Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)
Vol. XII (2013), 369-438

Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials

PETER MÜLLER

Abstract. We classify the finite primitive permutation groups which have a cyclic subgroup with two orbits. This extends classical topics in permutation group theory, and has arithmetic consequences. By a theorem of C. L. Siegel, affine algebraic curves with infinitely many integral points are parametrized by rational functions whose monodromy groups have this property. We classify the possibilities for these monodromy groups, and we give applications to Hilbert's irreducibility theorem.

Mathematics Subject Classification (2010): 12E25 (primary); 20B15, 12E05, 12F12, 14H30 (secondary).

Contents

1. Introduction

The aim of this paper is twofold: first, it provides the group-theoretic and arithmetic classification results needed to obtain sharpenings of Hilbert's irreducibility theorem, like the following:

Theorem 1.1. *Let $f(t, X) \in \mathbb{Q}(t)[X]$ be an irreducible polynomial with Galois group G, where G is a simple group not isomorphic to an alternating group or C_2. Then $\mathrm{Gal}(f(\bar{t}, X)/\mathbb{Q}) = G$ for all but finitely many specializations $\bar{t} \in \mathbb{Z}$.*

More results of this kind are given in Section 6. The second purpose is to obtain a group-theoretic classification result, namely to determine those primitive permutation groups which contain a cyclic subgroup with only two orbits. This classification completes and generalizes previous results about permutation groups. The list of possibilities is quite long and involved, we give it in Section 3.2.

In the following we explain how these seemingly unrelated topics are connected. Let k be a field of characteristic 0, and $f(X) \in k[X]$ be a functionally indecomposable polynomial. Let t be transcendental over k, and be A the Galois

Received December 7, 2010; accepted August 22, 2011.

group of $f(X)-t$ over $k(t)$, considered as a permutation group by its action on the roots of $f(X)-t$. It is easy to see that this group action is primitive. Furthermore, A contains a transitive cyclic subgroup I, the inertia group of a place of the splitting field of $f(X)-t$ over the place $t \mapsto \infty$. By classical theorems of Schur and Burnside, it is known that a primitive permutation group A with a transitive cyclic subgroup is either doubly transitive, or a subgroup of the affine group $\mathrm{AGL}_1(p)$ for a prime p. Using the classification of the doubly transitive groups, which rests on the knowledge of the finite simple groups, these groups have been determined, see [13, Theorem 4.1], [25]. Furthermore, if k is algebraically closed, then one can determine the subset of these groups which indeed are Galois groups as above, see [45], which completes (and corrects) [12]. Besides the alternating, symmetric, cyclic and dihedral groups only finitely many cases arise. For applications of these results see [15,26,47,49].

A more general situation arises if one considers Hilbert's irreducibility theorem over a number field k. Let $\mathcal{O}_k$ be the integers of k, and $f(t, X) \in k(t)[X]$ an irreducible polynomial. Then $f(\bar{t}, X)$ is irreducible over k for infinitely many integral specializations $\bar{t} \in \mathcal{O}_k$. Using Siegel's deep theorem about algebraic curves with infinitely many integral points, one can, to some extent, describe the set $\mathrm{Red}_f(\mathcal{O}_k)$ of those specializations $\bar{t} \in \mathcal{O}_k$ such that $f(\bar{t}, X)$ is defined and reducible. There are finitely many rational functions $g_i(Z) \in k(Z)$, such that $|g_i(k) \cap \mathcal{O}_k| = \infty$ and $\mathrm{Red}_f(\mathcal{O}_k)$ differs by finitely many elements from the union of the sets $g_i(k) \cap \mathcal{O}_k$. Thus, in order to get refined versions of Hilbert's irreducibility theorem, one has to get information about rational functions $g(Z)$ which assume infinitely many integral values on k, see [48]. We call such a function a *Siegel function*. A theorem of Siegel shows that a Siegel function has at most two poles on the Riemann sphere $\mathbb{P}^1(\mathbb{C})$. Suppose that $g(Z)$ is functionally indecomposable, and let A be the Galois group of the numerator of $g(Z)-t$ over $k(t)$. It follows that A is primitive on the roots of $g(Z)-t$, and the information about the poles of $g(Z)$ yields a cyclic subgroup I of A such that I has at most two orbits.

This generalizes the situation coming from the polynomials, where I has just one orbit. In the two-orbit situation not much was known. There is a result by Wielandt [61] (see also [62, V.31]), if the degree of A is $2p$ for a prime p, and both orbits of I have length p. Then A is either doubly transitive, or $2p-1$ is a square, and a point stabilizer of A has three orbits of known lengths. Another case which has been dealt with is that I has two orbits of relatively prime lengths $i < j$. If $i > 1$, then a classical result by Marggraf [62, Theorem 13.5] immediately shows that A contains the alternating group in its natural action. The more difficult case $i = 1$ was treated in [46]. In Section 3 we classify the primitive groups with a cyclic two-orbits subgroup without any condition on the orbit lengths.

As in the polynomial case, we again want to know which of these groups indeed are Galois groups of $g(Z)-t$ over $k(t)$, with $g(Z)$ a Siegel function as above. This amounts to finding genus 0 systems (to be defined later) in normal subgroups of A, see Section 4.1. As a result, we obtain a complete list of monodromy groups of rational function $g(Z) \in k(Z)$ which have at most two poles on $\mathbb{P}^1(\bar{k})$, where $\bar{k}$ denotes the algebraic closure of the characteristic 0 field k. See Theorem 4.8. Note that Laurent polynomials share this property, so in particular we obtain a classification of their monodromy groups too.

Finally, for applications to Hilbert's irreducibility theorem over the rationals, we classify the Galois groups of $g(Z) - t$ over $\mathbb{Q}(t)$ of those rational functions $g(Z) \in \mathbb{Q}(Z)$ with $|g(\mathbb{Q}) \cap \mathbb{Z}| = \infty$. Section 5 is devoted to that. In contrast to the other mostly group-theoretic sections, we need several arithmetical and computational considerations related to the regular inverse Galois problem over $\mathbb{Q}(t)$.

2. Permutation groups – Notation and some results

Here we collect definitions and easy results about finite groups and finite permutation groups, which are used throughout the work.

General notation: For a, b elements of a group G set $a^b := b^{-1}ab$. Furthermore, if A and B are subsets of G, then A^b, a^B and A^B have their obvious meaning. If H is a subgroup of G, then for a subset S of G let $C_H(S)$ denote the centralizer of S in H and $N_H(S)$ denote the normalizer $\{h \in H \mid S^h = S\}$ of S in H.
If $A, B, \dots$ is a collection of subsets or elements of G, then we denote by $<A, B, \dots>$ the group generated by these sets and elements.
The order of an element $g \in G$ is denoted by $\mathrm{ord}(g)$.

Permutation groups: Let G be a permutation group on a finite set Ω. Then $|\Omega|$ is the *degree* of G. We use the exponential notation ω^g to denote the image of $\omega \in \Omega$ under $g \in G$. The stabilizer of ω in G is denoted by G_ω. If G is transitive and G_ω is the identity subgroup, then G is called *regular*.
The number of fixed points of g on Ω will be denoted by $\chi(g)$.
Let G be transitive on Ω of degree ≥ 2, and let G_ω be the stabilizer of $\omega \in \Omega$. Then the number of orbits of G_ω on Ω is the *rank* of G. In particular, the rank is always ≥ 2, and exactly 2 if and only if the group is doubly transitive. The *subdegrees* of G are defined as the orbit lengths of G_ω on Ω.
Let G be transitive on Ω, and let Δ be a nontrivial subset of Ω. Set $S := \{\Delta^g \mid g \in G\}$. We say that Δ is a *block* of G if S is a partition of Ω. If this is the case, then S is called a *block system* of G. A block (or block system) is called trivial if $|\Delta| = 1$ or $\Delta = \Omega$. If each block system of G is trivial, then G is called *primitive*. Primitivity of G is equivalent to maximality of G_ω in G. Note that the orbits of a normal subgroup N of G constitute a block system, thus a normal subgroup of a primitive permutation group is either trivial or transitive.

Specific groups: We denote by C_n and D_n the cyclic and dihedral group of order n and $2n$, respectively. If not otherwise said, then C_n and D_n are regarded as permutation groups in their natural degree n action. The alternating and symmetric group on n letters is denoted by $\mathcal{A}_n$ and $\mathcal{S}_n$, respectively.
We write $\mathcal{S}(M)$ for the symmetric group on a set M.
Let $m \geq 1$ be an integer, and q be a power of the prime p. Let $\mathbb{F}_q$ be the field with q elements. We denote by $\mathrm{GL}_m(q)$ (or sometimes $\mathrm{GL}_m(\mathbb{F}_q)$) the general linear group of $\mathbb{F}_q^m$, and by $\mathrm{SL}_m(q)$ the special linear group. Regard these groups as acting on $\mathbb{F}_q^m$. The group $\Gamma := \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ acts componentwise on

$\mathbb{F}_q^m$. This action of Γ normalizes the actions of $\mathrm{GL}_m(q)$ and $\mathrm{SL}_m(q)$. We use the following symbols for the corresponding semidirect products: $\Gamma\mathrm{L}_m(q) := \langle \mathrm{GL}_m(q), \Gamma\rangle = \mathrm{GL}_m(q) \rtimes \Gamma$, $\Sigma\mathrm{L}_m(q) := \langle \mathrm{SL}_m(q), \Gamma\rangle = \mathrm{SL}_m(q) \rtimes \Gamma$. Note that if $q = p^e$ then we have the natural inclusion $\Gamma\mathrm{L}_m(q) \leq \mathrm{GL}_{me}(p)$.
Let G be a subgroup of $\Gamma\mathrm{L}_m(q)$, and denote by N the action of $\mathbb{F}_q^m$ on itself by translation. Then G normalizes the action of N. If $G = \mathrm{GL}_m(q)$, $\mathrm{SL}_m(q)$, $\Gamma\mathrm{L}_m(q)$, or $\Sigma\mathrm{L}_m(q)$, then denote the semidirect product of G with N by $\mathrm{AGL}_m(q)$, $\mathrm{ASL}_m(q)$, $\mathrm{A\Gamma L}_m(q)$, or $\mathrm{A\Sigma L}_m(q)$, respectively. A group A with $N \leq A \leq \mathrm{A\Gamma L}_m(q)$ is called an *affine permutation group*.
Let $G \leq \Gamma\mathrm{L}_m(q)$ act naturally on $V := \mathbb{F}_q^m$. We denote by $\mathbb{P}^1(V)$ the set of one–dimensional subspaces of V. As G permutes the elements in $\mathbb{P}^1(V)$, we get an (in general not faithful) action of G on $\mathbb{P}^1(V)$. The induced faithful permutation group on $\mathbb{P}^1(V)$ is named by prefixing a P in front of the group name, so we get the groups $\mathrm{PGL}_m(q)$, $\mathrm{PSL}_m(q)$, $\mathrm{P\Gamma L}_m(q)$, or $\mathrm{P\Sigma L}_m(q)$, respectively.
The group $\mathrm{GL}_m(q)$ contains, up to conjugacy, a unique cyclic subgroup which permutes regularly the non–zero vectors of $\mathbb{F}_q^m$. This group, and also its homomorphic image in $\mathrm{PGL}_m(q)$, is usually called *Singer group*. Existence of this group follows from the regular representation of the multiplicative group of $\mathbb{F}_{q^m}$ on $\mathbb{F}_{q^m} \cong \mathbb{F}_q^m$, uniqueness follows for example from Schur's Lemma and the Skolem–Noether Theorem (or by Lang's Theorem).
For $n \in \{11, 12, 22, 23, 24\}$ we denote by M_n the five *Mathieu groups* of degree n, and let M_{10} be a point stabilizer of M_{11} in the transitive action on 10 points.

2.1. The Aschbacher–O'Nan–Scott theorem

The Aschbacher–O'Nan–Scott Theorem makes a rough distinction between several possible types of actions of a primitive permutation group. This theorem had first been announced by O'Nan and Scott at the Santa Cruz Conference on Finite groups in 1979, see [53]. In their statement a case was missing, and the same omission appears in [4]. To our knowledge, the first complete version is in [1]. Very concise and readable proofs are given in [19] and [37], see also [11].

Let A be a primitive permutation group of degree n on Ω. Then one of the following actions occurs:

Affine action. We can identify Ω with a vector space $\mathbb{F}_p^m$, and $\mathbb{F}_p^m \leq A \leq \mathrm{AGL}_m(p)$ is an affine group as described above.

Regular normal subgroup action. A has a non–Abelian normal subgroup which acts regularly on Ω. (There are finer distinctions in this case, see [37], but we don't need that extra information.)

Diagonal action. A has a unique minimal normal subgroup of the form $N = S_1 \times S_2 \times \cdots \times S_t$, where the S_i are pairwise isomorphic non–Abelian simple groups, and the point stabilizer N_ω is a diagonal subgroup of N.

Product action. We can write $\Omega = \Delta \times \Delta \cdots \times \Delta$ with $t \geq 2$ factors, and A is a subgroup of the wreath product $\mathcal{S}(\Delta) \wr \mathcal{S}_t = \mathcal{S}(\Delta)^t \rtimes \mathcal{S}_t$ in the natural product action on this cartesian product. In such a case, we will say that A preserves a product structure.

Almost simple action. There is $S \leq A \leq \mathrm{Aut}(S)$ for a simple non–Abelian group S. In this case, S cannot act regularly.

3. Elements with two cycles

3.1. Previous results

Our goal is the classification of those primitive permutation groups A of degree n which contain an element σ with at most two cycles. If σ actually is an n–cycle, the result is a well–known consequence of the classification of doubly transitive permutation groups.

Theorem 3.1 ([13, 4.1], [25]). *Let A be a primitive permutation group of degree n which contains an n–cycle. Then one of the following holds.*

(a) $A \leq \mathrm{AGL}_1(p)$, $n = p$ *a prime; or*
(b) $A = \mathcal{A}_n$ *or* $\mathcal{S}_n$*; or*
(c) $\mathrm{PSL}_k(q) \leq A \leq \mathrm{P\Gamma L}_k(q)$, $k \geq 2$, q *a prime power, A acting naturally on the projective space with* $n = (q^k - 1)/(q - 1)$ *points; or*
(d) $n = 11$, $A = \mathrm{PSL}_2(11)$ *or* M_{11}*; or*
(e) $n = 23$, $A = \mathrm{M}_{23}$.

If σ has two cycles of coprime length, say k and $l = n - k$ with $k \leq l$, then it follows immediately from Marggraf's theorem [62, Theorem 13.5], applied to the subgroup generated by σ^l, that $\mathcal{A}_n \leq A$ unless $k = 1$. The critical case thus is $k = 1$. We quote the classification result [46, 6.2].

Theorem 3.2. *Let A be a primitive permutation group of degree n which contains an element with exactly two cycles, of coprime lengths $k \leq l$. Assume that $\mathcal{A}_n \not\leq A$. Then $k = 1$, and one of the following holds.*

(a) $n = q^m$ *for a prime power* q, $\mathrm{AGL}_m(q) \leq A \leq \mathrm{A\Gamma L}_m(q)$*; or*
(b) $n = p + 1$, $\mathrm{PSL}_2(p) \leq A \leq \mathrm{PGL}_2(p)$, $p \geq 5$ *a prime; or*
(c) $n = 12$, $A = \mathrm{M}_{11}$ *or* M_{12}*; or*
(d) $n = 24$, $A = \mathrm{M}_{24}$.

In the remainder of this chapter, we deal with the case where k and l are not necessarily coprime. The assumptions in the Theorems 3.1 and 3.2 quickly give that A is doubly transitive (or $A \leq \mathrm{AGL}_1(p)$, a trivial case) — this is clear under existence of an $(n-1)$–cycle, and follows from Theorems of Schur [62, 25.3] and Burnside [24, XII.10.8] under the presence of an n–cycle. So one basically has to check the list of doubly transitive groups.

In the general case however, A no longer need to be doubly transitive. Excluding the case $A \leq \mathrm{AGL}_1(p)$, we will obtain as a corollary of our classification that A has permutation rank ≤ 3, though I do not see how to obtain that directly. I know only two results in the literature where this has been shown under certain restrictions. The first one is by Wielandt [62, Theorem 31.2], [61], under the assumption that $k = l$, and k is a prime, and the other one is by Scott, see the announcement of the never published proof in [54]. In Scott's announcement, however, there are several specific assumptions on A. First $k = l$, and A has to have a doubly transitive action of degree k, such that the point–stabilizer in this action is intransitive in the original action, but that the element with the two cycles of length k in the original action is a k–cycle in the degree k action.

3.2. Classification result

Recall that if t is a divisor of m, then we have $\Gamma\mathrm{L}_{m/t}(p^t)$ naturally embedded in $\mathrm{GL}_m(p)$. We use this remark in the main result of this chapter.

Theorem 3.3. *Let A be a primitive permutation group of degree n which contains an element with exactly two cycles of lengths k and $n - k \geq k$. Then one of the following holds, where A_1 denotes the stabilizer of a point.*

1. (*Affine action*) *$A \leq \mathrm{AGL}_m(p)$ is an affine permutation group, where $n = p^m$ and p is a prime number. Furthermore, one of the following holds.*
   (a) *$n = p^m$, $k = 1$, and $\mathrm{GL}_{m/t}(p^t) \leq A_1 \leq \Gamma\mathrm{L}_{m/t}(p^t)$ for a divisor t of m;*
   (b) *$n = p^m$, $k = p$, and $A_1 = \mathrm{GL}_m(p)$;*
   (c) *$n = p^2$, $k = p$, and $A_1 < \mathrm{GL}_2(p)$ is the group of monomial matrices (here $p > 2$);*
   (d) *$n = 2^m$, $k = 4$, and $A_1 = \mathrm{GL}_m(2)$;*
   (e) (*Sporadic affine cases*)
      i. *$n = 4$, $k = 2$, and $A_1 = \mathrm{GL}_1(4)$ (so $A = \mathcal{A}_4$);*
      ii. *$n = 8$, $k = 2$, and $A_1 = \Gamma\mathrm{L}_1(8)$;*
      iii. *$n = 9$, $k = 3$, and $A_1 = \Gamma\mathrm{L}_1(9)$;*
      iv. *$n = 16$, $k = 8$, and $[\Gamma\mathrm{L}_1(16) : A_1] = 3$ or $A_1 \in \{\Gamma\mathrm{L}_1(16), (C_3 \times C_3) \rtimes C_4, \Sigma\mathrm{L}_2(4), \Gamma\mathrm{L}_2(4), \mathcal{A}_6, \mathrm{GL}_4(2)\}$;*
      v. *$n = 16$, $k = 4$ or 8, and $A_1 \in \{(\mathcal{S}_3 \times \mathcal{S}_3) \rtimes C_2, \mathcal{S}_5, \mathcal{S}_6\}$;*
      vi. *$n = 16$, $k = 2$ or 8, and $A_1 = \mathcal{A}_7 < \mathrm{GL}_4(2)$;*
      vii. *$n = 25$, $k = 5$, and $[\mathrm{GL}_2(5) : A_1] = 5$;*
2. (*Product action*) *One of the following holds.*
   (a) *$n = r^2$ with $1 < r \in \mathbb{N}$, $k = ra$ with $\gcd(r, a) = 1$, $A = (\mathcal{S}_r \times \mathcal{S}_r) \rtimes C_2$, and $A_1 = (\mathcal{S}_{r-1} \times \mathcal{S}_{r-1}) \rtimes C_2$;*
   (b) *$n = (p+1)^2$ with $p \geq 5$ prime, $k = p+1$, $A = (\mathrm{PGL}_2(p) \times \mathrm{PGL}_2(p)) \rtimes C_2$, and $A_1 = (\mathrm{AGL}_1(p) \times \mathrm{AGL}_1(p)) \rtimes C_2$.*
3. (*Almost simple action*) *$S \leq A \leq \mathrm{Aut}(S)$ for a simple, non–Abelian group S, and one of the following holds.*
   (a) *$n \geq 5$, $\mathcal{A}_n \leq A \leq \mathcal{S}_n$ in natural action;*
   (b) *$n = 10$, $k = 5$, and $\mathcal{A}_5 \leq A \leq \mathcal{S}_5$ in the action on the 2–sets of $\{1, 2, 3, 4, 5\}$;*

(c) *$n = p + 1$, $k = 1$, and* $\mathrm{PSL}_2(p) \le A \le \mathrm{PGL}_2(p)$ *for a prime p;*
(d) *$n = (q^m - 1)/(q - 1)$, $k = n/2$, and* $\mathrm{PSL}_m(q) \le A \le \mathrm{P\Gamma L}_m(q)$ *for an odd prime power q and $m \ge 2$ even;*
(e) *$n = 19$, $k = 2$, and* $\mathrm{M}_{10} \le A \le \mathrm{P\Gamma L}_2(9)$*;*
(f) *$n = 21$, $k = 7$, and* $\mathrm{P\Sigma L}_3(4) \le A \le \mathrm{P\Gamma L}_3(4)$*;*
(g) *$n = 12$, $k = 1$ or 4, and $A = \mathrm{M}_{11}$ in its action on 12 points;*
(h) *$n = 12$, $k = 1, 2, 4$, or 6, and $A = \mathrm{M}_{12}$;*
(i) *$n = 22$, $k = 11$, and* $\mathrm{M}_{22} \le A \le \mathrm{Aut}(\mathrm{M}_{22}) = \mathrm{M}_{22} \rtimes C_2$*;*
(j) *$n = 24$, $k = 1, 3$, or 12, and $A = \mathrm{M}_{24}$.*

The proof of this theorem is given in the following sections. We distinguish the various cases of the Aschbacher-O'Nan-Scott theorem, because the cases require quite different methods. The almost simple groups comprise the most complex case. We split this case further up into the subcases where the simple normal subgroup S is alternating, sporadic, a classical Lie type group, or an exceptional Lie type group.

We note an interesting consequence of the previous theorem which generalizes several classical results on permutations groups. It would be very interesting to have a direct proof, without appealing to the classification of the finite simple groups.

Corollary 3.4. *Let A be a primitive permutation group which contains an element with exactly two cycles. Then A has rank at most 3.*

3.3. Affine action

We need the following well–known fact:

Lemma 3.5. *Let K be a field of positive characteristic p, and $\sigma \in \mathrm{GL}_m(K)$ of order $p^b \ge p$. Then $p^{b-1} \le m - 1$. In particular,* $\mathrm{ord}(\sigma) \le p(m-1)$ *if $m \ge 2$.*

Proof. 1 is the only eigenvalue of σ, therefore σ is conjugate to an upper triangular matrix with 1's on the diagonal. So $\sigma - \mathbf{1}$ is nilpotent. Now $(\sigma - \mathbf{1})^{p^{b-1}} = \sigma^{p^{b-1}} - \mathbf{1} \neq 0$, thus $p^{b-1} < m$, and the claim follows. □

We note the following easy consequence:

Lemma 3.6. *Let A be an affine permutation group of degree p^m. Let A contain an element of order p^r for $r \in \mathbb{N}$. Then $p^{r-1} \le m$. In particular, if $r = m$, then $m \le 2$, and $m = 1$ for $p > 2$.*

Proof. Without loss $A = \mathrm{AGL}_m(p)$. We use the well–known embedding of A in $\mathrm{GL}_{m+1}(p)$: Let $g \in \mathrm{GL}_m(p)$, $\mathbf{v} \in N$. Then define the action of $g\mathbf{v} \in A$ on the vector space $N \times \mathbb{F}_p$ via $(\mathbf{w}, w_{m+1})^{g\mathbf{v}} := (\mathbf{w}g + w_{m+1}\mathbf{v}, w_{m+1})$ for $\mathbf{w} \in N$, $w_{m+1} \in \mathbb{F}_p$.

This way we obtain an element σ of order p^r in $\mathrm{GL}_{m+1}(p)$. The claim follows from Lemma 3.5. □

In the following we use the notation $X^\sharp := X \setminus \{0\}$ for the nonzero elements of a vector space X.

Lemma 3.7. *Let $G \leq \mathrm{GL}_m(p)$ act irreducibly on $V = \mathbb{F}_p^m$. Suppose that G contains a subgroup which fixes a nonzero element from V, and acts transitively on the nonzero elements of a hyperplane in V. If $m \geq 3$, then G acts doubly transitively on $\mathbb{P}^1(V)$; or $p = 2$, $m = 3$, and $G = \Gamma\mathrm{L}_1(8)$.*

Proof. Let H be the subgroup which fixes pointwise a line $U < V$, and acts transitively on the nonzero elements of a hyperplane $W < V$.

The orbits of H on $V^\sharp$ consist of $\{u\}, 0 \neq u \in U$, and the sets $W^\sharp + u, u \in U$. Since U is 1–dimensional, we see that H has three orbits on $\mathbb{P}^1(V)$, of lengths 1, $(p^{m-1} - 1)/(p - 1)$ (corresponding to W) and $p^{m-1} - 1$ (corresponding to $u + W$ for some fixed $0 \neq u \in U$).

Assume $m \geq 3$. We contend that G is transitive on $\mathbb{P}^1(V)$. Since G is irreducible, neither U nor W are G–invariant, so none of the two smaller orbits of H is a G–orbit. So if G is not transitive on $\mathbb{P}^1(V)$, then $U \cup W$ is G–invariant. Pick $g \in G$ with $W^g \neq W$. From $W^g \subseteq W \cup U$ we get $W^g = (W \cap W^g) \cup (U \cap W^g)$, hence $p^{m-1} = p^{m-2} + p - 1$, so $m = 2$, a contradiction.

We see that G is even transitive on $V^\sharp$: Pick $v_1, v_2 \in V^\sharp$. Choose $g_1, g_2 \in G$ with $v_i^{g_i} \in W$, and $h \in H$ with $(v_1^{g_1})^h = v_2^{g_2}$. Thus $g_1 h g_2^{-1}$ maps v_1 to v_2.

Since H has 3 orbits on $\mathbb{P}^1(V)$, one of size 1, we see that the action of G on $\mathbb{P}^1(V)$ is either doubly transitive or has rank 3. Thus assume that the action has rank 3. We are going to use consequences from Higman's eigenvalue techniques for rank 3 permutation groups. Let $\{a\}$, Δ, and Γ be the orbits of H of size 1, $k = (p^{m-1} - 1)/(p - 1)$, and $l = p^{m-1} - 1 = (p - 1)k$, respectively. By [22, Lemma 2] there are λ and μ such that $\lambda = |\Delta \cap \Delta^g|$ for any $g \in G$ with $a^g \in \Delta$, and $\mu = |\Delta \cap \Delta^g|$ if $a^g \in \Gamma$. If $a^g \in \Delta$, then $\Delta \cap \Delta^g$ is the image in $\mathbb{P}^1(V)$ of two distinct hyperplanes in V. Thus $\lambda = (p^{m-2} - 1)/(p - 1)$. By [22, Lemma 5], $\mu l = k(k - \lambda - 1)$, hence $\mu = (p^{m-2} - 1)/(p - 1) = \lambda$.

First suppose that $|G|$ is even. Then [22, Lemma 7] shows that $d = (\lambda - \mu)^2 + 4(k - \mu)$ is a square, and $\sqrt{d}$ divides $2k + (\lambda - \mu)(k + l)$. In our situation, $d = 4(k - \mu) = 4p^{m-2}$ and $2k + (\lambda - \mu)(k + l) = 2(1 + p + \cdots + p^{m-2})$. Again, we get the contradiction $m = 2$.

If $|G|$ is odd, then, by transitivity of G on $V^\sharp$, we have $p = 2$. Note that G is solvable by the odd order theorem. As a consequence of Huppert's classification of the finite solvable transitive linear groups (see *e.g.* [24, Theorem 7.3], we get that $G \leq \Gamma\mathrm{L}_1(2^m)$, where we identify V with $\mathbb{F}_{2^m}$. The stabilizer in $\Gamma\mathrm{L}_1(2^m)$ of 1 is $\Gamma = \mathrm{Aut}(\mathbb{F}_{2^m})$. We get $m = |\Gamma| \geq |W^\sharp| = 2^{m-1} - 1$, hence $m = 3$ and $G = \Gamma\mathrm{L}_1(8)$. This case arises indeed, as one can see by the action of Γ on a normal basis of $\mathbb{F}_8/\mathbb{F}_2$. □

Proposition 3.8. *Let $m \geq 5$, and $G \leq \mathrm{GL}_m(2)$ be irreducible on $V := \mathbb{F}_2^m$. Suppose that there is an element $\tau \in G$ and decomposition $V = U \oplus W$ into τ–invariant subspaces with $\dim U = 2$ such that τ is a Singer cycle on W and an involution on U. Then $G = \mathrm{GL}_m(2)$.*

Proof. We first show that G is transitive on $V^\sharp$. Set $H = <\tau>$. Let u_1 and u_2 be the two elements from U which are interchanged by τ, and u_3 be the third element from $U^\sharp$. The orbits of H on $V^\sharp$ are $\{u_3\}, \{u_1, u_2\}, W^\sharp, W^\sharp + u_3$, and $(W^\sharp + u_1) \cup (W^\sharp + u_2)$.

If C_1 and C_2 are subsets of $V^\sharp$ such that each C_i lies completely in an G–orbit, then we say that C_1 and C_2 are *connected* if they lie in the same G–orbit. The latter is equivalent to the existence of $g \in G$ with $C_1 \cap C_2^g \neq \emptyset$. Each of the H–orbits from above lies in an G–orbit. Consider the graph with vertex set these orbits, and let two vertices be connected if and only if the corresponding orbits are connected. The aim is to show that this graph is connected.

We first show that for each $u \in U$ there is $u \neq u' \in U$ such that $W^\sharp + u$ and $W^\sharp + u'$ are connected. Suppose that were not the case. Then, for each $g \in G$,

$$(W^\sharp + u)^g \subseteq (W^\sharp + u) \cup U^\sharp,$$

so

$$W^g \subseteq (W + u - u^g) \cup (U^\sharp - u^g).$$

Not each element of $U^\sharp - u^g$ can be contained in W^g, for this would imply $(U^\sharp)^{g^{-1}} \subseteq W^\sharp + u$. But by irreducibility of G, the union of the sets $(U^\sharp)^{g^{-1}}$ generates V, while $W^\sharp + u$ does not generate V. Thus we get

$$|W^g \cap (W + u - u^g)| \geq 2^{m-2} - 3.$$

Let r be the dimension of $W^g \cap (W + u - u^g)$ as an affine space. It follows that $2^r \geq 2^{m-2} - 3$, so $r = m - 2$ as $m \geq 5$. Thus $W^g = W$ for all $g \in G$, again contrary to irreducibility of G.

Let $u \in U^\sharp$ be such that $W^\sharp$ and $W^\sharp + u$ are connected. We show that these two sets must also be connected to another $W^\sharp + u'$ for $u' \in U^\sharp$ different from u. Suppose that this were not the case. Let W' be the $(m-1)$–dimensional space $W \cup (W + u)$. Then, similar as above, $(W')^g \subseteq W' \cup U$ for all $g \in G$, hence $(W')^g \setminus U \subseteq W' \cap (W')^g$. Pick $g \in G$ with $(W')^g \neq W'$. Then comparing of dimensions yields $2^{m-1} - 4 \leq 2^{m-2}$, so $m \leq 4$, a contradiction.

From these two steps we see that all the $W^\sharp + u$ for $u \in U$ are connected. Finally, let $u' \in U^\sharp$. Then also $\{u'\}$ is connected to some and hence all the $W^\sharp + u$, because $(u')^G$ generates V by irreducibility, so $(u')^G \subseteq U^\sharp$ cannot hold.

Thus G is transitive on $V^\sharp$. Note that τ has odd order $2^{m-2} - 1$ on W. Thus $\tau^{2^{m-2}-1}$ is a transvection on V. Let X be the normal subgroup of G which is generated by the conjugates of this transvection. By an easy result of Hering, we get that X is irreducible, for otherwise $|X|$ would be odd by [21, Lemma 5.1], contrary to the assumption that X contains a transvection.

Thus X is irreducible, and we can apply McLaughlin's classification of irreducible subgroups of $\mathrm{GL}_m(2)$ which are generated by transvections, see [44]. Either $X = \mathrm{GL}(V)$; or $m = \dim(V)$ is even and one of the following holds: $X = \mathrm{Sp}(V)$, $X = O(V)$ for some nondegenerate quadratic form, or X is isomorphic to the symmetric group $\mathcal{S}_{m+1}$ or $\mathcal{S}_{m+2}$.

We have to rule out all the possibilities but the first one. Note that X is normal in the transitive group G, so G permutes transitively the orbits of X on $V^\sharp$, in particular they all have the same size. This excludes the orthogonal case $X = O(V)$. For if Q is the nondegenerate quadratic form describing X, then by Witt's Theorem, X has the two orbits $\{v \in V^\sharp | Q(v) = 0\}$ and $\{v \in V^\sharp | Q(v) = 1\}$ (see also [30, Lemma 2.10.5]). But the sizes of these orbits are distinct because they add up to $2^m - 1$.

