HABILITATIONSSCHRIFT

eingereicht bei der
Fakultät für Mathematik
der
Ruprecht–Karls–Universität
Heidelberg

Vorgelegt von
Dr. rer. nat. Peter Müller
aus Nürnberg
1999

Cofinite Integral Hilbert Sets

Preface

0.1 Hilbertian Fields

In 1892, D. Hilbert obtained the following basic result, which along with certain generalizations is nowadays called Hilbert's irreducibility theorem.

Theorem 0.1.1 ([30]). *Let $f(X,t) \in \mathbb{Q}[X,t]$ be an irreducible polynomial. Then $f(X,t_0)$ is irreducible for infinitely many integers $t_0 \in \mathbb{Z}$.*

Hilbert's original proof has been simplified subsequently, see for instance [71, I.1] for a modern version based on a later proof by Dörge. There are also more algebraic proofs by Eichler and Fried, based on reduction of the polynomial modulo various primes, see [15], [20, Section 3]. However, also these proofs rely on analytic techniques, as they use Chebotarëv's density theorem or the Weil bounds for the number of points on curves over finite fields. To my knowledge, no purely algebraic proof of Hilbert's irreducibility theorem is known to date.

There are well–known extensions of Hilbert's irreducibility theorem, for instance the variables X and t can be replaced by tuples of variables X_i and t_j, where we specialize the t_j. Additionally, one can consider finite sets of polynomials, and require that they are simultaneously irreducible for infinitely many specializations of the t_j. Also, one can replace $\mathbb{Q}$ by a field finitely generated over $\mathbb{Q}$. These extensions involve only minor new ideas, so the basic version of interest is as stated above.

Hilbert's irreducibility theorem has many important applications in arithmetic geometry and number theory. For instance, if L is a regular finite Galois extension of the rational field $\mathbb{Q}(t)$ (i. e., $\mathbb{Q}$ is algebraically closed in L) with group $G \neq 1$, then there are infinitely many mutually non–isomorphic Galois extensions of $\mathbb{Q}$ with group G. Similarly as in the inverse problem of Galois theory, one frequently uses geometric constructions to obtain certain objects

of interest over rational function fields, and afterwards specializes the parameters using Hilbert's irreducibility theorem to get these objects over the rationals – preserving certain properties. An example is the construction of elliptic curves of high rank.

There are other fields k besides those which are finitely generated over $\mathbb{Q}$ for which the statement of Hilbert's irreducibility theorem (with $\mathbb{Z}$ replaced by k) holds, see [24], [44].

0.2 Hilbert Sets over Number Fields

In the following let k be a number field, and $\mathcal{O}_k$ its ring of integers. In [66] Siegel proved the fundamental result that an irreducible algebraic curve over k of positive genus has only finitely many points with coordinates in $\mathcal{O}_k$. He also gave a description of the genus 0 curves which do have infinitely many integral points.

In that work, he already remarked the applicability of this result to Hilbert's irreducibility theorem, indeed one can get the result in a few lines.

If one wants to prove Hilbert's irreducibility theorem only in the form as stated above, then it is however vast overkill to use Siegel's theorem, because the latter is by far deeper and more difficult to prove, see [44], [60]. The latter reference uses a fair amount of nonstandard arguments.

Hilbert's original analytic argument is not suited to give very precise versions of his theorem. The best versions known to date use Siegel's theorem (applied to polynomials associated to, but different from $f(X,t)$). For f as in the theorem, let $\mathcal{R}_f$ be the set of those integers t_0 such that $f(X,t_0)$ is reducible over $\mathbb{Q}$. Then one of the tighter versions asserts that $|\mathcal{R}_f \cap [-n,n]| \leq cn^{1/2}$ for a constant c, and if we put no restriction on f, then this result is optimal in view of the example $f(X,t) = X^2 - t$.

A recent development is the explicit construction of universal Hilbert sets $\mathcal{H}$ (over the rationals). An infinite set $\mathcal{H} \subset \mathbb{Z}$ is called a universal Hilbert set if for any irreducible $f(X,t) \in \mathbb{Q}[X,t]$, there are only finitely many $t_0 \in \mathcal{H}$ with $f(X,t_0)$ reducible. The existence of universal Hilbert sets is easy to show, one uses a set–theoretic diagonal argument and Hilbert's irreducibility theorem for finite families of polynomials (see eg. [24, Chap. 14, Exercise 2]). It is considerably more difficult to construct explicit examples. The first explicit universal Hilbert set had been given by Sprindžuk [67] in 1981 – it looks as ugly as $\{[\exp\sqrt{\log\log m}] + m!2^{m^2} \mid m = 3,4,\dots\}$. Later, simpler

series were found, like $\{2^m + m | \ m = 1, 2, \dots\}$ by Dèbes and Zannier in [13]. The present trend is to find or prove the existence of universal Hilbert sets with good density properties – a recent result is that such sets with asymptotic density 1 do exist. However, no explicit universal Hilbert set of density 1 is known so far. See [2], [13], [74], and the references given there for questions of this kind.

0.3 Finiteness Results

Here we want to follow a different direction. Obviously, a universal Hilbert set cannot be cofinite in $\mathbb{Z}$. However, it turns out that the sets $\mathcal{R}_f$ are finite quite often. A trivial instance for $\mathcal{R}_f$ being infinite is if the polynomial $f(X,t)$ has a linear factor for infinitely many specializations $t \mapsto t_0 \in \mathbb{Z}$. But then (by Siegel's theorem), the curve given by $f(X,t) = 0$ has genus 0. (By the genus of $f(X,t) = 0$ we mean the genus of the field $\mathbb{C}(t,x)$, where x is a root of $f(X,t)$. This is well–defined even if $f(X,t)$ is not absolutely irreducible).

So it seems to be natural to ask for irreducible polynomials $f(X,t) \in \mathbb{Q}[X,t]$, such that the curve given by $f(X,t) = 0$ has positive genus, but where $f(X,t_0)$ is nevertheless reducible for infinitely many $t_0 \in \mathbb{Z}$.

It is very easy to write down such polynomials for each degree $n > 1$ which is *not* a prime, see Example 5.2.2. Surprisingly however, for prime degrees, no such polynomials exist. This was shown in [57], as a precursor of the present work, and is restated in (a) in the theorem below.

In the proof of that fact, we were not able to work in a purely number theoretic context, just using the assumption that $\deg_X(f)$ is a prime. Even though the proof is elementary, we used quite a few group theoretic arguments and results. In turns out that much of the finiteness question is encoded in the Galois group of $f(X,t)$ over $\mathbb{Q}(t)$. For instance, if this group is the alternating or symmetric group in the natural action on the roots of $f(X,t)$, then the finiteness statement holds again, see (b) of the theorem below. This result, which is easier to obtain than (a), is already contained in [57], too.

The present work is an attempt to connect the validity of a finiteness statement to the Galois group of $f(X,t)$. For this we have to invoke much more group theory, arithmetic arguments, and also some explicit computations at several points. In particular, we make frequent use of the classification of the finite simple groups, which is not the case in proving (a) and (b).

We doubt that this can be avoided in order to prove for instance (c) and (d) or Theorem 0.3.2 below.

For simplicity we state a sample result here, see Chapter 5 for more and stronger finiteness results and cases where this fails, and analogues for number fields.

Theorem 0.3.1. *Let $f(X,t) \in \mathbb{Q}[X,t]$ be irreducible, and let A be the Galois group of $f(X,t)$ over $\mathbb{Q}(t)$ in its natural action on the roots of $f(X,t)$. Suppose that $f(X,t) = 0$ has positive genus. Then $f(X,t_0)$ is irreducible for all but finitely many integers $t_0 \in \mathbb{Z}$, if one of the following conditions is fulfilled.*

(a) $\deg_X(f)$ *is a prime.*

(b) A is the alternating or symmetric group in its natural action.

(c) A is a simple group not isomorphic to an alternating group $\mathcal{A}_n$.

(d) A acts primitively, and has a non–abelian composition factor which is not isomorphic to $\mathcal{A}_j$ ($j \geq 5$), $\mathrm{PSL}_2(7)$, or $\mathrm{PSL}_2(8)$.

Part (d) is a strong assertion in the sense that it requires only one of the composition factors of A to be not contained in a very small list. In Example 5.2.8 we show how primitive groups with non–abelian composition factors only among $\mathcal{A}_j$ ($j \geq 5$), $\mathrm{PSL}_2(7)$, or $\mathrm{PSL}_2(8)$ give rise to counter examples. In Remark 5.2.3 we explain why primitivity of A is a reasonable assumption to make.

In (c) and (d) we excluded the infinite series of alternating groups, even though they are no problem in the natural action by part (b). In Example 5.2.7 we give a result showing that we indeed need to exclude alternating groups.

From part (c) of the above theorem (and a little extra argument), we obtain the following result about the preservation of Galois groups.

Theorem 0.3.2. *Let $f(X,t) \in \mathbb{Q}[X,t]$ be irreducible of degree ≥ 3 with Galois group G, where G is a simple group not isomorphic to an alternating group. Then $\mathrm{Gal}(f(X,t_0)/\mathbb{Q}) = G$ for all but finitely many specializations $t_0 \in \mathbb{Z}$.*

Theorem 0.3.2 becomes false if we consider rational specializations $t_0 \in \mathbb{Q}$ rather than integral specializations, see Example 5.2.1.

There are other results about the rareness of exceptional specializations for very specific polynomials. M. Fried investigates polynomials of the form $h(X) - t$, where $h(X) \in \mathbb{Z}[X]$ is functionally indecomposable, and proves in [22] that unless $\deg(h) = 5$, then $h(X) - t_0$ is reducible for $t_0 \in \mathbb{Z}$ only if t_0 is in the value set of h or in a certain finite set. This analysis can be extended to polynomials of the form $h(X) - tX^i$, where i is relatively prime to $\deg(h)$. See [22] for the case $i \neq 1, \deg(h) - 1$, and [55] for the more difficult cases $i = 1$ or $\deg(h) - 1$.

Fried's observation of the applicability of group theoretic methods in the analysis of Hilbert sets inspired this work, where we try to give a reasonably complete investigation of the question when an integral Hilbert set is cofinite in $\mathbb{Z}$ or not.

Using quite different methods, K. Langmann shows cofiniteness of integral Hilbert sets (under certain assumptions) for so-called Thue-polynomials, which are polynomials of the form $H(X,t) - 1$, where $H(X,t) \in \mathbb{Q}[X,t]$ is homogeneous. He also obtains other arithmetic results about integral Hilbert sets. See [45], [46] and his other work quoted there. In the final section of this paper we show how our setup yields various generalizations of Langmann's result about the Thue-polynomial. For this part we hardly use any group theory. In particular, we do not need the difficult Chapters 2 and 3 for this.

0.4 Overview of the Proofs

The main part of the proofs is group–theoretic. We give a rough picture of the proof of Theorem 0.3.1 and its number theoretic analogue. For this let $\mathcal{O}_k$ be the ring of integers of a number field k. If t is a transcendental, and $g(Z) \in k(Z)$ is a non–constant rational function, then terms like splitting field and Galois group of $g(Z) - t$ refer to the corresponding terms of an irreducible numerator of $g(Z) - t$.

Suppose that the irreducible polynomial $f(X,t) \in k[X,t]$ has infinitely many specializations $t_0 \in \mathcal{O}_k$ with $f(X,t_0)$ reducible. Using a well–known reduction argument, which basically goes back to Hilbert, and Siegel's theorem, we get rational functions $g(Z) \in k(Z)$, such that $f(X, g(Z))$ is reducible over $k(Z)$, and $|g(k) \cap \mathcal{O}_k| = \infty$. The last property gives, by another theorem of Siegel, that $|g^{-1}(\infty)| \leq 2$. This implies that the Galois group of $g(Z) - t$ over $k(t)$ contains an element with at most two cycles. Also, we relate this Galois group to the Galois group of $f(X,t)$ over $k(t)$.

Thus we need a good knowledge of permutation groups which contain an element with at most two cycles. In this generality, a classification is hopeless. However, we obtain a complete classification if we assume that the group is primitive. (This reduction to primitive groups corresponds to writing $g(Z)$ as a composition of functionally indecomposable rational functions.) The classification of these groups is achieved in Chapter 2 and comprises the most technical part of this work. If we had only the proof of the stated theorems in mind, we could somewhat simplify the arguments by employing other properties of the Galois group of $g(Z) - t$, like the existence of genus 0 systems (see Chapter 3). However, we believe that the classification of primitive groups with a two–cycle element is of independent interest, so we classify them under no further restrictions. The classification result is in Theorem 2.3.3, page 11.

The proof makes use of a rough distinction of the primitive permutation groups into five classes, given by the Aschbacher–O'Nan–Scott Theorem. Each case requires quite different techniques and kinds of arguments. Only in three of the five cases there are actually examples, namely for the groups in affine, product, or almost simple action. We make heavy use of the classification of the finite simple groups throughout the proof.

In the next stage we classify the possibilities that a two–cycle element of a primitive group is part of a genus 0 system of a normal subgroup of this group. This condition comes from the Riemann–Hurwitz genus formula and the interpretation of $g(Z)$ as a covering map between Riemann spheres, sending z to $g(z)$. See Chapter 3.

If we allow k to be an arbitrary number field, then we are basically finished at this point.

Thus assume that $k = \mathbb{Q}$. The main conditions used so far came from geometric considerations, that is by seeing $g(Z)$ over the complex numbers $\mathbb{C}$. Now we are concerned with the question which of the group–theoretic possibilities indeed come from rational functions $g(Z) \in \mathbb{Q}(Z)$ with the correct arithmetic properties. The proof of actual existence in certain cases uses techniques from the inverse Galois problem (mainly rational rigidity) or explicit computations in a few cases. In most cases where examples do not exist, we rule them out by considering the interplay between inertia and decomposition groups. Again, we will also require some explicit computations to rule out certain candidates. This is the subject of Chapter 4 for the theoretical arguments, and Section 4.4 for the computations.

Chapter 5 eventually states and proves our main results and gives exam-

ples to show that our finiteness results are optimal in a certain sense.

I thank the DFG who supported this work through a Habilitandenstipendium.

Contents

Preface **v**
0.1 Hilbertian Fields v
0.2 Hilbert Sets over Number Fields vi
0.3 Finiteness Results vii
0.4 Overview of the Proofs ix

1 Galois Theoretic Preparation **1**
1.1 Description of Hilbert Sets 1
1.2 Group Theoretic Consequences 3
1.3 Not Absolutely Irreducible Polynomials 5

2 Primitive Groups with a two–cycles Element **7**
2.1 Permutation Groups – Notations, Definitions, and Elementary Results 7
2.2 The Aschbacher–O'Nan–Scott Theorem 9
2.3 Previous Results 10
2.4 Affine Action 12
2.5 Product Action 20
2.6 Regular Action 22
2.7 Diagonal Action 22
2.8 Almost Simple Action 24
2.8.1 Alternating Groups 25
2.8.2 Sporadic Groups 29
2.8.3 Element Orders in Classical Groups 31
2.8.4 Classical Groups 41
2.8.5 Projective Special Linear Groups 48
2.8.6 Exceptional Groups of Lie Type 54
2.8.7 Proof of Theorem 2.8.1 56

2.9 Tables on Minimal Permutation Degrees, Maximal Element Orders, etc. 58

3 Genus 0 Systems **61**
3.1 Branch Cycle Descriptions 61
3.1.1 Algebraic and Topological Description 61
3.1.2 Branch Cycle Descriptions in Permutation Groups . . . 63
3.2 Some General Lemmas about Genus 0 Systems 64
3.3 Genus 0 Systems for Affine Action 68
3.4 Genus 0 Systems for Product Action 71
3.5 Genus 0 Systems for Almost Simple Action 72
3.6 Genus 0 Systems with n–Cycle 81

4 Rationality Questions **83**
4.1 Siegel Functions 83
4.2 A Galois Theoretic Existence Criterion 85
4.3 Monodromy Groups of Siegel Functions 86
4.4 Computations 92
4.4.1 $n = 8$, $G = \mathrm{AGL}_3(2)$. 92
4.4.2 $n = 16$, $G = (S_4 \times S_4) \rtimes C_2$ 93
4.4.3 $n = 16$, $G = C_2^4 \rtimes S_5$ 96
4.4.4 $n = 12$, $G = \mathrm{M}_{12}$ 97
4.5 Davenport Polynomials 98

5 Results, Proofs, and Examples **101**
5.1 Cofiniteness of Hilbert Sets 101
5.2 Failure of Finiteness Property 106
5.3 Thue–Polynomials, on a Result of Langmann 114

Bibliography **117**

List of Tables

2.1 Classical Groups 58
2.2 Exceptional Groups 59
2.3 Sporadic Groups 60

Chapter 1

Galois Theoretic Preparation

1.1 Description of Hilbert Sets

In this section k will denote a number field, and $\mathcal{O}_k$ its ring of integers. The following proposition follows from a variation of the classical reduction argument in the proof of Hilbert's irreducibility theorem (see e.g. [44, Chapter 9]), combined with Siegel' theorem about integral points on algebraic curves. As this proposition is the key for the Galois theoretic investigation of Hilbert sets, we supply a proof. An alternative argument, which also relies on a reduction to Siegel's Theorem, has been given by Fried, see [20].

Proposition 1.1.1. *Let $f(X,t) \in k(t)[X]$ be an irreducible polynomial of positive degree n in X. Let $m \in \{1,2,\ldots,n-1\}$. Set $\mathcal{R}_m := \{t_0 \in \mathcal{O}_k | f(X,t_0)$ is defined and has a factor of degree m over $k\}$. Then there are finitely many non–constant rational functions $g_i(Z) \in k(Z)$ and a finite set $W \subset \mathcal{O}_k$, such that*

$$\mathcal{R}_m \subseteq W \cup \bigcup_i (g_i(k) \cap \mathcal{O}_k)$$

and $f(X, g_i(Z))$ is reducible over $k(Z)$ with a factor of degree m.

Proof. By replacing X and $f(X,t)$ by multiples with elements in $k(t)$, we may assume that $f(X,t) \in \mathcal{O}_k[t,X]$ is monic in X. Let $x_1, x_2, \ldots, x_n$ be the roots of $f(X,t)$ in an algebraic closure of $k(t)$. Let $I \subset \{1,2,\ldots,n\}$ with $1 \leq |I| \leq n-1$, and set

$$f_I(X) := \prod_{i \in I} (X - x_i).$$

Let K_I be the field generated by $k(t)$ and the coefficients of f_I. As f is irreducible, at least one of these coefficients is not in $k(t)$, so $[K_I : k(t)] \geq 2$. Let $\beta_I \in \mathcal{O}_k[t][x_1, x_2, \ldots, x_n]$ be a primitive element of $K_I/k(t)$, and let $P_I(Y,t) \in \mathcal{O}_k[t,Y]$ be the minimal polynomial of β_I over $k(t)$. By definition of K_I, we get that $\beta_I = \sum_j \alpha_j(t)A_j$, where $\alpha_j(t) \in k(t)$ and A_j is a product of coefficients of f_I. Denote by S the union of the k–rational roots of the denominators of all these rational functions α_j, taken for all such index sets I. Denote by $k[t]_S$ the ring of rational functions in $k(t)$ whose denominators have no roots in S.

Now take $t_0 \in \mathcal{R}_m$ such that $f(X,t_0)$ is separable of degree n and $t_0 \notin S$ — this assumption excludes only finitely many elements from $\mathcal{R}_m$. Write $f(X,t_0) = f_1(X)f_2(X)$ with $f_1, f_2 \in \mathcal{O}_k[X]$ and $\deg(f_1) = m$. As $(k[t]_S)[x_1, x_2, \ldots, x_n]$ is integral over $k[t]_S$, the specialization map $t \mapsto t_0$ from $k[t]_S$ to k extends to a k–algebra homomorphism $\omega : (k[t]_S)[x_1, x_2, \ldots, x_n] \to k[\bar{x_1}, \bar{x_2}, \ldots, \bar{x_n}]$, where the $\bar{x_i}$ are the roots of $f(X,t_0)$. Label these roots such that $\omega(x_i) = \bar{x_i}$. Let I be the set of i such that $\bar{x_i}$ is a root of f_1. Denote by $\omega(f_I)$ the polynomial f_I with ω applied to its coefficients. Then $\omega(f_I) = f_1$ and $P_I(\omega(\beta_I), t_0) = 0$. But, by the construction above, β_I is a polynomial over $k[t]_S$ in the coefficients of f_I, hence $\omega(\beta_I) \in k$, and then $\omega(\beta_I) \in \mathcal{O}_k$ because $\omega(\beta_I)$ fulfills an integral equation over $\mathcal{O}_k$. Thus each such t_0 gives rise to an integral point $(\omega(\beta_I), t_0)$ on P_I for some index set I.

Now fix an I which appears infinitely many times. Thus the curve $P_I(Y,t) = 0$ has infinitely many points in $\mathcal{O}_k \times \mathcal{O}_k$. Siegel's Theorem [66] implies that this curve admits a rational parametrization $Y = r(Z)$, $t = g(Z)$ with $r, g \in k(Z)$, such that all but finitely many k–rational points on $P_I(Y,t) = 0$ are of the form $(r(z_0), g(z_0))$ for some $z_0 \in k$.

Next we show that $f(X, g(Z))$ is reducible over $k(Z)$ with a factor of degree m. Let z be a root of $g(Z) - t$, so z is transcendental over k with $g(z) = t$. By the previous paragraph, $P_I(r(z), t) = 0 = P_I(\beta_I, t)$. Thus $r(z)$ is conjugate to β_I over $k(t)$. But the algebraic conjugates of z over $k(t)$ are precisely the roots of $g(Z) - t$, so we may assume that $r(z) = \beta_I$. But $f_I(X) \in k(t, \beta_I)[X] = k(z)[X]$, and the claim follows. □

The following consequence is from [57] (see also [20] for a similar version), for the sake of completeness we supply the easy proof.

Proposition 1.1.2. *Let $f(X,t) \in k(t)[X]$ be an irreducible polynomial of*

positive degree in X. Set

$$\mathcal{R} := \{t_0 \in \mathcal{O}_k | f(X, t_0) \text{ is defined and reducible over } k\}.$$

Then there are finitely many rational functions $g_i(Z) \in k(Z)$ and a finite set $W \subset \mathcal{O}_k$, such that the following holds.

(a) $\mathcal{R} \subseteq W \cup \bigcup_i (g_i(k) \cap \mathcal{O}_k)$.

(b) $|g_i(k) \cap \mathcal{O}_k| = \infty$.

(c) $f(X, g_i(Z))$ *is reducible over* $k(Z)$.

(d) If $g_i(Z) = a(b(Z))$ *with* $a, b \in k(Z)$ *and* $\deg(b) > 1$, *then* $f(X, g_i(Z))$ *is irreducible over* $k(b(Z))$.

Proof. By Proposition 1.1.1, there is a finite set of rational functions $g_i(Z) \in k(Z)$ such that (a) and (c) hold. Subject to these two conditions, assume that among the possible choices of the g_i the sum $\sum \deg(g_i)$ is minimal. Let g be one of the g_i.

