ISRAEL JOURNAL OF MATHEMATICS 94 (1996), 59–91

REDUCIBILITY BEHAVIOR OF POLYNOMIALS WITH VARYING COEFFICIENTS

BY

PETER MÜLLER

Mathematisches Institut, Universität Erlangen-Nürnberg
Bismarckstrasse $1\frac{1}{2}$, D-91054 Erlangen, Germany
e-mail: mueller@mi.uni-erlangen.de

ABSTRACT

Let K be a number field, and let $h \in K[Y]$ be a polynomial of degree n. Fix an integer $0 \leq i \leq n$ and compare the set $\mathcal{V}$ of those integers a of K such that $h(Y) - aY^i$ has a root in K with the set $\mathcal{R}$ of those integers a, such that $h(Y) - aY^i$ is reducible over K. If i is coprime to n, then we classify the rare cases where $\mathcal{V}$ is not cofinite in $\mathcal{R}$. The main tools are a theorem of Siegel about integral points on algebraic curves and the theory of finite groups.

1. Introduction

Throughout this paper K denotes a number field, and $\mathcal{O}_K$ is the ring of integers in K. Let $h(Y) \in K[Y]$ be a polynomial of positive degree n. M. Fried [8], [10] studied the question of reducibility of h upon varying the constant coefficient inside $\mathcal{O}_K$. His result is as follows.

THEOREM 1.1: *Let $h \in K[Y]$ be a non-constant polynomial with $\deg h \neq 5$, which is not the composition of polynomials of lower degree. Denote by $\mathcal{R}_h$ the set of elements $x_0 \in \mathcal{O}_K$, such that $h(Y) - x_0$ is reducible over K. If $K = \mathbb{Q}$ or $\deg h \notin \{7, 11, 13, 15, 21, 31\}$, then all but finitely many $x_0 \in \mathcal{R}_h$ have the form $h(\kappa)$ for some $\kappa \in K$.*

Received October 20, 1994

Later, Fried [10] studied the case of varying other coefficients than the constant one. Again let $h(Y) \in K[Y]$ be of degree n, and fix an integer i with $1 \leq i \leq n-1$. Suppose $h(0) \neq 0$. Let $\mathcal{R}_h$ be the set of those $x_0 \in \mathcal{O}_K$, such that $h(Y) - x_0 Y^i$ is reducible, and let $\mathcal{V}_h$ be the set of those $x_0 \in \mathcal{O}_K$, such that $h(Y) - x_0 Y^i$ has a root in K. Observe that $\mathcal{V}_h$ is just the set of those integers of K which $h(Y)/Y^i$ does assume on K. Fried's result is

THEOREM 1.2: *If* $\gcd(i,n) = 1$ *and* $2 \leq i \leq n-2$, *then* $\mathcal{R}_h \setminus \mathcal{V}_h$ *is a finite set.*

Actually he proved this only for $K = \mathbb{Q}$. A slight extension of his arguments yields the general case; see section 10.

A quite different situation arises if $i = 1$ or $n-1$. This case, posed as Problem 7.5 in [10], requires a finer group-theoretic analysis. The main object of this paper is to give a complete answer in this case. Note that by passing to the reciprocal polynomial with respect to Y, we can assume $i = 1$ throughout. Our result is

THEOREM 1.3: *Let* $h(Y) \in K[Y]$ *be a polynomial of degree* n *with* $h(0) \neq 0$. *Denote by* $\mathcal{R}_h$ *the set of elements* $x_0 \in \mathcal{O}_K$, *such that* $h(Y) - x_0 Y$ *is reducible over* K, *and let* $\mathcal{V}_h$ *be the subset of those* $x_0 \in \mathcal{O}_K$, *such that* $h(Y) - x_0 Y$ *has a root in* K. *Then the following holds.*

(a) *If* $K = \mathbb{Q}$, *then* $\mathcal{R}_h$ *is finite.*

(b) *If* $n \notin \{4, 6, 8, 9, 12, 16\}$, *then* $\mathcal{R}_h \setminus \mathcal{V}_h$ *is finite.*

(c) *If* $n \in \{4, 6, 8, 9, 12, 16\}$, *then there are number fields* K *and polynomials* $h(Y) \in K[Y]$ *of degree* n, *such that* $\mathcal{R}_h \setminus \mathcal{V}_h$ *is infinite.*

(d) *There are polynomials* $h \in \mathbb{Q}[Y]$ *of degree* 4 *(for instance* $(Y-1)^4$*), such that* $\mathcal{R}_h \setminus \mathcal{V}_h$ *is infinite for every real-quadratic number field.*

These results can be seen as tightenings of Hilbert's irreducibility theorem for $h(Y) - XY^i$ (which says that if $f(X,Y) \in K[X,Y]$ is irreducible, then $f(x_0, Y)$ remains irreducible for infinitely many $x_0 \in \mathcal{O}_K$).

In our case we have $f(X,Y) = h(Y) - XY^i$, so by the above results the sets $\mathcal{R}_h$ of those x_0 making $f(x_0, Y)$ reducible differ from $\mathcal{V}_h$ just by finitely many elements in the specified cases. The importance of this lies in the fact that the sets $\mathcal{V}_h$ can be studied more easily than $\mathcal{R}_h$.

C. L. Siegel made this sort of problem accessible, when he demonstrated how to apply his theorem that every affine algebraic curve with infinitely many integral points admits a rational parametrisation. Later, Fried refined this approach, and

gave a convenient translation to a question about finite groups; see Proposition 4.1.

By this translation, one gets a lot of conditions on a finite group, together with two permutation representations. In the subsequent sections we narrow down, step by step, the possible configurations.

In the course of this we need to know the transitive groups of degree n which contain an $(n-1)$-cycle. In section 6 we classify them. That is the only place where the classification of finite simple groups comes in. However, we show without using the classification that such groups are affine groups acting on a vector space, or $\mathrm{PSL}_2(p)$ acting on the projective line (with $p \geq 5$ a prime), or they are 3-transitive. For this we invoke results of O'Nan and Aschbacher about 2-transitive groups. This allows us, using several rationality arguments, to give a classification-free proof of Theorem 1.3(a).

In order to prove part (b), we make use of the classification of the primitive genus 0 groups of affine type, given by R. Guralnick, J. Thompson, and M. Neubauer. As they are only determined up to small cases, we use the computer algebra system GAP to investigate the small cases.

To prove that the polynomials h to be given really fulfill the assertion in (c), we apply a sharpening of Hilbert's irreducibility theorem, which is due to P. Dèbes. I thank Dèbes and Fried for directing me to this and related results. Using the ramification data given in the proof of 8.1, these exceptional polynomials can be computed using the techniques described in [20].

The proof of part (d) is quite elementary.

The proof of 4.2 follows a suggestion by the referee, and simplifies the original argument.

2. Monodromy groups

Let $K \subset \mathbb{C}$ be a number field, and let t be a transcendental over $\mathbb{C}$. Fix an extension L of $K(t)$ of degree n, such that K is algebraically closed in L. Denote by Ω the Galois closure of $L|K(t)$, taken in an algebraic closure of $\mathbb{C}(t)$. Then $G = \mathrm{Gal}(\Omega|K(t))$ is called the **arithmetic monodromy group** of $L|K(t)$, where we regard G as a permutation group, permuting transitively the n conjugates of L in Ω.

Denote by $\hat{K}$ the algebraic closure of K in Ω. Then $\hat{G} = \mathrm{Gal}(\Omega|\hat{K}(t))$ is called the **geometric monodromy group** of $L|K(t)$. Note that $G/\hat{G} \cong \mathrm{Gal}(\hat{K}|K)$,

and that $\hat{G}$ still permutes the n conjugates of L transitively, as L and $\hat{K}(t)$ are linearly disjoint over $K(t)$.

The notion **monodromy group** is justified by the following connection with Riemann surfaces. As $\mathbb{C}(t) \cap \Omega = \hat{K}(t)$ (see [3, Corollary 2, V, §4]), we get $\mathrm{Gal}(\mathbb{C}\Omega|\mathbb{C}(t)) \cong \mathrm{Gal}(\Omega|\hat{K}(t))$ by restriction. For any holomorphic covering α: $A \to B$ of Riemann surfaces, denote by α^*: $\mathcal{M}(B) \hookrightarrow \mathcal{M}(A)$ the natural inclusion of the fields of meromorphic functions on B and A. Associated to $\mathbb{C}L|\mathbb{C}(t)$ is a branched, holomorphic covering π: $S \to \mathbb{P}^1$ of degree n with S a connected Riemann surface and $\mathbb{P}^1$ the Riemann sphere, such that the extension $\mathcal{M}(S)|\pi^*(\mathcal{M}(\mathbb{P}^1))$ can be identified with $\mathbb{C}L|\mathbb{C}(t)$. Observe that $\mathcal{M}(\mathbb{P}^1) \cong \mathbb{C}(t)$.

Let $\mathcal{B} = \{b_1, b_2, \ldots, b_r\}$ be the set of branch points of π. Fix $p \in \mathbb{P}^1 \setminus \mathcal{B}$, and denote by $\mathcal{G}$ the fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathcal{B}, p)$. Then $\mathcal{G}$ acts transitively on the points of the fiber $\pi^{-1}(p)$ by lifting of paths. We fix a numbering $1, 2, \ldots, n$ of this fiber. Thus we get a homomorphism $\mathcal{G} \to \mathrm{S}_n$. By standard arguments, the image of $\mathcal{G}$ can be identified with the geometric monodromy group $\hat{G}$ defined above, thus we write $\hat{G}$ for this group, too.

We choose a standard homotopy basis of $\mathbb{P}^1 \setminus \mathcal{B}$ as follows. Let γ_i be represented by paths w_i which wind once around b_i counterclockwise, and around no other branch point, such that $\gamma_1\gamma_2\cdots\gamma_r = 1$. Then $\gamma_1, \gamma_2, \ldots, \gamma_{r-1}$ freely generate $\mathcal{G}$.

Definition: For $\sigma \in \mathrm{S}_n$, let $e_1, \ldots, e_m$ be the cycle lengths of σ. Define the index of σ by $\mathrm{ind}\,\sigma = \sum_{j=1}^{m}(e_j - 1)$.

Let σ_i be the image of γ_i in S_n. If the points $s_1, \ldots, s_m$ in the fiber of b_i have multiplicities $e_1, \ldots, e_m$, respectively, then σ_i has cycle lengths $e_1, \ldots, e_m$. In particular $\mathrm{ind}\,\sigma_i = n - |\pi^{-1}(b_i)|$. If g denotes the genus of S, then we get

$\hat{G}$ is generated by $\sigma_1, \ldots, \sigma_r$, and the following holds:

$$\sigma_1\sigma_2\cdots\sigma_r = 1, \tag{1}$$

$$\sum_i \mathrm{ind}\,\sigma_i = 2(n - 1 + g), \tag{2}$$

where (2) is a consequence of the Riemann Hurwitz genus formula.

This tuple $\{\sigma_1, \sigma_2, \ldots, \sigma_r\}$ is usually called the **branch cycle description** of the covering π.

Definition: Let $R = P/Q$ be a reduced fraction of the non-trivial rational function $R \in K(X)$ with $P, Q \in K[X]$. Then let $\deg R = \max(\deg P, \deg Q)$ be the degree of R.

We are mainly concerned with the case that the field L is a rational field $K(x)$. Then $t = R(x)$ with a rational function R of degree n. Further, the Riemann surface S is just the Riemann sphere $\mathbb{P}^1$, and the covering map π is induced by the rational map sending $\omega \in \mathbb{P}^1$ to $R(\omega)$.

