma} \otimes \cdots \otimes = v_{t\sigma}g_{t\sigma}.$$

If non-degenerate forms f_i have been defined on the V_i, then, in addition, it is required that the g_i are elements of the Γ-group for that form.

(ii) A subgroup H of $\mathrm{GL}_n(q)$ is a *tensor induced group* if H preserves a tensor induced decomposition $\mathbb{F}_q^n = V_1 \otimes \cdots \otimes V_t$, with $\dim V_i = a$ for all i and $n = a^t$.

All members of class $\mathcal{C}_7$ are tensor induced. More in detail the following holds.

Definition 2.20. Let G be a group such that $\Omega \trianglelefteq G \leq A$ as in chain (2.3), and let $K \leq G$. Write G_i for the stabiliser in G of the set $0 \otimes \cdots \otimes V_i \otimes \cdots 0$ of pure tensors with the only nonzero element occurring in the i-th position.

(i) If $G \leq \Gamma$, then K lies in class $\mathcal{C}_7$ if K is the stabiliser in G of a tensor induced decomposition, with the property that the induced action of $K \cap G_i$ on V_i preserve a certain form f_i on V_i, given in [[KL90b], Table 4.7.A]. In this case, (V_1, f_1) is similar to (V_i, f_i) for each i.

(ii) Otherwise, K lies in Aschbacher class $\mathcal{C}_7$ if $K = N_A(H) \cap G$, where H is a $\mathcal{C}_7$-subgroup of Γ.

Example 2.6. If $G = \mathrm{GL}_n(q)$, then $K = (\mathrm{GL}_a(q) \circ \cdots \circ \mathrm{GL}_a(q)) \wr S_t$.

For a more detailed descripiton of the $\mathcal{C}_7$-subgroups we refer the reader to [[KL90b], §4.7].

2.2.8 Aschbacher class $\mathcal{C}_8$: classical subgroups

This class consists of classical subgroups.

Definition 2.21. Let G be a group such that $\Omega \trianglelefteq G \leq A$ as in chain (2.3), and let $K \leq G$.

(i) If $G \leq \Gamma$, then K lies in class $\mathcal{C}_8$ if K is the intersection with G of the Γ-group $\Gamma(V, \mathbb{F}, k_\#)$ of a classical group, where $\kappa_\#$ is a non-degenerate form given in [[KL90b], Table 4.8.A].

(ii) Otherwise, K lies in Aschbacher class $\mathcal{C}_8$ if $K = N_A(H) \cap G$, where H is a $\mathcal{C}_8$-subgroup of Γ.

Example 2.7. If $G = \mathrm{GL}_n(q)$, then K is isomorphic to one of the following groups:

(i) $\mathrm{GSp}_n(q)$, if $k_\#$ is symplectic, n is even and $n \geq 4$;

(ii) $\mathrm{GU}_n(q^{1/2}) \circ C_{q-1}$, if $k_\#$ is unitary, q is a square and $n \geq 3$;

(iii) $\mathrm{GO}_n^\epsilon(q)$, if $\kappa_\#$ is a non-degenerate quadratic form of ϵ-type, q is odd and $n \geq 3$.

See [[KL90b], §4.8] for further details on this class.

2.2.9 The collection $\mathcal{C}_9$

Recall that given a group K, we may define by induction its derived series $\{K^{(i)}\}_{i\geq 0}$, where $K^{(0)} = K$, and, for $n \geq 0$, $K^{(n+1)} = [K^{(n)}, K^{(n)}]$. Moreover, we define $K^{\infty} = \cap_{i\geq 0} K^{(i)}$. Note that, if S is non-abelian simple, with $S \trianglelefteq G \leq \mathrm{Aut}(S)$, then $K^{\infty} = S$.

The members of the residual collection $\mathcal{C}_9$ are defined as follows.

Definition 2.22. Let K be a subgroup of G, where $\Omega \trianglelefteq G \leq A$ as in series (2.3). Then K is a member of the collection $\mathcal{C}_9$ if $K/(K \cap Z(GL_n(q^u)))$ is almost simple and the following all hold:

(i) K does not contain Ω;

(ii) K^{∞} acts absolutely irreducibly;

(iii) there does not exist a $g \in \mathrm{GL}_n(q^u)$ such that $(K^{\infty})^g$ is defined over a proper subfield of $\mathbb{F}_{q^u}$;

(iv) K^{∞} preserves a non-zero unitary form if and only if $\Omega = \mathrm{SU}_n(q)$;

(v) K^{∞} preserves a non-zero quadratic form if and only if $\Omega = \Omega_n^{\epsilon}(q)$;

(vi) K^{∞} preserves a non-zero symplectic form and no non-zero quadratic form if and only if $\Omega = \mathrm{Sp}_n(q)$;

(vii) K^{∞} preserves no non-zero classical form if and only if $\Omega = \mathrm{SL}_n(q)$.

2.2.10 Shintani descent

Shintani descent is a technique from the theory of algebraic groups that provides a bijection, the *Shintani map*, between conjugacy classes of almost simple groups. In this paragraph we state Shintani descent without dwelling too much on the general theory, since it goes beyond the scope of this work, and we refer the reader to the book of Harper [[Har21], Chapter 3], which we will closely follow, for a detailed treatment of the subject. Instead, we will consider some concrete examples that will be useful in the next chapter, in the context of studing maximal subgroups in Aschbacher class $\mathcal{C}_3$.

We begin by establishing some terminology. By an *algebraic group* we mean a linear algebraic group over an algebraically closed field $\overline{\mathbb{F}}_p$, namely, a closed subgroup X of $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$, for some n, where $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$ is endowed with the Zariski topology. We will moreover require that algebraic groups are *connected*, meaning that that the underlying affine variety is connected for the Zariski topology.

Definition 2.23. A *Steinberg endomorphism* of an algebraic group X is a bijective morphism $\sigma : X \to X$ whose fixed point subgroup

$$X_{\sigma} = \{x \in X \mid x^{\sigma} = x\}$$

is finite.

The modern way of studying finite groups of Lie type is to view them as the fixed points under Steinberg endomorphisms of semisimple algebraic groups. In the next example we briefly show how to construct the finite classical groups $\mathrm{GL}_n(q)$, $\mathrm{Sp}_n(q)$, $\mathrm{GU}_n(q)$ and $\mathrm{O}_n^{\epsilon}(q)$ in this way and, in doing so, we will mostly follow the book of Malle and Testerman [MT11].

Example 2.8. As usual, let $q = p^r$.

(i) The Frobenius automorphism $\varphi_q : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$, $t \mapsto t^q$ is a field automorphism of $\overline{\mathbb{F}}_p$ which fixes $\mathbb{F}_q$ pointwise. In fact, the Galois group $Gal(\overline{\mathbb{F}}_p/\mathbb{F}_q)$ is generated (as a profinite group) by this map. Letting φ_q act on the matrix entries, this induces a Steinberg endomorphism of $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$, which we call the *standard q-Frobenius endomorphism* with respect to the basis $\mathcal{B}$ for $\overline{\mathbb{F}}_p^n$:

$$\varphi_q : \mathrm{GL}_n(\overline{\mathbb{F}}_p) \to \mathrm{GL}_n(\overline{\mathbb{F}}_p), \qquad (a_{ij}) \mapsto (a_{ij}^q),$$

where the elements of $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$ are written as matrices with respect to $\mathcal{B}$. If the basis $\mathcal{B}$ is understood, we will omit reference to it. Moreover, in the following, we will also identify φ_q with the map induced on φ_q-stable subgroups of $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$. The fixed point subgroup of φ_q is

$$\mathrm{GL}_n(\overline{\mathbb{F}}_p)_{\varphi_q} = \{(a_{ij}) \in \mathrm{GL}_n(\overline{\mathbb{F}}_p) \mid (a_{ij}^q) = (a_{ij})\} = \mathrm{GL}_n(q).$$

(ii) Analogously, we can consider the standard q-Frobenius endomorphism φ_q of X, with respect to the basis $\mathcal{B}$, where $X \in \{\mathrm{Sp}_n(\overline{\mathbb{F}}_p), \mathrm{O}_{2m}(\overline{\mathbb{F}}_p), \mathrm{O}_{2m+1}(\overline{\mathbb{F}}_p)\}$ and $\mathcal{B}$ is the corresponding standard basis described in Remark 2.1, points (i), (ii) and (iii) respectively. In this way, the fixed point subgroups are respectively:

- $\mathrm{Sp}_n(\overline{\mathbb{F}}_p)_{\varphi_q} = \mathrm{Sp}_n(q)$,
- $\mathrm{O}_{2m}(\overline{\mathbb{F}}_p)_{\varphi_q} = \mathrm{O}_{2m}^{+}(q)$,
- $\mathrm{O}_{2m+1}(\overline{\mathbb{F}}_p)_{\varphi_q} = \mathrm{O}_{2m+1}^{\circ}(q)$.

(iii) Now, let us move to the unitary case. Let $\mathcal{B}$ be the orthonormal basis for a unitary form described in Remark 2.1, point (v), and let us consider the Steinberg endomorphism

$$\phi : \mathrm{GL}_n(\overline{\mathbb{F}}_p) \to \mathrm{GL}_n(\overline{\mathbb{F}}_p), \qquad (a_{ij}) \mapsto (a_{ij}^q)^{-t},$$

which is the composite of φ_q, which we write with respect to $\mathcal{B}$, with the standard involutory graph automorphism, which sends a matrix to the transpose of its inverse, and these two maps commute. Here, the fixed point subgroup is

$$\mathrm{GL}_n(\overline{\mathbb{F}}_p)_{\phi} = \mathrm{GU}_n(q).$$

Indeed, note that $\phi^2 : \mathrm{GL}_n(\overline{\mathbb{F}}_p) \to \mathrm{GL}_n(\overline{\mathbb{F}}_p)$, $(a_{ij}) \mapsto (a_{ij}^{q^2})$ is the standard q^2-Frobenius endomorphism and, therefore, the fixed points under ϕ satisfy

$$\mathrm{GL}_n(\overline{\mathbb{F}}_p)_\phi \leq \mathrm{GL}_n(\overline{\mathbb{F}}_p)_{\phi^2} = \mathrm{GL}_n(\overline{\mathbb{F}}_p)_{\varphi_{q^2}} = \mathrm{GL}_n(q^2).$$

To conclude, recall that, writing elements of $\mathrm{GU}_n(q)$ with respect to the basis $\mathcal{B}$, an element $A \in \mathrm{GL}_n(q^2)$ belongs to $\mathrm{GU}_n(q)$ exactly when $A(A^{(q)})^t = \mathbb{1}$, where if $A = (a_{ij})$, then $A^{(q)} = (a_{ij}^q)$.