Next we show that $X = \mathrm{Sp}(V)$ cannot happen. Suppose that $X = \mathrm{Sp}(V)$. By [30, Lemma 2.10.6], X acts absolutely irreducibly on V. In particular, the centralizer of X in G is trivial. So $G = X$, because the outer automorphism group of $\mathrm{Sp}(V)$ is trivial, see *e.g.* [30, Chapter 2]. Let $(\cdot, \cdot)$ be the associated symplectic form on V. If $v \in V$ is non–zero, then the stabilizer of v in $\mathrm{Sp}_m(2)$ has two orbits on $V^\sharp \setminus \{v\}$ – the orbit of length $2^{m-1} - 2$ through those v' with $(v, v') = 0$, and the orbit of length 2^{m-1} through those v' with $(v, v') = 1$, see [23, II.9.15]. Since $<\tau^2>$ is transitive on $W^\sharp$ and fixes U pointwise, we get that for each $u \in U$ either $(u, W^\sharp) = 0$ or $(u, W^\sharp) = 1$. We aim to show that the restriction of the symplectic form to W is not degenerate. This is clear if $(U, W) = 0$. So suppose there is $u \in U$ with $(u, W^\sharp) = 1$. The orthogonal complement $W^\perp$ intersects U non-trivially (for if u_1 and u_2 are different elements in U with $(u_i, W) = 1$, then $(u_1 + u_2, W) = 0$). So the radical of W has dimension ≤ 1, hence in fact is trivial, because W has even dimension.

Therefore W is a non-degenerate symplectic space, where τ^2 acts irreducibly on. So $\mathrm{ord}(\tau^2)$ divides $2^{(m-2)/2} + 1 = 2^{\dim W/2} + 1$, see Lemma 3.28, contrary to $\mathrm{ord}(\tau^2) = 2^{m-2} - 1$.

It remains to exclude the symmetric groups. So $X = \mathcal{S}_{m+1}$ or $X = \mathcal{S}_{m+2}$ is normal in $G \leq \mathrm{GL}(V)$, where $V = \mathbb{F}_2^m$. First note that the centralizer of X in G is X. For otherwise, the centralizer of X in $\mathrm{End}(V)$ would be a proper field extension E of $\mathbb{F}_2$. But then X would have a linear representation over E of degree $\leq m/2$, contrary to the lower bounds of degrees of 2–modular representations of symmetric groups, see *e.g.* [60]. Since $m \geq 6$ (recall that m is even), we have $X = \mathcal{S}_i$ with $i \geq 7$. In this case it is well known that $\mathrm{Aut}(X) = X$. Thus $G = X$.

The element $\tau \in G = X$ has order $2(2^{m-2} - 1)$. On the other hand, the element orders in the symmetric group $\mathcal{S}_{m+2}$ are at most $e^{(m+2)/e}$, see Proposition 3.22. From $2(2^{m-2} - 1) \leq e^{(m+2)/e}$ one quickly gets $m \leq 4$, a case excluded here. □

We need to know the doubly transitive permutation subgroups of the collineation group of a projective linear space.

Proposition 3.9 (Cameron, Kantor [6, Theorem I]). *Let $m \geq 3$, p be a prime, and $H \leq \mathrm{GL}_m(p)$ be acting doubly transitively on the lines of $\mathbb{F}_p^m$. Then $\mathrm{SL}_m(p) \leq H$ or $H = \mathcal{A}_7 < \mathrm{SL}_4(2)$.*

Several years ago, the proof (and finer versions of the results) have turned out to be false. In [5] the authors have begun to fix the proof. The main interest of their approach is that they get a very deep classification result without using the classification of the finite simple groups. If one is willing to to use the classification of the finite simple groups and, as a consequence of that, the classification of the finite doubly transitive groups, then it is not hard to prove Proposition 3.9.

In order to handle the case $m = 2$, we need the following:

Lemma 3.10. *Let p be a prime, and let $H \leq \mathrm{GL}_2(p)$ act irreducibly on $\mathbb{F}_p^2$. Let ω be a generator of the multiplicative group of $\mathbb{F}_p$, and suppose that $\tau := \left(\begin{smallmatrix} 1 & 0 \\ 0 & \omega \end{smallmatrix}\right) \in H$. Then one of the following holds.*

(a) $H = \mathrm{GL}_2(p)$.
(b) *H is the group of monomial matrices.*
(c) *$p = 5$, and* $[\mathrm{GL}_2(5) : H] = 5$.
(d) *$p = 3$, and H is a Sylow 2–subgroup of* $\mathrm{GL}_2(3)$.
(e) *$p = 2$, and $H \cong C_3$.*

Proof. The cases $p = 2$ and 3 are straightforward. So assume $p \geq 5$. If $\mathrm{SL}_2(p) \leq H$, then $H = \mathrm{GL}_2(p)$ and (a) holds, because the determinant of $\tau \in H$ is a generator of $\mathbb{F}_p^\star$.

So we assume in the following that H does not contain $\mathrm{SL}_2(p)$. We first contend that p does not divide the order of H. Suppose it does. Then H contains a Sylow p–subgroup P of H. If P is normal in H, then H is conjugate to a group of upper triangular matrices, hence not irreducible. Therefore P is not normal in H, thus H contains at least $1 + p$ Sylow p–subgroups of $\mathrm{GL}_2(p)$ (by Sylow's Theorem). But $\mathrm{GL}_2(p)$ has exactly $p + 1$ Sylow p–subgroups, so H contains all the $p + 1$ Sylow p–subgroups of $\mathrm{GL}_2(p)$. But these Sylow p–subgroups generate $\mathrm{SL}_2(p)$, contrary to our assumption.

Set $C = \langle\tau\rangle$, and let $S \cong \mathbb{F}_p^\star$ be the group of scalar matrices. So CS is the group of diagonal matrices. First assume that H normalizes CS. Then, by irreducibility of H, some element in H must switch the two eigenspaces of C. It follows quickly that H is monomial.

So finally suppose that CS is not normalized by H. Then there is a conjugate $(CS)^h$ with $h \in H$, such that $(CS) \cap (CS)^h = S$. So we have $|HS| \geq |(CS)(CS)^h| = (p-1)^3$ and $(p-1)^2 \mid |HS|$. First note that we cannot have $|HS| = (p-1)^3$ simply because $(p-1)^3$ does not divide $|\mathrm{GL}_2(p)| = (p-1)^2 p(p+1)$. So $|HS| \geq p(p-1)^2$. But again equality cannot hold, for we noted already that p does not divide $|H|$. So $|HS| \geq (p+1)(p-1)^2$, hence $[\mathrm{GL}_2(p) : HS] \leq p$. But $\mathrm{PGL}_2(p) = \mathrm{GL}_2(p)/S$ acts faithfully on the coset space $\mathrm{PGL}_2(p)/(HS/S)$ and has an element of order p, hence $[\mathrm{GL}_2(p) : HS] = p$. A classical theorem of Galois [23, II.8.28] says that if $\mathrm{PSL}_2(p)$ has a transitive permutation representation of degree p, then $p \leq 11$. But one checks that $\mathrm{GL}_2(p)$ does not have a subgroup of index p for $p = 7$ and 11, thus $p = 5$. So $|HS| = 96 = 16 \cdot 2 \cdot 3$. Therefore CS (of order 16) has a proper normalizer in HS. By an argument as above, we thus obtain an element $h \in H$ which switches the eigenspaces of C. So $\langle C, C^h\rangle \leq H$ is the group of diagonal matrices, in particular $S \leq H$. The claim follows. □

The proof of the following lemma is straightforward, we leave it to the reader.

Lemma 3.11. *Let $m \geq 2$, p a prime, and $\mathbb{F}_p^m = U \oplus W$ with U and W invariant under $\tau \in \mathrm{GL}_m(p)$. Assume that τ acts as a Singer cycle on W.*

(a) *Let* $\dim U = 1$, *and suppose that τ act as the identity on U. Choose $u \in U^\sharp$. Then $(\tau, u) \in \mathrm{AGL}_m(p)$ acts as an element with cycle lengths p and $p^m - p$ on $\mathbb{F}_p^m$.*
(b) *Let* $\dim U = 2$, *$p = 2$, and suppose that τ act as an involution on U. Choose $u \in U$ with $u \neq u^\tau$. Then $(\tau, u) \in \mathrm{AGL}_m(2)$ acts as an element with cycle lengths* 4 *and* $2^m - 4$ *on* $\mathbb{F}_2^m$.

3.3.1. *Proof of part* 1 *of Theorem* 3.3

We may assume that $A \leq \mathrm{AGL}_m(p)$, acting on $V = \mathbb{F}_p^m$. So A is a semidirect product $A = A_1 \rtimes V$, where A_1 is a subgroup of $\mathrm{GL}_m(p)$ in its natural action on V.

Let σ be the element with the cycle lengths k and l. First note that k divides l, for otherwise σ^l would fix $p^m > l > p^m/2$ points, which of course cannot happen because σ^l is conjugate to an element in $\mathrm{GL}_m(p)$, so the number of fixed points is a power of p. Thus $k = p^r$, $l = p^r(p^{m-r} - 1)$ for some $r \in \mathbb{N}_0$.

If $k = l$, then of course $p = 2$ and $k = l = \mathrm{ord}(\sigma) = 2^{m-1}$. Lemma 3.6 gives $2^{m-2} \leq m$, hence $r = m - 1 \leq 3$. The subgroups of $\mathrm{AGL}_m(2)$ for $m \leq 2$ are easily handled with the computer algebra systems GAP [17] or Magma [3], yielding the cases from the theorem. Also the other possibilities for the pairs (k, l) can be quickly done with these systems. So if $p = 2$, we assume $m \geq 5$.

From now on we assume $k < l$. Then σ^k fixes exactly $k = p^r$ points on V. We may assume that $\sigma^k \in \mathrm{GL}_m(p)$, so the fixed point set of σ^k is a subspace U of V. Thus the elements of U constitute the k–cycle of σ, so σ acts as an affine map of order p^r on the r–dimensional space U. Apply Lemma 3.6 to see that $r \in \{0, 1, 2\}$, and $r \leq 1$ if $p > 2$.

We need to determine the possible groups A. If $k = 1$ we use a result of Kantor [27] which classifies linear groups over a finite field containing an element which cyclically permutes the non-zero elements. Note that σ is just such an element.

Now suppose $k = p$. The element $\tau := \sigma^p \in \mathrm{GL}_m(p)$ fixes a line $U \cong \mathbb{F}_p$ pointwise. As $\gcd(\mathrm{ord}(\tau), p) = 1$, Maschke's Theorem gives a complement W of U which is τ–invariant. As τ has cycles of length $\mathrm{ord}(\tau) = p^{m-1} - 1 = |W^\sharp|$ on $W^\sharp$, we see that τ permutes the elements of $W^\sharp$ cyclically. If $m \geq 3$, then Lemma 3.7 together with Proposition 3.9 handles the possibilities. If however $m = 2$, then apply Lemma 3.10.

It remains to analyze the case $p = 2, r = 2$, so $k = 4, l = 4(2^{m-2} - 1)$. Recall that $m \geq 5$. Let σ be the element with cycle lengths 4 and $2^m - 4$. We may assume that $\sigma^4 \in \mathrm{GL}_m(2)$. Similarly as above, we get $V = U \oplus W$ with $\dim(U) = 2$, such that σ^4 is a Singer cycle on W and fixes U pointwise. Write $\sigma = \tau t$ with $\tau \in \mathrm{GL}_m(2)$ and $t \in V$. Note that $\tau \in A$ since $t \in A$. The action of σ on V is given by $h^\sigma = h^\tau t$ for $h \in V$. Thus the 4–cycle through 0 is $\{0, t, t^\tau t, t^{\tau^2} t^\tau t\}$. These four elements are just the elements of the Klein four group U. The sum of the elements in U is 0, this gives $t^{\tau^2} = t$, so $U = \{t, t^\tau, t^\tau t\}$. So τ induces an involution on U. Next we want to see that W is τ–invariant. For $v \in V$ one has $v^{\sigma^4} = v^{\tau^4} t^{\tau^3} t^{\tau^2} t^{\tau} t = v^{\tau^4} (t^{\tau} t)^2 = v^{\tau^4}$. We have $W^{\tau^2} = W$, for otherwise $W' = W^{\tau^2} \cap W$ is a proper subspace of W of positive dimension (since $m \geq 5$) which is τ^2–invariant. But then W' is also invariant under $\sigma^4 = \tau^4$, contrary to the fact that σ^4 is a Singer cycle on W. But $W^{\tau^2} = W$ implies that $W^{\tau} \cap W$ is τ–invariant, and the same reasoning as before shows that $W^{\tau} = W$. Thus τ itself is a Singer cycle on W, and we have exactly the situation given in Lemma 3.8.

We have covered all possibilities. Use Lemma 3.11 to see that the groups listed in 1b, 1c, and 1d indeed have an element of the required cycle type.

3.4. Product action

Set $\Delta = \{1, 2, \ldots, r\}$ for $r \geq 2$, and let $m \geq 2$ be an integer. Then the wreath product $\mathcal{S}_r \wr \mathcal{S}_m = (\mathcal{S}_r \times \mathcal{S}_r \times \cdots \times \mathcal{S}_r) \rtimes \mathcal{S}_m$ acts in a natural way on $\Omega := \Delta \times \Delta \times \cdots \times \Delta$. We say that a permutation group A acts via the *product action*, if it is permutation equivalent to a transitive subgroup of $\mathcal{S}_r \wr \mathcal{S}_m$ in this action.

In order to avoid an overlap with the affine permutation groups, we quickly note the easy:

Lemma 3.12. *Let A be a primitive subgroup of $\mathcal{S}_r \wr \mathcal{S}_m$ where $r \leq 4$. Then A is affine.*

Proof. Let N be the minimal normal subgroup of $\mathcal{S}_r \wr \mathcal{S}_m$. Then N is elementary Abelian of order r^m. If A intersects N non-trivially, then $N \cap A$ is a minimal normal subgroup of A, and the claim follows. So suppose that $|A \cap N| = 1$. Then A embeds into $(\mathcal{S}_r \wr \mathcal{S}_m)/N$. But r^m divides $|A|$ by transitivity, so r^m divides $(r!)^m m!/r^m$. We get that 2^m divides $m!$ if $r = 2$ or 4, and 3^m divides $m!$ if $r = 3$. But if p is a prime, then the exponent of p in $m!$ is $\sum_{\nu \geq 0} \left[\frac{m}{p^\nu}\right] < \sum_{\nu \geq 0} \frac{m}{p^\nu} = \frac{m}{p-1} \leq m$, a contradiction. $\square$

Remark. One might expect that any primitive subgroup of an affine group is affine. However, that is *not* the case. There seem to be very few counter-examples. The smallest is as follows: Set $A = \mathrm{AGL}_3(2) = C_2^3 \rtimes A_1$. Then it is known (see *e.g.* [23, page 161]) that $H^1(\mathrm{GL}_3(2), C_2^3) = C_2$. So there is a complement U of C_2^3 in A which is not conjugate to A_1. One checks that U acts primitively on the 8 points via $U \cong \mathrm{GL}_3(2) \cong \mathrm{PSL}_2(7)$.

The following two lemmas are trivial but useful.

Lemma 3.13. *Let $\Delta_1, \Delta_2, \ldots, \Delta_m$ be finite sets, and g_i be in the symmetric group of Δ_i. Let o_i be the cycle length of g_i through $\delta_i \in \Delta_i$. Then the cycle length of $(g_1, g_2, \ldots, g_m)$ through $(\delta_1, \delta_2, \ldots, \delta_m) \in \Delta_1 \times \Delta_2 \times \cdots \times \Delta_m$ is* $\mathrm{lcm}(o_1, o_2, \ldots, o_m)$. *In particular, $\delta_1^{<g_1>} \times \delta_2^{<g_2>} \times \cdots \times \delta_m^{<g_m>}$ is the orbit of $<(g_1, g_2, \ldots, g_m)>$ through $(\delta_1, \delta_2, \ldots, \delta_m)$ if and only if the o_i are relatively prime.*

Lemma 3.14. *Let $\Delta_1, \Delta_2, \dots, \Delta_m$ be finite sets, and g_i be in the symmetric group of Δ_i. Let c_i be the number of cycles of g_i on Δ_i. Then $(g_1, g_2, \dots, g_m)$ has at least $c_1 c_2 \cdots c_m$ cycles on $\Delta_1 \times \Delta_2 \times \cdots \times \Delta_m$.*

Lemma 3.15. *Suppose $r \geq 5$ and $m \geq 2$. Let $g = (\sigma_1, \sigma_2, \dots, \sigma_m)\tau$ be an element of $\mathcal{S}_r \wr \mathcal{S}_m$, with $\sigma_i \in \mathcal{S}_r$ and $\tau \in \mathcal{S}_m$ an m–cycle. Then g has at least 3 cycles in the product action.*

Proof. Set $\overline{g} := g^m = (\overline{\sigma_1}, \overline{\sigma_2}, \dots, \overline{\sigma_m}) \in \mathcal{S}_r^m$. Then

$$\overline{\sigma_i} = \sigma_i \sigma_{i+1} \cdots \sigma_m \sigma_1 \cdots \sigma_{i-1},$$

so in particular the $\overline{\sigma_i}$ are pairwise conjugate in $\mathcal{S}_r$. Suppose that g has at most 2 cycles. Then $\overline{g}$ has at most $2m$ cycles.

Let λ be the number of cycles of $\overline{\sigma_1}$. Then $\overline{g}$ has at least λ^m cycles by Lemma 3.14, hence $\lambda^m \leq 2m$. This gives $\lambda = 1$ unless $m = 2$ and $\lambda = 2$. If $\lambda = 1$, then $\overline{g}$ has r^{m-1} cycles by Lemma 3.13, so $r^{m-1} \leq 2m$, hence $r \leq 4$, a contradiction. So suppose that $m = 2$ and $\overline{\sigma_1}$ has two cycles. Then $\overline{g}$ has obviously at least $6 > 2m$ cycles, a contradiction. □

3.4.1. *Proof of part* 2 *of Theorem* 3.3

We assume that $A \leq \mathcal{S}_r \wr \mathcal{S}_m$ with $r \geq 5$ (by Lemma 3.12) and $m \geq 2$. Let $g = (\sigma_1, \sigma_2, \dots, \sigma_m)\tau$ with $\sigma_i \in \mathcal{S}_r$, $\tau \in \mathcal{S}_m$. Assume that g has exactly 2 cycles. By the previous lemmas, we get that $m = 2$ and $\tau = 1$, one of the σ_i must be an r–cycle, and the other σ_i has two cycles, with lengths relatively prime to r.

We need to determine the groups which arise this way. The description of the product action as in [37] shows that there is a primitive group U with socle S acting on $\Delta = \{1, 2, \dots, r\}$, such that $S \times S \trianglelefteq A \leq (U \times U) \rtimes C_2$. Let $g = (\sigma_1, \sigma_2)$ be the element with the two cycles from above. Then $(\sigma_2, \sigma_1) \in (U \times U) \rtimes C_2$. Thus U contains an r–cycle, and an element with two cycles of coprime lengths. In particular, U is not contained in the alternating group $\mathcal{A}_r$, and so is not simple. Furthermore, U is not affine. Taking Theorems 3.1 and 3.2 together gives that either $U = \mathrm{PGL}_2(p)$ for a prime $p \geq 5$, or $U = \mathcal{S}_r$ for $r \geq 5$. The element g shows that $U \times U \leq A$, but $U \times U$ is not primitive, so $A = (U \times U) \rtimes C_2$, and the claim follows.

Remark 3.16. Case 1c of Theorem 3.3, that is $A < \mathrm{AGL}_2(p)$ for a prime $p > 2$ and A_1 the group of monomial matrices, can also be seen as a product action, namely as $A = (\mathrm{AGL}_1(p) \times \mathrm{AGL}_1(p)) \rtimes C_2$ on p^2 points.

3.5. Regular action

As an immediate consequence of the previous section we obtain

Theorem 3.17. *Let A be a primitive non–affine permutation group with a regular normal subgroup. Then A does not contain an element with two cycles.*

Proof. Let N be a regular normal subgroup of A. Then, by regularity, N is a minimal normal subgroup of A, so $N \cong L^m$ for some simple non–Abelian group L and $m \geq 2$. Identify N with the set of points A is acting on, and let C be the centralizer of N in the symmetric group $\mathcal{S}(N)$ of N. If N acts from the right on N, then $C \cong N$ acts from the left on N. Set $H = L \times L$, and let the first and second component act from the left and from the right, respectively. Then A is contained in the wreath product $H \wr \mathcal{S}_m$ in product action, see [37, page 392]. Now apply Theorem 3.3 to see that this cannot occur, a distinguishing property of H being that it is not doubly transitive (in contrast to $\mathrm{PGL}_2(p)$). $\square$

3.6. Diagonal action

Let S be a non–Abelian simple group, and $m \geq 2$ an integer. Set $N := S^m$. Let N act on itself by multiplication from the right. Furthermore, let the symmetric group $\mathcal{S}_m$ act on N by permuting the components, and $\mathrm{Aut}(S)$ act on N componentwise. Define an equivalence relation $\sim$ on N by $(l_1, l_2, \dots, l_m) \sim (cl_1, cl_2, \dots, cl_m)$ for $c \in S$. The above actions respect the equivalence classes, so we get a permutation group D acting on the set $N/\sim$ of size $|S|^{m-1}$. Note that the diagonal elements of N in right multiplication induce inner automorphisms of S on $N/\sim$, for $(i^{-1}l_1 i, i^{-1}l_2 i, \dots, i^{-1}l_m i) \sim (l_1, l_2, \dots, l_m)(i, i, \dots, i)$.

We say that a permutation group A acts in *diagonal action*, if it embeds as a transitive group of D with $N \leq A$. We begin with a technical result:

Proposition 3.18. *Let S be a non–Abelian simple group, $m \geq 2$ be an integer, and D be the group in diagonal action as above. Let $o(\mathrm{Out}(S))$ and $o(S)$ be the largest order of an element in $\mathrm{Out}(S)$ and S, respectively. Then each element of D has at least $\frac{1}{o(\mathrm{Out}(S))|S|}(|S|/o(S))^m$ cycles.*

Proof. Choose an element in D. Raise it to the smallest power such that the contribution from $\mathrm{Out}(S)$ disappears. Let $\sigma \in N \rtimes \mathcal{S}_m$ be this element. Set $o = o(S)$. We are done once we know that σ has at least $\frac{1}{|S|}(|S|/o)^m$ cycles. Write $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_m)\tau$ with $\tau \in \mathcal{S}_m$ and $\sigma_i \in S$. Let τ have u cycles of lengths $\rho_1, \rho_2, \dots, \rho_u$.

Without loss assume that the first ρ_1 coordinates of $N = S^m$ are permuted in an ρ_1–cycle $(1\ 2\ \cdots\ \rho_1)$. Write ρ for ρ_1. Then σ^ρ acts by right multiplication with

$$(\overline{\sigma_1}, \overline{\sigma_2}, \dots, \overline{\sigma_\rho}) = (\sigma_1\sigma_2\cdots\sigma_\rho, \sigma_2\sigma_3\cdots\sigma_\rho\sigma_1, \dots, \sigma_\rho\sigma_1\cdots\sigma_{\rho-1}) \in S^\rho$$

on these first ρ coordinates. Note that all the elements $\overline{\sigma_i}$ have the same order o' because they are conjugate in S. So, by Lemma 3.13, σ^ρ induces $|S|^\rho/o' \geq |S|^\rho/o$ cycles on S^ρ, thus σ induces at least $|S|^\rho/(\rho o)$ cycles on S^ρ. Apply this consideration to the other τ–cycles and use Lemma 3.14 to see that the number of cycles of σ on N is at least

$$\prod_{i=1}^{u} \frac{|S|^{\rho_i}}{\rho_i o} = \frac{|S|^m}{o^u}\prod_{i=1}^{u}\frac{1}{\rho_i} \geq |S|^m\left(\frac{u}{mo}\right)^u,$$

where we used the inequality between the arithmetic and geometric mean in the last step. But the function $(x/(mo))^x$ is monotonously decreasing for $0 \le x \le mo/e$. Note that $o \ge 5$ (because a group with element orders ≤ 4 is solvable), so $mo/e > m$, but $u \le m$. So the above expression is $\ge (|S|/o)^m$. Furthermore, the number of cycles of σ on N is at most $|S|$ times the number of cycles on $N/{\sim}$. From that we get the assertion. □

Theorem 3.19. *Let A be a primitive permutation group in diagonal action. Then A does not contain an element with at most two cycles.*

Proof. Suppose there is a counterexample A, with associated simple group S. Proposition 3.18 gives, as $m \ge 2$,

$$|S| \le 2o(S)^2 o(\mathrm{Out}(S)).$$

If S is sporadic, then use list 3.3 on page 411 along with the group orders given in the atlas [9] to see that this inequality has no solution. Next suppose that $S = \mathcal{A}_n$ is alternating. Then $\mathrm{Out}(S) = C_2$ if $n \ne 6$, and $\mathrm{Out}(\mathcal{A}_6) = C_2 \times C_2$, so $o(\mathrm{Out}(S)) = 2$ in any case (see *e.g.* [23, II.5.5]). Use the bound $o(S) \le e^{n/e}$ from Proposition 3.22 to see that only $n = 5$ is possible with $m = 2$. But it is easy to take into account the possible outer automorphism and show along the lines of the previous proposition that the minimal number of cycles of an element in A is 4 (all of length 15), or one checks that with a GAP computation.

So we are left with the case that S is simple of Lie type. Using the information about $\mathrm{Out}(S)$ and $o(S)$ in the Tables 3.2 (page 410) and 3.1 (page 410) and in Section 3.7.3 together with the order of S given for instance in the atlas [9], one sees that the only group which does fulfill the above inequality is $S = \mathrm{PSL}_2(7)$. (One also has to use the atlas [9] in some small cases where the given bounds for $o(S)$ are too coarse in order to exclude S.)

However, the proof of the proposition above shows that we have $m = 2, u = 2$, and $\mathrm{ord}(\overline{\sigma_1})\mathrm{ord}(\overline{\sigma_2}) \ge 168/4 = 42$, hence $\mathrm{ord}(\overline{\sigma_1}) = \mathrm{ord}(\overline{\sigma_2}) = 7$, so σ has at least $168^2/(7 \cdot 168) = 24$ cycles on $S^2/{\sim}$, a clear contradiction. □

3.7. Almost simple action

By what we have seen so far, the only remaining case is the almost simple action. The aim of the following sections is to show that only the cases listed in part 3 of Theorem 3.3 appear. See Section 3.7.11 where all the results achieved in the following sections are bundled to give a proof of this assertion.

Many cases of almost simple permutation groups can be ruled out by comparing element orders with indices of (maximal) subgroups of almost simple groups, though some other require finer arguments. We give the following:

Definition 3.20. For a finite group X let $\mu(X)$ be the smallest degree of a faithful, transitive permutation representation of X, and $o(X)$ the largest order of an element in X.

We use the trivial:

Lemma 3.21. *Let A be a transitive permutation group of degree n, and let $\sigma \in A$ have two cycles in this action. Then*

$$n \leq 2\mathrm{ord}(\sigma) \tag{3.1}$$
$$n \leq 3\mathrm{ord}(\sigma)/2, \text{ if } n \text{ is odd.} \tag{3.2}$$

3.7.1. *Alternating groups*

Using methods and results from analytic number theory, one can show that the logarithm of the maximal order of an element in $\mathcal{S}_n$ is asymptotically $\sqrt{n \log n}$, see [34, Section 61]. Here, the following elementary but weaker result is good enough for us – besides, we need an exact bound rather than an asymptotic bound anyway.

Proposition 3.22. *The order of an element in $\mathcal{S}_n$ is at most $e^{n/e}$ for all $n \in \mathbb{N}$, and at most $(n/2)^{\sqrt{n/2}}$ for $n \geq 6$. (Here $e = 2.718\ldots$ denotes the Euler constant.)*

Proof. Let $\nu_1, \nu_2, \ldots, \nu_r$ be the different cycle lengths > 1 of an element $g \in \mathcal{S}_n$. Then

$$\mathrm{ord}(g) = \mathrm{lcm}(\nu_1, \nu_2, \ldots, \nu_r) \leq \nu_1\nu_2\cdots\nu_r,$$

and

$$\nu_1 + \nu_2 + \cdots + \nu_r \leq n. \tag{3.3}$$

The inequality between the arithmetic and geometric mean yields

$$\mathrm{ord}(g) = \mathrm{lcm}(\nu_1, \nu_2, \ldots, \nu_r) \leq \nu_1\nu_2\cdots\nu_r \leq \left(\frac{\sum \nu_i}{r}\right)^r \leq \left(\frac{n}{r}\right)^r.$$

The function $x \mapsto (n/x)^x$ is increasing for $0 < x \leq n/e$, and decreasing for $x > n/e$. From that we obtain the first inequality. Suppose that $\nu_1 < \nu_2 < \cdots < \nu_r$. Then $\nu_i \geq i + 1$, and we obtain

$$n \geq \sum \nu_i \geq 2 + 3 + \cdots + r + (r+1) = \frac{r^2 + 3r}{2} > \frac{r^2}{2}.$$

If $n > 2e^2 = 14.7\ldots$, then $r < \sqrt{2n} < n/e$, and the claim follows from the monotonicity consideration above. Check the cases $6 \leq n \leq 14$ directly. □

Now suppose that $\mathcal{A}_n \leq A \leq \mathrm{Aut}(\mathcal{A}_n)$ for $n \geq 5$. Note that except for $n = 6$, $\mathrm{Aut}(\mathcal{A}_n) = \mathcal{S}_n$ by [23, II.5.5]. We exclude $n = 6$ in this section, and treat this case in Section 3.7.3 about classical groups, because $\mathcal{A}_6 \cong \mathrm{PSL}_2(9)$. So A_1 is a maximal subgroup of A not containing $\mathcal{A}_n$. Let $\sigma \in A$ have at most two cycles on A/A_1. We regard A_1 as a subgroup of $\mathcal{S}_n \geq A$ in the natural action on $\{1, 2, \ldots, n\}$ points. There are three possibilities for A_1 with respect to this embedding: A_1 is intransitive, or transitive but imprimitive, or primitive. We treat these three possibilities separately.

A_1 intransitive. A_1 leaves a set of size m invariant, with $1 \le m < n$. Denote by M_m the subsets of size m of $\{1, 2, \dots, n\}$. By maximality of A_1 in A and transitivity of A on M_m we see that A_1 is the full stabilizer in A of a set of m elements, thus the action of A is given by the action on M_m. If $m = 1$, then we have the natural action of A, leading to case 3a in Theorem 3. So for the remainder assume $m \ge 2$.

First consider the case that σ is an n–cycle in the natural action. One of the two cycles of σ has length at least $\binom{n}{m}/2$, so $n \ge \binom{n}{m}/2 \ge n(n-1)/4$, thus $n = 5$. This case really occurs, and gives case 3b in Theorem 3.

Next suppose that σ is not an n–cycle. Then σ leaves (on $\{1, 2, \dots, n\}$) a set S of size $1 \le |S| \le n/2$ invariant. Without loss $m \le n/2$ (as the action on the m–sets is the same as the action on the $(n-m)$–sets). Note that σ cannot be an $(n-1)$–cycle by an order argument as above. So we can assume $|S| \ge 2$. For $i = 0, 1, 2$ choose sets S_i of size m, such that i points of S_i are in S, and the remaining $m - i$ points are in the complement of S. Then these three sets of course are not conjugate under $<\sigma>$.

A_1 transitive but imprimitive. Let $1 < u < n$ be the size of the blocks of a non–trivial system of imprimitivity. Then $v := n/u$ is the number of blocks, and $A_1 = (\mathcal{S}_u \wr \mathcal{S}_v) \cap A = ((\mathcal{S}_u)^v \rtimes \mathcal{S}_v) \cap A$ in the natural action (not to mistake with the product action).

The index of A_1 in A thus is $n!/((u!)^v v!)$. We will use the bounds in Lemma 3.21 and Proposition 3.22 to see that this case does not occur. The proof is based on the following

Lemma 3.23. *Let $u, v \ge 2$ be integers, then*

$$u!^v v! < \frac{1}{2}\frac{(uv)!}{e^{uv/e}}, \tag{3.4}$$

except for $(u, v) = (2, 2), (3, 2), (4, 2),$ *and* $(2, 3)$.

Proof. We contend that if the inequality (3.4) holds for (u, v), then it holds also for $(u, v+1)$. First

$$3 < 4.31\ldots = \left(\frac{3}{e^{1/e}}\right)^2 \le \left(\frac{3}{e^{1/e}}\right)^u \Longrightarrow e^{u/e} < 3^{u-1} \le (v+1)^{u-1}.$$

This implies

$$(v+1)e^{u/e} < (v+1)^u. \tag{3.5}$$

But

$$v + 1 \le \frac{uv + i}{i}$$

for $i = 1, 2, \dots, u$, so taking the product over these i yields

$$(v+1)^u \le \binom{uv+u}{u} \Longrightarrow (v+1)e^{u/e} \le \binom{uv+u}{u}$$

by (3.5). Multiply the resulting inequality

$$u!(v+1) < \frac{(uv+u)!}{(uv)!e^{u/e}}$$

with (3.4) to obtain the induction step for v. Next we show that (3.4) holds for $v = 2$ and $u \geq 7$. As $\binom{2u}{u}$ appears as the biggest binomial coefficient in the expansion of $(1+1)^{2u}$, we obtain $\binom{2u}{u} \geq \frac{1}{2u+1}2^{2u}$. Inequality (3.4) for $v = 2$ reduces to

$$\binom{2u}{u} > 4e^{2u/e}.$$

So we are done once we know that

$$\frac{1}{2u+1}2^{2u} > 4e^{2u/e},$$

which is equivalent to

$$\left(\frac{2}{e^{1/e}}\right)^{2u} > 4(2u+1).$$

But it is routine to verify this for $u \geq 7$. In order to finish the argument, one verifies (3.4) directly for $u < 7$ and the least value of v where the inequality is supposed to hold. □

As $uv \geq 5$ and $uv \neq 6$ by our assumption, we have the only case $u = 4, v = 2$. But $8!/(4!^2 2!) = 35$, and the maximal order of an element in $\mathcal{S}_8$ is 15, contrary to Lemma 3.21.