If we are talking about the arithmetic (or geometric) monodromy group of R, we mean the arithmetic (or geometric) monodromy group of the extension $K(x)|K(t)$. In this case $g = 0$ in (2). A transitive subgroup of S_n with (1) and (2) with $g = 0$ is called a **genus 0 group**, and the two equations will be called the **genus 0 conditions** on a finite group $\hat{G}$.

For later use we record an immediate consequence of Lüroth's theorem, where G is the arithmetic monodromy group of R.

LEMMA 2.1: *Let U be the stabilizer of x in G. Then every group M with $U \leq M \leq G$ yields a composition $R(X) = a(b(X))$ with $a, b \in K(X)$, such that M is the stabilizer of $b(X)$. Furthermore, $[G: M] = \deg a$ and $[M: U] = \deg b$.*

3. Consequences from Siegel's theorem

Let $f(X, Y) \in K[X, Y]$ be an irreducible polynomial, which is monic with respect to Y. Set

$$\mathcal{R}_f = \{x_0 \in \mathcal{O}_K |\ f(x_0, Y) \text{ is reducible in } K[Y]\}.$$

For $R \in K(X)$ define

$$\mathcal{V}_R = R(K) \cap \mathcal{O}_K,$$

that is $\mathcal{V}_R$ consists of those integers of K which R assumes on K. The number-theoretic key for effective versions to Hilbert's irreducibility is Fried's following refinement of an observation of Siegel [26, pp. 244–245]. Fried's proof of [8, Theorem 1] extends easily to a proof of the following result.

THEOREM 3.1: *There are finitely many non-constant rational functions*

$$R_1, R_2, \ldots, R_l \in K(X)$$

with

$$\mathcal{R}_f = \bigcup_{i=1}^{l} \mathcal{V}_{R_i} \cup W,$$

where W is a finite set and the polynomials $f(R_i(X), Y) \in K(X)[Y]$ are reducible for $i = 1, \ldots, l$.

We are going to show that the rational functions R_i can be chosen with rather specific properties. For this choose the R_i subject to $\sum_{i=1}^{l} \deg R_i$ being minimal. Then the following holds. If R_i admits a decomposition $R_i(X) = a(b(X))$ with $a, b \in K(X)$ and $\deg b > 1$, then $f(a(X), Y)$ is irreducible. This is clear, for otherwise $\mathcal{V}_{R_i} \subseteq \mathcal{V}_a \subseteq \mathcal{R}_f$, and we could replace R_i by a. Further, $\mathcal{V}_{R_i}$ is an infinite set, or R_i were superfluous, because we may enlarge W. The latter property on the value set of R_i yields a strong conclusion. By another deep theorem of Siegel [26] (see also the proof of [18, Theorem 8.5.2]), the function R_i has exactly two values over ∞. Interpreting R_i as a map from $K \cup \{\infty\}$ to itself, we write $|R_i^{-1}(\infty)| \leq 2$. We summarize.

COROLLARY 3.2: *There are finitely many rational functions $R_1, R_2, \ldots, R_l \in K(X)$ with*

$$\mathcal{R}_f = \bigcup_{i=1}^{l} \mathcal{V}_{R_i} \cup W,$$

where W is a finite set. For every $R \in \{R_1, R_2, \ldots, R_l\}$ the following holds.

(a) *$f(R(X), Y)$ is reducible in $K(X)[Y]$.*

(b) *If $R(X) = a(b(X))$ with $a, b \in K(X)$ and $\deg b > 1$, then $f(a(X), Y)$ is irreducible.*

(c) $|R^{-1}(\infty)| \leq 2$.

(d) $|R(K) \cap \mathcal{O}_K| = \infty$.

As remarked above, (c) is a consequence (d). However, (d) cannot be interpreted galois-theoretically. So we use the weaker condition (c) instead. At the very late state of the investigation we have to use (d) though.

4. Group-theoretic consequences

In the case of $f(X, Y) = h(Y) - XY^i$ with $\gcd(i, \deg h) = 1$, we outline the translation of conditions (a), (b), and (c) of 3.2 via Galois theory and the monodromy considerations in section 2 to a bunch of conditions on a finite group. This is already contained in [10].

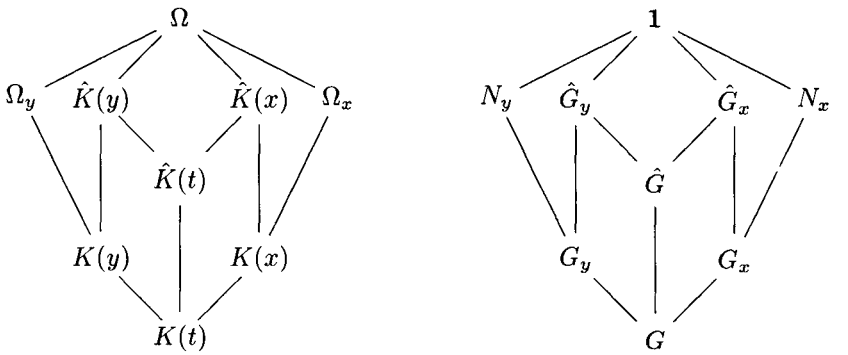
Notations: In the following let $h(Y) \in K[Y]$ be a polynomial of degree n, and i be an integer with $1 \leq i \leq n-1$. Set $H(Y) := h(Y)/Y^i$, and let $R(X) \in K(X)$

be a non-constant rational function. Let t be a transcendental over $\mathbb{C}$, and choose x and y in an algebraic closure of $\mathbb{C}(t)$, such that

$$H(y) = R(x) = t.$$

Denote by Ω the normal closure of $K(x,y)|K(t)$, and set $G = \mathrm{Gal}(\Omega|K(t))$. Denote the normal closure of $K(x)|K(t)$ by Ω_x. Let G_x be the stabilizer in G of x, and denote the stabilizer of Ω_x by N_x. With T_x we denote the permutation representation of G on the $\deg R$ conjugates of x over $K(t)$. Then N_x is just the kernel of this representation, and G/N_x is the arithmetic monodromy group of R. Analogously define the symbols indexed by y.

Let $\hat{K}$ be the algebraic closure of K in Ω. Set $\hat{G} = \mathrm{Gal}(\Omega|\hat{K}(t))$ and $\hat{G}_x = \hat{G} \cap G_x$. The following diagram illustrates the various inclusions of groups and fields.



PROPOSITION 4.1: *Let $h(Y) \in K[Y]$ be a polynomial of degree n, and $1 \leq i \leq n-1$ with $\gcd(i,n) = 1$. Further let $R \in K(X)$ be a non-constant rational function with the following properties.*

(a) *$h(Y) - R(X)Y^i$ is reducible in $K(X)[Y]$.*

(b) *If $R(X) = a(b(X))$ with $a, b \in K(X)$ and $\deg b > 1$, then $h(Y) - a(X)Y^i$ is irreducible in $K(X)[Y]$.*

(c) *$|R^{-1}(\infty)| \leq 2$.*

Then, with the notation from above, the following holds.

(1) $G_xG_y \subset G$ *(proper subset).*

(2) $MG_y = G$ *if* $G_x < M \leq G$.

(3) $T_y(\hat{G})$ *is a primitive group (or equivalently,* $\hat{G} \cap G_y$ *is maximal in* $\hat{G}$*).*

(4) $N_x = N_y = 1$*, that is the representations* T_y *and* T_x *are faithful.*

(5) $T_y(\hat{G})$ *and* $T_x(\hat{G})$ *are transitive. Further,* $\hat{G}$ *possesses a generating system* $\sigma_1, \sigma_2, \ldots, \sigma_r$ *with the following properties.*

(i) $\sigma_1\sigma_2 \cdots \sigma_r = 1$.

(ii) $T_y(\sigma_r)$ *has two cycles, of lengths* i *and* $n - i$.

(iii) $\sum \operatorname{ind} T_y(\sigma_i) = 2(n-1)$.

(iv) $T_x(\sigma_r)$ *has at most two cycles.*

(v) $\sum \operatorname{ind} T_x(\sigma_i) = 2(\deg R - 1)$.

Proof:

To (1): The condition (a), namely that $h(Y) - R(X)Y^i$ is reducible over $K(X)$, says that G_x does permute the conjugates of y intransitively. Since the operation of G_x on the conjugates of y is equivalent to the operation on the left cosets of G_y in G, the assertion follows.

To (2): Now let M fulfill $G_x < M \leq G$. Then there are $a, b \in K(X)$ with $R(X) = a(b(X))$, $\deg b = [M\colon G_x] > 1$, and M is the stabilizer of $K(b(x))$ (see 2.1). The irreducibility of $h(Y) - a(X)Y^i$ (by (b)) just says that M does permute the conjugates of y transitively, thus (2) holds.

The proof of (3) depends on the element σ_r of (5), so we first prove (5).

To (5): The transitivity of $T_y(\hat{G})$ is a direct consequence of the fact that $h(Y) - tY^i$ is irreducible even over $\hat{K}(t)$. Indeed, $T_y(\hat{G})$ is just the geometric monodromy group of H. The same argument works for $T_x(\hat{G})$.

Let $\mathcal{B}$ be the union of the branch points in $\mathbb{P}^1$ of the coverings $H\colon \mathbb{P}^1 \to \mathbb{P}^1$ and $R\colon \mathbb{P}^1 \to \mathbb{P}^1$. Suppose further $\infty \in \mathcal{B}$ (that is automatically the case if $n > 2$). Fix $p \in \mathbb{P}^1 \setminus \mathcal{B}$, and choose a generating system $\gamma_1, \gamma_2, \ldots, \gamma_r$ of the fundamental group $\mathcal{G} = \pi_1(\mathbb{P}^1 \setminus \mathcal{B}, p)$ as in section 2, where γ_r corresponds to ∞. We get homomorphisms $\mathcal{G} \to \hat{G}/(\hat{G} \cap N_x)$ and $\mathcal{G} \to \hat{G}/(\hat{G} \cap N_y)$ of $\mathcal{G}$ into the geometric monodromy groups of R and H, respectively. As Ω is the composite of Ω_x and Ω_y, the groups N_x and N_y intersect trivially. Thus we get a canonical injection

$\hat{G} \to \hat{G}/(\hat{G} \cap N_x) \times \hat{G}/(\hat{G} \cap N_y)$. From this we obtain a natural homomorphism $\mathcal{G} \to \hat{G}$, and the images σ_i of the elements γ_i fulfill (i), (iii), and (v).

We get (ii), because above ∞ there are, with respect to $H(Y) = h(Y)/Y^i$, the i-fold point 0 and the $(n-i)$-fold point ∞. Analogously (iv) follows from (c).

To (3): If $T_y(\hat{G})$ were not primitive, then there would be a non-trivial partition of the set which $T_y(\hat{G})$ acts on in blocks of imprimitivity. However, $T_y(\sigma_r^{n-i})$ is an i-cycle as $\gcd(i, n-i) = 1$, and $T_y(\sigma_r^i)$ is an $(n-i)$-cycle. This shows that every block would be contained in one of the cycles of $T_y(\sigma_r)$, a contradiction for divisibility reasons.

To (4): From (1) we get $N_x G_y < G$, and (3) implies that G_y is maximal in G (because $T_y(G) \geq T_y(\hat{G})$ is primitive). Thus N_x is contained in G_y, and we get $N_x \leq N_y$ (as N_y is the biggest normal subgroup of G which is contained in G_y). We get the other inclusion as follows. Suppose $N_y \not\leq N_x$, then $N_y \not\leq G_x$. Now, with $M = G_x N_y$ and using (1), we get a contradiction to (2): $G_x < MG_y = G_x G_y < G$. As N_x and N_y intersect trivially, (4) follows. ∎

Next we show that the configuration is rather restricted if $2 \leq i \leq n-2$.