(iv) Finally, we move to minus-type orthogonal groups. Following a comment in [[Har19], Introduction to Chapter 5], we remark that there are two natural definitions of the minus-type orthogonal group $\mathrm{O}^-_{2m}(q)$. On one side, as we previously defined it, it is the isometry group of a quadratic form of minus-type on the vector space $\mathbb{F}_q^{2m}$, and consequently it is a subgroup of $\mathrm{GL}_{2m}(q)$ in a natural way. On the other side, as in [[MT11], Example 22.9], we can define it as the group of fixed points under a Steinberg endomorphism of the algebraic group $\mathrm{O}_{2m}(\overline{\mathbb{F}}_p)$, and the group obtained in this way is not a subgroup of $\mathrm{GL}_{2m}(q)$ but is naturally a subgroup of $\mathrm{O}^+_{2m}(q^2)$. This perspective allows one to make use of the theory of algebraic groups, in particular Shintani descent. We now define minus-type orthogonal groups using this second viewpoint and we highlight the isomorphism between the two groups.

With respect to the basis $\mathcal{B}^+$ described in Remark 2.1, point (ii), let us consider the standard q-Frobenius endomorphism φ_q of $\mathrm{O}_{2m}(\overline{\mathbb{F}}_p)$ and the element

$$g := I_{2m-2} \perp \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{O}_{2m}(\overline{\mathbb{F}}_p),$$

that centralises the decomposition $\langle e_1, \dots, f_{m-1}\rangle \perp \langle e_m, f_m\rangle$.

Let γ be the Steinberg endomorphism $\gamma := g\varphi_q$ of $\mathrm{O}_{2m}(\overline{\mathbb{F}}_p)$. Following [MT11], the general orthogonal group of minus-type is the fixed point subgroup $\mathrm{O}_{2m}(\overline{\mathbb{F}}_p)_\gamma$.

Following [[Har19], Lemma 2.6.17], there exists an inner automorphism Ψ of $\mathrm{GL}_{2m}(\overline{\mathbb{F}}_p)$ such that, if $X = \mathrm{O}_{2m}(\overline{\mathbb{F}}_p)$, then

$$\Psi(X_\gamma) = \mathrm{O}^-_{2m}(q).$$

To view this, let Q^+ be the quadratic form on $\overline{\mathbb{F}}_p^{2m}$ with bilinear form $(\cdot,\cdot)$. Let Ψ be the endomorphism of $\mathrm{GL}_{2m}(\overline{\mathbb{F}}_p)$ induced by conjugation by the element $A = I_{2m-2} \perp A'$ that centralises $\langle e_1, \dots, f_{m-1}\rangle \perp \langle e_m, f_m\rangle$, where

$$A' := \begin{pmatrix} \zeta & \zeta^{-1} \\ \zeta^{-1} & \zeta \end{pmatrix},$$

with $\zeta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, such that $\zeta^{q+1} = 1$.

Write $x_m = e_m A$ and $y_m = f_m A$. An easy calculation yields $Q(x_m) = Q(y_m) = 1$ and $(x_m, y_m) = \zeta^2 + \zeta^{-2}$, therefore, without loss of generality, we may assume that $\mathcal{B}^+ A$ is the basis $\mathcal{B}^-$ defined in Remark 2.1, point (iv).

Now, let $\varphi_{\mathcal{B}^\epsilon}$ denote the standard q-Frobenius endomorphism with respect to the basis $\mathcal{B}^\epsilon$, with $\epsilon \in \{+,-\}$. It is straightforward to check that $AA^{-(q)} = g$ and putting all this together, we obtain that $\Psi(X_\gamma) = A^{-1} X_\gamma A = X_{\varphi_{\mathcal{B}^-}} = \mathrm{O}^-_{2m}(q)$. Note that in the following we will use both viewpoints and we adopt the notation $\mathrm{O}^-_{2m}(q)$ in both cases.

Now, we record the following crucial fact, known as the Lang-Steinberg theorem, and the subsequent corollary, which allows us to well-define Shintani maps.

Theorem 2.11 (Lang-Steinberg Theorem). *Let X be a connected algebraic group and let σ be a Steinberg endomorphism of X. The map $L : X \longrightarrow X$ defined as $L(x) = xx^{-\sigma}$ is surjective.*

Corollary 2.12. *Let X be a connected algebraic group and let σ be a Steinberg endomorphism of X. The map $L' : X \longrightarrow X$ defined as $L'(x) = xx^{-\sigma^{-1}}$ is surjective.*

Proof. Let $y \in X$. By Theorem 2.11, there exists $x \in X$ such that $y^{-\sigma} = xx^{-\sigma}$. Therefore, $y = xx^{-\sigma^{-1}}$ and L' is surjective. □

Let X be a connected algebraic group and let σ be a Steinberg endomorphism of X. We consider the semidirect product $X \rtimes \langle \sigma \rangle$, where $\sigma^{-1} x \sigma = x^\sigma = \sigma(x)$ for all $x \in X$. For $e > 1$ the subgroup X_{σ^e} is σ-stable, so σ restricts to an automorphism $\tilde{\sigma} = \sigma|_{X_{\sigma^e}}$ of X_{σ^e}. Therefore, we may also consider the finite semidirect product $X_{\sigma^e} \rtimes \langle \tilde{\sigma} \rangle$, where $g^{\tilde{\sigma}} = \tilde{\sigma}(g) = \sigma(g)$ for all $g \in X_{\sigma^e}$, noting that $|\tilde{\sigma}| = e$.

Definition 2.24 (Shintani map). A *Shintani map* is a map of conjugacy classes of the form

$$\begin{aligned} S : \{(g\tilde{\sigma})^{X_{\sigma^e} \rtimes \langle \tilde{\sigma} \rangle} \mid g \in X_{\sigma^e}\} &\longrightarrow \{x^{X_\sigma} \mid x \in X_\sigma\} \\ (g\tilde{\sigma})^{X_{\sigma^e} \rtimes \langle \tilde{\sigma} \rangle} &\longmapsto (a^{-1}(g\tilde{\sigma})^e a)^{X_\sigma}, \end{aligned}$$

where $a \in X$ satisfies $g = aa^{-\sigma^{-1}}$ (which exists by Corollary 2.12).

Remark 2.4. If $g\tilde{\sigma}$ and $h\tilde{\sigma}$ are $(X_{\sigma^e} \rtimes \langle \tilde{\sigma} \rangle)-$conjugate, then they are $X_{\sigma^e}-$conjugate. For the sake of brevity, in the following let us slightly abuse notation by writing σ for $\tilde{\sigma}$. To see this, assume that $g\sigma = (w\sigma^i)^{-1} h\sigma (w\sigma^i)$, for some $w \in X_{\sigma^e}$ and $i \geq 0$. Then

$$g\sigma = (g\sigma)^i (w\sigma^i)^{-1} h\sigma (w\sigma^i)(g\sigma)^{-i}$$

and $(g\sigma)^i (w\sigma^i)^{-1} \in X_{\sigma^e}$, therefore $g\sigma$ and $h\sigma$ are in fact $X_{\sigma^e}-$conjugate. Consequently, S is a map from the set of $X_{\sigma^e}-$conjugacy classes in the coset $X_{\sigma^e}\sigma$ to the set of $X_\sigma-$classes in X_σ.

Theorem 2.13 (Shintani Descent). *Let X be a connected algebraic group. Let σ be a Steinberg endomorphism of X and let $e > 1$. Let S be a Shintani map of (X, σ, e). Then, the map S is a well-defined bijection, which does not depend on the choice of $a \in X$.*

We give some explicit applications of Shintani descent, which will be useful in Chapter 3, in the context of determining the number of conjugacy classes in maximal subgroups of classical groups in Aschbacher class $\mathcal{C}_3$.

Example 2.9 (GL_n)**.** Let S be the Shintani map of (X, φ_q, b), where $X = \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ and φ_q is the standard q-Frobenius endomorphism of X.

Note that $X_{\varphi_q} = \mathrm{GL}_n(q)$ and $X_{\varphi_q^b} = X_{\varphi_{q^b}} = \mathrm{GL}_n(q^b)$. Therefore, Shintani descent tells us that the Shintani map

$$S : \{(g\varphi_q)^{\mathrm{GL}_n(q^b)} \mid g \in \mathrm{GL}_n(q^b)\} \longrightarrow \{x^{\mathrm{GL}_n(q)} \mid x \in \mathrm{GL}_n(q)\}$$

gives a bijection between the set of conjugacy classes of $\mathrm{GL}_n(q^b) \rtimes \langle \varphi_q \rangle$ in the coset $\mathrm{GL}_n(q^b)\varphi_q$ and the set of conjugacy classes of $\mathrm{GL}_n(q)$.

In a similar fashion, let us fix $1 < i < b$, with $i \mid b$. Let now S be the Shintani map of (X, φ_q^i, e), where X and φ_q are as before and $e := b/i$. Then, $X_{\varphi_q^i} = \mathrm{GL}_n(q^i)$ and $X_{(\varphi_q^i)^e} = X_{\varphi_q^b} = \mathrm{GL}_n(q^b)$. Therefore, S provides a bijection between the set of conjugacy classes of $\mathrm{GL}_n(q^b) \rtimes \langle \varphi_q \rangle$ in the coset $\mathrm{GL}_n(q^b)\varphi_q^i$ and the set of conjugacy classes of $\mathrm{GL}_n(q^i)$.

Let us consider other examples, respectively in the symplectic, unitary and orthogonal cases. We always denote with b a positive integer, and we consider $0 < i < b$, with $i \mid b$ and $e := b/i$.

Example 2.10 (Sp_n)**.** Proceeding as in the previous example, let now S be the Shintani map of (X, φ_q^i, e), where $X = \mathrm{Sp}_n(\overline{\mathbb{F}}_p)$ and φ_q is the standard q-Frobenius endomorphism with respect to the basis $\mathcal{B}$, described in Example 2.8, point (i). Then S gives a $1-1$ correspondence between the set of conjugacy classes of $\mathrm{Sp}_n(q^b) \rtimes \langle \varphi_q \rangle$ in the coset $\mathrm{Sp}_n(q^b)\varphi_{q^i}$ and the set of conjugacy classes of $\mathrm{Sp}_n(q^i)$.

Example 2.11 (GU_n)**.** Now, we consider general unitary groups. Note that, given the nature of the Steinberg endomorphism, in this case we also need to assume that b is odd to obtain the desired bijection. Let S be the Shintani map of (X, ϕ^i, e), where $X = \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ and ϕ is the Steinberg endomorphism described in Example 2.8. Then S puts in bijection the set of conjugacy classes of $\mathrm{GU}_n(q^b) \rtimes \langle \phi \rangle$ in the coset $\mathrm{GU}_n(q^b)\phi^i$ and the set of conjugacy classes of $\mathrm{GU}_n(q^i)$.

Example 2.12 (SO_n)**.** Finally, we consider orthogonal groups: let us first deal with those of plus and zero-type. Let S be the Shintani map of (X, φ_q^i, e), where $X \in \{\mathrm{SO}_{2m}(\overline{\mathbb{F}}_p), \mathrm{SO}_{2m+1}(\overline{\mathbb{F}}_p)\}$ and φ_q is the standard q-Frobenius endomorphism with respect to the corresponding standard bases in Example 2.8, points (ii) and (iii). Then, respectively, $X_{\varphi_q^i} = X_{\varphi_{q^i}} \in \{\mathrm{SO}^+_{2m}(q^i), \mathrm{SO}^\circ_{2m+1}(q^i)\}$ and $X_{(\varphi_q^i)^e} = X_{\varphi_{q^b}} \in \{\mathrm{SO}^+_{2m}(q^b), \mathrm{SO}^\circ_{2m+1}(q^b)\}$, so S is a bijection between the set of $X_{\varphi_{q^b}} \rtimes \langle \varphi_q \rangle$- conjugacy classes in the coset $X_{\varphi_{q^b}}\varphi_{q^i}$ and the set of conjugacy classes of $X_{\varphi_{q^i}}$.