A_1 primitive. Now suppose that A_1 is primitive on $\{1, 2, \ldots, n\}$, hence $\left[\frac{n+1}{2}\right]! \leq [\mathcal{S}_n : A_1]$ by a result of Bochert, see [2] or [62, 14.2]. Here $[x]$ denotes the biggest integer less than or equal x. As A has index at most 2 in $\mathcal{S}_n$, we obtain from Lemma 3.21 and Proposition 3.22

$$\left[\frac{n+1}{2}\right]! \leq 2[A : A_1] \leq 4e^{n/e}.$$

However, one verifies that for $n = 9$ and 12 the following holds

$$\left[\frac{n+1}{2}\right]! > 4e^{n/e}. \tag{3.6}$$

But if (3.6) holds for some $n \geq 9$, then it holds for $n+2$ as well, as the left side grows by the factor $[(n+3)/2]$, whereas the right side grows by the factor $e^{2/e} < [(n+3)/2]$. So we are left to look at the cases $n \in \{5, 7, 8, 10\}$.

Suppose $n = 5$. The only maximal transitive subgroup of $\mathcal{S}_5$ not containing $\mathcal{A}_5$ is $A := C_5 \rtimes C_4$, and the only maximal transitive subgroup of $\mathcal{A}_5$ is $A \cap \mathcal{A}_5 =$

$C_5 \rtimes C_2$. So the index is 6, and these cases indeed occur and give 3c in Theorem 3 for $p = 5$.

Now assume $n = 7$. The only transitive subgroups of $\mathcal{S}_7$ which are maximal subject to not containing $\mathcal{A}_7$ are $\mathrm{AGL}_1(7)$ and $\mathrm{PSL}_3(2)$. Of course, the index of $\mathrm{AGL}_1(7)$ in $\mathcal{S}_7$ is much too big. The group $\mathrm{PSL}_3(2)$ is contained in $\mathcal{A}_7$, and has index 15. But the maximal order of an element in $\mathcal{A}_7$ is $7 < 15/2$, so this case does not occur by Lemma 3.21.

Now assume $n = 8$. Similarly as above, we see that the only case which does not directly contradict Lemma 3.21 is $A_1 = \mathrm{AGL}_3(2)$ inside $\mathrm{PSL}_4(2) \cong \mathcal{A}_8$. But then $A = \mathrm{PSL}_4(2)$ in the natural degree 15 action on the projective space. Lemma 3.48 shows that this case actually does not occur.

Finally, if $n = 10$, then we keep Bochert's bound, but we use Proposition 3.22 to see that the order of an element in $\mathcal{S}_{10}$ is at most $5^{\sqrt{5}} = 36.55\ldots$, hence at most 36. (The exact bound is 30.) So $5! \leq 2 \cdot 36$ by Lemma 3.21, a contradiction.

3.7.2. *Sporadic groups*

Let S be one of the 26 sporadic groups. Table 3.3 on page 411 contains information about small permutation degrees, big element orders, and the outer automorphism group. The atlas [9] contains all this information except for the maximal subgroups of the Janko group J_4, the Fischer groups Fi_{22}, Fi_{23}, and Fi'_{24}, the Thompson group Th, the baby monster B, and the monster group M. For the groups J_4, Fi_{22}, Fi_{23}, and Th we find the necessary information in [31–33], and [39], respectively. The bounds for the groups Fi'_{24}, B, and M are not sharp, and have been obtained as follows from the character tables in [9]: If M is a proper subgroup of S with index n, then the permutation character for the action of S on S/M is the sum of the trivial character and a character of degree $n-1$ which does not contain the trivial character. Thus $n-1$ is at least the degree of the smallest non–trivial character of S. (In view of the applications we have in mind we could have used this argument in most other cases as well.)

Now $S \leq A \leq \mathrm{Aut}(S)$ for a sporadic group S. Let $\sigma \in A$ be an element with only two cycles in the given permutation action. By Lemma 3.21 we get $\mu(S) \leq 2|\mathrm{Out}(S)|o(S)$. We see that the only possible candidates for S are the five Mathieu groups.

The atlas [9] provides the permutation characters of the simple groups of not too big order on maximal subgroups of low index. In the case of the Mathieu groups in the representations which are possible, we thus can immediately read off the cycle lengths of an element. Namely the atlas also tells in which conjugacy class a power of an element lies, so we can compute the fixed point numbers of all powers of a fixed element.

$\mathbf{S} = \mathbf{M_{11}}$. Then $A = \mathrm{M}_{11}$ either in the natural action of degree 11, or in the action of degree 12. The degree 11 case cannot occur for the following reason. By Lemma 3.21 $\mathrm{ord}(\sigma) \geq (2/3)11$, so $\mathrm{ord}(\sigma) = 8$ or 11. An element of order 11 is an 11–cycle. An element of order 8 has a fixed point, so if it would have two cycles, the other cycle length had to be 10, which is nonsense. Now look at the degree

12 action. Then of course an element of order 11 has cycle lengths 1 and 11, and one readily checks that an element of order 8 has cycle lengths 4 and 8, whereas an element of order 6 has a fixed point, hence must have more than 2 cycles.

S $=$ **M**$_{\mathbf{12}}$. The smallest degree of a faithful primitive representation of Aut(M_{12}) is 144 (see [9]), which is considerably too big. So we have $A = \mathrm{M}_{12}$ in its natural action. As $\mathrm{M}_{11} < \mathrm{M}_{12}$, the elements of order 11 and 8 in M_{11} with only two cycles appear also in M_{12}. Besides them, an element of order 10 has cycle length 2 and 10, and an element in one of the two conjugacy classes of elements of order 6 has cycle lengths 6.

S $=$ **M**$_{\mathbf{22}}$. We have the natural action of S of degree 22, and $A \leq \mathrm{M}_{22} \rtimes C_2$. An element of order 11 has two cycles of length 11. An element in S of order 8 has cycle lengths $2, 4, 8, 8$, so this element cannot be the square of an element with only 2 cycles. An element of order 7 has one fixed point, so it cannot arise either. And an element in S of order 6 has 6 cycles, so is out too.

S $=$ **M**$_{\mathbf{23}}$. Here $A = \mathrm{M}_{23}$ in the natural action of degree 23. An element of order 23 is a 23–cycle. Looking at the fixed points of elements of order 3 and 5 we see that an element of order 15 has cycle lengths $3, 5$, and 15. Similarly, an element of order 14 has cycle lengths $2, 7$, and 14. So this group does not occur at all.

S $=$ **M**$_{\mathbf{24}}$. Here $A = \mathrm{M}_{24}$ in the action on 24 points. One quickly checks that the elements of order 14 and 15 have a fixed point, so they do not occur. The elements of order $23, 21$, and from one of the two conjugacy classes of elements of order 12 have indeed two cycles of the lengths as claimed.

3.7.3. *Element orders in classical groups*

Suppose that S is a classical group. Our goal is to show that $S = \mathrm{PSL}_m(q)$, and that except for a few small cases, the action is the natural one on the projective space over $\mathbb{F}_q$. The main tool for doing that are good upper bounds for element orders in automorphism groups of classical groups.

The following lemma controls the maximal possible orders of elements in linear groups, if they are decorated with a field automorphism.

Lemma 3.24. *Let q be a power of the prime p, $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p$, and $G \leq \mathrm{GL}_n(\overline{\mathbb{F}_p})$ be a connected linear algebraic group defined over $\mathbb{F}_p$. For E a subfield of $\overline{\mathbb{F}_p}$, denote by $G(E)$ the group $G \cap \mathrm{GL}_n(E)$ of E–rational elements.*

Suppose that E is finite, and let $\gamma \in \mathrm{Aut}(E)$. Then $G(E)$ is normalized by $<\gamma>$. Take $g = \gamma h$ in the semidirect product of $<\gamma>$ with $G(E)$, where $h \in G(E)$. Let f be the order of γ, and F the fixed field in E of γ. Then g^f is conjugate in G to an element in $G(F)$.

Proof. Clearly $<\gamma>$ normalizes $G(E)$, as G is defined over $\mathbb{F}_p$. We compute

$$g^f = h^{\gamma^{f-1}} \cdots h^{\gamma} h,$$

thus

$$(g^f)^{\gamma} = h g^f h^{-1}.$$

Extend γ to $\overline{\mathbb{F}_p}$, and denote the induced action on G also by γ. By Lang's Theorem (see [57, Theorem 10.1]), the map $w \mapsto w^\gamma w^{-1}$ from G to G is surjective. Thus there is $b \in G$ with

$$h = b^\gamma b^{-1}.$$

Therefore

$$(b^{-1}g^f b)^\gamma = b^{-1}g^f b,$$

so $b^{-1}g^f b$ is fixed under γ, hence contained in $G(F)$. $\square$

In order to apply this lemma, we need the following easy estimate:

Lemma 3.25. *Let q, f, r be positive integers such that $2^f \leq q$. Then $f \cdot q^{r/f} \leq q^r$.*

Proof. We have

$$q^{r(1-1/f)} \geq 2^{r(f-1)} \geq 2^{f-1} \geq f,$$

and the claim follows after multiplying with $q^{r/f}$. $\square$

Lemma 3.26. *Let q be a power of the prime p. Let $\sigma \in \mathrm{GL}_n(q)$ act indecomposably on $V := \mathbb{F}_q^n$. Then the order of σ divides $p^b(q^u - 1)$, where u divides n, and $p^{b-1} \leq n/u - 1$ if $b > 0$. Furthermore, $\sigma^{p^b(q^u-1)/(q-1)}$ is a scalar, and $p^b(q^u - 1) \leq q^n - 1$. So in particular* $\mathrm{ord}(\sigma) \leq q^n - 1$, *and the order of the image of σ in* $\mathrm{PGL}_n(q)$ *is at most $(q^n - 1)/(q - 1)$.*

Proof. Write $\sigma = \sigma_{p'}\sigma_p$, where $\sigma_{p'}$ and σ_p are the p'–prime part and p–part of σ, respectively. Let

$$V = U_1 \oplus U_2 \oplus \cdots \oplus U_m,$$

be a decomposition into irreducible $\sigma_{p'}$–modules. Such a decomposition exists by Maschke's theorem. Let U be the sum of those U_i which are $\sigma_{p'}$–isomorphic to U_1. As σ_p commutes with $\sigma_{p'}$, we get that $U_i^{\sigma_p}$ is $\sigma_{p'}$–isomorphic to U_i for each i. By Jordan–Hölder, U is a σ–invariant direct summand of V. The indecomposability of V with respect to σ gives $U = V$, so all U_i are $\sigma_{p'}$–isomorphic.

Let u be the common dimension of U_i, so $n = um$. By Schur's Lemma, the restriction of $\sigma_{p'}$ to each U_i can be identified with an element of the multiplicative group of $\mathbb{F}_{q^u}$. As σ commutes with $\sigma_{p'}$, we can consider σ and σ_p as elements in $\mathrm{GL}_m(q^u)$. So either $\sigma_p = 1$, or $p^b := \mathrm{ord}(\sigma_p) \leq p(m-1)$ by Lemma 3.5. Also, with respect to this identification, $\sigma_{p'}$ is a diagonal matrix. So $\sigma_{p'}^{(q^u-1)/(q-1)}$ acts as a scalar $\lambda_i \in \mathbb{F}_q^\star$ on U_i. However, the λ_i are independent of i, because the U_i are $\sigma_{p'}$–isomorphic.

To finish the claim, we need to show that $p^b(q^u - 1) \leq q^{um} - 1$. This is clear for $b = 0$. For $b \geq 1$, this follows from $p^b \leq p(m-1)$ and

$$\frac{q^{um} - 1}{q^u - 1} = 1 + q^u + \cdots + q^{u(m-1)} \geq 1 + q^u(m-1) > p^b.$$

(Note that $b \geq 1$ implies $m > 1$.) $\square$

We obtain the following consequence

Proposition 3.27. *Let q be a prime power, and $n \geq 2$.*

1. *If $\sigma \in \Gamma\mathrm{L}_n(q)$, then* $\mathrm{ord}(\sigma) \leq q^n - 1$.
2. *If $\overline{\sigma} \in \mathrm{P}\Gamma\mathrm{L}_n(q)$, then* $\mathrm{ord}(\overline{\sigma}) \leq (q^n - 1)/(q - 1)$, *except for* $(n, q) = (2, 4)$.

Proof. First assume that $\sigma \in \mathrm{GL}_n(q)$, and denote by $\overline{\sigma}$ the image of σ in $\mathrm{PGL}_n(q)$. Let $\mathbb{F}_q^n =: V = V_1 \oplus \cdots \oplus V_r$ be a decomposition of V into σ–invariant and σ–indecomposable modules V_i. Let n_i be the dimension of V_i. By Lemma 3.26, the order of the restriction of σ to V_i divides $a_i := p^{b_i}(q^{u_i} - 1)$, where u_i divides n_i, and $a_i \leq q^{n_i} - 1$. The order of σ divides the least common multiple of the a_i. First suppose that $r > 1$. Then $q - 1$ divides each a_i, so

$$\begin{aligned}
\mathrm{ord}(\sigma) &\leq \mathrm{lcm}(a_1, \ldots, a_r) \\
&\leq (a_1 \cdots a_r)/(q - 1) \\
&\leq (q^{n_1} - 1) \cdots (q^{n_r} - 1)/(q - 1) \\
&\leq (q^n - 1)/(q - 1).
\end{aligned}$$

If however $r = 1$, then Lemma 3.26 applies directly. So in either case, (a) and (b) hold for $\mathrm{GL}_n(q)$ and $\mathrm{PGL}_n(q)$, respectively.

Now assume that $\sigma \in \Gamma\mathrm{L}_n(q) \setminus \mathrm{GL}_n(q)$, and let f be the smallest positive integer with $\sigma^f \in \mathrm{GL}_n(q)$. Note that $f \geq 2$. By Lemma 3.24, $\tau := \sigma^f$ is conjugate to an element $\tau' \in \mathrm{GL}_n(r)$, where $r := q^{1/f}$. (We take the natural inclusion $\mathrm{GL}_n(r) < \mathrm{GL}_n(q)$.) Part (a) is clear, as, by what we saw already, $\mathrm{ord}(\sigma) \leq f \mathrm{ord}(\sigma^f) < f r^n \leq q^n$, where we used Lemma 3.25 in the last step.

Part (b) requires a little more work. We have, similarly as above,

$$\mathrm{ord}(\overline{\sigma}) \leq f \frac{r^n - 1}{r - 1},$$

and are done once we know that

$$f \frac{r^n - 1}{r - 1} \leq \frac{r^{nf} - 1}{r^f - 1} = \frac{q^n - 1}{q - 1}$$

which is equivalent to

$$f \frac{r^f - 1}{r - 1} \leq \frac{r^{nf} - 1}{r^n - 1}. \tag{3.7}$$

Note that $(x^f - 1)/(x - 1) = 1 + x + \cdots + x^{f-1}$ is strongly monotonously increasing for $x > 1$, so inequality (3.7) holds once it holds for $n = 2$. In this case, we have to show that $f \leq (r^f + 1)/(r + 1)$. It is easy to see that this last inequality holds except for $f = 2, r = 2$. But then (3.7) is equivalent to $6 \leq 2^n + 1$, which is clearly the case for $n \geq 3$. □

Remark. $\mathrm{P\Gamma L}_2(4)$ is indeed an exception for part (b) of the previous theorem. Note that $\mathrm{P\Gamma L}_2(4) \cong \mathcal{S}_5$, so this group contains an element of order $6 > 5 = (4^2 - 1)/(4 - 1)$.

Lemma 3.28. *Let V be a vector space of dimension $n \geq 2$ over $\mathbb{F}_q$ with a non–degenerate bilinear form $\kappa = (\cdot, \cdot)$. Let $\tau \in \mathrm{Isom}(V, \kappa)$ be an isometry with respect to this form, and assume that τ is irreducible on V. Then n is even and the order of τ divides $q^{n/2} + 1$.*

Proof. By Schur's Lemma we have $V \cong \mathbb{F}_{q^n}$, and the action of τ induced on $\mathbb{F}_{q^n}$ is by multiplication with $\lambda \in \mathbb{F}_{q^n}^*$, where $\mathbb{F}_q[\lambda] = \mathbb{F}_{q^n}$. The eigenvalues of τ then are the powers λ^{q^i} for $i = 0, 1, \ldots, n-1$. Let $v_i \in V \otimes \mathbb{F}_{q^n}$ be an eigenvector to the eigenvalue λ^{q^i}. The form $(\cdot, \cdot)$ extends naturally to a non–degenerate form on $V \otimes \mathbb{F}_{q^n}$. Thus there exists i with $(v_0, v_i) = c \neq 0$. This gives $c = (v_0^\tau, v_i^\tau) = (\lambda v_0, \lambda^{q^i} v_i) = \lambda^{1+q^i}(v_0, v_i) = \lambda^{1+q^i} c$, so $\lambda^{1+q^i} = 1$. Thus $\lambda \in \mathbb{F}_{q^{2i}}$, so $n \mid 2i$. But $i < n$, hence $2i = n$, and the claim follows. □

Lemma 3.29. *Let V be a vector space over the finite field F with a non–degenerate symmetric, skew–symmetric, or hermitian form $\kappa = (\cdot, \cdot)$. Write $F = \mathbb{F}_q$ if κ is bilinear, and $F = \mathbb{F}_{q^2}$ if κ is hermitian. Let $\sigma \in \mathrm{Isom}(V, \kappa)$ be an isometry with respect to κ. Suppose that σ is semisimple and orthogonally indecomposable, but reducible on V. Then the following holds:*

$V = Z \oplus Z'$, where Z and Z' are σ–irreducible and totally isotropic spaces of the same dimension. Let Λ and Λ' be the set of eigenvalues of σ on Z and Z', respectively. Then

$$\Lambda' = \begin{cases} \{\lambda^{-1} \mid \lambda \in \Lambda\} & \text{if } \kappa \text{ is bilinear,} \\ \{\lambda^{-q} \mid \lambda \in \Lambda\} & \text{if } \kappa \text{ is hermitian.} \end{cases}$$

Furthermore, if κ is not skew–symmetric, then Z is not σ–isomorphic to Z'.

Proof. Let Z be a σ–invariant subspace of minimal positive dimension, in particular Z is σ–irreducible. Also $Z^\perp$ is σ–invariant. Furthermore, Z is totally isotropic, for otherwise $V = Z \perp Z^\perp$ by irreducibility of Z. As σ is semisimple, there is a σ–invariant complement Z' of $Z^\perp$ in V. From $\dim(Z') = \dim(V) - \dim(Z^\perp) = \dim(Z)$ and the minimality of $\dim(Z)$ we get that Z' is σ–irreducible as well. We get $V = Z \oplus Z'$ once we know that $Z \oplus Z'$ is not degenerate. But this follows from

$$(Z \oplus Z') \cap (Z \oplus Z')^\perp = (Z \oplus Z') \cap Z^\perp \cap (Z')^\perp = Z \cap (Z')^\perp = \{0\},$$

where the latter equality holds because Z' is a complement to $Z^\perp$, therefore Z is not contained in $(Z')^\perp$. Next we show the assertion about the eigenvalues if κ is bilinear. Let λ be an eigenvalue of σ with eigenvector $v \in Z \otimes \overline{\mathbb{F}_q}$. Let $w \in Z' \otimes \overline{\mathbb{F}_q}$

be such that $V \otimes \overline{\mathbb{F}_q}$ is the span of w and $v^\perp$, and that w is an eigenvector of σ. Let μ be the corresponding eigenvalue. By construction, $\rho := (v, w) \neq 0$, hence

$$\rho = (v, w) = (v^\sigma, w^\sigma) = (\lambda v, \mu w) = \lambda\mu\rho,$$

and the claim follows, as we can also switch the role of Z and Z' in this argument.

The case that κ is hermitian is completely analogous.

Finally, suppose that κ is not skew–symmetric, and assume in contrary that there is a σ–isomorphism $\phi : Z \mapsto Z'$. Let $R = \mathbb{F}_q[\sigma] \leq \mathrm{End}(V)$ be the algebra generated by σ. As κ is not skew–symmetric, there is an element $v \in V$ with $(v, v) \neq 0$. Write $v = z + z'$ with z and z' in Z and Z', respectively. Clearly z and z' are non–zero. By Schur's Lemma, R acts sharply transitively on the non–zero elements of Z', in particular, there is $\rho \in R$ such that $(z^\phi)^\rho = z'$. Let $\psi : Z \mapsto V$ be the homomorphism defined by $w^\psi := w + (w^\phi)^\rho$. This map is clearly injective, ψ commutes with σ, so the image Z^ψ has the same dimension as Z, and of course is σ–irreducible as well. By construction, the element $v = z^\psi$ is not isotropic, so Z^ψ is not totally isotropic, thus κ restricted to Z^ψ is not degenerate. We get $V = Z^\psi \perp (Z^\psi)^\perp$, contrary to indecomposability. ☐

Remark. Let V be 2–dimensional with a non–degenerate skew–symmetric form, and σ the identity map. As V is clearly not the orthogonal sum of two 1-dimensional spaces, we cannot dispense of the assumption that κ is not skew–symmetric in the last part of the lemma.

We now extend the previous lemma to those σ which are not necessarily semisimple.

Lemma 3.30. *Let V be a vector space over $\mathbb{F}_q$ with a non–degenerate symmetric, skew–symmetric, or hermitian form $\kappa = (\cdot, \cdot)$. Let $\sigma \in \mathrm{Isom}(V, \kappa)$ be an isometry with respect to this form. Assume that σ is orthogonally indecomposable, but reducible on V. Denote by $\sigma_{p'}$ the p'–part of σ. Then the following holds:*

$$V = (U_1 \perp U_2 \perp \ldots \perp U_r) \perp ((Z_1 \oplus Z_1') \perp \ldots \perp (Z_s \oplus Z_s')),$$

where the U_i, Z_i and Z_i' are $\sigma_{p'}$–irreducible, the U_i and $(Z_i \oplus Z_i')$ are not degenerate, the Z_i and Z_i' are totally isotropic and the U_i, Z_i and Z_i' have all the same dimension. Also, $r + 2s \geq 2$.

Proof. Choose an orthogonal decomposition of V into non–trivial $\sigma_{p'}$–invariant subspaces of maximal length, so these subspaces do not decompose orthogonally into smaller $\sigma_{p'}$–invariant spaces. Let the U_i be those subspaces which are $\sigma_{p'}$–irreducible, and let the $(Z_i \oplus Z_i')$ be the remaining ones according to the previous lemma.

The $\sigma_{p'}$–homogeneous components $H_1, H_2, \ldots$ are σ–invariant as a consequence of Jordan–Hölder. Let H be the sum of those H_k where the irreducible summands of H_k have the same dimension as those of H_1. Then Z_i appears in H if and only if Z_i' appears in H. The orthogonal indecomposability of σ forces $H = V$.

Suppose that $r + 2s < 2$. Then $s = 0$ and $r = 1$, that is σ is irreducible on $V = U_1$, a contradiction. □

Lemma 3.31. *Let $q \geq 2$ and $m_1, m_2, \dots, m_\rho$ be distinct positive integers with sum m. Then*

$$\prod_{i=1}^{\rho}(q^{m_i} + 1) \leq e^{1/(q-1)} q^m.$$

Proof. For x real we have $1 + x \leq e^x$. Substitute $x = 1/q^{m_i}$ and multiply by q^{m_i} to obtain

$$q^{m_i} + 1 \leq q^{m_i} e^{1/q^{m_i}}.$$

Multiply these inequalities for $i = 1, 2, \dots, \rho$ to obtain

$$\prod(q^{m_i} + 1) \leq q^m e^{\Sigma},$$

with

$$\Sigma = \sum_{i=1}^{\rho} \frac{1}{q^{m_i}} \leq \sum_{k=1}^{\infty} \frac{1}{q^k} = \frac{1}{q-1},$$

as the m_i are distinct. The claim follows. □

Lemma 3.32. *Use the notation from Lemma* 3.30 *with κ bilinear, and let z be the common dimension of the spaces Z_i, Z_i', U_i. Set $w := r + 2s$, thus $v := \dim(V) = wz$. Then there is a non–negative integer b, such that* $\mathrm{ord}(\sigma)$ *divides $p^b(q^z - 1)$. Furthermore,*

$$\mathrm{ord}(\sigma) \leq \begin{cases} 2q^{[v/2]} & \textit{in any case,} \\ q^{[v/2]} & \textit{if } \mathrm{ord}(\sigma) \textit{ is odd,} \\ q^{[v/2]} & \textit{if } q \textit{ is even, and } (q, w, z) \neq (2, 2, 2) \textit{ or } (2, 3, 2), \end{cases}$$

If $q = 2$ and $v = 4$ or 6 and $\mathrm{ord}(\sigma) > 2^{v/2}$, then $\mathrm{ord}(\sigma) = 6$ if $v = 4$, and $\mathrm{ord}(\sigma) = 12$ if $v = 6$.

Proof. As the spaces Z_i, Z_i', and U_i are all $\sigma_{p'}$–irreducible of dimension z, it follows that the order of $\sigma_{p'}$ divides $q^z - 1$. Let p^b be the order of the p–part of σ. As $w \geq 2$, hence $z \leq [v/2]$, the stated inequalities clearly hold for $b = 0$. Thus assume $b \geq 1$ from now on.

First assume $p > 2$. We are clearly done except if

$$p^b(q^z - 1) > 2q^{[wz/2]}. \tag{3.8}$$

From (3.8) we obtain

$$p^b q^z > 2q^{[wz/2]}.$$

As each factor except 2 is divisible by p, we obtain from that even sharper

$$p^b q^z \geq p q^{[wz/2]},$$

hence

$$p^{b-1} q^z \geq q^{[wz/2]}. \tag{3.9}$$

Let w' be the number of elements in a maximal subset of the summands Z_i, Z_i', and U_i which are pairwise $\sigma_{p'}$–isomorphic. Then the restriction of σ_p to the sum of these spaces can be seen as an element in $\mathrm{GL}_{w'}(q^z)$, so the order of this restriction is bounded by $p(w'-1)$, see Lemma 3.5. Clearly $w' \leq w$, hence $p^{b-1} \leq w-1$. So with (3.9) we obtain further

$$w - 1 \geq q^{[wz/2]-z}.$$

We first contend that $w \leq 5$, and that $z = 1$ if $w > 2$. For suppose $z \geq 2$. Then $[wz/2] - z \geq w - 2$, as $w \geq 2$. So $w - 1 \geq q^{w-2}$, which gives $w = 2$. Is is easy to see that $w - 1 \geq q^{[w/2]-1}$ gives $w \leq 5$. Suppose $w = 4$ or 5. We obtain $q = 3$. Furthermore, $b \leq 2$, so $b = 2$ for otherwise we are done (check (3.9)). As V decomposes into 1–dimensional eigenspaces for $\sigma_{3'}$, the eigenvalues are in $\mathbb{F}_3 \setminus \{0\}$, so we have that $\mathrm{ord}(\sigma_{3'})$ is at most 2, hence the order of σ is at most $2 \cdot 3^2 = 18$, the exact bound we wanted to prove (and which is sharp indeed).

Now suppose $w = 3$. Clearly $b = 1$. We have either $r = 3, s = 0$, or $r = 1$, $s = 1$. In the first case $\sigma_{p'}$ restricts to an element of order at most 2 on each U_i, so the order of σ divides $2p$, and the claim follows. Thus assume $r = 1, s = 1$. Let λ be the eigenvalue of $\sigma_{p'}$ on U_1. Clearly $\lambda = \pm 1$. Also, λ is an eigenvalue on Z_1 or Z_1', for otherwise U_1 were σ–invariant, contrary to orthogonal irreducibility. By Lemma 3.29 the eigenvalues on Z and Z' then are ± 1, so the order of $\sigma_{p'}$ is at most 2, and we are done again.

Finally, we have to look at $w = 2$. Here we have not necessarily $z = 1$. First suppose that $s = 0$, that is $V = U_1 \oplus U_2$. The order of $\sigma_{p'}$ on V divides $q^{[z/2]} + 1$. The claim follows as $p(q^{[z/2]} + 1) \leq 2q^z = 2q^{[v/2]}$. Thus suppose that $r = 0, s = 1$, so $V = Z_1 \oplus Z_1'$. Let $\lambda \in \mathbb{F}_{q^z}$ be an eigenvalue of $\sigma_{p'}$ on Z_1. By irreducibility, the eigenvalues of $\sigma_{p'}$ on Z_1 are λ^{q^i} for $i = 0, 1, \dots, z-1$. By Lemma 3.29, the inverses of these eigenvalues are the eigenvalues of $\sigma_{p'}$ on Z_1'. We contend that these two sets are the same. Namely as σ is not semisimple, it cannot leave invariant both Z_1 and Z_1'. So without loss $Z_1^{\sigma_p} \neq Z_1$, and we obtain that Z_1 and Z_1' are $\sigma_{p'}$–isomorphic by Jordan–Hölder. So the set of eigenvalues on Z_1 is closed under inversion, in particular there is an i such that $\lambda^{-1} = \lambda^{q^i}$. This gives $\lambda^{q^{2i}-1} = 1$, so $\lambda \in \mathbb{F}_{q^{2i}}$. We obtain that z divides $2i < 2z$, as $\mathbb{F}_{q^z} = \mathbb{F}_q[\lambda]$. If $i = 0$, then $\lambda = \pm 1$, so $\sigma_{p'}$ has order at most 2, and the claim clearly follows, as $b = 1$. If $i > 0$, then $z = 2i$, so the order of $\sigma_{p'}$ divides $q^{z/2} + 1$, and the claim follows again from $(q^{z/2} + 1)p < 2q^{z/2} q \leq 2q^z = 2q^{[v/2]}$.

We are left to look at the case $p = 2$. As the form is not degenerate, we have necessarily $v = wz$ even. We proceed similarly as above. Recall that $b \geq 1$. We are done unless

$$2^b(q^z - 1) > q^{wz/2}. \tag{3.10}$$

From that we obtain

$$2^b > q^{wz/2-z},$$

hence

$$2^{b-1} \geq q^{wz/2-z}, \qquad w - 1 \geq q^{wz/2-z}, \tag{3.11}$$

as $2^{b-1} \leq w - 1$. If $z \geq 2$, then $w - 1 \geq q^{w-2}$, hence either $w = 3, q = 2, z = 2$; or $w = 2$. The first case gives $2^{b-1} \leq w - 1 = 2$, so $b \leq 2$, hence $\mathrm{ord}(\sigma) = 12$ or $\leq 6 < 2^3 = 2^{v/2}$.

Thus we have $z = 1$ except possibly for $w = 2$. First assume $w > 2$, so $w \geq 4$ is even. We obtain $w \leq 6$ from (3.11). Suppose $w = 6$. Then $q = 2$ and $b \leq 3$, and we obtain a contradiction to (3.10). Next suppose $w = 4$. Again $q = 2$. From (3.10) we obtain $2^b > 2^2$, hence $b \geq 3$, a contradiction to $4 \leq 2^{b-1} \leq w - 1 = 3$.

Finally, suppose $w = 2$. Clearly $b = 1$. The argument from the last paragraph in the case $p > 2$ shows that the critical case is when z is even and $\mathrm{ord}(\sigma)$ divides $2(q^{z/2} + 1)$. Now

$$2(q^{z/2} + 1) = q^z - ((q^{z/2} - 1)^2 - 3) \leq q^z = q^{[v/2]}$$

except for $q = 2, z = 2$. □

Proposition 3.33. *Let $\sigma \in \mathrm{GL}_n(q)$ be an isometry with respect to a non-degenerate skew–symmetric or symmetric bilinear form on $\mathbb{F}_q^n$. Then*

$$\mathrm{ord}(\sigma) \leq \begin{cases} 2q^{[n/2]} & \text{if } q \text{ is odd,} \\ q^{[n/2]} & \text{if } q \text{ and } \mathrm{ord}(\sigma) \text{ are odd,} \\ e^{1/(q-1)}q^{[n/2]} < 2q^{[n/2]} & \text{if } q \neq 2 \text{ is even,} \\ (3e/2)2^{[n/2]} & \text{if } q = 2. \end{cases}$$

Proof. Choose a decomposition of V into orthogonally indecomposable σ-invariant subspaces. The order of σ is the least common multiple of the orders of the restriction of σ to these subspaces. Lemmas 3.28 and 3.32 give upper bounds for these orders.

In the following we use several times the trivial inequality

$$[u_1/2] + [u_2/2] + \cdots + [u_k/2] \leq [(u_1 + u_2 + \cdots + u_k)/2]$$

for integers u_i.

