Transitive Permutation Groups of Prime Degree

Master thesis

presented by

Svenja Fengler

Student ID no. 323771

A thesis submitted in partial fulfillment

of the requirements for the degree

Master of Science in Mathematics

to the

Lehrstuhl D für Mathematik
Faculty of Mathematics, Computer Science and Natural Sciences of Rheinisch-Westfälische Technische Hochschule Aachen

Name of 1^{st} examiner: Prof. Dr. Gerhard Hiß

Name of 2^{nd} examiner: Prof. Dr. Alice Niemeyer

September 2018

Acknowledgements

I would like to express my deep gratitude to Prof. Dr. Gerhard Hiß, my supervisor, for his patient guidance and useful critiques of the present Master thesis. I would also like to thank Dominik Bernhardt for his constant encouragement and several helpful discussions. Finally, my thanks are extended to Jens Brandt who came through the last two years of my studies with me and shared my enthusiasm for algebra.

Contents

Chapter 1

Introduction

The transitive permutation groups of prime degree were widely studied before the classification of the finite simple groups (in the following abbreviated as CFSG) was complete in the 1980s. As there did not exist a uniform method to classify the transitive permutation groups of prime degree, many papers dealt with various approaches to examine the structure of these groups or to find possible generators. Some of the authors used theoretical methods to determine some properties of the groups whereas others computed some of them on computers. Nevertheless, before the CFSG was published, there were many unanswered questions regarding transitive permutation groups of prime degree.

Basically we can distinguish between two types of transitive permutation groups of prime degree. On the one hand we have the solvable groups. They were taken care of by Galois. He proved that each solvable transitive permutation group of prime degree is permutationally equivalent to a subgroup of the affine group, that is the group of all affine transformations of the one-dimensional vector space $\mathbb{F}_p$. Basically, this means that a solvable transitive group of prime degree p acts on the corresponding p elements in the same way as the affine group on the elements of $\mathbb{F}_p$. The affine transformations can be represented as 2×2 matrices which act on the 2-dimensional row vector space over $\mathbb{F}_p$ by right matrix multiplication. This action gives us a better understanding of the group actions of the abstract solvable transitive permutation groups.

On the other hand there are the non-solvable groups whose classification is not as easy as the classification of the solvable transitive permutation groups of prime degree. Throughout this thesis our attention will be directed to these type of groups. After the publication of the CFSG, only four theorems were necessary to classify them. First, Burnside proved that a transitive group of prime degree is either solvable or 2-fold transitive. Further, he found out that 2-fold transitive permutation groups of prime degree are almost simple, meaning they contain a simple non-abelian minimal normal subgroup S and lie in the automorphism group of S. A concrete connection is given by Guralnick. He classified all simple non-abelian groups with a subgroup of prime power index, which leads directly to the non-abelian simple groups S we are looking for.

Now the question arises why the classification of the (non-solvable) transitive permutation groups of prime degree is still of interest for many mathematicians. One could think that all problems which existed before the publication of the CFSG are solved with this theorem. But there is one detail that troubles many mathematicians, that is the length of its proof. The proof of the CFSG contains more than 10.000 pages which makes it quite hard to understand and to work with. Thus the search for an easier way to classify all transitive permutation groups of prime degree without using the CFSG continues.

In this thesis the main goal is the computation of non-solvable transitive permutation groups of prime degree which are proper subgroups of the alternating group of the same degree. For that, we examine the structure of the non-solvable transitive permutation groups G of prime degree as many authors such as Brauer ([3]) and Fryer ([8]) did before. More precisely, using the given properties like transitivity or the fact that the groups are non-solvable we determine generating sets of the groups. We will see that such groups can be generated by three generators a, b, c such that a is a p-cycle, $b \in N_G(\langle a \rangle) \setminus C_G(\langle a \rangle)$ and $c \in N_G(\langle b \rangle) \setminus \langle b \rangle$. As said before, it is our goal to compute the non-solvable transitive permutation groups of prime degree which are proper subgroups of the alternating group of the same degree. In particular, we restrict ourselves to primes $p \leqslant 23$. For the computation, we implement two algorithms: the first computes the generators a and b as described above and the second algorithm determines the desired groups given a and b as input. This method is based on the results of Fryer ([8]) and Parker and Nikolai ([23]) who studied transitive permutation groups of prime degree, where the prime p has a specific form; in particular $p = 2q+1$, where q also is prime. In Fryer's research q is the order of the element b given above. The method we use to find suitable generators is a generalization of the method used by Fryer as we allow q to be composite. Then we obtain more possibilities for the order of the element b, namely all divisors of q.

The present thesis is structured as follows: In Chapter 1, we give a short introduction to permutation groups and some basic terms. Then we prove the theorem of Galois classifying the solvable transitive groups of prime degree. In the next section of this chapter we prove the two theorems of Burnside mentioned above and show how the classification of finite simple groups is related to our matter. For that, we introduce the theorem of Guralnick. After establishing which groups are non-solvable transitive permutation groups of prime degree, we give an explanation of their actions.

The second chapter starts with some useful results which we need proving the main theorem of this chapter which states that each non-solvable transitive permutation group of prime degree contains elements a, b, c as described above. Further we prove some assertions on the cycle structure and order of these elements and their uniqueness up to conjugation. As said before we implement two algorithms in GAP ([10]) to determine the desired groups. A third algorithm is implemented to test whether the resulting groups are maximal in the alternating group of the same degree. The GAP codes can be found in Appendix A. The next sections of the second chapter deal with the verification of the algorithms and the results we obtain using them. At last, we give an alternative way to compute representatives of all conjugacy classes of transitive permutation groups of prime degree up to 13 using the table of marks. Here it is our goal to use the GAP functions provided by the library of table of marks to determine all conjugacy classes of subgroups of the symmetric group of prime degree and then to check whether they are transitive or not. A GAP code for this method can be found in Appendix B.

Chapter 2

Transitive permutation groups of prime degree

In the present chapter we summarize the known results on the classification of transitive permutation groups of prime degree. Basically, we can distinguish between two types of such groups: solvable and non-solvable groups. The solvable transitive permutation groups of prime degree have been classified by Galois (cf. Theorem 2.26), whereas the non-solvable groups can be listed by means of the classification of finite simple groups, which we will abbreviate by CFSG in the following.

Theorem 2.1 (CFSG, [6, Chapter 4, Theorem 4.9]) *A non-abelian finite simple group is one of the following:*

(1) an alternating group A_n, $n \geqslant 5$*;*

(2) a finite group of Lie type;

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

This chapter is structured as follows: First, we give a short introduction on permutation groups in general. Then we list a few useful results on transitive and primitive permutation groups of prime degree. After proving the theorem of Galois treating the solvable permutation groups we show how the CFSG classifies the non-solvable permutation groups. Further, we prove two theorems of Burnside regarding those groups.

We start with the concept of group actions, which is the basis of permutation groups, and some basic terms. Let Ω be a finite set. Introductory, we consider the set of all bijections on Ω. This set forms a group with respect to function compositions, which is called the *symmetric group* on Ω. We denote the symmetric group by S_Ω. For all $n \in \mathbb{N}$ and $\Omega = \{1, \dots, n\}$ we set $S_\Omega := S_n$. The elements of the symmetric group are called *permutations*.

Definition 2.2 Let G be a finite group and let Ω be a finite set.

(1) The group G *acts* on Ω if and only if there exists a map

$$\Omega \times G \to \Omega, \ (\omega, g) \mapsto \omega^g$$

with

(a) $(\omega^g)^h = \omega^{gh}$ for all $\omega \in \Omega, \ g, h \in G$;

(b) $\omega^{\mathrm{id}_G} = \omega$ for all $\omega \in \Omega$.

(2) If G acts on Ω, we call Ω a *G-set*.

(3) If G acts on Ω, there exists a group homorphism $\phi : G \to S_\Omega$. We call ϕ a *permutation representation* of G.

By Definition 2.2, the symmetric group S_Ω acts on the corresponding set Ω. Definition 2.2(3) states that we can define the action of each $g \in G$ on some $\omega \in \Omega$ as an application of the corresponding permutation $\phi(g)$ in S_Ω, hence $\omega^g := \omega^{\phi(g)}$.

Definition 2.3 Let G be a finite group and let Ω be a G-set.

1. For $\omega \in \Omega$ we call $G_\omega := \{g \in G \mid \omega^g = \omega\} \leqslant G$ the *stabilizer* of ω in G.
2. For $\omega \in \Omega$ we call $\omega^G := \{\omega^g \mid g \in G\} \subseteq \Omega$ the *orbit* of ω under the action of G.

The concept of a permutation group was first introduced by Galois. Although many mathematicians in the 18th century gave consideration to the concept of permutations and to what today is known as a group, Galois was the first to use the name *group*. Originally, he used the theory of permutations to understand how the roots of a given polynomial equation relate to each other, which helped him to decide whether a polynomial equation was solvable by radicals. For instance he managed to prove that to decide whether a polynomial equation is solvable or not is equivalent to whether or not the Galois group of the polynomial is solvable.

In the following we give a few basic definitions, including the definition of a transitive permutation group.

Definition 2.4 Let G be a finite group and let Ω be a G-set.

(1) The action of G on Ω is called *faithful* if and only if $\bigcap_{\omega\in\Omega} G_\omega = \{\mathrm{id}_G\}$.

(2) We call G a *permutation group* on Ω if and only if the action of G on Ω is faithful.

(3) The *degree* of a permutation group is the cardinality of Ω.

(4) The action of G on Ω is called *transitive* if and only if $\omega^G = \Omega$ for every $\omega \in \Omega$.

(5) The action of G on Ω is called *regular* if and only if the action of G on Ω is transitive and $G_\omega = \{\mathrm{id}_G\}$ for all $\omega \in \Omega$.

In this thesis we will also say that G is transitive or regular and so on meaning the same as in Definition 2.4.

Remark 2.5 Let G be a finite group and let Ω be a G-set. The action of G on Ω is faithful if and only if the permutation representation $\phi : G \to S_\Omega$ is injective. In particular, the group G is isomorphic to a subgroup of S_Ω.

Definition 2.6 Let G be a permutation group on the finite set Ω.

(1) A subset $\Delta \subseteq \Omega$ is called a *block* if and only if $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$.

(2) Let G be transitive on Ω, then G is called *imprimitive* on Ω if and only if there exists a block Δ with $|\Delta| > 1$ and $\Delta \neq \Omega$. Otherwise, the group G is called *primitive*.

The next property we introduce is a generalization of transitivity: the k-fold transitivity.

Definition 2.7 Let G be a permutation group on a finite set Ω and let k be an integer with $2 \leqslant k \leqslant |\Omega|$. We call G *k-fold transitive* on Ω if and only if for each pair of k-tuples $(a_1, \ldots, a_k), (b_1, \ldots, b_k) \in \Omega^k$ with $a_i \neq b_i$ for all $i \in \{1, \ldots, k\}$, there exists $g \in G$ with $a_i^g = b_i$ for all $i \in \{1, \ldots, k\}$. The group G is called *sharply k-fold transitive* on Ω if and only if the element g is unique; in particular, the above defined action is regular.

Later on, we will see that transitive permutation groups of prime degree, which are not solvable, are 2-fold transitive.

Theorem 2.8 ([16, Kapitel II, Satz 1.9]) *A 2-fold transitive permutation group is primitive.*

A very useful concept is the permutation equivalence of two permutation groups, which we introduce next. Having only an abstract description of a group and its action on a finite set does not always reveal how the group acts on the set. Hence, it is helpful to transfer the group and its action to a permutationally equivalent group of which we might have a better understanding. In the next section, we use the permutation equivalence of solvable transitive permutation groups of prime degree to subgroups of the affine group to understand the action of those groups.

Definition 2.9 Let G be a finite permutation group on a finite set Ω and let H be a finite permutation group on a finite set Δ.

(1) We call G and H (or both actions) *permutationally equivalent* if and only if there exist an invertible map $\epsilon : \Omega \to \Delta$ and an isomorphism $\varphi : G \to H$ such that
$$\epsilon(\omega^g) = \epsilon(\omega)^{\varphi(g)}$$
for all $\omega \in \Omega$ and all $g \in G$.

(2) If $G = H$ and the actions of G on Ω and on Δ are permutationally equivalent with $\varphi = \mathrm{id}$, we call Ω and Δ *isomorphic G-sets*.

Lemma 2.10 *Let $n \in \mathbb{N}$ and let $U, H \leqslant S_n$. If U and H are conjugate in S_n then they are permutationally equivalent on $\Omega := \{1, \ldots, n\}$.*

Proof. Let U be a subgroup of S_n and let H be conjugate to U, i.e. there exists $x \in S_n$ such that $H = x^{-1}Ux$. Then

$$\varphi : U \to H = x^{-1}Ux, \ u \mapsto x^{-1}ux$$

is an isomorphism between U and H. Moreover, the map

$$\alpha : \Omega \to \Omega, \ \omega \mapsto \omega^x$$

is a bijection. Let $\omega \in \Omega$ and let $u \in U$. We obtain

$$\alpha(\omega^u) = (\omega^u)^x = \omega^{ux} = \omega^{xx^{-1}ux} = \alpha(\omega)^{\varphi(u)},$$

hence U and H are permutationally equivalent. □

The next theorem does not require the given group to be a permutation group. Nevertheless it is very useful and finds application almost everywhere in the theory of groups.

Theorem 2.11 (N/C-Theorem, [16, Kapitel I, Satz 4.5]) *Let G be a finite group and let U be a subgroup of G. Then the quotient $N_G(U)/C_G(U)$ is isomorphic to a subgroup of* $\mathrm{Aut}(U)$.

Theorem 2.12 ([16, Kapitel II, Satz 1.3]) *If G is a transitive permutation group of prime degree, then G is primitive.*

Theorem 2.12 states that transitivity is equivalent to primitivity given a permutation group of prime degree.

Theorem 2.13 ([16, Kapitel II, Satz 1.4]) *Let G be a transitive permutation group on Ω with $|\Omega| > 1$ and let $\omega \in \Omega$. Then G is primitive if and only if G_ω is a maximal subgroup of G.*

Galois also introduced the concept of a normal subgroup. The next theorem shows how normal subgroups of transitive, respectively primitive permutation groups act on the corresponding G-set.

Theorem 2.14 ([16, Kapitel II, Satz 1.5]) *Let G be a transitive permutation group on a set Ω and let $N \neq \{\mathrm{id}_G\}$ be a normal subgroup of G. If N is not transitive on Ω, then the orbits of N form a partition of Ω which is* *preserved under the action of G, and where the blocks have the same length. In particular, if G is primitive on Ω then N is transitive on Ω.*

The next two theorems deal with abelian transitive permutation groups. As we see later, the groups we consider have a minimal normal subgroup which is abelian, so both theorems can be applied to the normal subgroups of transitive permutation groups.

Theorem 2.15 ([16, Kapitel I, Satz 5.13]) *If G is an abelian and transitive permutation group, then G is regular.*

Theorem 2.16 ([16, Kapitel II, Satz 3.1]) *Let G be an abelian transitive permutation group on $\Omega = \{1, \ldots, n\}$. Then G is equal to its centralizer $C_{S_n}(G)$ in the symmetric group S_n.*

Another significant result of Galois is the following theorem. We will use it to prove the main result regarding solvable transitive permutation groups of prime degree.

Theorem 2.17 (Galois, [16, Kapitel II, Satz 3.2]) *Let G be a primitive permutation group of degree n on a finite set Ω and let N be a minimal normal subgroup of G. Let $\omega \in \Omega$ be fixed. If N is solvable, then the following statements hold:*

(1) N is regular and elementary abelian. Moreover, the degree of G is a prime power p^m.

(2) G is the semidirect product of N and the stabilizer of ω, i.e. $G = G_\omega N$ and $G_\omega \cap N = \{\mathrm{id}_G\}$.

(3) N is the unique minimal normal subgroup of G.

(4) G_ω does not contain a normal subgroup other than the trivial group.

(5) If G is solvable, then all complements of N are conjugate to each other in G.

The above theorem reveals some useful properties of minimal normal subgroups in primitive permutation groups. The next theorem we introduce gives a restriction on the number of minimal normal subgroups in such groups.

Theorem 2.18 (Baer, [25, Kapitel 4, Satz 4.1]) *Let G be a primitive permutation group. Then one of the following statements holds:*

(1) The group G has a unique minimal normal subgroup N and $N = C_G(N)$ is regular.

(2) The group G has a unique minimal normal subgroup N and $C_G(N)$ is the trivial group.

(3) The group G has exactly two minimal normal subgroups N and M such that $M = C_G(N) \cong N$ and both are regular.

Remark 2.19 Let G be a permutation group on a finite set Ω and let N be a normal subgroup of G such that N is regular on Ω. Then for all $x \in \Omega$ the action of G_x on Ω is permutationally equivalent to the action of G_x on N by conjugation.

Proof. Let $x \in \Omega$ be fixed. As N is regular on Ω, for each $\omega \in \Omega$ there exists a unique $\alpha(\omega) \in N$ such that $x^{\alpha(\omega)} = \omega$. Hence

$$\alpha : \Omega \to N,\ \omega \mapsto \alpha(\omega),$$

is a bijection. Let $g \in G_x$. Then for all $\omega \in \Omega$ we obtain

$$x^{g^{-1}\alpha(\omega)g} = x^{\alpha(\omega)g} = \omega^g,$$

and thus

$$\alpha(\omega^g) = g^{-1}\alpha(\omega)g = \alpha(\omega)^g.$$

Hence the actions of G_x on Ω and on N are permutationally equivalent. $\square$

Finally, we prove the permutation equivalence of the actions of G on a G-set and on a minimal normal subgroup of G.

Lemma 2.20 *Let p be a prime and $m \in \mathbb{N}$. Let G be a primitive permutation group of degree p^m on the finite set Ω and let N be a minimal normal subgroup of G such that N solvable. Let $x \in \Omega$ be fixed. Then $G = G_xN$ is the semidirect product with $G_x \cap N = \{\mathrm{id}_G\}$ and G acts on the normal subgroup N via $n^g = n^{\tilde{g}\tilde{n}} := \tilde{g}^{-1}n\tilde{g}\tilde{n}$, where $\tilde{g} \in G_x$ and $\tilde{n} \in N$. Moreover, the set Ω and the group N are isomorphic G-sets.*

Proof. Let $x \in \Omega$ be fixed. By Theorem 2.17(2), the group G is the semidirect product of N and the stabilizer of x, namely G_x. Let $g = \tilde{g}\tilde{n} \in G$, where $\tilde{g} \in G_x$ and $\tilde{n} \in N$, and let $n \in N$. First, we show that $n^g = n^{\tilde{g}\tilde{n}} := \tilde{g}^{-1}n\tilde{g}\tilde{n}$ is an action. Let $h = \tilde{h}m \in G$, where $\tilde{h} \in G_x$ and $m \in N$. Then we have $gh = \tilde{g}\tilde{n}\tilde{h}m = \tilde{g}\tilde{h}\hat{n}m$, where $\hat{n} \in N$, and therefore

$$(n^g)^h = (\tilde{g}^{-1}n\tilde{g}\tilde{n})^h = \tilde{h}^{-1}\tilde{g}^{-1}n\tilde{g}\tilde{n}\tilde{h}m = (\tilde{g}\tilde{h})^{-1}n\tilde{g}\tilde{h}\hat{n}m = n^{gh}.$$

Further, $n^{\mathrm{id}_G} = \mathrm{id}_G^{-1}n\mathrm{id}_G = n$. Hence, the group G acts on N as defined above.

Assume, that there exists $\mathrm{id}_G \neq g = \tilde{g}\tilde{n} \in G$ such that $n^g = n$ for all $n \in N$. Then

$$n = n^g = \tilde{g}^{-1}n\tilde{g}\tilde{n} \text{ for all } n \in N.$$

For $x \in \Omega$ it follows that

$$x^n = x^{\tilde{g}^{-1}n\tilde{g}\tilde{n}} = x^{n\tilde{g}\tilde{n}}$$

and therefore, $g = \tilde{g}\tilde{n} \in G_{x^n}$ for all $n \in N$. Since N is transitive on Ω, we obtain $g \in G_\omega$ for all $\omega \in \Omega$. Since $\tilde{g} \in G_x$ and $\tilde{g}\tilde{n} \in G_x$, the element $\tilde{n}$ is in G_x as well, contradicting the fact that the intersection of G_x and N is the trivial group. Hence the action of G on N is faithful.

Since N is regular on Ω, for each ω there exists a unique $n \in N$ such that $x^n = \omega$. Then $\alpha : N \to \Omega,\ n \mapsto x^n$ is a bijection. Let $n \in N,\ g = \tilde{g}\tilde{n} \in G$. Then

$$\alpha(n)^g = \alpha(n)^{\tilde{g}\tilde{n}} = x^{n\tilde{g}\tilde{n}} = x^{\tilde{g}\tilde{g}^{-1}n\tilde{g}\tilde{n}} = x^{\tilde{g}^{-1}n\tilde{g}\tilde{n}} = \alpha(n^{\tilde{g}\tilde{n}}) = \alpha(n^g).$$

Thus the actions of G on N and on Ω are permutationally equivalent. □

2.1 The theorem of Galois

After having set the foundations of permutation groups in the previous section it is now our goal to get an understanding of the solvable transitive permutation groups of prime degree. The theorem of Galois states that such groups are permutationally equivalent to subgroups of $\mathrm{Aff}(1, p)$. Therefore the first step is to examine the affine group. It is a subgroup of the so-called general linear group.

Definition 2.21 Let p be a prime and let $q = p^r$, $r \in \mathbb{N}$, be a power of p. Let $\mathbb{F}_q$ be the corresponding Galois field with q elements and let $V := \mathbb{F}_q^m$ denote an m-dimensional vector space over $\mathbb{F}_q$. We call $\mathrm{GL}(V) := \mathrm{Aut}_{\mathbb{F}_q}(V)$ the *general linear group* over $\mathbb{F}_q$. For a suitable basis we also can describe $\mathrm{GL}(V)$ as a matrix group which we denote by $\mathrm{GL}(m, q)$.

Definition 2.22 Let p be a prime, $q = p^r$ for some $r \in \mathbb{N}$. Let $V := \mathbb{F}_q^m$ be the row vector space over the Galois field $\mathbb{F}_q$ of dimension $m \geqslant 1$. Let $A \in \mathrm{GL}(m, q)$ and $b \in V$. The map

$$f_{A,b} : V \to V,\ v.f_{A,b} = vA + b,$$

is called an *affine transformation* on V. Further, we call

$$\mathrm{Aff}(m, q) := \{f_{A,b} \mid A \in \mathrm{GL}(m, q),\ b \in V\} \leqslant S_V$$

the *affine group* on V.