To conclude, let us consider the special orthogonal groups of minus-type. As in Example 2.11, here we need to assume that b is odd. let S be the Shintani map of (X, γ^i, e), where $X \in \mathrm{SO}_{2m}(\overline{\mathbb{F}}_p)$ and γ is the Steinberg endomorphism described in Example 2.8. Then S provides a bijection between the set of conjugacy classes of $\mathrm{SO}^-_{2m}(q^b) \rtimes \langle\gamma\rangle$ in the coset $\mathrm{SO}^-_{2m}(q^b)\gamma^i$ and the set of conjugacy classes of $\mathrm{SO}^-_{2m}(q^i)$.

2.3 Generals on finite groups of Lie type

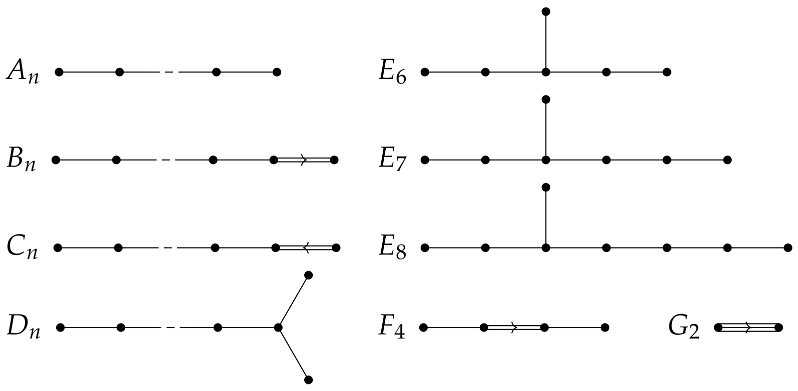
Classical groups and exceptional groups together make up the so-called finite *groups of Lie type*. Following [[Con+03], §§3.1 and 3.2] and [[Men13], §2.3], we shall now give a very short general introduction to this important collection of groups, which will allow us to define the exceptional groups and also to point out the division in untwisted and twisted groups.

By the classification due to Killing and Cartan, simple complex Lie algebras are parametrised by *Dynkin diagrams*, which are denoted:

$$A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4 \text{ or } G_2.$$

These are displayed the following figure.

Figure 2.1: Dynkin diagrams



The subscripts denote the number of nodes in the Dynkin diagram. For each of these diagrams we get a corresponding family of *adjoint Chevalley groups* defined over finite fields $\mathbb{F}_q$: these give us the *untwisted groups of Lie type*, which fall into the following families:

$$A_n(q), B_n(q), C_n(q), D_n(q), E_6(q), E_7(q), E_8(q), F_4(q) \text{ and } G_2(q). \tag{2.5}$$

Steinberg showed that new finite groups could be obtained from the previous ones by considering the fixed points of particular automorphisms (induced by graph automorphisms and Frobenius automorphisms). Elements of the groups $A_n(q^2)$, $D_n(q^2)$,

$D_4(q^3)$ and $E_6(q^2)$ which are fixed by such automorphisms give us the *twisted groups*:

$$^2A_n(q),^2D_n(q),^3D_4(q) \text{ and } ^2E_6(q). \tag{2.6}$$

Other automorphisms only occur over particular fields and give the remaining twisted groups, discovered by Suzuki and Ree:

$$^2B_2(2^{2m+1}) \leq B_2(2^{2m+1}),\ ^2G_2(3^{2m+1}) \leq G_2(3^{2m+1}) \text{ and } ^2F_4(2^{2m+1}) \leq F_4(2^{2m+1}). \tag{2.7}$$

Definition 2.25. The finite *groups of Lie type* are the 16 families of untwisted and twisted groups listed in (2.5), (2.6) and (2.7).

To each group of Lie type we can associate a *Lie rank*. For the untwisted groups, such rank is given by the number of nodes in the Dynkin diagram. On the other hand, twisted Lie groups have both a Lie rank and an *untwisted Lie rank*: the latter is just the Lie rank of the corresponding untwisted group.

The following groups of Lie type are classical groups:

(i) $A_n(q) = \mathrm{PSL}_{n+1}(q)$,

(ii) $^2A_n(q) = \mathrm{PSU}_{n+1}(q)$,

(iii) $B_n(q) = \mathrm{P\Omega}_{2n+1}(q)$,

(iv) $C_n(q) = \mathrm{PSp}_{2n}(q)$,

(v) $D_n(q) = \mathrm{P\Omega}^+_{2n}(q)$,

(vi) $^2D_n(q) = \mathrm{P\Omega}^-_{2n}(q)$.

The remaining groups of Lie type are the exceptional groups: these are all simple, except for

$$^2B_2(2) \cong 5:4,\ G_2(2) \cong \mathrm{PSU}_3(3).2,$$
$$^2G_2(3) \cong \mathrm{PSL}_2(8).3 \text{ and } ^2F_4(2) = {}^2F_4(2)'.2.$$

Remark 2.5. From the list (i)-(vi) of classical groups above we obtain the relation between the untwisted Lie rank and the dimension of the natural module for a classical group.

3

An upper bound for $C(G)$

3.1 Introduction

In this chapter, we consider the case of *invariable generation*, which was firstly introduced in early nineties, with motivation from computational Galois theory, by Dixon [Dix92]. Following his work, we say that a subset $\{g_1, ..., g_t\}$ of a finite group G *invariably generates* G if ${g_1}^{x_1}, \dots, {g_t}^{x_t}$ generate G for every t-tuple $(x_1, \dots, x_t) \in G^t$. Equivalently, following Kowalski and Zywina [KZ12], we say that a subset $\{C_1, \dots, C_t\}$ of conjugacy classes of G invariably generates G if for any choice of representatives $g_i \in C_i$, for $1 \le i \le t$, the elements $g_1, \dots, g_t$ generate G.

Example 3.1 (S_3)**.** Any 2-cycle and any 3-cycle invariably generate S_3. The set $\{(12), (23)\}$ is an example of a generating set for S_3 which is not an invariably generating set.

For every maximal subgroup M of a group G, let $\widetilde{M} = \cup_{g \in G} M^g$ denote the union of the G-conjugates of M. Clearly, $\widetilde{M}_1 = \widetilde{M}_2$ if the maximal subgroups M_1 and M_2 are conjugate in G. Moreover, let $\mathcal{M}$ be a set of representatives of conjugacy classes of maximal subgroups of G. The following lemma is straightforward.

Lemma 3.1. *A subset $\{g_1, \dots, g_t\}$ of a finite group G invariably generates G if and only if $\{g_1, \dots, g_t\} \nsubseteq \widetilde{M}$ for all $M \in \mathcal{M}$.*

If G is a finite group, then a set of representatives for its conjugacy classes always invariably generates the group. This immediately follows from the next lemma.

Lemma 3.2. *If H is a proper subgroup of a finite group G, then there is a conjugacy class of G which is disjoint from H.*

Proof. Let us assume a well-known theorem of Jordan (see [Jor72]), which states that if G is a group acting transitively on a finite set Ω of cardinality at least 2, then there exists

$g \in G$ which acts on Ω without fixed points. Let now G be a finite group, acting by right multiplication on the set $G/H = \{Hg \mid g \in G\}$ of right cosets of H in G. Clearly, this action is transitive and therefore, by Jordan theorem, there exists $g \in G$ which acts on G/H without fixed points. We claim that the conjugacy class of g has empty intersection with H. Indeed, if $g^G \cap H \neq \emptyset$, then there exists $x \in G$ such that $xgx^{-1} \in H$, and therefore $Hxg = Hx$, contradicting the hypothesis on the element g. □

Remark 3.1 ([KLS11])**.** The "only if" part of Lemma 3.1 also holds for infinite groups. Moreover, note that $Y \subseteq G$ generates an arbitrary group G invariably only if $Y \nsubseteq \widetilde{H}$ for all $H < G$. As pointed out in [KLS11], this observation allows us to show that some infinite groups are not invariably generated by any set of elements. For example, Higman, B.H. Neumann and H. Neumann [HNN49] showed that there are countable groups G all of whose non-trivial elements are conjugate, so that $\widetilde{H} = G$ for every non-trivial subgroup H and therefore not even G itself generates G invariably.

However, for finite groups we do not have this kind of anomalies, since $\widetilde{H} \neq G$ for all proper subgroups H, and, as pointed out in last Lemma 3.2, the cardinality of a minimal invariably generating set is at most equal to the number of conjugacy classes of elements in G.

3.1.1 The Chebotarev invariant

Definition 3.1 (Chebotarev invariant)**.** Let G be a finite group and let $x = (x_n)_{n\in\mathbb{N}}$ be a sequence of independent, uniformly distributed, G-valued random variables. We may define a random variable $\tau_{I,G}$ (a waiting time) by

$$\tau_{I,G} := \min\{n \geq 1 \mid \{x_1, \dots, x_n\} \text{ invariably generates } G\ \} \in [1, +\infty].$$

The *Chebotarev invariant* of G, denoted $C(G)$, is the expectation of this random variable: in other words, it is the expected number of elements of G which have to be drawn at random, with replacement, before a set of invariably generating elements is found.

The Chebotarev invariant was firstly introduced by Kowalski and Zywina in 2012 [KZ12], motivated by its relationship to the Chebotarev Density Theorem: now, we give a rough idea of this.

Motivation from Number Theory

Let K be a Galois extension of $\mathbb{Q}$ with Galois group G and let O_K be the ring of algebraic integers of K.

Let p be a prime ideal in $\mathbb{Z}$. Then, the ideal pO_K has the following unique factorization in O_K (see for example [[Neu99], Chapter I, §8 and §9]):

$$pO_K = \left(\prod_{i=1}^{r} \mathfrak{p}_i\right)^e ,$$

where the $\mathfrak{p}_i$'s are the distinct prime ideals of K above p, i.e. the ideals $\mathfrak{p} \trianglelefteq \mathcal{O}_K$ such that $\mathfrak{p} \cap \mathbb{Z} = p$, and e is called the ramification index of p. If e is not equal to 1, the prime ideal p is called *ramified* in K. Otherwise, the prime ideal p is *unramified* in K.

Let $\mathfrak{p}$ be one of the $\mathfrak{p}_i$'s and let $G_\mathfrak{p}$ be the decomposition group of the ideal $\mathfrak{p}$ over p: this is the stabiliser of $\mathfrak{p}$ in G. Moreover, let $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ and $k(p) = \mathbb{Z}/p$: these are finite fields of p-power order. By basic ramification theory (see for example [[Neu99], §9]), we have a surjective group homomorphism

$$G_\mathfrak{p} \xrightarrow{\pi_\mathfrak{p}} Gal(k(\mathfrak{p})/k(p)),\ g \mapsto \bar{g},$$

and assuming that p is unramified, this homomorphism becomes an isomorphism. For each prime p that is unramified in K, we have a well-defined Frobenius conjugacy class in G, defined in the following way.