Of course $|g(k) \cap \mathcal{O}_k| = \infty$, for otherwise we could drop g and enlarge W by a finite set. Next suppose that $g(Z) = a(b(Z))$ with $a, b \in k(Z)$, $\deg(b) > 1$, and $f(X, g(Z)) = f(X, a(b(Z)))$ is reducible over $k(b(Z))$. Upon replacing $b(Z)$ by the variable Y, this means that $f(X, a(Y))$ is reducible over $k(Y)$. In particular, $f(X, u_0)$ is reducible for each $u_0 \in a(k) \cap \mathcal{O}_k$, so $a(k) \cap \mathcal{O}_k \subseteq \mathcal{R}$. Clearly $g(k) \cap \mathcal{O}_k \subseteq a(k \cup \{\infty\}) \cap \mathcal{O}_k = (a(k) \cup \{a(\infty)\}) \cap \mathcal{O}_k$. So we could replace g by a and enlarge W by $a(\infty)$ (if this element is in $\mathcal{O}_k$), contrary to our minimality assumption. □

1.2 Group Theoretic Consequences

Proposition 1.1.2 has the following important Galois theoretic translation. Similar considerations appear already in [20], [22], [55], and [57]. Again, for the sake of completeness, we give the straightforward proof from [57].

Lemma 1.2.1. *Let $f(X, t) \in k(t)[X]$ be an irreducible polynomial of positive degree n, and let $g(Z) \in k(Z)$ be one of the rational functions g_i as in Proposition 1.1.2. Choose x and z in an algebraic closure of $k(t)$ such that $f(x, t) = g(z) - t = 0$. Let L be a normal closure of $k(x, z)/k(t)$, and $A := \mathrm{Gal}(L/k(t))$. Let A_x and A_z be the stabilizers in A of x and z, respectively. Furthermore, let B be a group with $A_z < B \leq A$. Then the following holds.*

(a) $A_z A_x \subsetneqq A$.

(b) $BA_x = A$.

(c) $A_z(A_x \cap B) \subsetneqq B$.

(d) *A acts faithfully on A/A_x, and B acts faithfully on $B/(A_x \cap B)$.*

(e) *If A acts primitively on A/A_x, then A acts faithfully on A/A_z.*

(f) *If B acts primitively on $B/(A_x \cap B)$, then B acts faithfully on B/A_z.*

Proof. By Lüroth's Theorem, the fixed field in L of B has the form $k(b(z))$ for $b(Z) \in k(Z)$ of degree $[B : A_z] > 1$. Also, $k(t) \subseteq k(b(z))$, so $t = a(b(z))$ for $a(Z) \in k(Z)$. Thus $g(Z) = a(b(Z))$, and the statements (a) and (b) are the direct translations of the properties (c) and (d) from Proposition 1.1.2, namely that $f(X, g(z))$ is reducible over $k(z)$, but irreducible over $k(b(z))$.

(c) follows from (b), for if $A_z(A_x \cap B) = B$, then

$$A = BA_x = A_z(A_x \cap B)A_x = A_z A_x,$$

contrary to (a).

Let N_x and N_z be the kernel of the actions of A on A_x and A_z, respectively. As L is the normal closure of $k(x, z)/k(t)$, we have $N_x \cap N_z = \mathbf{1}$. Suppose that $N_x \neq \mathbf{1}$. Then N_x is not a subgroup of N_z, hence N_x is also not a subgroup of A_z, because N_z is the intersection of the conjugates of A_z. Thus $A_z < A_z N_x \leq A$. Set $B := A_z N_x$. So $A = BA_x$ by (b). However, (a) gives the contradiction

$$A = BA_x = (A_z N_x)A_x = A_z(N_x A_x) = A_z A_x \subsetneqq A.$$

This establishes the first part of (d). As $BA_x = A$ by (b), the action of B on $B/(A_x \cap B)$ is a subgroup of the action of A on A/A_x. As the latter action is faithful by what we have seen already, the former one is faithful as well.

Next suppose that A does not act faithfully on A/A_z, hence $N_z \neq \mathbf{1}$. Similarly as before, we obtain $A_x N_z > A_x$. On the other hand, because $A_x N_z A_z = A_x A_z \subsetneqq A$, the group $A_x N_z$ is properly between A_x and A. Thus A is not primitive on A/A_x. This gives (e).

We need to show (f). Let $N \leq A_z$ be the kernel of the action of B on B/A_z. Then N is not contained in $A_x \cap B$ by (d), but on the other hand $N(A_x \cap B)$ is a proper subgroup of B by (c). This contradicts the maximality of $A_x \cap B$ in B. □

1.3 Not Absolutely Irreducible Polynomials

In this section k may be any field of characteristic 0.

It is a well–known consequence from Bezout's Theorem that if $f(X,Y) \in k[X,Y]$ is irreducible, but not absolutely irreducible, then there are only finitely many $(a,b) \in k^2$ with $f(a,b) = 0$. Corollary 1.3.2 shows that under certain additional assumptions an analogue of this observation holds in the context of Hilbert sets.

Lemma 1.3.1. *Let $f(X,t) \in k(t)[X]$ be an irreducible polynomial over k, and suppose that $f(X,t_0)$ is reducible for all t_0 in an infinite subset $\mathcal{R}$ of k. Let ℓ be a Galois extension of k, and $h(X,t) \in \ell(t)[X]$ be an ℓ–irreducible factor of $f(X,t)$. Then $h(X,t_0)$ is reducible over ℓ for all but finitely many $t_0 \in \mathcal{R}$.*

Proof. Without loss assume that $f(X,t) \in k[t,X]$ is monic in X. Write $h(X,t) = \sum h_i(t)X^i$, where $h_i(t) \in \ell[t]$, and assume also (Gauß Lemma) that $h(X,t)$ is monic in X. Let $\ell_1 \leq \ell$ be the field generated by k and the coefficients of the h_i.

We claim that there is a cofinite set M in k, such that the coefficients of $h(X,t_0) \in \ell_1[X]$ generate ℓ_1 for each $t_0 \in M$. Suppose that is not the case. Then, by the pigeon hole principle, there is an infinite set M' in k such that the coefficients of the $h(X,t_0)$ generate a proper subfield ℓ_2 of ℓ_1 for all $t_0 \in M'$. Thus for each $t_0 \in M'$, we have $h_i(t_0) \in \ell_2$ for all i. As this holds for infinitely many $t_0 \in k \subseteq \ell_2$, this implies that the coefficients of the h_i are in ℓ_2, a contradiction.

Let M be as above. By removing finitely many elements from M, we may assume that the $\mathrm{Gal}(\ell/k)$–conjugates of $h(X,t_0)$ are relatively prime for each $t_0 \in M$. The product of the $\mathrm{Gal}(\ell/k)$–conjugates of $h(X,t)$ is $f(X,t)$. This implies that the product of the $\mathrm{Gal}(\ell/k)$–conjugates of $h(X,t_0)$ is $f(X,t_0)$ for each $t_0 \in M$. Now take $t_0 \in M$ such that $h(X,t_0)$ is irreducible over ℓ. Then $h(X,t_0)$ divides some irreducible factor $f_1(X) \in k[X]$ of $f(X,t_0)$, hence each Galois conjugate of $h(X,t_0)$ divides f_1, so also the product of these Galois conjugates divides f_1, hence $f_1 = f(X,t_0)$ by the previous consideration. Thus $t_0 \notin \mathcal{R}$, which proves the assertion. □

Corollary 1.3.2. *Let $f(X,t) \in k(t)[X]$ be an irreducible polynomial over k, denote by L its splitting field over $k(t)$, and set $A := \mathrm{Gal}(L/k(t))$. Assume that $f(X,t_0)$ is reducible over k for infinitely many $t_0 \in k$, and that one of the following holds.*

(a) A is a simple group.

(b) A acts primitively on the roots of $f(X,t)$.

Then $f(X,t)$ is absolutely irreducible over k.

Proof. Let $\hat{k} = L \cap \bar{k}$, and $G := \mathrm{Gal}(L/\hat{k}(t))$. Suppose that $f(X,t)$ is not absolutely irreducible. Then G is an intransitive normal subgroup of A. Hypothesis (a) as well as hypothesis (b) imply that $G = 1$. That means that $f(X,t)$ decomposes into linear factors over $\ell = \hat{k}$, contrary to the previous lemma. □

Remark 1.3.3. The assertion of the corollary becomes false if we relax the assumption on A. For instance, take $f(X,t) = X^4 + 2(1-t)X^2 + (1+t)^2$. Then $f(X,t)$ is irreducible over $\mathbb{Q}(t)$, but $f(X,t) = (X^2 + 2ix - 1 - t)(X^2 - 2ix - 1 - t)$, where $i^2 = -1$. Furthermore, from $f(X,u^2) = (X^2 + 2uX + u^2 + 1)(X^2 - 2uX + u^2 + 1)$ we see that $f(X,t_0)$ is reducible over $\mathbb{Q}$ for each square $t_0 \in \mathbb{Z}$.

Chapter 2

Primitive Groups with a two–cycles Element

2.1 Permutation Groups – Notations, Definitions, and Elementary Results

Here we collect definitions and easy results connected to finite groups and finite permutation groups, which are being used throughout the work. Note that many notations and definitions which are only used locally, especially those which are only used in proofs in rare cases, are defined where they first appear. The index of symbols and notions may help finding quickly those definitions.

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 $\{h \in H |\ S^h = S\}$ of S in H.

If $A, B, \ldots$ is a collection of subsets or elements of G, then we denote by $<A, B, \ldots>$ 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 $S := \{\Delta^g |\ g \in G\}$. 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: $\Gamma\mathrm{L}_m(q) := <\mathrm{GL}_m(q), \Gamma> = \mathrm{GL}_m(q) \rtimes \Gamma$, $\Sigma\mathrm{L}_m(q) := <\mathrm{SL}_m(q), \Gamma> = \Sigma\mathrm{L}_m(q) \rtimes \Gamma$.

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 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 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.

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.

2.2 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 on the Santa Cruz Conference on Finite groups in 1979, see [62]. In their statement a case was missing, and the same omission appears in [4]. To our knowledge, the first complete version is in [1]. A very concise and readable proof is given in [48], see also [14].

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 [48], 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.

2.3 Previous Results

The aim of this chapter 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.

Proposition 2.3.1 (Feit [17, 4.1]). *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 Marggrafs theorem [73, 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 [55, 6.2].

Proposition 2.3.2. *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 is a prime power, A is affine; 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 Propositions 2.3.1 and 2.3.2 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 [73, 25.3] and Burnside [32, 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 [73, Theorem 31.2], [72], 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 [63]. 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.

The main result of this chapter is

Theorem 2.3.3. *Let A be a primitive permutation group which contains an element with exactly two cycles. Then one of the following holds.*

(a) *A is affine, with the possibilities given in Theorem 2.4.9, page 17; or*

(b) *A acts via product action, with the possibilities given in Theorem 2.5.5, page 21; or*

(c) *A is almost simple, with the possible actions listed in Theorem 2.8.1, page 24.*

2.4 Affine Action

Here and later we will need the following well–known

Lemma 2.4.1. *Let K be a field of positive characteristic p, and $\sigma \in \mathrm{GL}_m(K)$ of order $p^b \geq p$. Then $p^{b-1} \leq m-1$. In particular, $ord(\sigma) \leq p(m-1)$ if $m \geq 2$.*

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 easy consequence

Lemma 2.4.2. *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 $p^{r-1} \leq m$. In particular, if $r = m$, then $m \leq 2$, 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 2.4.1. □

Lemma 2.4.3. *Let H be a rank 3 permutation group with subdegrees $1 \leq u \leq v$. Suppose that H is imprimitive. Then $1+u$ divides v.*

Proof. Let Δ be a nontrivial block, and $\delta \in \Delta$. Let $\epsilon \neq \delta$ be in Δ. Then Δ contains the orbit ϵ^{H_δ}. Also, Δ does not meet a point from an H_δ–orbit different from $\{\delta\}$ and ϵ^{H_δ}, for then Δ were the full set H is acting on. Thus $\Delta = \{\delta\} \cup \epsilon^{H_\delta}$. But

$$|\epsilon^{H_\delta}| = |\Delta| - 1 \leq (1+u+v)/2 - 1 < v,$$

so the orbit ϵ^{H_δ} has length u, and $1+u$ divides v because the orbit of size v is a union of conjugates of Δ. □

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

Proposition 2.4.4 (Cameron, Kantor [5, 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 $H = \mathcal{A}_7 < \mathrm{SL}_4(2)$.*

Also, the primitive rank 3 permutation subgroups of even order of the collineation group of a projective linear space have been classified by Perin in an unpublished thesis. We use a result of Cameron and Kantor which extends this result. The odd order case is easily handled by a result of Huppert.

Proposition 2.4.5. *Let $m \geq 3$, p be a prime, and $H \leq \mathrm{GL}_m(p)$ be acting primitively of rank 3 on the lines of $\mathbb{F}_p^m$. Then $Sp_m(p) \trianglelefteq H$, or $p = 2$, $m = 3$, $H = \Gamma\mathrm{L}_1(8)$, and the subdegrees are 1, 3, 3.*

Proof. If H has even order see the remarks preceding [5, Prop. 8.5]. So assume that H has odd order. Then H is solvable, so also $\tilde{H} = \mathbb{F}_p^\star H$ is solvable. Furthermore, $\tilde{H}$ is transitive on $\mathbb{F}_p^m$. These groups have been classified by Huppert [32, XII.7.3]. Either $\tilde{H} \leq \Gamma\mathrm{L}_1(p^m)$, or $p^m = 3^4$. (The other exceptional cases in Huppert's classification have $m = 2$.) Let us look at the action of $\Gamma\mathrm{L}_1(p^m) = \mathbb{F}_{p^m}^\star \rtimes \mathrm{Aut}(\mathbb{F}_{p^m})$ on $\mathbb{F}_{p^m}^\star/\mathbb{F}_p^\star$. The stabilizer of the set $\mathbb{F}_p^\star$ is just $\mathbb{F}_p^\star \rtimes \mathrm{Aut}(\mathbb{F}_{p^m})$. So the orbit lengths of the point stabilizer on the projective space are at most m. Therefore we get that the rank is at least

$$1 + \frac{(p^m - 1)/(p-1) - 1}{m} > 1 + (p^{m-1} - 1)/m.$$

Thus $p^{m-1} - 1 < 2m$, hence $p = 2$ and $m = 3$ or 4. If $m = 4$, then H has no contribution coming from $\mathrm{Aut}(\mathbb{F}_{16})$ by the assumption of odd order, hence the point stabilizer is even trivial. The case $m = 3$ indeed does occur.

Now suppose $p = 3$, $m = 4$. The transitive soluble subgroups of $\mathrm{GL}_4(3)$ are available for instance via GAP [61], and one immediately checks that none of them induces a primitive group on the lines of $\mathbb{F}_3^4$. □

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

Lemma 2.4.6. *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 $C = <\tau>$, 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 $(p-1)^2 \,||HS|$. 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 [31, 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 $<C, C^h> \leq H$ is the group of diagonal matrices, in particular $S \leq H$. The claim follows. □

The following proposition is based on Hering's [28], [29] classification of transitive linear groups. Note that his results are incomplete, and the first complete treatment is given by Liebeck in [47, Appendix 1].

Proposition 2.4.7. *Let $m \geq 5$, and $H \leq \mathrm{GL}_m(2)$ be irreducible on $V := \mathbb{F}_2^m$. Suppose there is an element $\tau \in H$ which is the the identity on a 2–dimensional subspace U of V, and cyclically permutes the nonzero elements of a complement W of U in V. Then either $H = \mathrm{GL}_m(2)$, or m is even and $\mathrm{GL}_{m/2}(4) \leq H \leq \Gamma\mathrm{L}_{m/2}(4)$.*

Proof. For a subspace X of V set $X^\sharp := X \setminus \{0\}$. We first want to show that H is transitive on $V^\sharp$. The cycles of τ on $V^\sharp$ are $\{u\}$, $u \in U^\sharp$, and $W^\sharp + u$, $u \in U$. If C_1 and C_2 are subsets of $V^\sharp$ such that each C_i lies completely in an H–orbit, then we say that C_1 and C_2 are *connected* if they lie in the same H–orbit. The latter is equivalent to the existence of $h \in H$ with $C_1 \cap C_2^h \neq \emptyset$. Each of the cycles from above lies in an H–orbit, and the aim is to show that the graph is connected which has as vertices these cycles where to vertices are connected if and only if the corresponding cycles are 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 $h \in H$,

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

so

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

First assume that $u \neq 0$. Then not each element of $U^\sharp - u^h$ can be contained in W^h, for this would imply the nonsense $h^{-1}(U^\sharp) \subseteq W^\sharp + u$. Thus we get

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

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

Now suppose that $u = 0$. Then by the above

$$(W \setminus h^{-1}(U))^h = (W^\sharp \setminus h^{-1}(U^\sharp))^h \subseteq W^\sharp + u \subset W',$$

where W' is the $(m-1)$–dimensional space $W \cup (W+u)$. But the elements in $W \setminus h^{-1}(U))^h$ generate W, so $W^h \subset W'$ for all h, again contrary to irreducibility of H.

Let $u \in U^\sharp$ be such that $W^\sharp$ and $W^\sharp + u$ are connected. We show that these two cycles 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, $(W')^h \subset W' \cup U$, for all $h \in H$. But $W' \setminus (W' \cap h^{-1}(U))$ generates W', so W' is h–invariant for all $h \in H$, again contrary to irreducibility of H.

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 $(u')^H$ generates V by irreducibility, so $(u')^H \not\subseteq U^\sharp$.

Thus H is transitive on $V^\sharp$. So we can use the Hering–Liebeck list [47, Appendix 1] of such groups. Let $L \subseteq \mathrm{End}(V)$ be a maximal field which is normalized by H. (L is unique, see [28, Lemma 5.2].) So $|L| = 2^s$ where s divides m, and $H \leq \Gamma\mathrm{L}_{m/s}(2^s)$. We get that $\mathrm{SL}_{m/s}(2^s) \leq H \leq \Gamma\mathrm{L}_{m/s}(2^s)$, or $H \leq \mathrm{Sp}_m(2)$ with m even. (The Hering–Liebeck result is more precise, but this rough version is good enough here.) We claim that $s = 1$ or 2 in the first case. As $m \geq 5$, we have $s \leq m < 2^{m-2} - 1 = \mathrm{ord}(\tau)$, hence τ^s has exactly 4 fixed points on V and $\tau^s \in \mathrm{GL}_{m/s}(2^s)$. Thus $2^s \leq 4$. If $s = 2$, then note that the determinant of τ as an L–endomorphism of V is a generator of $L^\star$, hence $\mathrm{GL}_{m/2}(4) \leq H$ in this case.

Finally, we need to show that $H \leq \mathrm{Sp}_m(2)$ cannot happen. 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 [31, II.9.15]. Thus for $u \in U^\sharp$, 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 acts irreducibly on. So $\mathrm{ord}(\tau)$ divides $2^{(m-2)/2} + 1 = 2^{\dim W/2} + 1$, see Lemma 2.8.10, contrary to $\mathrm{ord}(\tau) = 2^{m-2} - 1$. □

The proof of the following lemma is straightforward.

Lemma 2.4.8. *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 $\mathbb{F}_2^m$.

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 following

Theorem 2.4.9. *Let A be a primitive affine permutation group of degree p^m. Suppose A contains an element which has exactly two cycles. Let $k \leq l$ be the lengths of these cycles. Let $A_1 \leq \mathrm{GL}_m(p)$ be a point–stabilizer of A. Then one of the following holds.*

(a) $(k, l) = (1, p^m - 1)$, 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) $(k, l) = (p, p^m - p)$, and $A_1 = \mathrm{GL}_m(p)$;

(c) $(k, l) = (p, p^2 - p)$, and $A_1 < \mathrm{GL}_2(p)$ is the group of monomial matrices (here $p > 2$);

(d) $(k, l) = (4, 2^m - 4)$, and $A_1 = \mathrm{GL}_m(2)$;

(e) (Sporadic cases)

(i) $(k, l) = (2, 2)$, and $A_1 = \mathrm{GL}_1(4)$;

(ii) $(k, l) = (2, 6)$, and $A_1 = \Gamma\mathrm{L}_1(8)$;

(iii) $(k, l) = (3, 6)$, and $A_1 = \Gamma\mathrm{L}_1(9)$;

(iv) $(k, l) = (8, 8)$, and $[\Gamma\mathrm{L}_1(16) : A_1] = 3$;

(v) $(k, l) = (8, 8)$, and $A_1 = \Gamma\mathrm{L}_1(16)$;

(vi) $(k, l) = (8, 8)$, and $A_1 = (C_3 \times C_3) \rtimes C_4$;

(vii) $(k, l) = (8, 8)$, and $A_1 = \Sigma\mathrm{L}_2(4)$;

(viii) $(k, l) = (8, 8)$, and $A_1 = \Gamma\mathrm{L}_2(4)$

(ix) $(k,l) = (8,8)$, *and* $A_1 = \mathcal{A}_6$;

(x) $(k,l) = (8,8)$, *and* $A_1 = \mathrm{GL}_4(2)$;

(xi) $(k,l) = (4,12)$ *or* $(8,8)$, *and* $A_1 = (\mathcal{S}_3 \times \mathcal{S}_3) \rtimes C_2$;

(xii) $(k,l) = (4,12)$ *or* $(8,8)$, *and* $A_1 = \mathcal{S}_5 < \mathrm{GL}_4(2)$;

(xiii) $(k,l) = (4,12)$ *or* $(8,8)$, *and* $A_1 = \mathcal{S}_6 < \mathrm{GL}_4(2)$;

(xiv) $(k,l) = (2,14)$ *or* $(8,8)$, *and* $A_1 = \mathcal{A}_7 < \mathrm{GL}_4(2)$;

(xv) $(k,l) = (5,20)$, *and* $[\mathrm{GL}_2(5) : A_1] = 5$;

Proof. Without loss $A \leq \mathrm{AGL}_m(p)$, acting on $N = \mathbb{F}_p^m$. Let σ be the element with the cycle lengths k and l. First note that k divides l, for otherwise σ^l would fix $l > p^m/2$ points, which of course is nonsense. So $k = p^r$, $l = p^r(p^{m-r} - 1)$ for some $r \in \mathbb{N}_0$.

First suppose $k < l$. Then σ^k fixes exactly $k = p^r$ points on N. Without loss $\sigma^k \in \mathrm{GL}_m(p)$, so the fixed point set of σ^k is a subspace N_1 of N. But the elements of N_1 constitute the k–cycle of σ, so σ acts as an affine map of order p^r on the r–dimensional space N_1. Apply Lemma 2.4.2 to see that $r \in \{0,1,2\}$, and $r \leq 1$ if $p > 2$.

If $k = l$, then of course $p = 2$ and $k = l = \mathrm{ord}(\sigma) = 2^{m-1}$. Lemma 2.4.2 gives $2^{m-2} \leq m$, hence $r = m - 1 \leq 3$.

We need to determine the possible groups A. If $k = 1$ we use a result of Kantor [33] 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. Look at the action which A_1 and τ induce on the projective space $P(\mathbb{F}_p^m)$. The element τ has a fixed point (corresponding to U), a cycle of length $(p^{m-1} - 1)/(p - 1)$ (corresponding to W) and a cycle of length $p^{m-1} - 1$ (corresponding to $u + W$ for $0 \neq u \in U$).

Lemma 2.4.6 handles the case $m = 2$. So for the rest of this argument we assume $m \geq 3$. We contend that A_1 is transitive on $P(\mathbb{F}_p^m)$. By primitivity, A_1 is irreducible on $\mathbb{F}_p^m$, so it moves the fixed point of τ as well as the cycle of length $(p^{m-1} - 1)/(p - 1)$. So if A_1 were not transitive, then A_1 would leave $U \cup W$ invariant. Let $a \in A_1$ with $W^a \neq W$, and choose $w \in W$ with

$w^a \in U$. Then $W \setminus \mathbb{F}_p w$ is invariant under a. But $W \setminus \mathbb{F}_p w$ generates W because of $m \geq 3$, a contradiction.