PROPOSITION 4.2: *Suppose that* $2 \leq i \leq n-2$ *in Proposition* 4.1. *Then* $G = A_n$ *or* S_n, T_y *is a natural representation of degree* n, *and the subgroups* G_x *and* G_y *are conjugate in* G.

Proof: Let σ be the element σ_r in (5). Obviously $n \geq 5$. As we will use only (1), (2), (3), (4), (5)(ii), and (5)(iv) of 4.1, we may assume $2 \leq i < n/2$. From (3) we get that $T_y(G)$ is primitive, and (5)(ii) tells us that $T_y(\sigma^{n-i})$ is an i-cycle. Hence $T_y(G) = \mathrm{A}_n$ or S_n in the natural representation, by an old theorem of Marggraf; see [27, 13.8]. Let m be the length of the smallest orbit of the (by (1)) intransitive subgroup $T_y(G_x)$ of $T_y(G)$. As $T_y(M)$ is transitive for every proper overgroup M of G_x, we get that $T_y(G_x)$ is the full stabilizer in $T_y(G)$ of a set of size m. Thus the representation T_x of G is given by the natural action of G on the subsets of size m of $\{1, 2, \ldots, n\}$. Suppose that $m \geq 2$. Let Γ be an orbit of size i of $T_y(\langle\sigma\rangle)$. Then there are subsets of $\{1, 2, \ldots, n\}$ of size m which intersect Γ in 0, 1, and 2 elements respectively. These three subsets cannot be conjugate under the action of σ, contradicting the assumption that $T_x(\sigma)$ has at most 2 cycles. Thus $m = 1$ and G_x and G_y are conjugate. ∎

5. Some results for $i = 1$

As mentioned already in the Introduction, the case $i = 1$ differs strongly from the easy case $2 \leq i \leq n-2$ we just dealt with. Later we will classify all configurations such that (1) through (4) in Proposition 4.1 hold, and that $T_y(G)$ contains an $(n-1)$-cycle. The following Proposition 5.2 is a preparatory result towards this. The technical part (ii) of 5.2 will replace the usage of the classification of the finite simple groups when proving Theorem 1.3(a). That is if we would use the classification, the proof of (a) could be shortened.

Before this we need a simple character-theoretic fact about 2-transitive groups.

LEMMA 5.1: *Let G be 2-transitive of degree n, and let V be a subgroup of G. Denote by χ the permutation character of G (i.e. $\chi(g)$ is the number of fixed points of $g \in G$). Let $\mathbf{1}_V$ be the trivial character of V. Then the induced character $\mathbf{1}_V^G$ is the permutation character of G with respect to the action on the right cosets of V in G. Then the following holds.*

(i) *If $[G: V] < n$, then V is transitive.*

(ii) *If $[G: V] = n$, and V is intransitive, then $\chi = \mathbf{1}_V^G$.*

Proof: Let b be the number of orbits of V. Then (see [13, 4.3.5])

$$b = (\chi|_V, \mathbf{1}_V)_V.$$

Frobenius' reciprocity [13, 4.4.5] yields

$$b = (\chi|_V, \mathbf{1}_V)_V = (\chi, \mathbf{1}_V^G)_G.$$

As G is 2-transitive, χ is the sum $\mathbf{1} + \psi$ of the trivial character and an irreducible character ψ [13, 4.3.4(ii)]. In order to show (i) and (ii), suppose that V is intransitive, hence $b > 1$. From the above, ψ is a summand of the character $\mathbf{1}_V^G$. Because the trivial character is also a summand of $\mathbf{1}_V^G$, we get

$$\mathbf{1}_V^G = \chi + \phi$$

with ϕ a sum of non-negative multiples of irreducible characters of G. Evaluating in $1 \in G$ yields

$$[G: V] = n + \phi(1) \geq n$$

with equality if and only if ϕ is 0. From this the assertion follows. ∎

In the following it does not matter whether we consider right or left cosets, as changing the side amounts to passing to a permutation equivalent representation.

PROPOSITION 5.2: *Let G_x and G_y be two subgroups of a finite group G, such that G acts faithfully via T_x (resp. T_y) on the cosets of G_x (resp. G_y) in G. Let $n = [G\colon G_y]$ be the degree of T_y. Let σ be an element of G, such that the following conditions hold.*

(1) $G_xG_y < G$.

(2) $MG_y = G$ *if* $G_x < M \leq G$.

(3) $T_y(\sigma)$ *is an* $(n-1)$*-cycle.*

(4) $T_x(\sigma)$ *has at most two cycles.*

Then the following holds.

(i) $T_x(\sigma)$ *has two cycles of lengths* l *and* $n-1$*, where* l *divides* $n-1$*. Furthermore,* $T_x(G_y)$ *has exactly two orbits of lengths* l *and* $n-1$.

(ii) *Suppose that* $T_y(G)$ *is 3-transitive and that* G_x *and* G_y *are not conjugate. Then* $l = n-1$*. Let* Σ *be the support of* T_y *(i.e. the coset space* G/G_y*), and* $\Sigma^\star$ *be the set* Σ *minus the point fixed by* $T_y(G_y)$*. Hence* $T_y(G_y)$ *acts 2-transitively on* $\Sigma^\star$*. Let* U *and* V *be subgroups of* G_y*, such that* $T_y(U)$ *is a point stabilizer of this representation on* $\Sigma^\star$*, and that* $T_x(V)$ *is a point stabilizer of the representation of* $T_x(G_y)$ *on one of its two orbits. Then* $\mathbf{1}_U^{G_y} = \mathbf{1}_V^{G_y}$*, however* U *and* V *are not conjugate in* G_y*, except for* $n = 4$.

Proof: Without loss of generality assume $\sigma \in G_y$. Obviously $T_y(G)$ is a 2-transitive permutation group. The group $T_x(G_y)$ is intransitive by (1), on the other hand it has at most two orbits by (4). Thus $T_x(G_y)$ has exactly two orbits of lengths $k \geq l \geq 1$, and these are just the cycles of $T_x(\sigma)$. As the orders of $T_x(\sigma)$ and $T_y(\sigma)$ are the same, we get $n-1 = \operatorname{lcm}(k,l)$. The intransitivity of $T_x(G_y)$, together with 5.1(i), implies $k+l \geq n$. From this we conclude $k = n-1$ and $l|n-1$. This proves (i).

From now on let $T_y(G)$ be 3-transitive. We are going to apply 5.1(i) and (ii) to the action of $T_y(G_y)$ on the $(n-1)$-element set $\Sigma^\star$. Note that $V = G_y \cap G_x^g$ for a suitable $g \in G$. First suppose that $T_y(V)$ is transitive on $\Sigma^\star$. Then $T_y(G_x)$ is either transitive on Σ — contrary to (1), or $G_x^g \leq G_y$ — contrary to (2) in connection with the non-conjugacy of G_y and G_x. Thus $T_y(V)$ acts intransitively on $\Sigma^\star$, and from 5.1(i) we get $[G_y\colon V] \geq n-1$, hence $l = n-1$ by (i). The assertion about the induced characters then follows from 5.1(ii).

It remains to show that the subgroups U and V of G_y are not conjugate in G_y, except for $n = 4$. Suppose they are conjugate. Then $T_y(V)$ has an orbit of length $n-2$ on $\Sigma^\star$, since $T_y(U)$ has an orbit of this length on $\Sigma^\star$. Thus $T_y(G_x)$

has an orbit of length at least $n-2$ on Σ. We have seen above that $T_y(G_x)$ is neither transitive, nor does it fix a point. Thus $T_y(G_x)$ has an orbit of length 2. Without loss we may assume that $T_y(G_y)$ fixes one of these two points. Then the following holds:

$$2 = \frac{|G_y G_x|}{|G_y|} = \frac{|G_x G_y|}{|G_x|}\frac{[G\colon G_y]}{[G\colon G_x]} = (n-1)\frac{n}{2(n-1)} = \frac{n}{2},$$

hence $n = 4$, and the assertion follows. ∎

6. Permutation groups of degree n containing an $(n-1)$-cycle

Let G be a group acting primitively on an n-set Σ. Denote by A a minimal normal subgroup of G. Suppose that A is elementary abelian of order p^m with p a prime. Then A acts sharply transitively on Σ. Fix a point $\omega \in \Sigma$, and identify the elements $a \in A$ bijectively with $\omega^a \in \Sigma$. Denote by U the stabilizer in G of ω. Then $G = A \rtimes U$, and the action of U on Σ yields a linear action on A via this identification, as $(\omega^a)^u = \omega^{u^{-1}au}$. U acts faithfully on A by conjugation, because A is transitive. Thus we can identify A with the vector space $\mathbb{F}_p^m$, and U is a subgroup of $\mathrm{GL}_m(p)$. The action of G on Σ is described by the action of $A \rtimes U$ on the affine space A.

If this situation arises, we will say that G is an **affine group**.

We say that a group G is **projective**, if $\mathrm{PSL}_m(q) \leq G \leq \mathrm{P\Gamma L}_m(q)$ (q a prime power), where G acts naturally on the points of the projective space of dimension $m-1$.

In particular, the projective special linear group $\mathrm{PSL}_2(p)$ (p a prime) will always, unless otherwise said, be considered as the permutation group of degree $p+1$ on the projective line over $\mathbb{F}_p$.

By M_n ($n \in \{11, 12, 22, 23, 24\}$) we denote the Mathieu group in its natural multiply transitive representation of degree n. However, for M_{11} we will mostly consider the 3-transitive representation of degree 12.

Without using the classification of finite simple groups (and results derived from this), we prove

THEOREM 6.1: *Let G be a transitive permutation group of degree n which contains an $(n-1)$-cycle. Then G is affine, or $\mathrm{PSL}_2(p)$ with $p \geq 5$ prime, or 3-transitive.*

Using the classification of the 3-transitive permutation groups, which rests on the classification of the finite simple groups, we will get

THEOREM 6.2: *Let G be a transitive permutation group of degree n which contains an $(n-1)$-cycle. Then G is affine or A_n (n even), S_n, $\mathrm{PSL}_2(p)$ or $\mathrm{PGL}_2(p)$ with $p \geq 5$ prime, M_{11} of degree 12, M_{12}, or M_{24}.*

Using a result of W. Kantor [16], which does not rely on the classification of the finite simple groups, we can specify the affine groups with an $(n-1)$-cycle.

LEMMA 6.3: *Let G be an affine group of degree n containing an $(n-1)$-cycle. Then $n = q^e$ with some prime power q and $G = \mathbb{F}_q^e \rtimes U$ with $\mathrm{GL}_e(q) \leq U \leq \Gamma L_e(q)$. Thereby G acts naturally on the affine space $\mathbb{F}_q^e$.*

The essential tools in the proof of Theorem 6.1 are the following pre-classification results of O'Nan and Aschbacher.