Remark 2.23 The map

$$\vartheta : \mathrm{Aff}(m, q) \to \mathrm{GL}(m + 1, q),\ f_{A,b} \mapsto \begin{pmatrix} A & 0 \\ b & 1 \end{pmatrix},$$

where $A \in \mathrm{GL}(m, q)$ and $b \in V$, is a group monomorphism.

Proof. Let $A_1, A_2 \in \mathrm{GL}(m, q)$ and $b_1, b_2 \in V$. Since

$$\begin{aligned} \vartheta(f_{A_1,b_1} f_{A_2,b_2}) &= \vartheta(f_{A_1A_2,b_1A_2+b_2}) \\ &= \begin{pmatrix} A_1A_2 & 0 \\ b_1A_2 + b_2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} A_1 & 0 \\ b_1 & 1 \end{pmatrix} \begin{pmatrix} A_2 & 0 \\ b_2 & 1 \end{pmatrix} \\ &= \vartheta(f_{A_1,b_1})\vartheta(f_{A_2,b_2}), \end{aligned}$$

we have a group homomorphism of $\mathrm{Aff}(m, q)$ into $\mathrm{GL}(m + 1, q)$. Further, ϑ

is injective, as

$$\ker(\vartheta) = \left\{ f_{A,b} \in \mathrm{Aff}(m,q) \mid \vartheta(f_{A,b}) = \begin{pmatrix} E_m & 0 \\ 0 & 1 \end{pmatrix} \right\} = \{f_{E_m,0}\}$$

In summary, ϑ is a group monomorphism. □

Using ϑ we identify $\mathrm{Aff}(m,q)$ with a subgroup $\mathrm{AGL}(m,q)$ of $\mathrm{GL}(m+1,q)$, which we define as follows:

$$\mathrm{AGL}(m,q) := \left\{ \begin{pmatrix} A & 0 \\ b & 1 \end{pmatrix} \mid A \in \mathrm{GL}(m,q),\ b \in V \right\}.$$

By Remark 2.23 we have an isomorphism

$$\phi : \mathrm{Aff}(1,p) \to \mathrm{AGL}(1,p),\ f_{a,b} \mapsto \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix},$$

where $a \in \mathbb{F}_p^*$ and $b \in \mathbb{F}_p$. The affine group $\mathrm{Aff}(1,p)$ acts on $\mathbb{F}_p$ via affine transformations, whereas the matrix group $\mathrm{AGL}(1,p)$ acts on the elements of $M := \{(x,1) \mid x \in \mathbb{F}_p\}$ by right matrix multiplication. Let

$$\alpha : \mathbb{F}_p \to M,\ x \mapsto (x,1)$$

be the bijective function mapping an element $x \in \mathbb{F}_p$ to the row vector $(x,1) \in M$. Let $x \in \mathbb{F}_p$ and $g = f_{a,b} \in \mathrm{Aff}(1,p)$. Since

$$\alpha(x^g) = \alpha(x.f_{a,b}) = \alpha(xa+b) = (xa+b,1) = (x,1) \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} = \alpha(x)^{\phi(g)},$$

the groups $\mathrm{Aff}(1,p)$ and $\mathrm{AGL}(1,p)$ are permutationally equivalent. Furthermore, the affine group $\mathrm{Aff}(m,q)$ is isomorphic to a semidirect product of $\mathrm{GL}(m,q)$ and V, as the next result shows.

Lemma 2.24 *Let V be a row vector space of dimension m over the Galois field $\mathbb{F}_q$. Further, let*

$$N := \{f_{E_m,b} \mid b \in V\} \leqslant \mathrm{Aff}(m,q),$$

and let

$$K := \{f_{A,0} \mid A \in \mathrm{GL}(m,q)\} \leqslant \mathrm{Aff}(m,q).$$

Then N is a normal subgroup of the affine group $\mathrm{Aff}(m,q)$ *and we have*

$$\mathrm{Aff}(m,q) = K \ltimes N \cong \mathrm{GL}(m,q) \ltimes V.$$

Proof. First, we prove that N is a normal subgroup of the affine group $\mathrm{Aff}(m,q)$. Let $A_2 \in \mathrm{GL}(m,q)$ and $b_1, b_2 \in V$ with the affine transformations $f_{E_m,b_1} \in N$ and $f_{A_2,b_2} \in \mathrm{Aff}(m,q)$. Note, that the inverse of an affine transformation is $f^{-1}_{A_2,b_2} = f_{A_2^{-1},-b_2A_2^{-1}} \in \mathrm{Aff}(m,q)$. We prove that

$$f^{-1}_{A_2,b_2} f_{E_m,b_1} f_{A_2,b_2} = f_{E_m,b_1A_2^{-1}}.$$

Let $v \in V$, then

$$\begin{aligned} ((v.f^{-1}_{A_2,b_2}).f_{E_m,b_1}).f_{A_2,b_2} &= (vA_2 + b_2 + b_1)A_2^{-1} - b_2A_2^{-1} \\ &= v + b_1A_2^{-1} \\ &= v.f_{E_m,b_1A_2^{-1}}. \end{aligned}$$

Therefore N is a normal subgroup of $\mathrm{Aff}(m,q)$.

Let $f_{A_2,0} \in K$ and $f_{E_m,b_1} \in N$. Then $f_{A_2,0}f_{E_m,b_1} = f_{A_2,b_1A_2}$ and thus $KN = \mathrm{Aff}(m,q)$. Moreover, by definition of N and K, the intersection $N \cap K$ is the trivial group $\{\mathrm{id}_{\mathrm{Aff}(m,q)}\}$. In summary, $\mathrm{Aff}(m,q) = K \ltimes N$. The isomorphisms

$$N \to (V,+),\ f_{E_m,b} \mapsto b,$$

and

$$K \to \mathrm{GL}(m,q),\ f_{A,0} \mapsto A,$$

where $b \in V$ and $A \in \mathrm{GL}(m,q)$, yield $\mathrm{Aff}(m,q) \cong \mathrm{GL}(m,q) \ltimes V$. □

Before we get to the main theorem of this section, which is the theorem of Galois, we prove the next theorem, which will be helpful in the proof of the main result.

Theorem 2.25 *Let G be a primitive permutation group of degree p^m on a finite set $\Omega = \{1, \ldots, p^m\}$ such that a minimal normal subgroup $\widetilde{N}$ of G is* *abelian. Let* $\widetilde{H} = G_x$ *for a fixed* $x \in \Omega$ *and further, let* $K, N \leqslant \mathrm{Aff}(m,p)$ *be as in Lemma 2.24. Then* $\widetilde{N}$ *is the unique minimal normal subgroup of* G *and there exist* $H \leqslant K$ *and an isomorphism* $\varphi : G \to U := H \ltimes N \leqslant \mathrm{Aff}(m,p)$ *with* $\varphi(\widetilde{N}) = N$ *and* $\varphi(\widetilde{H}) = H$*. Additionally, the action of* G *on* Ω *and the action of* U *on* $V := \mathbb{F}_p^m$ *are permutationally equivalent.*

Proof. Since $\widetilde{N}$ is abelian, $\widetilde{N}$ is solvable and by Theorem 2.17(3) the unique minimal normal subgroup of G. Moreover, $\widetilde{N}$ is regular on Ω, elementary abelian and $|\widetilde{N}| = p^m$. Further, the group $\widetilde{H}$ acts on $\widetilde{N}$ by conjugation. As $\widetilde{N}$ is regular on Ω, for each $\omega \in \Omega$ there exists a unique $\alpha(\omega) \in \widetilde{N}$ such that $x^{\alpha(\omega)} = \omega$. Then $\alpha : \Omega \to \widetilde{N},\ \omega \mapsto \alpha(\omega)$, is a bijection. Notice that α is defined as in Remark 2.19, and there we already proved that $\alpha(\omega)^h = \alpha(\omega^h)$ for all $h \in \widetilde{H}$. Further, as $\widetilde{N}$ is elementary abelian, by the main theorem of finitely generated abelian groups we have

$$\widetilde{N} \cong C_p \times \cdots \times C_p \cong (\mathbb{F}_p, +) \oplus \cdots \oplus (\mathbb{F}_p, +) \cong (\mathbb{F}_p^m, +) = (V, +).$$

Let

$$\pi : \widetilde{N} \to (V, +),\ n \mapsto n^\pi,$$

denote a group isomorphism of $\widetilde{N}$ and $(V,+)$ and further, let

$$\gamma : \Omega \to V,\ \omega \mapsto \alpha(\omega)^\pi$$

be a map from Ω to V. Since γ is the composition of α and π and both maps are bijective, the map γ is bijective as well. We define an action of G on V by $\gamma(\omega)^g := \gamma(\omega^g)$ for all $\omega \in \Omega$ and all $g \in G$. Recall that we have $\omega = x^{\alpha(\omega)}$ for each $\omega \in \Omega$. Then for $n \in \widetilde{N}$ we obtain

$$\omega^n = (x^{\alpha(\omega)})^n = x^{\alpha(\omega)n}$$

and thus, $\alpha(\omega^n) = \alpha(\omega)n$ and

$$\gamma(\omega)^n = \gamma(\omega^n) = \alpha(\omega^n)^\pi = (\alpha(\omega)n)^\pi = \alpha(\omega)^\pi + n^\pi = \gamma(\omega) + n^\pi \qquad (2.1)$$

for $\omega \in \Omega$ and $n \in \widetilde{N}$.

Let $h \in \widetilde{H}$ be fixed. We prove that the map

$$\phi : (V, +) \to (V, +),\ \gamma(\omega) \mapsto \gamma(\omega)^h$$

is a group automorphism. Let $\omega, \nu \in \Omega$. Then by the definition of the action of G on V and the definition of γ we obtain

$$\begin{aligned}\phi(\gamma(\omega)) + \phi(\gamma(\nu)) &= \gamma(\omega)^h + \gamma(\nu)^h \\ &= \gamma(\omega^h) + \gamma(\nu^h) \\ &= \alpha(\omega^h)^\pi + \alpha(\nu^h)^\pi = (*).\end{aligned}$$

By Remark 2.19 we have

$$\begin{aligned}(*) &= (\alpha(\omega)^h)^\pi + (\alpha(\nu)^h)^\pi \\ &= (\alpha(\omega)^h \alpha(\nu)^h)^\pi \\ &= ((\alpha(\omega)\alpha(\nu))^h)^\pi = (\dagger).\end{aligned}$$

As $\alpha(\omega)\alpha(\nu) \in \widetilde{N}$ we have $\alpha(\omega)\alpha(\nu) = \alpha(\mu)$ for some $\mu \in \Omega$. Thus

$$(\dagger) = (\alpha(\mu)^h)^\pi = (\alpha(\mu^h))^\pi = \gamma(\mu^h) = \gamma(\mu)^h = (\alpha(\mu)^\pi)^h = (\ddagger)$$

and further,

$$\begin{aligned}(\ddagger) &= ((\alpha(\omega)\alpha(\nu))^\pi)^h \\ &= (\alpha(\omega)^\pi + \alpha(\nu)^\pi)^h \\ &= (\gamma(\omega) + \gamma(\nu))^h = \phi(\gamma(\omega) + \gamma(\nu)).\end{aligned}$$

Further, as h is a permutation, the map ϕ is bijective with the inverse map

$$\phi^{-1} : (V, +) \to (V, +),\ \gamma(\omega) \mapsto \gamma(\omega)^{h^{-1}}.$$

Hence ϕ is a group automorphism of $(V, +)$ and therefore lies in $\mathrm{GL}(m, p)$.

Let $\varphi : G \to S_V$ be the permutation representation of the action of G on the vector space V. As

$$\begin{aligned} G_{\gamma(\omega)} &= \{g \in G \mid \gamma(\omega)^g = \gamma(\omega)\} \\ &= \{g \in G \mid \gamma(\omega^g) = \gamma(\omega)\} \\ &= \{g \in G \mid \omega^g = \omega\} = G_\omega \end{aligned}$$

for each $\omega \in \Omega$ and

$$\bigcap_{\gamma(\omega) \in V} G_{\gamma(\omega)} = \bigcap_{\omega \in \Omega} G_\omega = \{\mathrm{id}_G\},$$

the action of G on V is faithful and hence φ is injective. Since ϕ is a group automorphism we obtain $H := \varphi(\widetilde{H}) \leqslant K \cong \mathrm{GL}(V)$. Further, by (2.1), the element $n \in \widetilde{N}$ acts on V as the translation $\gamma(\omega) \mapsto \gamma(\omega) + n^\pi$. Hence we obtain $\varphi(\widetilde{N}) = N$. In summary, φ is an isomorphism of G and $H \ltimes N$ and we obtain the permutation equivalence via the bijective map γ. $\square$

Now we have everything we need to prove the theorem of Galois.

Theorem 2.26 (Galois, [16, Kapitel II, Satz 3.6]) *Let G be a transitive permutation group of prime degree p on the finite set $\Omega = \{1, \dots, p\}$. The following statements are equivalent:*

(1) G contains a unique Sylow p-subgroup.

(2) G is solvable.

(3) G is permutationally equivalent to a subgroup of the affine group $\mathrm{Aff}(1, p)$.

(4) If $g \in G$ stabilizes two different elements of Ω, then $g = \mathrm{id}_G$.

Proof. Let P be a Sylow p-subgroup of G. The group G being transitive on Ω implies that $|\Omega| = p$ divides $|G|$. Additionally, $|G|$ divides $|S_p| = p!$. As p^2 is not a factor of $p!$, the order of P is p. Furthermore, the group P is generated by a p-cycle. In particular, P is regular on Ω. Theorem 2.16 implies that P is equal to its centralizer in the symmetric group S_p. Since G is a subgroup of S_p, the equality also holds in G.
(1) $\Rightarrow$ (2): Let P be the unique Sylow p-subgroup of G. Then P is normal in G, i.e. $G = N_G(P)$. By Theorem 2.11 and the preliminary remark, the

quotient G/P is isomorphic to a subgroup of the automorphism group $\mathrm{Aut}(P)$ of P and since $\mathrm{Aut}(P)$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$, the quotient is cyclic. Hence G is solvable.
$\underline{(2) \Rightarrow (3)}$: Let $\widetilde{N}$ be a minimal normal subgroup of G. Since G is solvable, $\widetilde{N}$ is abelian and the claim follows from Theorem 2.25.
$\underline{(3) \Rightarrow (4)}$: Since G is permutationally equivalent to a subgroup of $\mathrm{Aff}(1,p)$ and $\mathrm{Aff}(1,p)$ is permutationally equivalent to $\mathrm{AGL}(1,p)$, it suffices to prove the claim for the matrix group $\mathrm{AGL}(1,p)$. Assume there exists an element $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \in \mathrm{AGL}(1,p)$ such that

$$(x,1)\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} = (x,1) \text{ and } (y,1)\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} = (y,1)$$

for different $(x,1)$, $(y,1) \in M := \{(z,1) \mid z \in \mathbb{F}_p\}$. Then $xa+b=x$ and $ya+b=y$ and thus $x(1-a)=b=y(1-a)$, implying either $a=1$ and thus $b=0$, which we ruled out, or $x=y$. This contradicts the assumption of $(x,1)$ and $(y,1)$ being different from each other, hence the matrix stabilizes at most one element of M.
$\underline{(4) \Rightarrow (1)}$: We assume that G contains two distinct Sylow p-subgroups P_1 and P_2. Then P_1P_2 is a subset of G. As both Sylow p-subgroups have cardinality p, the intersection of P_1 and P_2 is $\{\mathrm{id}_G\}$. Hence, the cardinality of P_1P_2 is

$$|P_1P_2| = \frac{|P_1||P_2|}{|P_1 \cap P_2|} = p^2.$$

Therefore, $p^2 \leqslant |G|$. Let $H = \{g \in G \mid 1^g = 1\}$ be the stabilizer of 1 in G and let $R = \{g \in G \mid 1^g = 1, 2^g = 2\}$ be the stabilizer of 2 in H. Since we require that no non-trivial permutation of G stabilizes more than one element of Ω, the group R is trivial. We have $|G| = |G:H||H|$. By the orbit stabilizer theorem, the index $|G:H|$ is equal to $|\Omega| = p$. Moreover,

$$|H| = |H_2||2^H| = |R||2^H| = |2^H| \leqslant p-1$$

and thus,

$$p^2 \leqslant |G| \leqslant p(p-1),$$

a contradiction. Hence G contains only one Sylow p-subgroup. $\square$

As Theorem 2.26 states, a solvable transitive permutation group is permutationally equivalent to a subgroup U of $\mathrm{Aff}(1,p)$ and thus it is also permutationally equivalent to its image $A := \phi(U)$ in $\mathrm{AGL}(1,p)$. Let G be a solvable transitive permutation group on $\Omega = \{1,\ldots,p\}$. Let $x \in \Omega$ be fixed and let P be the unique Sylow p-subgroup of G. By Theorem 2.17 and Lemma 2.24, we have $G = G_x \ltimes P \cong F \ltimes \mathbb{F}_p$, where F is a subgroup of $\mathrm{Aut}(\mathbb{F}_p) \cong \mathbb{F}_p^*$. Examining the subgroup structure of F yields the desired subgroup U or its image $\phi(U)$ in $\mathrm{Aff}(1,p)$ respectively $\mathrm{AGL}(1,p)$.

Example 2.27 Let $p = 17$ and let G be the dihedral group D_{34}. Then

$$G = \langle (1,2,\ldots,17),(1,16)(2,15)(3,14)(4,13)(5,12)(6,11)(7,10)(8,9) \rangle$$

is a solvable, transitive permutation group on $\Omega = \{1,\ldots,17\}$ and thus, by Theorem 2.26, the group G is permutationally equivalent to a subgroup U of the affine group $\mathrm{Aff}(1,17)$. We obtain the subgroup U as follows:
The unique Sylow 17-subgroup of G is $C_{17} = \langle (1,2,\ldots,17) \rangle$. Moreover, C_{17} is a minimal normal subgroup of G and thus, by Theorem 2.25, it is isomorphic to the subgroup of translations in $\mathrm{Aff}(1,17)$, which is generated by the affine transformation $f_{1,1} \in \mathrm{Aff}(1,17)$. Further, Theorem 2.17 states that G is the semidirect product of C_{17} and the stabilizer G_x for some fixed $x \in \Omega$. Without loss of generality we set $x = 17$. The cycle $(1,16)(2,15)(3,14)(4,13)(5,12)(6,11)(7,10)(8,9)$ generates G_{17} and has order 2. Hence, $G_{17} \cong C_2$. As G and U are permutationally equivalent, the subgroup of $\mathrm{Aff}(1,17)$, which is isomorphic to G_{17}, stabilizes $\alpha(17) = (17,1)$ and has order 2 as well. It is easy to check that the subgroup of $\mathrm{Aff}(1,17)$ generated by the affine transformation $f_{16,0} \in \mathrm{Aff}(1,17)$ has the desired properties. In summary, we obtain

$$G \cong U := \langle f_{16,0} \rangle \ltimes \langle f_{1,1} \rangle.$$

Transfering both subgroups of $\mathrm{Aff}(1,17)$ to their images in $\mathrm{AGL}(1,17)$ under the isomorphism ϕ, we also get

$$G \cong A := \langle \begin{pmatrix} 16 & 0 \\ 0 & 1 \end{pmatrix} \rangle \ltimes \langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \rangle.$$

2.2 Almost simple groups

In this section we consider the non-solvable transitive permutation groups of prime degree. We first prove that such groups are 2-fold transitive. This result is due to Burnside, but we follow a proof given by Müller. Further, we classify those groups using the theorem of Guralnick (cf. Theorem 2.38).

The following lemma is the foundation of the proof of Burnside's theorem. By $P^{(\ell)}$ we denote the ℓth derivative of a polynomial P, where $\ell \in \{0, \ldots, \deg(P)\}$.