Looking at τ we see that A_1 is a transitive group on $P(\mathbb{F}_p^m)$ of rank at most 3. If A_1 is even doubly transitive, then by Proposition 2.4.4 either $p = 2$, $m = 4$, and $A_1 = \mathcal{A}_7$, or $\mathrm{SL}_m(p) \leq A_1$. It is easy to see that the determinant of τ is a generator of the multiplicative group of $\mathbb{F}_p$. Thus $A_1 = \mathrm{GL}_m(p)$ in the latter case.

Next assume that A_1 has rank 3 on $P(\mathbb{F}_p^m)$. We first use Lemma 2.4.3 to see that A_1 is also primitive. For if not, then $1 + \alpha$ divides $(p-1)\alpha$ with $\alpha = (p^{m-1} - 1)/(p-1)$, so $1 + \alpha$ divides $p - 1$, which of course is nonsense.

So we can apply Proposition 2.4.5. Suppose that $\mathrm{Sp}_m(p) \trianglelefteq A_1$. However, $\mathrm{Sp}_m(p)$ has rank 3 on $P(\mathbb{F}_p^m)$ and subdegrees 1, p^{m-1} and $p(p^{m-2}-1)/(p-1)$ (see [31, II.9.15]), which is not compatible with the cycle lengths of τ we determined above. Thus the other possibility of the proposition holds, that is $p = 2$, $m = 3$, $A_1 = \Gamma\mathrm{L}_1(8)$, which indeed gives case (e)(ii) in the theorem.

To see that the groups listed in (b) and (c) indeed have an element with cycle lengths p and $p^m - p$ use Lemma 2.4.8, and similarly for the cycle lengths 4 and $2^m - 4$ in (d).

Next we look at the case $p = 2$ and $k = 4$. The case $m \leq 4$ is done by inspection, so assume $m \geq 5$. Set $\tau := \sigma^4$. As above we see that $\mathbb{F}_2^m = U \oplus W$ with $\dim U = 2$, τ is trivial on U, and acts as a Singer cycle on W. In view of Proposition 2.4.7 we need to show that $GL_{m/2}(4) \leq A_1 \leq \Gamma\mathrm{L}_{m/2}(4)$ is not possible. Suppose that were the case. Write $\sigma = (\beta, v)$ with $\beta \in \Gamma\mathrm{L}_{m/2}(4)$, and $v \in \mathbb{F}_4^{m/2}$. First note that $U^\beta + v = U$, so $v \in U$ and β leaves U invariant. This easily implies $\beta^4 = \tau$. The intersection $W \cap W^{\beta^2}$ is not trivial (by dimension reasons) and invariant under β^2, so in particular invariant under τ. Hence $W = W^{\beta^2}$ by irreducibility of τ on W. But $W \cap W^\beta$ is also τ–invariant, so β leaves W invariant by the same argument. As $\tau = \beta^4$ permutes the elements of $W^\sharp$ cyclically, the same holds true for β. Hence β has odd order $2^{m-2} - 1$ when restricted to W. In particular, $\beta \in \mathrm{GL}_{m/2}(4)$. On the other hand, as (β, v) has order 4 on U, the order of β on U must be a divisor of 4. However, $|\mathrm{GL}_1(4)| = 3$, hence β is trivial on U. But then (β, v) has order 2 on U, a contradiction.

The case $k = l = 8$, $p = 2$, is most conveniently done by inspection using GAP [61]. □

2.5 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 2.5.1. *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. □

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. [31, 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 2.5.2. *Let Δ_1, Δ_2, ... , Δ_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 2.5.3. *Let Δ_1, Δ_2, ... , Δ_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 $(g_1, g_2, \ldots, g_m)$ has at least $c_1 c_2 \cdots c_m$ cycles on $\Delta_1 \times \Delta_2 \times \cdots \times \Delta_m$.*

Lemma 2.5.4. *Suppose $r \geq 5$ and $m \geq 2$. Let $g = (\sigma_1, \sigma_2, \ldots, \sigma_m)\tau$ 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 $\overline{g} := g^m = (\overline{\sigma_1}, \overline{\sigma_2}, \ldots, \overline{\sigma_m}) \in \mathcal{S}_r^m$. 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 2.5.3, 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 2.5.2, 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. □

The main result of this section is

Theorem 2.5.5. *Let A be a primitive non–affine permutation group in product action. Suppose A contains an element which has exactly two cycles. Let $k \leq l$ be the lengths of these cycles. Then one of the following holds.*

(a) $A = (\mathcal{S}_r \times \mathcal{S}_r) \rtimes C_2$ with $r \geq 5$, $k = ra$, $l = r(r-a)$ with $\gcd(r, a) = 1$; or

(b) $A = (\mathrm{PGL}_2(p) \times \mathrm{PGL}_2(p)) \rtimes C_2$ with $p \geq 5$ prime, $k = p+1$, $l = p^2+p$.

Proof. We assume that $A \leq \mathcal{S}_r \wr \mathcal{S}_m$ with $r \geq 5$ (by Lemma 2.5.1) and $m \geq 2$. Let $g = (\sigma_1, \sigma_2, \ldots, \sigma_m)\tau$ 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 [48] shows that there is a primitive group U with socle S acting on $\Delta = \{1, 2, \ldots, r\}$, 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 Propositions 2.3.1 and 2.3.2 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 2.5.6. Case (c) of Theorem 2.4.9, that is $A < \mathrm{GL}_2(p)$ 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.

2.6 Regular Action

As an immediate consequence of the previous section we obtain

Theorem 2.6.1. *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 [48, page 392]. Now apply Theorem 2.5.5 to see that this cannot occur, a distinguishing property of H being that it is not doubly transitive (in contrast to $\mathrm{PGL}_2(p)$). □

2.7 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 $(l_1, l_2, \ldots, l_m) \sim (cl_1, cl_2, \ldots, cl_m)$ 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 $(i^{-1}l_1 i, i^{-1}l_2 i, \ldots, i^{-1}l_m i) \sim (l_1, l_2, \ldots, l_m)(i, i, \ldots, i)$.

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

Proposition 2.7.1. *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 $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_m)\tau$ with $\tau \in \mathcal{S}_m$ and $\sigma_i \in S$. Let τ have u cycles of lengths $\rho_1, \rho_2, \ldots, \rho_u$.

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

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

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 2.5.2, 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 2.5.3 to see that the number of cycles of σ on N is at least

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

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 $0 \leq x \leq mo/e$. Note that $o \geq 5$ (because a group with element orders ≤ 4 is solvable), so $mo/e > m$, but $u \leq m$. So the above expression is $\geq (|S|/o)^m$. 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 2.7.2. *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 2.7.1 gives, as $m \geq 2$,

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

If S is sporadic, then use list 2.3 on page 60 along with the group orders given in the atlas [8] to see that this inequality has no solution. Next suppose that $S = \mathcal{A}_n$ is alternating. Then $\mathrm{Out}(S) = C_2$ if $n \neq 6$, and $\mathrm{Out}(\mathcal{A}_6) = C_2 \times C_2$, so $o(\mathrm{Out}(S)) = 2$ in any case (see e.g. [31, II.5.5]). Use the bound $o(S) \leq e^{n/e}$ from Proposition 2.8.4 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 2.2 (page 59) and 2.1 (page 58) and in Section 2.8.3 together with the order of S given for instance in the atlas [8], 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 [8] 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 $\mathrm{ord}(\overline{\sigma_1})\mathrm{ord}(\overline{\sigma_2}) \geq 168/4 = 42$, 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. □

2.8 Almost Simple Action

The aim of this section is

Theorem 2.8.1. *Let A be a primitive permutation group of degree n, such that $S \leq A \leq \mathrm{Aut}(S)$ for a simple, non–abelian group S. Suppose A contains an element which has exactly two cycles. Let $k \leq l$ be the lengths of these cycles. Then one of the following holds.*

(a) $\mathcal{A}_n \leq A \leq \mathcal{S}_n$ *in natural action.*

(b) $(k, l) = (5, 5)$, *and* $\mathcal{A}_5 \leq A \leq \mathcal{S}_5$ *in the action on the 2–sets of* $\{1, 2, 3, 4, 5\}$.

(c) $(k, l) = (1, p)$, *and* $\mathrm{PSL}_2(p) \leq A \leq \mathrm{PGL}_2(p)$ *for a prime* p.

(d) $k = l = (q^m - 1)/(2(q - 1))$, *and* $\mathrm{PSL}_m(q) \leq A \leq \mathrm{P\Gamma L}_m(q)$ *for an odd prime power* q *and* $m \geq 2$ *even.*

(e) $(k, l) = (2, 8)$, *and* $\mathrm{M}_{10} \leq A \leq \mathrm{P\Gamma L}_2(9)$.

(f) $(k,l) = (7,14)$, *and* $\mathrm{P\Sigma L}_3(4) \leq A \leq \mathrm{P\Gamma L}_3(4)$.

(g) $(k,l) = (1,11)$ *or* $(4,8)$, *and* $A = \mathrm{M}_{11}$ *in its action on* 12 *points.*

(h) $(k,l) = (1,11)$, $(2,10)$, $(4,8)$, *or* $(6,6)$, *and* $A = \mathrm{M}_{12}$.

(i) $(k,l) = (11,11)$, *and* $\mathrm{M}_{22} \leq A \leq \mathrm{Aut}(\mathrm{M}_{22}) = \mathrm{M}_{22} \rtimes C_2$.

(j) $(k,l) = (1,23)$, $(3,21)$, *or* $(12,12)$, *and* $A = \mathrm{M}_{24}$.

Remark 2.8.2. The simple group S is either alternating, sporadic or of Lie type. We deal with these cases in separate sections, as they require quite different arguments. See Section 2.8.7 where all the results achieved in the following parts are bundled to give a proof of the above theorem.

Many cases of almost simple permutation groups can be ruled out by comparing element orders with indices of (maximal) subgroups of groups between S and A, though some other require finer arguments. For a finite groups X let $\mu(X)$ be the smallest degree of a faithful, transitive permutation representation, and $o(X)$ the largest order of an element in X. We use the trivial

Lemma 2.8.3. *Let A be a transitive permutation group of degree n, and let $\sigma \in A$ have two cycles in this action. Then*

$$n \leq 2ord(\sigma) \tag{2.1}$$

$$n \leq 3ord(\sigma)/2, \text{ if } n \text{ is odd.} \tag{2.2}$$

2.8.1 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 [42, §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 2.8.4. *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

$$\nu_1 + \nu_2 + \cdots + \nu_r \leq n. \tag{2.3}$$

The inequality between the arithmetic and geometric mean yields

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

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 [31, II.5.5]. We exclude $n = 6$ in this section, and treat this case in Section 2.8.3 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 $1 \leq m < n$. Denote by M_m the subsets of size m of $\{1, 2, \ldots, n\}$. 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 (a) in Theorem 2.8.1. So for the remainder assume $m \geq 2$.

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 $n \geq \binom{n}{m}/2 \geq n(n-1)/4$, thus $n = 5$. This case really occurs, and gives case (b) in Theorem 2.8.1.

Next suppose that σ is not an n–cycle. Then σ leaves (on $\{1, 2, \ldots, n\}$) a set S of size $1 \leq |S| \leq n/2$ invariant. Without loss $m \leq n/2$ (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 $|S| \geq 2$. 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 2.8.3 and Proposition 2.8.4 to see that this case does not occur. The proof is based on the following

Lemma 2.8.5. *Let $u, v \geq 2$ be integers, then*

$$u!^v v! < \frac{1}{2} \frac{(uv)!}{e^{uv/e}}, \tag{2.4}$$

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

Proof. We contend that if the inequality (2.4) holds for (u, v), then it holds also for $(u, v+1)$. First

$$3 < 4.31\ldots = \left(\frac{3}{e^{1/e}}\right)^2 \leq \left(\frac{3}{e^{1/e}}\right)^u,$$

hence

$$e^{u/e} < 3^{u-1} \leq (v+1)^{u-1}.$$

This implies

$$(v+1)e^{u/e} < (v+1)^u. \tag{2.5}$$

But

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

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

$$(v+1)^u \leq \binom{uv+u}{u},$$

so

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

by (2.5). Multiply the resulting inequality

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

with (2.4) to obtain the induction step for v.

Next we show that (2.4) 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 (2.4) 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 (2.4) 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 2.8.3.

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 [3] or [73, 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 2.8.3 and Proposition 2.8.4

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

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

$$\left[\frac{n+1}{2}\right]! > 4e^{n/e}. \tag{2.6}$$

But if (2.6) 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 (c) in Theorem 2.8.1 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 2.8.3.

Now assume $n = 8$. Similarly as above, we see that the only case which does not directly contradict Lemma 2.8.3 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 2.8.30 shows that this case actually does not occur.

Finally, if $n = 10$, then we keep Bochert's bound, but use Proposition 2.8.4 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 2.8.3, a contradiction.

2.8.2 Sporadic Groups

Let S be one of the 26 sporadic groups. Table 2.3 on page 60 contains information about small permutation degrees, big element orders, and the outer

automorphism group. The atlas [8] 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 [39], [38], [37], and [50], respectively. The bounds for the groups Fi'_{24}, B, and M have been marked with a *, as they are not sharp. We got them, using the following trivial remark, from the character tables in [8]: 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 2.8.3 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 [8] 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.

$\mathbf{S = M_{11}}$. 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 2.8.3 $\mathrm{ord}(\sigma) \geq (2/3)11$, 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.

$\mathbf{S = M_{12}}$. The smallest degree of a faithful primitive representation of $\mathrm{Aut}(\mathrm{M}_{12})$ is 144 (see [8]), 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.

$\mathbf{S = M_{22}}$. 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.

$\mathbf{S = M_{23}}$. 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.

$\mathbf{S = M_{24}}$. 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.

2.8.3 Element Orders in Classical Groups

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 2.8.6. *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 [68, 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 $G(F)$. □

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

Lemma 2.8.7. *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 $q^{r/f}$. □

Lemma 2.8.8. *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 $ord(\sigma) \leq q^n - 1$, 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 2.4.1. 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 $m > 1$.) □

We obtain the following consequence

Proposition 2.8.9. *Let q be a prime power, and $n \geq 2$.*

(a) If $\sigma \in \Gamma\mathrm{L}_n(q)$, then $ord(\sigma) \leq q^n - 1$.

(b) If $\overline{\sigma} \in \mathrm{P}\Gamma\mathrm{L}_n(q)$, then $ord(\overline{\sigma}) \leq (q^n-1)/(q-1)$, 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 2.8.8, 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 2.8.8 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 2.8.6, $\tau := \sigma^f$ 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, $\mathrm{ord}(\sigma) \leq f\mathrm{ord}(\sigma^f) < fr^n \leq q^n$, where we used Lemma 2.8.7 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

$$f\frac{r^f-1}{r-1} \leq \frac{r^{nf}-1}{r^n-1}. \tag{2.7}$$

Note that $(x^f-1)/(x-1) = 1+x+\cdots+x^{f-1}$ is strongly monotonously increasing for $x > 1$, so inequality (2.7) 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 (2.7) 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 2.8.10. *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 2.8.11. *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 singular 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 singular, 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

$$\begin{aligned} (Z \oplus Z') \cap (Z \oplus Z')^\perp &= (Z \oplus Z') \cap Z^\perp \cap (Z')^\perp \\ &= Z \cap (Z')^\perp \\ &= \{0\}, \end{aligned}$$

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 singular, 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 2.8.12. *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 2.8.13. *Let $q \geq 2$ and $m_1, m_2, \ldots, m_\rho$ 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 $i = 1, 2, \ldots, \rho$ 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 2.8.14. *Use the notation from Lemma 2.8.12 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 $ord(\sigma)$ divides $p^b(q^z - 1)$. Furthermore,*

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

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

$$p^b(q^z - 1) > 2q^{[wz/2]}. \tag{2.8}$$

From (2.8) we obtain

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

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

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

hence

$$p^{b-1}q^z \geq q^{[wz/2]}. \tag{2.9}$$

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 2.4.1. Clearly $w' \leq w$, hence $p^{b-1} \leq w - 1$. So with (2.9) 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 (2.9)). 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 2.8.11 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 $i = 0, 1, \ldots, z-1$. By Lemma 2.8.11, 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

$$2^b(q^z - 1) > q^{wz/2}. \tag{2.10}$$

From that we obtain

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

hence

$$2^{b-1} \geq q^{wz/2-z}$$

and

$$w - 1 \geq q^{wz/2-z}, \tag{2.11}$$

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 (2.11). Suppose $w = 6$. Then $q = 2$ and $b \leq 3$, and we obtain a contradiction to (2.10). Next suppose $w = 4$. Again $q = 2$. From (2.10) 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 2.8.15. *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*

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

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 2.8.10 and 2.8.14 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 $1 < w_1 < w_2 < \ldots$ 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 2.8.10, 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 2.8.13. If $q \neq 2$, then apply the bounds in Lemma 2.8.14 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. □

At a few places we need the following trivial

Lemma 2.8.16. *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. □

2.8.4 Classical Groups

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 [36, Theorem 5.2.2] which still contains a mistake (giving the wrong μ for $P\Omega_8^+(3)$). 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 [36, 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 $\mathrm{Sp}_4(2)' \cong \mathrm{PSL}_2(9)$.

We combine this information about minimal permutation degrees, in order to show that we necessarily have $S = \mathrm{PSL}_m(q)$, if a primitive almost simple group with a classical minimal normal subgroup S contains an element with only two cycles.

S symplectic

We rule out the symplectic groups, using the following

Lemma 2.8.17. *Let $S = \mathrm{PSp}_{2m}(q)$ be the simple symplectic group, and $\sigma \in \mathrm{Aut}(S)$. Then*

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

In particular, $ord(\sigma) \leq 4q^m$ 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 [36, 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 2.8.6, 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 2.8.15. Thus τ has order at most $2fq^{m/f} \leq 2q^m$, where we used Lemma 2.8.7. The claim follows in the odd case.

If q is even, then $\mathrm{Out}(S) = C_r$ if $m \geq 3$. 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 [7, Chapter 12]. The claim follows as above. □

Now we rule out the symplectic groups in the order as they appear in Table 2.1 on page 58.

$\mathbf{m \geq 2,\ q \geq 3,\ (m, q) \neq (2, 3)}$. Let $\sigma \in \mathrm{Aut}(S)$. The minimal faithful permutation degree of S is $(q^{2m} - 1)/(q - 1)$. As $q \geq 3$, we get $\mathrm{ord}(\sigma) \leq 4q^m$ by the previous Lemma. So Lemma 2.8.3 gives

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

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

$\mathbf{m \geq 3}$, $\mathbf{q = 2}$. We get $\mu(S) = 2^{m-1}(2^m - 1) \leq 2(3e/2)2^m$, hence $2^m - 1 \leq 6e$, so $m = 3$ or 4. If $m = 4$, then the atlas gives $\mathrm{ord}(\sigma) \leq 30$, contrary to $\mu(S) \leq 2\mathrm{ord}(\sigma)$. Thus $m = 3$. The atlas gives $\mathrm{ord}(\sigma) \leq 15$, 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.

S orthogonal in odd dimension

Now suppose that $S = \Omega_{2m+1}(q)$.

Lemma 2.8.18. *Let $S = \Omega_{2m+1}(q)$ be the simple orthogonal group with q odd, $m \geq 3$, and $\sigma \in \mathrm{Aut}(S)$. Then*

$$ord(\sigma) \leq 2q^m.$$

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 [36, 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 2.8.6 together with Proposition 2.8.15 and Lemma 2.8.7 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.

S orthogonal of plus type

Lemma 2.8.19. *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*

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

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 [36, Theorem 2.1.4, Table 2.1.D]. Now apply Proposition 2.8.15, 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 2.8.15, 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 [36, 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 2.8.15 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 [8]. □

$\mathbf{m \geq 4}$, $\mathbf{q \geq 3}$. The case $(m, q) = (4, 3)$ obviously does not occur, see Table 2.1 on page 58.

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 2.8.16, 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 $q < 4$, so $q = 3$, a case already dealt with above. 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 $\mathrm{ord}(\sigma) \leq (9/4)4^5 = 2304$, whereas $\mu(S) = 5525 > 2 \cdot 2304$, a contradiction.

$\mathbf{m \geq 4}$, $\mathbf{q = 2}$. If $m = 4$, then $\mathrm{ord}(\sigma) \leq 30$, 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.

S orthogonal of minus type

Lemma 2.8.20. *Let $S = P\Omega^-_{2m}(q)$ be the simple orthogonal group with Witt defect 1, and $\sigma \in \mathrm{Aut}(S)$. Write $q = p^f$ for p a prime. Then*

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

Proof. The proof follows exactly as in Lemma 2.8.19, 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 [8]. □

Now $S = P\Omega^-_{2m}(q)$ for $m \geq 4$. From Lemma 2.8.16 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 $\mathrm{ord}(\sigma) \leq 4 \cdot 3^4 = 324$. 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 $\mathrm{ord}(\sigma)$ from Lemma 2.8.20.

S unitary

Lemma 2.8.21. *Suppose that $\sigma \in \mathrm{GU}_n(q)$ acts irreducibly on $\mathbb{F}_q^n$. Then n is odd, and $ord(\sigma)$ divides $q^n + 1$. The order of the image of σ in $\mathrm{PGU}_n(q)$ 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 2.8.10, there exists an index i in the given range such that $\lambda^{-q} = \lambda^{q^{2i}}$, so

$$\lambda^{q^{2i-1}+1} = 1. \tag{2.12}$$

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 (2.12). 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 2.8.22. *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.*

(a) If $n = 1$, then ord(σ) divides $q+1$.

(b) If $n = 2$, then ord(σ) divides q^2-1 or $p(q+1)$.

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

(d) If $n = 4$, then ord$(\overline{\sigma})$ divides q^3+1, q^3-q^2+q-1, or $p^r(q^2-1)$ where $r \leq 2$ and $r = 1$ if $p > 2$. For $p = 3$, there is the additional possibility 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 2.8.21, 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 2.8.21. 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 2.8.11 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 $p^{r-1} \leq 2$ by Lemma 2.4.1, 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

2.8.11. 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 2.8.11.

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 $b \geq 2$, 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 2.8.11 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 2.8.11. We get the stated divisibilities. □

Lemma 2.8.23. *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 2.8.22. Also, if $f = 1$, we are obviously done. Therefore we are concerned with $r = 2f$ with $f \geq 2$.

By Lemma 2.8.6, 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 2.8.9. 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 2.8.24. *Let $S = \mathrm{PSU}_n(q)$ be the simple unitary group with $n \geq 3$, and $\sigma \in \mathrm{Aut}(S)$. Then*

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

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 2.8.15 to obtain the claim. □

We rule out the unitary groups in the order as they appear in the list 2.1 on page 58. 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 2.8.22 and the structure of the automorphism group of $\mathrm{PSU}_m(q)$ given in [36, 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 [8] 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 [8]. 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 2.8.23. We obtain $(q+1)(q^3+1) = \mu(S) \leq 2f(q^3+1)$, hence $q + 1 \leq 2f$. But $q \geq 2^f \geq 2f$, so there is no solution. Next suppose $f = 1$, so $q = p$. We obtain $p + 1 \leq 4$, so $p = 3$. However, the maximal element order in $\mathrm{Aut}(\mathrm{PSU}_4(3))$ is 28, see the atlas [8], a contradiction. Similarly, if $q = 2$, then $o(\mathrm{Aut}(\mathrm{PSU}_4(2))) = 12$, which is too small.