First suppose that q is odd. Let U be such a subspace of dimension u. If U is σ–irreducible, then $\mathrm{ord}(\sigma|_U)$ is at most $q^{[u/2]} + 1$, so the order is at most $(q^{[u/2]} +$

$1)/2 \leq q^{[u/2]}$ if $\mathrm{ord}(\sigma|_U)$ is odd, and at most $q^{[u/2]} + 1 \leq 2q^{[u/2]}$ otherwise. The assertion follows if $U = V$. So suppose $U < V$. By induction, the stated bound holds for the restriction of σ to $U^\perp$. Let $\overline{u} = \dim(U^\perp)$. If the orders of the restriction of σ to U and $U^\perp$ are relatively prime, then at least one of the orders is odd, and we obtain the claim by multiplying the corresponding upper bounds. If these orders are not relatively prime, then the product of these orders divided by 2 is an upper bound for the order of σ, so the claim holds as well.

Now suppose that q is even. Let W_i be those subspaces from above on which σ acts irreducibly, and let W be the sum of these spaces. Set $w := \dim(W)$, and let $1 < w_1 < w_2 < \dots$ be the distinct dimensions of the spaces W_i. Note that if $\dim(W_i) = 1$, then the restriction of σ to W_i is trivial. By Lemma 3.28, the w_i are even, and the order of the restriction of σ to the associated space divides $q^{w_i/2} + 1$. Thus the order of $\sigma|_W$ divides the product of the $q^{w_i/2}+1$. This product is less than $e^{1/(q-1)} q^{[w/2]}$ by Lemma 3.31. If $q \neq 2$, then apply the bounds in Lemma 3.32 to the summands of $W^\perp$ to get the claim. Finally suppose $q = 2$. We are done except if one of the summands Q of $W^\perp$ has dimension 4 or 6, and $\sigma|_Q$ has order 6 or 12, respectively. The stated inequality then holds for $W \perp Q$. If there are more such summands Q' in $W^\perp$, then they do contribute at most by a factor $2 < 2^{[\dim(Q')/2]}$ to the order of σ. All other summands of dimension r contribute by a factor of at most $2^{[r/2]}$, so the claim follows. □

In a few places we need the following trivial fact:

Lemma 3.34. *Let $1 \leq i < m$ and $q \geq 2$ be integers. Let ε be -1 or 1. Then*

$$\frac{(q^m + \varepsilon)(q^{m-1} - \varepsilon)}{q^i - 1} > q^{2m-1-i}.$$

Proof. Clearly $q^{m-i} - 1 \geq \varepsilon(q-1)$. Multiply by q^{m-1} to get $q^{2m-1-i} - q^{m-1} \geq \varepsilon(q^m - q^{m-1})$, hence $q^{2m-1-i} - 1 > \varepsilon(q^m - q^{m-1})$. But this inequality is equivalent to the stated one. □

As before denote by $\mu(S)$ and $o(S)$ a lower bound for the degree of a faithful permutation representation and an upper bound for the order of an element, respectively. The minimal permutation degrees $\mu(S)$ have been determined by Cooperstein and Patton – we use the "corrected" list [30, Theorem 5.2.2] which still contains a mistake (giving the wrong μ for $P\Omega_{2m}^+(3)$). We exclude the group $\mathrm{PSL}_2(5)$, as $\mathrm{PSL}_2(5) \cong \mathcal{A}_5$, a case we already dealt with. Besides that, the list [30, Theorem 5.2.2] contains a few duplications. Accordingly, we drop $\mathrm{PSp}_4(3)$ in view of $\mathrm{PSp}_4(3) \cong \mathrm{PSU}_4(2)$ and $\mathrm{Sp}_4(2)'$ in view of $\mathrm{Sp}_4(2)' \cong \mathrm{PSL}_2(9)$.

Assume that the almost simple group A acts primitively and contains an element with at most two cycles. We consider the case that the minimal normal subgroup S of A is a classical group. The aim of this section is to show that S is isomorphic $\mathrm{PSL}_m(q)$, a case to be handled afterwards.

3.7.4. *S symplectic*

Lemma 3.35. *Let $S = \mathrm{PSp}_{2m}(q)$ be the simple symplectic group, and $\sigma \in \mathrm{Aut}(S)$. Then*

$$\mathrm{ord}(\sigma) \le \begin{cases} 4q^m & \text{if } q \text{ is odd,} \\ e^{1/(q-1)}q^m & \text{if } q \neq 2 \text{ is even, } m \ge 3, \\ 2e^{1/(q-1)}q^2 & \text{if } q \neq 2 \text{ is even, } m = 2, \\ (3e/2)2^m & \text{if } q = 2, m \ge 3. \end{cases}$$

In particular, $\mathrm{ord}(\sigma) \le 4q^m$ *if* $q \neq 2$.

Proof. Let $q = p^r$ with p a prime. If q is odd, then $\mathrm{Out}(S) = C_2 \times C_r$, see [30, Theorem 2.1.4, Prop. 2.4.4], where C_r comes from a field automorphism. Thus σ^2 has a preimage τ in $\mathrm{Sp}_{2m}(q) \rtimes \mathrm{Aut}(\mathbb{F}_q)$. Let f be the order of the associated field automorphism. By Lemma 3.24, τ^f is conjugate to an element in the group $\mathrm{Sp}_{2m}(q^{1/f})$, whose element orders are bound by $2q^{m/f}$ by Proposition 3.33. Thus τ has order at most $2fq^{m/f} \le 2q^m$, where we used Lemma 3.25. The claim follows in the odd case.

If q is even, then $\mathrm{Out}(S) = C_r$ if $m \ge 3$. Argue as above. If $m = 2$, then $\mathrm{Out}(S)$ is cyclic of order $2r$, and the square of a generator is a field automorphism, see [8, Chapter 12]. The claim follows as above. □

Now we rule out the symplectic groups in the order as they appear in Table 3.1 on page 410.

$\mathbf{m \ge 2}$, $\mathbf{q \ge 3}$, $\mathbf{(m, q) \neq (2, 3)}$. Let $\sigma \in \mathrm{Aut}(S)$. The minimal faithful permutation degree of S is $(q^{2m} - 1)/(q - 1)$. As $q \ge 3$, we get $\mathrm{ord}(\sigma) \le 4q^m$ by the previous Lemma. So Lemma 3.21 gives

$$\frac{q^{2m} - 1}{q - 1} \le 2\mathrm{ord}(\sigma) \le 2 \cdot 4 \cdot q^m.$$

Note that the left hand side is bigger than q^{2m-1}, so it follows that $q^{m-1} < 8$. Thus $m = 2$ and $q \le 7$. But $(7^4 - 1)/(7 - 1) = 400 > 392 = 8 \cdot 7^2$, so $q = 7$ is out. Thus $q = 4$ or 5. But $\mathrm{ord}(\sigma) \le 20$ for $q = 4$, and $\mathrm{ord}(\sigma) \le 30$ for $q = 5$, see the atlas [9]. These improved bounds contradict the above inequality.

$\mathbf{m \ge 3}$, $\mathbf{q = 2}$. We get $\mu(S) = 2^{m-1}(2^m - 1) \le 2(3e/2)2^m$, hence $2^m - 1 \le 6e$, so $m = 3$ or 4. If $m = 4$, then the atlas gives $\mathrm{ord}(\sigma) \le 30$, contrary to $\mu(S) \le 2\mathrm{ord}(\sigma)$. Thus $m = 3$. The atlas gives $\mathrm{ord}(\sigma) \le 15$, and the next biggest element order is 12. Also, there is a maximal subgroup of index 28, and the next smallest has index 36. So $\mathrm{ord}(\sigma) = 15$ and $n = 28$. But $15 = \mathrm{lcm}(k, 28 - k)$ has no solution, therefore σ must have more than 2 cycles in this representation.

3.7.5. *S orthogonal in odd dimension*

Lemma 3.36. *Let $S = \Omega_{2m+1}(q)$ be the simple orthogonal group with q odd, $m \ge 3$, and $\sigma \in \mathrm{Aut}(S)$. Then*

$$\mathrm{ord}(\sigma) \le 2q^m.$$

Proof. Set $V = \mathbb{F}_q^{2m+1}$, $\overline{V} = V \otimes \overline{\mathbb{F}_q}$, and let κ be the standard bilinear form on $\overline{V}$. The algebraic group $G := \mathrm{SL}(\overline{V}) \cap \mathrm{Isom}(\overline{V}, \kappa)$ is connected. Let σ be in $\mathrm{Aut}(S)$. By the structure of the automorphism group of S (see [30, Prop. 2.6.3]), we find a preimage τ of σ in $\mathrm{Isom}(V, \kappa) \rtimes \mathrm{Aut}(\mathbb{F}_q)$. As $\mathrm{Isom}(V, \kappa)$ is an extension of $G(\mathbb{F}_q)$ by the scalar -1, we may assume that $\tau \in G(\mathbb{F}_q) \rtimes \mathrm{Aut}(\mathbb{F}_q)$. Now use Lemma 3.24 together with Proposition 3.33 and Lemma 3.25 to get the conclusion. □

$\mathbf{m \geq 3}$, $\mathbf{q \geq 5}$ odd. We get a stronger inequality as in the previous case $S = \mathrm{PSp}_{2m}(q)$, where we saw that there is no solution for $m \geq 3$.

$\mathbf{m \geq 3}$, $\mathbf{q = 3}$. We get $3^m(3^m - 1)/2 \leq 2 \cdot 2 \cdot 3^m$, hence $3^m \leq 9$, so $m \leq 2$, a contradiction.

3.7.6. *S Orthogonal of Plus Type*

Lemma 3.37. *Let $S = P\Omega_{2m}^+(q)$ be the simple orthogonal group with Witt defect 0, and $\sigma \in \mathrm{Aut}(S)$. Write $q = p^f$ for p a prime. Then*

$$\mathrm{ord}(\sigma) \leq \begin{cases} 4fq^m \leq 2q^{m+1} & \text{if } q \text{ is odd, } m \geq 5, \\ 8fq^4 \leq 4q^5 & \text{if } q \text{ is odd, } m = 4, \\ 2fq^m \leq q^{m+1} & \text{if } q \neq 2 \text{ is even, } m \geq 5, \\ (9/2)fq^4 \leq (9/4)q^5 & \text{if } q \neq 2 \text{ is even, } m = 4, \\ (3e/2)2^m & \text{if } q = 2, m \geq 5, \\ 30 & \text{if } q = 2, m = 4. \end{cases}$$

Proof. Let κ be the bilinear form associated to S. First suppose that $m \geq 5$. Assume q odd first. Then σ^{2f} has a preimage in $\mathrm{Isom}(\mathbb{F}_q^{2m}, \kappa)$, this follows from the structure of the automorphism group of S, see [30, Theorem 2.1.4, Table 2.1.D]. Now apply Proposition 3.33, and note that $2f \leq q$. If q is even, then σ^f already has a preimage in $\mathrm{Isom}(\mathbb{F}_q^{2m}, \kappa)$, hence if $q \neq 2$, then $\mathrm{ord}(\sigma) \leq fe^{1/(q-1)}q^m < 2fq^m \leq q^{m+1}$ by Proposition 3.33, or $\mathrm{ord}(\sigma) \leq (3e/2)2^m$ if $q = 2$.

Now suppose that $m = 4$. We have $\mathrm{Out}(P\Omega_8^+(q)) \cong \mathcal{S}_3 \times C_f$ if q is even, and $\cong \mathcal{S}_4 \times C_f$ if q is odd, see [30, p.38]. Thus if q is odd, then either σ^{3f} or σ^{4f} has a preimage in $\mathrm{Isom}(\mathbb{F}_q^{2m}, \kappa)$, so $\mathrm{ord}(\sigma)$ is at most $4f$ times the maximal order of an element in $\mathrm{Isom}(\mathbb{F}_q^{2m}, \kappa)$, and we use Proposition 3.33 again. If $q \neq 2$ is even, then analogously $\mathrm{ord}(\sigma) \leq 3fe^{1/(q-1)}q^4 \leq 3e^{1/3}fq^4 < (9/2)fq^4$. If $q = 2$, then use the atlas information [9]. □

$\mathbf{m \geq 4}$, $\mathbf{q \geq 4}$. First suppose that $m \geq 5$. We get

$$\frac{(q^m - 1)(q^{m-1} + 1)}{q - 1} \leq 2\mathrm{ord}(\sigma) \leq 4q^{m+1}.$$

The left hand side is bigger than q^{2m-2} by Lemma 3.34, so we obtain further $q^{2m-2} < 4q^{m+1}$, hence $q^2 \leq q^{m-3} < 4$, a contradiction.

Next assume $m = 4$. First assume q odd. Similarly as above we obtain $q^6 < 16fq^4 \leq 8q^5$. Note that if $f = 1$, then $q < 4$, a contradiction. Thus assume $f \geq 2$. We obtain $q < 8$, so $f = 2$, hence $q^2 < 32$, thus $q \leq 5$, giving the contradiction $f = 1$.

Now assume that $q \neq 2$ is even. We obtain $q^6 < 2 \cdot (9/4)q^5$, hence $q = 4$. But $\operatorname{ord}(\sigma) \leq (9/4)4^5 = 2304$, whereas $\mu(S) = 5525 > 2 \cdot 2304$, a contradiction.

$\mathbf{m \geq 4}$, $\mathbf{q = 3}$. First consider $m = 4$. One verifies that $o(P\Omega_8^+(3)) = 40$, so $\operatorname{ord}(\sigma) \leq 4 \cdot 40 = 160$, because $\operatorname{Out}(P\Omega_8^+(3)) = \mathcal{S}_4$. In view of $\mu(S) = 1080$ this case is out. Suppose $m \geq 5$. We obtain $3^{m-1}(3^m - 1)/2 \leq 2 \cdot 2 \cdot 3^{m+1}$, hence $m < 5$, a contradiction.

$\mathbf{m \geq 4}$, $\mathbf{q = 2}$. If $m = 4$, then $\operatorname{ord}(\sigma) \leq 30$, whereas $\mu(S) = 120$, so this case is out. Suppose $m \geq 5$. We obtain $2^{m-1}(2^m - 1) \leq 2 \cdot (3e/2)2^m$, hence $2^m \leq 6e + 1 = 17.3\ldots$, thus $m \leq 4$, a contradiction.

3.7.7. *S orthogonal of minus type*

Lemma 3.38. *Let $S = P\Omega_{2m}^-(q)$ be the simple orthogonal group with Witt defect* 1*, and $\sigma \in \operatorname{Aut}(S)$. Write $q = p^f$ for p a prime. Then*

$$\operatorname{ord}(\sigma) \leq \begin{cases} 4fq^m \leq 2q^{m+1} & \text{if } q \text{ is odd}, m \geq 4, \\ 2fq^m \leq q^{m+1} & \text{if } q \neq 2 \text{ is even}, m \geq 4, \\ (3e/2)2^m & \text{if } q = 2, m \geq 4, \\ 30 & \text{if } q = 2, m = 4, \\ 60 & \text{if } q = 2, m = 5. \end{cases}$$

Proof. The proof follows exactly as in Lemma 3.37, except that for $m = 4$, there is no exceptional (graph) automorphism of order 3. For $q = 2$ and $m = 4$ or 5 use the atlas [9]. ☐

Now $S = P\Omega_{2m}^-(q)$ for $m \geq 4$. From Lemma 3.34 we get $\mu(S) > q^{2m-2}$. First suppose $q \neq 2$. We obtain $q^{2m-2} < 2 \cdot 2q^{m+1}$, hence $q^{m-3} < 4$. Thus $m = 4$ and $q = 3$. But this contradicts the sharper bound $\operatorname{ord}(\sigma) \leq 4 \cdot 3^4 = 324$. If $q = 2$, then $2^{2m-2} < 2 \cdot (3e/2)2^m$, hence $2^{m-2} \leq 3e = 8.1\ldots$, so $m \leq 5$. Arrive at a contradiction using the upper bounds for $\operatorname{ord}(\sigma)$ from Lemma 3.38.

3.7.8. *S unitary*

Lemma 3.39. *Suppose that $\sigma \in \operatorname{GU}_n(q)$ acts irreducibly on $\mathbb{F}_q^n$. Then n is odd, and* $\operatorname{ord}(\sigma)$ *divides $q^n + 1$. The order of the image of σ in* $\operatorname{PGU}_n(q)$ *divides $(q^n + 1)/(q + 1)$.*

Proof. Let λ be an eigenvalue of σ. Then $\mathbb{F}_{q^2}[\lambda] = \mathbb{F}_{q^{2n}}$. All the eigenvalues of σ are $\lambda^{q^{2i}}$ with $i = 1, \cdots, n$. Similarly as in the proof of Lemma 3.28, there exists an index i in the given range such that $\lambda^{-q} = \lambda^{q^{2i}}$, so

$$\lambda^{q^{2i-1}+1} = 1. \tag{3.12}$$

It follows that $\lambda^{q^{4i-2}-1} = 1$, so $\lambda \in \mathbb{F}_q^{4i-2}$. Therefore $n \mid 2i-1 < 2n$, so $n = 2i-1$. The assertion about the order of σ follows from (3.12). By the irreducibility, the element σ is a subgroup of a Singer group of order $q^{2n}-1$ on $\mathbb{F}_{q^2}^n$. The (unique) subgroup of order $q+1$ of this Singer group consists of scalars, because $q+1$ divides q^2-1. Also, $q+1$ divides q^n+1, so modulo scalars σ has order at most $(q^n+1)/(q+1)$. □

Lemma 3.40. *Let $\sigma \in \mathrm{GU}_n(q)$, and denote by $\overline{\sigma}$ the image of σ in $\mathrm{PGU}_n(q)$. Let $q = p^f$ with p prime. The following holds.*

1. *If $n = 1$, then* $\mathrm{ord}(\sigma)$ *divides $q+1$.*
2. *If $n = 2$, then* $\mathrm{ord}(\sigma)$ *divides q^2-1 or $p(q+1)$.*
3. *If $n = 3$, then* $\mathrm{ord}(\sigma)$ *divides q^3+1, q^2-1, or $p^r(q+1)$ with $r \le 2$ and $r = 1$ if $p > 2$. Furthermore,* $\mathrm{ord}(\overline{\sigma})$ *divides q^2-q+1, q^2-1 or $p(q+1)$. For $p = 2$, there is the additional possibility* $\mathrm{ord}(\overline{\sigma}) = 4$.
4. *If $n = 4$, then* $\mathrm{ord}(\overline{\sigma})$ *divides q^3+1, q^3-q^2+q-1, or $p^r(q^2-1)$ where $r \le 2$ and $r = 1$ if $p > 2$. For $p = 3$, there is the additional possibility* $\mathrm{ord}(\overline{\sigma}) = 9$.

Proof. Denote by $\sigma_{p'}$ the p'–part of σ. Set $F = \mathbb{F}_{q^2}$, so $\mathrm{GU}_n(q)$ is the isometry group of the unique hermitian from on F^n. The case $n = 1$ is trivial.

Suppose that $n = 2$. By Lemma 3.39, σ is reducible on $V = F^n$. If σ is semisimple, then the eigenvalues of σ are in F, so $\mathrm{ord}(\sigma) \mid q^2-1$. If σ is not semisimple, then $\sigma_{p'}$ is the centralizer of an element of order p, hence $\sigma_{p'}$ is a scalar, and the claim follows again.

Now assume $n = 3$. If σ is irreducible, then apply Lemma 3.39. If σ is orthogonally decomposable, then apply (a) and (b) to get that $\mathrm{ord}(\sigma)$ divides q^2-1 or $p(q+1)$. Next assume σ reducible, but orthogonally indecomposable. Choose a maximal orthogonal decomposition of V in $\sigma_{p'}$–invariant subspaces. By Lemma 3.29 and the notation from there, either $V = U_1 \perp U_2 \perp U_3$, or $V = U_1 \perp (Z_1 \oplus Z_1')$. Assume the first possibility. By orthogonal irreducibility of σ, the U_i are pairwise $\sigma_{p'}$–isomorphic, thus $\sigma_{p'}$ is a scalar on V, with order dividing $q+1$. Let p^r be the order of the p–part of σ. Then $p^{r-1} \le 2$ by Lemma 3.5, and we get the divisibilities as stated. If we have the latter orthogonal decomposition, then U_1 must be $\sigma_{p'}$–isomorphic to Z_1 or Z_1', say to Z_1. On the other hand, Z_1 and Z_1' are not $\sigma_{p'}$–isomorphic by Lemma 3.29. We get that σ_p leaves invariant $U_1 \perp Z_1$ and Z_2, thus the order of σ_p divides p. The order of $\sigma_{p'}$ divides $q+1$, because the restriction to U_1 satisfies this, so this holds also for the restriction to Z_1, and then also for the restriction to Z_1' by Lemma 3.29.

Now assume $n = 4$. Let p^b be the order of σ_p. First assume that $\sigma_{p'}$ is orthogonally decomposable. From (a), (b), and (c), we get that $\mathrm{ord}(\sigma_{p'})$ divides q^2-1 or q^3+1. If the latter occurs, then $b = 0$. If $b \ge 2$, then $b = 2$, and either $p = 3$, and σ_3 acts indecomposably on V, or $p = 2$. In the former case $\sigma_{3'}$ must be a scalar, so $\mathrm{ord}(\overline{\sigma})$ divides 9. Next assume that $\sigma_{p'}$ acts orthogonally indecomposably on V. Then $V = Z_1 \oplus Z_1'$ with $\dim(Z_1) = 2$. Let $\lambda \in \mathbb{F}_{q^4}$ be an eigenvalue on Z_1. Then the other eigenvalue is λ^{q^2}, and Lemma 3.29 tells us that the eigenvalues on Z_1' are λ^{-q} and λ^{-q^3}. Set $m = q^3 - q^2 + q - 1$. Raising these 4 eigenvalues to the m–th power gives equal values (use $\lambda^{q^4} = \lambda$), hence $\sigma_{p'}^m$ is a scalar. Also, $\sigma_p = 1$, because Z_1 and Z_1' are not $\sigma_{p'}$–isomorphic by Lemma 3.29. We get the stated divisibilities. □

Lemma 3.41. *Let $q = p^f \geq 3$ for a prime p. Then each element in* $\mathrm{Aut}(\mathrm{PSU}_4(q))$ *has order at most* $\max(2, f) \cdot (q^3 + 1)$.

Proof. Let $\sigma \in \mathrm{GU}_4(q) \rtimes \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_p)$ be a preimage of a given element $\overline{\sigma} \in \mathrm{Aut}(\mathrm{PSU}_4(q))$. Let r be smallest positive integer with $\sigma^r \in \mathrm{GU}_4(q)$, so r divides $2f$. If $r < 2f$, then $r \leq f$, and $\overline{\sigma}^r \in \mathrm{PGU}(4, q)$, so the claim follows from $\mathrm{ord}(\overline{\sigma}) \leq f \mathrm{ord}(\overline{\sigma}^r)$ and Lemma 3.40. Also, if $f = 1$, we are obviously done. Therefore we are concerned with $r = 2f$ with $f \geq 2$.

By Lemma 3.24, we get that σ^{2f} is conjugate to an element in $\mathrm{GL}_4(p)$, and an upper bound for the element orders in the latter group is p^4, see Proposition 3.27. Thus $\mathrm{ord}(\sigma) \leq 2fp^4$. From $f \geq 2$ we obtain $2fp^4 < f(p^6+1) \leq f(q^3+1)$, and we are done. □

Lemma 3.42. *Let $S = \mathrm{PSU}_n(q)$ be the simple unitary group with $n \geq 3$, and $\sigma \in \mathrm{Aut}(S)$. Then*

$$\mathrm{ord}(\sigma) \leq \begin{cases} 2q^n & \text{if } q \text{ is odd,} \\ (3e/2)q^n & \text{in any case.} \end{cases}$$

Proof. Write $q = p^f$ with p a prime. Then σ has a preimage τ in $\mathrm{GU}_n(q) \rtimes \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_p)$. Under restricting the scalars to $\mathbb{F}_p$, we obtain an embedding of the latter group into $\mathrm{Isom}(\mathbb{F}_p^{2fn}, \kappa)$, where κ is a symmetric non–degenerate $\mathbb{F}_p$–bilinear form. Now apply the bounds in Proposition 3.33 to obtain the claim. □

We rule out the unitary groups in the order as they appear in the list 3.1 on page 410. So suppose that $S = \mathrm{PSU}_m(q)$.

$\mathbf{m = 3}$, $\mathbf{q \neq 2, 5}$. First suppose that $f \geq 2$, so $q > p$. By Lemma 3.40 and the structure of the automorphism group of $\mathrm{PSU}_m(q)$ given in [30, Prop. 2.3.5] we get $\mathrm{ord}(\sigma) \leq 2f(q^2-1)$. But $\mu(S) = q^3+1$, so $q^3+1 \leq 2 \cdot 2f(q^2-1)$, hence $q^2 - q + 1 \leq 4f(q-1)$. This shows $q^2 - q < 4f(q-1)$, so $3^f \leq q < 4f$, contrary to $f \geq 2$.

Next suppose $f = 1$, so $q = p$. We obtain $\mathrm{ord}(\sigma) \leq 2p(p+1)$. Thus $p^3 + 1 \leq 4p(p+1)$, so $p^2 - p + 1 \leq 4p$, therefore $p - 1 < 4$, so $p = 3$. Check the atlas [9] to see that $\mathrm{ord}(\sigma) \leq 12$, so this case is out by $3^3 + 1 > 2 \cdot 12$.

$\mathbf{m = 3}$, $\mathbf{q = 5}$. Then $\mathrm{Out}(S) = \mathcal{S}_3$ and $o(\mathrm{Aut}(S)) = 30$. Thus the degree is at most 60. But the only representation of S with degree ≤ 60 has degree 50, see [9]. Now $o(S) = 10$, so $A > S$. As $S.3$ does not have a permutation representation of degree 50, we have $A = S.2$. However, $o(S.2) = 20$, and this case is out too.

$\mathbf{m = 4}$. Suppose $q \neq 2$ for the moment. First suppose $f \geq 2$. Then $\mathrm{ord}(\sigma) \leq f(q^3+1)$ by Lemma 3.41. We obtain $(q+1)(q^3+1) = \mu(S) \leq 2f(q^3+1)$, hence $q+1 \le 2f$. But $q \ge 2^f \ge 2f$, so there is no solution. Next suppose $f = 1$, so $q = p$. We obtain $p + 1 \le 4$, so $p = 3$. However, the maximal element order in $\mathrm{Aut}(\mathrm{PSU}_4(3))$ is 28, see the atlas [9], a contradiction. Similarly, if $q = 2$, then $o(\mathrm{Aut}(\mathrm{PSU}_4(2))) = 12$, which is too small.

$6 \mid m$, $q=2$. Use Lemma 3.42 to get $2^{m-1}(2^m-1)/3 \le 2(3e/2)2^m = 6e2^{m-1}$, hence $2^m - 1 \le 18e = 48.9\ldots$, so $m \le 5$, a contradiction.

$m \ge 5$, $(m, q) \ne (6m', 2)$. From Lemma 3.34 we obtain $\mu(S) > q^{2m-3}$. On the other hand, $\mathrm{ord}(\sigma) \le (3e/2)q^m$ by Lemma 3.42, so $q^2 \le q^{m-3} \le 3e = 8.1\ldots$, thus $q = 2$ and $m = 5$. (Also $m = 6$ would fulfill the inequality, but this is excluded here.) However, in this case $\mu(S) = 165$, whereas $o(\mathrm{Aut}(S)) = 24$, see the atlas [9], a contradiction.

3.7.9. *Projective special linear groups*

Now we assume that $S = \mathrm{PSL}_n(q)$, and show that except for some small cases, only the expected elements can act with at most 2 cycles in the natural representation.

In this section, we use results by Tiep and Zalesskii [58, Section 9] on the three smallest faithful permutation degrees for the simple groups $\mathrm{PSL}_n(q)$. Unfortunately, their result is mis–stated. Apparently they mean to give the degrees of the three smallest faithful *primitive* permutation representations. In order to make use of their result, we need a little preparation.

Lemma 3.43. *Let S be a simple non–Abelian group, and $n = \mu(S)$ be the degree of the smallest faithful permutation representation. Let A be a group between S and* $\mathrm{Aut}(S)$. *If A has a primitive permutation representation on Ω such that S is imprimitive on Ω, then $|\Omega| \ge 3n$.*

Proof. Suppose that S acts imprimitively on Ω, and assume that $|\Omega| < 3n$. Let Δ be a non–trivial block for S, and M be a setwise stabilizer in S of this block. Primitivity of A forces transitivity of S on Ω, in particular S is transitive on the block system containing Δ. As there must be at least n blocks by assumption,

$$n|\Delta| \le |\Omega| < 3n,$$

hence $|\Delta| < 3$, so $|\Delta| = 2$. Let A_1 be the stabilizer of a point in A. Set $S_1 = S \cap A_1$, a point–stabilizer in S. Clearly $[M : S_1] = |\Delta| = 2$, so S_1 is normal in M. Also, S_1 is normal in A_1, and maximality of A_1 in A forces $A_1 = N_A(S_1)$. So $M \le A_1$, a contradiction. □

Lemma 3.44. *Let* $S = \mathrm{PSL}_n(q)$ *with* $(n, q) \ne (4, 2), (2, 2), (2, 3), (2, 4), (2, 5), (2, 7), (2, 9)$, *or* $(2, 11)$. *Let A be a group with* $S \le A \le \mathrm{Aut}(S)$. *Suppose that A acts primitively, and there is $\sigma \in A$ with at most two cycles in this action. Then S is primitive as well.*

Proof. In these cases the natural action of S on the $\mu = (q^n - 1)/(q - 1)$ lines of $\mathbb{F}_q^n$ is the one of smallest possible degree. Let N be the degree of the action of A. Suppose that S is imprimitive. From Lemma 3.43 we obtain $N \ge 3\mu$. If

$\sigma \in \mathrm{P\Gamma L}_n(q)$, then $\mathrm{ord}(\sigma) \le \mu$ by Proposition 3.27, contrary to Lemma 3.21. Thus σ involves a graph automorphism of $\mathrm{PSL}_n(q)$, hence also $n \ge 3$.

As $\sigma^2 \in \mathrm{P\Gamma L}_n(q)$, we have $\mathrm{ord}(\sigma) \le 2\mu$, hence $N \le 4\mu$. Let A_1 be a point–stabilizer in A, and set $S_1 = A_1 \cap S$. Let M be a maximal subgroup of S containing S_1. Then $[S : M] \le [S : S_1]/2 \le 2\mu$, so it follows easily from [58, Section 9] that M fixes a line (or hyperplane) with respect to the natural action, except possibly for $(n, q) = (3, 2)$. Exclude this single exception for a moment. As $A = A_1 S$ by transitivity of S, also A_1 involves a graph automorphism τ. As A_1 normalizes S_1, and the action of τ on S interchanges point–stabilizers with hyperplane–stabilizers, we get that there is a hyperplane $H < \mathbb{F}_q^n$ and a line $L < \mathbb{F}_q^n$, such that S_1 fixes H and L. Clearly, S acts transitively on the $q^{n-1}(q^n - 1)/(q - 1)$ non–incident line–hyperplane pairs, and also transitively on the $(q^n - 1)(q^{n-1} - 1)/(q - 1)^2$ incident line–hyperplane pairs. The latter size is smaller than the former, so $N \ge (q^n - 1)(q^{n-1} - 1)/(q - 1)^2 = (q^{n-1} - 1)/(q - 1)\mu$. From $N \le 2\mathrm{ord}(\sigma) \le 4\mu$ we obtain $1 + q + \cdots + q^{n-2} \le 4$. Hence $n = 3$ and $q = 3$ or 2. However, for $q = 3$ we have $\mathrm{ord}(\sigma) \le 13$ by [9], contrary to $N \ge 52$. If $q = 2$, then $\mathrm{Aut}(S) \cong \mathrm{PGL}_2(7)$, so $\mathrm{ord}(\sigma) \le 8$, but $N \ge 21$, a contradiction.

It remains to check the case $(n, q) = (3, 2)$. Then $\mathrm{Aut}(S) \cong \mathrm{PGL}_2(7)$, so $\mathrm{ord}(\sigma) \le 8$, hence $N \le 16$. But this contradicts the above estimation $N \ge 3\mu = 21$. □

Lemma 3.45. *Let $S = \mathrm{PSL}_n(q)$ with $(n, q) \ne (4, 2), (2, 2), (2, 3), (2, 4), (2, 5), (2, 7), (2, 9), (2, 11)$ and $S \le A \le \mathrm{Aut}(S)$. Assume that A acts primitively on Ω. Suppose that $\sigma \in A$ has at most 2 cycles on Ω. Then either $A \le \mathrm{P\Gamma L}_n(q)$ and A acts naturally on the lines of $\mathbb{F}_q^n$, or $(n, q) = (3, 2)$, and $A \le \mathrm{Aut}(\mathrm{PSL}_3(2)) \cong \mathrm{PGL}_2(7)$ acts naturally of degree 8.*

Proof. Let $N = |\Omega|$ be the permutation degree of A, and suppose that we do not have the natural action of $S = \mathrm{PSL}_n(q)$ on the points of the projective space.