Lemma 2.28 (Müller, [21]) *Let U be a non-empty, proper subset of $\mathbb{F}_p^*$. Let π be a permutation of $\mathbb{F}_p$ such that $i - j \in U$ for $i, j \in \mathbb{F}_p$ implies that $\pi(i) - \pi(j) \in U$. Then there exist $a, b \in \mathbb{F}_p$ such that $\pi(i) = ai + b$ for all $i \in \mathbb{F}_p$.*

Proof. As $i - j \in U$ implies $\pi^k(i) - \pi^k(j) \in U$ for all $k \in \{1, \ldots, |\pi|\}$, where $|\pi|$ denotes the order of π in S_p, we obtain $i - j \in U$ if and only if $\pi(i) - \pi(j) \in U$. Thus, replacing U by its complement in $\mathbb{F}_p^*$ preserves the assumption and therefore, we may and will assume $|U| \leqslant (p-1)/2$. Let $i \in \mathbb{F}_p$ be fixed. For $u \in U$ we have $(i+u)-i \in U$ and thus $\pi(i+u)-\pi(i) \in U$. Since π permutes the elements of $\mathbb{F}_p$, the elements $\pi(i+u) - \pi(i)$ differ for different $u \in U$. We obtain $\{\pi(i+u) - \pi(i) \mid u \in U\} = U$, implying that for $u \in U$ we have

$$\pi(i + u) - \pi(i) = \tilde{u} = \pi(i) + \tilde{u} - \pi(i)$$

for some $\tilde{u} \in U$ and thus, we obtain $\{\pi(i+u) \mid u \in U\} = \{\pi(i) + u \mid u \in U\}$. Moreover, we get

$$\sum_{u \in U} \pi(i + u)^n = \sum_{u \in U} (\pi(i) + u)^n. \tag{2.2}$$

for all $n \in \mathbb{N}$. Regarding the pairs $(j, \pi(j))$, $j \in \{1, \ldots, p-1\}$, as $p-1$ data points, by means of the polynomial interpolation there exists a polynomial $f(X) = \sum_{k=0}^{d} a_k X^k \in \mathbb{F}_p[X]$ of degree $d \leqslant p - 1$ such that $f(j) = \pi(j)$

for all $j \in \mathbb{F}_p^*$. Note that $d \neq 0$, since π is a permutation and therefore bijective. Further, we obtain a system of linear equations in the coefficients $a_k \in \mathbb{F}_p$ from the equation $f(j) = \pi(j)$ inserting $f(j) = \sum_{k=0}^{d} a_k j^k$ for all $j \in \{1, \ldots, p-1\}$. As the data points are all different from each other, the system is uniquely solvable, establishing the uniqueness of f. If $d = 1$ then f is of the form $aX + b$, which is our claim. Hence it suffices to show that $d = 1$. For each $n \in \mathbb{N}$, set

$$A_n(X) := \sum_{u \in U} f(X+u)^n - \sum_{u \in U} (f(X)+u)^n \in \mathbb{F}_p[X].$$

Then by (2.2), we obtain $A_n(i) = 0$ for each $i \in \mathbb{F}_p$. Setting $S(k) = \sum_{u \in U} u^k$ for $k \in \{1, \ldots, n\}$, by the binomial identity we obtain

$$\begin{aligned}
\sum_{u \in U} (f(X+u)^n - f(X)^n) &= \sum_{u \in U} ((f(X)+u)^n - f(X)^n) \\
&= \sum_{u \in U} \left(\sum_{k=1}^{n} \binom{n}{k} f(X)^{n-k} u^k \right) \\
&= \sum_{k=1}^{n} \binom{n}{k} \left(\sum_{u \in U} u^k \right) f(X)^{n-k} \\
&= \sum_{k=1}^{n} \binom{n}{k} S(k) f(X)^{n-k}.
\end{aligned}$$

Now let n be such that $dn \leqslant p-1$. All derivatives $P^{(\ell)}$, $\ell \in \{0, \ldots, \deg(P)\}$, of a polynomial $P \in \mathbb{F}_p[X]$ of degree $\leqslant p-1$ are linearly independent with decreasing degrees. As $f(X)^n$ is a polynomial of degree dn and $dn \leqslant p-1$, the derivatives of $f(X)^n$ generate the vector space of polynomials in $\mathbb{F}_p[X]$ with degree at most dn, that is $\{P(X) \in \mathbb{F}_p[X] \mid \deg(P) \leqslant dn\}$. Hence the monomial X^{dn} can be written as an $\mathbb{F}_p$-linear combination of the derivatives of $f(X)^n$. Thus there exist elements $\alpha_\ell \in \mathbb{F}_p$ with $0 \leqslant \ell \leqslant dn$, such that $X^{dn} = \sum_{\ell=0}^{dn} \alpha_\ell (f(X)^n)^{(\ell)}$. We obtain

$$\sum_{u \in U} ((X+u)^{dn} - X^{dn}) = \sum_{u \in U} \left(\sum_{\ell=0}^{dn} \alpha_\ell (f(X+u)^n)^{(\ell)} - \sum_{\ell=0}^{dn} \alpha_\ell (f(X)^n)^{(\ell)} \right)$$

$$
\begin{aligned}
&= \sum_{\ell=0}^{dn} \alpha_\ell \left(\sum_{u \in U} (f(X+u)^n - f(X)^n) \right)^{(\ell)} \\
&= \sum_{\ell=0}^{dn} \alpha_\ell \left(\sum_{k=1}^{n} \binom{n}{k} S(k) f(X)^{n-k} \right)^{(\ell)} \\
&= \sum_{\ell=0}^{dn} \alpha_\ell \left(\sum_{k=1}^{n} \binom{n}{k} S(k) (f(X)^{n-k})^{(\ell)} \right) \\
&= \sum_{k=1}^{n} S(k) \left(\sum_{\ell=0}^{dn} \alpha_\ell \binom{n}{k} (f(X)^{n-k})^{(\ell)} \right).
\end{aligned}
$$

Note that $\sum_{\ell=0}^{dn} \alpha_\ell \binom{n}{k} (f(X)^{n-k})^{(\ell)}$ has degree at most $(n-k)d$. Let $r \geqslant 1$ be minimal such that $S(r) \neq 0$. Then the degree of

$$
\sum_{u \in U} ((X+u)^{dn} - X^{dn}) = \sum_{k=1}^{n} S(k) \left(\sum_{\ell=0}^{dn} \alpha_\ell \binom{n}{k} (f(X)^{n-k})^{(\ell)} \right)
$$

is at most $d(n-r)$.

Assume that $r \leqslant dn$. As

$$
\begin{aligned}
\sum_{u \in U} ((X+u)^{dn} - X^{dn}) &= \sum_{u \in U} \left(\sum_{k=1}^{dn} \binom{dn}{k} u^k X^{dn-k} \right) \\
&= \sum_{k=1}^{dn} \binom{dn}{k} S(k) X^{dn-k},
\end{aligned}
$$

the coefficient of X^{dn-r} is $\binom{dn}{r} S(r)$. As $S(r) \neq 0$ and $\sum_{u \in U} ((X+u)^{dn} - X^{dn})$ has degree at most $d(n-r)$, we obtain $dn - r \leqslant d(n-r)$ and therefore, $d = 1$.

It remains to consider the case $r - 1 \geqslant dn$. Further, assume that n is maximal such that $dn \leqslant p - 1$. Then we obtain

$$
p - 1 < d(n+1) \leqslant 2dn \leqslant 2(r-1),
$$

in particular, $r > (p-1)/2$. Therefore, we obtain $S(\ell) = 0$ for each $\ell = 1, 2, \ldots, (p-1)/2$. Assume that $U = \{u_1, \ldots, u_k\}$. The corresponding Vandermonde matrix $V := (u_j^{i-1})_{i,j=1,\ldots,k}$ is invertible. Now let M be the matrix $(u_j^i)_{i,j=1,\ldots,k}$. Then, by the multilinearity of the determinant, it follows that

$$\det(M) = \det(M^T) = u_1 \dots u_k \cdot \det(V^T) = u_1 \dots u_k \cdot \det(V) \neq 0,$$

since $0 \notin U$ and $\det(V) \neq 0$. Therefore, M is invertible as well. Note that the sum of the entries of each column j of M is equal to $S(j)$. As $k = |U| \leqslant (p-1)/2$ and $S(j) = 0$ for $j = 1, 2, \dots, (p-1)/2$, we obtain $vM = 0$ for $v = (1, \dots, 1) \in \mathbb{F}_p^k$, contradicting the fact that M is invertible. Thus, $|U| \geqslant (p+1)/2$, again a contradiction. Therefore, the case $r - 1 \geqslant dn$ does not occur and we are done. □

Now we can prove the following theorem.

Theorem 2.29 (Burnside, [5, Chapter XVI, Theorem VII]) *A transitive permutation group G of prime degree p is 2-fold transitive or solvable.*

Proof. Let G be a transitive permutation group of prime degree p. Since $|\Omega| = p$ divides the order of G, there exists an element g of order p. Then g is a p-cycle. Let $P := \langle g \rangle$. As P is abelian, it is solvable and therefore permutationally equivalent to a subgroup U of $\mathrm{Aff}(1, p)$. Then there exist an isomorphism $\varphi : P \to U$ and a bijective map $\alpha : \Omega \to \mathbb{F}_p$ such that $\alpha(\omega^h) = \alpha(\omega)^{\varphi(h)}$ for all $h \in P$. Hence we can assume that g acts on $\mathbb{F}_p$ such that $g(i) = i + 1 \pmod p$ for all $i \in \mathbb{F}_p$. Further, suppose that G is not 2-fold transitive on $\mathbb{F}_p$.

Let $i, j \in \mathbb{F}_p,\ i \neq j$, be fixed. We define

$$U := \{\pi(i) - \pi(j) \mid \pi \in G\} \subseteq \mathbb{F}_p^*.$$

Let $k,\ \ell \in \mathbb{F}_p,\ k \neq \ell$, such that $k - \ell \in U$. Then there exists $\pi \in G$ such that $\pi(i) - \pi(j) = k - \ell$. Moreover, there exists $m \in \{1, \dots, p-1\}$ with

$$g^m(\pi(i)) = \pi(i) + m = k \text{ and } g^m(\pi(j)) = \pi(j) + m = \ell,$$

implying for all $\sigma \in G$ that

$$\sigma(k) - \sigma(\ell) = \sigma(g^m(\pi(i))) - \sigma(g^m(\pi(j))) \in U.$$

As G is not 2-fold transitive on $\mathbb{F}_p$, there exist $k,\ \ell \in \mathbb{F}_p,\ k \neq \ell$, such that $(\pi(i), \pi(j)) \neq (k, \ell)$ for all $\pi \in G$. Assume that $k - \ell \in U$. The same argument as above implies that there exist $\pi \in G$ and $m \in \{1, \ldots, p-1\}$ such that $g^m(\pi(i)) = \pi(i) + m = k$ and $g^m(\pi(j)) = \pi(j) + m = \ell$, a contradiction.

Hence $k - \ell \notin U$ and thus U is a proper subset of $\mathbb{F}_p^*$. By Lemma 2.28 for each $\pi \in G$ there exist $a, b \in \mathbb{F}_p$ with $\pi(i) = ai + b$ for all $i \in \mathbb{F}_p$. Therefore, G is a subgroup of $\mathrm{Aff}(1, p)$ and thus by Theorem 2.26, the group G is solvable. □

Let S be a simple and non-abelian group. Let $a \in S$. Then

$$\gamma_a : S \to S,\ s \mapsto s^a = a^{-1}sa,$$

denotes the conjugation with a. As the map $S \to \mathrm{Inn}(S),\ a \mapsto \gamma_a$, is a surjective group homomorphism with kernel $Z(S)$ we have $\mathrm{Inn}(S) \cong S/Z(S)$. The center $Z(S)$ is a normal subgroup of S. Since S is simple and non-abelian we obtain $Z(S) = \{\mathrm{id}_S\}$ and thus, $S \cong \mathrm{Inn}(S) \leqslant \mathrm{Aut}(S)$. Hence we have an embedding of S into its automorphism group. This leads to the definition of almost simple groups.

Definition 2.30 A finite group G is *almost simple* if there exists a non-abelian simple group S such that $S \leqslant G \leqslant \mathrm{Aut}(S)$.

The next lemma reveals the structure of the centralizer of a non-abelian and simple minimal normal subgroup of a transitive permutation group of prime degree. It will be very useful in the proofs of the following results.

Lemma 2.31 *Let G be a transitive permutation group of prime degree p and let S be a minimal normal subgroup of G such that S is non-abelian and simple. Then $C_G(S) = \{\mathrm{id}_G\}$.*

Proof. Let $s \in C_G(S) \cap S$ and $g \in S$; then $g^{-1}sg = g^{-1}gs = s$, hence $C_G(S) \cap S$ is a normal subgroup of S. As S is a simple group, we have either $C_G(S) \cap S = \{\mathrm{id}_G\}$ or $C_G(S) \cap S = S$. If $C_G(S) \cap S = S$, then S is a subgroup of $C_G(S)$ and thus abelian, which is a contradiction to the fact that S is non-abelian. Therefore $C_G(S) \cap S = \{\mathrm{id}_G\}$.

Moreover, the group $C_G(S)$ is a normal subgroup of $G = N_G(S)$. Let M be a minimal normal subgroup of G such that $M \leqslant C_G(S)$. As G is primitive, the normal subgroup M is transitive on p elements by Theorem 2.14, hence p is a factor of $|M|$. This is a contradiction to $C_G(S) \cap S = \{\mathrm{id}_G\}$, as p is also a divisor of $|S|$. Therefore we have $C_G(S) = \{\mathrm{id}_G\}$. $\square$

Definition 2.32 Let G be a finite group. The product of all minimal normal subgroups of G is called the *socle* of G.

Lemma 2.33 *Let G be an almost simple group, i.e. there exists a non-abelian simple group S such that $S \leqslant G \leqslant \mathrm{Aut}(S)$. Then S is the socle of G.*

Proof. As $S \cong \mathrm{Inn}(S)$ is normal in $\mathrm{Aut}(S)$ and $G \leqslant \mathrm{Aut}(S)$, the group S is a normal subgroup of G as well. Let N be a minimal normal subgroup of G. As $N \cap S$ is a normal subgroup of S and S is simple, we have $S \cap N = S$ or $S \cap N = \{\mathrm{id}_G\}$. If $N \cap S = S$, then $N \leqslant S$. Since N is a minimal normal subgroup of G and thus normal in S as well, we obtain $N = S$ and the claim follows.

Now assume that $N \cap S = \{\mathrm{id}_G\}$. As $n^{-1}s^{-1}ns \in N \cap S$ for some $n \in N$ and $s \in S$, we have $[N, S] \leqslant N \cap S = \{\mathrm{id}_G\}$, where $[N, S]$ denotes the commutator of the subgroups N and S of G. As the commutator is the trivial group, we obtain $N \leqslant C_G(S)$, which contradicts the fact that $C_G(S) = \{\mathrm{id}_G\}$ by Lemma 2.31 and $N \neq \{\mathrm{id}_G\}$. Hence the case $N \cap S = \{\mathrm{id}_G\}$ does not occur. $\square$

Our next goal is to prove that a 2-fold transitive permutation group of prime degree is almost simple. This result implies that every transitive permutation group of prime degree is either solvable or almost simple. In order to verify this assertion we need the concept of characteristically simple groups and some results on this matter.

Definition 2.34 Let $G \neq \{\mathrm{id}_G\}$ be a finite group and let $U \leqslant G$.

(1) The subgroup U is called *characteristic* in G if and only if $U^\alpha = U$ for all $\alpha \in \mathrm{Aut}(G)$.

(2) The group G is called *characteristically simple* if and only if $\{\mathrm{id}_G\}$ and G are the only characteristic subgroups of G.

Theorem 2.35 ([16, Kapitel I, Satz 9.12]) *Let G be a characteristically simple group. Then $G \cong S_1 \times \cdots \times S_k$ with S_1 simple and $S_i \cong S_1$ for all $1 \leqslant i \leqslant k$.*

Remark 2.36 Let G be a finite group and let N be a minimal normal subgroup of G. Then N is characteristically simple.

Finally, we prove Burnside's theorem.

Theorem 2.37 (Burnside, [5, Chapter X, Section 151-154]) *A non-solvable transitive permutation group G of prime degree p is almost simple.*

Proof. Let G be a 2-fold transitive permutation group of prime degree p on a finite set Ω and let $N \neq \{\mathrm{id}_G\}$ be a minimal normal subgroup of G. Theorem 2.8 implies that G is primitive on p elements, hence N is transitive on Ω by Theorem 2.14. Further, N is characteristically simple by Remark 2.36. Thus there exist simple groups $S_1, \ldots, S_k$ such that $N \cong S_1 \times \cdots \times S_k$ and $S_i \cong S_1$ for all $1 \leqslant i \leqslant k$. If N is solvable, then by Theorem 2.17, N is regular and thus $|N| = p$, implying $N = S_1 \cong C_p$. Moreover, N is the unique minimal normal subgroup, hence the unique Sylow p-subgroup of G and therefore, by Theorem 2.26, the group G is solvable, which is a contradition. Hence N is non-solvable. Then S_1 is non-solvable as well, hence it is non-abelian. As N is transitive on Ω, we have $p \mid |N|$; in particular $p \mid |S_1|$. If $k \geqslant 2$, then p^k is a factor of $|N|$, a contradiction to $N \leqslant G \leqslant S_p$. Therefore $k = 1$ and $N = S_1$. Hence G contains a non-abelian simple minimal normal subgroup N.

Now it remains to show that $G \leqslant \mathrm{Aut}(N)$. Lemma 2.31 implies that $C_G(N) = \{\mathrm{id}_G\}$. Therefore we have

$$G = G/\{\mathrm{id}_G\} = N_G(N)/C_G(N) \cong U \leqslant \mathrm{Aut}(N)$$

by Theorem 2.11 and thus, the claim follows.

In conclusion, we have $N \leqslant G \leqslant \mathrm{Aut}(N)$ with N non-abelian and simple; in particular, the group G is almost simple. $\square$

Now the question arises which non-abelian simple groups listed in Theorem 2.1 give rise to non-solvable transitive groups of prime degree. The answer to this question is given by R. M. Guralnick in [12].

Theorem 2.38 (Guralnick, [12]) *Let S be a non-abelian simple group with $H < S$ and $|S : H| = p^a$, p prime. Then one of the following statements holds:*

(1) $S = A_n$ and $H = A_{n-1}$ with $n = p^a$.

(2) $S = \mathrm{PSL}(n, q)$ and H is the stabilizer of a point or a hyperplane of $\mathbb{F}_q^n$. Then $|S : H| = (q^n - 1)/(q - 1) = p^a$. (Note that n also is prime.)

(3) $S = \mathrm{PSL}(2, 11)$ and $H = A_5$.

(4) $S = M_{23}$ and $H = M_{22}$ or $S = M_{11}$ and $H = M_{10}$.

(5) $S = \mathrm{PSU}(4, 2) \cong \mathrm{PSp}(4, 3)$ and H is a parabolic subgroup of S of index 27.

The proof of the above theorem uses the CFSG by distinguishing the cases S being the alternating group, a group of Lie type or a sporadic group. No proof of Guralnick's theorem which does not use the CFSG is known. Hence up until today the CFSG is essential in the classification of transitive permutation groups of prime degree. Considering $a = 1$ in Guralnick's theorem we obtain the desired groups.

Corollary 2.39 *Let G be an almost simple transitive permutation group of prime degree p, in particular, $S \leqslant G \leqslant \mathrm{Aut}(S)$ for some non-abelian simple group S. Then S is one of the following groups:*

(1) $S = A_p$;

(2) $S = \mathrm{PSL}(n, q)$ with $p = (q^n - 1)/(q - 1)$, where n is prime;

(3) $S = \mathrm{PSL}(2, 11)$ with $p = 11$;

(4) $S = M_{11}$ with $p = 11$ or $S = M_{23}$ with $p = 23$.

Proof. Let G be almost simple and let S be non-abelian and simple such that $S \leqslant G \leqslant \mathrm{Aut}(S)$. Further let G be a transitive permutation group of prime degree p on Ω. Let $\omega \in \Omega$ be fixed. We set $H := G_\omega$. Then, by the orbit stabilizer theorem, we have $|G : H| = p$. Further, H is a maximal subgroup of G. Hence $HS = H$ or $HS = G$. Since S is a subgroup of G, the action of

S on Ω is faithful. If $HS = H$ then $S \leqslant H = G_\omega$ and thus every element of S stabilizes ω, a contradiction to S being transitive on Ω, since $\omega^S = \Omega$ by the definition of transitivity. Hence $HS = G$ and the second isomorphism theorem implies

$$p = |G : H| = |HS : H| = |S : S \cap H|.$$

The claim follows by applying Theorem 2.38 to S. □

In the next sections of this chapter we introduce the groups S we just determined in Corollary 2.39 and their actions. Further, for each S we search for almost simple groups with socle S which also are transitive permutation groups of the corresponding degree. With an outlook on to the next chapter, we exclude the alternating groups of prime degree. As they are maximal in the corresponding symmetric groups and the actions of both groups are well-known, we are more interested in the other groups.

2.2.1 The almost simple groups with socle $\mathrm{PSL}(n, q)$

First, we give a definition of the projective special linear group. For that, we recall the definition of the general linear group.

Definition 2.40 Let s be a prime and let $q = s^m,\ m \in \mathbb{N}$, be a power of s. Let $\mathbb{F}_q$ be the corresponding Galois field with q elements and let $V := \mathbb{F}_q^n$ denote an n-dimensional vector space over $\mathbb{F}_q$.

(1) We call $\mathrm{GL}(V) := \mathrm{Aut}_{\mathbb{F}_q}(V)$ the *general linear group* over $\mathbb{F}_q$.

(2) We call $\mathrm{SL}(V) := \{\alpha \in \mathrm{GL}(V) \mid \det(\alpha) = 1\}$ the *special linear group* over $\mathbb{F}_q$.

(3) The *projective special linear group* is defined as

$$\mathrm{PSL}(V) := \mathrm{SL}(V)/Z(\mathrm{SL}(V)),$$

where $Z(\mathrm{SL}(V)) := \mathrm{SL}(V) \cap Z(\mathrm{GL}(V)) = \{\alpha \mathrm{id}_V \mid \alpha \in \mathbb{F}_q^*,\ \alpha^n = 1\}$.

As $\mathrm{GL}(V)$ is the group of all $\mathbb{F}_q$-linear transformations we can describe each element of the groups just defined as a matrix by choosing a suitable basis B. The corresponding matrix group is denoted by $\mathrm{GL}(n,q)$, where q is the number of elements in $\mathbb{F}_q$ and n is the dimension of the corresponding row vector space $V := \mathbb{F}_q^n$. In particular, we have an isomorphism

$$\mathrm{GL}(V) \to \mathrm{GL}(n,q),\ \alpha \mapsto M_B(\alpha),$$

where $M_B(\alpha)$ denotes the representation of α as a matrix with basis B. Analogously we obtain $\mathrm{SL}(n,q) \cong \mathrm{SL}(V)$ and $\mathrm{PSL}(n,q) \cong \mathrm{PSL}(V)$. For a better understanding of the actions of these groups we consider the matrix groups in the following.

Definition 2.41 Let $V := \mathbb{F}_q^n$ be an n-dimensional vector space over the Galois field $\mathbb{F}_q$, where $q = s^m$ is a prime power. We call

$$\mathbb{P}(V) := \{\langle v\rangle \mid 0 \neq v \in V\}$$

the *projective space* of V.

Now we determine the number of elements of the projective space.

Lemma 2.42 *Let $V := \mathbb{F}_q^n$. The number of elements of the projective space $\mathbb{P}(V)$ is $(q^n - 1)/(q - 1)$.*

Proof. The number of elements in $V \setminus \{0\}$ is $q^n - 1$. As each of the one-dimensional subspaces $\langle v\rangle$ of V consists of $q - 1$ non-zero elements, namely the non-zero multiples of v, we obtain $|\mathbb{P}(V)| = (q^n - 1)/(q - 1)$. □

The group $S := \mathrm{SL}(n,q)$ acts on V via right matrix multiplication, hence we can define the action of $\mathrm{SL}(n,q)$ on the set of subspaces of V of a given dimension. In particular, the group S acts on $\mathbb{P}(V)$, which is the set of the one-dimensional subspaces of V. There is a second permutation representation of $\mathrm{SL}(n,q)$ on the $(q^n - 1)/(q - 1)$ hyperplanes of V, that are the $(n - 1)$-dimensional subspaces of V. For $n \geqslant 3$, these two permutation representations of $\mathrm{SL}(n,q)$ are not equivalent, as the next lemma shows.

Lemma 2.43 *Let n and q be as above with $n \geqslant 3$ and $G = \mathrm{PSL}(n,q)$.*

Further, let H be a hyperplane of V and let

$$G_H := \left\{ \begin{pmatrix} A & 0 \\ w & \kappa \end{pmatrix} \mid A \in \mathrm{GL}(n-1,q), w \in \mathbb{F}_q^{n-1}, \kappa = \det(A)^{-1} \right\}$$

be the stabilizer of H in G. Then G_H does not fix any one-dimensional subspace of V.