$\mathbf{6 \mid m}$, $\mathbf{q = 2}$. Use Lemma 2.8.24 to get $2^{m-1}(2^m - 1)/3 \leq 2(3e/2)2^m = 6e2^{m-1}$, hence $2^m - 1 \leq 18e = 48.9\ldots$, so $m \leq 5$, a contradiction.

$\mathbf{m \geq 5}$, $(\mathbf{m, q}) \neq (\mathbf{6m', 2})$. From Lemma 2.8.16 we obtain $\mu(S) > q^{2m-3}$. On the other hand, $\mathrm{ord}(\sigma) \leq (3e/2)q^m$ by Lemma 2.8.24, so $q^2 \leq q^{m-3} \leq 3e = 8.1\ldots$, 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 [8], a contradiction.

2.8.5 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 [70, 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 2.8.25. *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 $|\Omega| \geq 3n$.*

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,

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

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 $M \leq A_1$, a contradiction. □

Lemma 2.8.26. *Let $S = \mathrm{PSL}_n(q)$ with $(n, q) \neq (4, 2)$, $(2, 2)$, $(2, 3)$, $(2, 4)$, $(2, 5)$, $(2, 7)$, $(2, 9)$, or $(2, 11)$. Let A be a group with $S \leq A \leq \mathrm{Aut}(S)$. 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 2.8.25 we obtain $N \geq 3\mu$. If $\sigma \in \mathrm{P\Gamma L}_n(q)$, then $\mathrm{ord}(\sigma) \leq \mu$ by Proposition 2.8.9, contrary to Lemma 2.8.3. Thus σ involves a graph automorphism of $\mathrm{PSL}_n(q)$, hence also $n \geq 3$.

As $\sigma^2 \in \mathrm{P\Gamma L}_n(q)$, we have $\mathrm{ord}(\sigma) \leq 2\mu$, hence $N \leq 4\mu$. 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 $[S : M] \leq [S : S_1]/2 \leq 2\mu$, so it follows easily from [70, 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 $A = A_1S$ 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 $N \geq (q^n-1)(q^{n-1}-1)/(q-1)^2 = (q^{n-1}-1)/(q-1)\mu$. From $N \leq 2\mathrm{ord}(\sigma) \leq 4\mu$ we obtain $1 + q + \cdots + q^{n-2} \leq 4$. Hence $n = 3$ and $q = 3$ or 2. However, for $q = 3$ we have $\mathrm{ord}(\sigma) \leq 13$ by [8], contrary to $N \geq 52$. If $q = 2$, then $\mathrm{Aut}(S) \cong \mathrm{PGL}_2(7)$, so $\mathrm{ord}(\sigma) \leq 8$, but $N \geq 21$, a contradiction.

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

Lemma 2.8.27. *Let $S = \mathrm{PSL}_n(q)$ with $(n, q) \neq (4, 2)$, $(2, 2)$, $(2, 3)$, $(2, 4)$, $(2, 5)$, $(2, 7)$, $(2, 9)$, $(2, 11)$ and $S \leq A \leq \mathrm{Aut}(S)$. Assume that A acts primitively on Ω. Suppose that $\sigma \in A$ has at most 2 cycles on Ω. Then either $A \leq \mathrm{P\Gamma L}_n(q)$ and A acts naturally on the lines of $\mathbb{F}_q^n$, or $(n, q) = (3, 2)$, and $A \leq \mathrm{Aut}(\mathrm{PSL}_3(2)) \cong \mathrm{PGL}_2(7)$ 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 $\mathrm{ord}(\sigma) \leq 2(q^n-1)/(q-1)$ by Proposition 2.8.9.

S is primitive by the previous lemma, so we can use the results by Tiep and Zalesskii [70, Section 9] on the three smallest primitive permutation degrees for the simple groups $\mathrm{PSL}_n(q)$, see the comment before Lemma 2.8.25.

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

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

(This second smallest primitive representation is given by the action on the 2–spaces in $\mathbb{F}_q^n$.) Now use $N \leq 2\mathrm{ord}(\sigma)$ to obtain $q^{n-1} - 1 \leq 4(q^2-1)$. 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 [8], whereas $N = 130 > 2 \cdot 40$, so this case is out.

Next assume $n = 3$. Using [70, Section 9], one easily verifies that $N \geq q^3 - 1$ except for $q = 4$ and 2. Exclude $q = 2$ and 4 for a moment. So

$q^3 - 1 \leq 4(q^3-1)/(q-1)$, 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 [8] gives $\mathrm{ord}(\sigma) \leq 21$, whereas $N \geq 56 > 2 \cdot 21$ by [70, 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 [70, 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 2.8.28. *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 2.8.25, 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 2.8.25.

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 2.8.29. *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 2.8.6, $(\gamma g)^f$ 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 2.8.9. Thus

$$f(q^{n/f}-1) \geq \mathrm{ord}(\gamma g) \geq \frac{1}{2}\frac{q^n-1}{q-1}. \tag{2.13}$$

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

$$n < \frac{2f}{f-1} = 4 - 2\frac{f-2}{f-1} \leq 4, \tag{2.14}$$

so $n \leq 3$.

First suppose $n = 3$. Then (2.14) shows $f < 3$, hence $f = 2$. Set $r = q^{1/2}$. Then (2.13) 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. [8].

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 $\mathrm{ord}(\overline{h}) \,|\, \mathrm{ord}(h) \,|\, r-1$. 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

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

hence

$$\frac{r^f+1}{r+1} \leq 2f.$$

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 2.8.30. *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:*

(a) q is a prime, $n = 2$, and σ has order q.

(b) 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

$$q^u \text{ divides } \mathrm{ord}(\hat{\sigma}), \text{ where } u = \dim(U). \tag{2.15}$$

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 (2.15) 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 (2.15) 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. □

2.8.6 Exceptional Groups of Lie Type

Here we rule out the case that S is an exceptional group of Lie type. Table 2.2 on page 59 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 f.

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 [43]. We use the corrected list [36, 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 [25, 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 [49, 1.3A]. The order of a p–element g is bounded as follows. Suppose $S \leq \mathrm{PGL}_w(F)$ for a field F of characteristic p. Then the order of g is a p–power at most $p(w-1)$, see Lemma 2.4.1. Small values w with an embedding as above are classically known, see [36, Prop. 5.4.13]. However, for the Suzuki groups ${}^2B_2(q)$ we used [32, XI, §3] to determine μ and o. To determine μ for $G_2(q)$ and ${}^3D_4(q)$ we use the papers by Kleidman [34] and [35] 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 2.2 on page 59 rules out all but a few little cases, which require extra data obtained from the atlas [8].

$\mathbf{S = {}^2B_2(q)}$. 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 [8]), 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 [8], 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 [8]), 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 [36, 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 [6, 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 [6, 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 $\mu(E_6(2)) \geq \mu(F_4(2)) = 69615$ ([8]), a contradiction.

$\mathbf{S = E_7(q)}$. We get $q = 2$. Use [6, 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.

2.8.7 Proof of Theorem 2.8.1

Now we are ready to prove Theorem 2.8.1, 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 2.8.2 gives the possibilities. This is the easiest case, as the result can be directly read off from the atlas information [8]. Only the Mathieu groups M_{11}, M_{12}, M_{22}, and M_{24} give rise to examples, listed as (g), (h), (i), and (j) in Theorem 2.8.1, respectively.

Section 2.8.1 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 (b)), or $S = \mathcal{A}_5$ acting on 6 points (case (c) for $p = 5$, note that $\mathcal{A}_5 \cong \mathrm{PSL}_2(5)$).

By Section 2.8.6, S cannot be of exceptional Lie type.

In Section 2.8.3 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 2.8.5. We can exclude a couple of small pairs (n, q) in view of exceptional isomorphisms, see [36, 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 2.8.1. 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 2.8.27. Lemma 2.8.28 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 2.8.29, 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 (f) in Theorem 2.8.1. 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 (e) of Theorem 2.8.1.

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 2.8.30 finishes this case: Either q is a prime, $n = 2$, $\mathrm{ord}(\sigma) = q$ (so σ has cycle lengths 1 and q, case (c) of Theorem 2.8.1), or σ is the square of a Singer cycle (case (d) of Theorem 2.8.1).

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

2.9 Tables on Minimal Permutation Degrees, Maximal Element Orders, etc.

Table 2.1: 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	$m\geq 3$
$\mathrm{P}\Omega^+_{2m}(q)$	$(q^m-1)(q^{m-1}+1)/(q-1)$	$2(4,q^m-1)f, m\neq 4$ $6(4,q^m-1)f, m=4$	$m\geq 4,\ q\geq 3$ $(m,q)\neq(4,3)$
$\mathrm{P}\Omega^+_{2m}(2)$	$2^{m-1}(2^m-1)$	$2, m\neq 4$ $6, m=4$	$m\geq 4$
$\mathrm{P}\Omega^+_8(3)$	1080	24	
$\mathrm{P}\Omega^-_{2m}(q)$	$(q^m+1)(q^{m-1}-1)/(q-1)$	$2(4,q^m+1)f$	$m\geq 4$
$\mathrm{PSU}_3(q)$	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 2.2: 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 2.3: Sporadic Groups

Group S	Orders of elements	Indices of maximal subgroups	$\lvert\mathrm{Out}(S)\rvert$
M_{11}	11, 8, 6, ≤ 5	11, 12, ≥ 55	1
M_{12}	11, 10, 8, 6, ≤ 5	12, ≥ 66	2
M_{22}	11, 8, 7, 6, ≤ 5	22, ≥ 77	2
M_{23}	23, 15, 14, ≤ 11	23, ≥ 253	1
M_{24}	23, 21, 15, 14, 12, ≤ 11	24, ≥ 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	$\geq 8672^*$	2
HN	≤ 40	≥ 1140000	2
Th	≤ 39	≥ 143127000	1
B	≤ 70	$\geq 4372^*$	1
M	≤ 119	$\geq 196883^*$	1

Chapter 3

Genus 0 Systems

3.1 Branch Cycle Descriptions

3.1.1 Algebraic and Topological Description

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 $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ be the places of $k(t)$ which are ramified in L. Then, by a consequence of Riemann's Existence Theorem (see [53], [71]), we can choose places $\mathfrak{P}_i$ of L lying above $\mathfrak{p}_i$, $i = 1, 2, \ldots, r$, 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:

$$\text{The } \sigma_i,\ i = 1, 2, \ldots, r \text{ generate } G, \text{ and } \sigma_1\sigma_2 \ldots \sigma_r = 1.$$

We call the tuple $(\sigma_1, \sigma_2, \ldots, \sigma_r)$ 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.

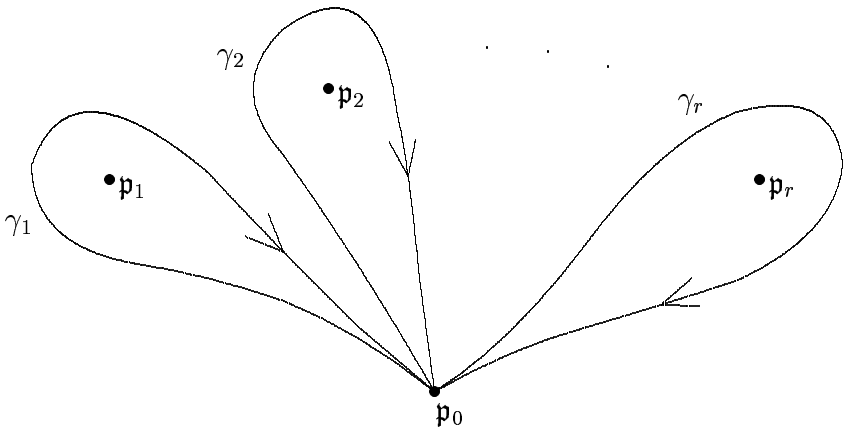
Let g_E be the genus of the field E. The Riemann–Hurwitz genus formula gives

$$2(n - 1 + g_E) = \sum_{i=1}^{r} \mathrm{ind}(\sigma_i). \tag{3.1}$$

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 $(\sigma_1, \sigma_2, \ldots, \sigma_r)$ 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 $\sigma_1, \sigma_2, \ldots, \sigma_r$, such that $\sigma_1\sigma_2 \ldots \sigma_r = 1$. 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 [53] and [71], where the latter one contains a self–contained treatment.

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 $\hat{\mathcal{X}} \to \mathcal{X} \stackrel{\pi}{\to} \mathbb{P}^1(\mathbb{C})$, 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 $\gamma_1, \gamma_2, \ldots, \gamma_r$ of the fundamental group Γ of $\mathbb{P}^1(\mathbb{C}) \setminus \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ 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 $\gamma_1\gamma_2\ldots\gamma_r = 1$. 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 [53] and [71].

3.1.2 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 [59]. Later, Feit, Lyndon, and Scott gave an elementary group theoretic argument of this observation, see [18].

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 [61]. For bigger groups, especially certain sporadic groups, we can use the character tables in the atlas [8]. Here, and at other places, the following easy observation (see [54, 2.4]) is useful.

Lemma 3.1.1. *Let $\sigma \in G$, where G is a permutation group of degree n, then*

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

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

3.2 Some General Lemmas about Genus 0 Systems

Lemma 3.2.1. *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. □

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 $\tau_1, \ldots, \tau_{m-1}$ 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

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

where σ_2' is conjugate to σ_2^{-1}, and the τ_i' are transpositions. As $\mathrm{ind}(xy) \leq \mathrm{ind}(x)+\mathrm{ind}(y)$ and $(\sigma_1, \tau_1, \ldots, \tau_{m-1}, \rho^{-1})$ 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 $\lambda := \sigma_1\tau_1 \ldots \tau_{m-2}$ 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 $(\sigma_1, \tau_1, \ldots, \tau_{m-2}, \lambda^{-1})$ 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 $(\sigma_1, \tau_1, \ldots, \tau_{m-1})$ with d blocks being permuted cyclically. It remains to show that this block system is preserved also by $(\sigma_2', \tau_1', \ldots, \tau_{m-1}')$. 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.

Lemma 3.2.2. *Let $m \geq 3$ and fix a set Δ with $|\Delta| = m$. Let $\sigma_1, \sigma_2, \ldots, \sigma_r \in Sym(\Delta) \times Sym(\Delta)$ be a genus 0 system on $\Delta \times \Delta$. Write $\sigma_i = (a_i, b_i)$ with a_i, b_i acting on the first and second component, respectively. Then $b_1, \ldots, b_r$ is a genus 0 system on Δ (and likewise for a_i).*

Furthermore, suppose that σ_r has only two cycles on $\Delta \times \Delta$. Then a_r or b_r is an m–cycle. Assume that b_r is an m–cycle. If $B := <b_1, b_2, \ldots, b_r>$ is primitive on Δ, then B is cyclic.

Proof. Let $\sigma = (a, b)$ be one the elements σ_k. Let $\mu_1, \mu_2, \ldots$ and $\nu_1, \nu_2, \ldots$ be the cycle lengths of a and b, respectively. Clearly

$$\mathrm{ind}(\sigma) = m^2 - \sum_{i,j} \gcd(\mu_i, \nu_j), \tag{3.2}$$

hence

$$\begin{aligned}\operatorname{ind}(\sigma) &\geq m^2 - \sum_{i,j} \nu_j \\ &\geq m^2 - \sum_j m\nu_j \\ &= m \operatorname{ind}(b).\end{aligned}$$

Summing for $\sigma = \sigma_k$, $k = 1, 2, \ldots, r$, yields

$$2(m^2 - 1) \geq m \sum_k \operatorname{ind}(b_k),$$

hence $\sum_k \operatorname{ind}(b_k) \leq 2(m-1) + 2(1 - 1/m)$. But $\sum_k \operatorname{ind}(b_k)$ is an even integer $\geq 2(m-1)$, see Section 3.1.2, hence the b_k constitute a genus 0 system on Δ.

Now suppose that σ has only two cycles. Then $\operatorname{ind}(\sigma) = m^2 - 2$, so $\sum_{i,j} \gcd(\mu_i, \nu_j) = 2$ with the notation from above. As each summand on the left hand side is ≥ 1, either a_r or b_r is an m–cycle.

Suppose that b_r is an m–cycle. The previous argument shows that a_r is a product of two cycles. Assume that B is primitive, but not cyclic. We contend that

$$\operatorname{ind}(\sigma_k) \geq m \operatorname{ind}(b_k) + \operatorname{ind}(a_k) \text{ for all } 1 \leq k \leq r-1. \tag{3.3}$$

Suppose that is not the case for some $\sigma = \sigma_k$. Then, with the notation from above,

$$\begin{aligned}m^2 - \sum_{i,j} \gcd(\mu_i, \nu_j) &< m \sum_j (\nu_j - 1) + \sum_i (\mu_i - 1) \\ &= m^2 - m \sum_j 1 + \sum_i (\mu_i - 1) \\ &= m^2 - \sum_{i,j} \mu_i + \sum_i (\mu_i - 1).\end{aligned}$$

Hence there is a least one index i such that

$$\sum_j \gcd(\mu_i, \nu_j) > \sum_j \mu_i + 1 - \mu_i.$$

Note that this gives $\mu_i > 1$. Rewrite this inequality as

$$\sum_j (\mu_i - \gcd(\mu_i, \nu_j)) < \mu_i - 1.$$

Let w be the number of those j such that μ_i does not divide ν_j. Clearly, $\mu_i - \gcd(\mu_i, \nu_j) \geq \mu_i/2$ for those j, so

$$w\mu_i/2 \leq \sum_j (\mu_i - \gcd(\mu_i, \nu_j)) < \mu_i - 1,$$

hence $w \leq 2(\mu_i - 1)/\mu_i < 2$, so $w \leq 1$. Suppose $w = 1$, so there is exactly one index j_0 with μ_i not dividing ν_{j_0}. We obtain $d := \gcd(\mu_i, \nu_{j_0}) > \mu_i + 1 - \mu_i = 1$. So the integer $d > 1$ divides all the numbers ν_j, and if $w = 0$, we may take $d := \mu_i > 1$. As d does also divide m, and b_r is an m–cycle by assumption, we get inequality (3.3) in view of Lemma 3.2.1.

Note that

$$\begin{aligned} \operatorname{ind}(\sigma_r) &= m^2 - 2 \\ &= m(m-1) + (m-2) \\ &= m \operatorname{ind}(b_r) + \operatorname{ind}(a_r), \end{aligned}$$

so we have equality in (3.3) for $k = r$. Compute the sum of (3.3) for $k = 1, 2, \ldots, r$ to obtain

$$\begin{aligned} 2(m^2 - 1) &= \sum_{k=1}^{r} \operatorname{ind}(\sigma_k) \\ &\geq \sum_{k=1}^{r} (m \operatorname{ind}(b_k) + \operatorname{ind}(a_k)) \\ &= m(2(m-1)) + 2(m-1) \\ &= 2(m^2 - 1). \end{aligned}$$

As we obtain equality, we have equality everywhere. In particular, the proof of (3.3) shows that that for any $\sigma = \sigma_k$, $k = 1, 2, \ldots, r-1$, the following holds:

> For each i, either $\mu_i = 1$, or there is exactly one j such that μ_i does not divide ν_j.

For $k = 1, 2, \ldots, r-1$, let m_k be the maximum of the μ_i associated to σ_k. It follows that $m_k \leq \nu_j$ for all but at most one index j_0. So summing up for all $j \neq j_0$, we obtain

$$(m - \mathrm{ind}(b_k) - 1)m_k \leq m - m_{j_0} \leq m - 1.$$

Now divide by m_k and sum up for $k = 1, 2, \ldots, r$ to obtain

$$\sum_{k=1}^{r-1}(1 - \frac{1}{m_k}) \leq 1.$$

This shows that there are at most 2 indices k with $m_k > 1$, and if there are two of them, then $m_k = 2$ for these indices. On the other hand, as a_r is a product of two cycles, so in particular $<a_r>$ is intransitive, there must be at least two non–trivial elements among $a_1, a_2, \ldots, a_{r-1}$. This shows that among these a_k, there are precisely two involutions. Thus $A := <a_1, a_2, \ldots, a_r>$ is a dihedral group of order $2\mathrm{ord}(a_r)$. However, m is relatively prime to the cycle lengths of a_r, hence $\gcd(m, \mathrm{ord}(a_r)) = 1$. But m divides $|A| = 2\mathrm{ord}(a_r)$ by transitivity, contrary to $m > 2$. □

3.3 Genus 0 Systems for Affine Action

In order to apply results by Guralnick, Neubauer, and Thompson on genus 0 systems in primitive permutation groups of affine type we need the following

Lemma 3.3.1. *Let A be a primitive affine permutation group of degree $n > 2$, and G be a normal subgroup of A which contains an element σ with only two cycles. Then G is primitive, or one of the following holds:*

(a) $A = \mathcal{A}_4$ or $\mathcal{S}_4$ on 4 points, $G = C_2 \times C_2$.

(b) $p \geq 3$ is prime, $A = (\mathrm{AGL}_1(p) \times \mathrm{AGL}_1(p)) \rtimes C_2$ in product action of degree p^2, $G = \mathrm{AGL}_1(p) \times \mathrm{AGL}_1(p)$.

Proof. The case $n = 4$ is obvious, thus suppose $n \neq 4$. Theorem 2.4.9 lists the possibilities for A. Use the notation from this theorem. First suppose that $A = (\mathrm{AGL}_1(p) \times \mathrm{AGL}_1(p)) \rtimes C_2$ in product action, so (c) of Theorem 2.4.9 holds. As the cycle lengths of σ are distinct, we must have $\sigma \in \mathrm{AGL}_1(p) \times \mathrm{AGL}_1(p)$. Let $\Delta_1 \times \Delta_2$ be the product structure preserved by A. The proof

of Theorem 2.5.5 shows that σ acts as a $(p-1)$–cycle on Δ_1, and as a p–cycle on Δ (or vice versa). Let τ be the element in A which switches Δ_1 and Δ_2. Then also $\sigma^\tau \in G$, thus G restricted to Δ_i is doubly transitive for $i = 1$ and 2. Clearly $\mathrm{AGL}_1(p) \times \mathrm{AGL}_1(p) \leq G$, so possibility (b) holds.

If σ has a fixed point, then G is clearly doubly transitive, so in particular primitive. Thus assume that σ has no fixed point.

First consider that $A_1 = \mathrm{GL}_m(p)$ with $m \geq 2$ and $p \neq 2, 3$ if $m = 2$. As $G_1 \trianglelefteq A_1$, either $\mathrm{SL}_m(p) \leq G_1$, and thus G is primitive, or G_1 is a group of scalar matrices. But then each element in G is either a translation by a vector, so has $p^m/p = p^{m-1} > 2$ cycles, or has a fixed point, contrary to $\sigma \in G$.

Check the claim directly in the finitely many remaining cases of Theorem 2.4.9. □

Proposition 3.3.2. *Let A be a primitive affine permutation group of degree $n > 2$, and G be a normal subgroup of A which admits a genus 0 system $(\sigma_1, \sigma_2, \ldots, \sigma_r)$. Let $T := (ord(\sigma_1), ord(\sigma_2), \ldots, ord(\sigma_r))$ be the type of this system. Suppose that σ_r has exactly two cycles. Then one of the following holds:*

(a) $n = 3$, $G = \mathcal{S}_3 = A$, $T = (2, 2, 3)$, *or* $(2, 2, 2, 2)$.

(b) $n = 4$, $G = C_2 \times C_2 < A \leq \mathcal{S}_4$, $T = (2, 2, 2)$.

(c) $n = 4$, $G = \mathcal{A}_4 \leq A \leq \mathcal{S}_4$, $T = (2, 3, 3)$, $(3, 3, 2)$, *or* $(3, 3, 3)$.