The Galois group $Gal(k(\mathfrak{p})/k(p))$ is the finite cyclic group generated by the Frobenius automorphism:

$$x \mapsto x^p.$$

The inverse image of the Frobenius automorphism of $Gal(k(\mathfrak{p})/k(p))$ under $\pi_\mathfrak{p}$ is the *Frobenius element* $\sigma_\mathfrak{p} \in G_\mathfrak{p}$. It can be easily shown that, if $\mathfrak{q}$ is another prime ideal of $\mathcal{O}_K$ above p, then the Frobenius elements $\sigma_\mathfrak{p}$ and $\sigma_\mathfrak{q}$ are conjugated in G and therefore it is natural to consider the conjugacy class of the Frobenius element $\sigma_\mathfrak{p} \in G$, which depends only on the prime p and it is called the *Frobenius class* of p, denoted Frob_p.

For simplicity, we set $\mathrm{Frob}_p = 1$ when p is ramified in K. The *Chebotarev density theorem* (see for example [Neu99], Theorem 13.4) states that

$$\lim_{y\to\infty} \frac{|\{p \leq y \mid \mathrm{Frob}_p = C\}|}{\pi(y)} = \frac{|C|}{|G|}, \tag{3.1}$$

where C is a fixed conjugacy class of G and $\pi(y)$ is the prime-counting function, i.e. the number of primes $p \leq y$. In other words, the Chebotarev density theorem says that, asymptotically, a proportion $|C|/|G|$ of primes has associated Frobenius class equal to C.

Now, fix a real number y large enough that every conjugacy class of G is of the form Frob_p for some $p \leq y$. For each $i \geq 1$, select uniformly and independently a random prime p from the set $\{p \mid p \leq y\}$ and define $C_{p_i,y} = \mathrm{Frob}_p$. We thus have a sequence of independent and identically distributed random variables $(C_{p_i,y})_{i\in\mathbb{N}}$ with values in the set of conjugacy classes of G.

We define the waiting time

$$\tau_{C_y} := \min\{n \geq 1 \mid \{C_{p_1,y}, \dots, C_{p_n,y}\} \text{ invariably generates } G\}.$$

Using the Chebotarev density theorem, one can show that

$$\lim_{y\to\infty} \mathbb{E}[\tau_{C_y}] = C(G). \tag{3.2}$$

Therefore, in this setting, $C(G)$ can be thought of as the expected number of random primes p needed for Frob_p to invariably generate G, and this is the motivation for using the name "Chebotarev invariant".

Proof of (3.2). Let Φ be the set of t-tuples of conjugacy classes which invariably generate G:

$$\Phi := \{(C_1, \dots, C_t) \mid C_1, \dots, C_t \text{ invariably generate } G\}.$$

Then

$$\mathbb{P}(x_1, \dots, x_t \text{ invariably generate } G) = \sum_{(C_1,\dots,C_t)\in\Phi} \mathbb{P}(x_1 \in C_1, \dots, x_t \in C_t)$$
$$= \sum_{(C_1,\dots,C_t)\in\Phi} \frac{|C_1|}{|G|} \cdots \frac{|C_t|}{|G|}.$$

On the other side:

$$\mathbb{P}(C_{p_1,y}, \dots, C_{p_t,y} \text{ inv. gen. } G) = \sum_{(C_1,\dots,C_t)\in\Phi} \mathbb{P}(C_{p_1,y} = C_1, \dots, C_{p_t,y} = C_t)$$
$$= \sum_{(C_1,\dots,C_t)\in\Phi} \frac{|\{p \le y \mid \mathrm{Frob}_p = C_1\}|}{\pi(y)} \cdots \frac{|\{p \le y \mid \mathrm{Frob}_p = C_t\}|}{\pi(y)},$$

and taking the limit for $y \longrightarrow \infty$ in the last expression, using (3.1) we obtain

$$\sum_{(C_1,\dots,C_t)\in\Phi} \frac{|C_1|}{|G|} \cdots \frac{|C_t|}{|G|}.$$

To conclude, recall the fact that, for a real-valued random variable τ:

$$\sum_{t=0}^{\infty} \mathbb{P}(\tau > t) = \sum_{t=0}^{\infty} \sum_{v=t+1}^{\infty} \mathbb{P}(\tau = v) = \sum_{v=1}^{\infty} \sum_{t=0}^{v-1} \mathbb{P}(\tau = v) = \sum_{v=1}^{\infty} v\mathbb{P}(\tau = v).$$

Therefore

$$C(G) = \sum_{t=0}^{\infty} \mathbb{P}(\tau_{I,G} > t) = \sum_{t=0}^{\infty} (1 - \mathbb{P}(x_1, \dots, x_t \text{ inv. gen. } G)), \tag{3.3}$$
$$\mathbb{E}[\tau_{C_y}] = \sum_{t=0}^{\infty} \mathbb{P}(\tau_{C_y} > t)) = \sum_{t=0}^{\infty} (1 - \mathbb{P}(C_{p_1,y}, \dots, C_{p_t,y} \text{ inv. gen. } G)).$$

The limit in (3.2) follows. □

Comparing invariants

Given a finite group G, one may ask how differently $e_1(G)$ and $C(G)$ behave: clearly we have $e_1(G) \le C(G)$ and, if G is abelian, $C(G) = e_1(G)$. Moreover, Kantor, Lubotzky and Shalev [KLS11] showed that a finite group is nilpotent if and only if every generating set is an invariable generating set, and therefore $C(G) = e_1(G)$ also whenever G is a finite nilpotent group. But the difference $C(G) - e_1(G)$ is not small in general. For example, Kowalski and Zywina have proved the following.

Proposition 3.3 ([KZ12]). *Let q be a prime power, and consider the affine group $G_q := \mathbb{F}_q \rtimes \mathbb{F}_q^*$. Then $C(G_q) = q - f(q)$, where $f(q) \longrightarrow 0$ as $q \longrightarrow \infty$, and in particular $C(G_q) \sim \sqrt{|G_q|}$ as $q \longrightarrow \infty$.*

On the other side, Lubotzky [Lub03] and, independently, Detomi and Lucchini [DL03] have proved the following estimate, which has settled a conjecture by Pak.

Theorem 3.4 ([Lub03],[DL03]). *Let G be a finite group. Then*

$$e_1(G) = d(G) + O(\log\log|G|) = O(\log|G|).$$

Therefore, comparing Proposition 3.3 and Theorem 3.4, we see that, even in the metabelian case, $C(G)$ and $e_1(G)$ have a quite different behaviour.

To conclude this overview, we remark that the example of Proposition 3.3 led Kowalski and Zywina to conjecture that $C(G) = O(\sqrt{|G|})$ for every finite group G. Progress on the conjecture was first made by Kantor, Lubotzky and Shalev in [KLS11], where it was shown that $C(G) = O(\sqrt{|G|}\log|G|)$, and the conjecture was confirmed by A. Lucchini in [Luc18].

Theorem 3.5 ([Luc18], Theorem 1). *There exists and absolute constant β such that $C(G) \leq \beta\sqrt{|G|}$ whenever G is a finite group.*

Moreover, in [LT17], Lucchini and Tracey showed that $\beta \leq 5/3$ whenever G is soluble, and that this is best possible, with equality if and only if $G = C_2 \times C_2$. Furthermore, in the same paper, they showed that, in general, for each $\epsilon > 0$, there exists a constant c_ϵ such that $C(G) \leq (1+\epsilon)\sqrt{|G|} + c_\epsilon$.

3.1.2 Main result and strategy

Despite in general $C(G)$ can behave wildly differently to $e_1(G)$, the goal of this chapter is to prove that, for a direct product of non-abelian finite simple groups, we can obtain an analogous result to Theorem 1.10 for the Chebotarev invariant. Our main result reads as follows.

Theorem 3.6. *Let $G = T_1 \times T_2 \times \ldots \times T_k$ be a direct product of k non-abelian finite simple groups. Then there exists an absolute constant γ such that $C(G) \leq \gamma \log k$.*

At the end of the chapter (Subsection 3.6.1), we will note, however, that although there is again a logarithmic bound for the case of invariable generation, the difference between the two invariants $C(G)$ and $e_1(G)$ can be arbitrarily large.

Our strategy for proving Theorem 3.6 is the following. As observed in (3.3):

$$C(G) = \sum_{t=0}^{\infty} \mathbb{P}(\tau_{I,G} > t) = \sum_{t=0}^{\infty}(1 - \mathbb{P}_I(G,t)),$$

where $\mathbb{P}_I(G,t)$ denotes the probability that t randomly chosen elements of G invariably generate G. As noted in Lemma 3.1, a subset $\{g_1, \cdots, g_t\}$ fails to invariably generate G if and only if it is contained in $\widetilde{M}$, for some maximal subgroup $M \in \mathcal{M}$. Hence,

$$1 - \mathbb{P}_I(G,t) \leq \sum_{M \in \mathcal{M}} \left(\frac{|\widetilde{M}|}{|G|} \right)^t .$$

For a non-negative integer n, let $\widetilde{m}_n(G)$ denote the number of conjugacy classes of maximal subgroups M of G satisfying $\lfloor |G|/|\widetilde{M}| \rfloor = n$. Our strategy for proving Theorem 3.6 is to prove that $\widetilde{m}_n(G)$ is polynomial in n whenever G is a non-abelian finite simple group. Our claim is trivial for sporadic groups, so we need only prove that $\widetilde{m}_n(G)$ has a polynomial bound in n when G is an alternating, classical or exceptional simple group.

We start by dealing with the alternating case.

3.2 Almost simple groups with alternating socle

Before stating the main result of this section, we require a theorem of Eberhard, Ford and Green [EFG16]. Following their notation, we define the constant

$$\delta := 1 - \frac{1 + \ln \ln 2}{\ln 2} \approx 0.08607.$$

Their result is as follows.

Theorem 3.7 ([EFG16, Theorem 1]). *For positive integers r and k with $1 \leq k \leq r/2$, let $i(r,k)$ denote the proportion of elements of the symmetric group S_r which fix a k-set (set-wise). There are absolute constants D_1 and D_2 such that*

$$D_2 k^{-\delta}(1 + \log k)^{-3/2} \leq i(r,k) \leq D_1 k^{-\delta}(1 + \log k)^{-3/2}.$$

Proposition 3.8. *Let G be an almost simple group with alternating socle. Then there exists an absolute constant C_1 such that $\widetilde{m}_n(G) \leq C_1 n^{1/\delta}$ for all $n \geq 1$.*

Proof. Write $\operatorname{soc}(G) = A_r$. Note first that we have to show that the assertion holds for r big enough, therefore we may assume that $r > 6$, since, for those r, G is equal to A_r or S_r. We will also assume that $G = S_r$, the case $G = A_r$ being similar.