As $\sigma^2 \in \mathrm{P\Gamma L}_n(q)$, we get $\mathrm{ord}(\sigma) \le 2(q^n - 1)/(q - 1)$ by Proposition 3.27.

S is primitive by the previous lemma, so we can use the results by Tiep and Zalesskii [58, Section 9] on the three smallest primitive permutation degrees for the simple groups $\mathrm{PSL}_n(q)$, see the comment before Lemma 3.43.

First suppose that $n \ge 4$, and if $n = 4$, then $q \ne 2$. Then

$$N \ge \frac{(q^n - 1)(q^{n-1} - 1)}{(q^2 - 1)(q - 1)}.$$

(This second smallest primitive representation is given by the action on the 2–spaces in $\mathbb{F}_q^n$.) Now use $N \le 2\mathrm{ord}(\sigma)$ to obtain $q^{n-1} - 1 \le 4(q^2 - 1)$. So $n = 4$ and $q = 3$. (Note that $(n, q) = (4, 2)$ is already excluded from the statement of the lemma.) But $o(\mathrm{Aut}(\mathrm{PSL}_4(3))) = 40$ by the atlas [9], whereas $N = 130 > 2 \cdot 40$, so this case is out.

Next assume $n = 3$. Using [58, Section 9], one easily verifies that $N \ge q^3 - 1$ except for $q = 4$ and 2. Exclude $q = 2$ and 4 for a moment. So $q^3 - 1 \le$

$4(q^3-1)/(q-1)$, hence $q = 3$ or 5. But for $q = 5$, we actually have $N \geq 5^2(5^3-1)$, but $\mathrm{ord}(\sigma) \leq 2(5^3-1)/(5-1)$, clearly a contradiction. If $q = 3$, then $N \geq 144$, contrary to $\mathrm{ord}(\sigma) \leq 2(3^3-1)/(3-1) = 26$. Now suppose $q = 4$. The atlas [9] gives $\mathrm{ord}(\sigma) \leq 21$, whereas $N \geq 56 > 2 \cdot 21$ by [58, Section 9], a contradiction. If $q = 2$, and we do not have the natural action, then necessarily $N = 8$, which corresponds to the natural action of $\mathrm{PGL}_2(7) \cong \mathrm{Aut}(\mathrm{PSL}_3(2))$. Finally we have to look at $n = 2$. As $A \leq \mathrm{P\Gamma L}_2(q)$ now, we have $\mathrm{ord}(\sigma) \leq (q^2-1)/(q-1) = q+1$.

We go through the cases in [58, Section 9]. If $q > 4$ is an even square, then $2(q+1) \geq N \geq \sqrt{q}(q+1)$, hence $q \leq 4$, a contradiction. If q is an odd square $\neq 9, 49$, then $2(q+1) \geq N \geq \sqrt{q}(q+1)/2$, hence $q \leq 16$, a contradiction. If $q \in \{19, 29, 31, 41\}$, then $2(q+1) \geq N \geq q(q^2-1)/120$, so $q \leq 16$, a contradiction. If $q = 17$ or $q = 49$, then $N = 102$ or 175, respectively, so these cases do not occur. If q is not among the cases treated already (and $\neq 7, 9$, and 11,) then $N \geq q(q-1)/2$, so $q(q-1) \leq 4(q+1)$, hence $q \leq 5$, a contradiction. □

Lemma 3.46. *Let $S = \mathrm{PSL}_2(q)$ with $q = 9$ or 11 and $S \leq A \leq \mathrm{Aut}(S)$. Assume that A acts primitively on Ω, and that there exists $\sigma \in A$ with at most 2 cycles on Ω. Then either $A \leq \mathrm{P\Gamma L}_2(q)$ and A acts naturally on the lines of $\mathbb{F}_q^n$, or $q = 9$, $A \leq \mathcal{S}_6 < \mathrm{Aut}(\mathrm{PSL}_2(9))$ acting naturally on 6 points, or $q = 11$, $|\Omega| = 11$, $A = \mathrm{PSL}_2(11)$, and σ is an 11–cycle.*

Proof. Suppose $q = 9$. We have $S \cong \mathcal{A}_6$, and the maximal subgroups of S have index 6, 10, and 15, respectively. Of course, the degree 6 occurs. Degree 10 corresponds to the natural action of S. The degree 15 corresponds to $\mathcal{A}_6$ acting on 2–sets. Then $A \leq \mathcal{S}_6$, and one verifies easily that each element has ≥ 3 cycles. This settles the case that S is primitive. If S is imprimitive, then $N \geq 3 \cdot 6 = 18$ by Lemma 3.43, but also $N \leq 2\mathrm{ord}(\sigma) \leq 20$. As A contains no element of order 9, we actually have $N = 20$. Hence $\mathrm{ord}(\sigma) = 10$, so $\mathrm{PGL}_2(9) \leq A$. But neither $\mathrm{PGL}_2(9)$ nor $\mathrm{P\Gamma L}_2(9)$ act primitively on 20 points, *e.g.* by the argument in the proof of Lemma 3.43.

Next suppose $q = 11$. As $\mathrm{ord}(\sigma) \leq 12$, we have $N \leq 24$, but $24 < 33 = 3 \cdot \mu(S)$, so S is primitive. The maximal subgroups of S of index ≤ 24 have index 11 and 12, and correspond to the actions covered by the claim. □

Lemma 3.47. *Let $\mathrm{P\Gamma L}_n(q)$ act naturally on the lines of $\mathbb{F}_q^n$ for $n \geq 2$. Suppose that an element $\sigma \in \mathrm{P\Gamma L}_n(q) \setminus \mathrm{PGL}_n(q)$ has at most 2 cycles. Then $(n, q) = (3, 4)$, $(2, 4)$, $(2, 8)$, or $(2, 9)$.*

Proof. Let $\gamma g \in \mathrm{GL}_n(q) \rtimes \mathrm{Aut}(\mathbb{F}_q)$ be a preimage of such a σ, with $\gamma \in \mathrm{Aut}(\mathbb{F}_q)$ and $g \in \mathrm{GL}_n(q)$. Then

$$\mathrm{ord}(\gamma g) \geq \frac{1}{2}\frac{q^n-1}{q-1}.$$

Let $f \geq 2$ be the order γ. By Lemma 3.24, $(\gamma g)^f$ is conjugate to an element in $\mathrm{GL}_n(q^{1/f})$, and the orders of elements in this latter group are at most $q^{n/f}-1$ by Proposition 3.27. Thus

$$f(q^{n/f}-1) \geq \mathrm{ord}(\gamma g) \geq \frac{1}{2}\frac{q^n-1}{q-1}. \tag{3.13}$$

This gives

$$2fq > 2f(q-1) \geq \frac{q^n - 1}{q^{n/f} - 1} > q^{n-n/f},$$

hence

$$2f > q^{n-n/f-1}.$$

Now use $2f \leq 2^f$ and $q \geq 2^f$ to obtain

$$2^f > 2^{nf-n-f},$$

hence

$$n < \frac{2f}{f-1} = 4 - 2\frac{f-2}{f-1} \leq 4, \tag{3.14}$$

so $n \leq 3$. First suppose $n = 3$. Then (3.14) shows $f < 3$, hence $f = 2$. Set $r = q^{1/2}$. Then (3.13) gives $2(r^3 - 1) \geq \frac{1}{2}\frac{r^6-1}{r^2-1}$, so $4(r^2 - 1) \geq r^3 + 1$, hence $r < 4$. One verifies easily that $r = 3$ is not possible, because the maximal order of an element in $\mathrm{P\Gamma L}_3(9) \setminus \mathrm{PGL}_3(9)$ is 26, see *e.g.* [9].

Next assume $n = 2$. Again set $r = q^{1/f} \geq 2$. Let h be an element in $\mathrm{GL}_2(r) < \mathrm{GL}_2(q)$ which is conjugate (in $\mathrm{GL}_2(\overline{\mathbb{F}_q})$) to $(\gamma g)^f$. Denote by $\overline{h}$ the image of h in $\mathrm{PGL}_2(q)$. There are three possibilities for h: If h is irreducible on $\mathbb{F}_q^2$, then $\mathrm{ord}(h)$ divides $r^2 - 1$, so $\mathrm{ord}(\overline{h})$ divides $(r^2-1)/\gcd(r^2-1, q-1)$. But $r - 1$ divides the denominator, so $\mathrm{ord}(\overline{h})$ divides $r + 1$. Next assume that h is reducible. If h is semisimple, then clearly $\mathrm{ord}(\overline{h}) \mid \mathrm{ord}(h) \mid r - 1$. If however h has a unipotent part, then this p–part has order p, and its centralizer is the group of scalar matrices. Hence in this case, $\mathrm{ord}(\overline{h}) = p \leq r$.

We have seen that $\mathrm{ord}(\overline{h}) \leq r + 1$ in any case, hence $\mathrm{ord}(\sigma) \leq f(r+1)$. We obtain

$$f(r+1) \geq \frac{q+1}{2} = \frac{r^f + 1}{2} \Longrightarrow \frac{r^f + 1}{r+1} \leq 2f.$$

The left hand side is monotonously increasing in r. For $r = 2$ we obtain $2^f + 1 \leq 6f$, hence $f \leq 4$. For $f = 3$ and 4 there are only the solutions $r = 2$. If $r > 2$, then $f = 2$ and $r = 3$ or 4. In order to obtain the claim, we have to exclude the possibility $q = r^f = 16$. The previous consideration shows that each element in $\mathrm{P\Gamma L}_2(16) \setminus \mathrm{PGL}_2(16)$ has order at most 12. But then we clearly cannot have at most 2 cycles in a representation of odd degree 17. □

Lemma 3.48. *Let $2 \leq n \in \mathbb{N}$. Suppose that $\sigma \in \mathrm{PGL}_n(q)$ has at most 2 cycles in the action on the lines of $\mathbb{F}_q^n$. Then one of the following holds:*

1. *q is a prime, $n = 2$, and σ has order q.*
2. *σ is a Singer cycle or the square of a Singer cycle.*

Proof. For a subset S of $\mathbb{F}_q^n$ denote by $P(S)$ the "projectivization" of S, namely the set of 1–dimensional spaces through the non–zero elements of S. Denote by $\hat{\sigma} \in \mathrm{GL}_n(q)$ a preimage of σ. If $\hat{\sigma}$ is irreducible on $\mathbb{F}_q^n$, then Schur's Lemma shows that (b) holds. Thus assume that $\hat{\sigma}$ is reducible, and let $0 < U < \mathbb{F}_q^n$ be a $\hat{\sigma}$–irreducible subspace. The assumption shows that $<\sigma>$ permutes transitively the elements in $P(U)$, as well as those of $P(\mathbb{F}_q^n \setminus U)$. The transitivity of this latter action shows

$$q^u \text{ divides } \mathrm{ord}(\hat{\sigma}), \text{where } u = \dim(U). \tag{3.15}$$

Denote by $\hat{\sigma}_p$ and $\hat{\sigma}_{p'}$ the p–part and p'–part of $\hat{\sigma}$, respectively. Let W be a $\hat{\sigma}_{p'}$–invariant complement to U in $\mathbb{F}_q^n$. As $\hat{\sigma}$ is transitive on $P(U)$ and $P(\mathbb{F}_q^n/U)$, we have in particular that $\hat{\sigma}$ is irreducible on the quotient space $\mathbb{F}_q^n/U$, so $\hat{\sigma}_p$ is trivial on this quotient, hence $\hat{\sigma}_{p'}$ is irreducible on W. From (3.15) we get that $\hat{\sigma}_p$ is not trivial, in particular W is not $\hat{\sigma}_p$–invariant. Then we see from Jordan–Hölder that U and W are $\hat{\sigma}_{p'}$–isomorphic, so $\hat{\sigma}_p \in \mathrm{GL}_2(q^u)$. Thus $\mathrm{ord}(\hat{\sigma}_p) = p$. Combine this with (3.15) to get $n = 2u = 2$, and $q = p$. Finally, $\hat{\sigma}_{p'}$ centralizes $\hat{\sigma}_p$, so must be a scalar, that is σ has order p. □

3.7.10. *Exceptional groups of Lie type*

Here we rule out the case that S is an exceptional group of Lie type. Table 3.2 on page 410 contains the exceptional group of Lie type S, a lower bound $\mu(S)$ for the degree of a non-trivial transitive faithful permutation representation, an upper bound $o(S)$ for the orders of elements, the order of the outer automorphism group, and finally restricting condition on q. In the list $q = p^f$ for a prime p.

The lower bound for $\mu(S)$ has been computed as follows. If S has a permutation representation of degree m, and F is any field, then the permutation module of S over F has a submodule of dimension $m-1$. So $m-1$ is at least the dimension of the lowest–dimensional projective representation of S in characteristic different from the defining characteristic. But these minimal dimensions have been determined by Landazuri and Seitz in [35]. We use the corrected list [30, Theorem 5.3.9]. Note that if S does not have a doubly transitive representation, then the $(m-1)$–dimensional module is reducible, so one summand has dimension at most $(m-1)/2$, see [18, 4.3.4]. This is the case for all S except for ${}^2B_2(q)$ and ${}^2G_2(q)$. So $\mu(S)$ is then at least 1 plus 2 times the minimal dimension of a representation of S.

The upper bound for $o(S)$ has been obtained as follows. Each element of S is the product of a p–element with a commuting p'–element, so we multiply upper bounds for each. If ℓ is the Lie rank of S, then the order of p'–elements is at most $(q+1)^\ell$, see [38, 1.3A]. The order of a p–element g is bounded as follows. Suppose $S \le \mathrm{PGL}_w(F)$ for a field F of characteristic p. Then the order of g is a p–power at most $p(w-1)$, see Lemma 3.5. Small values w with an embedding as above are classically known, see [30, Prop. 5.4.13]. However, for the Suzuki groups ${}^2B_2(q)$ we used [24, XI, Section 3] to determine μ and o. To determine μ for $G_2(q)$ and ${}^3D_4(q)$ we use the papers by Kleidman [28] and [29] respectively.

Now assume that $S \leq A \leq \mathrm{Aut}(S)$ and $\sigma \in A$ has at most two cycles in a transitive action of A. Then $\mu(S) \leq 2o(A) \leq 2|\mathrm{Out}(S)|o(S)$. Comparing with the information in the Table 3.2 on page 410 rules out all but a few little cases, which require extra data obtained from the atlas [9].

$\mathbf{S = {}^2B_2(q)}$. We get $1+q^2 \leq 2f(q+\sqrt{2q}+1)$. As $q \geq 8$, we have $\sqrt{2q}+1 \leq \frac{5}{8}q$. So we get $q^2 < 1+q^2 \leq 2f(q+\frac{5}{8}q)$, hence $2^f < \frac{13}{4}f$. This implies $f = 3$. But $o(\mathrm{Aut}({}^2B_2(8))) = 15$ (see the atlas [9]), contrary to $\mu({}^2B_2(8)) = 65 > 2\cdot 15$.

$\mathbf{S = {}^2G_2(q)}$. We get $1+q(q-1) \leq 2f\cdot 9(q+1)$. Now $q+1 \leq \frac{28}{27}q$, which gives $3^f = q < \frac{56}{3}f+1$, hence $f = 3$. But $\mu({}^2G_2(27)) = 19684$, see [9], whereas $o({}^2G_2(27)) = 37$, so this case is clearly out.

$\mathbf{S = G_2(q)}$. Obviously $q \geq 5$. First assume that q is odd. Bound $(q^6-1)/(q-1)$ from below by q^5, and $q+1$ from above by $6q/5$. We then obtain $q^5 \leq 2\cdot 2f\cdot 6p(q+1)^2 \leq 24q(6q/5)^2$, hence $p^{2f} \leq 864f/25$, which gives $q = 5$. But then $\mathrm{Out}(S)$ has order 1, and when we use the estimations in the table, we get a contradiction. The case $p = 2$ and $f \geq 3$ also does not occur by a similar calculation.

$\mathbf{S = {}^3D_4(q)}$. We get $(q+1)(q^8+q^4+1)/2 \leq 2\cdot 3f\cdot 8p(q+1)^2$. One quickly checks that this holds only for $q = 2$. But $\mu({}^3D_4(2)) = 819$, whereas $o({}^3D_4(2)) = 28$ (see [9]), so this case does not occur.

$\mathbf{S = {}^2F_4(2)'}$. This clearly does not occur.

$\mathbf{S = {}^2F_4(q)}$. One gets $1+q^4\sqrt{2q}(q-1) \leq 2f\cdot 32(q+1)^2$, and one easily checks that this inequality has no solutions.

$\mathbf{S = F_4(q)}$. The case $q = 2$ does not occur. We have $1+2q^6(q^2-1) \leq 2(2,p)f\cdot 25p(q+1)^4$, which implies that $q = 3$ or 4. However, Theorem [30, 5.3.9] for even q shows that the minimal degree of a $2'$–representation of $F_4(4)$ is 1548288, so $\mu(S) \geq 3096577$. But this violates the estimation $o(F_4(4)) \leq 31250$. So $q = 3$. The maximal order of a $3'$–element is ≤ 73, see [7, page 316]. Furthermore, the 3–order is at most 27. Thus $o(S) \leq 1971$. But $\mu(S) \geq 11665$, a contradiction.

$\mathbf{S = {}^2E_6(q)}$. We get quickly $q = 2$. But $o({}^2E_6(2)) = 35$, which is much too small compared to $\mu({}^2E_6(2)) = 3073$.

$\mathbf{S = E_6(q)}$. We quickly get that $q = 2$, 3, or 4. The p'–part is bounded by 91, 949, and 5061, respectively (again by [7, page 316]), and the p–part is bounded by 32, 27, and 32, respectively. So $o(S)$ is at most 2912, 25623, and 161952, respectively. If we compare this with the estimation for $\mu(S)$, then only $q = 2$ survives. We get $\mu(S) \leq 2\cdot 2\cdot 2912 = 11648$. However, $E_6(2)$ contains $F_4(2)$, and $\mu(E_6(2)) \geq \mu(F_4(2)) = 69615$ ([9]), a contradiction.

$\mathbf{S = E_7(q)}$. We get $q = 2$. Use [7, page 316] to obtain $o(S) \leq 171\cdot 64 = 10944$. But from the table we have $\mu(S) \geq 196609$, which is clearly too big.

$\mathbf{S = E_8(q)}$ gives also no examples.

3.7.11. *Proof of part* 3 *of Theorem* 3.3

Now we are ready to prove part 3 of Theorem 3.3, by collecting the information achieved in the last sections. Thus suppose that A acts primitively, $S \leq A \leq \mathrm{Aut}(S)$ for a non–Abelian simple group S, and that A contains an element σ which has exactly 2 cycles.

If S is sporadic, then Section 3.7.2 gives the possibilities. This is the easiest case, as the result can be directly read off from the atlas information [9]. Only the Mathieu groups $\mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{22}$, and M_{24} give rise to examples.

Section 3.7.1 treats the case that $S = \mathcal{A}_n$, the alternating group with $n \geq 5$. The case $n = 6$ has been excluded there, and postponed to the analysis of the linear groups, in view of $\mathcal{A}_6 \cong \mathrm{PSL}_2(9)$. The only examples coming not from the natural action of S are as follows: $S = \mathcal{A}_5$ acting on the 2–sets of $\{1, 2, 3, 4, 5\}$, hence of degree 10 (case 3b), or $S = \mathcal{A}_5$ acting on 6 points (case 3c for $p = 5$, note that $\mathcal{A}_5 \cong \mathrm{PSL}_2(5)$).

By Section 3.7.10, S cannot be of exceptional Lie type.

In Section 3.7.3 it is shown that if S is a classical group, then S is isomorphic to some $\mathrm{PSL}_n(q)$.

This is dealt with in Section 3.7.9. We can exclude a couple of small pairs (n, q) in view of exceptional isomorphisms, see [30, Prop. 2.9.1]. As S is simple, $(n, q) \neq (2, 2), (2, 3)$. Also, $(n, q) \neq (2, 4), (2, 5)$, as $S = \mathcal{A}_5$ has been dealt with already. Also $(n, q) \neq (4, 2)$, as $\mathcal{A}_8$ had been ruled out in Section 3.7.1. Furthermore, we assume $(n, q) \neq (2, 7)$ in view of $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$.

Suppose that $q \neq 9$, or 11, if $n = 2$. Then $A \leq \mathrm{P\Gamma L}_n(q)$ acting naturally on the projective space, or $(n, q) = (3, 2)$, and we have the natural action of $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$ of degree 8, see Lemma 3.45. Lemma 3.46 shows that for $(n, q) = (2, 9)$ the action is either the natural one, or the natural one of $\mathcal{A}_6 \cong \mathrm{PSL}_2(9)$, and for $(n, q) = (2, 11)$, only the natural action is possible.

In conclusion, we are left to look at the natural action of $\mathrm{PSL}_n(q) \leq A \leq \mathrm{P\Gamma L}_n(q)$, and to determine the possibilities for σ. By Lemma 3.47, we have actually $\sigma \in \mathrm{PGL}_n(q)$, except possibly for $(n, q) = (3, 4), (2, 8)$, or $(2, 9)$. The case $(n, q) = (3, 4)$ accounts for 3f in Theorem 3. One easily verifies that $\mathrm{P\Gamma L}_2(8)$ does not contain an element with just 2 cycles (but it does contain 9–cycles not contained in $\mathrm{PGL}_2(8)$!). Similarly, if an element in $\mathrm{P\Gamma L}_2(9) \setminus \mathrm{PGL}_2(9)$ has only 2 cycles, then $\sigma \in \mathrm{M}_{10}$, and the cycle lengths are 2 and 10. This gives case 3e of Theorem 3.

So in addition to the assumption that $A \leq \mathrm{P\Gamma L}_n(q)$ acts naturally, we may finally assume $\sigma \in \mathrm{PGL}_n(q)$. Lemma 3.48 finishes this case: Either q is a prime, $n = 2$, $\mathrm{ord}(\sigma) = q$ (so σ has cycle lengths 1 and q, case 3c of Theorem 3), or σ is the square of a Singer cycle (case 3d of Theorem 3.3).

By the classification theorem of the finite simple groups, we have covered all possibilities of S.

3.7.12. *Tables on minimal permutation degrees, maximal element orders, etc.*

Table 3.1. Classical groups

S	$\mu(S)$	$\lvert\mathrm{Out}(S)\rvert$	m, q
$\mathrm{PSL}_m(q)$	$(q^m-1)/(q-1)$	$2(m,q-1)f,\ m\geq 3$ $(m,q-1)f,\ m=2$	$(m,q)\neq(2,5)$, $(2,7)$, $(2,9)$, $(2,11)$, $(4,2)$
$\mathrm{PSL}_2(7)$	7	2	
$\mathrm{PSL}_2(9)$	6	4	
$\mathrm{PSL}_2(11)$	11	2	
$\mathrm{PSL}_4(2)\cong\mathcal{A}_8$	8	2	
$\mathrm{PSp}_{2m}(q)$	$(q^{2m}-1)/(q-1)$	$(2,q-1)f,\ m\geq 3$ $2f,\ m=2$	$m\geq 2, q\geq 3$, $(m,q)\neq(2,3)$
$\mathrm{Sp}_{2m}(2)$	$2^{m-1}(2^m-1)$	1	$m\geq 3$
$\Omega_{2m+1}(q)$	$(q^{2m}-1)/(q-1)$	$2f$	$m\geq 3$, $q\geq 5$ odd
$\Omega_{2m+1}(3)$	$3^m(3^m-1)/2$	2	$m\geq 3$
$\mathrm{P}\Omega^+_{2m}(q)$	$(q^m-1)(q^{m-1}+1)/(q-1)$	$2(4,q^m-1)f, m\neq 4$ $6(4,q^m-1)f, m=4$	$m\geq 4,\ q\geq 4$
$\mathrm{P}\Omega^+_{2m}(2)$	$2^{m-1}(2^m-1)$	$2, m\neq 4$ $6, m=4$	$m\geq 4$
$\mathrm{P}\Omega^+_{2m}(3)$	$3^{m-1}(3^m-1)/2$	$4, m>4$ odd $8, m>4$ even $24, m=4$	$m\geq 4$
$\mathrm{P}\Omega^-_{2m}(q)$	$(q^m+1)(q^{m-1}-1)/(q-1)$	$2(4,q^m+1)f$	$m\geq 4$
$\mathrm{PSU}_3(q)$	q^3+1	$2(3,q+1)f$	$q\neq 2,5$
$\mathrm{PSU}_3(5)$	50	6	
$\mathrm{PSU}_4(q)$	$(q+1)(q^3+1)$	$2(4,q+1)f$	
$\mathrm{PSU}_m(2)$	$2^{m-1}(2^m-1)/3$	6	$6\mid m$
$\mathrm{PSU}_m(q)$	$\frac{(q^m-(-1)^m)(q^{m-1}-(-1)^{m-1})}{q^2-1}$	$2(m,q+1)f$	$m\geq 5$, $(m,q)\neq(6m',2)$

Table 3.2. Exceptional groups

S	$\mu(S)\geq$	$o(S)\leq$	$\lvert\mathrm{Out}(S)\rvert$	q
${}^2B_2(q)$	$1+q^2$	$q+\sqrt{2q}+1$	f	$q=2^{2u+1}>2$
${}^2G_2(q)$	$1+q(q-1)$	$9(q+1)$	f	$q=3^{2u+1}>3$
$G_2(3)$	351	13	2	
$G_2(4)$	416	21	2	
$G_2(q)$	$(q^6-1)/(q-1)$	$8(q+1)^2$	f	$q\geq 8$ even
$G_2(q)$	$(q^6-1)/(q-1)$	$6p(q+1)^2$	$\leq 2f$	$q\geq 5$ odd
${}^3D_4(q)$	$(q+1)(q^8+q^4+1)/(2,q-1)$	$7p(q+1)^2$	$3f$	
${}^2F_4(2)'$	1600	16	2	
${}^2F_4(q)$	$1+q^4\sqrt{2q}(q-1)$	$32(q+1)^2$	f	$q=2^{2u+1}>2$
$F_4(2)$	69615	30	2	
$F_4(q)$	$1+2q^6(q^2-1)$	$25p(q+1)^4$	$(2,p)f$	$q\geq 3$
${}^2E_6(q)$	$1+2q^9(q^2-1)$	$26p(q+1)^4$	$2(3,q+1)f$	
$E_6(q)$	$1+2q^9(q^2-1)$	$26p(q+1)^6$	$2(3,q-1)f$	
$E_7(q)$	$1+2q^{15}(q^2-1)$	$55p(q+1)^7$	$(2,q-1)f$	
$E_8(q)$	$1+2q^{27}(q^2-1)$	$247p(q+1)^8$	f	

Table 3.3. Sporadic groups

Group S	Orders of elements	Indices of maximal subgroups	$\lvert\mathrm{Out}(S)\rvert$
M_{11}	$11,\ 8,\ 6,\ \leq 5$	$11,\ 12,\ \geq 55$	1
M_{12}	$11,\ 10,\ 8,\ 6,\ \leq 5$	$12,\ \geq 66$	2
M_{22}	$11,\ 8,\ 7,\ 6,\ \leq 5$	$22,\ \geq 77$	2
M_{23}	$23,\ 15,\ 14,\ \leq 11$	$23,\ \geq 253$	1
M_{24}	$23,\ 21,\ 15,\ 14,\ 12,\ \leq 11$	$24,\ \geq 276$	1
J_1	≤ 19	≥ 266	1
J_2	≤ 15	≥ 100	2
J_3	≤ 19	≥ 6156	2
J_4	≤ 66	≥ 173067389	1
HS	≤ 20	≥ 100	2
Suz	≤ 24	≥ 1782	2
McL	≤ 30	≥ 275	2
Ru	≤ 29	≥ 4060	1
He	≤ 28	≥ 2058	2
Ly	≤ 67	≥ 8835156	1
O'N	≤ 31	≥ 122760	2
Co_1	≤ 60	≥ 98280	1
Co_2	≤ 30	≥ 2300	1
Co_3	≤ 60	≥ 276	1
Fi_{22}	≤ 30	≥ 3510	2
Fi_{23}	≤ 60	≥ 31671	1
Fi'_{24}	≤ 60	≥ 8672	2
HN	≤ 40	≥ 1140000	2
Th	≤ 39	≥ 143127000	1
B	≤ 70	≥ 4372	1
M	≤ 119	≥ 196883	1

4. Genus 0 systems

4.1. Branch cycle descriptions

4.1.1. *Algebraic setting*

Let k be a subfield of the complex numbers $\mathbb{C}$, t be a transcendental over $\mathbb{C}$, and $L/k(t)$ be a finite Galois extension with groups G. We assume that $L/k(t)$ is regular, that means k is algebraically closed in L. Let $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$ be the places of $k(t)$ which are ramified in L. Then, by a consequence of Riemann's Existence Theorem (see [43], [59]), we can choose places $\mathfrak{P}_i$ of L lying above $\mathfrak{p}_i$, $i = 1, 2, \dots, r$, and elements $\sigma_i \in G$ such that σ_i is a generator of the inertia group of $\mathfrak{P}_i$, so that the following holds:

The σ_i, $i = 1, 2, \dots, r$ generate G, and $\sigma_1\sigma_2 \dots \sigma_r = 1$.

We call the tuple $(\sigma_1, \sigma_2, \dots, \sigma_r)$ a *branch cycle description* of the extension $L/k(t)$.

Now let E be a field between L and $k(t)$, and consider G as a permutation group on the conjugates of a primitive element of $E/k(t)$. Set $n := [E : k(t)]$. For $\sigma \in G$ let $\mathrm{ind}(\sigma)$ be n minus the number of cycles of σ. We call $\mathrm{ind}(\sigma)$ the *index* of σ. This notion obviously applies to any permutation group of finite degree.

Let g_E be the genus of the field E. The Riemann–Hurwitz genus formula gives

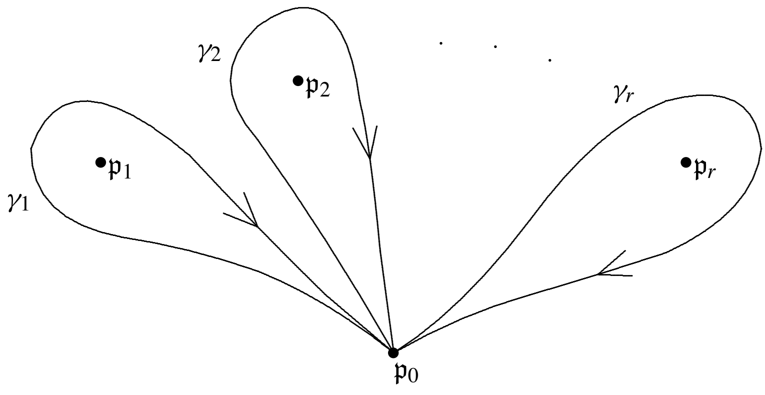
$$2(n-1+g_E)=\sum_{i=1}^{r}\operatorname{ind}(\sigma_i). \tag{4.1}$$

We will frequently use this relation for the case that E is a rational field, so that in particular $g_E=0$, and will call the corresponding equation *genus* 0 *relation*, and the tuple $(\sigma_1,\sigma_2,\dots,\sigma_r)$ a *genus* 0 *system*.

The process of constructing a branch cycle description from the extension $L/k(t)$ can be reverted to some extent. Namely let G be any finite group, generated by $\sigma_1,\sigma_2,\dots,\sigma_r$, such that $\sigma_1\sigma_2\dots\sigma_r=1$. Then there exists a finite extension $k/\mathbb{Q}$, and a regular Galois extension $L/k(t)$, such that the σ_i arise exactly as described above. This again follows from (the difficult direction of) Riemann's Existence Theorem. Modern references are [43] and [59], where the latter one contains a self–contained treatment.

4.1.2. *Topological setting*

For explicit computations and a conceptual understanding of branch cycle descriptions, the topological interpretation of the σ_i is indispensable. Also $\mathbb{C}L/\mathbb{C}(t)$ has Galois group G. Again let E be a field between $k(T)$ and L. There is a composition of ramified coverings of Riemann surfaces $\hat{\mathcal{X}}\to\mathcal{X}\xrightarrow{\pi}\mathbb{P}^1(\mathbb{C})$, such that the natural inclusion of the fields of meromorphic functions $\mathbb{C}(t)=M(\mathbb{P}^1(\mathbb{C}))\subseteq M(\mathcal{X})\subseteq M(\hat{\mathcal{X}})$ is just the extension $\mathbb{C}(t)\subseteq\mathbb{C}E\subseteq\mathbb{C}L$. If we identify the places of $\mathbb{C}(t)$ with the elements in $\mathbb{P}^1(\mathbb{C})$ in the natural way, then the branch points of $\hat{\mathcal{X}}\to\mathbb{P}^1(\mathbb{C})$ are exactly the places of $\mathbb{C}(t)$ ramified in $\mathbb{C}L$. Choose a point $\mathfrak{p}_0\in\mathbb{P}^1(\mathbb{C})$ away from the branch points $\mathfrak{p}_i$, and choose a standard set of generators $\gamma_1,\gamma_2,\dots,\gamma_r$ of the fundamental group Γ of $\mathbb{P}^1(\mathbb{C})\setminus\{\mathfrak{p}_1,\dots,\mathfrak{p}_r\}$ with base point $\mathfrak{p}_0$, where γ_i comes from a path starting and ending in $\mathfrak{p}_0$, winding clockwise around $\mathfrak{p}_i$ just once and not around any other branch point, see the diagram.