(d) $n = 4$, $G = \mathcal{S}_4 = A$, $T = (2, 4, 3)$, $(2, 2, 3, 3)$, $(2, 2, 2, 2, 3)$, $(2, 2, 2, 3)$, *or* $(2, 2, 2, 2, 2)$.

(e) $n = 5$, $G = \mathrm{AGL}_1(5) = A$, $T = (2, 4, 4)$.

(f) $n = 7$, $G = \mathrm{AGL}_1(7) = A$, $T = (2, 3, 6)$.

(g) $n = 8$, $G = \mathrm{A\Gamma L}_1(8) = A$, $T = (3, 3, 6)$, *or* $(3, 3, 7)$.

(h) $n = 8$, $G = \mathrm{AGL}_3(2) = A$, $T = (3, 4, 7)$, $(2, 6, 7)$, *or* $(2, 4, 7)$, $(4, 4, 7)$, $(2, 7, 7)$, $(2, 2, 2, 7)$, $(2, 2, 3, 7)$, $(2, 2, 4, 7)$, $(2, 2, 2, 2, 7)$, $(2, 7, 6)$, $(3, 4, 6)$, $(4, 4, 6)$, $(2, 2, 3, 6)$, $(2, 2, 4, 6)$, $(2, 2, 2, 2, 6)$, $(2, 4, 7)$, $(3, 4, 4)$, $(4, 4, 4)$, $(2, 2, 3, 4)$, $(2, 2, 4, 4)$, *or* $(2, 2, 2, 2, 4)$.

(i) $n = 9$, $G = (\mathcal{S}_3 \times \mathcal{S}_3) \rtimes C_2 = A$, $T = (2, 4, 6)$, *or* $(2, 2, 2, 6)$.

(j) $n = 9$, $G = \mathrm{A\Gamma L}_1(9) = A$, $T = (2, 4, 8)$.

(k) $n = 9$, $G = \mathrm{AGL}_2(3) = A$, $T = (2, 3, 8)$, $(2, 6, 8)$, *or* $(2, 2, 2, 8)$.

(l) $n = 16$, $G = A$, $[\Gamma\mathrm{L}_1(16) : A_1] = 3$, $T = (2, 4, 8)$.

(m) $n = 16$, $G_1 = (C_3 \times C_3) \rtimes C_4 \leq A_1 \leq (\mathcal{S}_3 \times \mathcal{S}_3) \rtimes C_2$, $T = (2, 4, 8)$.

(n) $n = 16$, $G = (\mathcal{S}_4 \times \mathcal{S}_4) \rtimes C_2 = A$, $T = (2, 6, 8)$, $(2, 2, 2, 8)$, $(2, 4, 12)$, *or* $(2, 2, 2, 12)$.

(o) $n = 16$, $G_1 = \mathcal{S}_5 = A_1$, $T = (2, 5, 8)$, $(2, 6, 8)$, $(2, 2, 2, 8)$, $(2, 4, 12)$, $(2, 5, 12)$, $(2, 6, 12)$, *or* $(2, 2, 2, 12)$.

(p) $n = 16$, $G = \mathrm{A\Gamma L}_2(4) = A$, $T = (2, 4, 15)$.

(q) $n = 16$, $G_1 = \mathcal{A}_7 = A_1$, $T = (2, 4, 14)$.

(r) $n = 16$, $G = \mathrm{AGL}_4(2) = A$, $T = (2, 5, 14)$, $(2, 6, 14)$, $(2, 2, 2, 14)$, $(2, 4, 15)$, $(2, 5, 15)$, $(2, 6, 15)$, *or* $(2, 2, 2, 15)$.

(s) $n = 32$, $G = \mathrm{AGL}_5(2) = A$, *probably several possibilities for* T.

(t) $n = 64$, $G = \mathrm{AGL}_6(2) = A$, *probably several possibilities for* T.

Proof. The cases that A has degree ≤ 4 are immediate, so assume $n \geq 5$.

Let N be the minimal normal subgroup of A. We start by assuming that G is primitive. 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 $q \leq 7$, yielding the cases (e) and (f).

Next suppose that $G'' > 1$, but still G is primitive. Write $n = p^m$. We use [27, 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 [58, Theorem

1.5] (the statement is already in [27], 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 2.4.9.

So we have $p = 3$ or 2. Suppose that $p = 3$. Use [58, Theorem 1.5] to see that necessarily $n = 9$. Check directly that only the cases listed as (i), (j), and (k) are possible.

Now suppose $p = 2$. By [26], we automatically get $n \leq 64$. The cases for $n \leq 16$ are small enough to be checked with GAP. The cases which we could not check but which do not deserve a closer analysis are those listed in (s) and (t).

Finally, if G is imprimitive, then $G = \mathrm{AGL}_1(p) \times \mathrm{AGL}_1(p)$ in product action by Lemma 3.3.1, and there is no genus 0 system of the required type by Lemma 3.2.2. □

3.4 Genus 0 Systems for Product Action

Proposition 3.4.1. *Let A be a primitive non–affine permutation group in product action. Let G be a normal subgroup of A which admits a genus 0 system $(\sigma_1, \sigma_2, \ldots, \sigma_r)$. Suppose that σ_r has exactly two cycles. Then $G = (\mathcal{S}_m \times \mathcal{S}_m) \rtimes C_2 = A$.*

Proof. By Theorem 2.5.5, 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 $p \geq 5$. It follows from Lemma 3.2.2 that 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 2.5.5, 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 $\Delta := \{1, 2, \ldots, m\}$. Let $\tau \in G$ be the element which maps (i, j) to (j, i). Let $1 \leq a < m$ be prime to m. For $\alpha := (1, 2, \ldots, m) \in \mathcal{S}_m$ and $\beta := (a, a-1, \ldots, 2, 1)(m, m-1, \ldots, a+2, a+1) \in \mathcal{S}_m$ 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 3.1.1 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 $\sigma_1, \ldots, \sigma_{r-1}$ 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. □

3.5 Genus 0 Systems for Almost Simple Action

Proposition 3.5.1. *Let A be a primitive permutation group of degree $n > 2$, such that $S \leq A \leq \mathrm{Aut}(S)$ for a simple, non–abelian group S. Let G be a normal subgroup of A which admits a genus 0 system $(\sigma_1, \sigma_2, \ldots, \sigma_r)$. Let $T := (ord(\sigma_1), ord(\sigma_2), \ldots, ord(\sigma_r))$ be the type of this system. Suppose that σ_r has exactly two cycles. Then one of the following holds:*

(a) $n \geq 5$, $\mathcal{A}_n \leq G \leq A \leq \mathcal{S}_n$ *in natural action. Many (unclassifiable) possibilities for* T.

(b) $n = 6$, $G = \mathrm{PSL}_2(5) \leq A \leq \mathrm{PGL}_2(5)$, $T = (2,3,5)$, $(2,5,5)$, $(2,2,2,5)$, $(2,5,3)$, *or* $(2,2,2,3)$.

(c) $n = 6$, $G = \mathrm{PGL}_2(5) = A$, $T = (2,4,5)$, $(4,4,5)$, *or* $(4,4,3)$.

(d) $n = 8$, $G = \mathrm{PSL}_2(7) \leq A \leq \mathrm{PGL}_2(7)$, $T = (2,3,7)$, $(3,3,7)$, *or* $(3,3,4)$.

(e) $n = 8$, $G = \mathrm{PGL}_2(7) = A$, $T = (2,6,7)$, *or* $(2,6,4)$.

(f) $n = 10$, $G = \mathcal{A}_5 \leq A \leq \mathcal{S}_5$, $T = (2,3,5)$.

(g) $n = 10$, $G = \mathcal{S}_5 = A$, $T = (2,4,5)$, $(2,6,5)$, *or* $(2,2,2,5)$.

(h) $n = 10$, $G = \mathrm{PSL}_2(9) \leq A \leq \mathrm{P\Gamma L}_2(9)$, $T = (2,4,5)$.

(i) $n = 10$, $G = \mathrm{P\Sigma L}_2(9) \leq A \leq \mathrm{P\Gamma L}_2(9)$, $T = (2,6,5)$, *or* $(2,2,2,5)$.

(j) $n = 10$, $G = \mathrm{M}_{10} \leq A \leq \mathrm{P\Gamma L}_2(9)$, $T = (2,4,8)$.

(k) $n = 10$, $G = \mathrm{P\Gamma L}_2(9) = A$, $T = (2,8,8)$.

(l) $n = 12$, $G = \mathrm{M}_{11} = A$, $T = (2,5,8)$, $(2,6,8)$, $(3,3,8)$, $(2,2,2,8)$, $(2,4,11)$, $(2,5,11)$, $(2,6,11)$, *or* $(2,2,2,11)$.

(m) $n = 12$, $G = \mathrm{M}_{12} = A$, *many possibilities for* T.

(n) $n = 14$, $G = \mathrm{PSL}_2(13) \leq A \leq \mathrm{PGL}_2(13)$, $T = (2,3,7)$, *or* $(2,3,13)$.

(o) $n = 21$, $G = \mathrm{P\Sigma L}_3(4) \leq A \leq \mathrm{P\Gamma L}_3(4)$, $T = (2,4,14)$.

(p) $n = 21$, $G = \mathrm{P\Gamma L}_3(4) = A$, $T = (2,3,14)$, $(2,6,14)$, *or* $(2,2,2,14)$.

(q) $n = 22$, $G = \mathrm{M}_{22} \leq A \leq \mathrm{M}_{22} \rtimes C_2$, $T = (2,4,11)$.

(r) $n = 22$, $G = \mathrm{M}_{22} \rtimes C_2 = A$, $T = (2,4,11)$, $(2,6,11)$, *or* $(2,2,2,11)$.

(s) $n = 24$, $G = \mathrm{M}_{24} = A$, *many possibilities for* T.

(t) $n = 40$, $G = \mathrm{PSL}_4(3) \leq A \leq \mathrm{PGL}_4(3)$, $T = (2,3,20)$.

(u) $n = 40$, $G = \mathrm{PGL}_4(3) = A$, $T = (2, 4, 20)$.

Proof. We have to check the groups in Theorem 2.8.1 for the existence of genus 0 systems of the required form.

If $S = \mathcal{A}_n$ 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 (b), (e), (f), (g), (h), (i), (j) of Theorem 2.8.1 are easily dealt with, using the atlas [8] and some easy ad hoc arguments, or more conveniently using [61].

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. [54]) 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 2.8.29. 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 [54]. This

information, combined with the index relation, gives

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

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 [54]) or simply check with [61] that $q = 25$ does not occur.

The main case which is left to investigate is (d) of Theorem 2.8.1, 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 proof of Proposition 3.5.1, we need to show that $m = 4$, $q = 3$, giving the cases (t) and (u) in that proposition.

For this we need the following index bounds.

Lemma 3.5.2. *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:*

(a) $\mathrm{ind}(\sigma) \geq (1-1/ord(\sigma))(q^{m-1}-1)$.

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

(c) If $ord(\sigma)$ is a prime dividing q, and $\sigma \in \mathrm{PGL}_m(q)$, then $\mathrm{ind}(\sigma) = (1-1/ord(\sigma))(q^m-q^j)/(q-1)$ *for some* $1 \leq j \leq m-1$.

Proof. For (a) see [54].

Set $N := (q^m-1)/(q-1)$, and let s be the order of σ.

Now assume the hypothesis in (b). 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 $\chi(\sigma) \leq (q^d - 1)/(q - 1)$, 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 $d \leq m - 2$, and the claim follows.

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

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

$$\sum_{k=1}^{r-1} \mathrm{ind}(\sigma_k) = N. \tag{3.4}$$

Claim 3.5.3. $r = 3$.

Proof. Suppose that $r \geq 4$. From (a) in Lemma 3.5.2 we have $\mathrm{ind}(\sigma_k) \geq (1 - 1/\mathrm{ord}(\sigma_k))(q^{m-1} - 1)$, hence

$$\begin{aligned} \sum_{k=1}^{r-1} (1 - 1/\mathrm{ord}(\sigma_k)) &\leq \frac{N}{q^{m-1} - 1} \\ &= 1 + \frac{1}{q-1} + \frac{1}{q^{m-1} - 1} \\ &\leq 1 + \frac{1}{q-1} + \frac{1}{q^3 - 1} \\ &< 1 + \frac{2}{q-1}. \end{aligned} \tag{3.5}$$

First note that if $r \geq 4$, then $3/2 < 1 + \frac{2}{q-1}$, so $q < 5$ and hence $q = 3$. We get more precisely $\sum_{k=1}^{r-1}(1 - 1/\mathrm{ord}(\sigma_k)) \leq 1 + 1/(3-1) + 1/(27-1) = 20/13$. However, $2(1 - 1/2) + (1 - 1/3) = 5/3 > 20/13$, so besides $q = 3$ we obtain

$r = 4$, and σ_1, σ_2, σ_3 are involutions. Note that σ_4 has cycles of even length, as $4|N$. So these involutions do have fixed points by Lemma 3.2.1. 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

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

a contradiction. □

Claim 3.5.4. $q \leq 7$.

Proof. From (3.5) and $r = 3$ we obtain

$$\frac{1}{\mathrm{ord}(\sigma_1)} + \frac{1}{\mathrm{ord}(\sigma_2)} \geq 1 - \frac{1}{q-1} - \frac{1}{q^{m-1}-1} \geq 1 - \frac{1}{q-1} - \frac{1}{q^3-1}. \quad (3.6)$$

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

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

Claim 3.5.5. $q \neq 7$.

Proof. Suppose $q = 7$. From (3.5) 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 3.5.6. $q \neq 5$.

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 3.2.1, 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 3.1.1 gives

$$2\chi(\sigma_1) + 2\chi(\sigma_2) + \chi(\sigma_2^2) = N. \tag{3.7}$$

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 3.2.1, 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 (3.7) 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

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

a contradiction as previously. □

Claim 3.5.7. *If $q = 3$, then $m = 4$ and $(ord(\sigma_1), ord(\sigma_2)) = (2,3)$ or $(2,4)$.*

Proof. As $\mathrm{ind}(\sigma_k) \geq (3^{m-1}-1)/2$, and $\mathrm{ind}(\sigma_k) \geq 2(3^{m-2}-1)$ unless σ_k is an involution in $\mathrm{PGL}_m(3)$ of minimal possible index, we obtain from the index relation (3.4) that

$$\mathrm{ind}(\sigma_k) \leq \begin{cases} 3^{m-1} \text{ in any case,} \\ \frac{5\cdot 3^{m-2}+3}{2} \text{ for } k=2 \text{ if } \sigma_1 \text{ has not minimal possible index.} \end{cases} \tag{3.8}$$

We first note that no prime $s \geq 5$ does divide $\mathrm{ord}(\sigma_k)$, for (3.8) and Lemma 3.5.2(b) would give

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

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 2.4.1. Thus $\chi(\sigma) \leq (3^{m-3}-1)/2$, and also $\chi(\sigma^3) \leq (3^{m-1}-1)/2$. Now

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

by Lemma 3.1.1. Use the above estimation to obtain after some calculation that $\mathrm{ind}(\sigma) \geq 32 \cdot 3^{m-4} > 3^{m-1}$, contrary to (3.8).

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 3.2.1, 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 $2 \leq a+b \leq m-2$. 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

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

Note that $\mathrm{ind}(\sigma_k) \geq \mathrm{ind}(\sigma)$. From that we see that $k = 2$, and by (3.8) it follows that σ_1 is an involution with minimal possible index. Thus $\mathrm{ind}(\sigma_2) = 3^{m-1}$ again by (3.8). 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 (3.8).

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

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

and

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

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 (3.8), 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 (3.8) that $k = 2$ and σ_1 is an involution with minimal index. So $\mathrm{ind}(\sigma_2) = 3^{m-1}$ by (3.4), 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 3.5.2(c), 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 3.2.1 shows that σ_1 has fixed points. Then $\mathrm{ind}(\sigma_1) = (3^m - 3^i - 3^{m-i} + 1)/4$, where $1 \leq i \leq m - 1$ 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 $2 \leq i \leq m - 2$. 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. □

This previous claim finishes the proof of Proposition 3.5.1. □

3.6 Genus 0 Systems with n–Cycle

We will need the following

Proposition 3.6.1. *Let G be a non–trivial normal subgroup of a primitive permutation group of degree n, such that G admits a genus 0 system $(\sigma_1, \sigma_2, \ldots, \sigma_r)$. Let $T := (ord(\sigma_1), ord(\sigma_2), \ldots, ord(\sigma_r))$ be the type of this system, and suppose that σ_r is an n–cycle. Then one of the following holds:*

(a) Infinite series:

(i) $n = p$, $G = C_p$, $T = (p, p)$, *p a prime.*

(ii) $n = p$, $G = D_p$, $T = (2, 2, p)$, *p an odd prime.*

(iii) $G = \mathcal{A}_n$ *(n odd) or* $\mathcal{S}_n$, *many possible types.*

(b) Davenport polynomial cases (see Section 4.5):

(i) $n = 7$, $G = \mathrm{PGL}_3(2)$, $T = (2, 3, 7)$, $(2, 4, 7)$, *or* $(2, 2, 2, 7)$.

(ii) $n = 11$, $G = \mathrm{PSL}_2(11)$, $T = (2, 3, 11)$.

(iii) $n = 13$, $G = \mathrm{PGL}_3(3)$, $T = (2, 3, 13)$, $(2, 4, 13)$, $(2, 6, 13)$, *or* $(2, 2, 2, 13)$.

(iv) $n = 15$, $G = \mathrm{PGL}_4(2)$, $T = (2, 4, 15)$, $(2, 6, 15)$, *or* $(2, 2, 2, 15)$.

(v) $n = 21$, $G = \mathrm{P\Gamma L}_3(4)$, $T = (2, 4, 21)$.

(vi) $n = 31$, $G = \mathrm{PGL}_5(2)$, $T = (2, 4, 31)$.

(c) Sporadic cases:

(i) $n = 6$, $G = \mathrm{PGL}_2(5)$, $T = (2, 4, 6)$.

(ii) $n = 8$, $G = \mathrm{PGL}_2(7)$, $T = (2, 3, 8)$.

(iii) $n = 9$, $G = \mathrm{P\Gamma L}_2(8)$, $T = (2, 3, 9)$ *or* $(3, 3, 9)$.

(iv) $n = 10$, $G = \mathrm{P\Gamma L}_2(9)$, $T = (2, 4, 10)$.

(v) $n = 11$, $G = \mathrm{M}_{11}$, $T = (2, 4, 11)$.

(vi) $n = 23$, $G = \mathrm{M}_{23}$, $T = (2, 4, 23)$.

Proof. Let A be the primitive group where G is the normal subgroup of, and set $C := <\sigma_r>$. The result follows from [54] once we know that G is primitive. But this is the case. Namely let S be a block system of G. Then S consists of the orbits of a subgroup of C. As C is cyclic, S is the unique block system of this size. On the other hand, for $a \in A$, $S^a = \{\Delta^a | \ \Delta \in S\}$ is a block system of G as well. Thus S is a block system of A, and hence a trivial one, because A is primitive. □

Chapter 4

Rationality Questions

To ease the language in the following, we make the

Definition 4.0.2. Let k be a number field, and $g(Z) \in k(Z)$ be a non–constant rational function. Choose a transcendental t, let L be a splitting field of $g(Z) - t$ over $k(t)$, and $\hat{k}$ the algebraic closure of k in L. Then $A := \mathrm{Gal}(L/k(t))$ and $G := \mathrm{Gal}(L/\hat{k}(t))$ are the *arithmetic* and *geometric monodromy group* of g over k, respectively. We regard both groups as permutation groups on the roots of $g(Z) - t$. Note that $A/G \cong \mathrm{Gal}(\hat{k}/k)$. (This notion is motivated by the fact that the geometric monodromy group can be seen as the monodromy group in the usual sense defined by the branched covering $\mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$, $z \mapsto g(z)$ of Riemann spheres, see Section 3.1.1.)

4.1 Siegel Functions

Let k be a number field, and $f(X,t) \in k(t)[X]$ be an irreducible polynomial over $k(t)$. Proposition 1.1.1 gives a description of the set $\mathcal{R}$ of specializations $t_0 \in \mathcal{O}_k$, such that $f(X,t_0)$ becomes reducible, as a union of a finite set and finitely many infinite sets of the form $g(k) \cap \mathcal{O}_k$, where $g(Z) \in k(Z)$ is a rational function. The condition that g assumes infinitely many values in $\mathcal{O}_k$ on k is quite strong, and puts severe restrictions on the form of g. This basic result is due to Siegel [66].

Proposition 4.1.1. *Let k be a number field, $\mathcal{O}_k$ its ring of integers, and let $g(Z) \in k(Z)$ be a rational function such that $|g(k) \cap \mathcal{O}_k| = \infty$. Then $|g^{-1}(\infty)| \leq 2$.*

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

Remark. It is easy to see that not much more can be said about g, see the proof of Lemma 5.2.5.

As is clear from the Galois theoretic setup in Lemma 1.2.1, the monodromy groups of rational functions g as above will play a crucial role. The arithmetic and geometric monodromy groups of rational functions over k do not change if we compose the rational function with linear fractional functions over k. We will frequently take advantage of this trivial fact without further notice.

Definition 4.1.2. Let k be a number field, and $g(Z) \in k(Z)$ be a non–constant rational function. Suppose there is $\alpha \in \mathbb{P}^1(k)$ such that $j := |g^{-1}(\alpha)| \leq 2$. We call $g(Z)$ a *Siegel function of the first kind* if $j = 1$. We say that $g(Z)$ is a *Siegel function of the second kind* if $j = 2$, where for $k = \mathbb{Q}$ we additionally require that the elements in $g^{-1}(\alpha)$ are real and algebraically conjugate. Also, g is called a *Siegel function* if it is a Siegel function of first or second kind.

Remark 4.1.3. It follows immediately from the definition that a Siegel function of the first kind is of the form $\lambda(h(\mu(Z)))$, where $h(Z) \in k[Z]$ is a polynomial, and λ, μ are linear fractional functions over k.

The following lemma is almost trivial.

Lemma 4.1.4. *Let $g(Z) = a(b(Z))$ with $a, b \in k(Z)$ non–constant rational functions, and assume that g is a Siegel function.*

If g is of first kind, then a and b are Siegel functions of the first kind.

If g is of second kind, then either a and b are Siegel functions of the first and second kind, respectively; or a is a Siegel function of the second kind, and $b(Z) = \lambda((\mu(Z))^m)$ for $m \in \mathbb{N}$ and linear fractional functions $\lambda, \mu \in \bar{k}(Z)$.

Proof. Use the notation from the definition. We have $g^{-1}(\alpha) = b^{-1}(a^{-1}(\alpha))$. If $|g^{-1}(\alpha)| = 1$, then clearly g, a, and b are Siegel functions of the first kind.

Thus assume that $g^{-1}(\alpha) = \{\gamma_1, \gamma_2\}$ with $\gamma_1 \neq \gamma_2$. Clearly $|a^{-1}(\alpha)| \leq 2$. If $a^{-1}(\alpha) = \{\beta\}$, then $\beta \in \mathbb{P}^1(k)$, and a is a Siegel function of the first kind, whereas b is a Siegel function of the second kind.