Fix $n \geq 1$, and let $C_{intrans}(G)$ [resp. $C_{imprim}(G)$, $C_{prim}(G)$] be a set of representatives for the G-conjugacy classes of maximal subgroups M of G which are intransitive [resp. imprimitive, primitive], and satisfy $\lfloor |G|/|\widetilde{M}| \rfloor = n$. Moreover, define $C_{trans}(G) := C_{imprim}(G) \cup C_{prim}(G)$. We aim to show that, for all $n \geq 1$:

(i) $|C_{intrans}(G)| \leq c_{intrans} n^{1/\delta}$, for some absolute constant $c_{intrans}$;

(ii) $|C_{trans}(G)| = n^{o(1)}$.

Since $\widetilde{m}_n(G) = |C_{intrans}(G)| + |C_{trans}(G)|$, the result will follow.

We first deal with the intransitive case. If $C_{intrans}(G)$ is empty then the claim is trivial, so assume otherwise. Since, as we have seen in Proposition 2.5, the intransitive maximal subgroups of G are of the form $S_k \times S_l$, with $k + l = r$ and $k \neq l$, we may write $C_{intrans}(G) = \{M_{k_1}, M_{k_2}, \ldots, M_{k_s}\}$, where the k_i's are distinct integers, $1 \leq k_i < r/2$ and each $M_{k_i} \cong S_{k_i} \times S_{r-k_i}$ fixes a k_i-set (set-wise). Assume also that $k_1 < k_2 < \ldots < k_s$. In this way, $|C_{intrans}(G)| \leq k_s$.

Note that $\pi \in G$ fixes a k_i-set if and only if π belongs to some subgroup of the form $S_{k_i} \times S_{r-k_i}$, that is $\pi \in \widetilde{M}_{k_i}$. Therefore, the proportion $i(r, k_i)$ of elements of G fixing a k_i-set is equal to $|\widetilde{M}_{k_i}|/|G|$.

By Theorem 3.7, there exists an absolute constant D_1' such that

$$D_1' k_s^{\delta}(1 + \log k_s)^{3/2} \leq |G|/|\widetilde{M}_{k_s}|.$$

It follows that $D_1' k_s^{\delta} \leq 2\lfloor |G|/|\widetilde{M}_{k_s}| \rfloor = 2n$, and hence

$$|C_{intrans}(G)| \leq k_s \leq \left(\frac{2}{D_1'}\right)^{1/\delta} n^{1/\delta}.$$

Therefore, we may set $c_{intrans} := \left(2/D_1'\right)^{1/\delta}$.

Now, we consider $C_{trans}(G)$, which again we may assume non-empty. By Proposition 2.5, the imprimitive maximal subgroups of G are of the form $S_k \wr S_l$, where $kl = r$, $k > 1$ and $l > 1$. Therefore, $|C_{imprim}(G)| \leq d(r)$, where $d(r)$ denotes the set of positive integer divisors of r. Also, as stated in Theorem 2.7, S_r has $r^{o(1)}$ conjugacy classes of primitive subgroups, thus $|C_{prim}(G)| \leq r^{o(1)}$. Finally, by Theorem 2.8, $n \geq r^{\alpha}$ for some $\alpha > 0$. Since it is well known that $d(r) = r^{o(1)}$ (see the Appendix, Proposition A.1 for a proof), we have $|C_{trans}(G)| = n^{o(1)}$, and in particular there exists an absolute constant c_{trans} such that $|C_{trans}(G)| \leq c_{trans} n^{1/\delta}$ for all $n \geq 1$. The result follows by taking $C_1 := c_{intrans} + c_{trans}$. □

3.3 Classical simple groups

In order to prove the main result of this section, we will need the following preliminary Lemma 3.9. The proof of this lemma relies on a series of papers by Fulman and Guralnick on *derangements* (fixed-point-free elements in a transitive group), in which they proved that the proportion of such elements is bounded away from zero for any simple transitive group, confirming a conjecture of Boston and Shalev. Fulman and Guralnick's main result is stated and used later in this chapter (see Theorem 3.14). Moreover, we will make use of Shintani descent, which we have described in Subsection 2.2.10.

Lemma 3.9. *Let $G = X_r(q)$ be a finite simple classical group of (untwisted) Lie rank r, defined over a field $\mathbb{F}$ of order q, and let m be the dimension of the natural module V for G. Let M be* *a maximal subgroup of G. Then there exist absolute constants C_1, C_2, C_4, B', α and β, and a function $f(r,q)$ which tends to 0 if either r or q is increasing, such that the following holds.*

(i) If M stabilises a k-dimensional subspace of V, with $1 \leq k \leq m/2$, then $\lfloor |G|/|\widetilde{M}| \rfloor \geq C_1 k^{0.005}$.

(ii) If M lies in the Aschbacher class $\mathcal{C}_2$, then $\lfloor |G|/|\widetilde{M}| \rfloor \geq C_2 r^{\alpha}$.

(iii) If M stabilizes an extension field of $\mathbb{F}$ of degree b, for an odd prime b, then $|\widetilde{M}|/|G| \leq 1/b + f(r,q)$, where $f(r,q) := B'(1+\log_q r)/q^{r/2-1}$.

(iv) If M lies in one of the Aschbacher classes $\mathcal{C}_i$ for $4 \leq i \leq 9$, then $\lfloor |G|/|\widetilde{M}| \rfloor \geq C_4 q^{r/3}$.

Proof. Part (i) follows from [FG18, Theorems 2.2, 2.3, 2.4 and 2.5] . More explicitly, from [FG18, Theorem 2.2] we obtain that if $1 \leq k \leq m/2$, then the proportion of elements of $\mathrm{SL}_m(q)$ which fix a k-space is at most $A/k^{0.005}$ for a universal constant A and, if $H \leq \mathrm{SL}_m(q)$ is a maximal subgroup fixing a k-dimensional subspace, such probability is exactly equal to $|\widetilde{H}|/|\mathrm{SL}_m(q)|$. Completely analogous results for the groups $\mathrm{SU}_m(q^{1/2}), \mathrm{Sp}_m(q)$ and $\Omega^{\epsilon}_m(q)$ follow from [FG18], Theorems 2.3, 2.4 and 2.5, respectively. Now, let $Q_m(q) \in \{\mathrm{SL}_m(q), \mathrm{SU}_m(q^{1/2}), \mathrm{Sp}_m(q), \Omega^{\epsilon}_m(q)\}$, and recall that if $G = Q_m(q)/Z(Q_m(q))$ is simple, then the corresponding group $Q_m(q)$ is quasisimple. Let us call $Q = Q_m(q)$ and $Z = Z(Q_m(q))$ for brevity. If M is a maximal subgroup of G fixing a k-dimensional subspace of V, then $M = H/Z$, where H is a maximal subgroup of Q that fixes a k-dimensional subspace of V. To conclude, just observe that

$$\frac{|\widetilde{M}|}{|G|} = \frac{|\bigcup_{g\in G}(H/Z)^g|}{|Q/Z|} = \frac{|\bigcup_{y\in Q}(H^y/Z)|}{|Q/Z|} = \frac{|(\bigcup_{y\in Q} H^y)/Z|}{|Q/Z|} = \frac{|\widetilde{H}|}{|Q|}.$$

Part (ii) follows from [FG18, Theorem 1.4], which asserts that if M is a $\mathcal{C}_2$-subgroup, then $|\widetilde{M}|/|G| \leq A/n^{\delta}$, for some absolute constants A and δ. To conclude, just recall from Remark 2.5 the relation between the (untwisted) Lie rank r and the dimension m of the natural module.

Part (iv) follows from [FG12, Lemmas 7.8, 7.9, 7.10, 7.11 and 7.12]. More explicitly, Lemma 7.8 asserts that if $\mathcal{X}(G)$ denotes the set of maximal subgroups of G contained in $\mathcal{C}_i$, for $3 < i < 8$. Then

$$\frac{\bigcup_{M\in\mathcal{X}(G)} M}{|G|} < O(q^{-r/3}).$$

A completely analogous result for the maximal subgroups of G contained in $\mathcal{C}_9$ follows from Lemmas 7.9, 7.10, 7.11 and 7.12.

Finally, Part (iii) follows by arguing as in the proof of Corollary 5.3 of [FG18]; we repeat the details here for the readers benefit. (Note that our argument fixes a slight imprecision in the use of Shintani descent in [FG18]). Set

$$(H,H_0) := \begin{cases} (\mathrm{GL}_{m/b}(q^b).b, \mathrm{GL}_{m/b}(q^b)), & \text{if } X = \mathbf{L} \\ (\mathrm{GU}_{m/b}(q^{b/2}).b, \mathrm{GU}_{m/b}(q^{b/2})), & \text{if } X = \mathbf{U} \\ (\mathrm{Sp}_{m/b}(q^b).b, \mathrm{Sp}_{m/b}(q^b)), & \text{if } X = \mathbf{S} \\ (\mathrm{SO}^{\epsilon}_{m/b}(q^b).b, \mathrm{SO}^{\epsilon}_{m/b}(q^b)), & \text{if } X = \mathbf{O}^{\epsilon}, \text{with } \epsilon \in \{+,-,\circ\}\,. \end{cases}$$

Recall from Remark 2.5 that $m = r+1$ if $X = \mathbf{L}$ or $X = \mathbf{U}$, $m = 2r$ if $X = \mathbf{S}$ or $X = \mathbf{O}^{\pm}$, and $m = 2r+1$ if $X = \mathbf{O}^{\circ}$.

Let $Y_m(q) \in \{\mathrm{GL}_m(q), \mathrm{GU}_m(q^{1/2}), \mathrm{Sp}_m(q), \mathrm{SO}^{\epsilon}_m(q)\}$ and let $Q_m(q) \in \{\mathrm{SL}_m(q), \mathrm{SU}_m(q^{1/2}), \mathrm{Sp}_m(q), \mathrm{SO}^{\epsilon}_m(q)\}$. Also, let φ be the generator of the cyclic group of order b in the definition of H, and recall that φ induces a generalised q-Frobenius map on H_0, as described in Examples 2.9–2.12.