Proof. Let $0 \neq (v,x) \in V$ with $v \in \mathbb{F}_q^{n-1}$ and $x \in \mathbb{F}_q$. Assume that G_H fixes the one-dimensional subspace generated by (v,x), hence $\langle (v,x) \rangle = \langle (v,x).B \rangle$ for all $B \in G_H$. Thus $(v,x).B = a_B(v,x)$ with $a_B \in \mathbb{F}_q \setminus \{0\}$ for all $B \in G_H$. First, let

$$B_1 := \begin{pmatrix} E_{n-1} & 0 \\ w & 1 \end{pmatrix} \in G_H$$

with $w \neq 0$. Then we have $a_{B_1}(v,x) = (v,x).B_1 = (v + xw, x)$ for some $0 \neq a_{B_1} \in \mathbb{F}_q$. If $a_{B_1} \neq 1$ then we have $x = 0$ and therefore, $v = a_{B_1} v$ which leads to $v = 0$, which is a contradiction to the fact that $(v,x) \neq 0$. Assume now that $a_{B_1} = 1$. Then we obtain $v + xw = v$ and as $w \neq 0$ we have $x = 0$. Let

$$B_2 := \begin{pmatrix} A & 0 \\ z & \kappa \end{pmatrix} \in G_H$$

with $A \neq E_{n-1}$, $\kappa \neq 1$ and $z \neq 0$. Then $a_{B_2}(v,0) = (v,0).B_2 = (v.A, 0)$ and thus $a_{B_2} v = v.A$, implying $A = a_{B_2} E_{n-1}$. Moreover, we have

$$B_2 = \begin{pmatrix} a_{B_2} E_{n-1} & 0 \\ z & (a_{B_2}^{n-1})^{-1} \end{pmatrix}.$$

Hence each element in G_H is of the form of B_1 or B_2, which is a contradiction. In conclusion, the group G_H does not fix any one-dimensional subspace of the vector space V. □

Set $p := (q^n - 1)/(q - 1)$. The next lemma shows that for p prime, the center of $\mathrm{SL}(n,q)$ is the trivial group, hence we obtain the equality of $\mathrm{SL}(n,q)$ and $\mathrm{PSL}(n,q)$.

Lemma 2.44 *Let n and q be as above. For $p = (q^n - 1)/(q - 1)$ prime the following statements hold:*

(1) The number n is prime and not a factor of $q-1$;

(2) $\mathrm{SL}(n,q) = \mathrm{PSL}(n,q)$.

Proof. (1) : Assume that $n = rs$ for $r, s \in \mathbb{N} \setminus \{0\}$. Set $Q := q^r$. Then

$$q^n - 1 = Q^s - 1 = (Q-1)(Q^{s-1} + Q^{s-2} + \cdots + Q + 1).$$

As

$$q^r - 1 = (q-1)(q^{r-1} + q^{r-2} + \cdots + q + 1),$$

we obtain $q - 1 \mid q^r - 1$ and thus

$$q^n - 1 = (q-1)(q^{r-1} + q^{r-2} + \cdots + q + 1)(Q^{s-1} + Q^{s-2} + \cdots + Q + 1),$$

which is a contradiction to $(q^n-1)/(q-1)$ prime. Hence n is prime. Further, as

$$p = (q^n - 1)/(q-1) = 1 + q + q^2 + \cdots + q^{n-1} > q - 1,$$

we have $p \nmid (q-1)$.

Now assume that $n \mid (q-1)$. Then $q \equiv 1 \pmod{n}$, hence

$$p = (q^n - 1)/(q-1) = \sum_{i=0}^{n-1} q^i \equiv \sum_{i=0}^{n-1} 1^i \equiv n \equiv 0 \pmod{n}.$$

As p is prime, we have $p = n$ and thus $p \mid (q-1)$, a contradiction. Thus n can not be a factor of $(q-1)$.

(2) : The order of $Z(\mathrm{SL}(n,q)) = \{aE_n \mid a \in \mathbb{F}_q^*,\ a^n = 1\}$ is $\gcd(n, q-1)$, but as n is prime and does not divide $q-1$, we have $\gcd(n, q-1) = 1$, hence $\mathrm{SL}(n,q) = \mathrm{PSL}(n,q)$. □

Now it is our goal to find all almost simple groups G with socle $\mathrm{PSL}(n,q)$ which are transitive and faithful on p elements. For that, we have to examine the automorphism group of $\mathrm{PSL}(n,q)$, as it is an upper bound for G.

First, we need the concept of a complement.

Definition 2.45 Let G be a finite group and let N be a normal subgroup of G. A subgroup H of G is called a *complement* to N in G if and only if $G = HN$ and $H \cap N = \{\mathrm{id}_G\}$.

The next theorem reveals the structure of $\mathrm{Aut}(\mathrm{PSL}(n,q))$.

Theorem 2.46 (Lucchini et. al., [18, Theorem 1.12]) *Let $q = s^m$ with s prime and $m \in \mathbb{N}$ and let $d = \gcd(n, q-1)$. The group $\mathrm{PSL}(n,q)$ has a complement in $\mathrm{Aut}(\mathrm{PSL}(n,q))$ if and only if $\gcd((q-1)/d, d, m) = 1$.*

For p prime, Lemma 2.44(1) implies that $d = \gcd(n, q-1) = 1$, hence $\gcd((q-1), 1, m) = 1$. Thus $\mathrm{PSL}(n,q)$ has a complement in its automorphism group. The next two theorems give an idea of the structure of this complement.

Theorem 2.47 (Wielandt, [16, Kapitel V, Bemerkung 21.7]) *Let G be a transitive permutation group of prime degree p. The outer automorphism group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is cyclic and its order is a divisor of $p-1$.*

Theorem 2.48 ([27, Chapter 3, Theorem 3.2]) *Let $q = s^m$, where p is prime, $m \in \mathbb{N}$.*

(1) If $n > 2$ then $\mathrm{Out}(\mathrm{PSL}(n,q)) \cong D_{2\gcd(n,q-1)} \times C_m$.

(2) If $n = 2$ then $\mathrm{Out}(\mathrm{PSL}(2,q)) \cong C_{\gcd(2,q-1)} \times C_m$

As each complement of $\mathrm{PSL}(n,q)$ in its automorphism group is isomorphic to the factor group

$$\mathrm{Aut}(\mathrm{PSL}(n,q))/\mathrm{Inn}(\mathrm{PSL}(n,q)) \cong \mathrm{Aut}(\mathrm{PSL}(n,q))/\mathrm{PSL}(n,q),$$

that is the outer automorphism group $\mathrm{Out}(\mathrm{PSL}(n,q))$, Theorem 2.47 implies that $\mathrm{Aut}(\mathrm{PSL}(n,q)) = \mathrm{PSL}(n,q) \rtimes C$, where C is a subgroup of C_{p-1}. Hence each almost simple transitive permutation group G of prime degree p, which satisfies $\mathrm{PSL}(n,q) \leqslant G \leqslant \mathrm{Aut}(\mathrm{PSL}(n,q))$, is a semidirect product of $\mathrm{PSL}(n,q)$ and a subgroup of C.

If $q = s^m$ is not a prime, in particular $m \geqslant 2$, then the automorphism group $\mathrm{Aut}(\mathbb{F}_q)$ is a cyclic group of order m. This follows from the fact that the automorphism group of $\mathbb{F}_q = \mathbb{F}_{s^m}$ is the Galois group of the algebraic field extention $\mathbb{F}_{s^m}/\mathbb{F}_s$, which is generated by the Frobenius homomorphism $\mathbb{F}_q \to \mathbb{F}_q,\ x \mapsto x^s$. The automorphism group $\mathrm{Aut}(\mathbb{F}_q)$ acts on the matrices of $\mathrm{PSL}(n,q)$ via componentwise application. Thus for $\alpha \in \mathrm{Aut}(\mathbb{F}_q)$ and $A \in \mathrm{PSL}(n,q)$ we have $A^\alpha = ((a_{i,j})_{i,j=1,\dots,n})^\alpha := (a_{i,j}^\alpha)_{i,j=1,\dots,n}$.

Lemma 2.49 *Let $V = \mathbb{F}_q^n$ be a row vector space of the Galois field over $q = s^m$ elements. Let C_m denote the automorphism group of $\mathbb{F}_q$. Then the group $G := \mathrm{PSL}(n,q) \rtimes C_{\widetilde{m}}$, where $\widetilde{m}$ is a factor of m, acts transitively and faithfully on the $(q^n-1)/(q-1)$ points of $\mathbb{P}(V)$ via $\langle v\rangle^{A\alpha} := \langle v^{A^\alpha}\rangle$, where $A \in \mathrm{PSL}(n,q)$ and $\alpha \in C_{\widetilde{m}}$.*

Proof. Let $A, B \in \mathrm{PSL}(n,q)$ and $\alpha, \beta \in C_{\widetilde{m}}$. As the matrices A^α and B^β act on the vector space V by right matrix vector multiplication and the size of A^α and B^α is equal, we have $(v.A^\alpha).B^\beta = v.(A^\alpha B^\beta)$ for a vector $v \in V$ and thus, $\langle (v^{A^\alpha})^{B^\beta}\rangle = \langle v^{A^\alpha B^\beta}\rangle$. Further, we have $\langle v^{E_n^{\mathrm{id}_{C_{\widetilde{m}}}}}\rangle = \langle v\rangle$ and therefore, the action of G on $\mathbb{P}(V)$ we defined above is valid.

The group G is transitive on $\mathbb{P}(V)$ as $\mathrm{PSL}(n,q) \leqslant G$ and $\mathrm{PSL}(n,q)$ is transitive on the elements of $\mathbb{P}(V)$.

Assume that there exists an element $g = A\alpha \in G$ such that $\langle v\rangle^{A\alpha} = \langle v\rangle$ for all $\langle v\rangle \in \mathbb{P}(V)$. Then for all $0 \neq v \in V$, we have $\langle v^{A^\alpha}\rangle = \langle v\rangle$ which is equivalent to $v^{A^\alpha} = av$ for some $a \in \mathbb{F}_q$ which depends on the vector v. Then A^α maps each vector of V to one of its multiples and therefore, either $A^\alpha = E_n$ or $A^\alpha = aE_n$ and each $v \in V$ is mapped to av. In the second case we have $A^\alpha = aE_n$ and thus $A^\alpha \in Z(\mathrm{SL}(n,q))$. Further, Lemma 2.44 implies $A^\alpha = E_n$. In conclusion, the action of G on $\mathbb{P}(V)$ is faithful. □

Let G be as in Lemma 2.49. By the next theorem and the fact that the complement of $\mathrm{PSL}(n,q)$ in its automorphism group is abelian imply that $\mathrm{PSL}(n,q)$ is the commutator subgroup of G. As $\mathrm{PSL}(n,q)$ is simple, the group G is non-solvable.

Theorem 2.50 ([16, Kapitel II, Satz 6.10]) *For $n \geqslant 3$ or $n = 2$ and $q > 3$, the commutator group of both* $\mathrm{GL}(n,q)$ *and* $\mathrm{SL}(n,q)$ *is* $\mathrm{SL}(n,q)$.

In summary, the group G is almost simple with socle $\mathrm{PSL}(n,q)$. Finally, we give an example.

Example 2.51 For $q = 16$ and $n = 2$, we have $(q^n-1)/(q-1) = 17$. Let $V := \mathbb{F}_{16}^2$ be a row vector space over the Galois field $\mathbb{F}_{16}$. Then $\mathrm{PSL}(2,16)$ acts transitively on 17 elements by $\langle v\rangle^A = \langle v^A\rangle$ for all $v \in V,\ A \in \mathrm{PSL}(2,16)$. As $q = 16 = 2^4$, we have $s = 2$ and $m = 4$. Hence the automorphism group of $\mathbb{F}_{16}$ is $\mathrm{Aut}(\mathbb{F}_{16}) = C_4$. Further, we have $\mathrm{Aut}(\mathrm{PSL}(2,16)) = \mathrm{PSL}(2,16) \rtimes C_4$

and the almost simple groups $S \leqslant G \leqslant \mathrm{Aut}(S)$ with $S = \mathrm{PSL}(2,16)$ are $\mathrm{PSL}(2,16)$, $\mathrm{PSL}(2,16) \rtimes C_2$ and $\mathrm{PSL}(2,16) \rtimes C_4$.

2.2.2 The almost simple groups with socle PSL(2,11)

In his *Lettre testamentaire* ([9]) to Chavelier, Galois proved that the groups $\mathrm{PSL}(2,q)$ for q prime act transitively on $q+1$ elements. Further, he found out that for $\mathrm{PSL}(2,q)$ to act transitively on less than $q+1$ points, the number q must be an element of the set $\{2,3,5,7,11\}$. In this section we only consider the group $\mathrm{PSL}(2,11)$ as the other cases are taken care of in the previous section.

Note that in this case we have $(q^n-1)/(q-1) = 12$, hence $\mathrm{PSL}(2,11)$ also acts transitively on the points of $\mathbb{P}(\mathbb{F}_{11}^2)$ by the action defined in the previous section. Nevertheless, as 12 is not a prime, this action is not of interest in this section.

As we consider the action of $\mathrm{PSL}(2,11)$ on 11 points, we regard the group as a subgroup of the symmetric group S_{11} and the right notation would be $\mathrm{PSL}(\mathbb{F}_{11}^2)$ as introduced in Definition 2.40, but for the sake of consistency we continue using the notation $\mathrm{PSL}(2,11)$ instead of $\mathrm{PSL}(\mathbb{F}_{11}^2)$.

In this section we we will see that $\mathrm{PSL}(2,11)$ is the automorphism group of a block design. Thus, we start with a short introduction on this notion.

Definition 2.52 Let S be a set with v elements and let $\mathcal{B}$ be a collection of subsets of S such that

(1) $|B| = k$ for every $B \in \mathcal{B}$;

(2) for every $T \subset S$ with $|T| = t$ there are exactly λ subsets $B \in \mathcal{B}$ such that $T \subset B$.

Then the pair $(S, \mathcal{B})$ is called a *t-(v,k,λ)-design*. The elements of S are called the *points* and the elements of $\mathcal{B}$ are called *blocks* of the design.

We will abbreviate the t-(v,k,λ)-design to *block design* if the values of t, v, k and λ are clear from the context.

Definition 2.53 Let D be a t-(v,k,λ)-design and let $|\mathcal{B}| = b$. Then D is *symmetric* if and only if $v = b$.

Definition 2.54 Two t-(v,k,λ)-designs $D=(S,\mathcal{B})$ and $D'=(S',\mathcal{B}')$ with $|S|=|S'|$ are *isomorphic* if and only if there exists a bijective map $\alpha : S \to S'$ such that $\{\{\alpha(x) \mid x \in B\} \mid B \in \mathcal{B}\} = \mathcal{B}'$. If $D=D'$, then α is called an *automorphism.*

Remark 2.55 The automorphisms of any t-(v,k,λ)-design D form a group.

Theorem 2.56 ([14, Chapter 15, Section 15.8.2]) *The group* $\mathrm{PSL}(2,11)$ *is the automorphism group of a* 2-$(11,5,2)$-*design.*

Now we explain the relation between $\mathrm{PSL}(2,11)$ and the 2-$(11,5,2)$-design. With the results given in [19] by Martín and Singerman we can construct a matrix A in GAP from which we can read a set of blocks satisfying the requirements of a 2-$(11,5,2)$-design by looking at the entries containing zero in each row.

Following the instructions given in [19] we obtain the following matrix:

$$A = \begin{pmatrix} 0&1&0&1&1&0&0&0&1&1&1\\ 1&0&1&0&1&1&0&0&1&0&1\\ 1&1&0&1&0&1&1&0&0&0&1\\ 0&1&1&0&1&1&1&0&0&1&0\\ 1&0&1&1&0&0&1&0&1&1&0\\ 0&0&1&1&1&0&1&1&0&0&1\\ 1&1&0&0&1&0&1&1&1&0&0\\ 0&1&1&1&0&1&0&1&1&0&0\\ 0&0&0&0&0&1&1&1&1&1&1\\ 1&1&1&0&0&0&0&1&0&1&1\\ 1&0&0&1&1&1&0&1&0&1&0 \end{pmatrix}.$$

As said before, we can read a set of blocks from the entries containing zero. For example the entries containing zero in the first row of the matrix are $1,3,6,7,8$, giving us the first block of the design. All in all, we obtain the blocks

$$B_1 = \{1,3,6,7,8\},$$
$$B_2 = \{2,4,7,8,10\},$$
$$B_3 = \{3,5,8,9,10\},$$

$$\begin{aligned}
B_4 &= \{1, 4, 8, 9, 11\}, \\
B_5 &= \{2, 5, 6, 8, 11\}, \\
B_6 &= \{1, 2, 6, 9, 10\}, \\
B_7 &= \{3, 4, 6, 10, 11\}, \\
B_8 &= \{1, 5, 7, 10, 11\}, \\
B_9 &= \{1, 2, 3, 4, 5\}, \\
B_{10} &= \{4, 5, 6, 7, 9\}, \\
B_{11} &= \{2, 3, 7, 9, 11\}.
\end{aligned}$$

As we see, for each subset T of S with $|T| = 2$ there exist exactly two blocks containing T. For instance, the set $\{2, 3\}$ is contained in the two blocks B_9 and B_{11}, whereas the set $\{3, 10\}$ occurs in the blocks B_3 and B_7. In conclusion, we have a 2-(v, k, λ)-design $D = (S, \mathcal{B})$ with $S = \{1, \ldots, 11\}$ and $\mathcal{B} = \{B_1, \ldots, B_{11}\}$. Moreover, the block design D is symmetric.

Lemma 2.57 *Let $G = \mathrm{PSL}(2, 11)$ and let $D = (S, \mathcal{B})$ be a 2-$(11, 5, 2)$-design. Further, let G_s be the stabilizer of some element $s \in S$. Then G_s does not fix any block $B \in \mathcal{B}$.*

Proof. By Theorem 2.29, the group G is 2-fold transitive on S. Hence G_s is transitive on the remaining 10 elements of S. Assume that there exists a block $B \in \mathcal{B}$ such that $B^g = B$ for all $g \in G_s$. If $s \in B$ then we obtain two orbits of the action of G_s on $S \setminus \{s\}$, namely $B \setminus \{s\}$, which has length 4, and $S \setminus B$, which has length 6. This is a contradiction to the fact that G_s is transitive on $S \setminus \{s\}$. If $s \notin B$, the action of G_s on $S \setminus \{s\}$ also forms two orbits, namely the block B of length 5 and the remaining elements of $S \setminus \{s\}$ which is an orbit of length 5 as well. Again, we have a contradiction. In summary, the stabilizer G_s can not fix any block $B \in \mathcal{B}$. $\square$

From the above theorem it follows that the actions of $\mathrm{PSL}(2, 11)$ on the points and on the blocks of a 2-$(11, 5, 2)$-design are not permutationally equivalent and thus this leads to two different permutation representations of $\mathrm{PSL}(2, 11)$ in S_{11}.

The rest of this section is dedicated to the examination of the automorphism group of $\mathrm{PSL}(2, 11)$ and the almost simple groups lying between

PSL$(2,11)$ and Aut(PSL$(2,11)$). By Theorem 2.46, the group PSL$(2,11)$ has a complement C in its automorphism group. Further, by Theorem 2.48 the outer automorphism group of PSL$(2,11)$ is isomorphic to C_2 as in our case $m = 1$ and $\gcd(2,10) = 2$. As PSL$(2,11)$ is simple and non-abelian, we can identify the group with its inner automorphism, i.e. we have PSL$(2,11) \cong$ Inn(PSL$(2,11)$) and thus

$$C_2 \cong \mathrm{Aut}(\mathrm{PSL}(2,11)/\mathrm{Inn}(\mathrm{PSL}(2,11)) = \mathrm{Aut}(\mathrm{PSL}(2,11))/\mathrm{PSL}(2,11).$$

Hence the complement C of PSL$(2,11)$ in its automorphism group is isomorphic to C_2 and we obtain Aut(PSL$(2,11)$) = PSL$(2,11) \rtimes C_2$. As the index of PSL$(2,11)$ in its automorphism group is 2, the group is maximal in Aut(PSL$(2,11)$) and thus, there exist only two possible almost simple groups with socle $S =$ PSL$(2,11)$; namely PSL$(2,11)$ itself and its automorphism group PSL$(2,11) \rtimes C_2$. But the next theorem shows that PSL$(2,11) \rtimes C_2$ is not a transitive permutation group of degree 11.

Theorem 2.58 ([17, Chapter XII, Theorem 10.13]) *If G is a non-solvable transitive permutation group of degree* 11 *and G is a proper subgroup of A_{11}, then either $G = M_{11}$ or $G =$* PSL$(2,11)$.

A quick check in GAP shows that Aut(PSL$(2,11)$) is not a subgroup of the symmetric group S_{11}, hence there does not exist a non-trivial action of Aut(PSL(n,q)) on 11 elements.

Example 2.59

```
gap> G := PSL(2,11);;
gap> AutG := Image(NiceMonomorphism(AutomorphismGroup(G)));;
gap> S11 := SymmetricGroup(11);;
gap> IsSubgroup(S11, AutG);
false
```

2.2.3 The almost simple groups with socles M_{11} and M_{23}

We start with two defining theorems.

Theorem 2.60 (Mathieu, [25, Kapitel 3, Satz 3.16 & Definition 3.17]) *Let*

$$\begin{aligned}
a &= (1,4)(7,8)(9,11)(10,12),\\
b &= (1,2)(7,10)(8,11)(9,12),\\
c &= (2,3)(7,12)(8,10)(9,11),\\
d &= (4,5,6)(7,8,9)(10,11,12),\\
e &= (4,7,10)(5,8,11)(6,9,12),\\
f &= (5,7,6,10)(8,9,12,11),\\
g &= (5,8,6,12)(7,11,10,9).
\end{aligned}$$

Then $M_{12} := \langle a,b,c,d,e,f,g\rangle \leqslant S_{12}$ *is a sharply* 5*-fold transitive group of degree* 12 *and* $M_{11} := \langle a,b,d,e,f,g\rangle$ *is a sharply* 4*-fold transitive group of degree* 11*. Further, the groups* M_{11} *and* M_{12} *are called Mathieu groups of degree* 11 *respectively* 12 *and we have the orders* $|M_{11}| = 11\cdot 10\cdot 9\cdot 8$ *and* $|M_{12}| = 12\cdot 11\cdot 10\cdot 9\cdot 8$.