THEOREM 6.4 (O'Nan [24, Theorem D]): *Let G be a 2-transitive group on the finite set Σ. Denote by G_ω the stabilizer of some $\omega \in \Sigma$. Suppose N is a normal subgroup of G_ω which is 2-transitive on each of its orbits on $\Sigma \setminus \{\omega\}$. Then one of the following holds.*

(1) *N is transitive on $\Sigma \setminus \{\omega\}$ and G is 3-transitive.*
(2) *G is projective.*
(3) *$|N| = 2$ and G is affine.*

THEOREM 6.5 (O'Nan [24, Proposition 4]): *Let G be a 2-transitive group on the finite set Σ. Let N be a normal subgroup of the stabilizer G_ω of $\omega \in \Sigma$. Then one of the following holds.*

(1) *N restricts faithfully to its orbits on $\Sigma \setminus \{\omega\}$.*
(2) *G is projective.*

THEOREM 6.6 (Aschbacher [1, Theorem 3]): *Let G be a 2-transitive group on the finite set Σ. Let N be a non-trivial cyclic normal subgroup of the stabilizer G_ω of $\omega \in \Sigma$. Then one of the following holds.*

(1) *G is affine.*
(2) *G normalizes $\mathrm{PSL}_2(q)$.*
(3) *G normalizes $\mathrm{PSU}_3(q)$ in its natural 2-transitive representation of degree $q^3 + 1$ (cf. [15, II, 10.12]).*
(4) *$G = \mathrm{P\Gamma L}_2(8)$ of degree 28.*

Remark: That the groups in 6.2, and, for the affine case, in 6.3, really contain an $(n-1)$-cycle is clear. In the affine case, this follows from the existence of a Singer group in $\mathrm{GL}_m(q)$ (to be obtained from the regular representation of the multiplicative group of $\mathbb{F}_{q^e}$ on $\mathbb{F}_{q^e} \cong A$). If G is neither affine, alternating, nor symmetric, then the degree is $p+1$ with a prime p. As p divides the order of G, it contains an element of order p.

PROOF OF 6.1 AND 6.3. We proceed in several steps. If G is affine, then $G = A \rtimes U$ with $A \cong \mathbb{F}_p^m$ and $U \leq \mathrm{GL}_m(p)$. Then U contains an element which cyclically permutes the non-zero elements of A. W. Kantor classified linear groups with these properties; we just get 6.3 from [16].

From now on assume that G is not affine, and denote by Σ the set which G is acting on. Let σ be an $(n-1)$-cycle in G, and $\omega \in \Sigma$ be a fix-point of σ. Denote by G_ω the stabilizer of ω. We are going to construct a normal subgroup of G_ω. Set $\Sigma \setminus \{\omega\} = \Sigma^\star$ and $Z := \langle\sigma\rangle$. Then Z acts sharply transitively on $\Sigma^\star$. Write $\Sigma^\star$ as a disjoint union $\Delta_1 \cup \Delta_2 \cup \cdots \cup \Delta_t$ of subsets Δ_i which are permuted by G_ω, subject to $|\Delta_1| > 1$ being minimal. Set $\Delta = \Delta_1$ and let $G_\Delta \leq G_\omega$ be the setwise stabilizer of Δ. By minimality of $|\Delta_1|$, the group G_Δ restricts to a primitive group on Δ. Set $Z_\Delta = Z \cap G_\Delta$. The cyclic group Z permutes the Δ_i's transitively, and Z_Δ fixes every Δ_i as Z is abelian. Thus the sets Δ_i are just the orbits of Z_Δ on $\Sigma^\star$. Denote by N the kernel of the action of G_ω on $\{\Delta_1, \Delta_2, \ldots, \Delta_t\}$. Then clearly $Z_\Delta \leq N \trianglelefteq G_\omega$.

STEP 6.7: *N acts primitively on every Δ_i.*

Proof: It suffices to show that N is primitive on Δ. Suppose that Δ admits a non-trivial partition in blocks $\Gamma_1, \ldots, \Gamma_m$ of imprimitivity with respect to the action of N. Similarly as above, we see that the sets Γ_j are the orbits of a subgroup of Z_Δ with order $|\Gamma_1|$. Let $g \in G_\Delta$ and $x \in N$ be arbitrary. Then $x' = gxg^{-1} \in N$ and $\Gamma_j^{x'} = \Gamma_{j'}$. From

$$(\Gamma_j^g)^x = \Gamma_j^{gxg^{-1}g} = \Gamma_j^{x'g} = \Gamma_{j'}^g$$

we see that $\{\Gamma_1^g, \ldots, \Gamma_m^g\}$ is also a partition of Δ in blocks of imprimitivity with respect to the action of N. In particular, the sets Γ_j^g are the orbits of the same subgroup of Z_Δ, as Z_Δ is cyclic. This shows that $\{\Gamma_1, \ldots, \Gamma_m\}$ is a partition in blocks which are permuted by G_Δ, contrary to the primitivity of G_Δ on Δ. ∎

STEP 6.8: *N is either 2-transitive on its orbits in $\Sigma^\star$, or G is either projective, or $\mathrm{P\Gamma L}_2(8)$ of degree 28, or normalizes $\mathrm{PSU}_3(q)$ in its natural representation of degree q^3+1.*

Proof: N is primitive on Δ by 6.7. N contains the on Δ sharply transitive subgroup Z_Δ. Suppose that N is not 2-transitive on Δ. By classical theorems of Schur and Burnside (see [27, 11.7 and 25.3]), we get $|Z_\Delta| = p$ with p a prime, and Z_Δ is a characteristic subgroup of the restriction $N|_\Delta$. Suppose that G is not projective. Then N acts faithfully on Δ by Theorem 6.5. In particular Z_Δ is a non-trivial cyclic normal subgroup of G_ω. Now Theorem 6.6 yields the assertion. ∎

STEP 6.9: *G is projective or 3-transitive.*

Proof: If N acts 2-transitively on its orbits in $\Sigma^\star$, then Theorem 6.4 yields the assertion. In virtue of 6.8 we merely have to exclude the groups $\mathrm{P\Gamma L}_2(8)$ and G with $\mathrm{PSU}_3(q) \trianglelefteq G$.

We begin with $G = \mathrm{P\Gamma L}_2(8)$. Suppose that G contains an element of order 27. Then a suitable power of a preimage of this element in $\Gamma\mathrm{L}_2(8)$ has order 27 as well. We use the natural embedding $\Gamma\mathrm{L}_2(8) \hookrightarrow \mathrm{GL}_6(2)$ to find an element $\tau \in \mathrm{GL}_6(2)$ of order 27. We use $\gcd(27,2) = 1$, together with Maschke's Theorem [13, 3.3.1], to write $\mathbb{F}_2^6$ as a direct sum $V_1 \oplus \cdots \oplus V_r$ of subspaces which are invariant and irreducible under τ. Now 27 is the lowest common multiple of the orders of the restrictions $\tau|_{V_i}$. Thus $\tau|_{V_i}$ has order 27 for one index i. Let d be the dimension of this V_i. Schur's Lemma [13, 3.5.2] tells us that τ can be regarded in a natural way as an element of the multiplicative group of $\mathbb{F}_{2^d}$. However $27|(2^d-1)$, together with $1 \le d \le 6$, yields a contradiction.

Now let G normalize $\mathrm{PSU}_3(q)$, hence $G \le \mathrm{P\Gamma U}_3(q)$ as we conclude from the knowledge of the group of outer automorphisms of $\mathrm{PSU}_3(q)$, cf. [4]. Note that $q \ge 3$ as G is supposed to be not affine. Assume that $\mathrm{P\Gamma U}_3(q)$ does contain an element of order q^3. From $\Gamma\mathrm{L}_3(q^2) \ge \Gamma\mathrm{U}_3(q)$ we see that also $\Gamma\mathrm{L}_3(q^2)$ does contain an element of order q^3. Set $q = p^e$ with p a prime. Using the embedding $\Gamma\mathrm{L}_3(q^2) \hookrightarrow \mathrm{GL}_{6e}(p)$, we find an element $\tau \in \mathrm{GL}_{6e}(p)$ of order p^{3e}. Obviously τ is a unipotent matrix. Write $1 + \mathcal{N}$ with a nilpotent matrix $\mathcal{N}$. Let w be the smallest power of p with $w \ge 6e$. Then $w < 6pe$ and $\mathcal{N}^w = 0$. We get

$$\tau^w = (1+\mathcal{N})^w = 1^w + \mathcal{N}^w = 1,$$

hence $p^{3e} \leq w$. This yields $p^{3e} < 6pe$, and finally we get $e = 1$ and $p = 2$, contrary to $q \geq 3$. ∎

STEP 6.10: *Let G be projective. Then $G = \mathrm{PSL}_2(p)$ or $G = \mathrm{PGL}_2(p)$ for a prime p, or $G = \mathrm{P\Gamma L}_2(4) = S_5$.*

Proof: We investigate the group $\mathrm{P\Gamma L}_m(q)$ with $m \geq 2$ and $n = \frac{q^m-1}{q-1}$ with $q = p^e$, $p \in \mathbb{P}$. It suffices to show that the presence of an $(n-1)$-cycle forces $m = 2$ and $q \in \mathbb{P} \cup \{4\}$. Let $\tau \in \Gamma\mathrm{L}_m(q)$ be a preimage of an $(n-1)$-cycle in $\mathrm{P\Gamma L}_m(q)$. Then $|\tau| = (n-1) \cdot l$ with $l | q-1$. Furthermore, $\langle \tau \rangle$ fixes a one-dimensional subspace L of $\mathbb{F}_q^m$, and acts with orbits of lengths $\geq n-1$ on $\mathbb{F}_q^m \setminus L$. Set $\rho := \tau^q$, then $|\rho| = |\tau|/q = l \cdot (q^{m-1}-1)/(q-1)$. We identify $\mathbb{F}_q^m$ with $\mathbb{F}_p^{em}$. Then $\langle \rho \rangle$ has orbits of lengths $\geq (n-1)/q$ on $\mathbb{F}_p^{em} \setminus L$. From $\gcd(|\rho|, p) = 1$ and Maschke's Theorem we get

$$\mathbb{F}_p^{em} = L \oplus V_1 \oplus V_2 \oplus \ldots \oplus V_r$$

with ρ-irreducible subspaces V_i. For any $\mathbf{0} \neq \mathbf{v} \in V_i$ we get

$$|V_i| > |\mathbf{v}^{\langle \rho \rangle}| \geq \frac{n-1}{q} = \frac{q^{m-1}-1}{q-1} = 1 + p^e + \cdots + p^{e(m-2)} \geq p^{e(m-2)},$$

hence

$$\dim V_i \geq 1 + e(m-2).$$

First consider $m \geq 3$. From

$$me = \dim L + \sum_{i=1}^{r} \dim V_i$$

we get

$$me \geq e + r \cdot (1 + e(m-2)),$$

hence

$$r \leq \frac{e(m-1)}{1+e(m-2)} < \frac{m-1}{m-2} \leq 2,$$

and therefore $r = 1$. This implies

$$\dim V_1 = e(m-1). \tag{3}$$

Now V_1^τ is also invariant and irreducible under ρ. But $V_1 \cap V_1^\tau = \{0\}$ is impossible, for this would imply $e + 2e(m-1) \leq em$, hence $m = 1$. This leaves the only alternative $V_1^\tau = V_1$. For $\mathbf{0} \neq \mathbf{v} \in V_1$ we get

$$|V_1| > |\mathbf{v}^{\langle \tau \rangle}| \geq n - 1 = q + q^2 + \cdots + q^{m-1},$$

hence $\dim V_1 > e(m-1)$, contradicting (3).

Thus $m = 2$. Then $n-1 = q$, and τ^l is an element of order q in $\Gamma\mathrm{L}_2(q)$, because $\gcd(l, q) = 1$. We conclude that $\mathrm{GL}_{2e}(p)$ contains an element σ of order q. We finish similarly as in the proof of 6.9. The element σ is unipotent, so $\sigma = \mathbf{1} + \mathcal{N}$ with a nilpotent matrix $\mathcal{N}$. Let w be the smallest p-power greater than or equal to $2e$. Then $\mathcal{N}^w = 0$ and $w < 2pe$. It follows $\sigma^w = 1$, hence

$$p^e = q = |\sigma| \leq w < 2pe$$

and therefore

$$p^{e-1} < 2e.$$

From $2^{e-1} < 2e$ if $e \geq 4$ we get $e \leq 3$. If $e > 1$, then $p = 2$, $e = 2$ or 3, or $p = 3$, $e = 2$.