As showed in the just mentioned examples, by Shintani descent, there is a bijection between H-conjugacy classes in the coset $H_0\varphi^i$ and conjugacy classes in $Y_{m/b}(q^i)$, for each $0 < i < b$, with $i \mid b$. Now, by [FG12, Corollary 1.2], there is a constant c (independent of q and r) such that

$$k(Y_{m/b}(q^i)) \leq cq^{ri/b}.$$

So there are at most $\sum_{i=1}^{\lfloor b/2 \rfloor} cq^{ri/b}$ H-conjugacy classes in $H \setminus H_0$. This number is easily seen to be at most $2cq^{r/2}$. Therefore, there are at most $2cq^{r/2}$ $Y_m(q)$-conjugacy classes of H that intersect $H \setminus H_0$, and these are exactly the conjugacy classes of $Y_m(q)$ that intersect $H \setminus H_0$. By [FG18, Theorem 2.1], there is an absolute constant A such that, for all $y \in Y_m(q)$:

$$|C_{Y_m(q)}(y)| \geq \frac{q^r}{A(1+\log_q r)}. \tag{3.4}$$

This implies that the proportion of elements of $Y_m(q)$ which intersect some conjugate of $H \setminus H_0$ is bounded above by $B(1+\log_q r)/q^{r/2}$ for some universal constant B: indeed if $y_1^{Y_m(q)}, \dots, y_t^{Y_m(q)}$ are the distinct conjugacy classes of $Y_m(q)$ which intersect $H \setminus H_0$, then we have just proved that $t \leq 2cq^{r/2}$, and using (3.4) yields:

$$\begin{aligned} \frac{\bigcup_{i=1}^t |y_i^{Y_m(q)}|}{|Y_m(q)|} &= \frac{\bigcup_{i=1}^t [Y_m(q) : C_{Y_m(q)}(y_i)]}{|Y_m(q)|} = \bigcup_{i=1}^t \frac{1}{|C_{Y_m(q)}(y_i)|} \\ &\leq t\frac{A(1+\log_q r)}{q^r} \leq 2cq^{r/2}\frac{A(1+\log_q r)}{q^r} = \frac{B(1+\log_q r)}{q^{r/2}}, \end{aligned}$$

where we defined $B := 2cA$.

Thus, the proportion of elements of $Q = Q_m(q)$ contained in a conjugate of $H \setminus H_0$ is at most $B'(1+\log_q r)/q^{r/2-1} := f(r,q)$, for an absolute constant B'.

Finally, by the orbit-stabiliser theorem, $|\{H_0^y \mid y \in Q\}| = [Q : N_Q(H_0)]$, and since $[N_Q(H_0) : H_0] = b$, the union of the Q-conjugates of H_0 contains at most $[Q : N_Q(H_0)]|H_0| = |Q|/b$ elements and therefore the proportion of elements of Q contained in a conjugate of H is

$$\frac{|\widetilde{H \cap Q}|}{|Q|} \leq \frac{1}{b} + \frac{B'(1+\log_q r)}{q^{r/2-1}}.$$

We can now conclude in the same way as Part (i).

□

We also require the following lemma.

Lemma 3.10. *Let G be a classical simple group of (untwisted) Lie rank r, defined over a field $\mathbb{F}$ of order q and let m be the dimension of the natural module V for G. Let $\rho_i(G)$ be the number of G-conjugacy classes of maximal subgroups of G in Aschbacher class $\mathcal{C}_i$. Then*

(i) $\rho_1(G) \leq (3/2)m$;

(ii) $\rho_2(G) \leq 2d(m) + 1$, *where $d(m)$ is the number of divisors of m;*

(iii) $\rho_3(G) \leq \pi(m) + 2$, *where $\pi(m)$ is the number of prime divisors of m;*

(iv) $\rho_4(G) \leq 2d(m)$;

(v) $\rho_5(G) \leq \log\log(q)$;

(vi) $\rho_6(G) \leq 1$;

(vii) $\rho_7(G) \leq 3\log m$;

(viii) $\rho_8(G) \leq 4$;

(ix) $\rho_9(G) \leq Br^6$, *for some absolute constant B.*

Proof. The statements $(i) - (viii)$ are [[GKS94], Lemma 2.1], and their proof follows from [[KL90b], Chapter 4]; while part (ix) follows from the proof of [[GLT12], Theorem 6.3]. □

Proposition 3.11. *Let G be a finite simple classical group. Then there exists an absolute constant C such that $\widetilde{m}_n(G) \leq Cn^{200}$ for all $n \geq 1$.*

Proof. Fix a positive integer n, and for each $1 \leq i \leq 9$, let $C_i(G)$ be a set of representatives for the conjugacy classes of maximal subgroups M of G which lie in the Aschbacher class $\mathcal{C}_i$, and satisfy $\lfloor |G|/|\widetilde{M}| \rfloor = n$. Write $G = X_r(q)$, where r is the Lie rank of G, q is the order of the field over which G is defined, and let m be the dimension of the natural module. Similarly to the proof of Proposition 3.8, our strategy will be to prove that for each $1 \leq i \leq 3$, there exists an absolute constant c_i such that $|C_i(G)| \leq c_i n^{200}$; furthermore, we will show that there exists an absolute constant c_4 such that $|\bigcup_{i=4}^{9} C_i(G)| \leq c_4 n^{200}$. The result will then follow by taking $C := c_1 + c_2 + c_3 + c_4$.

If $\mathcal{C}_1(G)$ is non-empty, write $\mathcal{C}_1(G) = \{M_{k_1}, M_{k_2}, \ldots, M_{k_s}\}$, where for each i, we have $1 \leq k_i \leq m/2$, and M_{k_i} fixes a k_i-dimensional subspace of the natural module for G. We may also assume that $k_1 \leq k_2 \leq \ldots \leq k_s$. By [[KL90b], §4.1], for a fixed k_i, there at most 3 distinct conjugacy classes of maximal subgroups which fix a k_i-set. So, $|\mathcal{C}_1(G)| \leq 3k_s \leq 3(n/C_1)^{200}$, where the last inequality follows from Lemma 3.9 Part (i), and therefore we may take $c_1 := 3(1/C_1)^{200}$.

If $\mathcal{C}_2(G)$ is non-empty, then Lemma 3.9 Part (ii) implies that there exist absolute constants C_2 and α such that $n \geq C_2 r^{\alpha}$. Moreover, by Lemma 3.10, $|\mathcal{C}_2(G)| \leq 2d(m) + 1$, where $d(m)$ is the number of divisors of m. As mentioned in the proof of Proposition 3.8, it is well known that $d(m) = m^{o(1)}$. Recalling also the relation between the Lie rank r and the dimension m of the natural module, it follows that $|\mathcal{C}_2(G)| = n^{o(1)}$, and hence that the constant c_2 exists.

Now, we consider $\mathcal{C}_3(G)$, which again we may assume non-empty. Write $\mathcal{C}_3(G) = \{M_{b_1}, M_{b_2}, \ldots, M_{b_t}\}$, where the b_i's are prime divisors of m, and M_{b_i} stabilizes an extension field of $\mathbb{F}$ of degree b_i. Assume also that $b_1 \leq b_2 \leq \ldots \leq b_t$. Now, it follows from Lemma 3.10 that at least $t - 2$ of the b_i are distinct. Hence, $|\mathcal{C}_3(G)| = t \leq b_t + 2$. If $b_t = 2$, then $|\mathcal{C}_3(G)| \leq 4$ and the result is clear, so we may assume that b_t is odd. By Lemma 3.9 Part (iii), there is an absolute constant C_3 such that if $\max\{q, r\} > C_3$, then $B'(1 + \log_q r)/q^{r/2-1} \leq 1/r \leq 3/m \leq 1/b_t$. Hence, if $\max\{q, r\} > C_3$, then $|\mathcal{C}_3(G)| = t \leq b_t + 2 \leq 2b_t \leq 4n$. If $\max\{q, r\} < C_3$, then $\mathcal{C}_3(G) = O(1)$. Either way, the existence of the constant c_3 follows.

Finally, by Lemma 3.9 Part (iv), there exists an absolute constant C_4 such that if $\mathcal{C}_i(G)$ is non-empty for some $4 \leq i \leq 9$, then $n \geq C_4 q^{r/3}$. One can now easily deduce, from the upper bounds $(iv) - (ix)$ in Lemma 3.10, that $|\bigcup_{i=4}^{9} \mathcal{C}_i(G)| = c_4 n^6$, for some absolute constant c_4, and this completes the proof. □

3.4 Exceptional groups of Lie type

Proposition 3.12. *Let G be a simple exceptional group of Lie type. For $n \geq 1$, we have $\widetilde{m}_n(G) = n^{o(1)}$ and $\widetilde{m}_n(G) = O(n)$.*

Proof. Write $G = {}^{\epsilon}X_r(q)$, where r is the (untwisted) Lie rank of G, and q is the order of the field of definition. By Corollary 4 of [LS04], there exists an absolute constant D such that if a maximal subgroup M of G has order larger than D, then M falls into at most $O(\log\log q)$ conjugacy classes of subgroups of G. Furthermore, the number of conjugacy classes of maximal subgroups M of G satisfying $|M| \leq D$ is $O(1)$, by [LMS05, Theorem 1.2]. Also, it is shown in [FG03] that there exists an absolute constant C such that $|G|/|\widetilde{M}| \geq Cq$ if M is not a maximal subgroup of G which has maximal rank. Finally, the number of conjugacy classes of maximal subgroups of G of maximal rank is $O(1)$, by [LSS92, Main Theorem and Table 5.1]. The proposition follows. □

3.5 A corollary

Before we deduce a key corollary of the results of this section, we require some additional notation: suppose that $G = T \times T$, where T is a non-abelian finite simple group, and fix $\alpha \in \mathrm{Aut}(T)$. Define the subgroup $D_\alpha \leq G$ by

$$D_\alpha := \{(t, t^\alpha) : t \in T\}.$$

Then, it is easy to see that D^α and D^β are conjugate in G if and only if $T\alpha = T\beta$ in $\mathrm{Out}(T) = \mathrm{Aut}(T)/T$. Moreover, D_α is a maximal subgroup of G, as we observed in Chapter 1. Finally, we note that, for a fixed $\alpha \in \mathrm{Aut}(T)$, the size of the G-conjugacy class of $(t, t^\alpha) \in G$ is $[T : C_T(t)]^2$, i.e. the square of the size of the T-conjugacy class of t. Indeed, $(t, t^\alpha)^G = \{(t^{g_1}, t^{\alpha g_2}) \mid g_1, g_2 \in T\}$. Therefore $|(t, t^\alpha)^G| = [T : C_T(t)][T : C_T(t^\alpha)]$, and since $C_T(t^\alpha) = C_T(t)^\alpha$ we obtain the above equality.

We are now ready to prove the afore mentioned corollary.

Corollary 3.13. *Let $G = T_1 \times T_2 \times \ldots \times T_k$ be a direct product of k non-abelian finite simple groups. Then there exists an absolute constant C' such that $\widetilde{m}_n(G) \leq C' k^2 n^{200}$ for all $n \geq 1$.*

Proof. As shown in Chapter 1 (Observation 1.1), the maximal subgroups M of G fall into two categories. We adopt here the following notation:

1. *Product type*: M is of the form $M = M_i \times \hat{T}_i$, where $\hat{T}_i := \prod_{l \neq i} T_l$, $1 \leq i \leq k$, and M_i is a maximal subgroup of T_i.
2. *Diagonal type*: M is of the form $M = D_{i,j,\alpha} \times \hat{T}_{i,j}$, where $\hat{T}_{i,j} := \prod_{l \neq i,j} T_l$, $T_i \cong T_j$, $1 \leq i < j \leq k$, $\alpha \in \mathrm{Aut}(T_i)$ and $D_\alpha \cong D_{i,j,\alpha} \leq T_i \times T_j$.