Theorem 2.61 ([17, Chapter XII, Theorem 1.4]) *Let* P *be the projective space over the* 3*-dimensional vector space* $\mathbb{F}_4^3$*. We represent the points of* P *by triples* $[x,y,z] \neq [0,0,0]$*. Let* $G = \mathrm{PSL}(3,4)$ *be regarded as a* 2*-fold transitive permutation group of degree* 21 *on the points of* P*. Let* k *be an element of* $\mathbb{F}_4$ *with* $k \neq 0,1$*. We put* $\Omega = P \cup \{u,v,w\}$ *and define the following mappings* s_1, s_2, s_3, s_4 *of* Ω *into* Ω*:*

- $u.s_1 = u,\ v.s_1 = v,\ w.s_1 = w,\ [x,y,z].s_1 = [y,x,z]$*;*
- $[1,0,0].s_2 = u,\ u.s_2 = [1,0,0],\ v.s_2 = v,\ w.s_2 = w,\ [x,y,z].s_2 = [x^2+yz, y^2, z^2]$ *for* $[x,y,z] \neq [1,0,0]$*;*
- $u.s_3 = v,\ v.s_3 = u,\ w.s_3 = w,\ [x,y,z].s_3 = [x^2, y^2, kz^2]$*;*
- $u.s_4 = u,\ v.s_4 = w,\ w.s_4 = v,\ [x,y,z].s_4 = [x^2, y^2, z^2]$.

Then s_1, s_2, s_3, s_4 *are permutations of* Ω *and we obtain the following groups:*

(1) The group $M_{22} := \langle G, s_2\rangle$ *is a* 3*-fold transitive permutation group of degree* 22 *on* $P \cup \{u\}$ *and* $|M_{22}| = 48\cdot 20\cdot 21\cdot 22$.

(2) The group $M_{23} := \langle M_{22}, s_3 \rangle$ *is a* 4*-fold transitive permutation group of degree* 23 *on* $P \cup \{u, v\}$ *and* $|M_{23}| = 48 \cdot 20 \cdot 21 \cdot 22 \cdot 23$.

(3) The group $M_{24} := \langle M_{23}, s_4 \rangle$ *is a* 5*-fold transitive permutation group of degree* 24 *on* $P \cup \{u, v, w\}$ *and* $|M_{24}| = 48 \cdot 20 \cdot 21 \cdot 22 \cdot 23 \cdot 24$.

The groups M_{22}, M_{23}, M_{24} *are called the Mathieu groups of degree* 22, 23, 24 *respectively. Further we have the stabilizers* $(M_{24})_w = M_{23}$, $(M_{23})_v = M_{22}$ *and* $(M_{22})_u = \mathrm{PSL}(3,4)$.

As our goal is to determine the almost simple groups with socle M_{11} and M_{23}, which are transitive of the corresponding degree, we examine the automorphims groups of both groups. The next theorem shows that the automorphism groups reveal no other almost simple groups with socle M_{11} respectively M_{23}.

Theorem 2.62 ([17, Chapter XII, Remark 1.15]) *For* $i = 11,\ 23,\ 24$ *we have* $\mathrm{Aut}(M_i) \cong M_i$ *and for* $i = 12,\ 22$ *we have* $|\mathrm{Aut}(M_i) : \mathrm{Inn}(M_i)| = 2$.

As $\mathrm{Aut}(M_{11}) \cong M_{11}$ and $\mathrm{Aut}(M_{23}) \cong M_{23}$, the only almost simple transitive permutation group of degree 11 respectively degree 23 with socle M_{11} respectively M_{23} is the Mathieu group of each degree itself.

Like the group $\mathrm{PSL}(2, 11)$, both Mathieu groups are full automorphism groups of t-(v, k, λ)-designs containing 11 respectively 23 points.

Theorem 2.63 ([17, Chapter XII, Remark 1.16])

(1) The Mathieu group M_{11} *is the automorphism group of a* 4-$(11, 5, 1)$-*design.*

(2) The Mathieu group M_{23} *is the automorphism group of a* 4-$(23, 7, 1)$-*design.*

A t-(v, k, λ)-design with $\lambda = 1$ as in Theorem 2.63 is called a *Steiner system*. Both Steiner systems are not symmetric, as the 4-$(11, 5, 1)$-design has 66 blocks and the 4-$(23, 7, 1)$-design has 253 blocks. This leads to the fact that both Mathieu groups each only have a single permutation representation.

Chapter 3

The computation of transitive groups of prime degree

In this chapter it is our goal to determine the non-solvable transitive permutation groups of prime degree $p \leqslant 23$, not using the classification of finite simple groups. Before the CFSG was published, the classification of transitive permutation groups of prime degree was an active field of research in group theory. The solvable permutation groups were easily classified by the theorem of Galois, whereas the classification of the non-solvable groups could not been solved with only one theorem. Many authors studied the structure of these groups. In [3], Brauer studied finite groups G containing elements $a \in G$ of prime order which only commute with their own powers. His results led Fryer in [8] to the consideration of groups G generated by three elements a, b and c which have the following properties: For a prime number $p = 2q + 1$, where q also is prime, the element a is a p-cycle, $b \in N_G(\langle a \rangle)$ with $b^{-1}\tilde{a}b \neq \tilde{a}$ for all $\mathrm{id}_G \neq \tilde{a} \in \langle a \rangle$ and $|b| = q$ and $c \in N_G(\langle b \rangle)$ with $c^{-1}\tilde{b}c \neq \tilde{b}$ for all $\mathrm{id}_G \neq \tilde{b} \in \langle b \rangle$. Further, Fryer showed that these groups are simple if they consist only of even permutations, giving Parker and Nikolai the basis to their research on groups resembling the Mathieu group M_{23} in [23]. The authors used the results of Fryer to construct generating sets which they hoped would lead to groups that are transitive on p elements, simple, not of order p and proper subgroups of the alternating group A_p. Here, the prime $p \geqslant 23$ also was of the form $2q + 1$ with q a prime. The calculations which would decide whether a group has the desired properties were made on the UNIVAC Scientific Computer, Model 1103A.

However, their calculations did not produce any other group than M_{23}. The range of the primes $p = 2q + 1$ that the authors had considered was 23 up to 1823, hence 33 primes had been checked giving rise to the author's conjecture, that a non-solvable transitive permutation group of prime degree $p = 2q + 1$, where q also is prime, is alternating or symmetric.

In the next two sections we show that the ideas of Parker and Nikolai also work for primes $p = 2q + 1$, where q not necessarily is a prime number. For that, we prove our main theorem which states that non-solvable transitive permutation groups of such degree contain elements a, b and c similiar to the elements we described above. This result is the basis for the algorithms we implemented to determine the non-solvable transitive permutation groups of prime degree $p \leqslant 23$. Moreover, we give an alternative way to construct representatives of all conjugacy classes of these groups with degree up to 13 using the table of marks.

First we introduce some results which are useful to understand why our method works.

3.1 Useful results

The first two theorems we introduce are well-known results by Burnside, Schur and Zassenhaus. We use both theorems to examine the structure of the non-solvable transitive permutation groups of prime degree in the next section.

Theorem 3.1 (Burnside's Transfer Theorem, [16, Kapitel IV, Satz 2.6]) *Let p be prime and let G be a finite group. Further, let P be a Sylow p-subgroup of G such that $P \leqslant Z(N_G(P))$. Then there exists a normal subgroup N of G with $G/N \cong P$.*

Remark 3.2 In Burnside's Transfer Theorem the condition $P \leqslant Z(N_G(P))$ is equivalent to $P \leqslant C_G(N_G(P))$ as

$$C_G(N_G(P)) = \{g \in G \mid gn = ng \text{ for all } n \in N_G(P)\}$$

and

$$Z(N_G(P)) = \{n \in N_G(P) \mid ng = ng \text{ for all } g \in N_G(P)\}$$

and both $P \leqslant C_G(N_G(P))$ respectively $P \leqslant Z(N_G(P))$ imply that $an = na$ for all $n \in N_G(P)$ and for all $a \in P$.

Theorem 3.3 (Schur-Zassenhaus, [16, Kapitel I, Sätze 18.1 & 18.2]) *If G is a finite group, and N is a normal subgroup of G such that* $\gcd(|G/N|, |N|) = 1$*, then the following statements hold:*

(1) The normal subgroup N has a complement in G.

(2) If either N or G/N is solvable then all complements to N are conjugate to each other.

The theorem of Schur-Zassenhaus yields necessary conditions for a normal subgroup of a group G to have a complement. The next result shows which subgroups of G are fit to be such a complement.

Lemma 3.4 *Let G be a finite group and let N be a normal subgroup of G. Let* $\gcd(|G/N|, |N|) = 1$ *and let H be a subgroup of G such that $|H| = |G/N|$. Then H is a complement to N in G.*

Proof. As $\gcd(|H|, |N|) = 1$ it follows that $H \cap N = \{\mathrm{id}_G\}$. Then we obtain

$$|HN| = |H||N| = |G/N||N| = |G|,$$

hence $HN = G$ and the claim follows. □

The next concept we introduce is a generalization of Sylow subgroups.

Definition 3.5 Let G be a group and let π be a set of primes.

(1) A subgroup $U \leqslant G$ is called a *π-subgroup* of G if and only if the order of U is a product of primes in π.

(2) A subgroup $H \leqslant G$ is called a *Hall π-subgroup* of G if and only if the following conditions are satisfied:

   (a) The order of H is a product of primes in π,

   (b) The index $|G : H|$ is not divisible by any prime in π.

Theorem 3.6 (Hall, [16, Kapitel VI, Satz 1.8]) *If G is a finite solvable group and π is any set of primes, then G has a Hall π-subgroup, and any two Hall π-subgroups of G are conjugate. Moreover, any π-subgroup of G is contained in some Hall π-subgroup of G.*

Later, we combine the concepts of Hall π-subgroups and complements to inspect the structure of the normalizer $N_G(\langle a \rangle)$ for a p-cycle a in a non-solvable transitive permutation group G. We will see that each Hall π-subgroup of G, for π the set of primes dividing $p-1$, is a complement of $\langle a \rangle$ in its normalizer and vice versa.

Definition 3.7 Let G be a finite group.

(1) A series $Z_1 \geqslant Z_2 \geqslant \cdots \geqslant Z_r$ is called *central series* if and only if Z_i is a normal subgroup of G for all $i = 1, \ldots, r$ and $Z_i/Z_{i+1} \leqslant Z(G/Z_{i+1})$ for all $i = 1, \ldots, r-1$.

(2) The group G is called *nilpotent* if and only if it has a central series with $Z_1 = G$ and $Z_r = \{\mathrm{id}_G\}$.

Theorem 3.8 ([5, Chapter VIII, Section 93]) *Let p be a prime and let G be a finite p-group. Then G is nilpotent.*

Theorem 3.9 ([16, Kapitel 3, Hauptsatz 2.3]) *Let G be a finite group. Then the following statements are equivalent:*

(1) G is nilpotent;

(2) $U \lneqq N_G(U)$ for each proper subgroup U of G.

Theorems 3.8 and 3.9 will help us in the proof of the main theorem in the next section. As $U \lneqq N_G(U)$ for each proper subgroup U of a p-group G we can guarantee the existence of an element $c \in N_G(U) \setminus U$.

Next, we introduce the concept of a Frobenius group.

Definition 3.10 Let $\{\mathrm{id}_G\} < H < G$ and $H \cap H^g = \{\mathrm{id}_G\}$ for all $g \in G \setminus H$. Then G is called a *Frobenius group* to H and $F := G \setminus \bigcup_{g \in G} (H \setminus \{\mathrm{id}_G\})^g$ is called the *Frobenius kernel* of G.

Theorem 3.11 ([16, Kapitel V, Satz 8.2a]) *Let G be a transitive non-regular permutation group on a finite set Ω such that each element $\mathrm{id}_G \neq g \in G$*

stabilizes at most one point $\omega \in \Omega$. Let $H := G_\omega$. Then G is a Frobenius group with complement H and the permutations of G which do not stabilize any element of Ω together with id_G form the Frobenius kernel F of G and F is regular on Ω.

Theorem 3.12 ([16, Kapitel V, Satz 8.5]) *Let G be a group and let H be a subgroup of G. The following statements are equivalent:*

(1) G is a Frobenius group to H with Frobenius kernel F.

(2) We have $G = FH$ with $H < G$ and F is a normal subgroup of G. Further, the map $\mu : H \to U$, where U is a fixed point free subgroup of $\mathrm{Aut}(F)$, such that $f^{h^\mu} = h^{-1}fh$ for $f \in F$ and $h \in H$, is an isomorphism.

At least, we introduce two well-known results of Borchert and Jordan. Later, it is our goal to show that the groups we compute with our algorithms are maximal in the alternating group with the same prime degree p. Otherwise, our algorithms would not generate all transitive permutation groups of the given degree. Assuming there exists a group H with $G \leqslant H \lneqq A_p$, the theorems help us to estimate all possible orders of H. Further, we check whether G is maximal by considering the Sylow s-subgroups of H for some prime s dividing the order of G.

Theorem 3.13 (Borchert, [16, Kapitel II, Satz 4.6]) *Let G be primitive on a finite set Ω and let $|\Omega| = n$ and $A_n \nleqslant G$. Then*

$$|S_n : G| \geqslant [(n+1)/2]!.$$

Theorem 3.14 (Jordan, [17, Chapter XII, Theorem 3.7]) *Let G be a primitive permutation group of degree $n = p + k$, where p is a prime and $k \geqslant 3$. If G contains a cycle of length p, then $G \geqslant A_n$.*

3.2 Mathematical aspects

In this section we discuss the mathematical background of our algorithms. Recall that we want to compute the transitive permutation groups of a given prime degree $p = 2q+1$, $q \in \mathbb{N}$, which are non-solvable and proper subgroups of the alternating group A_p. The results on the structure of these groups by Fryer in [8] yield a basis. The main result of this section shows that non-solvable transitive permutation groups of degree p contain elements a, b and c such that a is a p-cycle, $b \in N_{A_p}(\langle a \rangle)$ and $c \in N_{A_p}(\langle b \rangle)$. In our computations we use these elements to calculate generating sets and test whether the corresponding groups are non-solvable and proper subgroups of A_p.

The first lemma we prove shows that a Sylow p-subgroup of a permutation group of prime degree always has a cyclic complement in its normalizer.

Lemma 3.15 *Let G be a permutation group of prime degree p and let P be a Sylow p-subgroup of G. Then P has a cyclic complement C in $N_G(P)$ with $|C|$ dividing $p-1$.*

Proof. Let $M := N_G(P)$. We have $\gcd(|M/P|, |P|) = 1$, as p^2 does not divide $|M|$. By Theorem 3.3, the Sylow p-subgroup P has a complement C in M. Moreover, $C_G(P) = P$ by Theorem 2.16, since P is abelian. Then

$$N_G(P)/C_G(P) = M/P \cong A,$$

where A is a subgroup of $\mathrm{Aut}(P) \cong C_{p-1}$. Since C is a complement to P in M, we have $C \cong A$, hence C is cyclic and its order divides $p-1$. □

As p^2 does not divide the order of a transitive permutation group G of prime degree p, the group G always contains a Sylow p-subgroup of order p. Hence G contains a p-cycle, namely the generator of its Sylow p-subgroup which already proves the first statement we want to show later, that is the existence of a p-cycle in a non-solvable transitive permutation group of degree p.

Lemma 3.16 *Let G be a non-solvable transitive permutation group of prime degree p and let $G^{(i)}$ denote the ith commutator subgroup of G. Then $G^{(i)}$ is transitive on p elements for all $i \geqslant 0$. Moreover, $p \mid |G^{(i)}|$ for all $i \geqslant 0$.*

Proof. Induction on $i \geqslant 0$.

For $i = 0$ the group $G^{(0)} = G$ is transitive on p elements by assumption. By the orbit-stabilizer theorem we have $p \mid |G|$.

Let $i \geqslant 1$ and let $G^{(i)}$ be transitive on p elements. As $G^{(i+1)}$ is a normal subgroup of $G^{(i)}$, the group $G^{(i)}$ is either the trivial group or transitive on p elements as well by Theorem 2.14. If $G^{(i)}$ is trivial, then G is solvable, a contradiction. Hence $G^{(i+1)}$ is transitive and by the orbit-stabilizer theorem we obtain $p \mid |G^{(i+1)}|$. □

The next lemma deals with the cycle type and the order of elements in $N_{S_p}(\langle a \rangle)$ for a p-cycle $a \in S_p$.

Lemma 3.17 *Let $p = 2q + 1$ be prime, $q \in \mathbb{N}$. Further, let $a \in S_p$ be a p-cycle and $b \in N_{S_p}(\langle a \rangle)$ with $r := |b|$. If p does not divide r then b consists of k disjoint r-cycles and $rk = 2q$.*

Proof. Set $P := \langle a \rangle$. As P is normal in $N_{S_p}(P)$ and p^2 does not divide $|N_{S_p}(P)|$, the group P is the unique Sylow p-subgroup of $N_{S_p}(P)$. Theorem 2.26 implies that $N_{S_p}(P)$ is solvable and thus it is permutationally equivalent to a subgroup $U = K \ltimes N \leqslant \mathrm{Aff}(1, p)$, where $N = \{f_{0,d} \mid d \in \mathbb{F}_p\}$ and $K \leqslant \{f_{c,0} \mid c \in \mathbb{F}_p^*\}$. Let $\varphi : U \to N_{S_p}(P)$ denote the isomorphism between U and $N_{S_p}(P)$. Then $P = \varphi(N)$ by Theorem 2.25.

Put $B := \varphi(K)$. Let π be the set of all primes dividing $p-1$. Then $|B|$ has only prime factors in π as $|K|$ divides $p - 1$ and $|N_{S_p}(P) : B| = |P| = p$ does not contain any prime in π. Hence B is a Hall π-subgroup of $N_{S_p}(P)$. Let H be a Hall π-subgroup of $N_{S_p}(P)$. Then by the definition of Hall π-subgroups we have $|H| = |N_{S_p}(P) : P|$ and therefore by Lemma 3.4, the group H is a complement of P as well. Hence each complement of P is a Hall π-subgroup of $N_{S_p}(P)$ and vice versa.

As p does not divide the order of the element b, it lies in some Hall π-subgroup of $N_{S_p}(P)$. Since $N_{S_p}(P)$ is solvable, any two Hall π-subgroups are conjugate by Theorem 3.6, hence by replacing b with a conjugate we may assume that $b \in B$ and it is the image of $f_{t,0} \in K$ for some $t \in \mathbb{F}_p^*$ under the isomorphism φ.

Then we have $|f_{t,0}| = |b| = r$, hence $t^i x \neq x$ for $i < r$ and $t^r x = x$ for all $x \in \mathbb{F}_p^*$. Thus $f_{t,0}$ permutes the $p - 1 = 2q$ elements of $\mathbb{F}_p^*$ in $2q/r =: k$ cycles of length r. By the permutation equivalence, this implies our claim. □

Now we prove the main result of this section.

Theorem 3.18 *Let $p = 2q + 1$ be prime, $q \in \mathbb{N}$, and let $G \leqslant A_p$ be a finite group such that*

(a) G is a transitive permutation group of degree p;

(b) G is non-solvable.

Then there exist $a, b \in G$ such that

(1) a is a p-cycle;

(2) $b \in N_G(\langle a \rangle) \setminus C_G(\langle a \rangle)$ and if $r := |b|$, then $p \nmid r$, $r \neq 1$, and b consists of k disjoint r-cycles with $rk = 2q$. Further, we have

(i) If q is odd, then r is odd;

(ii) If q is even, then k is even.

In particular, r is a factor of q.

(3) There exists a prime $\ell \mid r$ and $b_1 \in \langle b \rangle$ such that $\langle b_1 \rangle$ is a Sylow ℓ-subgroup of $\langle b \rangle$ and an element $c \in N_G(\langle b_1 \rangle) \setminus \langle b_1 \rangle$ with $\langle a, b_1, c \rangle$ non-solvable. If $\langle b_1 \rangle$ is a Sylow ℓ-subgroup of G, then $c \notin C_G(\langle b_1 \rangle)$.

Proof. Let G be a non-solvable transitive permutation group of prime degree $p = 2q + 1$, $q \in \mathbb{N}$, such that $G \leqslant A_p$. As p divides the order of G, but p^2 does not, the group G contains a Sylow p-subgroup P of order p. Further, P is cyclic and generated by a p-cycle a, i.e. $P = \langle a \rangle$. Hence the claim in (1) follows.

Assume that P is in the centralizer of its normalizer, i.e. $P \leqslant C_G(N_G(P))$. Then Burnside's Transfer Theorem 3.1 implies that G contains a normal subgroup N such that $G/N \cong P$; in particular, the order of N is prime to p. As the order of G/N is p, we have $\gcd(|G/N|, |N|) = 1$. By Lemma 3.4, the group G is the semidirect product of P and N. Let K denote the commutator subgroup of G. As P is abelian and $G/N \cong P$, it follows that $K \leqslant N$. Hence K has order prime to p as well. This contradicts Lemma 3.16. Hence P is not a subgroup of the centralizer of its normalizer.

Put $M := N_G(P)$. The group P is a Sylow p-subgroup of M, hence it has a cyclic complement B in M by Lemma 3.15. We have $B \neq \{\mathrm{id}_G\}$ by the previous paragraph, thus there exists $\mathrm{id}_G \neq b \in B$ such that $B = \langle b \rangle$. Moreover, as P is not a subgroup of $C_G(M)$ and $b \in M$, we obtain $b^{-1}\tilde{a}b \neq \tilde{a}$ for all $\tilde{a} \in P$, $\tilde{a} \neq \mathrm{id}_G$, hence $b \notin C_G(P)$.

Put $r := |b|$. As $\gcd(|B|, |P|) = 1$ and thus p does not divide r, Lemma 3.17 implies that b consists of $k := 2q/r$ disjoint r-cycles. As G is a subgroup of A_p, the group G contains only even permutations and to establish the requirements on r and k we have to distinguish between two cases.

- If q is odd then $\nu_2(2q) = 1$, where $\nu_2(x)$ denotes the 2-adic valuation of an integer x. Assume that r is even. A cycle of even length is an odd permutation, hence the sign of each cycle of b is -1. As $2 \mid r$, the number k must divide q, thus k is odd as well. Therefore, the element b consists of an odd number of odd permutations, hence $\mathrm{sgn}(b) = -1$. Then b is not an element of A_p, a contradiction. Hence r must be odd.