But $\mathrm{P\Gamma L}_2(9)$ contains no element of order 9, because such an element was contained in $\mathrm{PGL}_2(9)$. However, the latter group has an elementary abelian Sylow 3-subgroup.

Analogously exclude $\mathrm{P\Gamma L}_2(8)$.

The case $\mathrm{P\Gamma L}_2(4) \cong \mathrm{S}_5$ occurs, of course. ∎

PROOF OF 6.2. In view of 6.1, we may assume that G is 3-transitive, but neither alternating, symmetric, or projective. But then the classification of the 3-transitive groups (see e.g. [2, Section 5], together with [4]) tells us $G = \mathrm{M}_{11}$ of degree 11 or 12, M_{12}, M_{22}, $\mathrm{Aut}(\mathrm{M}_{22})$, M_{23} or M_{24}. A look into [4] shows us that none of these groups contains an element of order $n-1$, except for M_{11} with $n = 12$.

7. Groups which meet the conditions from Proposition 5.2

In this section we classify the group theoretic configurations from 5.2. For the sake of easier reading, we change the notation a bit. We let G be the permutation group $T_y(G)$, and set $V = G_x$. The action T_x is then just the action of G on the coset space G/V.

The conclusions in Proposition 7.1(a) are just necessary conditions. A partial converse, i.e. a construction of V which meets all the requirements, is given in Proposition 7.2.

We adapt the conditions (1) to (4) from Proposition 5.2 to this new notation.

PROPOSITION 7.1: *Let G be a transitive group of degree n, which contains a subgroup V and an element σ subject to following conditions.*

(1) *V is intransitive.*

(2) *Every group M with $V < M \leq G$ is transitive.*

(3) *σ is an $(n-1)$-cycle.*

(4) *σ has at most two cycles on the coset space G/V.*

Then the cycle lengths of σ acting on the coset space G/V are $n-1$ and l as below, and one of the following holds.

(a) *$G = A \rtimes U$ is affine with $A \cong \mathbb{F}_p^m$, $U \leq \mathrm{GL}_m(p)$, and $n = p^m$. Let p^r be the index of $V \cap A$ in A. Then $l = \frac{p^m-1}{p^r-1}$. Let $\tilde{V}$ be a conjugate of V with $|\tilde{V} \cap U|$ being maximal. Then $\tilde{V} = N_U(\tilde{V} \cap A)(\tilde{V} \cap A)$.*

(b) *If G is not affine, then either G is a group as in 6.2, and V a point stabilizer, or one of the following holds.*

(i) *$n = 6$, $l = 5$, $G = \mathrm{PSL}_2(5)$, and V is isomorphic to the dihedral group of order 6.*

(ii) *$n = 8$, $l = 7$, $G = \mathrm{PSL}_2(7)$, and $V \cong A_4$.*

(iii) *$n = 12$, $l = 11$, $G = M_{11}$, and $V \cong A_6$.*

Proof: The action of G on G/V is faithful; see the proof of 4.1(4). Thus all conditions of 5.2 are fulfilled, so from 5.2(i) we know already that σ has orbits of lengths $n-1$ and l with $l|n-1$ on G/V.

TO (a): Without loss assume $\sigma \in U$. From 5.2(i) we get that the two cycles of σ on G/V are just the two orbits of U on G/V. Replace V by a conjugate of itself, such that $V \cap U$ is maximal. Then the orbit of U on G/V containing the coset V has length l, thus

$$l = \frac{|VU|}{|V|} = \frac{|U|}{|V \cap U|}.$$

Set $s = \frac{n-1}{l}$ and consider the orbit of V on G/U through U. This orbit has length

$$\frac{|UV|}{|U|} = \frac{|U|}{|U \cap V|} \cdot \frac{[G:U]}{[G:V]} = l \cdot \frac{n}{n-1+l} = \frac{n}{1+s}.$$

Further, the group $V \cap A$ of order p^{m-r} acts fixed-point-freely on this orbit. We get

$$p^{m-r} | \frac{n}{1+s} = \frac{p^m}{1+s},$$

hence

$$1 + s | p^r. \tag{4}$$

The lengths of the orbits of A on G/V are $[A\colon A \cap V] = p^r$. Thus

$$p^r | n - 1 + l = (n-1)\left(1 + \frac{1}{s}\right),$$

hence $p^r | 1 + s$. Together with (4) we get $s = p^r - 1$, thus l is as claimed. Further, as we have equality in (4), we see that $V \cap A$ — with respect to the action on G/U — is transitive on the V-orbit through U. Rephrased in terms of subgroups that means $UV = U(A \cap V)$. The modular property yields $V = (U \cap V)(A \cap V)$. Obviously $U \cap V \leq N_U(A \cap V)$, thus $V \leq N_U(A \cap V)(A \cap V)$. The other inclusion holds as well, for otherwise the (on G/U) intransitive group $N_U(V \cap A)(V \cap A)$ would properly contain V, contrary to condition (2).

To (b): Now G is not affine, and by (3) we know G from Theorem 6.2. The case $G = \mathrm{A}_n$ or S_n has been dealt with in the proof of Proposition 4.2; there we used the assumption $2 \leq i \leq n-2$ only to assure that G is the alternating or symmetric group.

Thus these groups are excluded by now. In the other cases $n = 1 + p$ with p a prime holds, and p divides the order of G. Let U be the stabilizer of a point. First suppose $l = 1$. Then U is contained in a conjugate of V, and therefore conjugate to V because both groups have the same index $n = n - 1 + l$ in G. That is V is a point stabilizer.

From now on suppose $l > 1$. We get $l = p$ from $l | n - 1$, hence $[G\colon V] = 2p$. Using the atlas of finite simple groups [4], we see that the Mathieu groups M_{12} and M_{24} do not contain subgroups of index $2p$.

Now we investigate M_{11} in its 3-transitive representation of degree 12, using [4]. The group M_{11} contains exactly one conjugacy class of subgroups of index 22. Let V be one of these groups; it is isomorphic to A_6. As A_6 does not contain a subgroup of index 12, it is intransitive. But every group M which contains V properly is transitive by Lemma 5.1(i). It is clear that an element $\sigma \in \mathrm{M}_{11}$ of order 11 has two cycles of length 11 on G/V, for otherwise it would be contained in some conjugate of V; however 11 does not divide $|\mathrm{A}_6|$.

Now suppose $G = \mathrm{PSL}_2(p)$. Then $|V| = \frac{|G|}{2p} = \frac{p^2-1}{4}$, and the Dickson list of subgroups of $\mathrm{PSL}_2(p)$, given in [15, II, 8.27], shows that only the possibilities from (b)(i) and (ii) can occur.

If $G = \mathrm{PSL}_2(5)$ and V dihedral of order 6, then V is intransitive, for otherwise V would be sharply transitive; however the involutions in $\mathrm{PSL}_2(5)$ have fixed points.

If $G = \mathrm{PSL}_2(7)$ and $V \cong \mathrm{A}_4$, then V is intransitive, as $n = 8 \nmid 12 = |V|$. The groups M containing V properly are again transitive by 5.1(i), and the same argument as above shows that an element of order p has two cycles on G/V.

Now we exclude $G = \mathrm{PGL}_2(p)$. Let $U \cong \mathrm{AGL}_1(p)$ be a point stabilizer. As G is 3-transitive, we can apply 5.2(ii) to get the assertion that $\mathrm{AGL}_1(p)$ would have two permutation inequivalent transitive representations of degree p. That is a contradiction, as any two subgroups of order $p-1$ in U are conjugate. ∎

A partial converse to 7.1(a) is

PROPOSITION 7.2: *Let q be a prime power and $G = A \rtimes U$ be an affine group with $A = \mathbb{F}_q^e$ and $U \leq \Gamma L_e(q)$, where U contains an (q^e-1)-cycle σ. Let B be a hyperplane in A, and $V := N_U(B) \cdot B$. Then G, V, and σ fulfill* (1) *to* (4) *in Proposition* 7.1.

Proof: With respect to the affine operation of G on A, the group V is just the setwise stabilizer of B. Thus V is intransitive. If $V < M \leq G$, then there is $x \in A \setminus B$ with $x \in B^M$. Then $A = B \oplus \mathbb{F}_q \cdot x \leq B^M$, and M is transitive.

It remains to show that $\langle\sigma\rangle$ has at most two orbits on G/V. As G is transitive on the set $\mathcal{B}$ of the affine hyperplanes, we get that the representation of G on G/V is equivalent to the representation on $\mathcal{B}$. The group $\langle\sigma\rangle$ acts transitively on $A \setminus \{0\}$, hence $\langle\sigma\rangle$ is also transitive on the parallel classes of $\mathcal{B}$. The assertion follows, as $\sigma^{(q^e-1)/(q-1)}$ generates the group of scalars, which has two orbits on every parallel class of $\mathcal{B}$. ∎

8. The genus 0 condition

We continue to investigate the configurations fulfilling (1) to (5) in Proposition 4.1 for $i = 1$, now by making heavy use of condition (5). Later we see that we merely need to know the cases when G_y is not conjugate to G_x.

By a **hyperplane stabilizer** we mean a subgroup V of G as in 7.2.

PROPOSITION 8.1: *Let G_x and G_y be two non-conjugate subgroups of the finite group G. Denote by T_x (resp. T_y) the action of G on the cosets of G_x (resp. G_y). Let $n = [G\colon G_y]$ be the degree of T_y. Furthermore, let $\hat{G}$ be a normal subgroup*

of G, such that the conditions (1) *to* (5) *in Proposition* 4.1 *are fulfilled for $i = 1$. Then one of the following holds, and each of these cases actually fulfills all these requirements.*

(a) $n = 4$, $T_y(\hat{G}) = A_4$, $T_y(\hat{G} \cap G_x)$ *has order* 2.

(b) $n = 4$, $T_y(\hat{G}) = T_y(G) = S_4$, $T_y(G_x)$ *is the intransitive subgroup of order* 4.

(c) $n = 16$, $T_y(\hat{G}) = T_y(G) = \mathrm{A\Gamma L}_2(4)$, $T_y(G_x)$ *is a hyperplane stabilizer (with* $q = 4$ *in* 7.2).

(d) $n = 9$, $T_y(\hat{G}) = T_y(G) = \mathrm{A\Gamma L}_1(9)$, $T_y(G_x)$ *is a hyperplane stabilizer.*

(e) $n = 9$, $T_y(\hat{G}) = T_y(G) = \mathrm{AGL}_2(3)$, $T_y(G_x)$ *is a hyperplane stabilizer.*

(f) $n = 6$, $T_y(\hat{G}) = T_y(G) = \mathrm{PSL}_2(5)$, $T_y(G_x) \cong D_3$.

(g) $n = 8$, $T_y(\hat{G}) = T_y(G) = \mathrm{PSL}_2(7)$, $T_y(G_x) \cong A_4$.

(h) $n = 12$, $T_y(\hat{G}) = T_y(G) = M_{11}$, $T_y(G_x) \cong A_6$.

Proof: We regard G as a permutation group represented via T_y, so we omit the symbol T_y during the proof.

We split the proof into two cases.