Now, fix n, and let $C_{prod}(G)$ [resp. $C_{diag}(G)$] be a set of representatives for the maximal subgroups M of G of product [resp. diagonal] type satisfying $\lfloor |G|/|\widetilde{M}| \rfloor = n$. Then $|C_{prod}(G)| \leq C_{prod} k n^{200}$ for some absolute constant C_{prod} follows immediately from Propositions 3.8, 3.11 and 3.12. So we just need to prove that there exists a constant C_{diag} such that $|C_{diag}(G)| \leq C_{diag} k^2 n^{200}$.

Let $M \in C_{diag}(G)$, and let $T := T_i \cong T_j$, and $\alpha \in \mathrm{Aut}\,(T)$ be as in the description of diagonal type subgroups at 2. Then, using the discussion preceding the corollary, we have

$$|C_{diag}(G)| \leq k(k-1)|\,\mathrm{Out}\,(T)|. \tag{3.5}$$

The result then follows when T is an alternating group, since $\mathrm{Out}(T) \leq 4$. So, assume that T is a finite simple group of Lie type, of (untwisted) Lie rank r, and field of definition of order q. Moreover

$$\widetilde{D}_\alpha = \{(t^x, t^{\alpha y}) \mid t, x, y \in T\} = \{(u, u^{x^{-1}\alpha y}) \mid u, x, y \in T\} = \{(u, u^{\alpha z}) \mid u, z \in T\}.$$

Thus

$$|\widetilde{M}| = |\hat{T}_{i,j}||\widetilde{D}_\alpha| = |\hat{T}_{i,j}| \sum_{u \in T} [T : C_T(u^\alpha)] = |\hat{T}_{i,j}| \sum_{u \in T} [T : C_T(u)].$$

Since $|C_T(t)| \geq (q-1)^r$ by [FG03, Lemma 3.4], $|\widetilde{M}| \leq |\hat{T}_{i,j}||T|^2/(q-1)^r = |G|/(q-1)^r$ and $2n = 2\lfloor |G|/|\widetilde{M}| \rfloor \geq |G|/|\widetilde{M}| \geq (q-1)^r$. Since $|\operatorname{Out}(T)| = O(r \log q)$ (see for example [Koh03]), the result now follows from (3.5). □

3.6 Proof of the main result

Before proceeding to the proof of Theorem 3.6, we note the following result of Fulman and Guralnick, which has settled a conjecture of Boston and Shalev.

Theorem 3.14 ([FG18, Theorem 1.1])**.** *Let G be a finite simple group acting faithfully and transitively on a set X of cardinality n. With possibly finitely many exceptions, the proportion of derangements in G is at least 0.016.*

Note that any faithful transitive action of a finite simple group G is isomorphic to the action by right multiplication on the set of right cosets of a subgroup M of G, and the stabiliser of Mg is M^g. Therefore, $\widetilde{M}$ is the set of elements of G having at least one fixed point under this action. Thus, Theorem 3.14 can be rephrased as follows.

Theorem 3.15. *There is an absolute constant $\delta > 1$ such that $|G|/|\widetilde{M}| > \delta$ whenever G is a non-abelian finite simple group and M is a subgroup of G.*

We are finally ready to prove Theorem 3.6.

Proof of Theorem 3.6. By Corollary 3.13, there exist absolute constants c and $\alpha = 200$ such that $\widetilde{m}_n(G) \leq ck^2 n^\alpha$ for all $n \geq 1$. Moreover, by Theorem 3.15, there exists an absolute constant $\delta > 1$ such that $|G|/|\widetilde{M}| > \delta$. Let

$$\beta = \left\lceil \max\left\{ \frac{\log(ck^2)}{\log(\delta)}, \alpha + \log(ck^2) \right\} \right\rceil.$$

Also, let Max$_2$(G) be a set of representatives for the conjugacy classes of those maximal subgroups M of G satisfying $|G|/|\widetilde{M}| < 2$.

Then we have

$$\begin{aligned}
1 - \mathbb{P}_I(G,t) &\leq \sum_{M \in \mathrm{Max}_2(\mathrm{G})} (|\widetilde{M}|/|G|)^t + \sum_{n\geq 2} \widetilde{m}_n(G)/n^t \\
&\leq \frac{ck^2}{\delta^t} + \sum_{n\geq 2} \frac{ck^2 n^\alpha}{n^t} \\
&\leq \frac{\delta^{\log(ck^2)/\log(\delta)}}{\delta^t} + \sum_{n\geq 2} \frac{n^{\alpha+\log(ck^2)}}{n^t} \\
&\leq \frac{\delta^\beta}{\delta^t} + \sum_{n\geq 2} \frac{n^\beta}{n^t} = \frac{1}{\delta^t} + \sum_{n\geq 2} \frac{1}{n^{t-\beta}}.
\end{aligned}$$

Where we used the logarithm identities to obtain:

$$ck^2 = \delta^{\log_\delta(ck^2)} = \delta^{\log(ck^2)/\log(\delta)},$$

$$ck^2n^\alpha = n^{\log_n(ck^2)n^\alpha} = n^{\frac{\log(ck^2)}{log(n)}+\alpha} \leq n^{\log(ck^2)+\alpha}.$$

Thus

$$\begin{aligned} C(G) &= \sum_{t\geq 0}(1-\mathbb{P}_I(G,t)) \\ &\leq \beta+2+\sum_{t\geq\beta+2}(1-\mathbb{P}_I(G,t)) \\ &\leq \beta+2+\sum_{u\geq 2}\frac{1}{\delta^u}+\sum_{u\geq 2}\sum_{n\geq 2}\frac{1}{n^u} \\ &= \beta+2+\frac{1}{\delta(\delta-1)}+\sum_{n\geq 2}\left(\sum_{u\geq 2}\frac{1}{n^u}\right) \\ &= \beta+2+\frac{1}{\delta(\delta-1)}+\sum_{n\geq 2}\frac{1}{n(n-1)} \\ &= \beta+2+\frac{1}{\delta(\delta-1)}+\sum_{n\geq 1}\frac{1}{n(n+1)} \\ &= \beta+\frac{1}{\delta(\delta-1)}+3 = \lceil\alpha+\log(ck^2)\rceil+\frac{1}{\delta(\delta-1)}+3. \end{aligned}$$

We have thus obtained that there is an absolute constant γ such that

$$C(G) \leq \gamma \log k.$$

□

To conclude, we show that the bound obtained for the Chebotarev invariant is best possible, at least when the direct factors are all isomorphic.

Remark 3.2. Let $G = {A_5}^k$ and define

$$M_i = A_5 \times \cdots \times D_{10} \times \cdots \times A_5,$$

where D_{10} occupies position i and D_{10} denotes the dihedral group of order 10. Note that M_i is a maximal subgroup of product type in G.

Let us consider

$$\widetilde{M}_i = \bigcup_{g\in G} M_i^g = A_5 \times \cdots \times \widetilde{D}_{10} \times \cdots \times A_5.$$

Since D_{10} contains an element of order 5 and the 5-Sylow subgroups of A_5 are cyclic of order 5, D_{10} contains a 5-Sylow subgroup, say P_5. Since all the p-Sylow subgroups are conjugate, $\bigcup_{g\in A_5} P_5^g$ contains all the 5-elements of A_5. Therefore, $\bigcup_{g\in A_5} {P_5}^g \subseteq$

$\bigcup_{g\in A_5} {D_{10}}^g$, and thus $\widetilde{D}_{10}$ contains all the 5-elements of A_5. Moreover, the 2-elements are conjugated in A_5, since even cycles always remain conjugated in the alternating group. Thus, since D_{10} contains an element of order 2, $\widetilde{D}_{10}$ also contains all the 2-elements of A_5. We obtained:

$$\widetilde{M}_i = \{(x_1, \cdots, x_k) \in A_5^k \mid x_i \text{ is not a 3-cycle}\}.$$

So, since the 3-cycles in A_5 are 20,

$$\frac{|\widetilde{M}_i|}{|G|} = \frac{40}{60} = \frac{2}{3} := \alpha. \tag{3.6}$$

For, $i_1 < \cdots < i_r$, let us define $\widetilde{M}_{i_1,\dots,i_r} := \bigcap_{j=1}^r \widetilde{M}_{i_j}$. Using (3.6), we have that $\frac{|\widetilde{M}_{i_1,\dots,i_r}|}{|G|} = \alpha^r$. Moreover, let $\Omega_t := \bigcup_{1\le i\le k} \widetilde{M}_i^t$. Using the inclusion-exclusion principle and the fact that a subset $\{g_1, \dots, g_t\}$ fails to invariably generate G if and only if it is contained in $\widetilde{M}$ for some maximal subgroup M of G, we have

$$\begin{aligned}
&1 - \mathbb{P}_I(G,t) \ge \frac{|\Omega_t|}{|G|^t} = \\
&= \frac{\sum_i |\widetilde{M}_i|^t - \sum_{i_1<i_2} |\widetilde{M}_{i_1,i_2}|^t + \cdots + (-1)^{k+1} \sum_{i_1<\cdots<i_k} |\widetilde{M}_{i_1,\dots,i_k}|^t}{|G|^t} \\
&= k\alpha^t - \binom{k}{2}\alpha^{2t} + \cdots + (-1)^{k+1}\binom{k}{k}\alpha^{kt} = 1 - \sum_{j=0}^{t} \binom{k}{j}(-\alpha^t)^j \\
&= 1 - (1-\alpha^t)^k.
\end{aligned}$$

Therefore,

$$C(G) = \sum_{t=0}^{\infty} 1 - \mathbb{P}_I(G,t) \ge \sum_{t=0}^{\infty} 1 - (1-\alpha^t)^k.$$

To conclude, we show that

$$\sum_{t=0}^{\infty} 1 - (1-\alpha^t)^k \ge \left(1 - \frac{1}{e}\right) \log_{1/\alpha} k.$$

Observe that $1 - (1-\alpha^x)^k$ is a decreasing function for $x \ge 0$. Therefore

$$\begin{aligned}
\sum_{n=0}^{\infty} 1 - (1-\alpha^n)^k &\ge \sum_{n \le \log_\alpha 1/k} 1 - (1-\alpha^n)^k \\
&\ge \sum_{n \le \log_\alpha 1/k} 1 - (1-\alpha^{\log_\alpha 1/k})^k
\end{aligned}$$

$$= \sum_{n \leq \log_\alpha 1/k} 1 - \left(1 - \frac{1}{k}\right)^k$$

$$= \log_{1/a} k \left(1 - \left(1 - \frac{1}{k}\right)^k\right) \geq \log_{1/a} k \left(1 - \frac{1}{e}\right),$$

where, to obtain the last inequality, we simply used the fact that $(1 - 1/k)^k \leq 1/e$ for all $k \geq 1$.

3.6.1 A final remark

Although we proved that both $C(G)$ and $e_1(G)$ are $O(\log k)$, one may ask if the difference $C(G) - e_1(G)$ can be arbitrarily large, when G is a direct product of non-abelian finite simple groups. The answer is affirmative and we can get it by comparing the results for A_5^k obtained in Remarks 1.3 and 3.2. We have that:

- $e_1(A_5^k) = \frac{\log k}{\log 5} + c(k)$, where $-3 \leq c(k) \leq 5$;
- $C(A_5^k) \geq \frac{\log k}{\log 3/2} \left(1 - \frac{1}{e}\right)$.