- If q is even then $\nu_2(2q) \geqslant 2$. If $2^{\nu_2(2q)} \mid r$, then k is odd and again, we have an odd number of cycles of even length, hence $\mathrm{sgn}(b) = -1$, contradicting the fact that b is an element of A_p. If r is even and $2^{\nu_2(2q)}$ does not divide r, then k is even.

These cases lead to the following requirements on r and k for b to be an even permutation: If q is odd, then r is odd and if q is even, then k is even. Both cases lead to r being a factor of q, hence the claim in (2) follows.

Now we prove the statements in (3). Assume there exists a prime divisor ℓ of r such that the corresponding Sylow ℓ-subgroup L of B is not a Sylow ℓ-subgroup of G. Further, let $b_1 \in B$ denote a generator of L, i.e. $L := \langle b_1 \rangle$. As $N_G(P) = \langle a, b \rangle$ and $|a| = p$, we have $\nu_\ell(|L|) = \nu_\ell(|N_G(P)|)$. Thus L is a Sylow ℓ-subgroup of $N_G(P)$. Let S be a Sylow ℓ-subgroup of G such that $L \leqslant S$. As S is an ℓ-group, the group S is nilpotent by Theorem 3.8. Moreover, by Theorem 3.9, for each proper subgroup U of S it follows that U is a proper subgroup of its normalizer $N_S(U)$ in S. As L is a proper subgroup of S, we can choose an element $c \in N_S(L) \setminus L$. As $N_S(L) \setminus L$ is a subset of $N_G(L) \setminus L$, we obtain $c \in N_G(L) \setminus L$. Further, as $c \in S$, its order is a power of ℓ.

Suppose that $c \in N_G(P)$. Then $\langle L, c \rangle$ is a subgroup of $N_G(P)$. Moreover, it is an ℓ-group and $|\langle L, c \rangle| > |L|$, as $c \notin L$. This is a contradiction to the fact that L is a Sylow ℓ-subgroup of $N_G(P)$ and thus, the element c can not lie in $N_G(P)$. If $\langle a, b_1, c\rangle$ is solvable, then P is a normal subgroup of $\langle a, b_1, c\rangle$ by Theorem 2.26 and thus, we have $c \in N_{\langle a,b_1,c\rangle}(P) \leqslant N_G(P)$, which we just ruled out. Hence $\langle a, b_1, c\rangle$ is non-solvable.

Assume now for each prime divisor m of r that the corresponding Sylow m-subgroup is a Sylow m-subgroup of G as well. As each Sylow m-subgroup of B is a Sylow m-subgroup of $N_G(P)$ as well, it follows that $\gcd(|N_G(P)|, |G/N_G(P)|) = 1$. Let ℓ be an arbitrary prime divisor of r and let $L := \langle b_1\rangle$ denote the corresponding Sylow ℓ-subgroup of B respectively G. Assume that L is a subgroup of the centralizer of its normalizer, i.e. $L \leqslant C_G(N_G(L))$. Then by Theorem 3.1, there exists a normal subgroup N of G such that $G/N \cong L$; in particular, the order of N is prime to $|L|$. As L is abelian, the commutator subgroup K of G is a subgroup of N and thus $\gcd(|K|, |L|) = 1$. As ℓ was arbitrary this follows for every prime divisor of r and the corresponding Sylow subgroup. Hence $\gcd(|K|, r) = 1$. By Lemma 3.16, the order of K is divisible by p and thus, we have $P \leqslant K$. As $N_K(P) \leqslant N_G(P)$ and $|N_G(P)| = pr$, the order of $N_K(P)$ is p. Hence Burnside's Transfer Theorem 3.1 applied to K and P implies that there exists a normal subgroup $\widetilde{N}$ of K such that $K/\widetilde{N} \cong P$. Since P is abelian, the second commutator group K' of G lies in $\widetilde{N}$ and thus, its order is prime to p as well. This contradicts Lemma 3.16. Hence our assumption was false and L is not a subgroup of the centralizer of its normalizer. Thus there exists $c \in N_G(L) \setminus C_G(L)$. Again, if $\langle a, b_1, c\rangle$ is solvable, the group P is a normal subgroup of $\langle a, b_1, c\rangle$ and thus $c \in N_{\langle a,b_1,c\rangle}(P)$. By Theorem 3.11, the group $\langle a, b_1, c\rangle$ is a Frobenius group with Frobenius kernel P. Let $x \in P \cap N_{\langle a,b_1,c\rangle}(L)$. Then the commutator $[x, y]$ lies in $P \cap L = \{\mathrm{id}_G\}$ for all $y \in L$. By Theorem 3.12 we have $x^{-1}yx \neq y$ and thus, we obtain $x = \mathrm{id}_G$. Hence $P \cap N_{\langle a,b_1,c\rangle}(L) = \{\mathrm{id}_G\}$. Thus, the group $N_{\langle a,b_1,c\rangle}(L)$ lies in the complement of P in $\langle a, b_1, c\rangle$ and theorefore, it is isomorphic to a subgroup of $\langle a, b_1, c\rangle/P$. By assumption, the group $\langle a, b_1, c\rangle$ is solvable, hence $N_{\langle a,b_1,c\rangle}(L)$ is abelian. Then we obtain $c \in \langle b_1\rangle$ which is a contradiction, since $c \notin C_G(\langle b_1\rangle$ and $\langle b_1\rangle \leqslant C_G(\langle b_1\rangle)$. Hence $\langle a, b_1, c\rangle$ is non-solvable and the claim follows. □

Remark 3.19 Let b_1 and b be as in Theorem 3.18. As $\langle b_1\rangle \leqslant \langle b\rangle$ and $\langle b\rangle$ is cyclic, the element b_1 is a power of b; in particular, there exists $t \in \mathbb{N}$ such that $b^t = b_1$.

The following proposition shows that the element a and the group $\langle b \rangle$ are unique up to conjugation in S_p. This result is essential for our algorithms as it allows us to consider only one set of generators $\{a, b\}$ for each divisor of q to obtain all groups $\langle a, b, c \rangle$ for $c \in N_{A_p}(\langle b \rangle)$ as in Theorem 3.18, which are non-solvable transitive permutation groups of degree $p = 2q + 1,\ q \in \mathbb{N}$.

Proposition 3.20 *Let $p = 2q+1,\ q \in \mathbb{N}$, be prime. Let $a_i,\ b_i \in A_p,\ i = 1, 2$, such that*

(1) a_1 and a_2 are p-cycles;

(2) $b_i \in N_{A_p}(\langle a_i \rangle),\ i = 1, 2$, with $|b_1| = |b_2|$ and $p \nmid |b_1|$.

Then there exist $x \in S_p$ such that $a_1^x = a_2$ and $\langle b_1^x \rangle = \langle b_2 \rangle$.

Proof. As a_1 and a_2 are p-cycles in A_p, they are conjugate in S_p, i.e. there exists $y \in S_p$ such that $a_1^y = a_2$. Put $P_2 := \langle a_2 \rangle$ and $M_2 := N_{A_p}(P_2)$. As P_2 is the unique Sylow p-subgroup subgroup of M_2, the group M_2 is solvable by Theorem 2.26. Further, we have $b_1^y,\ b_2 \in M_2$.

Let π denote the set of primes dividing $(p - 1)$. By Lemma 3.15, the group P_2 has a complement in M_2 whose order divides $p - 1$. As p does not divide $|b_2| =: r$, we obtain $r \mid q - 1$. Thus the groups $\langle b_1^y \rangle$ and $\langle b_2 \rangle$ are π-subgroups of M_2. By Theorem 3.6, each π-subgroup is contained in some Hall π-subgroup of M_2. Let $H, B_2 \leqslant M_2$ denote Hall π-subgroups of M_2 containing b_1^y respectively b_2. Since $\gcd(|M_2/P_2|, |P_2|) = 1$ and $|H| = |B_2| = |M_2/P_2|$ by definition, both H and B_2 are complements to P_2 in M_2 by Lemma 3.4. Moreover, Theorem 3.3 implies that H and B_2 are conjugate in M_2.

Let $z = hz' \in M_2 = HP_2$, where $h \in H$ and $z' \in P_2$, be such that $B_2 = H^z = H^{hz'} = H^{z'}$. Put $x := yz' \in S_p$. Then $a_1^x = a_1^{yz'} = a_2^{z'} = a_2$ as $z' \in P_2$. Further, we have $b_1^x = b_1^{yz'} \in H^{z'} = B_2$ and $|b_2| = |b_1| = |b_1^x|$. As B_2 is cyclic and $b_2,\ b_1^x \in B_2$, we obtain $\langle b_1^x \rangle = \langle b_2 \rangle$. $\square$

Let G_1 be a transitive permutation group of prime degree $p = 2q + 1$, where $q \in \mathbb{N}$, such that G_1 is non-solvable and a proper subgroup of A_p. By Theorem 3.18 there exist elements $a_1, b_1, c_1 \in G$ such that a_1 is a p-cycle,

$b_1 \in N_{G_1}(\langle a_1\rangle) \leqslant N_{A_p}(\langle a_1\rangle)$ with $|b_1| =: r$ and $c_1 \in N_{G_1}(\langle b_1\rangle) \leqslant N_{A_p}(\langle b_1\rangle)$. Let $a = (1, 2, \ldots, p)$ and b any element in $N_{A_p}(\langle a\rangle)$ with $|b| = r$. Proposition 3.20 implies that there exist $x \in S_p$ such that $a_1^x = a_2$ and $\langle b_1^x\rangle = \langle b\rangle$. We set $c := c_1^x$ and $G := G_1^x$. Hence G_1 is conjugate to G in the symmetric group S_p. By Lemma 2.10, both groups are permutationally equivalent. As we only want to classify the desired groups up to permutation equivalence, it suffices to choose the generating sets as follows: $a = (1, \ldots, p)$ and for each $r \mid q$ with $r \neq 1$ we choose an element $b \in N_{A_p}(\langle a\rangle)$ with $|b| = r$ such as a corresponding $\mathrm{id}_G \neq c \in N_{A_p}(\langle b\rangle)$. In order to obtain the desired groups we iterate over the elements of $N_{A_p}(\langle b\rangle)$.

3.3 The computations

3.3.1 Verification of the algorithms

Given a fixed prime number p, the goal of our computations is to determine the non-solvable transitive permutation groups of degree p which are proper subgroups of A_p. We take the approach introduced in the previous section as a basis, hence the groups we check are generated by elements a, b_1 and c as described above. Our computation is divided into two parts. In the first part it is our goal to determine elements $b \in N_{A_p}(\langle a\rangle)$ for $a = (1, \ldots, p)$ with $r = |b|$ for each $r \mid q$, $r \neq 1$. They are generated by Algorithm 2. These elements are used in Algorithm 3 to calculate the desired groups. Further, we check whether these groups are maximal in the alternating group A_p which means that no further generator is needed to generate the transitive permutation groups of degree p. For that, we implemented a third algorithm. The GAP codes of the algorithms are recorded in Appendix *A*. This section serves as a verification of these algorithms.

Theorem 3.21 *Let $a = (1, \ldots, p) \in A_p$. For a prime $p = 2q + 1,\ q \in \mathbb{N}$, Algorithm 2 computes for each divisor $r \neq 1$ of $q = (p-1)/2$ an element $\mathrm{id}_G \neq b \in N_{A_p}(\langle a\rangle)$ with $|b| = r$. Further, the algorithm terminates.*

Proof. If the input is not a prime or equal to 2 then there is nothing to prove.

Let $p = 2q + 1,\ q \in \mathbb{N}$, be a fixed prime number. For a list L, the GAP function `PermList(L)` returns a permutation, where $i \in \{1, \ldots, $ `Length(L)`$\}$ is mapped to `L[i]`. By inserting the list `Concatenation([2..p],[1])`, the function generates the p-cycle $a := (1, \ldots, p)$.

Put $P := \langle a \rangle$ and $N := N_{A_p}(P)$. To obtain an element $b \in N_{A_p}(P)$ for each divisor $r \neq 1$ of $q = (p-1)/2$, the algorithm takes the following steps: First, it computes the alternating group A_p of degree p and the normalizer N of P in A_p. Further, as P contains a complement in $N_{A_p}(P)$ by Lemma 3.15 and as each factor $r \mid q$ is not divisible by p, the elements we want to compute lie in a Hall π-subgroup of $N_{A_p}(P)$, where π denotes the set of all primes dividing q. Let H be a Hall π-subgroup of $N_{A_p}(P)$. Then by definition we have $|G/H| = |P| = p$ and thus $\gcd(|G/H|, |H|) = 1$, as H contains only primes in π and p does not divide q. By Lemma 3.4, the group H is a complement of P in $N_{A_p}(P)$. Hence the desired elements lie in a complement of P. Thus, the algorithm generates a list of representatives of the conjugacy classes of complements of P in N by the GAP function `ComplementClassesRepresentatives(N,P)`. By Theorem 3.3 the complements are all conjugate, hence the list contains a single group. Let K denote the representative. The generators of K are stored in the list `gens`. As K is cyclic by Lemma 3.15 we obtain the desired elements b for each factor of q by taking a generator g of order q and computing the powers g^x for all divisors x of q. Then g^x has order $q/x =: r$, hence the order of g^x is a divisor of q as well. To obtain a suitable generator g the algorithm iterates over all elements of the list `gens` and checks whether the order is q or not. Further, a list of all divisors of q is computed by the GAP function `DivisorsInt(q)`. As b is not supposed to be the identity, we do not need to calculate the power g^q, hence we exclude q from the list of the divisors of q. For that, the algorithm needs the GAP function `ShallowCopy`, since the list returned by `DivisorsInt` is not mutable. For a given list, the function `ShallowCopy` generates a mutable version of the list and the GAP function `Remove` removes the last entry of it. The divisors of q are arranged in ascending order in the list given by `DivisorsInt`, hence, in our case, q is removed. Let $L := \{x \in \mathbb{N} \mid x \mid q\} \setminus \{q\}$. For all x in L, the algorithm computes g^x and stores the elements in a list `res`, which, together with the p-cycle $a = (1, \ldots, p)$ is the output of Algorithm 2. Hence the first claim follows.

The list `gens` of all generators of K is finite, since $K \leqslant A_p$ is finite, and the number of divisors of q is finite as well. As the algorithm iterates over both the elements of `gens` and all divisors of q, the algorithm terminates. □

Remark 3.22 For each divisor $r := q/x$ of q, Algorithm 2 computes an element $b = g^x$ of order r. Now let y be another divisor of q such that $x \mid y$. Then g^y is an power of b. Hence the algorithm computes all powers of b and thus, if r is a factor of q consisting of at least two different primes, the algorithm also computes the element b_1 as in Theorem 3.18, as b_1 is a power of b by Remark 3.19.

Theorem 3.23 *Algorithm 3 terminates. Moreover, given a prime number* $p = 2q+1,\ q \in \mathbb{N}$, *and the corresponding elements* $a := (1, \dots, p)$ *and a fixed* $b \in N_{A_p}(\langle a \rangle)$ *generated by Algorithm 2, the algorithm computes a list of non-solvable transitive permutation groups of degree p, which are proper subgroups of* A_p *and generated by* a, b *and some* $\mathrm{id}_{A_p} \neq c \in N_{A_p}(\langle b \rangle)$. *Further, let* H *be a non-solvable proper subgroup of* A_p *such that* $H = \langle a_1, b_1, c_1 \rangle$, *where* $|a_1| = p$, $\mathrm{id}_{A_p} \neq b_1 \in N_{A_p}(\langle a_1 \rangle)$ *with* $|b_1| = |b|$ *and* $\mathrm{id}_{A_p} \neq c_1 \in N_{A_p}(\langle b_1 \rangle)$. *Then* H *is conjugate in the symmetric group* S_p *to a group, which is returned by Algorithm 3 by inserting* (a, b, p).

Proof. Let $p = 2q + 1,\ q \in \mathbb{N}$, be a fixed prime and let $a = (1, \dots, p)$ and $b \in N_{A_p}(\langle a \rangle)$ be fixed elements computed by Algorithm 2 with input p.

As the alternating group $A := A_p$ is finite, the normalizer $N_A(\langle b \rangle)$ is finite as well. Since the algorithm iterates over all elements of $N_A(\langle b \rangle)$, it terminates.

The `if` conditions in lines 3 to 11 check whether the input for Algorithm 3 is correct. For instance, it stops if the input p is not a prime number or if a or b is an odd permutation or if one of them is not even a permutation. For that, the algorithm uses the GAP functions `IsPrimeInt` and the function `IsEvenPerm` whose code also is recorded in Appendix A.

Algorithm 3 generates a group $G = \langle a, b, c \rangle$ for each $c \in N_A(\langle b \rangle)$ and checks whether G is non-solvable and a proper subgroup of A_p by using the following GAP functions: the term `Size(A) <> Size(G)` has boolean value `"true"` if G is a proper subgroup of A. By the term `not IsSolvable` the algorithm checks whether G is non-solvable. If the boolean values of all `if` conditions are `"true"`, the group G is stored in a list `res` which is the output of Algorithm 3. The groups which are generated in each step of the `for` loop are all transitive on p elements as they contain $\langle a\rangle$ and transitivity is transferred to overgroups. Further, they are faithful on p elements as they are subgroups of A_p. Hence the list which is returned only contains groups $G = \langle a, b, c\rangle$ which are non-solvable transitive permutation groups on p elements and proper subgroups of A.

Let $H = \langle a_1, b_1, c_1\rangle$ be a non-solvable transitive permutation group of degree p with a_1, b_1 and c_1 such that a_1 is a p-cycle, $\mathrm{id}_{A_p} \neq b_1 \in N_{A_p}(\langle a_1\rangle)$ with $r := |b_1| = |b|$, and $\mathrm{id}_{A_p} \neq c_1 \in N_{A_p}(\langle b_1\rangle)$. For $a = (1, \dots, p)$ and $b \in N_{A_p}(\langle a\rangle)$, Proposition 3.20 implies that there exist $x \in S_p$ such that $a_1^x = a$ and $\langle b_1^x\rangle = \langle b\rangle$. Hence H is conjugate to a group containing the p-cycle a and $b \in N_{A_p}(\langle a\rangle)$, which is returned by Algorithm 3. $\square$

We give a simple example for $p = 7$. As $q = 3$ is prime, we obtain only one element $b \in N_{A_7}(\langle a\rangle)$ for $a = (1, \dots, 7)$ from Algorithm 2. Instead of displaying all groups computed by Algorithm 3, we give a list of all elements $c \in N_{A_7}(\langle b\rangle)$ which lead to a group satisfying our requirements. Further, we check the computed groups for equality. If one of the computed groups is a subgroup of another one of the same isomorphism type, then they are equal, since they have the same size. In the following example, we see that Algorithm 3 only computes two different groups isomorphic to $\mathrm{PSL}(3, 2)$.

Example 3.24

```
gap> C := ComputationOfGenerators(7);
[(1,2,3,4,5,6,7), [(2,5,3)(4,6,7)]]
gap> a := C[1];; b := C[2][1];;
gap> T:= TransitiveGroupsViaNormalizer(a, b, 7);;
gap> L := List(T, x -> GeneratorsOfGroup(x)[3]);
[(3,5)(6,7),(2,5)(6,7),(2,3)(4,6),(2,5)(4,6),(3,5)(4,7),
(2,3)(4,7)]
gap> List(T, StructureDescription);
["PSL(3,2)", "PSL(3,2)", "PSL(3,2)", "PSL(3,2)", "PSL(3,2)",
"PSL(3,2)"]
gap> List(T, x -> IsSubgroup(x,T[1]));
[ true, false, false, true, false, true ]
```

```
gap> List(T, x -> IsSubgroup(x,T[2]));
[ false, true, true, false, true, false ]
```

Theorem 3.25 *Algorithm 4 terminates. Further, for a given transitive group G of prime degree p and a prime s dividing the order of G it checks whether there exists a transitive group H such that $G \leqslant H \lneqq A_p$ with a larger Sylow s-subgroup than G which is not the full Sylow s-subgroup of A_p.*

Proof. Let G be a transitive permutation group of prime degree p such that G is a proper subgroup of the alternating group A_p. The alternating group A_p is finite and thus, the normalizer $N_{A_p}(S)$ for a Sylow s-subgroup S of G is finite as well. As the algorithm iterates over all elements of $N_{A_p}(S) \setminus S$, it terminates.

Assume that there exists a group H such that $G \leqslant H \lneqq A_p$. Let T be a Sylow s-subgroup of H with $S \lneqq T$. Since $H \lneqq A_p$ and by means of Theorem 3.14, the group T is not the full Sylow s-subgroup of the alternating group. As T is an s-group, the group is nilpotent and by Theorem 3.9 we have $S \lneqq N_T(S)$. Thus, there exists an element $g \in N_T(S) \setminus S$ such that the order of g is a power of s. Further, the group $\langle G, g\rangle$ is a proper subgroup of A_p which has a larger Sylow s-subgroup than G which is not the full Sylow s-subgroup of A_p, namely the group $\langle S, g\rangle$.

To check whether the group $\langle G, g\rangle$ exists, the algorithm takes the following steps: For the input G, p and s it computes the alternating group A_p, a Sylow s-subgroup of G and its normalizer in the alternating group, namely $N_{A_p}(S)$. Then the algorithm computes the group $\langle G, g\rangle$ for each element $g \in N_{A_p}(S) \setminus S$, whose order is a power of s, and saves it in a list L. After the list L is completed, i.e. the `for` loop is done, the algorithm checks whether the groups in L are alternating by the GAP function `ForAll` with input L and the term `H` $\to$ `Size(H) = Size(A)`. If the boolean value of the `ForAll` function is `"true"`, meaning that each of the groups generated by G and an element g as above is alternating, the algorithm returns `"true"`. If there exists a group which is not the alternating group, then the `ForAll` function returns `"false"` and so does Algorithm 4. □

If Algorithm 4 returns `"true"` for each prime divisor s of $|G|$, then G is maximal in the corresponding alternating group, as there does not exist any group H with $G \leqslant H \lneqq A_p$ which has a larger Sylow s-subgroup than G and is not the alternating group itself.