G **affine.** As G normalizes the unique minimal normal subgroup A of $\hat{G}$ (uniqueness follows from 2-transitivity of $\hat{G}$), we get that $\hat{G}$ is affine too.

Affine primitive groups $\hat{G}$ which satisfy the conditions 4.1(5)(i) and (iii) have been classified by Guralnick, Thompson, and Neubauer up to small cases.

Choose an $(n-1)$-cycle $\sigma_r \in \hat{G}$ as in 4.1(5). Write $U = G_y$, $V = G_x$, $\hat{U} = \hat{G} \cap G_y$, and $\hat{V} = \hat{G} \cap G_x$. Without loss we assume $\sigma_r \in \hat{U}$. Then, for some prime power q, we get $A = \mathbb{F}_q^e$ and $\hat{G} = A \rtimes \hat{U}$ for some $\hat{U}$ with $\mathrm{GL}_e(q) \leq \hat{U} \leq \Gamma\mathrm{L}_e(q)$; see 6.3.

LEMMA 8.2: *If $\hat{G}'' = 1$, then* (a) *holds.*

Proof: Suppose $\hat{G}'' = 1$. We omit the trivial case $\hat{G} = Z_2$. Thus $n \geq 3$. Then $\hat{G}' \neq 1$, for otherwise $\hat{G} = Z_p$, contrary to the existence of $\sigma_r \in \hat{G}$. Therefore A is contained in the normal subgroup $\hat{G}'$. Now $\hat{G}'$ is abelian, hence $\hat{G}' = A$. Thus $\hat{U}$ is abelian. From this we get $\hat{U} = \langle \sigma_r \rangle$. From a Theorem of Zariski [14, 3.8], we see that (5)(i) and (iii) imply $\hat{G} = \mathrm{AGL}_1(p)$ with $p \in \{3, 5, 7\}$, or $\hat{G} = \mathrm{A}_4$.

First consider $\hat{G} = \mathrm{AGL}_1(p)$ with $p \in \{3, 5, 7\}$. As $\hat{G}$ is its own normalizer in S_p, we get $\hat{G} = G$. But then U and V are conjugate by 7.1.

Now let $\hat{G}$ be A_4. We also study $\hat{G} = \mathrm{S}_4$ in this paragraph. Now V is an intransitive subgroup of index 6 by our conditions. From this we see that the

action of $G \leq S_4$ on G/V is equivalent to the action of G on the 6 subsets of size 2 of $\{1,2,3,4\}$. Denote by ind_V the index with respect to the action on G/V. The conjugacy classes of S_4 are described by representatives. We get

Class	$(12) \in C_1$	$(12)(34) \in C_2$	$(123) \in C_3$	$(1234) \in C_4$
ind	1	2	2	3
ind_V	2	2	4	4

The conditions (5)(ii), (iii), (iv), and (v) yield $(\sigma_1,\sigma_2,\sigma_3) \in (C_1,C_4,C_3)$, $(\sigma_1,\sigma_2,\sigma_3) \in (C_2,C_3,C_3)$, or $(\sigma_1,\sigma_2,\sigma_3,\sigma_4) \in (C_2,C_1,C_1,C_3)$, up to interchanging the order of conjugacy classes (via $ab = ba^b$). Examples, which show that also (5)(i) can be fulfilled, are

$$\begin{aligned} &\sigma_1 = (12), && \sigma_2 = (1234), && \sigma_3 = (143) \\ &\sigma_1 = (12)(34), && \sigma_2 = (123), && \sigma_3 = (143) \\ &\sigma_1 = (12)(34), && \sigma_2 = (12), && \sigma_3 = (13), \quad \sigma_4 = (143). \end{aligned}$$

∎

LEMMA 8.3: *If $\hat{G}'' \neq 1$, then $q \in \{2,3\}$.*

Proof: We use the classification results of Guralnick and Thompson [14], together with (5)(i) and (iii). Suppose that $q > 3$. As the order of σ_r is $n-1 = q^e-1$, we first get $r = 3$ from [14, 4.1]. Then [14, 5.1] leaves $q = 5$, but also $q = 5$ is impossible, as we see from the cases listed in [14, 6.2]. ∎

The cases $p = 2$ and $p = 3$ have been investigated more closely by Neubauer. Using his results in [22, 1.5] and [23], we derive

LEMMA 8.4: *If $\hat{G}'' \neq 1$, then $n \in \{9,4,8,16,32\}$.*

Using 6.3, we see that we are left to investigate the following candidates for $\hat{G}$.

$$A\Gamma L_1(9),\ AGL_2(3),\ A\Gamma L_1(8),\ AGL_3(2),\ \mathbb{F}_{16} \rtimes \mathrm{Gal}(\mathbb{F}_{16}|\mathbb{F}_4),$$
$$A\Gamma L_1(16),\ AGL_2(4),\ A\Gamma L_2(4),\ AGL_4(2),\ A\Gamma L_1(32) \text{ and } AGL_5(2).$$

These groups are small enough to be checked with the help of the computer algebra system GAP. The strategy is as follows. First one checks which of these groups possess a generating system as required by (5)(i) and (iii). These are just the groups $A\Gamma L_1(9)$, $AGL_2(3)$, $A\Gamma L_1(8)$, $AGL_3(2)$, $A\Gamma L_2(4)$, $AGL_4(2)$, and $AGL_5(2)$.

Next 7.1(a) tells us what subgroups V of G to consider. Again with GAP we checked which of the generating systems computed above meet the genus 0

conditions with respect to the action on G/V, i.e. in what cases (5)(ii), (iv), and (v) hold as well. We get the cases (c), (d), and (e) listed in 8.1. The details and the GAP program can be found in [21].

G **non-affine.** By 7.1 we are left to look at $G = \mathrm{PSL}_2(5)$, $\mathrm{PSL}_2(7)$, and M_{11} of degree 12, together with the subgroups V of G specified there. As G is simple in these cases, we have $G = \hat{G}$. Again denote the index of the action of G on G/V by ind_V. We use the labeling of the non-trivial conjugacy classes of G given in the Atlas [4].

For $G = \mathrm{PSL}_2(5)$ we compute

Class	$1A$	$2A$	$3A$	$5A$	$5B*$
Order	1	2	3	5	5
ind	0	2	4	4	4
ind_V	0	4	6	8	8

The conditions in (5) yield (up to permutation of the conjugacy classes) $r = 3$ and $\sigma_1 \in 2A$, $\sigma_2 \in 3A$ and $\sigma_3 \in 5A \cup 5B*$. Again using the character table, one verifies that $(2A, 3A, 5A)$ and $(2A, 3A, 5B*)$ are strictly rigid systems of conjugacy classes of G, see [25].

Quite analogously we discuss $G = \mathrm{PSL}_2(7)$, and get

Class	$1A$	$2A$	$3A$	$4A$	$7A$	$7B**$
Order	1	2	3	4	7	7
ind	0	4	4	6	6	6
ind_V	0	6	8	10	12	12

Here we get $r = 3$, $\sigma_1 \in 2A$, $\sigma_2 \in 3A$ and $\sigma_3 \in 7A \cup 7B**$. Again we check that $(2A, 3A, 7A)$ and $(2A, 3A, 7B**)$ are strictly rigid systems for $\mathrm{PSL}_2(7)$.

Finally we have to consider M_{11}. We compute

Class	$1A$	$2A$	$3A$	$4A$	$5A$	$6A$	$8A$	$8B**$	$11A$	$11B**$
Order	1	2	3	4	5	6	8	8	11	11
ind	0	4	6	8	8	8	10	10	10	10
ind_V	0	8	12	14	16	16	18	18	20	20

The conditions (5) yield $r = 3$, $\sigma_1 \in 2A$, $\sigma_2 \in 4A$ and $\sigma_3 \in 11A \cup 11B**$. It is known that $(2A, 4A, 11A)$ and $(2A, 4A, 11B**)$ are strictly rigid systems of M_{11}, see [20, page 117f]. ∎

9. Some preliminary results

This section provides various results which will be needed to prove Theorem 1.3(a).

LEMMA 9.1: *Let $m \in \mathbb{N}$ and let $w(X) \in \mathbb{Q}[X]$ be a polynomial of degree $> m$ and $w(0) \neq 0$. Set $R(X) = w(X)/X^m$. Then $|R(\mathbb{Q}) \cap \mathbb{Z}| < \infty$.*

Proof: Set $r = \deg w > m$. Without loss assume $w(X) = a_r X^r + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$. Choose $q \in \mathbb{N}$, $p \in \mathbb{Z}$ with $\gcd(p, q) = 1$, such that $R(p/q) \in \mathbb{Z}$. Then

$$\frac{a_r p^r + a_{r-1} p^{r-1} q + \cdots + a_1 p q^{r-1} + a_0 q^r}{p^m q^{r-m}} \in \mathbb{Z}.$$

Now q divides a_r, as $r - m \geq 1$. Thus q is bounded. Furthermore, p divides $a_0 q^r \neq 0$, hence p is bounded as well, and the assertion follows. ∎

LEMMA 9.2: *Let $G = \mathbb{F}_p^m \rtimes \mathrm{GL}_m(p)$ be the affine general linear group with p a prime. Let σ be an $(p^m - 1)$-cycle which is conjugate to its inverse σ^{-1} in G. Then $G = S_3$ or S_4.*

Proof: Without loss assume $\sigma \in \mathrm{GL}_m(p)$. As σ fixes only one point, the elements σ and σ^{-1} are already conjugate inside $\mathrm{GL}_m(p)$. Thus we get an automorphism of the algebra generated by σ in $\mathrm{End}(\mathbb{F}_p^m)$ which inverts σ. Schur's lemma tells us that this algebra is isomorphic to the finite field $\mathbb{F}_{p^m}$, and σ is a generator of the multiplicative group. This automorphism is a power of the Frobenius automorphism, thus it maps $x \in \mathbb{F}_{p^m}$ to x^{p^i} for a suitable i in $\{0, 1, \ldots, m-1\}$. The relation $\sigma^{p^i} = \sigma^{-1} = \sigma^{p^m - 2}$ yields $p^i = p^m - 2$. The only solutions to $p^i(p^{m-i} - 1) = 2$ are $p = 2, i = 1, m = 2$ and $p = 3, i = 0, m = 1$. The assertion follows. ∎

As a consequence of [7, Theorem 2], we get

THEOREM 9.3 (Fried): *Let E be an extension of degree m of $\mathbb{Q}(t)$, such that $\mathbb{Q}$ is algebraically closed in E. Denote by Ω a Galois closure of $E|\mathbb{Q}(t)$, and set $G = \mathrm{Gal}(\Omega|\mathbb{Q}(t))$. Suppose that the extension $\mathbb{C}E|\mathbb{C}(t)$ has a totally ramified rational place, and that G is a 2-transitive group on the conjugates of E. If there is another permutation representation of G which admits the same permutation character, then these two representations are equivalent.*

The following is a special case of the so-called **branch cycle argument**. For a proof see [20, II, §4] or [11].