Next assume that $a^{-1}(\alpha) = \{\beta_1, \beta_2\}$, with $\beta_1 \neq \beta_2$. Then $|b^{-1}(\beta_i)| = 1$ for $i = 1, 2$, so the extension $\bar{k}(Z)/\bar{k}(b(Z))$ has the two totally ramified

places $b(Z) \mapsto \beta_i$. This implies that b is a linear fractional twist of a cyclic polynomial. Furthermore, if $k = \mathbb{Q}$, then the β_i are real and algebraically conjugate, because $b(g^{-1}(\alpha)) = \{\beta_1, \beta_2\}$. The claim follows. □

4.2 A Galois Theoretic Existence Criterion

If $g(Z) \in \mathbb{Q}(Z)$ is a Siegel function of the second kind over $\mathbb{Q}$, then $\deg(g) = 2m$ and the geometric monodromy group contains an element which is a product of two m–cycles. This, together with an analysis of genus 0 systems, gives a fair constraint on possible monodromy groups. However, if we are working over the rationals, another powerful tool is available, namely the interplay between the inertia and decomposition groups at ramified rational places. Such considerations appear already in Shih [65] and Fried [21], see also [71, Lemma 2.8] and [53, Sect. I.2.3]. The following lemma summarizes the necessary properties which are being used most frequently in the following.

Lemma 4.2.1. *Let $k = \mathbb{Q}$ and $g(Z) \in \mathbb{Q}(Z)$ be a Siegel function of the second kind of degree $n = 2m \geq 2$, such that $g^{-1}(\alpha)$ consists of two real elements, which are algebraically conjugate in $\mathbb{Q}(\sqrt{d})$, for $\alpha \in \mathbb{P}^1(\mathbb{Q})$ and $d > 1$ a square-free integer. Let t be a transcendental over $\mathbb{Q}$, L a splitting field of $g(Z) - t$ over $\mathbb{Q}(t)$, $A := \mathrm{Gal}(L/\mathbb{Q}(t))$, and $G := \mathrm{Gal}(L/\hat{\mathbb{Q}}(t)) \trianglelefteq A$, where $\hat{\mathbb{Q}}$ is the the algebraic closure of $\mathbb{Q}$ in L. Consider A as a permutation group on the roots of $g(Z) - t$.*

Let $\mathfrak{P}$ be a place of L lying above the place $t \mapsto \alpha$ of $\mathbb{Q}(t)$. Let $D \leq A$ and $I \leq G$ be the decomposition and inertia group of $\mathfrak{P}$, respectively. Then $I = <\sigma>$ for some $\sigma \in G$, and the following holds.

(a) σ is a product of two m–cycles.

(b) σ^k is conjugate in D to σ for all k prime to m.

(c) D contains an element which switches the two orbits of I.

(d) D contains an involution τ, such that $\sigma^\tau = \sigma^{-1}$, and τ fixes the orbits of I setwise.

(e) 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.

Proof. Changing the argument of g by a linear fractional substitution over $\mathbb{Q}$ allows to assume that $\alpha = \infty$, and that the two elements in the fiber $g^{-1}(\infty)$ are $\pm\sqrt{d}$ for $d > 1$ square-free. Thus, without loss, assume that $g(Z) = h(Z)/(Z^2 - d)^m$, where $h(Z) \in \mathbb{Q}[Z]$ with $\deg(h) \leq 2m$, and $h(\pm\sqrt{d}) \neq 0$.

Let y be a transcendental over $\mathbb{Q}$, such that $y^m = 1/t$. Fix a square root $\sqrt{d}$ of d, and let $\varepsilon \in \{-1, 1\}$. Substituting $y\tilde{Z} + \varepsilon\sqrt{d}$ for Z in the equation $h(Z) - t \cdot (Z^2 - d)^m = 0$ gives

$$h(y\tilde{Z} + \varepsilon\sqrt{d}) - \tilde{Z}^m(y\tilde{Z} + 2\varepsilon\sqrt{d})^m = 0. \tag{4.1}$$

This latter equation, by Hensel's Lemma, is solvable in the power series ring $\overline{\mathbb{Q}}[[y]]$.

Thus, for $i = 1, 2, \ldots, m$ and $\varepsilon \in \{-1, 1\}$, we can represent the $2m$ roots of $g(Z) - t$ in the form

$$z_{i,\varepsilon} = \varepsilon\sqrt{d} + a_{1,\varepsilon}\zeta^i y + a_{2,\varepsilon}\zeta^{2i}y^2 + \cdots \in \overline{\mathbb{Q}}[[y]],$$

where ζ is a primitive m–th root of unity.

Thus L can be regarded as a subfield of $\overline{\mathbb{Q}}((y))$. Each automorphism of $\overline{\mathbb{Q}}((y))$ which fixes $y^m = 1/t$ then restricts to an element in $D \leq A$, and if it is the identity on $\overline{\mathbb{Q}}$, then the restriction to L lies in $I \leq G$.

We will now construct suitable automorphisms of $\overline{\mathbb{Q}}((y))$ which, when restricted to L, give the required actions on the roots of $g(Z) - t$.

To (a). Let $\hat{\sigma} \in \mathrm{Gal}(\overline{\mathbb{Q}}((y))/\overline{\mathbb{Q}}((y^m)))$ with $y^{\hat{\sigma}} = \zeta y$. Then the restriction $\sigma := \hat{\sigma}|_L$ acts as required, sending $z_{i,\varepsilon}$ to $z_{i+1,\varepsilon}$ (first index taken modulo m).

To (b). Let $\hat{\tau} \in \mathrm{Gal}(\overline{\mathbb{Q}}((y))/\mathbb{Q}((y)))$ with $\zeta^{\hat{\tau}} = \zeta^k$, and $\tau := \hat{\tau}|_L$. Then $\tau^{-1}\sigma\tau$ is the identity on $\overline{\mathbb{Q}}$, but $y^{\tau^{-1}\sigma\tau} = y^{\sigma\tau} = (\zeta y)^\tau = \zeta^k y$, so $\tau^{-1}\sigma\tau = \sigma^k$.

To (c). Choose $\hat{\tau} \in \mathrm{Gal}(\overline{\mathbb{Q}}((y))/\mathbb{Q}((y)))$ such that $\sqrt{d}^{\hat{\tau}} = -\sqrt{d}$.

To (d). Choose $\hat{\tau} \in \mathrm{Gal}(\overline{\mathbb{Q}}((y))/\mathbb{Q}((y)))$, such that the restriction of $\hat{\tau}$ to $\overline{\mathbb{Q}}$ is the complex conjugation for a fixed embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$. Then $k = -1$ in the notation of case (b).

To (e). If $\sqrt{d} \notin \mathbb{Q}(\zeta)$, then there is an element $\hat{\tau} \in \mathrm{Gal}(\overline{\mathbb{Q}}((y))/\mathbb{Q}((y)))$ such that $\hat{\tau}$ moves $\sqrt{d}$, but is the identity on $\mathbb{Q}(\zeta)$. Set $\tau := \hat{\tau}|_L$. This gives $k = 1$ in case (b). □

4.3 Monodromy Groups of Siegel Functions

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

Theorem 4.3.1. *Let $k = \mathbb{Q}$ and $g(Z) \in \mathbb{Q}(Z)$ be a functionally indecomposable Siegel function of second kind 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:*

(a) n is even, $\mathcal{A}_n \leq G \leq A \leq \mathcal{S}_n$, many possibilities for T; or

(b) $n = 6$, $G = \mathrm{PSL}_2(5)$, $A = \mathrm{PGL}_2(5)$, $T = (2,5,3)$ and $(2,2,2,3)$; or

(c) $n = 6$, $G = \mathrm{PGL}_2(5) = A$, $T = (4,4,3)$; or

(d) $n = 8$, $G = \mathrm{AGL}_3(2) = A$, $T = (2,2,3,4)$, $(2,2,4,4)$, and $(2,2,2,2,4)$; or

(e) $n = 10$, $S \leq G \leq A \leq \mathrm{Aut}(S)$, where $S = \mathcal{A}_5$ or $\mathcal{A}_6$, with many possibilities for T; or

(f) $n = 16$, $G = (S_4 \times S_4) \rtimes C_2 = A$, $T = (2,6,8)$, $(2,2,2,8)$; or

(g) $n = 16$, $G = C_2^4 \rtimes S_5 = A$, $T = (2,5,8)$, $(2,6,8)$, and $(2,2,2,8)$.

Proof. 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 4.2.1. 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. Proposition 3.3.2 gives the candidates for G and A and genus 0 systems. The only possible degrees are 4, 8, and 16.

Suppose $n = 4$. If $G = C_2 \times C_2$, then $T = (2,2,2)$, and the three involutions in $\mathcal{E}$ are pairwise not conjugate in G. As A is primitive, A contains a subgroup C of order 3. This subgroup permutes the elements in $\mathcal{E}$ cyclically. The branch cycle argument [71, Lemma 2.8], [53, Sect. I.2.3] shows that the three branch points of g are also permuted transitively by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, in particular they are all irrational, a contradiction.

The cases $G = A_4$ and S_4 are easily seen to occur.

Next 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 [51], 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 4.4.

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 4.2.1, are the ones listed in (m), (n), and (o) of Proposition 3.3.2.

We start excluding the first case, 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.

The cases (n) and (o) however have the required arithmetic realizations. As the proof involves a considerable amount of computations, we postpone the analysis to Section 4.4.

Now assume that A is an almost simple group. Suppose that A is neither the alternating nor the symmetric group in natural action. Proposition 3.5.1 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 4.2.1, 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 4.2.1 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 4.2.1, 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 $[A : G] \leq 2$. 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

$$\tilde{g}(Z) = \frac{(Z^2 + a_1 Z + a_0)(Z^2 + p_1 Z + p_0)^3}{Z^4}.$$

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 $a_0 p_0 \neq 0$, and the ramification information in the other finite branch point, this gives a 0–dimensional quasi affine variety. See [53, 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 $S \leq A \leq \mathrm{Aut}(S)$ 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. But see Example 5.2.11 for the case $S = \mathcal{A}_5$.

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 4.4 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 4.2.1 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 [53, Sect. I.1.1] or [23, §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

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

and a similar transformation formula holds if there is a pair of complex conjugate branch points. For this old result by Hurwitz , see [53, Theorem I.1.2], [23].

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 [64, 8.4.3] (which does not apply here), see [23] and [53, 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. □

The analogue of the previous theorem for Siegel functions of the first kind follows immediately from [54] and the observation that primitivity of A implies primitivity of G, see Proposition 3.6.1.

Theorem 4.3.2. *Let $k = \mathbb{Q}$ and $g(Z) \in \mathbb{Q}(Z)$ be a functionally indecomposable Siegel function of first kind 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:*

(a) n is a prime, $C_n = G \leq A = \mathrm{AGL}_1(n)$, $T = (n, n)$; or

(b) $n \geq 3$ is a prime, $D_n = G \leq A = \mathrm{AGL}_1(n)$, $T = (2, 2, n)$; or

(c) $n \geq 4$, $\mathcal{A}_n \leq G \leq A \leq \mathcal{S}_n$, *many possibilities for* T*; or*

(d) $n = 6$, $G = \mathrm{PGL}_2(5) = A$, $T = (2, 4, 6)$*; or*

(e) $n = 9$, $G = \mathrm{P\Gamma L}_2(8) = A$, $T = (3, 3, 9)$*; or*

(f) $n = 10$, $G = \mathrm{P\Gamma L}_2(9) = A$, $T = (2, 4, 10)$.

4.4 Computations

This section completes the proof of Theorem 4.3.1 in those cases which require or deserve some explicit computations besides theoretical arguments. We continue to use the notation from there.

4.4.1 $n = 8$, $G = \mathrm{AGL}_3(2)$.

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 [52]. 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[9] 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 $(2,2,3,4)$.

4.4.2 $n = 16$, $G = (S_4 \times S_4) \rtimes C_2$

Here $n = 16$, and $G = A = (S_4 \rtimes S_4) \rtimes C_2$ in product action of the wreath product $S_4 \wr C_2$. 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 $(2-2-2-2-2-2-2,2-3-3-6,8-8)$. 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 $G = A = S_4 \wr C_2$ 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 $S_4 \wr C_2$ 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 $\mathbb{Q}(t)$:

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

$$-54tW^3 + 16t^2.$$

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 $H(W,t) = 0$:

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

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 Proposition 3.3.2, 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 [53, 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. The following computations will display 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 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 $g(Z)$, parameterized 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.

4.4.3 $n = 16$, $G = C_2^4 \rtimes S_5$

Now $G = A = C_2^4 \rtimes S_5$, where the action of S_5 is on the S_5–invariant hyperplane of the natural permutation module for 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, $A = V \rtimes S_5$, where $V < \mathbb{F}_2^5$ is the hyperplane of vectors with coordinate sum 0, and S_5 permutes the coordinates naturally. This interpretation of A as a subgroup of the wreath product $C_2 \wr S_5$ 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 $h(Y) - t$, $i = 1, \ldots, 5$, 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 occuring 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 de-

scribed above. An example (as part of a 1–parameter family) is

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

4.4.4 $n = 12$, $G = \mathrm{M}_{12}$

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

$$\begin{aligned} F(X,t) \;=\; & X^{12} + 44088X^{10} + 950400X^9 + 721955520X^8 + \\ & 31696106112X^7 + (2t + 5460734649920)X^6 + \\ & 393700011065856X^5 + \\ & (-120180t + 20231483772508800)X^4 + \\ & (-2587680t + 911284967252689920)X^3 + \\ & (137561760t + 21295725373309787136)X^2 + \\ & (4418468352t + 183784500436675461120)X + \\ & t^2 + 31440107840t + 3033666001201482093568. \end{aligned}$$

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.

4.5 Davenport Polynomials

Let A be a finite group. Let U and V be subgroups of A which are not conjugate, and χ_U, χ_V be the permutation characters of the action of A on the coset space A/U and A/V, respectively. Then U and V are said to be *Kronecker conjugate* if $\chi_U(a) > 0$ if and only if $\chi_V(a) > 0$ for each $a \in A$. This group theoretic property appeared for the first time in work of Kronecker [41]. If $\chi_U = \chi_V$, clearly a stronger property, then U and V are said to be *arithmetically equivalent*. See [40] for a recent book on this subject.

Let k be a number field and $\mathcal{O}_k$ be the ring of integers of k. Let $f(X), g(Y)$ be polynomials over k, and t a transcendental over k. Let x and y be in an algebraic closure of $k(t)$ with $f(x) = g(y) = t$. Let L be the normal closure of $k(x, y)/k(t)$, and set $A := \mathrm{Gal}(L/k(t))$, $U := \mathrm{Gal}(L/k(x))$, $V := \mathrm{Gal}(L/k(y))$. We apply the group theoretic terms defined above to f and g, if the corresponding property holds for A, U, V.

By a well known result of Fried (see [20, Section 2], [24, 19.27], or [56, Theorem 2.3] for an improved statement and simpler proof), Kronecker conjugacy of f and g is equivalent to the following arithmetic property: For all but finitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}_k$, the following equality of value sets on residue fields holds: $f(\mathcal{O}_k/\mathfrak{p}) = g(\mathcal{O}_k/\mathfrak{p})$, but f, g do not differ by a linear substitution over k.

Following Fried, we say that such a polynomial $f(X) \in k[X]$ is a *Davenport polynomial*.

Fried gave a close study of Davenport polynomials which in addition are assumed to be functionally indecomposable. If this holds for f, then it is not hard to see that there is $g(X) \in k[X]$ such that f and g are even arithmetically equivalent.

The original question of Davenport was whether there are Davenport polynomials over the rationals. Fried [19] gave a nice argument, without using any deep group theoretic classification results, that there are none:

Proposition 4.5.1. *There are no functionally indecomposable Davenport polynomials over* $\mathbb{Q}$.

(This was extended in [56] to composition length 2. For composition length 3, however, there are already Davenport polynomials over $\mathbb{Q}$.)

Without restriction on k, one can read off the possible monodromy groups of indecomposable Davenport polynomials directly from Proposition 3.6.1. A part of this Proposition had been proved by Feit [16]. (See [54] for a variant avoiding the use of a false lemma in [16].) This result relies on the classification of the finite simple groups (which was not completed at that time; but a consequence of it, the list of doubly transitive permutation groups, was believed to be complete). Only the groups listed in part (b) of Proposition 3.6.1 admit a subgroup which is Kronecker conjugate (and indeed arithmetically equivalent) to a point stabilizer. In particular, indecomposable Davenport polynomials exist only for the degrees 7, 11, 13, 15, 21, 31.

Chapter 5

Results, Proofs, and Examples

In this final chapter we state and prove the main results of our work. Throughout this chapter, let k be a number field, and $f(X,t) \in k[X,t]$ be an irreducible polynomial of positive degree n in X. Let $\mathcal{O}_k$ be the ring of integers of k. Set $\mathcal{R} := \{t_0 \in \mathcal{O}_k | f(X,t_0) \text{ is reducible over } k\}$, and $\mathcal{L} := \{t_0 \in \mathcal{O}_k | f(X,t_0) \text{ has a root in } k\}$. So clearly $\mathcal{L} \subseteq \mathcal{R}$.

It follows easily from Siegel's Theorem [66] that $\mathcal{L}$ is finite if the genus of the curve $f(X,t) = 0$ is positive. (If the polynomial $f(X,t)$ is not absolutely irreducible, then $\mathcal{L}$ is finite anyway, though $\mathcal{R}$ need not be finite, see Remark 1.3.3.)

Our purpose is to show finiteness of $\mathcal{R} \setminus \mathcal{L}$ under rather general assumptions, and also to exhibit interesting examples where $\mathcal{R} \setminus \mathcal{L}$ is infinite. We consider $k = \mathbb{Q}$ as the case of main interest, but also display the results for general number fields.

5.1 Cofiniteness of Hilbert Sets

This section contains positive results in the sense that we show finiteness of $\mathcal{R}$ (or of $\mathcal{R} \setminus \mathcal{L}$ if the genus of $f(X,t) = 0$ is 0) under rather general assumptions.

Theorem 5.1.1. *Let A be the Galois group of $f(X,t)$ over $k(t)$ in its action on the roots of $f(X,t)$. Then $\mathcal{R} \setminus \mathcal{L}$ is finite, if one of the following conditions is fulfilled.*

(a) $k = \mathbb{Q}$, $\deg_X(f)$ *is a prime* $\neq 5$.

(b) $\deg_X(f)$ *is a prime* $\neq 5, 7, 11, 13, 31$.

(c) $\deg_X(f) \in \{7, 11, 13, 31\}$ *and* f *does not come from a Davenport polynomial as described in Example 5.2.10. This holds in particular if the genus of* $f(X,t) = 0$ *is positive.*

(d) $\deg_X(f) = 5$ *and* f *does not come from the construction given in Example 5.2.11. This holds in particular if the genus of* $f(X,t) = 0$ *is positive.*

(e) A *is the alternating or symmetric group in its natural action, and* $\deg_X(f) \neq 5$.

(f) $k = \mathbb{Q}$, A *is a simple group not isomorphic to an alternating group* $\mathcal{A}_n$.

(g) A *is a simple group not isomorphic to an alternating group* $\mathcal{A}_n$ *or* $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(11)$, $\mathrm{PSL}_2(13)$, $\mathrm{PSL}_3(3)$, $\mathrm{PSL}_4(3)$, $\mathrm{PSL}_5(2)$, M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

(h) $k = \mathbb{Q}$, A *acts primitively, and has a non–abelian composition factor which is not isomorphic to* $\mathcal{A}_j$ *(*$j \geq 5$*),* $\mathrm{PSL}_2(7)$, *or* $\mathrm{PSL}_2(8)$.

(i) A *acts primitively, and has a non–abelian composition factor which is not isomorphic to* $\mathcal{A}_j$ *(*$j \geq 5$*),* $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(8)$, $\mathrm{PSL}_2(11)$, $\mathrm{PSL}_2(13)$, $\mathrm{PSL}_3(3)$, $\mathrm{PSL}_3(4)$, $\mathrm{PSL}_4(3)$, $\mathrm{PSL}_5(2)$, $\mathrm{PSL}_6(2)$, M_{11}, M_{12}, M_{22}, M_{23}, M_{24}.

Proof. Suppose that $\mathcal{R} \setminus \mathcal{L}$ is infinite. Then clearly $n \geq 4$. Let $g_i(Z) \in k(Z)$ be the rational functions from Proposition 1.1.2. It follows from Proposition 1.1.2(a) and $|\mathcal{R} \setminus \mathcal{L}| = \infty$ that the polynomial $f(X, g(z))$ does not have a factor of degree 1 over $k(z)$ for at least one $g = g_i$. Fix this rational function g. We are going to use Lemma 1.2.1 and the notation introduced there. It follows that A_z is not conjugate to a subgroup of A_x in A.

We start by assuming that $\deg_X(f)$ is a prime p. Choose a subgroup $B \leq A$ such that A_z is a maximal subgroup of B. Set $W := A_x \cap B$. Note that $[B : W] = p$, and that the actions of B on the coset spaces B/A_z and B/W are faithful by Lemma 1.2.1(d) and (f). Let π_z and π_x be the corresponding isomorphisms, where $\pi_z(B)$ and $\pi_x(B)$ are the permutation groups B acting on B/A_z and B/W, respectively.

Note that the group B is not solvable, for if it were, then $C_p \leq \pi_x(B) \leq \mathrm{AGL}_1(p)$. But $\pi_x(A_z)$ is a maximal intransitive subgroup of $\pi_x(B)$, so $\pi_x(A_z)$

is conjugate to $\pi_x(W)$, and therefore A_z is conjugate to the subgroup W of A_x, a contradiction. (See [57, Lemma 5.5] for the elementary facts about $\mathrm{AGL}_1(p)$ implicitly used here.)

By a theorem of Burnside (see [31, II.3.6]) any transitive non–solvable permutation group of prime degree is doubly transitive. Thus $\pi_x(B)$ is doubly transitive. Write $g(Z) = a(b(Z))$ with $a, b \in k(Z)$, such that $K(b(z))$ is the fixed field of B. Set $y := b(z)$. As g is a Siegel function, either b is a Siegel function, or a composition of Z^m with linear fractional functions over $\bar{k}$, see Lemma 4.1.4. The latter case does not occur, for then $\pi_z(B) = \mathrm{Gal}(b(Z) - t/k(t)) \leq \mathrm{AGL}_1(m)$ were solvable.

Thus there is $\alpha \in \mathbb{P}^1(k)$ with $|b^{-1}(\alpha)| \leq 2$. We may and will assume that $\alpha = \infty$. Let $\sigma \in \pi_z(B)$ be an inertia generator belonging to the place $y \mapsto \infty$ of $k(y)$.

First consider the case $|b^{-1}(\infty)| = 1$, so b is (up to a composition with linear fractional functions over k) a polynomial, and $<\sigma>$ is transitive on the roots of $b(Z) - y$. As b is functionally indecomposable, so $\pi_z(B)$ is primitive, it follows from a theorem of Schur [73, 25.3] that $\pi_z(B)$ is doubly transitive. Now use Lemma 5.1.3 below and the fact that $A_z W \subsetneqq B$ (Lemma 1.2.1(c)) to conclude that the permutation characters of π_z and π_x are the same. In particular, $k(y, x)$ has genus 0, and as $\pi_x(\sigma)$ is a transitive cycle by equality of permutation characters, $k(y, x)$ is a rational function field $k(v)$ and there is a polynomial $\bar{b}(Z) \in k[Z]$ with $\bar{b}(v) = y$. In the terminology of Section 4.5, b and $\bar{b}$ are arithmetically equivalent. Such pairs do not exist if $k = \mathbb{Q}$, see Proposition 4.5.1, and do exist of prime degree p only for $p = 7, 11, 13$, and 31, see Section 4.5. In all these cases, the degree p group $\pi_x(B)$ is contained in $\mathcal{A}_p$, and as such it is a maximal subgroup. It follows from (e) proved below that A cannot act as alternating or symmetric group on A/A_x. Therefore $A = B$, and the possibilities are of the form as given in Example 5.2.10.