3.3.2 Results

In this section we present the results of the computations using the algorithms recorded in Appendix A. The computations were carried out in the GAP Version 4.9.1. For each prime $p \in \{7, \ldots, 23\}$ we show the results of Algorithm 2 and the results of Algorithm 3 using the generators computed by Algorithm 2 and further, we test whether some of the groups are equal or subgroups of each other. The groups computed by these algorithms are all of the form $G = \langle a, b, c\rangle$ with a, b and c as described in the previous section. Thus for each prime p, the p-cycle $(1, \ldots, p)$ is always denoted by a and we refer to b and c as the second respectively the third generator of a group G.

The next two remarks show how the groups we compute with our algorithms relate to each other.

Remark 3.26 Let $p = 2q + 1,\ q \in \mathbb{N}$. Let $G = \langle a, b, c\rangle$ and $G' = \langle a, b, c'\rangle$ be two groups generated by Algorithm 3 for a fixed input $a = (1, \ldots, p)$ and $b \in N_{A_p}(\langle a\rangle)$. Further, let $|c| \mid |c'|$ and $(c')^s = c$ for some $s \in \mathbb{N}$. Then $G \leqslant G'$.

Remark 3.27 Let $p = 2q + 1,\ q \in \mathbb{N}$. Let $G = \langle a, b, c\rangle$ and $G' = \langle a, b', c\rangle$ be two groups generated by Algorithm 3 with input $a = (1, \ldots, p)$ and the element $b \in N_{A_p}(\langle a\rangle)$ respectively $b' \in N_{A_p}(\langle a\rangle)$. If $(b')^s = b$ for some $s \in \mathbb{N}$ then $G \leqslant G'$.

As Theorem 3.18 only states that a non-solvable transitive permutation group of prime degree contains the elements a, b and c but not that these elements always generate the whole group, we have to consider the fact that we do not compute all desired groups with our algorithms. To make sure that we do not miss any groups, we check for each resulting group G whether it is a maximal subgroup of the alternating group with the same degree with Theorem 3.13, Theorem 3.14 and Algorithm 4. Assuming that there exists a group H such that $G \leqslant H \lneqq A_p$, we estimate the order of H with both theorems. Further, for each common prime divisor of $|G|$ and some possible order of H, we check whether there exists a s-group in H which is larger than a Sylow s-subgroup of G but not the full Sylow s-subgroup of the alternating group using Algorithm 4. If there exists such a group for some prime divisor s, then the group G is not maximal in A_p. If for all s dividing $|G|$ the algorithm returns `"true"`, then G is maximal.

Degree 7

The list of the generators a and b computed by Algorithm 2 is already given in Example 3.24. Entering a and b into Algorithm 3, we obtain six sets of permutations generating groups isomorphic to $\mathrm{PSL}(3,2)$. The order of $N_{A_7}(\langle b\rangle)$ is 18, thus a third of all tested generating sets $\langle a,b,c\rangle$ satisfy the desired properties. As we have already seen in the example, most of the groups the algorithm has computed are equal. In conclusion, we obtain two groups isomorphic to $\mathrm{PSL}(3,2)$; in particular the groups $G_1 := \langle a,b,c_1\rangle$ and $G_2 := \langle a,b,c_2\rangle$, where

$$c_1 := (3,5)(6,7)$$

and

$$c_2 := (2,5)(6,7).$$

A quick test in GAP with the function `IsConjugate` shows that G_1 and G_2 are not conjugate in the symmetric group S_7.

Now we have to check if both resulting groups are maximal in A_7. We set $G := \mathrm{PSL}(3,2)$. Assume that there exists a group H such that $G \leqslant H \lneqq A_7$ and H is transitive on 7 elements. Then H is primitive and by Theorem 3.13 we obtain $|S_7 : H| \geqslant 4!$ and thus, we have $|H| \leqslant 7!/4! = 7\cdot 6\cdot 5$. Let $P := \langle a\rangle$. We have $|N_G(P)| = 7\cdot 3$ and as the alternating group A_7 does not contain a 6-cycle, the order of $N_H(P)$ is the same. Hence the order of H is of the form $|H| = 7\cdot 3\cdot (1+7n)$, where $(1+7n)$ is the number of Sylow 7-groups of H for some $n\in\mathbb{N}$ by the Sylow theorems. As $|G| = 168 = 7\cdot 3\cdot 8$ and the order of G divides the order of H, we obtain $|H| = 7\cdot 3\cdot 8u$ and $8u = (1+7n)$ for some $u\in\mathbb{N}$. Further, by the estimation of the order of H due to Borchert, we have $u \leqslant 2^2\cdot 5 = 20$ and additionally, we have $u \equiv 1 \pmod 7$.

As H is a subgroup of the alternating group A_7, the order of H divides $7!/2 = 7\cdot 5\cdot 3^2\cdot 2^3$. Since $7 = 3+4$, Theorem 3.14 implies that H contains no cycle of length 3 and thus the Sylow 3-subgroup of H must be a proper subgroup of the Sylow 3-subgroup of A_7, hence we have a further restriction of the order of H, namely $|H| \mid 7 \cdot 5 \cdot 3 \cdot 2^3$. As $|H| = |G|u$, this implies $u \mid 5$.

In summary we have the following restrictions for the value of u:

(1) $u \mid 5$;

(2) $u \leqslant 20$;

(3) $u \equiv 1 \pmod 7$.

The only integer satisfying all three requirements is $u = 1$. Thus $\mathrm{PSL}(3,2)$ is maximal in A_7 and so are the groups G_1 and G_2 computed by Algorithm 3.

Degree 11

As $q = (p-1)/2 = 5$ is prime, we obtain only one second generator from Algorithm 2, namely

$$b := (2, 5, 6, 10, 4)(3, 9, 11, 8, 7).$$

The normalizer of $\langle b \rangle$ in the alternating group of degree 11 contains exactly 100 elements. From the 100 groups which have been tested by Algorithm 3, we obtain a total of 30 groups which satisfy our conditions, where 20 of them are isomorphic to M_{11} and 10 are isomorphic to $\mathrm{PSL}(2,11)$. By checking the groups for equality using the GAP function `IsSubgroup`, we see that only two groups from each isomorphism type remain, i.e. we have the four groups $G_1 := \langle a, b, c_1 \rangle$, $G_2 := \langle a, b, c_2 \rangle$, $U_1 := \langle a, b, d_1 \rangle$ and $U_2 := \langle a, b, d_2 \rangle$, where

$$\begin{aligned} c_1 &:= (2, 5, 10, 6)(7, 8, 9, 11), \\ c_2 &:= (2, 5, 4, 10)(7, 11, 9, 8), \\ d_1 &:= (2, 10)(5, 6)(7, 9)(8, 11) \end{aligned}$$

and

$$d_2 := (2, 4)(5, 10)(7, 9)(8, 11).$$

The groups G_1 and G_2 are isomorphic to M_{11}, whereas the other two groups are isomorphic to $\mathrm{PSL}(2,11)$. Further, Remark 3.26 and the fact that $c_1^2 = d_1$

and $c_2^2 = d_2$, lead to the following relations:

$$U_1 \leqslant G_1 \text{ and } U_2 \leqslant G_2.$$

The groups U_1 and U_2 as well as G_1 and G_2 are not conjugate in the symmetric group S_{11}.

As U_1 and U_2 are subgroups of the groups isomorphic to M_{11} we only have to check G_1 and G_2 for maximality in A_{11}. Let $G := M_{11}$. Again, assume that there exists a group H such that $G \leqslant H \lneqq A_{11}$. Then H is primitive on 11 elements as a subgroup of the alternating group and by Theorem 3.13, we obtain $|S_{11} : H| \geqslant 6!$ and thus $|H| \leqslant 11!/6! = 11 \cdot 7 \cdot 5 \cdot 3^2 \cdot 2^4$. For $P := \langle a \rangle$ we have $|N_G(P)| = 11 \cdot 5$ and as A_{11} does not contain a 10-cycle, the order of the normalizer of P in H is the same. Hence we obtain $|H| = 11 \cdot 5 \cdot (1 + 11n)$, where $(1 + 11n)$ is the number of Sylow 11-subgroups of H for some $n \in \mathbb{N}$ due to the Sylow theorems. As the order of G divides the order of H there exists $u \in \mathbb{N}$ such that $|H| = |G|u$ and thus $|H| = 11 \cdot 5 \cdot 144u$, where $144u = (1 + 11n)$. By the estimation of the order of H above, we obtain $u \leqslant 7$ and further, we have $u \equiv 1 \pmod{11}$.

The group H is a subgroup of the alternating group of degree 11 and thus its order is a factor of $11!/2 = 11 \cdot 7 \cdot 5^2 \cdot 3^4 \cdot 2^7$. As $11 = 7 + 4 = 5 + 6 = 3 + 8$ we obtain a further restriction by Theorem 3.14 for the order of H, namely $|H| \mid 11 \cdot 5 \cdot 3^3 \cdot 2^7$. As the order of G is $7920 = 11 \cdot 5 \cdot 3^2 \cdot 2^4$, the number u must divide $3 \cdot 2^3 = 24$.

In summary, we obtain the following restrictions for the number u:

(1) $u \mid 24$;

(2) $u \leqslant 7$;

(3) $a \equiv 1 \pmod{11}$.

Again, we have only one possible value for u, that is $u = 1$. Thus the group M_{11} is maximal in A_{11} and so are the groups G_1 and G_2, which are isomorphic to M_{11}.

Degree 13

The results of Algorithm 2 regarding the second generator are

$$b_1 := (2,5,4,13,10,11)(3,9,7,12,6,8),$$
$$b_2 := (2,4,10)(3,7,6)(5,13,11)(8,9,12)$$

and

$$b_3 := (2,13)(3,12)(4,11)(5,10)(6,9)(7,8).$$

The corresponding normalizers in A_{13} have orders 72, 1944 and 23040. We obtain a total of 60 groups isomorphic to $\mathrm{PSL}(3,3)$ using Algorithm 3 with input a, b_2 and 13, hence only about 3% of the groups that have been checked by the algorithm yield a valid group. Apparently no results occur using b_1 and b_3 as second generators. For b_1 this result is not surprising as Theorem 3.18 states that there exists a prime ℓ dividing $|b_1| = 6$ such that there exists $\widetilde{b_1} \in \langle b_1 \rangle$ of order ℓ and a corresponding $c \in N_{A_{13}}(\langle \widetilde{b_1} \rangle) \backslash C_{A_{13}}(\langle \widetilde{b_1} \rangle)$ such that $\langle a, b_1, c \rangle$ is non-solvable. In this case we have $\ell = 3$ and $\widetilde{b_1} = b_2$. From the 60 groups only four groups remain after checking them for equality. Again, it suffices to test whether the groups are subgroups of each other by `IsSubgroup`. We have $G_1 := \langle a, b_2, c_1 \rangle$, $G_2 := \langle a, b_2, c_2 \rangle$, $G_3 := \langle a, b_2, c_3 \rangle$ and $G_4 := \langle a, b_2, c_4 \rangle$, where

$$c_1 := (3,9,13)(5,6,8)(7,12,11),$$
$$c_2 := (3,7)(4,10)(5,11)(8,9),$$
$$c_3 := (3,7)(4,10)(5,13)(8,12)$$

and

$$c_4 := (3,6)(4,10)(9,12)(11,13).$$

By using the GAP function `IsConjugate` we see that G_1 and G_2 as well as G_3 and G_4 are conjugate in S_{13}.

For the maximality of the groups we computed with Algorithm 3 in A_{13} we have to estimate the order of a group H such that $G \leqslant H \lneqq A_{13}$ for $G := \mathrm{PSL}(3,3)$. Assume that such group H exists. Then it is primitive on 13 elements and we obtain $|S_{13} : H| \leqslant 7!$ by Theorem 3.13. This yields

$|H| \leqslant 13!/7! = 13 \cdot 11 \cdot 5 \cdot 3^3 \cdot 2^6$. As A_{13} does not contain a 6-cycle nor a 12-cycle, we have $|N_H(P)| = |N_G(P)| = 13 \cdot 3$ for $P := \langle a \rangle$. The order of G, which is a factor of the order of H, is $5616 = 13 \cdot 3^3 \cdot 2^4$ and thus, the order of H has the following form: $|H| = 13 \cdot 3 \cdot 144u$ for some $u \in \mathbb{N}$. Further, $144u = 1 + 13n$ for $n \in \mathbb{N}$ and thus, we have $u \equiv 1 \pmod{13}$ and $u \leqslant 11 \cdot 5 \cdot 2^2 = 220$.

Additionally, the order of H divides the order of the group A_{13}, namely $13!/2 = 13 \cdot 11 \cdot 7 \cdot 5^2 \cdot 3^5 \cdot 2^9$ and as $13 = 7+6 = 5+8 = 3+10$, we obtain the following restriction: $|H| \mid 13 \cdot 11 \cdot 5 \cdot 3^4 \cdot 2^9$, implying $u \mid 11 \cdot 5 \cdot 3 \cdot 2^5 = 5280$ as $|H| = |G|u$.

Finally, we have three requirements on u:

(1) $u \mid 5280$;

(2) $u \leqslant 220$;

(3) $u \equiv 1 \pmod{13}$.

We obtain $u \in \{1, 40, 66\}$. If $u = 1$ there is nothing to prove. As the prime factors of G are $2, 3$ and 13 and 2 and 3 also are prime factors of 40 and 66, it suffices to use Algorithm 4 with input 2 and 3 for each G_i, $i = 1, 2, 3, 4$, computed by Algorithm 3. In all 8 cases the Algorithm returns `"true"` meaning there does not exist a group H such that $G \leqslant H \lneqq A_{13}$.

Degree 17

Here, we obtain three possible second generators from Algorithm 2. The results are

$$\begin{aligned} b_1 &:= (2,10,14,16,17,9,5,3)(4,11,6,12,15,8,13,7), \\ b_2 &:= (2,14,17,5)(3,10,16,9)(4,6,15,13)(7,11,12,8) \end{aligned}$$

and

$$b_3 := (2,17)(3,16)(4,15)(5,14)(6,13)(7,12)(8,11)(9,10).$$

Algorithm 3 computes a total of 176 generating sets which satisfy our requirements, where 28 of the groups obtained from the sets are isomorphic to

$\mathrm{PSL}(2,16)$, whereas 52 groups are isomorphic to $\mathrm{PSL}(2,16) \rtimes C_2$. The groups isomorphic to $\mathrm{PSL}(2,16) \rtimes C_4$ have the highest share; a total of 96 groups are isomorphic to $\mathrm{PSL}(2,16) \rtimes C_4$. It is worth mentioning that b_3 yields groups of every isomorphism type, whereas b_2 only generates groups isomorphic to $\mathrm{PSL}(2,16) \rtimes C_2$ and to $\mathrm{PSL}(2,16) \rtimes C_4$ and b_1 only is a generator of groups isomorphic to $\mathrm{PSL}(2,16) \rtimes C_4$. The orders of the corresponding normalizers $N_{A_{17}}(\langle b_1 \rangle)$, $N_{A_{17}}(\langle b_2 \rangle)$ and $N_{A_{17}}(\langle b_3 \rangle)$ are 256, 6144 and 5160960, hence there exists only a small amount of generating sets satisfying our requirements, comparing the numbers of the groups which have been returned by Algorithm 3 to the number of groups which actually have been tested. After having checked the groups of the same isomorphism type computed by Algorithm 3 for equality, we see that only two groups remain of each type. The groups isomorphic to $\mathrm{PSL}(2,16)$ are $U_1 := \langle a, b_3, c_1 \rangle$ and $U_2 := \langle a, b_3, c_2 \rangle$, where

$$c_1 := (2,3)(4,8)(5,13)(6,14)(7,10)(9,12)(11,15)(16,17)$$

and

$$c_2 := (2,3)(4,9)(5,12)(6,8)(7,14)(10,15)(11,13)(16,17).$$

Let

$$d_1 := (2,17)(3,16)(4,15)(5,14)(6,13)(7,12)(8,11)(9,10)$$

and

$$d_2 := (3,4)(5,14)(6,9)(7,12)(10,13)(15,16).$$

Then the two groups of isomorphism type $\mathrm{PSL}(2,16) \rtimes C_2$ are $H_1 := \langle a, b_2, d_1 \rangle$ and $H_2 := \langle a, b_2, d_2 \rangle$. At least, the groups isomorphic to $\mathrm{PSL}(2,16) \rtimes C_4$ are $G_1 := \langle a, b_1, e_1 \rangle$ and $G_2 := \langle a, b_1, e_2 \rangle$, where

$$e_1 := (2,4,17,15)(3,12,16,7)(5,13,14,6)(8,9,11,10)$$

and

$$e_2 := (2,4,14,6,17,15,5,13)(3,12,10,8,16,7,9,11).$$

Further, by means of Remark 3.26 and Remark 3.27 we obtain the following relations between these six groups:

$$U_2 \leqslant H_1 \leqslant G_1 \text{ and } U_1 \leqslant H_2 \leqslant G_2.$$

A quick check in GAP with the function `IsConjugate` shows that for each isomorphism type the two groups generated by our algorithm are not conjugate in the symmetric group of degree 17.

Due to the relations we just made out above, it suffices to show that G_1 and G_2 are maximal in A_{17}. Both groups are isomorphic to the group $G := \mathrm{PSL}(2,16) \ltimes C_4$. Assume that there exists H such that $G \leqslant H \lneqq A_{17}$. As H is a subgroup of A_{17} and the alternating group is primitive on 17 elements, so is H. Thus, by Theorem 3.13, we obtain $|S_{17} : H| \geqslant 9!$ and further, we have $|H| \leqslant 17!/9! = 17 \cdot 13 \cdot 11 \cdot 7 \cdot 5^2 \cdot 3^2 \cdot 2^8$. The order of G is $16320 = 17 \cdot 5 \cdot 3 \cdot 2^6$ and as A_{17} does not contain a 16-cycle, the order of $N_H(P)$ is equal to the order of $N_G(P)$ for $P := \langle a \rangle$, which is $17 \cdot 8$. We obtain $|H| = 17 \cdot 8 \cdot 120u$ for some $u \in \mathbb{N}$ such that $120u = 1 + 17n$ for $n \in \mathbb{N}$. In particular, we have $|H| = |G|u$ and by the restriction of $|H|$ due to Theorem 3.13, we get $u \leqslant 13 \cdot 11 \cdot 7 \cdot 5 \cdot 3 \cdot 2^2 = 60060$. Further, we have $u \equiv 1 \pmod{17}$.

As the order of H divides $17!/2 = 17 \cdot 13 \cdot 11 \cdot 7^2 \cdot 5^3 \cdot 3^5 \cdot 2^{14}$ and since $17 = 13 + 4 = 11 + 6 = 7 + 10 = 5 + 12 = 3 + 14$, Theorem 3.14 implies that the order of H divides $17 \cdot 7 \cdot 5^2 \cdot 3^5 \cdot 2^{14}$. With $|G|u = |H|$, we obtain $u \mid 7 \cdot 5 \cdot 3^4 \cdot 2^8 = 725760$. In conclusion, we have

(1) $u \mid 725760$;

(2) $u \leqslant 60060$;

(3) $u \equiv 1 \pmod{17}$.

With GAP we calculate all numbers sastisfying the three requirements and we obtain the following values

$$u \in \{1, 18, 35, 120, 256, 324, 630, 1344, 2160, 8960, 11340, 24192\}.$$

The common prime factors of $|G|$ and all possible values for u together are $2, 3$ and 5. Thus it suffices to check these primes together with the groups

G_1 and G_2 using Algorithm 4. For all cases, the algorithm returns `"true"` and thus, both groups are maximal in the alternating group A_{17}.

Degree 19

The second generators we obtain using Algorithm 2 are the permutations

$$b_1 := (2,5,17,8,10,18,12,7,6)(3,9,14,15,19,16,4,13,11)$$

and

$$b_2 := (2,8,12)(3,15,4)(5,10,7)(6,17,18)(9,19,13)(11,14,16).$$

In both cases, Algorithm 3 returns an empty list, which means that the algorithm does not find any transitive permutation groups of degree 19 which are non-solvable and proper subgroups of A_{19}. As we know from the results following from the CFSG, there are no non-solvable transitive permutation groups of degree 19 other than the alternating and symmetric groups of degree 19. Hence the output of Algorithm 3 agrees with the result obtained from the CFSG.

Degree 23

Algorithm 2 yields the permutation

$$b := (2,3,5,9,17,10,19,14,4,7,13)(6,11,21,18,12,23,22,20,16,8,15)$$

as second generator. Entering a and b, Algorithm 3 computes a total of 88 groups which are all isomorphic to the Mathieu group M_{23}. As the order of $N_{A_{23}}(\langle b\rangle)$ is 1210, approximately 7% of the generating sets which have been checked satisfy our requirements. Again we have checked whether the groups generated by the algorithm are subgroups of each other to exclude the sets which generate the same group. In the end, we obtain only two different groups isomorphic to M_{23}, namely $G_1 := \langle a,b,c_1\rangle$ and $G_2 := \langle a,b,c_2\rangle$, where

$$c_1 := (3,9,7,10,17)(4,5,19,14,13)(8,23,12,11,18)(15,16,21,22,20)$$

and

$$c_2 := (2, 7, 9, 14, 4)(5, 17, 13, 19, 10)(8, 23, 12, 11, 18)(15, 16, 21, 22, 20).$$

The two groups are not conjugate in the symmetric group S_{23}.

Now it remains to show that both resulting groups are maximal in A_{23}. We set $G := M_{23}$. We further assume that there exists a group H such that $G \leqslant H \lneqq A_{23}$. Then H is primitive on 23 elements due to the primitivity of the alternating group. By Theorem 3.13 we obtain $|S_{23} : H| \geqslant 12!$ and thus $|H| \leqslant 23!/12! = 23 \cdot 19 \cdot 17 \cdot 13 \cdot 11 \cdot 7^2 \cdot 5^2 \cdot 3^2 \cdot 2^9$. Further, we have $|G| = 10200960 = 23 \cdot 11 \cdot 7 \cdot 5 \cdot 3^2 \cdot 2^7$ and as A_{23} does not contain a 22-cycle, we have $|N_H(P)| = |N_G(P)| = 23 \cdot 11$ for $P := \langle a \rangle$. Additionally, there exists $u \in \mathbb{N}$ such that the order of H is $|H| = |G|u = 23 \cdot 11 \cdot 40320u$ and $40320u = 1 + 23n$ for some $n \in \mathbb{N}$ due to the Sylow theorems. Therefore, we obtain $u \leqslant 19 \cdot 17 \cdot 13 \cdot 7 \cdot 5 \cdot 3^3 \cdot 2^3 = 31744440$ and further, $u \equiv 1 \pmod{23}$.