THEOREM 9.4: *Let E be an extension of degree n of $\mathbb{Q}(t)$, such that $\mathbb{Q}$ is algebraically closed in E. Denote by Ω a Galois closure of $E|\mathbb{Q}(t)$. Let $G = \mathrm{Gal}(\Omega|\mathbb{Q}(t))$ be the arithmetic monodromy group of $E|\mathbb{Q}(t)$. Let $\hat{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in Ω, and $\sigma_1, \sigma_2, \ldots, \sigma_r$ be a generating system of the geometric monodromy group $\hat{G} = \mathrm{Gal}(\Omega|\hat{\mathbb{Q}}(t))$ as in section 2. Let σ be one of the σ_i, and suppose that the branch point corresponding to σ lies in $\mathbb{Q} \cup \{\infty\}$. Then σ^w is conjugate inside G to σ for every integer w prime to the order of σ.*

10. Proofs of the Theorems 1.2 and 1.3(a) and (b)

In the following we study a counter-example, where $h(Y) \in K[Y]$ is a polynomial of degree n, and i is as in the Theorems to be proved. Set $f(X,Y) := h(Y) - XY^i$, and choose the rational functions R_j according to Corollary 3.2. As we consider a counter-example, there is a rational function R among the R_j, such that infinitely many elements of the set $R(K) \cap \mathcal{O}_K$ are not of the form $h(\kappa)/\kappa^i$ with $\kappa \in K$. Note that in the situation of Theorem 1.3(a), we know that $\mathcal{V}_h$ is finite by Lemma 9.1.

We quickly repeat the Galois theoretic setup from section 4. Set $H(Y) = h(Y)/Y^i$, and let t be a transcendental over $\mathbb{C}$. In an algebraic closure $\overline{\mathbb{C}(t)}$ of $\mathbb{C}(t)$, pick elements x and y such that

$$H(y) = h(y)/y^i = R(x) = t.$$

Denote by Ω the Galois closure of $K(x,y)|K(t)$ inside $\overline{\mathbb{C}(t)}$. Set $G = \mathrm{Gal}(\Omega|K(t))$. The fix groups of y and x are labelled G_y and G_x, respectively. Further denote by $\hat{K}$ the algebraic closure of K in Ω. Set $\hat{G} = \mathrm{Gal}(\Omega|\hat{K}(t)) \cong \mathrm{Gal}(\mathbb{C}\Omega|\mathbb{C}(t))$. The properties of these groups are listed in Proposition 4.1.

LEMMA 10.1: *The groups G_x and G_y are not conjugate in G. Furthermore, $n \geq 4$.*

Proof: Suppose $G_x^g = G_y$ for some $g \in G$. Then x^g is fixed by G_y, hence $x^g \in K(y)$. From $\deg H = [G\colon G_y] = [G\colon G_x] = \deg R$ we get $x^g = \frac{ay+b}{cy+d}$ with $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(K)$. Then $H(y) = t = t^g = R(x)^g = R(x^g) = R(\frac{ay+b}{cy+d})$, in particular the value sets $R(K)$ and $H(K)$ differ only by finitely many elements. But this contradicts the choice of R. The assertion $n \geq 4$ then follows directly from 4.1(1) and (4). ∎

This already proves Theorem 1.2, as G_y and G_x are conjugate by Proposition 4.2. Also, we immediately get Theorem 1.3(b), because for the degrees n excluded from the consideration, the subgroups G_y and G_x are conjugate by Proposition 8.1.

Thus, from now on we have to discuss the case $i = 1$ with $K = \mathbb{Q}$. We will not use any results which depend on the classification of finite simple groups. In particular, we do not use Theorem 6.2.

As $T_y(G)$ contains the $(n-1)$-cycle σ_r, we know from Theorem 6.1 that $T_y(G)$ is affine, $\mathrm{PSL}_2(p)$, or 3-transitive. In these three cases, quite different arguments apply, and $n = 4$ needs a special treatment.

$n \neq 4$ and $T_y(G)$ affine or $\mathrm{PSL}_2(p)$. We consider the branched covering $\mathbb{P}^1 \to \mathbb{P}^1$ of the Riemann spheres, induced by the rational function $R \in \mathbb{Q}(X)$. We call this covering also R. Let $\sigma_1, \sigma_2, \ldots, \sigma_r$ be generators of $\hat{G}$, with σ_r belonging to the branch point ∞, according to section 2 and Proposition 4.1. Then $T_y(\sigma_r)$ is an $(n-1)$-cycle. As the branch point corresponding to σ_r is ∞, we can apply Theorem 9.4 to conclude that σ_r^w is conjugate in G to σ_r for every integer w prime to the order of σ_r.

In the affine case, this yields $n \leq 4$ by Lemma 9.2, and Lemma 10.1 shows $n = 4$, a case to be discussed later.

The other possibilities are $T_y(G) = T_y(\hat{G}) = \mathrm{PSL}_2(5)$ or $\mathrm{PSL}_2(7)$, see the proof of Proposition 7.1(b), together with Theorem 6.1. In the first case, one checks that σ_r and σ_r^2 are not conjugate in $\mathrm{PSL}_2(5)$, and in the second case σ_r and σ_r^3 are not conjugate in $\mathrm{PSL}_2(7)$.

$n \neq 4$ and $T_y(G)$ 3-transitive. We are going to apply Proposition 5.2(ii), together with Theorem 9.3. Again choose generators σ_i of $\hat{G}$ as in the previous paragraph. Without loss assume $\sigma_r \in \hat{G}_y$.

Choose the subgroups U and V of G_y as in Proposition 5.2(ii). Let E be the fixed field in Ω of U. Combining 5.2(ii) with Theorem 9.3, we see that we are done once we know the following: $\mathbb{Q}$ is algebraically closed in E, and $\mathbb{C}E|\mathbb{C}(y)$ has a totally ramified rational place.

As to the first statement. Suppose that the algebraic closure $\hat{\mathbb{Q}}$ of $\mathbb{Q}$ in E is bigger than $\mathbb{Q}$. Then $E \cap \hat{\mathbb{Q}}(y) > \mathbb{Q}(y)$. In terms of Galois groups, this means

$$U \cdot (\hat{G} \cap G_y) < G_y.$$

As G_y acts 2-transitively on the cosets of U in G_y, the subgroup U is maximal

in G_y. Therefore $\hat{G} \cap G_y \leq U$. The action of G_y on the conjugates of y different from y is faithful and transitive, hence U does not contain a non-trivial normal subgroup of G_y. We get $\hat{G} \cap G_y = 1$. The transitivity of the groups $T_y(\hat{G})$ and $T_x(\hat{G})$ (see 4.1(5)) implies $G = \hat{G}G_y = \hat{G}G_x$. Combining this with 5.2(ii), we arrive at the contradiction

$$n = [G\colon G_y] = |\hat{G}| \geq \frac{|\hat{G}|}{|\hat{G} \cap G_x|} = [G\colon G_x] = 2(n-1).$$

The second assertion follows from the fact that σ_r is a generator of an inertia group of the extension $\mathbb{C}\Omega|\mathbb{C}(y)$, permuting transitively the $(n-1)$ conjugates of $\mathbb{C}E$ over $\mathbb{C}(y)$. Note that the place of $\mathbb{C}(y)$ corresponding to σ_r is rational, as $H^{-1}(\infty) = \{0, \infty\}$.

$n = 4$. The interesting feature of this case is that, in contrast to the former cases, the consequences from Corollary 3.2(a), (b), and (c) do not suffice, as we will see later in the explicit construction yielding a proof of Theorem 1.3(d). We really have to use part (d) now.

Now $T_y(G) \leq \mathrm{S}_4$, and $T_x(G)$ is the action of degree 6, given by permuting the 2-sets of $\{1,2,3,4\}$ (see Proposition 8.1). In the proof of Proposition 8.1, we computed the possible systems $\sigma_1, \sigma_2, \ldots, \sigma_r$ fulfilling 4.1(5). σ_r has order 3 and corresponds to the branch point ∞. Then $T_x(\sigma_r)$ is a product of two 3-cycles. Let λ and μ be the the 2 triple points above ∞ with respect to R. We may assume that neither λ nor μ equals ∞. The absolute Galois group of $\mathbb{Q}$ fixes $\lambda + \mu$, thus $\lambda + \mu = 0$ without loss of generality. Then

$$R(X) = \frac{p(X)}{(X^2 - \lambda^2)^3},$$

with a polynomial $p \in \mathbb{Q}[X]$ of degree at most 6, and which has no roots at λ and $-\lambda$. Multiplying R by a non-zero rational doesn't affect the arithmetic and geometric monodromy group. So we assume for a moment that p is monic. Then, Puiseux' theorem allows us to express the 6 solutions of $R(X) = t$ in terms of power series:

$$x_{i,\epsilon} = \epsilon\lambda + a_{1,\epsilon}\zeta^i t^{-1/3} + a_{2,\epsilon}\zeta^{2i} t^{-2/3} + \cdots \in \overline{\mathbb{Q}}((t^{-1/3})),$$

with ζ a primitive cubic root of 1, $\epsilon \in \{-1, 1\}$, $i \in \{1,2,3\}$, and $a_{k,\epsilon} \in \mathbb{Q}$. This way we get an embedding of $\overline{\mathbb{Q}}\Omega$ in the field of Laurent series $\mathcal{L} = \overline{\mathbb{Q}}((t^{-1/3}))$. Consider the automorphism α of $\mathcal{L}$, which is trivial on $\overline{\mathbb{Q}}$ and replaces $t^{-1/3}$ by

$\zeta t^{-1/3}$ Then α fixes t and permutes the $x_{i,\epsilon}$. Thus α restricts to an element of the geometric monodromy group of R. The important observation is, that α permutes the elements in $\{x_{1,1}, x_{2,1}, x_{3,1}\}$ and $\{x_{1,-1}, x_{2,-1}, x_{3,-1}\}$ cyclically. Now suppose that λ is not rational. Then there is an automorphism of $\overline{\mathbb{Q}}$, which maps λ to $-\lambda$ ($\lambda^2 \in \mathbb{Q}$ by construction). Extend this automorphism to an automorphism β of $\mathcal{L}$, which fixes $t^{1/3}$. Then β restricts to an automorphism of the arithmetic monodromy group of R, which interchanges just the two sets from above.

However, S_4 in the action on the 2-sets of $\{1,2,3,4\}$ does not contain such a pair of elements. By abuse of notation, assume that $\alpha = (123) \in S_4$. Then α permutes the sets $\{1,4\}$, $\{2,4\}$, and $\{3,4\}$ cyclically. Thus there is a $\beta \in S_4$, which just interchanges these three sets with the sets $\{1,2\}$, $\{2,3\}$, and $\{1,3\}$. However, this is impossible. Observe that β has to move 4, and also has to move at least two of the numbers $1,2,3$. Further, it must not transpose any of the numbers $1,2,3$. This of course is nonsense.

This contradiction shows that λ is rational. Thus, replacing X by $(\lambda X+1)/X$ in R produces

$$\tilde{R}(X) = \frac{\tilde{p}(X)}{X^3},$$

with $\tilde{p} \in \mathbb{Q}[X]$. The ramification above ∞ tells us that $\tilde{p}$ has degree 6. Furthermore, the substitution didn't change the value set of the rational function on $\mathbb{Q} \cup \{\infty\}$. Thus $|\tilde{R}(\mathbb{Q}) \cap \mathbb{Z}| = \infty$, contrary to Lemma 9.1.

11. Proof of Theorem 1.3(c) and (d)

Before we start we need to investigate properties of value sets of rational functions on groups of units. Let K be a number field, $\mathcal{O}_K$ the ring of integers, and U be the group of units. Suppose that U is infinite. If R and H are non-constant rational functions over K, such that $R(U)$ is contained in $H(K)$ up to finitely many exceptions, then we conjecture that $R(Z) = H(c(Z))$ for some $c \in K(Z)$. We prove this under a certain additional hypothesis.

If $P(X,Y) \in \overline{\mathbb{Q}}(X)[Y]$ is irreducible over $\overline{\mathbb{Q}}$, then denote by $e(P)$ the smallest positive integer e such that $P(X,Y) = 0$ has a solution y in $\overline{\mathbb{Q}}((X^{1/e}))$. The existence of such an e follows from Puiseux' theorem.