Next suppose $|b^{-1}(\infty)| = 2$, so b is a Siegel function of the second kind. If $k = \mathbb{Q}$, then conclude $p = 5$ as in [57]. Thus allow k to be arbitrary. Note that p divides $|B|$, because $[B : W] = p$. On the other hand, p does not divide $|A_z|$, because an element in A_z of order p would be a transitive cycle on B/W, contrary to $A_z W \subsetneqq B$. Therefore p divides $[B : A_z]$. We saw already that $\pi_x(B)$ is a doubly transitive non–solvable group. Therefore $\pi_x(B)$ is almost simple by a theorem of Burnside, see [73, Exercise 12.4]. So $\pi_z(B)$ is almost simple as well, and primitive by maximality of A_z in B. This primitive group $\pi_z(B)$, as an arithmetic monodromy group of $b(Z)$, contains a transitive normal subgroup admitting a genus 0 system with σ being part

of it. Proposition 3.5.1 classifies the possibilities. Except for $\mathcal{A}_5$ and $\mathcal{S}_5$ in the degree 10 action, all examples are doubly transitive. Suppose that $\pi_z(B)$ is doubly transitive. By Lemma 5.1.3 below, the degree of $\pi_z(B)$ is p as well. The only prime degree cases are for $\mathcal{A}_p$ or $\mathcal{S}_p$ in the natural action. However, these groups have a unique conjugacy class of subgroups of index p, so they do not occur.

Thus $\pi_z(B) = \mathcal{A}_5$ or $\mathcal{S}_5$ in the degree 10 action. The only intransitive subgroup of prime index in $\mathcal{A}_5$ or $\mathcal{S}_5$ is the stabilizer of the natural action, thus $p = 5$. See Example 5.2.11 for a discussion of this case. These arguments finish the cases (a), (b), (c), and (d).

Now we prove (e), so A acts naturally as an alternating group $\mathcal{A}_n$ or symmetric group $\mathcal{S}_n$ on A/A_x. As the action of A_z on A/A_x is intransitive with orbit lengths ≥ 2, we get that A_z stabilizes an m–set of A/A_x, where $2 \leq m \leq n-2$. A permutes transitively the m–sets of A/A_x, therefore there is a subgroup B with $A_z \leq B < A$, such that the action of A on A/B is equivalent to the action on the m–sets of A/A_x. The existence of $\sigma \in A$ having at most two cycles on A/B implies $n \leq 5$ (see Section 2.8.1, the part where A_1 is intransitive). So $n = 4$, because $n = 5$ is excluded here. The case $n = 4$ does not exist for $k = \mathbb{Q}$. For if it would exist, σ were a product of two 3–cycles (because $\mathcal{S}_4$ has no elements of order 6). However, the normalizer of $<\sigma>$ in A stabilizes the two orbits of $<\sigma>$, contrary to Lemma 4.2.1(c).

Now let us prove (f) and (g). Note that if $A = C_p$, a cyclic group of prime order, then clearly $\mathcal{R} = \mathcal{L}$. Thus assume that A is not abelian. Let $B \geq A_z$ be a maximal subgroup of A, and $\sigma \in A$ be an inertia generator belonging to the place $t \mapsto \infty$. So σ has at most two cycles on A/A_z, and therefore also at most two cycles on A/B. By Theorems 4.3.1 and 4.3.2, there are no possibilities if $k = \mathbb{Q}$; and if k is arbitrary, apply Propositions 3.5.1 and 3.6.1.

Finally, we show (h) and (i). By faithful action of A on A/A_x and A/A_z (Lemma 1.2.1(d) and (e)) and $\mathrm{Gal}(f(X,t)/k(t)) = A$, we get the composition factors of A once we know the composition factors of $\mathrm{Gal}(g(Z) - t/k(t))$. Let $g(Z) = g_1(g_2(\dots g_r(Z))\dots)$ be a decomposition of g into functionally indecomposable rational functions $g_i(Z) \in k(Z)$. Then each composition factor of $\mathrm{Gal}(g(Z) - t/k(t))$ is a composition factor of $\mathrm{Gal}(g_i(Z) - t/k(t))$ for a suitable i, see Glauberman's argument in [27, Prop. 2.1] for this fact which is less obvious than it might appear at a first glance.

By Lemma 4.1.4, each g_i is either a Siegel function or a linear fractional twist (over $\bar{k}$) of a cyclic polynomial Z^m. In the latter case, $\mathrm{Gal}(g_i(Z) -$

$t/k(t)$) is solvable, so does not contribute non–abelian composition factors. If however g_i is a Siegel function, then apply Theorem 4.3.1 and 4.3.2 for $k = \mathbb{Q}$, and Propositions 3.3.2, 3.4.1, 3.5.1, and 3.6.1 otherwise. □

A consequence of part (f) of the previous theorem is

Theorem 5.1.2. *Let $f(X,t) \in \mathbb{Q}[X,t]$ be irreducible with Galois group G, where G is a simple group not isomorphic to an alternating group or C_2. Then $\mathrm{Gal}(f(X,t_0)/\mathbb{Q}) = G$ for all but finitely many specializations $t_0 \in \mathbb{Z}$.*

Proof. Let $F(X,t)$ be a minimal polynomial of a primitive element of a splitting field L of $f(X,t)$ over $\mathbb{Q}(t)$, and x a root of $F(X,t)$. Without loss assume that $F(X,t) \in \mathbb{Z}[X,t]$ is monic in X. By Theorem 5.1.1(f), there are only finitely many $t_0 \in \mathbb{Z}$ such that $F(X,t_0)$ is reducible without a linear factor. Suppose the theorem is wrong. Then there are infinitely many integers t_0 such that $F(X,t_0)$ has a rational root. Thus, by Siegel's theorem (see the proof of Proposition 1.1.2), there is $z \in L$ such that $L = \mathbb{Q}(z)$ with $t = g(z)$, where $g(Z) \in \mathbb{Q}(Z)$ is a Siegel function. In particular, the group G contains a genus 0 system with respect to the regular action. But this is classically known (and very easy to prove) to occur only for the groups C_n, D_n, $\mathcal{A}_4$, $\mathcal{S}_4$, and $\mathcal{A}_5$. By the assumption on G, only $G = C_p$ for a prime $p \geq 3$ could be a possibility, and G would be a Siegel function of the first kind. However, this case is out too, because $G = \mathrm{AGL}_1(p)$ by rationality in G of an inertia generator belonging to the place $t \mapsto \infty$ (see Theorem 4.3.2). □

Above we used the following elementary observation. For the convenience of the reader we include the easy proof from [57] which replaces the usual use of character theory by the Cauchy–Schwarz inequality.

Lemma 5.1.3. *Let G be a finite group with subgroups H_1 and H_2, such that $H_1H_2 \subsetneqq G$, and the actions of G on the coset spaces G/H_1 and G/H_2 are doubly transitive. Let χ_i be the permutation character of the action of G on G/H_i. Then $\chi_1 = \chi_2$, so in particular $[G:H_1] = [G:H_2]$.*

Proof. As G is doubly transitive on G/H_i, it follows easily that $\sum_{g\in G} \chi_i(g)^2 = 2|G|$, see [25, 2.7.4(i)]. Note that $\chi_1\chi_2$ is the permutation character of the action of G on the cartesian product $G/H_1 \times G/H_2$. The assumption $H_1H_2 \subsetneqq G$ implies that G has at least two orbits on this product, therefore

$\sum_{g\in G}\chi_1(g)\chi_2(g) \geq 2|G|$. Together with the Cauchy–Schwarz inequality we obtain

$$4|G|^2 \leq (\sum_{g\in G}\chi_1(g)\chi_2(g))^2 \leq \sum_{g\in G}\chi_1(g)^2 \sum_{g\in G}\chi_2(g)^2 = 4|G|^2.$$

As we obtain equality, there is a constant s such that $\chi_1(g) = s\chi_2(g)$ for all $g \in G$. But

$$|G| = \sum_{g\in G}\chi_1(g) = \sum_{g\in G}\chi_2(g) = s\sum_{g\in G}\chi_1(g) = s|G|,$$

so $s = 1$. The claim follows. □

5.2 Failure of Finiteness Property

The collection of examples in this section should make clear that, in a certain sense, Theorems 5.1.1 and 5.1.2 are optimal.

Example 5.2.1. We show that the analogues of the parts (a) and (f) of Theorem 5.1.1 as well as Theorem 5.1.2 are wrong for rational specializations. For instance, take

$$g(Z) = \frac{(Z^4 - 3Z^3 - Z + 4)(Z^3 - Z + 1)}{Z^2(Z-1)}$$

from [53, Appendix, Table 5]. Then the splitting field L of $g(Z) - t$ over $\mathbb{Q}(t)$ is a regular extension with group $A = \mathrm{GL}_3(2)$. Let A_z be the stabilizer of a root of $g(Z) - t$. If we identify A_z with the upper triangular matrices of A, then let A_x be the group of lower triangular matrices, and $x \in L$ be a primitive element of the fixed field of A_x. Let $f(X,t)$ be a minimal polynomial of x over $\mathbb{Q}(t)$. Computing the orbit lengths of A_z on A/A_x, we obtain that $f(X, g(Z))$ factors over $\mathbb{Q}(Z)$ into absolutely irreducible factors of degrees 3 and 4. These factors remain irreducible by Hilbert's irreducibility theorem for infinitely many rational z_0. Thus, while $f(X,t)$ has Galois group $\mathrm{GL}_3(2) \cong \mathrm{PSL}_2(7)$ over $\mathbb{Q}(t)$, the polynomial $f(X, t_0)$ becomes reducible without a linear factor for each $t_0 = g(z_0)$ for such z_0.

The following easy construction shows that the analogue of Theorem 5.1.1(a) is false for each non–prime degree ≥ 4. A similar example has been given by Dèbes (personal communication).

Example 5.2.2. Let $n = uv$ with $u, v > 1$ integers. Choose $h(Y, Z) \in \mathbb{Q}[Y, Z]$, such that $h(Y, Z)$ is absolutely irreducible, has positive genus, and degree u with respect to Y. Let t be a variable, z be a root of $Z^v - t$, y be a root of $h(Y, z)$, and x be a primitive element of $\mathbb{Q}(y, z)/\mathbb{Q}(t)$. Let $f(X, t)$ be the minimal polynomial of x over $\mathbb{Q}(t)$.

Then $f(X, t)$ is irreducible over $\mathbb{Q}(t)$ of degree n in X, and $f(X, t_0)$ has a rational root for only finitely many integers t_0, whereas $f(X, t_0)$ is reducible for each v–th power t_0 of an integer.

Remark 5.2.3. In the previous example, the Galois group A of $f(X, t)$ over $\mathbb{Q}(t)$ acts imprimitively on the roots of $f(X, t)$. In general, without the primitivity assumption on A, we get little restrictions on A if $|\mathcal{R} \setminus \mathcal{L}| = \infty$. The reason for this failure is that A is no longer a homomorphic image of a monodromy group of a Siegel function. Actually, for each finite simple group S which occurs regularly over $\mathbb{Q}(t)$, we can construct by a variant of this method an example over $\mathbb{Q}$, where S is a composition factor of A, but $\mathcal{R}$ is infinite (and $\mathcal{L}$ is finite).

In order to construct further examples where the finiteness result fails, we need

Lemma 5.2.4. *Let k be a number field, and $f_i(X, Z) \in k(Z)[X]$ be finitely many irreducible polynomials. Suppose that k has an infinite group of units. Then the polynomials $f_i(X, u)$ are irreducible for infinitely many units u.*

Proof. For each i let e_i be the smallest positive integer e such that $f_i(X, Z)$ has a root x in the Puiseux series field $\bar{k}((Z^{1/e}))$. It is well–known that the group of units of $\mathcal{O}_k$ is finitely generated. Let u be a base element of a complement to the torsion part of the group of units. It is easy to see that $T^e - u$ then is irreducible over k for each $e \in \mathbb{N}$. Let e be the product of the e_i. An easy argument (or see [10, Prop. 3]) shows that the polynomials $f_i(X, uZ^e)$ are irreducible. By construction, each $f_i(X, uZ^e)$ now has a root in the Laurent series field $\bar{k}((Z))$. By a tightening of Hilbert's irreducibility theorem due to Dèbes [11, Cor. 1.6(b)], the polynomials $f_i(X, u^{1+je})$ are irreducible for all but finitely many integers j. The claim follows. □

Lemma 5.2.5. *Let k be a number field, $f(X, t) \in k[X, t]$ be irreducible, and $g(Z) \in k(Z)$ of one of the following forms:*

(a) $g(Z) \in \mathcal{O}_k[Z]$; or

(b) $g(Z) = h(Z)/Z^m$, *where* $h(Z) \in \mathcal{O}_k[Z]$ *has degree* $2m$ *and* $h(0) \neq 0$, *and* $\mathcal{O}_k$ *has an infinite group of units; or*

(c) $k = \mathbb{Q}$, $g(Z) = h(Z)/(Z^2 - d)^m$, *where* $h(Z) \in \mathbb{Z}[Z]$ *is a polynomial of degree* $\leq 2m$ *with* $h(\pm\sqrt{d}) \neq 0$, *and* $d > 1$ *is a square–free integer. Furthermore, assume that each absolutely irreducible factor* $f_i(X, Z)$ *of* $f(X, g(Z))$ *has the following property: If* x *is a root of* $f_i(X, Z)$, *then* $\mathbb{C}(Z, x)/\mathbb{C}(Z)$ *has a ramified place* $Z \mapsto \alpha \in \mathbb{P}^1(\mathbb{C})$ *with* $\alpha \neq \pm\sqrt{d}$. *(This holds in particular if* $f_i(X, Z) = 0$ *has positive genus.)*

Suppose that $f(X, g(Z))$ *is reducible over* $k(Z)$, *but does not have a factor of degree* 1. *Then* $f(X, t_0)$ *is reducible for infinitely many integers* $t_0 \in \mathcal{O}_k$ *without a linear factor.*

Proof. Let $f(X, g(Z)) = \prod f_i(X, Z)$ be a decomposition into irreducible factors $f_i(X, Z) \in k(Z)[X]$.

Case (a) is easy. The multi–polynomial version of Hilbert's irreducibility theorem gives infinitely many integers $z_0 \in \mathcal{O}_k$ such that $f_i(X, z_0)$ is irreducible for each i. Now let $t_0 = g(z_0)$ for those z_0.

Case (b) follows from Lemma 5.2.4.

Case (c) is a little more subtle. Set $k := \mathbb{Q}(\sqrt{d})$. Then $\mathcal{O}_k$ has an infinite group of units, and from that it follows easily that there are $\alpha, \beta \in \mathbb{Z}$ with $\alpha^2 - \beta^2 d = 1$, such that $u := \alpha + \beta\sqrt{d}$ has infinite multiplicative order. Let $m \in \mathbb{N}$ be relatively prime to the degrees (in X) of the absolutely irreducible factors f_i. Let f_i be one of these factors, and w_i its degree. Then $\phi_i(X, Y) := f_i(X, \frac{Y^m+1}{Y^m-1}\sqrt{d})$ is again absolutely irreducible. We compute the genus g_i of $\phi_i(X, Y) = 0$ using the Riemann–Hurwitz genus formula and Abhyankar's Lemma [69, III.8.9] applied to the two extensions $\mathbb{C}(x, Y^m)$ and $\mathbb{C}(Y)$ over $\mathbb{C}(Y^m)$:

$$2(mw_i - 1 + g_i) \geq 2(m-1)w_i + m.$$

Here the places at 0 and ∞ each contribute at least $(m-1)w_i$ to the right hand side, and the assumption on the ramification gives that $\mathbb{C}(x, Y)/\mathbb{C}(Y^m)$ is ramified at least at m finite points $\neq 0$. The above inequality gives $g_i \geq 1 + m/2 - w_i$. So for m big enough, we may assure that the absolutely irreducible polynomials $\phi_i(X, Y)$ have positive genus.

Thus $\phi_i(X, u^{2j})$ has a degree 1 factor over k for only finitely many integers j by Siegel's theorem. Write $\alpha_j + \beta_j\sqrt{d} := u^j$ with $\alpha_j, \beta_j \in \mathbb{Z}$. Then $\alpha_j^2 -$

$\beta_j^2 d = 1$, thus

$$\begin{aligned}\frac{u^{2j}+1}{u^{2j}-1}\sqrt{d} &= \frac{u^j + 1/u^j}{u^j - 1/u^j}\sqrt{d} \\ &= \frac{2\alpha_j}{2\sqrt{d}\beta_j}\sqrt{d} \\ &= \frac{\alpha_j}{\beta_j}.\end{aligned}$$

Now, setting $t_0 := g(\alpha_j/\beta_j)$, we obtain

$$t_0 = g(\frac{\alpha_j}{\beta_j}) = \frac{\beta_j^{2m} h(\frac{\alpha_j}{\beta_j})}{(\alpha_j^2 - \beta_j^2 d)^m} = \beta_j^{2m} h(\frac{\alpha_j}{\beta_j}) \in \mathbb{Z}.$$

Therefore we obtain infinitely many $t_0 = g(\alpha_j/\beta_j) \in \mathbb{Z}$, such that $f(X, t_0)$ is reducible without a linear factor. □

Remark 5.2.6. We cannot get a statement in (c) analogous to (b), where we had no additional assumption on the factors f_i. The problem is that there are irreducible polynomials $f_i(X, Z)$ of X–degree > 1, such that $f_i(X, \alpha/\beta)$ has a linear factor for all rational α, β with $\alpha + \beta\sqrt{d}$ a unit of $\mathbb{Q}(\sqrt{d})$, an easy example being $d \equiv 3 \pmod 4$ and $f_i(X, Z) = X^2 - (Z^2 - d)$.

The general approach in applying the previous lemma is as follows. We choose a Siegel function $g(Z)$ over k, and let L be a splitting field of $g(Z) - t$ over $k(t)$. With $A := \mathrm{Gal}(L/k(t))$, let A_z be the stabilizer of a root of $g(Z) - t$. Suppose there is a subgroup A_x of A such that $A_z A_x \subsetneq A$, but A_z has orbits of length > 1 on A/A_x. Then let $f(X, t)$ be a minimal polynomial over $\mathbb{Q}(t)$ of a primitive element of the fixed field of A_x. It follows that $f(X, g(Z))$ is reducible over $k(Z)$ without a linear factor. By a linear fractional change over k, we may assume that we started with g of the form as given in Lemma 5.2.5. Thus $g(k) \cap \mathcal{O}_k$ is an infinite subset of $\mathcal{R}$, and we only have to assure that infinitely many of these elements are not in $\mathcal{L}$.

If $k = \mathbb{Q}$, then we classified precisely which primitive permutation groups can be arithmetic and geometric monodromy groups of Siegel functions. In the classification over general number fields k, we only used the necessary condition about the form of a genus 0 system. Suppose that the permutation group G admits a genus 0 system, where one of its members has at most two cycles. Then, by Riemann's existence theorem (see Section 3.1.1), there

is a number field k and a rational function $g(Z) \in k(Z)$ with geometric monodromy group G and ramification described by the genus 0 system. By possibly increasing k, we may assume that $g^{-1}(\infty) = \{\infty\}$ or $\{0, \infty\}$, k has an infinite group of units, and g has the form as in Lemma 5.2.5(a) or (b).

Example 5.2.7. In part (e) of Theorem 5.1.1 we got a nice finiteness result for $\mathcal{R}$ in case that the Galois group is an alternating or symmetric group in the natural action, but nevertheless we excluded alternating composition factors in the statements of part (f), (g), (h), and (i). The following observation from [57] makes clear that we have to do so.

Let $2 \leq k \leq m-2$ be integers with $2k \neq m$. Then there exists an absolutely irreducible polynomial $f(X,t) \in \mathbb{Q}[X,t]$ with $\deg_X f = \binom{m}{k}$ and $|\mathcal{R} \setminus \mathcal{L}| = \infty$, such that its Galois group over $\mathbb{Q}(t)$ is primitive and equivalent to the action of $\mathcal{S}_m$ on the k–sets of $\{1, 2, \ldots, m\}$.

The construction is as follows, for the details confer [57, Theorem 9.1]. Let $g(Z) = Z^m - Z$. Then $A := \mathrm{Gal}(g(Z) - t/\mathbb{Q}(t)) = \mathcal{S}_m$; indeed, there are $m-1$ finite branch points, and the corresponding inertia generators act as transpositions. Let L be a splitting field of $g(Z) - t$ over $\mathbb{Q}(t)$, and x be a primitive element of the fixed field of $A_x := \mathcal{S}_k \times \mathcal{S}_{m-k} < \mathcal{S}_m$. It is easy to see that A_x is a maximal subgroup of A (see the proof of [57, Theorem 9.1]). The stabilizer A_z of a root of $g(Z) - t$ has orbit lengths $\binom{m-1}{k-1}$ and $\binom{m-1}{k}$ on A/A_x. Let $f(X,t)$ be a minimal polynomial of x over $\mathbb{Q}(t)$. Then $f(X, g(Z))$ is reducible over $\mathbb{Q}(Z)$ with two factors of degree > 1, so we get the claim from Lemma 5.2.5(a).

It is easy to check that the genus of $f(X,t) = 0$ is positive in the previous example, so actually $|\mathcal{L}| < \infty$. For instance, for the given $g(Z)$, the genus of $f(X,t) = 0$ is $1 + \binom{m}{k}\frac{mk-k^2-m-1}{2m} \geq 1$ if m is a prime. If m is not a prime, then the genus computation is a little messy.

Example 5.2.8. In parts (h) and (i) of Theorem 5.1.1 we proved a strong finiteness result for polynomials $f(X,t)$ with primitive Galois group A over $k(t)$. At a first glance, it might appear that one can do even a little better. For instance if $k = \mathbb{Q}$, we had to include the group $\mathrm{PSL}_2(7)$ because there is a degree 8 Siegel function of second kind with monodromy group $\mathrm{AGL}_3(2) = C_2^3 \rtimes \mathrm{PSL}_2(7)$. However, $\mathrm{AGL}_3(2)$ does not have a primitive permutation representation with point stabilizer acting intransitively with orbits of length > 1 in the natural degree 8 action. So the obvious possibility for constructing an example as above fails. Nevertheless, a refined idea will show that, under the assumption of primitivity of A, the assertion about the

composition factors of A in Theorems 5.1.1(h) and (i) is optimal. One of the many possible kinds of construction will be given in the proof of the following

Proposition 5.2.9. *Let k be a number field, and S be a non–abelian composition factor of a Siegel function over k. Then there exists a finite extension ℓ of k, where $\ell = \mathbb{Q}$ if $k = \mathbb{Q}$, and $f(X,t) \in \ell[X,t]$, such that the following holds:*

$f(X,t)$ is irreducible, the Galois group over $\ell(t)$ is primitive, and each of its non–abelian composition factors is isomorphic to S. Furthermore, $\mathcal{R}$ is an infinite set while $\mathcal{L}$ is finite. Indeed, for fixed S, the genus of $f(X,t)$ can be made arbitrarily large.

Proof. Let $g(Z)$ be a functionally indecomposable Siegel function over k whose arithmetic monodromy group has S as a composition factor. It follows from our classification that S is the only non–abelian composition factor, and that it is also a composition factor of the geometric monodromy group.

Assume that $g(Z)$ has the form as in Lemma 5.2.5. For this we have to possibly go from k to ℓ if $k \neq \mathbb{Q}$. In addition, if $k \neq \mathbb{Q}$, we choose ℓ big enough such that the group of units of $\mathcal{O}_l$ is infinite. Thus $g(\ell) \cap \mathcal{O}_l$ is an infinite set. Let J be the arithmetic monodromy group of $g(Z)$ over ℓ.