As H is a subgroup of the alternating group A_{23}, the order of H divides $23!/2 = 23 \cdot 19 \cdot 17 \cdot 13 \cdot 11^2 \cdot 7^3 \cdot 5^4 \cdot 3^9 \cdot 2^{18}$. We have

$$23 = 19 + 4 = 17 + 6 = 13 + 10 = 11 + 12 = 7 + 16 = 5 + 18 = 3 + 20.$$

Thus Theorem 3.14 implies that the Sylow s-subgroup of H is a proper subgroup of the Sylow s-subgroup of A_{23} for all $s \in \{3, 5, 7, 11, 13, 17, 19\}$. Then we obtain $|H| \mid 23 \cdot 11 \cdot 7^2 \cdot 5^3 \cdot 3^8 \cdot 2^{18}$ and finally, the number u is a divisor of $7 \cdot 5^2 \cdot 3^6 \cdot 2^{11} = 261273600$.

In summary, we have

(1) $u \mid 261273600$;

(2) $u \leqslant 31744440$;

(3) $u \equiv 1 \pmod{23}$.

With GAP we calculate the possible values for u and we obtain

$$u \in \{1, 24, 70, 162, 300, 576, 1680, 2025, 2048, 3888, 7200, 11340, 13824, 25600, \\ 40320, 48600, 93312, 172800, 272160, 967680, 1166400, 4147200, 6531840\}.$$

The common prime factors of $|G|$ and all possible values for u are $2, 3, 5$ and 7, thus it suffices to check the maximality of G_1 and G_2 using Algorithm 4 with these primes as input. The result of all runs of the algorithm is `true` and thus both groups are maximal in the alternating group A_{23}.

Regarding the present results from our computations it is conspicuous that for each degree $p \in \{7, 11, 13, 17, 23\}$ only two groups of the same isomorphism type remain after checking all computed groups for equality. The results agree with the fact that alternating group of each degree p has two conjugacy classes of the maximal subgroups isomorphic to the groups we computed, which can be checked with GAP. Thus, the groups listed in the subsections above are representatives of the two conjugacy classes.

3.4 An alternative using tables of marks

In this section we discuss an alternative method to compute transitive permutation groups of degree at most 13. This method also does not use the classification of finite simple groups. Recall that every permutation group on the finite set $\Omega = \{1, \ldots, n\}$ is isomorphic to a subgroup of the symmetric group S_n. The basic idea of this method is to use the table of marks of S_n to obtain a set of representatives for the conjugacy classes of subgroups of S_n and then to check whether the representative is transitive on Ω or not. This approach is rather naive and, since the table of marks of a symmetric group is only precomputed up to a degree of 13 (in GAP, Version 4.9.1), it is not very useful for an attempt to classify transitive permutation groups in general. Nevertheless, it covers the transitive permutation groups of small degree and in particular the groups of small prime degree $p \in \{5, 7, 11, 13\}$. The computation can be carried out in the computer algebra system GAP or any other computer algebra system containing a library of table of marks.

First, we give a short introduction to tables of marks. Since it is not the purpose of this section to go in-depth we refer to [5] or [24] for more information on this matter. The concept of a table of marks was first introduced by Burnside in the second edition of his book [5, Chapter XII, Section 180]. The table of marks of a finite group G describes the partially ordered set of all conjugacy classes of subgroups of G.

Definition 3.28 Let G be a finite group.

(1) Let Ω be a finite G-set and let U be a subgroup of G. The *mark* $\beta_\Omega(U)$ of U on Ω is defined as

$$\beta_\Omega(U) = |\mathrm{Fix}_\Omega(U)|,$$

where $\mathrm{Fix}_\Omega(U)$ is the set of fixed points of the subgroup U on Ω.

(2) The *table of marks* of G is the square matrix

$$M(G) = (\beta_{G_i \setminus G}(G_j))_{i,j},$$

where $G_i \setminus G = \{G_i g \mid g \in G\}$ and both G_i and G_j run through a system of representatives of the conjugacy classes of subgroups of G.

Recall that for each subgroup U of G, the group G acts transitively on the set of right cosets of U via right multiplication. Therefore, the quotients $G_i \setminus G$ mentioned in Definition 3.28(2) are transitive G-sets.

Remark 3.29 ([24]) If Ω and Λ are isomorphic G-sets of a group G, we have $\beta_\Omega(U) = \beta_\Lambda(U)$ for all $U \leqslant G$. Moreover, the marks of U and its conjugate U^g are equal for all $U \leqslant G$.

The table of marks of a group G encodes a lot of its properties, in particular with respect to its subgroups. For instance we obtain access to the subgroup lattice of G through the group's table of marks. Here, it is important to note, that in [24] Pfeiffer introduces a way to calculate the table of marks of a group G without knowing the whole subgroup lattice of G.

Lemma 3.30 *Let G be a group, and let G_i and G_j be representatives of two distinct conjugacy classes of subgroups of G. Then $\beta_{G_i \setminus G}(G_j) \neq 0$ if and only if G_i contains a conjugate of G_j.*

Proof. If $\beta_{G_i \setminus G}(G_j) \neq 0$, there exists an element $g \in G$ such that $G_i g x = G_i g$ for all $x \in G_j$. Hence $g x g^{-1} \in G_i$ for all $x \in G_j$. Then $g G_j g^{-1} \leqslant G_i$.
If $g G_j g^{-1} \leqslant G_i$, then $g x g^{-1} \in G_i$ for all $x \in G_j$. Hence we get $G_i g x g^{-1} = G_i$

and therefore $G_i g x = G_i g$ for all $x \in G_j$. Then $G_i g \in \mathrm{Fix}_{G_i \backslash G}(G_j)$ and in particular, $\beta_{G_i \backslash G}(G_j) \geqslant 1$. $\square$

Other properties of the table of marks of a group G are listed in the following lemma. Here, we assume that the conjugacy classes of subgroups of G are arranged ascendingly by their orders in the table.

Lemma 3.31 ([24]) *Let $U,\ V \leqslant G$ be subgroups of G. Then the following statements hold:*

(1) The first entry of each row of $M(G)$ is the index of the corresponding subgroup, i.e.

$$\beta_{U \backslash G}(\{\mathrm{id}_G\}) = |G : U|.$$

(2) The diagonal entry is the index of U in its normalizer in G, i.e.

$$\beta_{U \backslash G}(U) = |N_G(U) : U|.$$

(3) The length of the conjugacy class $[U]$ of U is given by

$$|[U]| = |G : N_G(U)| = \frac{\beta_{U \backslash G}(\{\mathrm{id}_G\})}{\beta_{U \backslash G}(U)}.$$

(4) The number of conjugates of U that contain V is given by

$$|\{U^g \mid g \in G,\ V \leqslant U^g\}| = \frac{\beta_{U \backslash G}(V)}{\beta_{U \backslash G}(U)}.$$

Example 3.32 Table 3.1 provides an example of a table of marks $M(S_4)$ for the symmetric group S_4. The 11 conjugacy classes of subgroups of S_4 are denoted by $\{\mathrm{id}_{S_4}\}$, C_2, C_2*, C_3, D_4, C_4, D_4*, S_3, D_8, A_4 and S_4, where $C_2 = \langle(1,3)\rangle$ and $C_2* = \langle(1,3)(2,4)\rangle$ are the subgroups of order 2, and $D_4 = \langle(1,3),(1,3)(2,4)\rangle$ and $D_4* = \langle(1,2)(3,4),(1,3)(2,4)\rangle$ are the subgroups of order 4. The other subgroups of S_4 are denoted as usual.
As Lemma 3.30 states, we can read off the subgroup lattice of S_4 from $M(S_4)$ by looking at the non-zero entries of the table. For instance we see that $\{\mathrm{id}_{S_4}\}$, C_2*, C_3, D_4* and A_4 are subgroups of the alternating group A_4. Further, we obtain the index of every subgroup, respectively its conjugate,

Table 3.1: Table of marks $M(S_4)$

	$\{\mathrm{id}_{S_4}\}$	C_2*	C_2	C_3	D_4*	C_4	D_4	S_3	D_8	A_4	S_4
$\{\mathrm{id}_{S_4}\} \setminus S_4$	24										
$C_2 * \setminus S_4$	12	4									
$C_2 \setminus S_4$	12	.	4								
$C_3 \setminus S_4$	8	.	.	2							
$D_4 * \setminus S_4$	6	6	.	.	6						
$C_4 \setminus S_4$	6	2	.	.	.	2					
$D_4 \setminus S_4$	6	2	2	.	.	.	2				
$S_3 \setminus S_4$	4	.	2	1	.	.	.	1			
$D_8 \setminus S_4$	3	3	1	.	3	1	1	.	1		
$A_4 \setminus S_4$	2	2	.	2	2	.	.	.	.	2	
$S_4 \setminus S_4$	1	1	1	1	1	1	1	1	1	1	1

in G from the first entries of each row. To give an example, the index of C_3 in S_4 is $|S_4 : C_3| = 8$, which is equal to $M(S_4)_{4,1}$.

The most basic idea to compute all transitive permutation groups of prime degree $p \in \{4, \dots, 13\}$ is to derive all subgroups of S_p and to check whether they are transitive.

As conjugate groups are permutationally equivalent by Lemma 2.10, it suffices to examine a representative of each conjugacy class of the subgroups of S_p. The library of table of marks provides several functions to determine these representatives. The GAP code using these functions to obtain the transitive permutation groups of degrees 4 to 13 is recorded in Appendix B.

Theorem 3.33 *Algorithm 5 terminates and computes a list of representatives of all transitive permutation groups for a given degree $n \in \{4, \dots, 13\}$.*

Proof. Since S_n is finite, the table of marks and the number of subgroups of S_n is finite as well. Therefore, the algorithm terminates. For $n < 4$ and $n > 13$, there is nothing to prove. For $n \in \{4, \dots, 13\}$ the function `GeneratorsSubgroupsTom` in line 8 returns a list of length two. The first entry contains a list L of all possible generators of the representatives of the conjugacy classes of subgroups, whereas the second entry is a list containing at position i a list of positions in L of generators of a representative in class i. An example is given in Example 3.34. In the `for` loop iterating over the conjugacy classes contained in the second entry, the code generates a representative for each conjugacy class of the subgroups of S_n by constructing a group from the generators. Having generated a representative U, the algorithm checks whether it is transitive on $\{1, \ldots, n\}$ via `IsTransitive(U,[1..n])` in line 18. If the boolean value of `IsTransitive` is `"true"`, the representative U is added to a list, which is the output of the algorithm. As U is permutationally equivalent to all its conjugates, the list is complete at the end of the `for` loop. In summary, Algorithm 5 returns a list of representatives of all transitive permutation groups of degree n and thus the claim follows. □

Example 3.34

```
gap> s4 := SymmetricGroup(4);
gap> tom := TableOfMarks(s4);
TableOfMarks(Sym([1..4]))
gap> generators := GeneratorsSubgroupsTom(tom);
[[(3,4),(2,3,4),(1,2),(1,2)(3,4),(1,3)(2,4),(1,3,2,4),(1,2,3,4),
(1,2)], [[],[4],[1],[2],[4,5],[1,3],[4,6],[2,1],[1,3,5],[4,5,2],
[7,8]]]
```

The next example shows that the output of Algorithm 5 is equal to the output of the known GAP function using the CFSG constructed by Hulpke in [15].

Example 3.35

```
gap> L := TransitiveGroupsViaMarks(4);
[Group([(1,2)(3,4),(1,3)(2,4)]), Group([(1,2)(3,4),(1,3,2,4)]),
Group([(3,4),(1,2),(1,3)(2,4)]),
Group([(1,2)(3,4),(1,3)(2,4),(2,3,4)]),
Group([(1,2,3,4),(1,2)])]
gap> NrTransitiveGroups(4);
5
gap> M := List([1..5], x -> TransitiveGroup(4,x));
[C(4)=4; E(4) = 2[x]2, D(4), A4, S4]
gap> List(L, StructureDescription);
["C2 x C2", "C4", "D8", "A4", "S4"]
```

```
gap> List(M, StructureDescription);
["C4", "C2 x C2", "D8", "A4", "S4"]
```

Appendix A

Transitive groups via normalizer

This appendix serves to record the GAP codes of the algorithms used to compute the non-solvable transitive permutation groups of small prime degrees which are proper subgroups of the corresponding alternating groups. For an explanation of the individual GAP functions used in the codes we refer to [10].

Since we require the groups to be subgroups of the alternating group, we have to check that only even permutations are used. Thus, Algorithm 1 checks if a given object is an even permutation.

input : An object g.
output: True, if g is an even permutation; false, if g is neither a permutation nor an odd permutation.

```
IsEvenPerm := function(g)
if IsPerm(g) = true and SignPerm(g) = 1 then
      return true;
else
      return false;
fi;
end;
```

Algorithm 1: Check for even permutations

input : A prime number $p \geqslant 3$.
output: A list, where the first entry is the p-cycle $a = (1, \dots, p)$ and the second entry is a list of permutations $[b_1, \dots, b_n]$, where $b_i \in N_{A_p}(\langle a \rangle)$ for all $1 \leqslant i \leqslant n$.

```
ComputationOfGenerators := function(p)
local q, res, a, P, A, N, C, K, L, gens, i, g;
if p = 2 or not IsPrimeInt(p) then
    return "Wrong input!";
fi;
q := (p - 1)/2;
a := PermList(Concatenation([2 .. p],[1])); # returns p-cycle (1,..,p)
P := Group(a);
A := AlternatingGroup(p);
N := Normalizer(A,P);
C := ComplementClassesRepresentatives(N,P); # list of
  representatives of conjugacy classes of complements of P in N
K := C[1]; # C contains only a single group by Schur-Zassenhaus
gens := GeneratorsOfGroup(K);
for i in [1..Length(gens)] do # search for a generator of order q
    if Order(gens[i]) = q then
        g := gens[i];
    fi;
od;
L := ShallowCopy(DivisorsInt(q)); # mutable list of all divisors of q
Remove(L); # removes the last entry of the list L, which is q, as
  g^q = id
res := List(L, x -> g^x);
return [a, res];
end;
```

Algorithm 2: Algorithm to compute the elements a and b

input : The p-cycle $a = (1, \dots p)$, a permutation $b \in N_{A_p}(\langle a \rangle)$ and the corresponding prime number p.

output: A list of all subgroups of A_p which are generated by elements a, b and c as in Theorem 3.18.

```
TransitiveGroupsViaNormalizer := function(a, b, p)
local res, g, G, N, A, B;
 # check if input a, b, p is correct
if not IsPrimeInt(p) or p = 2 then
    return "Wrong input for p!";
fi;
if not IsEvenPerm(a) then
    return "Wrong input for a!";
fi;
if not IsEvenPerm(b) then
    return "Wrong input for b!";
fi;
res := [];
A := AlternatingGroup(p);
B := Group(b);
N := Normalizer(A, B);
for g in N do # iteration over all elements of N_A(B)
    G := Group(a, b, g);
    if Size(G) <> Size(A) then # check if G ≠ A_p
        if not IsSolvable(G) then
            # check if G is non-solvable
            Add(res, G);
        fi;
    fi;
od;
return res;
end;
```

Algorithm 3: Algorithm to determine all subgroups of A_p which are generated by a, b and c as in Theorem 3.18

input : A group G generated by Algorithm 3, its prime degree p and a prime s dividing the order of G

output: True, if there exists no group $G \leqslant H \lneqq A_p$ with a larger Sylow s-subgroup than G other than the alternating group; false, if there exists a group H such that $G \leqslant H \lneqq A_p$

```
IsMaximalInAlternatingGroup := function(G, p, s)
local A, S, N, L, g, H, o, gens;
if not IsGroup(G) or not IsPrimeInt(p) or not IsPrimeInt(s) then
    return "Wrong input!";
fi;
L := [];
A := AlternatingGroup(p);
S := SylowSubgroup(G, s);
N := Normalizer(A, S);
for g in N do
    if not g in S then # S is a proper subgroup of N
        o := Order(g);
        if IsPrimePowerInt(o) and s in PrimeDivisors(o) then
          # g lies in Sylow s-subgroup of A
            gens := ShallowCopy(GeneratorsOfGroup(G));
            Add(gens, g);
            H := Group(gens);
              # potential group between G and A
            Add(L, H);
        fi;
    fi;
od;
if ForAll(L, H -> Size(H) = Size(A)) then
    return true; # there exists no group between G and A
else
    return false;
      # there exists a group between G and H with larger Sylow
      s-subgroup than G
fi;
end;
```

Algorithm 4: Algorithm to check whether a group generated by Algorithm 3 is maximal in the alternating group

Appendix B

Transitive groups via marks

In this appendix we introduce the GAP code using tables of marks to compute representatives of all transitive permutation groups of prime degree from 5 up to 13. For an explanation of individual GAP functions used in the code we refer to [10]. The code can also be used to compute transitive groups of composite degree from 4 to 13 as it does not distinguish between primes and composite numbers.

input : An integer $n \in \{4, \ldots, 13\}$.
output: A list of representatives of all transitive permutation groups of degree n.

```
TransitiveGroupsViaMarks := function(n)
local tom, generators, elements, classes, G, temp, L, res, i, j;
if n > 13 or n < 4 then
      return "Wrong input!";
fi;
res := [];
if n = 4 then
      tom := TableOfMarks(SymmetricGroup(4));
        # GeneratorsSubgroupsTom("S4") returns intransitive
        representatives of the conjugacy classes of subgroups, hence we
        can not use the precomputed table of marks of S_4
else
      tom := TableOfMarks(Concatenation("S", String(n)));
        # retrieve the precomputed table of marks
fi;
generators := GeneratorsSubgroupsTom(tom);
elements := generators[1];
  # a list of all possible generators of the representatives of the
  conjugacy classes of subgroups
classes := generators[2];
  # a list, where at position i there is a list of positions in elements,
  which generate the representative of the ith conjugacy class
for i in [2..Length(classes)] do
        # computation of each representative of conjugacy classes of
        subgroups of S_n except for {id_{S_n}}
      temp := classes[i];
      L := [];
      for j in [1..Length(temp)] do
            Add(L, elements[temp[j]]);
              # generating set of representative of current conjugacy
              class
      od;
      G := Group(L);
      if IsTransitive(G,[1..n]) then # check if G is transitive
            Add(res, G);
      fi;
od;
return res;
end;
```

Algorithm 5: Transitive groups of degree up to 13 using table of marks

Bibliography

[1] P. T. Bateman, R. M. Stemmler, Waring's problem for algebraic number fields and primes of the form $(p^r - 1)/(p^d - 1)$, Illinois J. Math. 6 (1962), 142–156.

[2] S. Bosch, *Algebra*, Springer-Verlag, Berlin, Heidelberg, 1996.

[3] R. Brauer, On permutation groups of prime degree and related classes of groups, Ann. of Math. (2) 44, (1943), 57–79.

[4] F. Buekenhout, P. Cara, K. Vanmeerbeek, Geometries of the group PSL(2,11). Special issue dedicated to Helmut R. Salzmann on the occasion of his 70th birthday, Geom. Dedicata 83 (2000), 169–206.

[5] W. Burnside, *Theory of groups of finite order*, second edition, Cambridge University Press, 1911.

[6] P. J. Cameron, *Permutation groups*, London Mathematical Society Student Texts, 45, Cambridge University Press, Cambridge, 1999.

[7] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985.

[8] K. D. Fryer, A class of permutation groups of prime degree, Canad. J. Math. 7, (1955), 24-34.

[9] E. Galois, A. R. Singh, *The last mathematical testament of Galois*, https://www.ias.ac.in/article/fulltext/reso/004/10/0093-0100 (retrieved August 2018).

[10] The GAP Group, *GAP - Groups, Algorithms, and Programming*, Version 4.8.10, 2018, (http://gap-system.org).

[11] E. Giannelli, K. J. Lim, M. Wildon, Sylow subgroups of symmetric and alternating groups and the vertex of $S^{(kp-p,1^p)}$ in characteristic p, J. Algebra 455 (2016), 358–385.

[12] R. M. Guralnick, Subgroups of prime power index in a simple group, J. Algebra 81 (1983), 304–311.

[13] M. Hall Jr., *The theory of groups*, The Macmillan Company, New York, 1959.

[14] M. Hall Jr., *Combinatorial theory*, Second edition, Wiley-Interscience Series in Discrete Mathematics, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1986.

[15] A. Hulpke, Constructing transitive permutation groups, J. Symbolic Comput. 39 (2005), 1–30.

[16] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, Heidelberg, New York, 1967.

[17] B. Huppert, N. Blackburn, *Finite groups III*, Springer-Verlag, Berlin, Heidelberg, New York, 1982.

[18] A. Lucchini, F. Menegazzo, M. Morigi, On the existence of a complement for a finite simple group in its automorphism group, Illinois J. Math. 47 (2003), 395–418.

[19] P. Martín, D. Singerman, The geometry behind Galois' final theorem, European J. Combin. 33 (2012), 1619–1630.

[20] G. A. Miller, Limits of the degree of transitivity of substitution groups, Bull. Amer. Math. Soc. 22 (1915), 68–71.

[21] P. Müller, Permutation groups of prime degree, a quick proof of Burnside's theorem, Arch. Math. (Basel) 85 (2005), 15–17.

[22] P. M. Neumann, Transitive permutation groups of prime degree, Proceedings of the Second International Conference on the Theory of Groups (Australian Nat. Univ., Canberra, 1973), pp. 520–535, Lecture Notes in Math., Vol. 372, Springer, Berlin, 1974.

[23] E. T. Parker, P. J. Nikolai, A search for analogues of the Mathieu groups, Math. Tables Aids Comput. 12 (1958), 38–43.

[24] G. Pfeiffer, The subgroups of M_{24} or, how to compute the table of marks of a finite group, Experiment. Math. 6 (1997), 247–270.

[25] B. Sambale, *Endliche Permutationsgruppen*, Springer Spektrum, 2017.

[26] J. H. van Lint, *Introduction to coding theory*, Second edition, Graduate Texts in Mathematics, 86, Springer-Verlag, Berlin, 1992.

[27] R. A. Wilson, *The finite simple groups*, Graduate Texts in Mathematics, 251, Springer-Verlag, London, Ltd., London, 2009.

Statutory Declaration in Lieu of an Oath

I hereby declare in lieu of an oath that I have completed the present Master thesis independently and without illegitimate assistance from third parties. I have used no other than the specified sources and aids. In case that the thesis is additionally submitted in an electronic format, I declare that the written and electronic versions are fully identical. The thesis has not been submitted to any examination body in this, or similar, form.

Place, Date	Signature