PROPOSITION 11.1: *Let K be a number field with an infinite group U of units. Let $R, H \in K(Z)$ be non-constant rational functions, such that the value set*

$R(U)$ is contained in $H(K)$ up to finitely many exceptions. Write $R = R_1/R_2$, $H = H_1/H_2$ with $R_i, H_i \in K[Z]$ as reduced fractions. Let

$$R_1(X)H_2(Y) - R_2(X)H_1(Y) = \Pi\Phi_i(X,Y)$$

be a factorization in irreducible factors $\Phi_i \in K[X,Y]$. Set $e_i = e(\Phi_i)$ as defined above. If all the irreducible factors over K of $\Phi_i(X^{e_i},Y)$ are absolutely irreducible, then there is a rational function $c \in K(Z)$ such that $R(Z) = H(c(Z))$.

In the proof, we use the following two results of P. Dèbes.

PROPOSITION 11.2 ([5, Prop. 3]): *Let K be a number field, and $\Phi \in K[X,Y]$ be irreducible. For $e \in \mathbb{N}$, let $\Phi(X^e,Y) = \phi_1 \cdots \phi_r$ be a decomposition over $\overline{\mathbb{Q}}$ into irreducible factors ϕ_i. Denote by L the field generated by K and the coefficients of the polynomials ϕ_i. Choose $u \in L \setminus \{0\}$ with $T^e - u$ irreducible. Then $\Phi(uX^e,Y)$ is irreducible in $K[X,Y]$.*

THEOREM 11.3 ([6, Cor. 1.6(b)]): *Let K be a number field, and $P \in K[X,Y]$ be irreducible over K. Further, suppose $e(P) = 1$. Choose $u \in K \setminus \{0\}$ such that u is not a root of unity. Then $P(u^m,Y)$ is irreducible over K for all but finitely many integers m.*

Proof of 11.1: Let E be the group of roots of unity in K. Then $U = E \times A$ with a free abelian group A of finite rank ≥ 1 (see [19, V, §1]). Let $u \in A$ be a free generator of A. Then μu is not a power with exponent > 1 of an element in K for all $\mu \in E$. We may additionally assume that u is not of the form $-4w^4$ with $w \in K$. For if μu has this form for $\mu \in E$, then $\mu = \nu^4$ has a solution $\nu \in E$. But this cannot happen for each μ, because the map $X \mapsto X^4$ is not bijective on the finite set E by the presence of $-1 \in E$.

From Capelli's Theorem [17, VII, 9.1] we get that $X^m - u$ is irreducible over K for all $m \in \mathbb{N}$.

Using the notation from 11.1, we now get from 11.2: $\Phi_i(uX^{e_i},Y)$ is irreducible in $K[X,Y]$ for all i. Clearly $e(\Phi_i(uX^{e_i},Y)) = 1$. Applying 11.3 — with $P(X,Y) = \Phi_i(uX^{e_i},Y)$ — we get: $\Phi_i(u^{me_i+1},Y)$ is irreducible in $K[Y]$ for almost all $m \in \mathbb{Z}$. Set $e = \operatorname{lcm}(e_1,e_2,\ldots)$. Then $\Phi_i(u^{me+1},Y)$ is irreducible for every index i and all but finitely many $m \in \mathbb{Z}$.

Now recall that $R(U)$ is contained in $H(K)$ up to finitely many exceptions. Thus

$$R_1(u^{em+1})H_2(Y) - R_2(u^{em+1})H_1(Y) = \Pi\Phi_i(u^{em+1},Y)$$

has for almost all $m \in \mathbb{Z}$ a root $y_0 \in K$. Then one of the factors on the right hand side — let j be its index — has a root in K for infinitely many integers m, though it is irreducible by the considerations from above. Therefore Φ_j has degree 1 with respect to Y, hence $\Phi_j(X,Y) = c_1(X) - c_2(X)Y$ with $c_i \in K[X]$. Set $Y = \frac{c_1(X)}{c_2(X)} = c(X)$, then $R(X) - H(c(X)) = 0$. ∎

Now we are prepared to prove Theorem 1.3(c). Let $G = \hat{G}$ be one of the groups listed in Proposition 8.1, with subgroups G_x and G_y as given there. Then we showed the existence of a generating system $\sigma_1, \sigma_2, \ldots, \sigma_r$ of G, such that the conditions (1) to (5) in Proposition 4.1 are fulfilled. Note that the degrees of T_y are 4, 16, 9, 9, 6, 8 and 12, respectively. As a consequence of Riemann's existence theorem, there exists a Galois extension Π of $\overline{\mathbb{Q}}(t)$ with $G = \mathrm{Gal}(\Pi|\overline{\mathbb{Q}}(t))$, such that $(\sigma_1, \ldots, \sigma_r)$ is just a branch cycle description of this extension, as defined in section 2; see e.g. [20, §4].

From the Riemann Hurwitz genus formula, together with 4.1(5)(iii) and (v), we get that the fixed fields in Π of G_y and G_x have genus 0. As the base field is algebraically closed, these fields are rational fields $\overline{\mathbb{Q}}(y)$ and $\overline{\mathbb{Q}}(x)$, with $y, x \in \Pi$. Let σ_r correspond to the place at infinity. Choose $H, R \in \overline{\mathbb{Q}}(Z)$ with $H(y) = R(x) = t$. Then 4.1(5)(ii) says that $H^{-1}(\infty)$ consists of an $(n-1)$-fold point and a simple point. By linear fractional change of the variable Y, we may assume that the simple point is 0, and the multiple point is ∞. This means $H(Y) = h(Y)/Y$ with a polynomial h. Similarly, use 4.1(5)(iv) to show that (without loss of generality) $R(X) = w(X)/X^l$ for some integer l and a polynomial w.

Now define the number field K as follows. Build the field which is generated by the coefficients of H and R. Then enlarge it by a finite extension, such that the factors $\Phi_i(X^{e_i}, Y)$ as defined in 11.1 split in absolutely irreducible factors over this field. Furthermore, assume that this field has an infinite group of units (i.e. is not the field of rationals or an imaginary quadratic field). Call this tentative field F. Let Ω be the Galois closure of $F(x,y)|F(t)$ in Π. Now let K be the algebraic closure of F in Ω.

Thus G restricts to the Galois group of $\Omega|K(t)$. Let $\mathcal{O}_K$ be the ring of integers, and U the infinite group of units in $\mathcal{O}_K$. By multiplying the functions H and R with a suitable integer, we may assume

$$H(y) = \frac{h(y)}{y} \quad \text{and} \quad R(x) = \frac{w(x)}{x^l} \quad \text{with } h, w \in \mathcal{O}_K[Z], \quad l \in \mathbb{N}.$$

Condition 4.1(1) says that G_x permutes the conjugates of x intransitively. Thus $h(Y) - R(X)Y \in K(X)[Y]$ is reducible. In particular, $h(Y) - R(u)Y$ is reducible in $K[Y]$ for each unit $u \in U$. Note that $R(u) = w(u)(1/u)^l \in \mathcal{O}_K$. So we are done once we know that there are infinitely many $u \in U$, such that $R(u)$ has not the form $H(\kappa) = h(\kappa)/\kappa$ for some $\kappa \in K$. If this would not hold, then $R(X) = H(c(X))$ with a rational function c by Proposition 11.1. However, this cannot be the case for a degree reason, because $\deg H < \deg R \leq 2(\deg H - 1)$ by 5.2(i) and 2.1.

Finally we prove Theorem 1.3(d). The argument is similarly as above, except for the fact that we explicitly write down the rational functions h and R, and that we replace the use of 11.1 by a direct argument. Set $h(Y) = (Y-1)^4$ and $R(X) = (X+1)^4(X-1)^2/X^3$. One verifies

$$h(Y) - R(X)Y = \frac{\Phi_1(X,Y)\Phi_2(X,Y)}{X^3}$$

with

$$\Phi_1(X,Y) = X^3 + Y^2X + YX^2 - 2YX - Y$$

and

$$\Phi_2(X,Y) = 1 + Y^2X^2 - 2YX^2 + YX - YX^3.$$

As $K < \mathbb{R}$ is a real-quadratic number field, $\mathcal{O}_K$ has an infinite group U of units ([19, V, §1]). We have to show $|H(K) \setminus R(U)| = \infty$. For this suppose the contrary, that is $h(Y) - R(u)Y$ has a root in K for almost all $u \in U$. Thus for all sufficiently big values u the polynomial $\Phi_1(u,Y)$ or $\Phi_2(u,Y)$ has a root in K. The discriminant $\operatorname{dis}_Y \Phi_i(u,Y)$ has to be a square in K for such a u and Φ_i. As $\operatorname{dis}_Y \Phi_1(u,Y) = -3u^4 - 4u^3 + 2u^2 + 4u + 1$ is negative for all big u (and hence not a square in K), we get that $\Phi_2(u,Y)$ has a root in K for all big u, thus $\operatorname{dis}_Y \Phi_2(u,Y) = u^4 + 4u^3 + 2u^2 - 4u - 3$ is a square in K for all big u. If we replace u by its algebraic conjugate, then this discriminant also has to be a square. Thus $u^4 + 4u^3 + 2u^2 - 4u - 3$ is also a square for all small u. We get a contradiction, because this term becomes negative for small u.

References

[1] M. Aschbacher, *$\mathcal{F}$-sets and permutation groups*, Journal of Algebra **30** (1974), 400–416.

[2] P. J. Cameron, *Finite permutation groups and finite simple groups*, The Bulletin of the London Mathematical Society **13** (1981), 1–22.

[3] C. Chevalley, *Algebraic Functions of One Variable*, Mathematical Surveys VI, American Mathematical Society, Providence, 1951.

[4] J. Conway, R. Curtis, S. Norton, R. Parker and R. Wilson, *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*, Clarendon Press, Oxford, New York, 1985.

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

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

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

[8] M. Fried, *On Hilbert's Irreducibility Theorem*, Journal of Number Theory **6** (1974), 211–231.

[9] M. Fried, *Exposition on an arithmetic-group theoretic connection via Riemann's existence theorem*, The Santa Cruz conference on finite groups, Proc. Symp. Pure Math., Vol. 37, American Mathematical Society, Providence, R.I., 1980, pp. 571–602

[10] M. Fried, *Rigidity and applications of the classification of simple groups to monodromy, Part II — Applications of connectivity; Davenport and Hilbert–Siegel Problems*, preprint.

[11] M. Fried, *Review of Serre's 'Topics in Galois Theory'*, Bulletin of the American Mathematical Society **30** (1994), 124–135.

[12] M. Fried and M. Jarden, *Field Arithmetic*, Springer, Berlin–Heidelberg, 1986.

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

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

[15] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1983.

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

[17] S. Lang, *Algebra*, Addison-Wesley, Reading, 1984.

[18] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, New York, 1983.

[19] S. Lang, *Algebraic Number Theory*, Springer, New York, 1986.

[20] B. H. Matzat, *Konstruktive Galoistheorie*, Lecture Notes in Mathematics **1284**, Springer, Berlin, 1987.

[21] P. Müller, *Monodromiegruppen rationaler Funktionen und Polynome mit variablen Koeffizienten*, Thesis, 1994.

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

[23] M. Neubauer, *On primitive monodromy groups of genus zero and one, II*, preprint.

[24] M. E. O'Nan, *Normal structure of the one-point stabilizer of a doubly-transitive permutation group. II*, Transactions of the American Mathematical Society **214** (1975), 43–74.

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

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

[27] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York and London, 1964.