The γ_i generate Γ with the single relation $\gamma_1\gamma_2\dots\gamma_r=1$. Clearly Γ acts on the fiber $\pi^{-1}(\mathfrak{p}_0)$. The induced action gives the group G, and the images of the γ_i are the elements σ_i as above. Furthermore, the cycle lengths of σ_i on the fiber

$\pi^{-1}(\mathfrak{p}_0)$ are the multiplicities of the elements in the fiber $\pi^{-1}(\mathfrak{p}_i)$, and these cycle lengths are the same as for the corresponding action on the conjugates of a primitive element of $E/k(t)$.

For more details about this connection we refer again to [43] and [59].

4.2. Branch cycle descriptions in permutation groups

Let G be a transitive permutation group of degree n, and $\mathcal{E} := (\sigma_1, \sigma_2, \ldots, \sigma_r)$ be a generating system with $\sigma_1\sigma_2 \ldots \sigma_r = 1$. For $\sigma \in G$ define the index $\mathrm{ind}(\sigma)$ as above. Let the number $g_{\mathcal{E}}$ be given by

$$2(n - 1 + g_{\mathcal{E}}) = \sum_{i=1}^{r} \mathrm{ind}(\sigma_i).$$

The topological interpretation from above of the σ_i as coming from a suitable cover of Riemann surfaces shows that $g_{\mathcal{E}}$ is a non–negative integer, because it is the genus of a Riemann surface. This topological application in a purely group-theoretic context was first made by Ree, see [51]. Later, Feit, Lyndon, and Scott gave an elementary group-theoretic argument of this observation, see [14].

In this chapter we will determine such systems $\mathcal{E}$ for $g_{\mathcal{E}} = 0$ in specific groups G. According to the previous section, we will call such systems genus 0 systems. If we look for σ_i in a fixed conjugacy class $\mathcal{C}_i$, then it does not matter in which way we order the classes, for if σ_i and σ_{i+1} are two consecutive elements in $\mathcal{E}$, then we may replace these elements by σ_{i+1} and $\sigma_i^{\sigma_{i+1}}$, respectively.

The strategy of finding such genus 0 systems in G (or proving that there are none) depends very much on the specific situation. For many small groups, we simply check using a program written in GAP [17]. For bigger groups, especially certain sporadic groups, we can use the character tables in the atlas [9]. Here, and at other places, the following easy observation (see [45, 2.4]) is useful.

Lemma 4.1. *Let $\sigma \in G$, where G is a permutation group of degree n, then*

$$\mathrm{ind}(\sigma) = n - \frac{1}{\mathrm{ord}(\sigma)} \sum_{k|\mathrm{ord}(\sigma)} \chi(\sigma^k)\varphi\left(\frac{\mathrm{ord}(\sigma)}{k}\right),$$

where $\chi(\tau)$ is the number of fixed points of $\tau \in G$, and φ is the Euler φ–function.

4.3. A lemma about genus 0 systems

Lemma 4.2. *Let $(\sigma_1, \sigma_2, \ldots, \sigma_r)$ be a genus 0 system of a transitive permutation group G. Suppose that all cycle lengths of σ_1 and σ_2 are divisible by $d > 1$. Then G admits a block system of d blocks, which are permuted cyclically.*

Proof. Let n be the degree of G. Let $\mathcal{X} \to \mathbb{P}^1(\mathbb{C})$ be a connected cover of the Riemann sphere, such that $(\sigma_1, \sigma_2, \ldots, \sigma_r)$ is the associated branch cycle description. Without loss of generality let 0 and ∞ be branch points corresponding to σ_1 and σ_2, respectively. As our tuple is a genus 0 system, $\mathcal{X}$ has genus 0, thus $\mathcal{X} = \mathbb{P}^1(\mathbb{C})$ and the cover is given by a rational function $f(X)$. We may assume (by a linear fractional change) that ∞ is not mapped to 0 or ∞. Let α_i be the elements in $f^{-1}(0)$, and denote the multiplicity of α_i my m_i. Similarly, let β_i have multiplicity n_i in the fiber $f^{-1}(\infty)$. Thus, up to a constant factor, we have

$$f(X) = \frac{\prod(X-\alpha_i)^{m_i}}{\prod(X-\beta_i)^{n_i}}.$$

As the m_i and n_i are the cycle lengths of σ_1 and σ_2, respectively, we get $f(X) = g(X)^d$, where $g(X) \in \mathbb{C}(X)$ is a rational function. From that the claim follows. $\square$

Remark. The completely elementary nature of the lemma makes it desirable to have a proof which does not rely on Riemann's existence theorem. We sketch an elementary argument, and leave it to the reader to fill in the details: first note that if the claimed assertion about the permutation action holds for a group containing G (and acting on the same set), then it holds for G as well. For $i > 2$ write σ_i as a minimal product of transpositions, and replace the element σ_i by the tuple of these transpositions. This preserves the genus 0 condition. Also, the product of a k–cycle with a disjoint l–cycle with a transposition which switches a point of the k–cycle with one of the l–cycle is a $(k+l)$–cycle. This way, we can assume that all cycle lengths of σ_1 and σ_2 are d, at the cost of extra transpositions, but still preserving the genus 0 property. Write $n = md$. Clearly, there are $m-1$ transpositions in our system, such that they, together with σ_1, generate a transitive group. Let τ_1, ..., τ_{m-1} be these transpositions. As we have a genus 0 system, the total number of transpositions is $2(m-1)$. Using braiding we get an equation of the form

$$\sigma_1\tau_1\dots\tau_{m-1} = \sigma_2'\tau_1'\dots\tau_{m-1}' =: \rho,$$

where σ_2' is conjugate to σ_2^{-1}, and the τ_i' are transpositions. As $\mathrm{ind}(xy) \le \mathrm{ind}(x) + \mathrm{ind}(y)$ and $(\sigma_1, \tau_1, \dots, \tau_{m-1}, \rho^{-1})$ is a genus ≥ 0 system of a transitive subgroup of G, we obtain it must be a genus 0 system, and $\mathrm{ind}(\rho) = n-1$. Thus ρ is an n–cycle. Inductively, we see that $\lambda := \sigma_1\tau_1\dots\tau_{m-2}$ is a product of an $(n-d)$–cycle and a d–cycle, and that these two cycles are fused by τ_{m-1}. Now, by induction on the degree of G, we get that the group generated by the transitive genus 0 system $(\sigma_1, \tau_1, \dots, \tau_{m-2}, \lambda^{-1})$ with respect to the support of size $n-d$ admits a block system of d blocks being permuted cyclically. Now extend each block Δ by a single point from the remaining d points as follows: Choose j such that τ_{m-1} moves a point ω from $\Delta^{\sigma_1^j}$. Now append $\omega^{\tau_{m-1}\sigma_1^{-j}}$ to Δ. One verifies that this process is well–defined, and gives a block system for $(\sigma_1, \tau_1, \dots, \tau_{m-1})$ with d blocks being permuted cyclically. It remains to show that this block system is preserved also by $(\sigma_2', \tau_1', \dots, \tau_{m-1}')$. At any rate, by symmetry we get a block system for this tuple too, with d blocks being permuted cyclically. The point is that the product of the elements in this tuple is the same n–cycle as the product of the elements in the former tuple, and an n–cycle has a unique block system with d blocks. Therefore the block systems are the same, so are respected by G.

4.4. The Siegel-Lang theorem and Hilbert's irreducibility theorem

Let k be field which is finitely generated over $\mathbb{Q}$, and R a finitely generated subring. The Siegel-Lang Theorem about points with coordinates in R on algebraic curves over k has the following application to Hilbert's irreducibility theorem, see [48, 2.1].

Let $f(t, X) \in k(t)[X]$ be irreducible, and $\mathrm{Red}_f(R)$ the set of those $\bar{t} \in R$, such that $f(\bar{t}, X)$ is defined, and reducible over k. Then, up to a finitely many elements, $\mathrm{Red}_f(R)$ is the union of finitely many sets of the form $g(k) \cap R$, where $g(Z) \in k(Z)$ is a rational function.

In view of this result, it is important to know which rational functions $g(Z)$ have the property that $g(k) \cap R$ is an infinite set. By another theorem of Siegel-Lang (see [36, 8.5.1]), this property implies that there are at most two elements of $\bar{k} \cup \{\infty\}$ in the fiber $g^{-1}(\infty)$. The converse is true if we allow to enlarge R. More precisely, we have the following:

Lemma 4.3. *Let k be a finitely generated extension of k, $g(Z) \in k(Z)$ a non-constant rational function such that the fiber $g^{-1}(\infty)$ has at most two elements. Then there is a finitely generated subring R of k with $|g(k) \cap R| = \infty$.*

Proof. A linear fractional change of the argument of g allows to assume that $g(Z)$ has the following shape: There is $m \geq 0$ and a polynomial $A(Z) \in k[Z]$, such that either $g(Z) = A(Z)/Z^m$, or $g(Z) = A(Z)/(Z^2 - d)^m$, where $d \in k$ is not a square. In the first case let R be the ring generated by $1/2$ and the coefficients of $A(Z)$, then $g(z) \in R$ if $z = 2^r$ for $r \in \mathbb{Z}$, hence $g(k) \cap R$ is an infinite set.

The second case is a little more subtle: For $\alpha, \beta \in k$, define sequences $\alpha_n, \beta_n \in k$ for $n \in \mathbb{N}$ by $\alpha_n + \beta_n\sqrt{d} = (\alpha + \beta\sqrt{d})^n$. Suppose for the moment that $\beta_n \neq 0$ for all n. Define $z_n = \alpha_n/\beta_n$. Then the z_n are pairwise distinct, for if $z_j = z_i$ for $j > i$, then $\beta_j/\beta_i = (\alpha + \beta\sqrt{d})^{j-i} = \alpha_{j-i} + \beta_{j-i}\sqrt{d}$, so $\beta_{j-i} = 0$, a contradiction. Let R be the ring generated by the coefficients of $A(Z)$ and $1/(\alpha^2 - \beta^2 d)$. Note that $(\alpha^2 - \beta^2 d)^n = \alpha_n^2 - \beta_n^2 d$, so $g(z_n) \in R$ for all n.

It remains to show that we can choose suitable $\alpha, \beta \in k$. Write $\gamma = \alpha + \beta\sqrt{d}$. Then $\beta_n = 0$ is equivalent to $\gamma^n \in k$. Thus we have to find γ such $\gamma^n \notin k$ for all $n \in \mathbb{N}$. Suppose that $\gamma \notin k$, however $\gamma^n \in k$. Let σ be the involutory automorphism of $k(\sqrt{d})/k$. The minimal polynomial $(X - \gamma)(X - \sigma(\gamma))$ of γ over k divides $X^n - \gamma^n$, so $\sigma(\gamma) = \zeta\gamma$ for ζ an nth root of unity. In particular, $\zeta \in k(\sqrt{d})$. But $k(\sqrt{d})$ is finitely generated, so this field contains only finitely many roots of unity. For a fixed $\gamma \in k(\sqrt{d}) \setminus k$ consider the elements $\gamma + i$, for $i \in \mathbb{Z}$. For each i there is $n_i \in \mathbb{N}$ with $(\gamma + i)^{n_i} \in k$. By the above, each element $(\sigma(\gamma) + i)/(\gamma + i)$ is a root of unity. One of these roots of unity appears for infinitely many i, which of course is nonsense. □

If $k = \mathbb{Q}$, then one is mainly interested in the special case $R = \mathbb{Z}$. Then $|g(\mathbb{Q}) \cap \mathbb{Z}| = \infty$ has another strong consequence, see [56]: If $|g^{-1}(\infty)| = 2$, then the two elements in $g^{-1}(\infty)$ are real and algebraically conjugate. Motivated by these results, we give the following:

Definition 4.4. Let k be a field which is finitely generated over $\mathbb{Q}$, and $g(Z) \in k(Z)$ a non-constant rational function. We say that $g(Z)$ is a *Siegel function* over k, if there is a finitely generated subring R of k with $|g(k) \cap R| = \infty$. If $k = \mathbb{Q}$, then we require more strongly that $|g(\mathbb{Q}) \cap \mathbb{Z}| = \infty$.

In the analysis of Siegel functions we will make use of the fact about $g^{-1}(\infty)$. For this it will not be necessary to assume that k is finitely generated. Thus we define a more general property, which holds for Siegel functions.

Definition 4.5. Let k be a field of characteristic 0, and $g(Z) \in k(Z)$ a non-constant rational function. We say that $g(Z)$ fulfills the *Siegel property*, if $|g^{-1}(\infty)| \leq 2$.

If $k = \mathbb{Q}$, and $|g^{-1}(\infty)| = 2$, then we additionally require the two elements in $g^{-1}(\infty)$ to be real and algebraically conjugate.

4.5. Siegel functions and ramification at infinity

To ease the language, we start to define monodromy groups of rational functions.

Definition 4.6. Let k be a field of characteristic 0, and $g(Z) \in k(Z)$ be a non-constant rational function. Denote by L a splitting field of $g(Z) - t$ over $k(t)$. Set $A = \mathrm{Gal}(L/k(t))$, considered as a permutation group on the roots of $g(Z) - t$. Denote by $\hat{k}$ the algebraic closure of k in L, and let $G \trianglelefteq A$ be the normal subgroup $\mathrm{Gal}(L/\hat{k}(t))$. Then A and G are called the *arithmetic monodromy group* and *geometric monodromy group* of $g(Z)$, respectively. Note that A/G is naturally isomorphic to $\mathrm{Gal}(\hat{k}/k)$.

Our goal is to determine the genus 0 systems and the monodromy groups of functionally indecomposable rational functions with the Siegel property. Lüroth's Theorem shows that functional indecomposability of $g(Z)$ (over k) implies primitivity of A. The following lemma summarizes the properties we will use.

Lemma 4.7. *With the notation from above let $D \leq A$ and $I \trianglelefteq D$ be the decomposition and inertia group of a place of L lying above the place $t \mapsto \infty$ of $k(t)$, respectively. Suppose that $g(Z)$ has the Siegel property. Then the following holds.*

(a) *The cyclic group I has at most two orbits, with lengths equal the multiplicities of the elements in $g^{-1}(\infty)$.*
(b) *$A = GD$ and $I \leq G \cap D$. In particular, $A = N_A(I)G$.*
(c) *If A is primitive, then G is primitive, too.*
(d) *G has a genus 0 system, with a generator of I belonging to it.*

Proof. For (a) and (b) see [48, Lemma 3.4], for (c) see [48, Theorem 3.5], and (d) follows from Section 4.1. □

4.6. Monodromy groups and ramification of Siegel functions

The main result of this section is the following:

Theorem 4.8. *Let $g(Z)$ be a non-constant, functionally indecomposable rational function over a field k of characteristic 0. Suppose that $|g^{-1}(\infty)| = 2$. Let A and G be the arithmetic and geometric monodromy group of $g(Z)$, respectively,and $(\sigma_1, \sigma_2, \ldots, \sigma_r)$ a branch cycle description. Let T be the unordered tuple*

$(\mathrm{ord}(\sigma_1), \mathrm{ord}(\sigma_2), \ldots, \mathrm{ord}(\sigma_r))$. *Then either* $\mathcal{A}_n \leq G \leq A \leq \mathcal{S}_n$, *with many possibilities for* T, *or one of the following holds, where* $G \leq A \leq A_{max}$:

1. *A acts as an affine group, and one of the following holds:*

n	G	A_{max}	T
5	$\mathrm{AGL}_1(5)$	G	(2, 4, 4)
7	$\mathrm{AGL}_1(7)$	G	(2, 3, 6)
8	$\mathrm{A\Gamma L}_1(8)$	G	(3, 3, 6), (3, 3, 7)
8	$\mathrm{AGL}_3(2)$	G	*many cases*
9	$\mathrm{A\Gamma L}_1(9)$	G	(2, 4, 8)
9	$\mathrm{AGL}_2(3)$	G	(2, 3, 8), (2, 6, 8), (2, 2, 2, 8)
16	$C_2^4 \rtimes (C_5 \rtimes C_4)$	G	(2, 4, 8)
16	*index* 2 *in* A_{max}	$(\mathcal{S}_4 \times \mathcal{S}_4) \rtimes C_2$	(2, 4, 8)
16	$C_2^4 \rtimes \mathcal{S}_5$	G	*many cases*
16	$\mathrm{A\Gamma L}_2(4)$	G	(2, 4, 15)
16	$C_2^4 \rtimes \mathcal{A}_7$	G	(2, 4, 14)
16	$\mathrm{AGL}_4(2)$	G	*many cases*
32	$\mathrm{AGL}_5(2)$	G	*several cases*

2. (*Product action*) $n = m^2$, $G = A = (\mathcal{S}_m \times \mathcal{S}_m) \rtimes C_2$, *many possibilities for* T.

3. *A is almost simple, and one of the following holds:*

n	G	A_{max}	T
6	$\mathrm{PSL}_2(5)$	$\mathrm{PGL}_2(5)$	*many cases*
6	$\mathrm{PGL}_2(5)$	G	(2, 4, 5), (4, 4, 5), (4, 4, 3)
8	$\mathrm{PSL}_2(7)$	$\mathrm{PGL}_2(7)$	(2, 3, 7), (3, 3, 7), (3, 3, 4)
8	$\mathrm{PGL}_2(7)$	G	(2, 6, 7), (2, 6, 4)
10	$\mathcal{A}_5$	$\mathcal{S}_5$	(2, 3, 5)
10	$\mathcal{S}_5$	G	(2, 4, 5), (2, 6, 5), (2, 2, 2, 5)
10	$\mathrm{PSL}_2(9)$	$\mathrm{P\Gamma L}_2(9)$	(2, 4, 5)
10	$\mathrm{P\Sigma L}_2(9)$	$\mathrm{P\Gamma L}_2(9)$	(2, 6, 5), (2, 2, 2, 5)
10	M_{10}	$\mathrm{P\Gamma L}_2(9)$	(2, 4, 8)
10	$\mathrm{P\Gamma L}_2(9)$	G	(2, 8, 8)
12	M_{11}	G	*many cases*
12	M_{12}	G	*many cases*
14	$\mathrm{PSL}_2(13)$	$\mathrm{PGL}_2(13)$	(2, 3, 7), (2, 3, 13)
21	$\mathrm{P\Sigma L}_3(4)$	G	(2, 4, 14)
21	$\mathrm{P\Gamma L}_3(4)$	G	(2, 3, 14), (2, 6, 14), (2, 2, 2, 14)
22	M_{22}	$\mathrm{M}_{22} \rtimes C_2$	(2, 4, 11)
22	$\mathrm{M}_{22} \rtimes C_2$	G	(2, 4, 11), (2, 6, 11), (2, 2, 2, 11)
24	M_{24}	G	*many cases*
40	$\mathrm{PSL}_4(3)$	$\mathrm{PGL}_4(3)$	(2, 3, 20)
40	$\mathrm{PGL}_4(3)$	G	(2, 4, 20)

For completeness, we state the analogous result if $|g^{-1}(\infty)| = 1$. The proof follows immediately from Lemma 4.7 and the classification result in [45].

Theorem 4.9. *Let $g(Z)$ be a non-constant, functionally indecomposable rational function over a field k of characteristic 0 with $|g^{-1}(\infty)| = 1$. Let G be the geometric monodromy group of $g(Z)$, and $(\sigma_1, \sigma_2, \dots, \sigma_r)$ be a branch cycle description. Let T be the unordered tuple $(\mathrm{ord}(\sigma_1), \mathrm{ord}(\sigma_2), \dots, \mathrm{ord}(\sigma_r))$. Then one of the following holds holds:*

1. *Infinite series*:
   a) $n = p$, $G = C_p$, $T = (p, p)$, *p a prime.*
   b) $n = p$, $G = D_p$, $T = (2, 2, p)$, *p an odd prime.*
   c) $G = \mathcal{A}_n$ *(n odd) or* $\mathcal{S}_n$, *many possibilities for T.*
2. *Sporadic cases*:
   a) $n = 6$, $G = \mathrm{PGL}_2(5)$, $T = (2, 4, 6)$.
   b) $n = 7$, $G = \mathrm{PGL}_3(2)$, $T = (2, 3, 7)$, $(2, 4, 7)$, *or* $(2, 2, 2, 7)$.
   c) $n = 8$, $G = \mathrm{PGL}_2(7)$, $T = (2, 3, 8)$.
   d) $n = 9$, $G = \mathrm{P\Gamma L}_2(8)$, $T = (2, 3, 9)$ *or* $(3, 3, 9)$.
   e) $n = 10$, $G = \mathrm{P\Gamma L}_2(9)$, $T = (2, 4, 10)$.
   f) $n = 11$, $G = \mathrm{PSL}_2(11)$, $T = (2, 3, 11)$.
   g) $n = 11$, $G = \mathrm{M}_{11}$, $T = (2, 4, 11)$.
   h) $n = 13$, $G = \mathrm{PGL}_3(3)$, $T = (2, 3, 13)$, $(2, 4, 13)$, $(2, 6, 13)$, *or* $(2, 2, 2, 13)$.
   i) $n = 15$, $G = \mathrm{PGL}_4(2)$, $T = (2, 4, 15)$, $(2, 6, 15)$, *or* $(2, 2, 2, 15)$.
   j) $n = 21$, $G = \mathrm{P\Gamma L}_3(4)$, $T = (2, 4, 21)$.
   k) $n = 23$, $G = \mathrm{M}_{23}$, $T = (2, 4, 23)$.
   l) $n = 31$, $G = \mathrm{PGL}_5(2)$, $T = (2, 4, 31)$.

4.7. Proof of Theorem 4.8

The strategy is as follows. Functional indecomposability of $g(Z)$ implies that A is primitive. By Lemma 4.7(a) we can apply Theorem 3.3. It remains to find normal subgroups G of A for which (b) and (d) of Lemma 4.7 hold. For that it is useful to know that G is primitive as well by Lemma 4.7(c). The proof is split up into three sections, according to whether A acts as an affine group, preserves a product structure, or is almost simple.

4.7.1. *Affine action*

The proof is based on work by Guralnick, Neubauer, and Thompson on genus 0 systems in primitive permutation groups of affine type. Suppose that A is affine. The cases that A has degree ≤ 4 are immediate, so assume $n \geq 5$. G is primitive by Lemma 4.7. Let σ_r be a generator of I, so σ_r has two cycles. Let N be the minimal normal subgroup of A. First suppose that $G'' = 1$. As G' is Abelian, we have $G' = N$, and primitivity of G forces that G/N acts irreducibly on N. But $G/N = G/G'$ is Abelian, so G/N is cyclic by Schur's Lemma. More precisely, we can identify G as a subgroup of $\mathrm{AGL}_1(q)$, where $q = |N| = p^m$ for a prime p. As $q > 4$, we have necessarily that σ fixes a point and moves the remaining ones in a $(q-1)$–cycle. An element in N has index $q(1-1/p) \geq q/2$, whereas an element in $\mathrm{AGL}_1(q)$ of order $t|q-1$ has index $(q-1)(1-1/t) \geq (q-1)/2$. The index relation gives $r = 3$ and that neither σ_1 nor σ_2 is contained in N. So $2(q-1) = q-2+(q-1)(1-1/t_1+1-1/t_2) \geq q-2+(q-1)(1/2+2/3)$, where t_i is the order of σ_i. It follows $q \leq 7$.

Next suppose that $G'' > 1$. Write $n = p^m$. We use [20, Theorems 4.1, 5.1]. If $p > 5$, then $p = 7$ or 11, and $m = 2$. Furthermore $T = (2,4,6)$ for $p = 7$, or $T = (2,3,8)$ for $p = 11$. So this does not occur in view of $\mathrm{ord}(\sigma_r) \geq n/2 = p^2/2$. Next suppose $p = 5$. We use [50, Theorem 1.5] (the statement is already in [20], but only parts are proven there). Again compare $\mathrm{ord}(\sigma_r) \geq n/2$ with the possible genus 0 systems given for $p = 5$. Only $n = 25$ with $G = (C_5 \times C_5) \rtimes (\mathrm{SL}_2(5) \rtimes C_2)$ could arise. However, this group does not have an element with only two cycles by Theorem 3.3. So we have $p = 3$ or 2. Suppose that $p = 3$. Use [50, Theorem 1.5] to see that necessarily $n = 9$. Check directly that only the listed degree 9 cases occur. Now suppose $p = 2$. By [50], we get $n \leq 2^8$. Except for the cases $A = \mathrm{AGL}_7(2)$ and $A = \mathrm{AGL}_8(2)$, these cases are small enough to be checked with the computer algebra system Magma [3], giving the possibilities as stated. In order to see that there are no examples in $\mathrm{AGL}_7(2)$ and $\mathrm{AGL}_8(2)$, one also needs some character theoretic arguments based on [52, Theorem 1] to exclude potential generating systems, and [55, Theorem 7.2.1] in order to see that elements from certain conjugacy classses cannot multiply up to 1. The nonexistence of cases for $\mathrm{AGL}_7(2)$ and $\mathrm{AGL}_8(2)$ follows also from [40].

4.7.2. *Product action*

Let A be a non-affine group which preserves a product structure. Again let σ_r be the element with two cycles. By Theorem 3.3, we have have $A = (U \times U) \rtimes C_2$ in product action, where either $U = \mathcal{S}_m$, or $U = \mathrm{PGL}_2(p)$ for a prime $p \geq 5$. By primitivity of G we cannot have $G \leq (U \times U)$. On the other hand, the presence of σ_r forces $U \times U \leq G$, see the proof of Theorem 3.3, so $G = A$.

Let Δ be the set U is acting on, and let $\Omega := \Delta \times \Delta$ be the set $G = A$ acts on. We show the existence of a genus 0 system of the required form for $U = \mathcal{S}_m$. Write $\Delta := \{1, 2, \dots, m\}$. Let $\tau \in G$ be the element which maps (i, j) to (j, i). Let $1 \leq a < m$ be prime to m. For $\alpha := (1, 2, \dots, m) \in \mathcal{S}_m$ and $\beta := (a, a-1, \dots, 2, 1)(m, m-1, \dots, a+2, a+1) \in \mathcal{S}_m$ set $\sigma_1 := (\alpha, \beta) \in A$, $\sigma_2 := \tau$, $\sigma_3 := (\sigma_1\sigma_2)^{-1}$. We show that $(\sigma_1, \sigma_2, \sigma_3)$ is a genus 0 system of G.

First we show that σ_1 and σ_2 generate G. Note that a, $m-a$, and m are pairwise prime. Let r and s be integers such that $rm \equiv 1 \pmod{a(m-a)}$ and $sa(m-a) \equiv 1 \pmod{m}$. Then clearly $\sigma_1^{rm} = (1, \beta)$ and $\sigma_1^{sa(m-a)} = (\alpha, 1)$. Conjugating with τ shows that also $(\beta, 1), (1, \alpha) \in G$. We are done once we know that α, β generate $\mathcal{S}_m$. But this is clear, because it is easy to see that the generated group is doubly transitive and contains the transposition $\alpha\beta = (a, m)$.

We compute the index of σ_i. The element σ_1 has a cycle of length ma, and another one of length $m(m-a)$. So $\mathrm{ind}(\sigma_1) = m^2 - 2$. Furthermore, $\mathrm{ind}(\sigma_2) = (m^2-m)/2$, because $\sigma_2 = \tau$ has exactly m fixed points, and switches the remaining points in cycles of length 2. Next, $\sigma_3 := \tau(\alpha^{-1}, \beta^{-1})$. The element $(i, j) \in \Omega$ is a fixed point of σ_3 if and only if $j = i^\alpha$ and $i = j^\beta$, hence $j = i+1$ with $i \neq a, m$. Thus there are exactly $m-2$ fixed points. Now $\sigma_3^2 = ((a, m), (a+1, 1))$ has order 2 and exactly $(m-2)^2$ fixed points. Lemma 4.1 gives

$$\begin{aligned}\mathrm{ind}(\sigma_3) &= m^2 - \frac{1}{4}(\varphi(4)(m-2) + \varphi(2)(m-2)^2 + \varphi(1)m^2)\\ &= (m^2+m)/2,\end{aligned}$$

so the genus of $(\sigma_1, \sigma_2, \sigma_3)$ is 0.

We now show that $U = \mathrm{PGL}_2(p)$ does not occur. Again, let τ be the element which flips the entries of Ω. At least two of the elements in $\sigma_1, \dots, \sigma_{r-1}$ must be of the form $\sigma = (\alpha, \beta)\tau$, with $\alpha, \beta \in \mathrm{PGL}_2(p)$. This σ is conjugate in G to $(1, \alpha\beta)\tau$. If $\alpha\beta = 1$, then $\mathrm{ind}(\sigma) = ((p+1)^2 - (p+1))/2$. Otherwise, $\mathrm{ind}(\sigma) \geq 2((p+1)^2 - 4)/3$, because $\sigma^2 \sim (\alpha\beta, \alpha\beta)$ has at most 4 fixed points. If σ has the form (α, β), then σ has at most $4(p+1)$ fixed points, so $\mathrm{ind}(\sigma) \geq ((p+1)^2 - 4(p+1))/2$. As $\sum_{i=1}^{r-1} \mathrm{ind}(\sigma_i) = (p+1)^2$, it follows from these index bounds that $r = 3$, so σ_1 and σ_2 have the τ–part. Because not both σ_1 and σ_2 can be involutions (for G is not dihedral), we obtain $(p+1)^2 \geq ((p+1)^2 - (p+1))/2 + 2((p+1)^2 - 4)/3$, so $p < 5$, a contradiction.

4.7.3. *Almost simple action*

Let S be the simple non-Abelian group with $S \leq G \leq A \leq \mathrm{Aut}(S)$, and σ_r again the element with two cycles. We have to check the groups in Theorem 3.3(III) for the existence of genus 0 systems of the required form.

If $S = \mathcal{A}_n$ (n even) in natural action, then it is easy to check that there are many such genus 0 systems, and it is obviously not possible to give a reasonable classification of them. Next, the cases except the infinite series 3c and 3d of Theorem 3.3 are easily dealt with, using the atlas [9] and some ad hoc arguments, or more conveniently using [17]. Now assume $\mathrm{PSL}_2(q) \leq G \leq \mathrm{P\Gamma L}_2(q)$ in the natural action, with $q \geq 5$ a prime power. Note that q is odd. As $n = q+1$ and $\mathrm{ind}(\sigma_r) = n-2$, the index relation gives

$$q + 1 = \sum_{k=1}^{r-1} \mathrm{ind}(\sigma_k).$$

We distinguish two cases. First assume $G \leq \mathrm{PGL}_2(q)$. For $\sigma \in \mathrm{PGL}_2(q)$ we easily obtain (see e. g. [45]) that $\mathrm{ind}(\sigma) \geq (q-1)(1 - 1/\mathrm{ord}(\sigma))$. So the index relation gives

$$\sum_{k=1}^{r-1}(1 - 1/\mathrm{ord}(\sigma_k)) \leq \frac{q+1}{q-1}.$$

As G is not dihedral, either $r \geq 4$, or $r = 3$ and σ_1 and σ_2 are not both involutions. In the first case, we obtain $q = 5$, and in the second case, $\sum_{k=1}^{2}(1 - 1/\mathrm{ord}(\sigma_k)) \geq (1 - 1/2) + (1 - 1/3)$ gives $q \leq 13$. Check these cases directly.

Next suppose that $G \not\leq \mathrm{PGL}_2(q)$, but $G \leq \mathrm{P\Gamma L}_2(q)$. Check the case $q = 9$, $\sigma_r \notin \mathrm{PGL}_2(9)$ directly and exclude it in the following. Thus $\sigma_r \in \mathrm{PGL}_2(q)$ by Lemma 3.47. Denote by $\bar{\sigma}_k$ the image of σ_k in the Abelian group $\mathrm{P\Gamma L}_2(q)/\mathrm{PGL}_2(q)$. Then the elements $\bar{\sigma}_k$ for $k = 1, \ldots, r-1$ are not all trivial and have product 1. Thus the order of two of the elements $\sigma_1, \sigma_2, \ldots, \sigma_{r-1}$ have a common divisor ≥ 2. Furthermore, for $\sigma \in \mathrm{P\Gamma L}_2(q)$, we have the index bound $\mathrm{ind}(\sigma) \geq (1 - 1/\mathrm{ord}(\sigma))(q - \sqrt{q})$, see [45]. This information, combined with the index relation, gives

$$\frac{5}{4} = \left(1 - \frac{1}{2}\right) + \left(1 - \frac{1}{4}\right) \leq \sum_{k=1}^{r-1}(1 - 1/\mathrm{ord}(\sigma_k)) \leq \frac{1}{q - \sqrt{q}} \sum_{k=1}^{r-1} \mathrm{ind}(\sigma_k) = \frac{q+1}{q - \sqrt{q}}.$$

Hence $q \leq 5\sqrt{q} + 4$, so $q = 9, 25$, or 27. If $q = 27 = 3^3$, then the above argument shows that the common divisor can be chosen to be 3, so the analogous calculation gives $4/3 \leq (27 + 1)/(27 - \sqrt{27})$, which does not hold. Similarly, refine the argument (using [45]) or simply check with GAP [17] that $q = 25$ does not occur.