For p a prime let H be the Galois group of $X^p - t$ over $\ell(t)$, so H is a group normalizing C_p.

Let y be a variable. The Galois group of $(g(Z)-y)^p - t$ over $\ell(t,y)$ is the wreath product $W := J \wr H = J^p \rtimes H$. By Hilbert's irreducibility theorem, there are infinitely many $y_0 \in \mathcal{O}_k$ such that $(g(Z)-y_0)^p - t$ still has the Galois group W over $k(t)$. Among those y_0, choose one such that 0 and ∞ are not branch points of $g(Z) - y_0$, and that no two branch points of $g(Z) - y_0$ are mapped to the same point under X^p. These general position assumptions will be helpful in a genus computation below.

Let J_1 be the stabilizer of a point in the given action of J. Then, as J is primitive but not regular, the group $W_1 := J_1^p \rtimes H$ is a maximal subgroup of $W = J^p \rtimes H$, in fact the action of W on the coset space W/W_1 is the primitive product action of the wreath product $J \wr H$. Set $\hat{g}(Z) := (g(Z) - y_0)^p$, and note that $|\hat{g}(\ell) \cap \mathcal{O}_l| = \infty$. Let L be a splitting field of $\hat{g}(Z) - t$ over $\ell(t)$, and E the fixed field in L of W_1. Let n be the degree of g. Then $[E : \ell(t)] = n^p$. Let $f(X,t)$ be a minimal polynomial of a primitive element of $E/\ell(t)$. The stabilizer in W of a root of $\hat{g}(Z) - t$ has two orbits on W/W_1, one of length n^{p-1}, and the other one of length $n^p - n^{p-1}$. Accordingly, $f(X, \hat{g}(Z))$ factors over $\ell(Z)$ into two factors of degrees $n^{p-1} > 1$ and $n^p - n^{p-1} > 1$, respectively.

The assertion now follows from Lemma 5.2.5 once we know that the genus of $f(X,t)=0$ can be made arbitrarily large.

Let us compute the genus of E. We take advantage of the general position assumptions of the branching locus of $\hat{g}(Z)-t$ in order to get an easy genus computation using the Riemann–Hurwitz genus formula. Let σ_1 and σ_2 be inertia generators belonging to $t \mapsto 0$ and $t \mapsto \infty$, and let $\tau_1, \ldots, \tau_r$ be inertia generators coming from the branch points of $g(Z)$. Let ind refer to the action on W/W_1. Then σ_i has precisely n fixed points, and moves the remaining n^p-n points in p–cycles. Thus $\mathrm{ind}(\sigma_i)=(n^p-n)(1-1/p)$. If the inertia generator belonging to τ_i has orbit lengths $v_1, v_2, \ldots, v_s$ on the roots of $g(Z)-t$, then τ_i has the same orbit lengths on W/W_1, but each one occurs n^{p-1} times. As $\ell(Z)/\ell(g(Z))$ is an extension of genus 0 fields, we obtain

$$\sum_{i=1}^{r} \mathrm{ind}(\tau_i) = n^{p-1}(2(n-1)).$$

If g_E is the genus of E, then

$$\begin{aligned} 2(n^p-1+g_E) &= \mathrm{ind}(\sigma_1)+\mathrm{ind}(\sigma_2)+\sum_{i=1}^{r}\mathrm{ind}(\tau_i) \\ &= 2(n^p-n)(1-\frac{1}{p})+n^{p-1}(2(n-1)), \end{aligned}$$

so

$$g_E = (n^{p-1}-1)\frac{np-n-p}{p} > 0,$$

and clearly $g_E \to \infty$ for $p \to \infty$. □

Example 5.2.10. Let $h(X) \in k[X]$ be a Davenport polynomial of degree n (see Section 4.5 for definitions and properties), so there is $g(Z) \in k[Z]$ such that h and g are Kronecker conjugate over k. Let L be a common splitting field of $h(X)-t$ and $g(Z)-t$, and x, z be roots of $h(X)-t$ and $g(Z)-t$, respectively. Set $A := \mathrm{Gal}(L/k(t))$, and let A_x and A_z be the stabilizers of x and z. Using the inertia group of L of a place above $t \mapsto \infty$ of $k(t)$ one easily proves (or see [24, 19.29]) that h and g have the same degree. Thus A_z cannot be conjugate to a subgroup of A_x. On the other hand, as each element in A_z has a fixed point in the action on A/A_x, we get that A_z has more than one orbit on A/A_x. Therefore $h(X)-g(Z)$ is reducible over $k(Z)$ without a linear factor. Thus, for $f(X,t) := h(X)-t$, we obtain $|\mathcal{R}\setminus\mathcal{L}| = \infty$.

Example 5.2.11. Here we describe the exceptions to the finiteness results of Theorem 5.1.1 for degree 5, see case (d). Suppose that we have $|\mathcal{R} \setminus \mathcal{L}| = \infty$ for an irreducible degree 5 polynomial $f(X,t) \in k(t)[X]$. The proof of 5.1.1(d) shows that there is a Siegel function of the second kind $g(Z) \in k(Z)$ of degree 10, such that the Galois group A of $g(Z) - t$ over $k(t)$ is $\mathcal{A}_5$ or $\mathcal{S}_5$ in the action on the 2–sets of $\{1,2,3,4,5\}$, the splitting fields of $g(Z) - t$ and $f(X,t)$ over $k(t)$ coincide, and that $f(X,t)$ has Galois group A for the natural action. Let x be a root of $f(X,t)$. An easy index computation shows that $k(t,x)$ has genus 0, see also [57, Section 8]. Let σ be an inertia generator coming from the place $t \mapsto \infty$ of $k(t)$. Then, as g is a Siegel function of the second kind, σ has order 5. In particular, the place $t \mapsto \infty$ is totally ramified in $k(t,x)$. Thus, without loss, $f(X,t) = h(X) - t$ for a polynomial $h(X) \in k[X]$.

Conversely, let $h(X) \in k[X]$ be a polynomial of degree 5 such that $A := \mathrm{Gal}(h(X) - t/k(t)) = \mathcal{A}_5$ or $\mathcal{S}_5$. Let U be the setwise stabilizer in A of two distinct roots x_1 and x_2 of $h(X) - t$. A necessary condition that $f(X,t) = h(X) - t$ arises from a consideration as above is that $k(x_1,x_2)$ is a genus 0 field. We get many positive examples even for $k = \mathbb{Q}$. From now on suppose that $k = \mathbb{Q}$. Note that if $\mathbb{Q}(x_1,x_2)$ is a rational field, then we get automatically $\mathbb{Q}(x_1,x_2) = \mathbb{Q}(z)$ and $g(z) = t$ where $g(Z) = j(Z)/(Z^2-5)^5$ with $j(Z) \in \mathbb{Q}[Z]$ by Lemma 4.2.1(e).

An (essentially unique) example with Galois group $\cong \mathcal{A}_5$ over $\overline{\mathbb{Q}}(t)$ is $f(X,t) := X^3(X^2+5X+40) - t$. Set $g(Z) := 40000(Z-5)(2Z^2+5Z+5)^3/(Z^2-5)^5$. One verifies easily that $f(X,g(Z))$ is reducible over $\mathbb{Q}(Z)$ with absolutely irreducible factors of degrees 2 and 3, and that we are in the situation to apply Lemma 5.2.5(c).

In [12], Dèbes and Fried give a detailed analysis of this degree 5 case, especially if the splitting field of $h(X) - t$ over $\mathbb{Q}(t)$ has 4 ramified places. (There cannot be more than 4.) One can enhance their arguments easily by explicit computations to get more complete results. In this 4–point ramified case, we may either assume that $h(X) = X(X^2-\rho)^2$ with $0 \neq \rho \in \mathbb{Q}$, or $h(X) = (X-1)(X^2-\rho)^2$, where $0, \pm 1 \neq \rho \in \mathbb{Q}$. Then one computes that the field $\mathbb{Q}(x_1,x_2)$ from above is a rational field if and only if $-\rho$ is a norm of $\mathbb{Q}(\sqrt{5})$ in the first case, or if $5\rho - 1$ is a norm of $\mathbb{Q}(\sqrt{5})$ in the second case. It is not hard to compute explicitly the Siegel function $g(Z)$ in these cases. Dèbes and Fried rather give a theoretical argument that there are infinitely many $\rho \in \mathbb{Q}$ such that $\mathbb{Q}(x_1,x_2)$ is rational. (They use a different set up, so they actually do not have this normal form of $f(X,t) = h(X) - t$.)

5.3 Thue–Polynomials, on a Result of Langmann

Continuing work in [45], K. Langmann obtains in [46] the following finiteness result for exceptional specializations of Thue polynomials.

Theorem 5.3.1 (Langmann 1999). *Let $H(X,t) \in \mathbb{Q}[X,t]$ be a homogeneous polynomial of odd degree n, and suppose that H has no repeated linear factors over $\overline{\mathbb{Q}}$ and is not divisible by t. Then $H(X,t_0)-1$ is irreducible for all but finitely many $t_0 \in \mathbb{Z}$.*

Below we will prove a much more general result, which does not depend on our group theoretic classification results. In particular, we show that the separability assumption on H can be weakened, it is enough to assure that the greatest common divisor of the multiplicities of the linear factors of $H(X,t)$ (over $\overline{\mathbb{Q}}$) is 1. (Spending somewhat more work one can slightly lessen this condition, and assume that $H(X,t)$ is not of the form $J(X,t)^e$ with $e>1$ and $J(X,t) \in \mathbb{Q}[X,t]$, a condition which is clearly also necessary for the above theorem to hold.)

Furthermore, the above theorem holds without any change for number fields.

Langmann's theorem is wrong if we allow $\deg(H)=2$, because for $d>1$ a square–free integer, the Pell equation $X^2-dt^2=1$ has infinitely many integral solutions. However, extending the arguments given in the proof of Theorem 5.3.3 below (to be worked out in a future paper) shows that Langmann's theorem holds also for each even degree >2. Even for the number field analogue it is enough to assume $\deg(H) \neq 2$.

We claimed that we can lessen the separability assumption on H, and that we can also extend the result to number fields. The following example shows that we cannot do both at the same time, even if we assume odd degree.

Example 5.3.2. Set $H(X,t) := X^2(X-t)$, and assume that k is a number field with an infinite group of units. From

$$H(X, \frac{1-Z^3}{Z}) - 1 = (X - \frac{1}{Z})(X^2 + Z^2X + Z)$$

and the fact that $t_0 = (1-z_0^3)/z_0$ is an integer in $\mathcal{O}_k$ for each unit z_0 we obtain reducibility of $H(X,t_0)-1$ for infinitely many $t_0 \in \mathcal{O}_k$.

In order to prove the promised generalizations of Theorem 5.3.1, we remark the following: Let $H(X,t)$ be homogeneous of degree n. Then $H(X,t) = t^n h(X/t)$ with $h(X) \in k[X]$. Upon replacing X/t with X, we ask for the irreducibility of $t_0^n h(X) - 1$ for integral specializations $t_0 \in \mathcal{O}_k$. If we get reducibility infinitely often, then this is even more true for the polynomial $th(X) - 1$. Thus we obtain the claimed extensions from the following far more general

Theorem 5.3.3. *Let k be a number field, and $P_1(X) \in k[X]$ be a polynomial of odd degree n. Let $P_2(X) \in k[X]$ be a non–zero polynomial of degree $\leq n$, which is relatively prime to P_1. If $k = \mathbb{Q}$ then assume that the greatest common divisor of the multiplicities of the roots (in $\bar{k}$) of $P_1(X)$ is 1. If $k \neq \mathbb{Q}$, then assume more strongly that $P_1(X)$ is separable.*

Then $t_0 P_1(X) - P_2(X)$ is irreducible for all but finitely many $t_0 \in \mathcal{O}_k$.

Proof. Assume the contrary. Then, by Proposition 1.1.2 and Lemma 1.2.1, there is a rational function $g(Z) \in k(Z)$ such that $g(Z)P_1(X) - P_2(X)$ is reducible over $k(Z)$, and that the splitting field of $g(Z) - t$ over $k(t)$ is contained in the splitting field L of $tP_1(X) - P_2(X)$ over $k(t)$.

Furthermore, $|g(k) \cap \mathcal{O}_k| = \infty$, so $|g^{-1}(\infty)| \leq 2$, see Proposition 4.1.1. We use the notation from Lemma 1.2.1. Let $\mathfrak{P}$ be a place of L which lies above the place $t \mapsto \infty$ of $k(t)$. Let σ be a generator of the inertia group of $\mathfrak{P}$. Then σ has at most two cycles on A/A_z, with lengths which are the multiplicities of the elements in the fiber $g^{-1}(\infty)$.

We first treat the case $k = \mathbb{Q}$. Then either $[A : A_z] = m$, and σ is an m–cycle on A/A_z, or $[A : A_z] = 2m$, and σ is a product of two m–cycles on A/A_z, see Chapter 4. Let $a_1, a_2, \ldots, a_j$ be the multiplicities of the roots of $P_1(X)$. Then σ has on A/A_x the cycle lengths $a_1, a_2, \ldots, a_j$ (recall that $\deg(P_1) \geq \deg(P_2)$). Write $[A : A_z] = \lambda m$ with $\lambda = 1$ or 2, and let $u \leq \lambda m/2$ be the smallest degree in Z of an irreducible factor of $g(Z)P_1(X) - P_2(X)$. As σ^{a_i}, $1 \leq i \leq j$, fixes a root of x, and σ^{a_i} has orbits of lengths $m/\gcd(m, a_i)$ on A/A_z, we obtain that u is divisible by $m/\gcd(m, a_i)$. Thus $m/\gcd(m, u)$ divides $\gcd(m, a_i)$ for each a_i. But the a_i have the greatest common divisor 1 by assumption, hence $m = \gcd(m, u)$, so $\lambda = 2$ and $u = m$. So $g(Z)P_1(X) - P_2(X)$ factors into two irreducible factors which have the same degree with respect to Z. It follows that the two factors also have the same degree with respect to X (because the degrees are proportional to the sizes of the double cosets $A_z a A_x$, $a \in A$). But this contradicts the assumption that $g(Z)P_1(X) - P_2(X)$ has odd degree in X.

Now assume $k \neq \mathbb{Q}$. As P_1 is separable, we obtain that σ acts trivially on A/A_x. By faithful action of A on A/A_x, we have $\sigma = 1$. On the other hand, the cycle lengths of σ on A/A_z are the multiplicities of the elements in the fiber $g^{-1}(\infty)$, which consists of at most two elements. As g is clearly not fractional linear, we obtain that g has degree 2. Thus the group $\mathrm{Gal}(k(z)/k(t))$ interchanges the two $k(z)$–irreducible factors of $tP_1(X) - P_2(X)$, so we again obtain a contradiction to the assumption that $P_1(X)$ has odd degree. $\square$

Bibliography

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

[2] Y. Bilu, *A note on universal Hilbert sets*, J. Reine Angew. Math., **479** (1996) 195–203.

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

[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, *2–transitive and antiflag transitive collineation groups of finite projective spaces*, J. Algebra, **60** (1979) 384–422.

[6] R. 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.), volume 131 of *Lecture Notes in Mathematics*, pp. G1–G22, Springer–Verlag, Berlin, Heidelberg, (1970).

[7] R. W. Carter, *Simple Groups of Lie Type*, Wiley and Sons, London, (1972).

[8] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, (1985).

[9] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, S. M., and K. Wildanger, *KANT V4*, J. Symb. Comput., **24**(3) (1996) 267–283, KASH software available from ftp.math.tu-berlin.de in /pub/algebra/Kant/Kash/Binaries.

[10] P. Dèbes, *G-fonctions et théorème d'irréductibilité de Hilbert*, Acta Arith., **47** (1986) 371–402.

[11] P. Dèbes, *On the irreducibility of the polynomials* $P(t^m, Y)$, J. Number Theory, **42** (1992) 141–157.

[12] P. Dèbes and M. Fried, *Integral specialization of families of rational functions*, preprint.

[13] P. Dèbes and U. Zannier, *Universal Hilbert subsets*, Math. Proc. Cambridge Philos. Soc., **124** (1998) 127–134.

[14] J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer–Verlag, New York, (1996).

[15] M. Eichler, *Zum Hilbertschen Irreduzibilitätssatz*, Math. Ann., **116** (1939) 742–748.

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

[17] W. Feit, *Some consequences of the classification of finite simple groups*, in: *The Santa Cruz conference on finite groups*, volume 37 of *Proc. Sympos. Pure Math.*, pp. 175–181, Amer. Math. Soc., Providence, Rhode Island, (1980).

[18] W. Feit, R. Lyndon, and L. L. Scott, *A remark about permutations*, J. Combin. Theory Ser. A, **18** (1975) 234–235.

[19] M. Fried, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Illinois J. Math., **17** (1973) 128–146.

[20] M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory, **6** (1974) 211–231.

[21] M. Fried, *Fields of definition of function fields and Hurwitz families — Groups as Galois groups*, Comm. Algebra, **5** (1977) 17–82.

[22] M. Fried, *Rigidity and applications of the classification of simple groups to monodromy, part II – Applications of connectivity; Davenport and Hilbert-Siegel problems*, preprint.

[23] M. Fried and P. Dèbes, *Rigidity and real residue class fields*, Acta Arith., **56** (1990) 291–323.

[24] M. Fried and M. Jarden, *Field Arithmetic*, Springer–Verlag, Berlin Heidelberg, (1986).

[25] D. Gorenstein, *Finite Groups*, Harper and Row, New York–Evanston–London, (1968).

[26] R. Guralnick and M. Neubauer, *Genus zero monodromy groups of affine type*, Preprint.

[27] R. Guralnick and J. G. Thompson, *Finite groups of genus zero*, J. Algebra, **131** (1990) 303–341.

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

[29] C. Hering, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order, II*, J. Algebra, **93** (1985) 151–164.

[30] D. Hilbert, *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, J. Reine Angew. Math., **110** (1892) 104–129.

[31] B. Huppert, *Endliche Gruppen I*, Springer–Verlag, Berlin Heidelberg, (1967).

[32] B. Huppert and N. Blackburn, *Finite Groups III*, Springer–Verlag, Berlin Heidelberg, (1982).

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

[34] 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.

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

[36] P. Kleidman and M. W. Liebeck, *The subgroup structure of the finite classical groups*, Cambridge University Press, Cambridge, (1990).

[37] P. Kleidman, R. A. Parker, and R. A. Wilson, *The maximal subgroups of the Fischer group Fi_{23}*, J. London Math. Soc. (2), **39**(2) (1989) 89–101.

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

[39] P. Kleidman and R. A. Wilson, *The maximal subgroups of J_4*, Proc. London Math. Soc. (3), **56**(3) (1988) 484–510.

[40] N. Klingen, *Arithmetical Similarities — Prime Decomposition and Finite Group Theory*, Oxford Mathematical Monographs, Oxford University Press, Oxford, (1998).

[41] L. Kronecker, *Über die Irreduzibilität von Gleichungen*, Monatsberichte Deutsche Akademie für Wissenschaft, (1880) 155–163, (=Werke II, 85–93).

[42] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Teubner, Leipzig, (1909), second edition by Chelsea, New York, 1953.

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

[44] S. Lang, *Fundamentals of Diophantine Geometry*, Springer–Verlag, New York, (1983).

[45] K. Langmann, *Werteverhalten holomorpher Funktionen auf Überlagerungen und zahlentheoretische Analogien*, Math. Ann., **299** (1994) 127–153.

[46] K. Langmann, *Werteverhalten holomorpher Funktionen auf Überlagerungen und zahlentheoretische Analogien II*, Math. Nachr., (1999), to appear.

[47] M. W. Liebeck, *The affine permutation groups of rank three*, Proc. London Math. Soc. (3), **54** (1987) 477–516.

[48] 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.

[49] M. W. Liebeck and J. Saxl, *On the orders of maximal subgroups of the finite exceptional groups of Lie type*, Proc. London Math. Soc. (3), **55**(3) (1987) 299–330.

[50] S. Linton, *The maximal subgroups of the Thompson group*, J. London Math. Soc. (2), **39**(2) (1989) 79–88.

[51] G. Malle, *Fields of definition of some three point ramified field extensions*, in: *The Grothendieck theory of dessins d'enfants* (L. Schneps, ed.), volume 200 of *Lond. Math. Soc. Lect. Note Ser.*, pp. 147–168, Cambridge University Press, (1994).

[52] G. Malle, *Some multi-parameter polynomials with given Galois group*, in preparation.

[53] G. Malle and B. H. Matzat, *Inverse Galois Theory*, Springer Verlag, (1999), to appear.

[54] P. Müller, *Primitive monodromy groups of polynomials*, in: *Recent developments in the inverse Galois problem* (M. Fried, ed.), volume 186 of *Contemp. Maths.*, pp. 385–401, Amer. Math. Soc., (1995).

[55] P. Müller, *Reducibility behavior of polynomials with varying coefficients*, Israel J. Math., **94** (1996) 59–91.

[56] P. Müller, *Kronecker conjugacy of polynomials*, Trans. Amer. Math. Soc., **350** (1998) 1823–1850.

[57] P. Müller, *Hilbert's irreducibility theorem for prime degree and general polynomials*, Israel J. Math., **109** (1999) 319–337.

[58] M. Neubauer, *On primitive monodromy groups of genus zero and one, I*, Comm. Algebra, **21**(3) (1993) 711–746.

[59] R. Ree, *A theorem about permutations*, J. Combin. Theory Ser. A, **10** (1971) 174–175.

[60] A. Robinson and P. Roquette, *On the finiteness theorem of Siegel and Mahler concerning diophantine equations*, J. Number Theory, **7** (1975) 121–176.

[61] M. Schönert et al., *GAP – Groups, Algorithms, and Programming*, Lehrstuhl D für Mathematik, RWTH Aachen, Germany, (1995).

[62] L. Scott, *Representations in characteristic p*, in: *The Santa Cruz conference on finite groups*, volume 37 of *Proc. Sympos. Pure Math.*, pp. 319–331, Amer. Math. Soc., Providence, Rhode Island, (1980).

[63] L. L. Scott, *On the $n, 2n$ problem of Michael Fried*, in: *Proc. Conf. Finite Groups*, pp. 471–472, Academic Press, (1976).

[64] J.-P. Serre, *Topics in Galois Theory*, Jones and Bartlett, Boston, (1992).

[65] K. Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann., **207** (1974) 99–120.

[66] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Pr. Akad. Wiss., **1** (1929) 41–69, (=Ges. Abh., I, 209–266).

[67] V. G. Sprindžuk, *Diophantine equations with unknown prime numbers*, Proc. Steklov Inst. Math., **4** (1983) 197–214.

[68] R. Steinberg, *Endomorphisms of linear algebraic groups*, Mem. Amer. Math. Soc., (1968).

[69] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer–Verlag, Berlin Heidelberg, (1993).

[70] P. H. Tiep and A. E. Zalesskii, *Minimal characters of the finite classical groups*, Comm. Algebra, **24** (1996) 2093–2167.

[71] H. Völklein, *Groups as Galois Groups – an Introduction*, Cambridge University Press, New York, (1996).

[72] H. Wielandt, *Primitive Permutationsgruppen vom Grad $2p$*, Math. Z., **63** (1956) 478–485.

[73] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York London, (1964).

[74] U. Zannier, *Note on dense Hilbert sets*, C. R. Acad. Sci. Paris Sér. I Math., **322** (1996) 703–706.