Therefore,

$$C(A_5^k) - e_1(A_5^k) \geq \log k \left(\frac{1}{\log 3/2}\left(1 - \frac{1}{e}\right) - \frac{1}{\log 5}\right) - c(k),$$

and since $\frac{1}{\log 3/2}\left(1 - \frac{1}{e}\right) - \frac{1}{\log 5} > 0$, this shows that the difference between the two invariants can be an arbitrarily large number.

This completes the thesis.

A

Appendix

Proposition A.1. *For $n \in \mathbb{N}$, let $d(n)$ be the function counting the number of divisors of n, including 1 and n. Then, for all $\delta > 0$:*

$$d(n) = o(n^{\delta}).$$

This is a very well-known result in number theory. We follow one of the proofs contained in [HW79], (see [[HW79], Theorem 315]). Firstly, we require the following lemma, which corresponds to [[HW79], Theorem 316].

Lemma A.2. *If $f : \mathbb{N} \longrightarrow \mathbb{R}$ is a multiplicative function, and $f(p^m) \longrightarrow 0$ as $p^m \longrightarrow \infty$, then $f(n) \longrightarrow 0$ as $n \longrightarrow \infty$.*

Proof. Given any positive ϵ, we have:

(i) $|f(p^m)| < A$ for all p and m,

(ii) $|f(p^m)| < 1$ if $p > B$,

(iii) $|f(p^m)| < \epsilon$ if $p^m > N(\epsilon)$,

where A and B are independent of p, M and ϵ, and $N(\epsilon)$ depends on ϵ only. If n has prime factorisation $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then $f(n) = f(p_1)^{a_1} f(p_2)^{a_2} \cdots f(p_r)^{a_r}$.

Of the factors $p_1^{a_1}, \ldots, p_r^{a_r}$, at most C are less then or equal to B, where C is independent of n and ϵ. Hence, the product of the corresponding factors $f(p^a)$ is less than A^C, and the rest of the factors of $f(n)$ is less than 1.

The number of integers which can be obtained by multiplication of factors $p^a \leq N(\epsilon)$ is $M(\epsilon)$, and every such number is less than $P(\epsilon)$. Therefore, if $n > P(\epsilon)$, there is at least one factor p^a of n such that $p^a > N(\epsilon)$ and then, by (iii), $|f(p^a)| < \epsilon$. It follows that $|f(n)| < A^C \epsilon$, when $n > P(\epsilon)$, and so that $|f(n)| \rightarrow 0$. □

Proof of Proposition A.1. Take $f(n) = n^{-\delta}d(n)$. Then $f(n)$ is multiplicative and

$$f(p^m) = \frac{m+1}{p^{m\delta}} \leq \frac{2m}{p^{m\delta}} = \frac{2}{p^{m\delta}}\frac{\log p^m}{\log p} \leq \frac{2}{\log 2}\frac{\log p^m}{(p^m)^\delta} \longrightarrow 0,$$

when $p^m \longrightarrow \infty$. Hence, using Lemma A.2, $f(n) \longrightarrow 0$ when $n \longrightarrow \infty$, and thus $d(n) = o(n^\delta)$ for all $\delta > 0$. □

Bibliography

[Asc84] M. Aschbacher. "On the maximal subgroups of the finite classical groups". In: *Inventiones mathematicae* vol. 76 (1984), pp. 469–514.

[BHR13] J. N. Bray; D. F. Holt, and C. M. Roney-Dougal. *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*. London Math. Soc. Lecture Note Series, vol. 407, Cambridge University Press, 2013.

[BG16] T. Burness and M. Giudici. *Classical groups, Derangements and Primes*. Aust. Math. Soc. Lecture Series, vol. 25, Cambridge University Press, 2016.

[Cam99] P. Cameron. *Permutation Groups*. Cambridge University Press, 1999.

[Cam00] P. J. Cameron. *Notes on Classical Groups*. `https://webspace.maths.qmul.ac.uk/p.j.cameron/class_gps/cg.pdf`. 2000.

[Con+03] J. H. Conway et al. *ATLAS of Finite Groups*. Oxford University Press, 2003.

[DL03] E. Detomi and A. Lucchini. "Crowns and factorization of the probabilistic zeta function of a finite group". In: *Journal of Algebra* vol. 2, no. 265 (2003).

[Dix92] J. D. Dixon. "Random sets which invariably generate the symmetric group". In: *Discrete Math.* vol. 105 (1992), pp. 25–39.

[EFG16] S. Eberhard; K. Ford, and B. Green. "Permutations fixing a k-set". In: *Int. Math. Res. Notices IMRN* vol. 2016, no. 21 (2016), pp. 6713–6731.

[FG12] J. Fulman and R. M. Guralnick. "Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements". In: *Trans. Am. Math. Soc.* vol. 364, no. 6 (2012), pp. 3023–3070.

[FG18] J. Fulman and R. M. Guralnick. "Derangements in finite classical groups for actions related to extension field and imprimitive subgroups and the solution of the Boston-Shalev conjecture". In: *Trans. Am. Math. Soc.* vol. 370, no. 7 (2018), pp. 4601–4622.

[FG03] J. Fulman and R. M. Guralnick. "Derangements in simple and primitive groups". In: *Groups, Combinatorics and Geometry: Proc. Symp., Durham, 2001*. World Sci., River Edge, NJ, 2003, pp. 99–121.

[Gar21] M. Garonzi. "The maximal subgroups of the symmetric group". In: *Ensaios Matemáticos* vol. 36 (2021), pp. 1–51.

[GLS98] D. Gorenstein; R. Lyons, and R. Solomon. *The Classification of the Finite Simple Groups, Number 3*. Vol. 40. Mathematical Surveys and Monographs, Amer. Math. Soc, 1998.

[Gou89] E. Goursat. “Sur les substitutions orthogonales et les divisions régulières de l’espace”. In: *Annales scientifiques de l’École Normale Supérieure* vol. 6, no. 3 (1889), pp. 9–102.

[GKS94] R. M. Guralnick; W. Kantor, and J. Saxl. “The probability of generating a classical group”. In: *Comm. Algebra* vol. 22, no. 4 (1994), pp. 302–314.

[GLT12] R. M. Guralnick; M. Larsen, and P. H. Tiep. “Representation growth in positive characteristic and conjugacy classes of maximal subgroups”. In: *Duke Math J.* vol. 161, no. 1 (2012), pp. 107–137.

[HW79] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. 5th ed., The Clarendon Press, Oxford University, New York, 1979.

[Har19] S. Harper. “On the spread of classical groups”. PhD thesis. University of Bristol, 2019.

[Har21] S. Harper. *The spread of almost simple classical groups*. Vol. 2286. Lecture Notes in Mathematics, Springer, 2021.

[HNN49] G. Higman; B. H. Neumann, and H. Neumann. “Embedding theorems for groups”. In: *J. Lond. Math. Soc.* vol. 24 (1949), pp. 247–254.

[Jor72] C. Jordan. “Recherches sur les substitutions”. In: *Journal de Mathématiques Pures et Appliquées* vol. 17, no. 2 (1872).

[KL90a] W. M. Kantor and A. Lubotzky. “The probability of generating a finite classical group”. In: *Geometriae Dedicata* vol. 36 (1990), pp. 67–87.

[KLS11] W.M. Kantor; A. Lubotzky, and A. Shalev. “Invariable generation and the Chebotarev invariant of a finite group”. In: *J. Algebra* vol. 1, no. 348 (2011), pp. 302–314.

[KL90b] P. B. Kleidman and M. W. Liebeck. *The Subgroup Structure of the Finite Classical Groups*. London Math. Soc. Lecture Note Series, vol. 129, Cambridge university Press, 1990.

[Koh03] S. Kohl. “A bound on the order of the outer automorphism group of a finite simple group of given order”. https://stefan-kohl.github.io/preprints/outbound.pdf. 2003.

[KZ12] E. Kowalski and D. Zywina. “The Chebotarev invariant of a finite group”. In: *Exp. Math.* vol. 21, no. 1 (2012), pp. 38–56.

[LMS05] M. W. Liebeck; B. Martin, and A. Shalev. “On conjugacy classes of maximal subgroups of finite simple groups, and a related zeta function”. In: *Duke Math. J.* vol. 128, no. 3 (2005), pp. 541–557.

[LPS87] M. W. Liebeck; C. E. Praeger, and J. Saxl. “A classification of the maximal subgroups of the finite alternating and symmetric groups”. In: *J. Algebra* vol. 111 (1987), pp. 365–383.

[LSS92] M. W. Liebeck; J. Saxl, and G. Seitz. “Subgroups of maximal rank in finite exceptional groups of Lie type”. In: *Proc. London Math. Soc.* vol. 65, no. 3 (1992), pp. 297–325.

[LS04] M. W. Liebeck and G. Seitz. “The maximal subgroups of positive dimension in exceptional algebraic groups”. In: *Memoirs of the American Mathematical Society*. Vol. 169. Providence, RI, 2004.

[Lub03] A. Lubotzky. “The expected number of random elements to generate a finite group”. In: *Journal of Algebra* vol. 257, no. 2 (2003), pp. 452–459.

[Luc18] A. Lucchini. “The Chebotarev invariant of a finite group: a conjecture of Kowalski and Zywina”. In: *Proc. Amer. Math. Soc.* vol. 146 (2018), pp. 4549–4562.

[Luc15] A. Lucchini. “The expected number of random elements to generate a finite group”. In: *Monats. Math.* vol. 177, no. 3 (2015).

[LM20] A. Lucchini and M. Moscatiello. “Generation of finite groups and maximal subgroup growth”. In: *Advances in Group Theory and Applications* vol. 9 (2020), pp. 39–49.

[LT17] A. Lucchini and G. Tracey. “An upper bound on the Chebotarev invariant of a finite group”. In: *Israel J. Math.* vol. 219, no. 1 (2017), pp. 449–467.

[LP93] T. Luczak and L. Pyber. “On random generation of the symmetric group”. In: *Combin. Probab. Comput.* vol. 2, no. 4 (1993), pp. 505–512.

[MT11] G. Malle and D. Testerman. *Linear algebraic groups and finite groups of Lie type*. Vol. 133. Cambridge studies in advanced mathematics, 2011.

[Men13] N. E. Menezes. “Random generation and chief length of finite groups”. PhD thesis. University of St Andrews, 2013.

[Neu99] J. Neukirch. *Algebraic Number Theory*. Springer, 1999.

[Pak99] I. Pak. “On probability of generating a finite group”. `https://www.math.ucla.edu/~pak/papers/sim.pdf`. 1999.

[Suz82] M. Suzuki. *Group Theory II*. Springer, Berlin-Heidelberg-New York, 1982.

[Thé97] J. Thévenaz. “Maximal subgroups of direct products”. In: *Journal of Algebra* vol. 198, no. 2 (1997), pp. 352–361.

[Tra20] G. Tracey. “The Chebotarev invariant of a finite group”. Isaac Newton Institute for Mathematical Sciences, January 14th. 2020.

[Wil09] R. A. Wilson. *The Finite Simple Groups*. Springer, 2009.