The main case which is left to investigate is case III(d) of Theorem 3.3, namely that $\mathrm{PSL}_m(q) \leq G \leq \mathrm{P\Gamma L}_m(q)$ acts naturally on the projective space, q is an odd prime power, $m \geq 2$ is even, and σ_r is the square of a Singer cycle. The case $m = 2$ has been done above. The case $m \geq 4$, which is somewhat involved, will be handled in the remaining part of this section. In order to finish the almost simple case, we need to show that $m = 4$, $q = 3$, giving the degree $n = 40$ cases in Theorem 4.8. For this we need the following index bounds:

Lemma 4.10. *Let q be a prime power, and $1 \neq \sigma \in \mathrm{P\Gamma L}_m(q)$, where $m \geq 4$. Then the following holds:*

1. $\mathrm{ind}(\sigma) \geq (1 - 1/\mathrm{ord}(\sigma))(q^{m-1} - 1)$.
2. *If* $\mathrm{ord}(\sigma)$ *is a prime not dividing $q(q-1)$, and $\sigma \in \mathrm{PGL}_m(q)$, then* $\mathrm{ind}(\sigma) \geq (1 - 1/\mathrm{ord}(\sigma))q^{m-2}(q + 1)$.
3. *If* $\mathrm{ord}(\sigma)$ *is a prime dividing q, and $\sigma \in \mathrm{PGL}_m(q)$, then* $\mathrm{ind}(\sigma) = (1 - 1/\mathrm{ord}(\sigma))(q^m - q^j)/(q - 1)$ *for some $1 \leq j \leq m - 1$.*

Proof. For 1 see [45]. Set $N := (q^m - 1)/(q - 1)$, and let s be the order of σ. Now assume the hypothesis in 2. Let $\chi(\sigma)$ be the number of fixed points of σ. Then clearly $\mathrm{ind}(\sigma) = (N - \chi(\sigma))(1 - 1/s)$. Let $\hat{\sigma} \in \mathrm{GL}_m(q)$ be a preimage of σ of order s. For $\alpha \in \mathbb{F}_q$, let $d(\alpha)$ be the dimension of the eigenspace of $\hat{\sigma}$ with eigenvalue α. Clearly

$$\chi(\sigma) = \sum_{\alpha \in \mathbb{F}_q} \frac{q^{d(\alpha)} - 1}{q - 1}.$$

So $\chi(\sigma) \le (q^d - 1)/(q-1)$, where $d = \sum_\alpha d(\alpha)$. On the other hand, as s does not divide $q-1$, $\hat{\sigma}$ must have eigenvalues not in $\mathbb{F}_q$. So $d \le m-2$, and the claim follows.

To prove 3, note that a preimage of order s of σ in $\mathrm{GL}_m(q)$ admits Jordan normal form over $\mathbb{F}_q$. □

Recall that $N = (q^m - 1)/(q-1)$. Note that $\mathrm{ind}(\sigma_r) = N - 2$, so the index relation gives

$$\sum_{k=1}^{r-1} \mathrm{ind}(\sigma_k) = N. \tag{4.2}$$

Claim 4.11. $r = 3$.

Proof. Suppose that $r \ge 4$. From 1 in Lemma 4.10 we have $\mathrm{ind}(\sigma_k) \ge (1 - 1/\mathrm{ord}(\sigma_k))(q^{m-1} - 1)$, hence

$$\begin{aligned}\sum_{k=1}^{r-1}(1 - 1/\mathrm{ord}(\sigma_k)) &\le \frac{N}{q^{m-1}-1} = 1 + \frac{1}{q-1} + \frac{1}{q^{m-1}-1} \\ &\le 1 + \frac{1}{q-1} + \frac{1}{q^3-1} < 1 + \frac{2}{q-1}.\end{aligned} \tag{4.3}$$

First note that if $r \ge 4$, then $3/2 < 1 + \frac{2}{q-1}$, so $q < 5$ and hence $q = 3$. We get more precisely $\sum_{k=1}^{r-1}(1 - 1/\mathrm{ord}(\sigma_k)) \le 1 + 1/(3-1) + 1/(27-1) = 20/13$. However, $2(1 - 1/2) + (1 - 1/3) = 5/3 > 20/13$, so besides $q = 3$ we obtain $r = 4$, and $\sigma_1, \sigma_2, \sigma_3$ are involutions. Note that σ_4 has cycles of even length, as $4|N$. So these involutions do have fixed points by Lemma 4.2. Let $\hat{\sigma}$ be a preimage in $\mathrm{GL}_m(3)$ of an involution in $\mathrm{PGL}_m(3)$ with fixed points. Thus $\hat{\sigma}^2$ has eigenvalue 1 on the one hand, but is also scalar. So $\hat{\sigma}$ has only the eigenvalues 1 and -1, and both eigenvalues occur. This shows $\chi(\sigma) \equiv 2 \pmod 3$, hence $\mathrm{ind}(\sigma) \equiv (N-2)/2 \equiv 1 \pmod 3$. So we get the contradiction

$$1 \equiv N = \sum_{k=1}^{3} \mathrm{ind}(\sigma_k) \equiv 0 \pmod 3.$$ □

Claim 4.12. $q \le 7$.

Proof. From (4.3) and $r = 3$ we obtain

$$\frac{1}{\mathrm{ord}(\sigma_1)} + \frac{1}{\mathrm{ord}(\sigma_2)} \ge 1 - \frac{1}{q-1} - \frac{1}{q^{m-1}-1} \ge 1 - \frac{1}{q-1} - \frac{1}{q^3-1}. \tag{4.4}$$

σ_1 and σ_2 are not both involutions (because G is not dihedral). This gives $1/2 + 1/3 \ge 1 - 1/(q-1) - 1/(q^3-1)$, so $q < 8$. □

In the following we assume $\mathrm{ord}(\sigma_1) \le \mathrm{ord}(\sigma_2)$.

Claim 4.13. $q \neq 7$.

Proof. Suppose $q = 7$. From (4.3) we obtain $1/\mathrm{ord}(\sigma_1) + 1/\mathrm{ord}(\sigma_2) \geq 1 - 1/6 - 1/(7^3 - 1) > 3/4$, hence $\mathrm{ord}(\sigma_1) = 2$, $\mathrm{ord}(\sigma_2) = 3$. Again, as $2|(N/2) = \mathrm{ord}(\sigma_3)$, we get that σ_1 has fixed points, and so $\chi(\sigma_1) \equiv 2 \pmod 7$, hence $\mathrm{ind}(\sigma_1) \equiv 3 \pmod 7$. From $3 + 2(N - \chi(\sigma_2))/3 = 3 + \mathrm{ind}(\sigma_2) \equiv N \equiv 1 \pmod 7$ it follows that $\chi(\sigma_2) \equiv 4 \pmod 7$. So a preimage $\hat{\sigma}_2 \in \mathrm{GL}_m(7)$ of σ_2 has exactly 4 different eigenvalues λ in $\mathbb{F}_7$. Let $\hat{\sigma}_2^3$ be the scalar ρ. The equation $X^3 - \rho$ has at most 3 roots in $\mathbb{F}_7$, a contradiction. □

Claim 4.14. $q \neq 5$.

Proof. Suppose $q = 5$. The proof is similar to the argument in the previous claim, so we only describe the steps which differ from there. We obtain $\mathrm{ord}(\sigma_1) = 2$ and $\mathrm{ord}(\sigma_2) = 3$ or 4.

First assume that $\mathrm{ord}(\sigma_2) = 3$. As $3|N$, we obtain that σ_2 has fixed points by Lemma 4.2, so a preimage $\hat{\sigma}_2 \in \mathrm{GL}_m(5)$ has eigenvalues in $\mathbb{F}_5$. Suppose (without loss, as $\gcd(q - 1, 3) = 1$) that 1 is one of the eigenvalues. As $(X^3 - 1)/(X - 1)$ is irreducible in $\mathbb{F}_5$, this is the only $\mathbb{F}_5$–eigenvalue of $\hat{\sigma}_2$. So $\chi(\sigma_2) \equiv 1 \pmod 5$, hence $\mathrm{ind}(\sigma_2) \equiv 0 \pmod 5$. This gives $\chi(\sigma_1) \equiv 4 \pmod 5$, which is clearly not possible.

Now assume that $\mathrm{ord}(\sigma_2) = 4$. The index relation together with Lemma 4.1 gives

$$2\chi(\sigma_1) + 2\chi(\sigma_2) + \chi(\sigma_2^2) = N. \tag{4.5}$$

Clearly, $\chi(\sigma_2^2) \geq \chi(\sigma_2)$. If $\chi(\sigma_2^2) = 0$, then $\chi(\sigma_1) \equiv 3 \pmod 5$, which is not possible. Thus σ_2^2 has fixed points.

First assume that σ_2 has no fixed points. Then σ_1 has fixed points by Lemma 4.2, so $\chi(\sigma_1) \equiv 2 \pmod 5$. From that we obtain

$$2((5^a - 1) + (5^{m-a} - 1)) + ((5^b - 1) + (5^{m-b} - 1)) = 5^m - 1$$

for suitable $1 \leq a, b \leq m - 1$. However, $5^a + 5^{m-a} \leq 5 + 5^{m-1}$, and similarly for b, so $3(5 + 5^{m-1}) \geq 5(5^{m-1} + 1)$. This gives $5^{m-1} \leq 5$, a contradiction.

So σ_2 has fixed points as well, therefore all eigenvalues of a preimage $\hat{\sigma}_2 \in \mathrm{GL}_m(5)$ are in $\mathbb{F}_5$. Without loss assume that 1 is an eigenvalue of $\hat{\sigma}_2$, and denote by a, b, c, d the multiplicity of the the eigenvalue $1, 2, 3, 4 \in \mathbb{F}_5$, respectively. Clearly $b + c > 0$, as $\hat{\sigma}_2$ has order 4. Also, $a > 0$ by our choice. We obtain that $\chi(\sigma_2^2) = (5^{a+d} - 1)/4 + (5^{b+c} - 1)/4$, hence $\chi(\sigma_2^2) \equiv 2 \pmod 5$. Relation (4.5) gives $\chi(\sigma_1) + \chi(\sigma_2) \equiv 2 \pmod 5$. If σ_1 has fixed points, then $\chi(\sigma_1) \equiv 2 \pmod 5$, hence $\chi(\sigma_2) \equiv 0 \pmod 5$, which is not the case. Thus $\chi(\sigma_1) = 0$ and $\chi(\sigma_2) \equiv 2 \pmod 5$, so $d = 0$ and either $b = 0$ or $c = 0$. Suppose without loss $c = 0$. Hence $\chi(\sigma_2) = \chi(\sigma_2^2)$, and we obtain

$$N = \frac{5^m - 1}{4} = 2\chi(\sigma_2) + \chi(\sigma_2^2) = 3\chi(\sigma_2) = 3\left(\frac{5^a - 1}{4} + \frac{5^{m-a} - 1}{4}\right),$$

so

$$5^m + 5 = 3(5^a + 5^{m-a}) \le 3(5 + 5^{m-1}),$$

a contradiction as previously. □

Claim 4.15. If $q = 3$, then $m = 4$ and $(\mathrm{ord}(\sigma_1), \mathrm{ord}(\sigma_2)) = (2, 3)$ or $(2, 4)$.

Proof. As $\mathrm{ind}(\sigma_k) \ge (3^{m-1} - 1)/2$, and $\mathrm{ind}(\sigma_k) \ge 2(3^{m-2} - 1)$ unless σ_k is an involution in $\mathrm{PGL}_m(3)$ of minimal possible index, we obtain from the index relation (4.2) that

$$\mathrm{ind}(\sigma_k) \le \begin{cases} 3^{m-1} \text{ in any case,} \\ \frac{5 \cdot 3^{m-2}+3}{2} \text{ for } k = 2 \text{ if } \sigma_1 \text{ has not minimal possible index.} \end{cases} \tag{4.6}$$

We first note that no prime $s \ge 5$ does divide $\mathrm{ord}(\sigma_k)$, for (4.6) and Lemma 4.102 would give

$$(1 - \frac{1}{5})3^{m-2}4 \le \mathrm{ind}(\sigma_k) \le 3^{m-1},$$

which is nonsense. Similarly, we see that 9 does not divide $\mathrm{ord}(\sigma_k)$. Let $\sigma \in \mathrm{PGL}_m(3)$ have order 9, and let $\hat{\sigma} \in \mathrm{GL}_m(3)$ be a preimage of order 9. So $\hat{\sigma}$ admits Jordan normal form over $\mathbb{F}_3$, and there must be at least one Jordan block of size ≥ 4 by Lemma 3.5. Thus $\chi(\sigma) \le (3^{m-3} - 1)/2$, and also $\chi(\sigma^3) \le (3^{m-1} - 1)/2$. Now

$$\mathrm{ind}(\sigma) = (1 - \frac{1}{9})N - \frac{2}{3}\chi(\sigma) - \frac{2}{9}\chi(\sigma^3)$$

by Lemma 4.1. Use the above estimation to obtain after some calculation that $\mathrm{ind}(\sigma) \ge 32 \cdot 3^{m-4} > 3^{m-1}$, contrary to (4.6).

Now suppose that 4 divides the order of σ_k. Let σ be a power of σ_k of order 4. As σ_k must have a cycle of odd length by Lemma 4.2, σ must have a fixed point. Thus there is a preimage $\hat{\sigma} \in \mathrm{GL}_m(3)$ of σ with $\hat{\sigma}^4 = 1$. Let a and b be the number of Jordan blocks of size 1 with eigenvalue 1 and -1, respectively, and let j be the number of square blocks of size 2. The square of such a block matrix is a scalar with eigenvalue -1. We have $a + b + 2j = m$, and $2 \le a + b \le m - 2$. Also, $\chi(\sigma) = (3^a - 1 + 3^b - 1)/2$ and $\chi(\sigma^2) = (3^{a+b} - 1 + 3^{2j} - 1)/2$. From that we obtain

$$\begin{aligned} \mathrm{ind}(\sigma) &= \frac{3}{4}N - \frac{1}{2}\chi(\sigma) - \frac{1}{4}\chi(\sigma^2) \\ &= \frac{3}{4}N - \frac{3^a + 3^b - 2}{4} - \frac{3^{a+b} + 3^{m-a-b} - 2}{8} \\ &\ge \frac{3}{4}N - \frac{3^{m-2} - 1}{4} - \frac{3^{m-2} + 7}{8} = 3^{m-1} - 1. \end{aligned}$$

Note that $\mathrm{ind}(\sigma_k) \ge \mathrm{ind}(\sigma)$. From that we see that $k = 2$, and by (4.6) it follows that σ_1 is an involution with minimal possible index. Thus $\mathrm{ind}(\sigma_2) = 3^{m-1}$ again by (4.6). This shows that $\mathrm{ord}(\sigma_2)$ is not divisible by 3, because then a cycle of σ_2 of length divisible by 3 would break up into at least 3 cycles of σ, so $\mathrm{ind}(\sigma_2) \geq 2 + \mathrm{ind}(\sigma) \geq 1 + 3^{m-1}$, a contradiction to (4.6).

Similarly, we see that 8 does not divide $\mathrm{ord}(\sigma_2)$. Suppose otherwise. Then we get the same contradiction unless $\mathrm{ord}(\sigma_2) = 8$ and σ_2 has exactly 1 cycle of length 8. But then σ_2^4 has $N - 8$ fixed points, however $\chi(\sigma_2^4) \leq (3^{m-1} + 1)/2$, so $(3^m - 1)/2 - 8 \leq (3^{m-1} + 1)/2$, so $3^{m-1} \leq 9$, a contradiction.

So $\mathrm{ord}(\sigma_2) = 4$, and $\mathrm{ind}(\sigma_2) = 3^{m-1}$ by what we have seen so far. Express $\mathrm{ind}(\sigma_2)$ in terms of a and b as above. As $\hat{\sigma}_1$ fixes a hyperplane pointwise, and $<\hat{\sigma}_1, \hat{\sigma}_2>$ is irreducible, we infer that $a, b \leq 1$. Also, $a + b > 0$, so $a = b = 1$ because $a + b$ is even. Substitute $a = b = 1$ in the relation $\mathrm{ind}(\sigma_2) = 3^{m-1}$ to get $3^{m-1} = 27$, so $m = 4$. This case indeed occurs.

Next we look at elements of order 6. Let $\sigma \in \mathrm{PGL}_m(3)$ have order 6, and $\hat{\sigma} \in \mathrm{GL}_m(3)$ be a preimage. We have

$$\mathrm{ind}(\sigma) = \frac{5}{6}N - \frac{1}{3}\chi(\sigma) - \frac{1}{3}\chi(\sigma^2) - \frac{1}{6}\chi(\sigma^3).$$

Clearly

$$\chi(\sigma^2) \leq \frac{3^{m-1} - 1}{2}, \qquad \chi(\sigma^3) \leq \frac{3^{m-1} + 1}{2}.$$

If σ has no fixed points, then $\hat{\sigma}^6 = -\mathbf{1}$, and therefore σ^3 has no fixed points as well. In this case, we thus obtain $\mathrm{ind}(\sigma) \geq 5N/6 - \chi(\sigma^2)/3 \geq (13 \cdot 3^{m-1} - 3)/12 > 3^{m-1}$. This, in conjunction with (4.6), shows that if $\mathrm{ord}(\sigma_k) = 6$, then σ_k has a fixed point. Suppose that $\sigma = \sigma_k$ has order 6 and a fixed point. Then $\hat{\sigma}$ admits Jordan normal form over $\mathbb{F}_3$, and one realizes easily that

$$\chi(\sigma) \leq \frac{3^{m-2} - 1 + 3^1 - 1}{2} = \frac{3^{m-2} + 1}{2}.$$

Using this, one obtains after some calculation

$$\mathrm{ind}(\sigma) \geq \frac{17 \cdot 3^{m-1} - 9}{18}.$$

However, $(17 \cdot 3^{m-1} - 9)/18 > (5 \cdot 3^{m-2} + 3)/2$, so we get from (4.6) that $k = 2$ and σ_1 is an involution with minimal index. So $\mathrm{ind}(\sigma_2) = 3^{m-1}$ by (4.2), and σ_1 leaves a hyperplane invariant. The irreducibility of $<\sigma_1, \sigma_2>$ forces that $\hat{\sigma}_2$ has eigenspaces of dimension at most 1. On the other hand, the Jordan blocks of $\hat{\sigma}_2$ have size at most 3. As $m \geq 4$, there is thus exactly one Jordan block with eigenvalue 1, and exactly one with eigenvalue -1. Let u and $m - u$ be the size of these blocks, respectively. Clearly $\chi(\sigma_2) = 2$, $\chi(\sigma_2^2) = 4$, and $\chi(\sigma_2^3) = (3^u + 3^{m-u} - 2)/2$. From that one computes

$$\mathrm{ind}(\sigma_2) = \frac{5 \cdot 3^m - 3^u - 3^{m-u} - 27}{12}.$$

Now $\mathrm{ind}(\sigma_2) = 3^{m-1}$ yields the equation $3^m = 3^u + 3^{m-u} + 27$, which gives $3^{m-u} = (3^u + 27)/(3^u - 1)$. Check that the right hand side is never a power of 3 for $u = 1, 2, 3$.

It remains to look at $\mathrm{ord}(\sigma_2) = 3$. Then $\mathrm{ord}(\sigma_1) = 2$ or 3. Note that $\mathrm{ind}(\sigma_2) = 3^{m-1} - 3^{j_2-1}$ by Lemma 4.103, where j_2 is the number of Jordan blocks. Suppose that $\mathrm{ord}(\sigma_1) = 3$, and let j_1 be the number of Jordan blocks. The index relation yields $3^{m-1} + 1 = 2(3^{j_1-1} + 3^{j_2-1})$. Looking modulo 3 shows that $j_1 = j_2 = 1$. But this gives $m = 2$, a contradiction.

Finally, suppose $\mathrm{ord}(\sigma_1) = 2$. As the cycles of σ_3 are divisible by 2, Lemma 4.2 shows that σ_1 has fixed points. Then $\mathrm{ind}(\sigma_1) = (3^m - 3^i - 3^{m-i} + 1)/4$, where $1 \le i \le m-1$ is the multiplicity of the eigenvalue 1 of an involutory preimage of σ_1 in $\mathrm{GL}_m(3)$. The index relation yields

$$3^{m-1} = 3^i + 3^{m-i} + 4 \cdot 3^{j_2-1} - 3.$$

If $i = 1$ or $m-1$, then the right hand side is bigger than the left hand side. Thus $2 \le i \le m-2$. Looking modulo 9 then shows that $j_2 = 2$, so we get $3^{m-1} = 3^i + 3^{m-i} + 9$. Looking modulo 27 reveals that $3^i = 3^{m-i} = 9$, thus $m = 4$. This occurs indeed. $\square$

5. Siegel functions over the rationals

5.1. Monodromy groups and ramification

The main arithmetic constraint on monodromy groups is given in the following lemma, see [48, Lemma 3.4]:

Lemma 5.1. *Let $g(Z) \in \mathbb{Q}(Z)$ be a rational function of degree $n = 2m \ge 2$, such that $g^{-1}(\infty)$ consists of two real elements, which are algebraically conjugate in $\mathbb{Q}(\sqrt{d})$, for $d > 1$ a square-free integer. Let t be a transcendental over $\mathbb{Q}$, and L a splitting field of $g(Z) - t$ over $\mathbb{Q}(t)$.*

Let $D \le A$ and $I \trianglelefteq D$ be the decomposition and inertia group of a place of L lying above the place $t \mapsto \infty$ of $\mathbb{Q}(t)$, respectively.

Then $I = <\sigma>$ for some $\sigma \in G$, and the following holds.

1. *σ is a product of two m–cycles.*
2. *σ^k is conjugate in D to σ for all k prime to m.*
3. *D contains an element which switches the two orbits of I.*
4. *D contains an involution τ, such that $\sigma^\tau = \sigma^{-1}$, and τ fixes the orbits of I setwise.*
5. *If $\sqrt{d} \notin \mathbb{Q}(\zeta_m)$ (with ζ_m a primitive m–th root of unity), then the centralizer $C_D(I)$ contains an element which interchanges the two orbits of I.*

The main result about the monodromy groups of Siegel functions over $\mathbb{Q}$ is.

Theorem 5.2. *Let $g(Z) \in \mathbb{Q}(Z)$ be a functionally indecomposable rational function of degree $n \geq 2$ with $|g^{-1}(\infty)| = 2$. Let A and G be the arithmetic and geometric monodromy group of g, respectively. Let T be the ramification type of g. Then one of the following holds:*

1. *n is even, $\mathcal{A}_n \leq G \leq A \leq \mathcal{S}_n$, many possibilities for T; or*
2. *$n = 6$, $G = \mathrm{PSL}_2(5)$, $A = \mathrm{PGL}_2(5)$, $T = (2, 5, 3)$ and $(2, 2, 2, 3)$; or*
3. *$n = 6$, $G = \mathrm{PGL}_2(5) = A$, $T = (4, 4, 3)$; or*
4. *$n = 8$, $G = \mathrm{AGL}_3(2) = A$, $T = (2, 2, 3, 4)$, $(2, 2, 4, 4)$, and $(2, 2, 2, 2, 4)$; or*
5. *$n = 10$, $S \leq G \leq A \leq \mathrm{Aut}(S)$, where $S = \mathcal{A}_5$ or $\mathcal{A}_6$, with many possibilities for T; or*
6. *$n = 16$, $G = (\mathcal{S}_4 \times \mathcal{S}_4) \rtimes C_2 = A$, $T = (2, 6, 8)$, $(2, 2, 2, 8)$; or*
7. *$n = 16$, $G = C_2^4 \rtimes \mathcal{S}_5 = A$, $T = (2, 5, 8)$, $(2, 6, 8)$, and $(2, 2, 2, 8)$.*

The analogue of the previous theorem for Siegel functions with $|g^{-1}(\infty)| = 1$ follows from the classification of the monodromy groups of polynomials. For completeness, we give the result from [45].

Theorem 5.3. *Let $g(Z) \in \mathbb{Q}(Z)$ be a functionally indecomposable rational function with $|g^{-1}(\infty)| = 1$ and of degree $n \geq 2$. Let A and G be the arithmetic and geometric monodromy group of g, respectively. Let T be the ramification type of g. Then one of the following holds:*

1. *n is a prime, $C_n = G \leq A = \mathrm{AGL}_1(n)$, $T = (n, n)$.*
2. *$n \geq 3$ is a prime, $D_n = G \leq A = \mathrm{AGL}_1(n)$, $T = (2, 2, n)$.*
3. *$n \geq 4$, $\mathcal{A}_n \leq G \leq A \leq \mathcal{S}_n$, many possibilities for T.*
4. *$n = 6$, $G = \mathrm{PGL}_2(5) = A$, $T = (2, 4, 6)$.*
5. *$n = 9$, $G = \mathrm{P\Gamma L}_2(8) = A$, $T = (3, 3, 9)$.*
6. *$n = 10$, $G = \mathrm{P\Gamma L}_2(9) = A$, $T = (2, 4, 10)$.*

5.2. Proof of Theorem 5.2

Let $\mathcal{E} = (\sigma_1, \sigma_2, \ldots, \sigma_r)$ be a genus 0 system of G, and T its type, such that σ_r is the element σ from Lemma 5.1. So $n = 2m$, where σ_r has two cycles, both of length m. We denote by L a splitting field of $g(Z) - t$ over $\mathbb{Q}(t)$, and if U is a subgroup of $A = \mathrm{Gal}(L/\mathbb{Q}(t))$, then L_U is the fixed field of U in L. First suppose that A is an affine permutation group (different from $\mathcal{A}_4$ and $\mathcal{S}_4$). Theorems 3.3 and 4.8 gives the candidates for G and A and genus 0 systems. The only possible degrees are 8 and 16. Suppose $n = 8$. The only possible candidate with a genus 0 system is $G = \mathrm{AGL}_3(2) = A$. The rational genus 0 systems in G have type $(3, 4, 4)$, $(4, 4, 4)$, $(2, 2, 4, 4)$, $(2, 2, 3, 4)$, or $(2, 2, 2, 2, 4)$. The $(3, 4, 4)$–tuple must have all branch points rational. By [41], the minimal field of definition of such a cover has degree 2 over $\mathbb{Q}$, so this case is out. In the $(4, 4, 4)$ case, a minimal field of definition has degree 4 over $\mathbb{Q}$ if all branch points are rational. There could possibly be two of the branch points conjugate, which would lower the degree of the minimal field of definition by at most a factor 2, so this does not occur as well. The cases with 4 and

5 branch points all occur, see Section 5.3. Now suppose $n = 16$. The only cases where G has a genus 0 system of the required form, and σ_r fulfills the necessary properties in Lemma 5.1, are the following:

(a) G has index 2 in $(\mathcal{S}_4 \times \mathcal{S}_4) \rtimes C_2$, $T = (2, 4, 8)$.
(b) $G = A = (\mathcal{S}_4 \times \mathcal{S}_4) \rtimes C_2$, $T = (2, 6, 8)$ or $T = (2, 2, 2, 12)$. (This is case $m = 4$ in 2 of Theorem 4.8.)
(c) $G = A = C_2^4 \rtimes \mathcal{S}_5$, $T = (2, 5, 8), (2, 6, 8)$, and $(2, 2, 2, 8)$.

We start excluding case (a), where $G_1 = (C_3 \times C_3) \rtimes C_4$, and $\mathcal{E}$ has type $(2, 4, 8)$. Here $[A : G] \leq 2$. The group G has, up to conjugacy, a unique subgroup U of index 8. Set $\tilde{U} := N_A(U)$. Then $A = \tilde{U}G$, so the fixed field $L_{\tilde{U}}$ is a regular extension of $\mathbb{Q}(t)$. Look at the action of A on $A/\tilde{U}$. With respect to this action, the elements in $\mathcal{E}$ have cycle types $2-2, 2-2-4, 8$. From that we get that $L_{\tilde{U}}$ has genus 0, and because of the totally ramified place at infinity, we have $L_{\tilde{U}} = \mathbb{Q}(x)$ where $t = f(x)$ with $f \in \mathbb{Q}[X]$. Now A, in this degree 8 action, preserves a block system of blocks of size 4, and the last element in $\mathcal{E}$ leaves the two blocks invariant. Suppose without loss that σ_2 corresponds to 0. Then this yields (after linear fractional changes) $f(X) = h(X)^2$ with $h \in \mathbb{Q}[X]$, where $h(X) = X^2(X^2 + pX + p)$, where the ramification information tells us that h has, besides 0, two further branch points which are additive inverses to each other. This gives the condition $27p^2 - 144p + 128 = 0$, so $p \in \mathbb{Q}(\sqrt{3}) \setminus \mathbb{Q}$, a contradiction.

Cases (b) and (c) however have the required arithmetic realizations. As the proof involves a considerable amount of computations, we postpone the analysis to Section 5.3.

None of the product action cases in 2 with $m \geq 5$ can occur, because by 3.3 there is no element with two cycles of equal lengths.

Now assume that A is an almost simple group. Suppose that A is neither the alternating nor the symmetric group in natural action. Theorem 4.8 lists those cases where a transitive normal subgroup G has a genus 0 system. In our case, the permutation degree $n = 2m$ is even, and one member σ_r of the genus 0 system is a product of two m–cycles. The condition (b) in Lemma 5.1, namely that σ_r is rational in A, already excludes most examples. The two biggest degrees which survive that condition are $n = 22$ with $G = \mathrm{M}_{22}$, $A = \mathrm{M}_{22} \rtimes C_2$ and $n = 24$ with $G = A = \mathrm{M}_{24}$. However, σ_r violates condition (d) of Lemma 5.1 in both cases.

Excluding the case $n = 12$, $G = \mathrm{M}_{12}$ for a moment, the next smallest cases with rational σ_r have degree $n \leq 10$. We go through the possibilities which fulfill the necessary properties from Lemma 5.1, starting with the small degrees.

Let $n = 6$. Then $A = \mathrm{PGL}_2(5)$, and $G = \mathrm{PSL}_2(5)$ or $G = \mathrm{PGL}_2(5)$. If $G = A$, then $T = (4, 4, 3)$, and an example is given by

$$g(Z) = \frac{Z^4(13Z^2 - 108Z + 225)}{(Z^2 - 15)^3}.$$

Next suppose $G = \mathrm{PSL}_2(5)$. There is the possibility $T = (2, 5, 3)$, with an example

$$g(Z) = \frac{Z^5(Z-2)}{(Z^2-5)^3},$$

or $T = (2, 2, 2, 3)$, where

$$g(Z) = \frac{(Z^2-2Z+2)(Z^2-16Z+14)^2}{(Z^2-2)^3}$$

is an example.

Let $n = 8$. Then $A = \mathrm{PGL}_2(7)$, and $[A : G] \le 2$. First suppose $G = \mathrm{PSL}_2(7)$. Then $T = (3, 3, 4)$. Suppose the required $g(Z)$ exists. Without loss assume that ∞ is the branch point corresponding to σ_3. The two finite branch points could be algebraically conjugate. But there is a Galois extension $K/\mathbb{Q}$ of degree dividing 4, such that the branch points are in K, and $g^{-1}(\infty) \subset K$. So, by linear fractional twists over K, we can pass from g to

$$\tilde{g}(Z) = \frac{(Z^2+a_1Z+a_0)(Z^2+p_1Z+p_0)^3}{Z^4}.$$

If $a_1 \neq 0$, then we may assume that $a_1 = 1$. If however $a_1 = 0$, then $p_1 = 0$ cannot hold, because $\tilde{g}$ were functionally decomposable. Thus if $a_1 = 0$, we may assume that $p_1 = 1$. Thus we have two cases to consider. Together with the obvious requirement $a_0p_0 \neq 0$, and the ramification information in the other finite branch point, this gives a 0–dimensional quasi affine variety. See [43, Sect. I.9] where this kind of computation is explained in detail. By computing a Gröbner bases with respect to the lexicographical order we can solve the system. We obtain an empty set in the second case, and a degree 4 equation over $\mathbb{Q}$ for p_1 in the first case. However, this degree 4 polynomial turns out to be irreducible over $\mathbb{Q}$ with Galois group D_4, hence $p_1 \notin K$, a contradiction.

Now assume $G = A$. Then $T = (2, 6, 4)$. The corresponding triple is rationally rigid and σ_2 has a single cycle of length 6, so there exists a rational function $g(Z)$ with the required ramification data. Still, we need to decide about the fiber $g^{-1}(\infty)$. We do this by explicitly computing g, getting $g(Z) = \frac{Z^6(9Z^2-6Z+49)}{(Z^2+7)^4}$. So the fiber $g^{-1}(\infty)$ is not real, contrary to our requirement.

Let $n = 10$. Then $S \le A \le \mathrm{Aut}(S)$ with $S = \mathcal{A}_5$ or $S = \mathcal{A}_6$. In view of the results we want to achieve, there is little interest in investigating these cases more closely.

Finally, we have to rule out the case $n = 12$, $G = A = \mathrm{M}_{12}$. We have the following possibilities for T: $(2, 5, 6)$, $(3, 4, 6)$, $(3, 3, 6)$, $(4, 4, 6)$, $(2, 6, 6)$, $(2, 8, 6)$, and $(2, 2, 2, 6)$.

In the cases with three branch points, explicit computations are feasible, and it turns out that only the two cases $(3, 3, 6)$ and $(4, 4, 6)$ give Galois realizations over

$\mathbb{Q}(t)$. However, in both cases the subfields of degree 12 over $\mathbb{Q}(t)$ are not rational. Indeed, in the first case, we get the function field of the quadratic $X^2 + Y^2 + 1 = 0$, and in the second case, the function field of the quadratic $X^2 + 3Y^2 + 5 = 0$. In Section 5.3 we give explicit polynomials over $\mathbb{Q}(t)$ of degree 12 with Galois group M_{12} and ramification type $(3, 3, 6)$ or $(4, 4, 6)$, respectively. However, a variation of the argument below could be used as an alternative.

So we need to worry about the ramification type $T = (2, 2, 2, 6)$. The criterion in Lemma 5.1 is too coarse in order to rule out that case. However, we still get rid of this case by considering the action of complex conjugation, and what it does to a genus 0 system. Let $\mathcal{E}$ be a genus 0 system of type T, and suppose that a function $g(Z)$ exists as required. By passing to a real field k containing $g^{-1}(\infty)$, we may assume that $g(Z) = h(Z)/Z^6$, where $h[Z] \in k[Z]$ is a monic polynomial of degree 12 and $h(0) \neq 0$. If $h(0) < 0$, then $h(Z) - t_0 Z^6$ has exactly 2 real roots for $t_0 \ll 0$ (by a straightforward exercise in calculus). However, M_{12} does not have an involution with only 2 fixed points, so this case cannot occur.

Thus $h(0) > 0$. Then, for $t_0 \gg 0$, $h(Z) - t_0 Z^6$ has precisely 4 real roots. Choose such a $t_0 \in k$ with $\mathrm{Gal}(h(Z) - t_0 Z^6/k) = \mathrm{M}_{12}$. By a linear fractional change over k, we can arrange the following: t_0 is mapped to $\tilde{t}_0$, the branch points of the corresponding rational function $\tilde{g}$ are all finite, and the real branch points of $\tilde{g}$ are smaller than $\tilde{t}_0$. Let $\tilde{t}_0$ be the base point of a branch cycle description $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ coming from the "standard configuration" as in [43, Sect. I.1.1] or [16, Section 2]. Note that the order of the conjugacy classes here must *not* be chosen arbitrarily. So the element of order 6 is one of the σ_i. As $k \subset \mathbb{R}$, complex conjugation ρ leaves the set of branch points invariant, but reflects the paths at the real axis, inducing a new branch cycle description σ^ρ. For instance, if all branch points are real, we get

$$\sigma^\rho = \left(\sigma_1^{-1}, (\sigma_2^{-1})^{\sigma_1^{-1}}, (\sigma_3^{-1})^{\sigma_2^{-1}\sigma_1^{-1}}, (\sigma_4^{-1})^{\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}}\right),$$

and a similar transformation formula holds if there is a pair of complex conjugate branch points. For this old result by Hurwitz, see [43, Theorem I.1.2], [16].

Identify the Galois group $\mathrm{Gal}(\tilde{g}(Z) - \tilde{t}/k(\tilde{t}))$ with $\mathrm{Gal}(\tilde{g}(Z) - \tilde{t}_0/k)$, so that they are permutation equivalent on the roots of $\tilde{g}(Z) - \tilde{t}$ and $\tilde{g}(Z) - \tilde{t}_0$, respectively. Let ψ be the complex conjugation on the splitting field of $\tilde{g}(Z) - \tilde{t}_0$. Then, under this identification, $\sigma^\psi = \sigma^\rho$. (Here σ^ψ means simultaneously conjugating the components with ψ.) This is a result by Dèbes and Fried, extending a more special result by Serre [55, 8.4.3] (which does not apply here), see [16] and [43, Theorem I.10.3].

Now, for instance using GAP, one checks that in all possible configurations for σ and possibilities of real and complex branch points, an element ψ as above either does not exist, or is a fixed point free involution. However, as we have chosen $\tilde{t}_0$ such that $\tilde{g}(Z) - \tilde{t}_0$ has precisely 4 real roots, the case that ψ has precisely 4 fixed points should also occur. As this is not the case, we have ruled out the existence of M_{12} with this specific arithmetic data.

5.3. Computations

This section completes the proof of Theorem 5.2 in those cases which require or deserve some explicit computations besides theoretical arguments. We continue to use the notation from there.

5.3.1. $n = 8$, $G = \mathrm{AGL}_3(2)$.

Here $n = 8$, and $G = A = \mathrm{AGL}_3(2)$. We have already seen that the only possible ramification types could be $T = (2, 2, 2, 2, 4)$, $(2, 2, 4, 4)$, and $(2, 2, 3, 4)$. We will establish examples for all three cases. While deriving possible forms of $g(Z)$ we do not give complete justification for each step, because the required properties of $g(Z)$ can be verified directly from the explicit form. Thus the description of the computation is only meant as a hint to the reader how we got the examples.

In the construction of examples we employ a 2–parametric family of polynomials of degree 7 over $\mathbb{Q}(t)$ with a $(2, 2, 2, 2, 4)$ ramification type and Galois group $\mathrm{PSL}_2(7)$. This family is due to Malle, see [42]. Define

$$f_{\alpha,\beta}(X) := \frac{(X^3 + 2(\beta - 1)X^2 + (\alpha + \beta^2 - 4\beta)X - 2\alpha)}{X^2(X-2)} \cdot (X^4 - 2(\beta + 2)X^2 + 4\beta X - \alpha).$$

One verifies that for all $(\alpha, \beta) \in \mathbb{Q}^2$ in a non–trivial Zariski open subset of $\mathbb{Q}^2$, the following holds: $f_{\alpha,\beta}$ has arithmetic and geometric monodromy group $\mathrm{PSL}_2(7)$ with ramification type $(2, 2, 2, 2, 4)$. The elements of order 2 are double transpositions, while the element of order 4 has type $1 - 2 - 4$. We take the composition $f_{\alpha,\beta}(r(X))$, where $r \in \mathbb{Q}(X)$ has degree 2, and is ramified in 0 and 1. Multiplying r with a suitable constant (depending on α and β), one can arrange that the discriminant of the numerator of $f_{\alpha,\beta}(r(X)) - t$ is a square. This can be used to show that the arithmetic and geometric monodromy group of $f_{\alpha,\beta}(r(X))$ is $\mathrm{AGL}_3(2)$ in the degree 14 action. One can now pass to the fixed field E of $\mathrm{GL}_3(2) < \mathrm{AGL}_3(2)$ in a splitting field L of $f_{\alpha,\beta}(r(X)) - t$ over $\mathbb{Q}(t)$. A minimal polynomial $F_{\alpha,\beta}(X, t)$ for a primitive element of $E/\mathbb{Q}(t)$ can be computed, we do not print it here because it is very long. For that we used a program written by Cuntz based on KASH [10] which computes subfields in algebraic function fields.

It turns out that the degree in t of $F_{\alpha,\beta}(X, t)$ is 2. So we can easily derive a condition for the genus 0 field E to be rational. In this case, we get that E is rational if and only if $-\alpha$ is a sum of two squares in $\mathbb{Q}$. For instance, the choice $\alpha := -1/2$, $\beta = 1$ yields

$$g(Z) = \frac{(13Z^4 + 60Z^3 + 100Z^2 + 72Z + 20)(11Z^4 + 8Z^3 - 12Z^2 - 16Z + 12)}{(Z^2 - 2)^4}.$$

Next we want to see how to get the cases with 4 branch points. Let $\Delta_{\alpha,\beta}(t)$ be the discriminant of a numerator of $f_{\alpha,\beta} - t$ with respect to X. A necessary condition for having only 4 branch points is that the discriminant of $\Delta_{\alpha,\beta}(t)$ with respect to t vanishes. This gives a condition on α and β, and if one performs the computation, it follows that this condition is given by the union of two genus 0 curves which are birationally isomorphic to $\mathbb{P}^1(\mathbb{Q})$ over $\mathbb{Q}$. For the computation of such a birational map, we made use of the Maple package `algcurves` by Mark van Hoeij (available at http://klein.math.fsu.edu/~hoeij, also implemented in Maple V Release 5).

An example for the ramification type (2, 2, 4, 4) is

$$g(Z) = \frac{(3Z^2 - 15Z + 20)Z^2}{(Z^2 - 5)^4},$$

whereas

$$g(Z) = \frac{(11Z^2 + 30Z + 18)(3Z^2 + 30Z - 46)^3}{(Z^2 - 2)^4}$$

is an example of ramification type (2, 2, 3, 4).

5.3.2. $n = 16$, $G = (\mathcal{S}_4 \times \mathcal{S}_4) \rtimes C_2$

Here $n = 16$, and $G = A = (\mathcal{S}_4 \rtimes \mathcal{S}_4) \rtimes C_2$ in product action of the wreath product $\mathcal{S}_4 \wr C_2$. First suppose that $\mathcal{E}$ has type (2, 6, 8). There are two such possibilities, both being rationally rigid. The first has fine type $(2-2-2-2, 3-6-6, 8-8)$, and the second one has fine type $(2-2-2-2-2-2, 2-3-3-6, 8-8)$. From this we can already read off that there is a rational function $g(Z) \in \mathbb{Q}(Z)$ of degree 16 and the ramification data and monodromy groups given as above. Let σ_3 correspond to the place at infinity. One verifies that the centralizer $C_A(\sigma_3)$ is intransitive, so $g^{-1}(\infty) \subset K \cup \{\infty\}$, where K is a quadratic subfield of $\mathbb{Q}(\zeta_8)$, so $K = \mathbb{Q}(\sqrt{-1})$, $K = \mathbb{Q}(\sqrt{-2})$, or $K = \mathbb{Q}(\sqrt{2})$. The first two possibilities cannot hold, because complex conjugation would yield an involution in A, which inverts σ_3, and interchanges the two cycles of σ_3. One verifies that such an element does not exist. Let $\tilde{D}$ be the normalizer in A of $I := <\sigma_3>$. Then $\tilde{D}$ contains a decomposition group D of a place of L lying above the infinite place of $\mathbb{Q}(t)$. Also, $[D : I] \geq 4$ by rationality of σ_3. On the other hand, $[\tilde{D} : I] = 4$. Thus $D = \tilde{D}$. But $\tilde{D}$ interchanges the two cycles of σ_3, so the elements in $g^{-1}(\infty)$ cannot be rational. This establishes the existence of g of the required type.

In this situation, we were lucky that theoretical arguments gave a positive existence result. However, it is also quite amusing to take advantage of the specific form of A and compute an explicit example from the data given here.

Recall that $G = A = \mathcal{S}_4 \wr C_2$ is in product action. To this wreath product there belongs a subgroup U of index 8, which is a point stabilizer corresponding to the natural imprimitive action of A. The fine types of the two (2, 6, 8)–tuples with respect to this degree 8 action are $(2, 2-6, 8)$ and $(2-2-2-2, 2-3, 8)$, respectively. One verifies immediately that L_U is a rational field, indeed $L_U = \mathbb{Q}(x)$, where $t = h(x)^2$ with $h \in \mathbb{Q}[X]$. The idea is to compute this field, and then extract from that the degree 16 extension we are looking for.

In the first case, we may assume h of the form $h(X) = X^3(X-1)$, whereas $h(X) = X^3(X-8) + 216$ (note that $h(X) + 216 = (X-6)^2(X^4 + 4X + 12)$) in the second case.

We have $h(x)^2 = t$. Set $y := h(x)$, and let x' be a root of $h(X) = -y$. Then also $h(x')^2 = t$. However, $x + x'$ is fixed under a suitable point stabilizer of A with respect to the degree 16 action of the wreath product $\mathcal{S}_4 \wr C_2$ in power action.

Take the first possibility for h. Using resultants, one immediately computes a minimal polynomial $H(W,t)$ of $w := x + x'$ over $\mathbb{Q}(t)$:

$$\begin{aligned} H(W,t) = {} & W^{16} - 8W^{15} + 27W^{14} - 50W^{13} + 55W^{12} - 36W^{11} + 13W^{10} - 2W^9 \\ & +136tW^8 - 544tW^7 + 892tW^6 - 744tW^5 + 315tW^4 - 54tW^3 + 16t^2. \end{aligned}$$

Here, however, t appears quadratic, so this does not immediately yield the function g we are looking for. However, it is easy to write down a parametrization for the curve $H(W,t) = 0$:

$$\begin{aligned} W &= \frac{Z(2Z+3)}{Z^2-2} \\ t &= -\frac{1}{16}\frac{Z^6(Z+2)^6(2Z+3)^3}{(Z^2-2)^8} =: g(Z). \end{aligned}$$

The function $g(Z)$ parameterizing t is the function we are looking for.

Similarly, the second possibility of h gives a function

$$g(Z) = \frac{(Z^2+4Z+6)(Z-2)^2(3Z^2-4Z+2)^3}{(Z^2-2)^8}.$$

By Theorem 4.8, there is, for this setup, also the possibility of a (2, 2, 2, 8) system. This is no longer rigid. But even if we could show, for instance using a braid rigidity criterion as in [43, Chapt. III], the existence of a regular Galois extension $L/\mathbb{Q}(t)$ with the correct data, we would not be able to decide about rationality of the degree 16 subfield we are after. However, the following computations will display and solve the problem.

With $s \in \mathbb{Q}$ arbitrary set $h(X) := X^4 + 2sX^2 + (8s+32)X + s^2 - 4s - 24$. One verifies that the splitting field of $h(X)^2 - t$ over $\mathbb{Q}(t)$ is regular with Galois group A, and that we have the ramification given by the (2, 2, 2, 8) system, provided that $s \notin -4, -3, -12$. (The cases $s = -3$ and $s = -12$ give the first and second possibilities from above, whereas for $s = -4$ the monodromy group of h is D_4 rather than $\mathcal{S}_4$.) Again, let x be with $h(x)^2 = t$, and x' be with $h(x') = -h(x)$. As above, derive a minimal polynomial $H(W,t)$ for $x + x'$ over $\mathbb{Q}(t)$. One calculates that the curve $H(W,t) = 0$ is birationally isomorphic to the quadratic $U^2 - 2V^2 = 4s + 16$. Of course, it depends on s whether this quadratic has a rational point, which in turn is equivalent that L_U (U from above) is a rational function field. But if one chooses s such that $4s + 16 = u_0^2 - 2v_0^2$ for $u_0, v_0 \in \mathbb{Q}$, then L_U is rational, and from the explicit choice of a rational point on the quadratic we get $g(Z)$, parametrized by (u_0, v_0), where two such pairs give the same function if $u_0^2 - 2v_0^2 = {u'_0}^2 - 2{v'_0}^2$. Up to the details which are routine, this shows that the ramification type (2, 2, 2, 8) appears as well.

5.3.3. $n = 16$, $G = C_2^4 \rtimes \mathcal{S}_5$

Now $G = A = C_2^4 \rtimes \mathcal{S}_5$, where the action of $\mathcal{S}_5$ is on the $\mathcal{S}_5$–invariant hyperplane of the natural permutation module for $\mathcal{S}_5$ over $\mathbb{F}_2$. We verify that the genus 0 systems of type (2, 5, 8) and (2, 6, 8) are rationally rigid, also, it follows from the ramification type, that the degree 16 field we are looking for is rational. As in the previous case, we can recognize the decomposition group (belonging to the inertia group $I := <\sigma_3>$) as the normalizer of I in A, and from the properties of $N_A(I)$ we can read off, exactly as in the previous case, that $g(Z) = h(Z)/(Z^2-2)^8$ exists as required.

Explicit computation is different from the previous case. Suppose we have the ramification type (2, 5, 8). As an abstract group, $A = V \rtimes \mathcal{S}_5$, where $V < \mathbb{F}_2^5$ is the hyperplane of vectors with coordinate sum 0, and $\mathcal{S}_5$ permutes the coordinates naturally. This interpretation of A as a subgroup of the wreath product $C_2 \wr \mathcal{S}_5$ gives an imprimitive faithful degree 10 action of A. Let U be the corresponding subgroup of index 10. One verifies that L_U is the root field of $h(X^2) - t$, where $h(Y) = (Y-1)^5/Y$. Let y_i be the roots of $h(Y) - t$, $i = 1, \dots, 5$, and for each i, let x_i be a square root of y_i. Set $w = x_1 + x_2 + \cdots + x_5$. We compute a minimal polynomial $H(W, t)$ for w. Namely consider $H(W, t) := \prod(X + \epsilon_1 x_1 + \epsilon_2 x_2 + \cdots + \epsilon_5 x_5)$, where the product is over $\epsilon_i \in \{-1, 1\}$, such that the sum of the entries for each occurring tuple is 0. Obviously, $H(w, t) = 0$, and $H(W, t) \in \mathbb{Q}[W, t]$. As to the practical computation, we computed the solutions of $h(X) - t$ in Laurent series in $1/t^{1/5}$ around the place with inertia group order 5. Eventually, after calculations similar as above, we get

$$g(Z) = \frac{(Z-1)(Z^2+Z-1)^5}{(Z^2-2)^8}.$$

If the ramification type is (2, 6, 8), then L is the splitting field of $h(X^2) - t$, with $h(Y) = (2Y^2 - 27)^2(Y^2-1)^3/Y^2$, and after similar computations we get

$$g(Z) = \frac{(5Z^2+4Z-10)(Z+2)^2(5Z^2-12Z+6)^3}{(Z^2-2)^8}.$$

Also, the case (2, 2, 2, 8) is not hard to establish by the procedure described above. An example (as part of a 1–parameter family) is

$$g(Z) = \frac{(15Z^4 - 74Z^3 + 140Z^2 - 124Z + 44)^2}{(Z^2-2)^8} \cdot (47Z^8 - 472Z^7 + 1912Z^6 - 4272Z^5 + 4840Z^4 - 1824Z^3 - 288Z^2 - 64Z - 16).$$

5.3.4. $n = 12, G = \mathrm{M}_{12}$

In order to rule out the ramification types $T = (3, 3, 6)$ and $(4, 4, 6)$, we computed explicitly polynomials $F(X, t)$ of degree 12 over $\mathbb{Q}(t)$, such that the splitting field L has Galois group M_{12} over $\mathbb{Q}(t)$, and the ramification type T. From the explicit form of $F(X, t)$ we can read off that a degree 12 extension E in L of $\mathbb{Q}(t)$ cannot be a rational field. Nowadays such computations are routine, so we just give the polynomials.

For $T = (3, 3, 6)$ we obtain

$$\begin{aligned} F(X,t) = {} & X^{12} + 396X^{10} + 27192X^9 + 933174X^8 + 20101752X^7 \\ & + (-2t + 169737744)X^6 + 16330240872X^5 \\ & + (8820t + 538400028969)X^4 + (92616t + 8234002812376)X^3 \\ & + (-3895314t + 195276967064388)X^2 \\ & + (-48378792t + 3991355037576144)X \\ & + t^2 + 62267644t + 30911476378259268, \end{aligned}$$

and for $T = (4, 4, 6)$ we get

$$\begin{aligned} F(X,t) = {} & X^{12} + 44088X^{10} + 950400X^9 + 721955520X^8 \\ & + 31696106112X^7 + (2t + 5460734649920)X^6 \\ & + 393700011065856X^5 \\ & + (-120180t + 20231483772508800)X^4 \\ & + (-2587680t + 911284967252689920)X^3 \\ & + (137561760t + 21295725373309787136)X^2 \\ & + (4418468352t + 183784500436675461120)X \\ & + t^2 + 31440107840t + 303366600120148209356 8. \end{aligned}$$

As t is quadratic in both cases, it is easy to compute a quadratic Q such that E is the field of rational functions on Q. Then E is rational if and only if Q has a rational point. However, in both cases there is not even a real point on Q. This actually indicates that the argument we used to exclude $T = (2, 2, 2, 6)$ might be applicable here as well. One can verify that this is indeed the case.

6. Applications to Hilbert's irreducibility theorem

Immediate consequences of Theorems 4.8, 4.9, 5.2, and 5.3 are

Theorem 6.1. *Let k be a field of characteristic 0, and $g(Z) \in k(Z)$ a rational function with the Siegel property. Then each non-Abelian composition factor of* $\mathrm{Gal}(g(Z) - t/k(t))$ *is isomorphic to one of the following groups:* $\mathcal{A}_j$ $(j \geq 5)$, $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(8)$, $\mathrm{PSL}_2(11)$, $\mathrm{PSL}_2(13)$, $\mathrm{PSL}_3(3)$, $\mathrm{PSL}_3(4)$, $\mathrm{PSL}_4(3)$, $\mathrm{PSL}_5(2)$, $\mathrm{PSL}_6(2)$, M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

Theorem 6.2. *Let $g(Z) \in \mathbb{Q}(Z)$ be a Siegel function over $\mathbb{Q}$. Then each non-Abelian composition factor of* $\mathrm{Gal}(g(Z) - t/\mathbb{Q}(t))$ *is isomorphic to one of the following groups:* $\mathcal{A}_j$ $(j \geq 5)$, $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(8)$.

Theorem 6.3. *Let $g(Z) \in \mathbb{Q}(Z)$ be a Siegel function over $\mathbb{Q}$. Assume that $A =$* $\mathrm{Gal}(g(Z) - t/\mathbb{Q}(t))$ *is a simple group. Then A is isomorphic to an alternating group or C_2.*

In [48] we showed that this latter theorem implies the following:

Corollary 6.4. *Let $f(t, X) \in \mathbb{Q}(t)[X]$ be irreducible with Galois group G, where G is a simple group not isomorphic to an alternating group or C_2.*
Then $\mathrm{Gal}(f(\bar{t}, X)/\mathbb{Q}) = G$ *for all but finitely many specializations $\bar{t} \in \mathbb{Z}$.*

Similarly, Theorems 6.1 and 6.2 have the following application to Hilbert's irreducibility theorem. See [48], where we also have results of this kind which do not rely on group-theoretic classification results.

Corollary 6.5. *Let $f(t, X) \in \mathbb{Q}(t)[X]$ be irreducible, and assume that the Galois group of $f(t, X)$ over $\mathbb{Q}(t)$ acts primitively on the roots of $f(t, X)$ and has a non-Abelian composition factor which is not alternating and not isomorphic to* $\mathrm{PSL}_2(7)$ *or* $\mathrm{PSL}_2(8)$. *Then $f(\bar{t}, X)$ remains irreducible for all but finitely many $\bar{t} \in \mathbb{Z}$.*

Corollary 6.6. *Let k be a finitely generated field of characteristic* 0, *and R a finitely generated subring of k. Let $f(t, X) \in k(t)[X]$ be irreducible, and assume that the Galois group of $f(t, X)$ over $k(t)$ acts primitively on the roots of $f(t, X)$ and has a non-Abelian composition factor which is not alternating and is not isomorphic to one of the following groups:* $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(8)$, $\mathrm{PSL}_2(11)$, $\mathrm{PSL}_2(13)$, $\mathrm{PSL}_3(3)$, $\mathrm{PSL}_3(4)$, $\mathrm{PSL}_4(3)$, $\mathrm{PSL}_5(2)$, $\mathrm{PSL}_6(2)$, M_{11}, M_{12}, M_{22}, M_{23}, M_{24}. *Then $f(\bar{t}, X)$ remains irreducible for all but finitely many $\bar{t} \in R$.*

References

[1] M. ASCHBACHER and L. SCOTT, *Maximal subgroups of finite groups*, J. Algebra **92** (1985), 44–88.

[2] A. BOCHERT, *Über die Zahl verschiedener Werte, die eine Funktion gegebener Buchstaben durch Vertauschung derselben erlangen kann*. Math. Ann. **33** (1889), 584–590.

[3] W. BOSMA, J. CANNON and C. PLAYOUST, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[4] P. J. CAMERON, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), 1–22.

[5] P. J. CAMERON and W. M. KANTOR, *Antiflag–transitive collineation groups revisited*, Incomplete draft, www.maths.qmul.ac.uk/~pjc/odds/antiflag.pdf.

[6] P. J. CAMERON and W. M. KANTOR, *2–transitive and antiflag transitive collineation groups of finite projective spaces*, J. Algebra **60** (1979), 384–422.

[7] R. W. CARTER, *Conjugacy classes in the Weyl group*, In: "Seminar on Algebraic Groups and Related Finite Groups", A. Borel, R. Carter, C. W. Curtis *et al.* (eds.), Vol. 131, Lecture Notes in Mathematics, Springer–Verlag, Berlin, Heidelberg, G1–G22.

[8] R. W. CARTER, "Simple Groups of Lie Type". Wiley and Sons, London, 1972.

[9] J. H. CONWAY, R. T. CURTIS, S. P. NORTON, R. A. PARKER and R. A. WILSON, "Atlas of Finite Groups", Oxford University Press, Eynsham, 1985.

[10] M. DABERKOW, C. FIEKER, J. KLÜNERS, M. POHST, K. ROEGNER, S. M. and K. WILDANGER, *KANT V4*, J. Symb. Comput. **24** (1996), 267–283.

[11] J. D. DIXON and B. MORTIMER, "Permutation Groups", Springer-Verlag, New York, 1996.

[12] W. FEIT, *On symmetric balanced incomplete block designs with doubly transitive automorphism groups*, J. Combinatorial Theory Ser. A **14** (1973), 221–247.

[13] W. FEIT, *Some consequences of the classification of finite simple groups*, In: "The Santa Cruz Conference on Finite Groups", Vol. 37 of Proc. Sympos. Pure Math., Amer. Math. Soc., Providence, Rhode Island (1980), 175–181.

[14] W. FEIT, R. LYNDON and L. L. SCOTT, *A remark about permutations*, J. Combinatorial Theory Ser. A **18** (1975), 234–235.

[15] M. FRIED, *Exposition on an arithmetic–group-theoretic connection via Riemann's existence theorem*, In: "The Santa Cruz Conference on Finite Groups", Vol. 37 of *Proc. Sympos. Pure Math*. Amer. Math. Soc., Providence, Rhode Island (1980), 571–602.

[16] M. FRIED and P. DÈBES, *Rigidity and real residue class fields*, Acta Arith. **56** (1990), 291–323.

[17] THE GAP GROUP, GAP – Groups, Algorithms, and Programming, Version 4.4.12 (2008). URL `http://www.gap-system.org`.

[18] D. GORENSTEIN, "Finite Groups". Harper and Row, New York–Evanston–London, 1968.

[19] R. GURALNICK, *Monodromy groups of coverings of curves*, In: "Galois Groups and Fundamental Groups", Vol. 41 of Math. Sci. Res. Inst. Publ., Cambridge Univ. Press, Cambridge (2003), pages 1–46.

[20] R. M. GURALNICK and J. G. THOMPSON, *Finite groups of genus zero*, J. Algebra **131** (1990), 303–341.

[21] C. HERING, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order*, Geom. Dedicata **2** (1974), 425–460.

[22] D. G. HIGMAN, *Finite permutation groups of rank* 3. Math. Z. **86** (1964), 145–156.

[23] B. HUPPERT, "Endliche Gruppen I", Springer–Verlag, Berlin Heidelberg, 1967.

[24] B. HUPPERT and N. BLACKBURN, "Finite Groups III", Springer–Verlag, Berlin Heidelberg, 1982.

[25] G. A. JONES, *Cyclic regular subgroups of primitive permutation groups*, J. Group Theory **5** (2002), 403–407.

[26] G. A. JONES and A. ZVONKIN, *Orbits of braid groups on cacti*. Mosc. Math. J. **2** (2002), 127–160, 200.

[27] W. M. KANTOR, *Linear groups containing a Singer cycle*. J. Algebra **62** (1980), 232–234.

[28] P. KLEIDMAN, *The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, of the Ree groups ${}^2G_2(q)$, and of their automorphism groups*, J. Algebra **117** (1988), 30–71.

[29] P. KLEIDMAN, *The maximal subgroups of the Steinberg triality groups ${}^3D_4(q)$ and of their automorphism groups*. J. Algebra **115** (1988), 182–199.

[30] P. KLEIDMAN and M. W. LIEBECK, "The Subgroup Structure of the Finite Classical Groups", Cambridge University Press, Cambridge, 1990.

[31] P. KLEIDMAN, R. A. PARKER and R. A. WILSON, *The maximal subgroups of the Fischer group Fi_{23}*. J. London Math. Soc. **39** (1989), 89–101.

[32] P. KLEIDMAN and R. A. WILSON, *The maximal subgroups of Fi_{22}*, Math. Proc. Cambridge Philos. Soc. **102** (1987), 17–23.

[33] P. KLEIDMAN and R. A. WILSON, *The maximal subgroups of J_4*, Proc. London Math. Soc. **56** (1988), 484–510.

[34] E. LANDAU, "Handbuch der Lehre von der Verteilung der Primzahlen", Teubner, Leipzig (1909), Second edition by Chelsea, New York, 1953.

[35] V. LANDAZURI and G. M. SEITZ, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra **32** (1974), 418–443.

[36] S. LANG, "Fundamentals of Diophantine Geometry", Springer–Verlag, New York, 1983.

[37] M. W. LIEBECK, C. E. PRAEGER and J. SAXL, *On the O'Nan–Scott theorem for finite primitive permutation groups*, J. Austral. Math. Soc. Ser. A **44** (1988), 389–396.

[38] M. W. LIEBECK and J. SAXL, *On the orders of maximal subgroups of the finite exceptional groups of Lie type*, Proc. London Math. Soc. **55** (1987), 299–330.
[39] S. LINTON, *The maximal subgroups of the Thompson group*, J. London Math. Soc. **39** (1989), 79–88.
[40] K. MAGAARD, S. SHPECTOROV and G. WANG, *Generating sets of affine groups of low genus* (2011), arXiv:1108.4833.
[41] G. MALLE, *Fields of definition of some three point ramified field extensions*, In: "The Grothendieck theory of dessins d'enfants", L. Schneps (ed.), London Math. Soc. Lecture Note Ser. **200**, Cambridge Univ. Press (1984), 147–168.
[42] G. MALLE, *Multi-parameter polynomials with given Galois group. Algorithmic methods in Galois theory*, J. Symbolic Comput. **30** (2000), 717–731.
[43] G. MALLE and B. H. MATZAT, "Inverse Galois Theory", Springer Verlag, Berlin, 1999.
[44] J. MCLAUGHLIN, *Some subgroups of $SL_n(\mathbb{F}_2)$*. Illinois J. Math. **13** (1969), 108–115.
[45] P. MÜLLER, *Primitive monodromy groups of polynomials*, In: "Recent developments in the inverse Galois problem", M. Fried (ed.), Contemp. Math., Amer. Math. Soc. **186** (1995), 385–401.
[46] P. MÜLLER, *Reducibility behavior of polynomials with varying coefficients*, Israel J. Math. **94** (1996), 59–91.
[47] P. MÜLLER, *Kronecker conjugacy of polynomials*, Trans. Amer. Math. Soc. **350** (1998), 1823–1850.
[48] P. MÜLLER, *Finiteness results for Hilbert's irreducibility theorem*, Ann. Inst. Fourier Grenoble **52** (2002), 983–1015.
[49] P. MÜLLER and H. VÖLKLEIN, *On a question of Davenport*, J. Number Theory **58** (1996), 46–54.
[50] M. NEUBAUER, *On primitive monodromy groups of genus zero and one, I*, Comm. Algebra **21** (1993), 711–746.
[51] R. REE, *A theorem on permutations*, J. Combinatorial Theory Ser. A **10** (1971), 174–175.
[52] L. SCOTT, *Matrices and cohomology*, Anal. Math. **105** (1977), 473–492.
[53] L. SCOTT, *Representations in characteristic p*, In: "The Santa Cruz Conference on Finite Groups", Proc. Sympos. Pure Math., Amer. Math. Soc., Providence, R. I., **37** (1980), 319–331.
[54] L. L. SCOTT, *On the n, $2n$ problem of Michael Fried*, In: "Proceedings of the Conference on Finite Groups", Academic Press (1975), 471–475.
[55] J.-P. SERRE, "Topics in Galois Theory". Jones and Bartlett, Boston, 1992.
[56] C. L. SIEGEL, *Über einige Anwendungen diophantischer Approximationen*, Abh. Pr. Akad. Wiss. **1** (1929), 41–69. (=Ges. Abh., I, 209–266).
[57] R. STEINBERG, "Endomorphisms of Linear Algebraic Groups", Memoirs of the American Mathematical Society, No. 80. American Mathematical Society, Providence, R.I., 1968.
[58] P. H. TIEP and A. E. ZALESSKII, *Minimal characters of the finite classical groups*, Comm. Algebra **24** (1996), 2093–2167.
[59] H. VÖLKLEIN, "Groups as Galois Groups – an Introduction", Cambridge University Press, New York, 1996.
[60] A. WAGNER, *The faithful linear representation of least degree of S_n and A_n over a field of characteristic* 2, Math. Z. **151** (1976), 127–137.
[61] H. WIELANDT, *Primitive Permutationsgruppen vom Grad $2p$*, Math. Z. **63** (1956), 478–485.
[62] H. WIELANDT, "Finite Permutation Groups". Academic Press, New York London, 1964.

Institut für Mathematik
Universität Würzburg
Campus Hubland Nord
97074 Würzburg, Germany
peter.mueller@mathematik.uni-wuerzburg.de