Contemporary Mathematics
Volume **00**, 0000

Primitive Monodromy Groups of Polynomials

PETER MÜLLER

Abstract. For a polynomial $f \in \mathbb{C}[X]$, let G be the Galois group of the Galois closure of the field extension $\mathbb{C}(X)|\mathbb{C}(f(X))$. We classify the groups G in the indecomposable case. For polynomials with rational coefficients there are, besides four infinite series, only three more "sporadic" examples. In the Appendix we reprove the classical Theorems of Ritt about decompositions of polynomials using the group-theoretic setup.

1. Introduction

Let f be a polynomial of degree n with complex coefficients. In a fixed algebraic closure of the field of rational functions $\mathbb{C}(t)$ consider the field Ω which is generated over $\mathbb{C}$ by the n different elements x_i fulfilling $f(x_i) = t$. Then the Galois group $G = \mathrm{Gal}(\Omega|\mathbb{C}(t))$ permutes transitively the elements x_i. This group G is called the monodromy group of f. It is natural to ask what groups G can occur this way. A polynomial is called *indecomposable* if it cannot be written as a composition of two non–linear polynomials. In section 2 we classify the possible monodromy groups for indecomposable polynomials, there are four infinite series and twelve more cases which do not belong to these series. Section 3 is about the question of what groups occur as monodromy groups of polynomials with rational coefficients. The result is

Theorem. *Let $f \in \mathbb{Q}[X]$ be indecomposable and let G be its monodromy group. Then G is either alternating, symmetric, cyclic, or dihedral or G is $PGL_2(5)$, $P\Gamma L_2(8)$, or $P\Gamma L_2(9)$. In the latter three cases f is, up to composition with linear polynomials, uniquely given by $X^4(X^2+6X+25)$, $9X^9+108X^7+72X^6+486X^5+504X^4+1228X^3+888X^2+1369X$ or $(X^2-405)^4(X^2+50X+945)$.*

Some remarks about the appearance of monodromy groups are in order: Especially M. Fried (see [**7**], [**8**], [**9**], and his papers cited in [**11**]) exhibited the

1991 *Mathematics Subject Classification.* Primary 11C08, 20B15, 20B20; Secondary 12E05.

Financial support from the DAAD is greatfully acknowledged.

This paper is in final form, and no version of it will be submitted for publication elsewhere.

importance of these groups in discussing several arithmetical questions about polynomials. That is many questions depend merely on the monodromy group rather than on the full information given by a polynomial. One of these problems is a question of Davenport, which asks to classify the pairs of polynomials with integer coefficients such that the value sets on $\mathbb{Z}$ are the same modulo all but finitely many primes. See [**11, 19.6**], [**9**], and [**20**].

We merely classify the monodromy groups in the indecomposable case. By a Theorem of Ritt (see [**21**] or [**3**]) the study of arbitrary polynomials can be reduced to these polynomials to some extent. For instance (over fields of characteristic 0) any two decompositions of a polynomial into indecomposable polynomials have the same number of factors, and the degrees are the same up to a permutation. Ritt even gives an algorithm how to pass from one composition to the other one by interchanging and "twisting" consecutive factors. In the Appendix, we give a concise account of this, employing the group-theoretic setup.

I wish to thank H. Völklein for drawing my attention to this question. I thank B. H. Matzat for informing me about [**17**] where he already computed the polynomials for the groups $\mathrm{P\Gamma L}_2(8)$ and $\mathrm{P\Gamma L}_2(9)$. He also noted that I erroneously excluded $\mathrm{P\Gamma L}_2(8)$ in an earlier version of this paper.

2. Primitive Monodromy Groups

2.1 Notation and Definitions. We retain the notation from the Introduction. For technical reasons we need a further description of the monodromy group of $f \in \mathbb{C}[X]$ ($\deg f = n$):

Consider the branched n-fold covering $f: \mathbb{P}^1 \to \mathbb{P}^1$. Let $S = \{p_1, p_2, \dots, p_r\}$ be the set of branch points, where p_r is the point at infinity. Fix a point a in $\mathbb{P}^1 \setminus S$. Then $\pi_1 = \pi_1(\mathbb{P}^1 \setminus S, a)$ acts on $f^{-1}(a)$ by lifting of paths. The homomorphic image of π_1 in $\mathrm{S}_n \cong \mathrm{Sym}(f^{-1}(a))$ will also be denoted by G, as this group can be identified with the monodromy group defined in the Introduction, with G acting in the same way on the elements x_i as on the points of the fiber $f^{-1}(a)$. This identification relies on the isomorphism between the group of covering transformations of a Galois cover of compact connected Riemann surfaces and the Galois group of the corresponding extension of fields of meromorphic functions on these surfaces.

In this section we use the geometric description of G from above, i.e. we view G as a subgroup of S_n via identification of $\{1, 2, \dots, n\}$ with $f^{-1}(a)$.

Pick r generators λ_i of $\pi_1(\mathbb{P}^1 \setminus S, a)$ such that λ_i winds only around p_i and $\lambda_1\lambda_2 \cdots \lambda_r = 1$ (this is a so–called "standard homotopy basis"). These r generators of $\pi_1(\mathbb{P}^1 \setminus S, a)$ then yield generators $\sigma_1, \sigma_2, \dots, \sigma_r$ of G with

$$\sigma_1\sigma_2 \cdots \sigma_r = 1 \ .$$

As $p_r = \infty$ ramifies completely, σ_r is an n-cycle.

This tuple $(\sigma_1, \dots, \sigma_r)$ is called the branch cycle description of the cover $f : \mathbb{P}^1 \to \mathbb{P}^1$.

For $\sigma \in \mathrm{S}_n$ denote by $\operatorname{ind}\sigma$ the quantity '$n -$ the number of orbits of $\langle\sigma\rangle$'. The main constraint is imposed by the Riemann Hurwitz genus formula

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

For an elementary argument yielding this latter relation confer [**7, Lemma 5**]. Conversely, a finite permutation group having a set of generators fulfilling the above restrictions is the monodromy group of a suitable polynomial by Riemann's existence Theorem.

So we are reduced to a completely group–theoretic question. The purpose of this section is to give a complete classification in the indecomposable case. The corresponding question for rational functions instead of polynomials is much tougher and still open, see [**15**] and [**1**].

2.2 Notations and Main Result. Let G be a permutation group acting on n elements. We consider the following condition on G, which we later refer to as (*).

Condition (*). G is generated by $\sigma_1, \sigma_2, \dots, \sigma_s$ ($\sigma_i \neq 1$) such that $\sigma_1\sigma_2\cdots\sigma_s$ is an n-cycle and $\sum_{i=1}^{s} \operatorname{ind}\sigma_i = n-1$.

It is obvious that the situation in (*) is equivalent to the configuration of 2.1. Suppose (*) holds. Using $ab = ba^b$ we see that we may assume $|\sigma_1| \leq |\sigma_2| \leq \cdots \leq |\sigma_s|$, where $|\sigma|$ denotes the order of σ. Following Feit in [**4**] we say that G is of type $(|\sigma_1|, |\sigma_2|, \cdots, |\sigma_s| : n)$.

Denote by C_p and D_p the cyclic and dihedral groups of degree p, respectively. Let $\mathrm{PGL}_k(q)$ be the projective linear group over the field with q elements, acting on the projective space of dimension $k-1$. This group, together with the component–wise action of $\mathrm{Aut}(\mathbb{F}_q)$ on the projective space, generates the semilinear group $\mathrm{P\Gamma L}_k(q)$. The Mathieu groups of degree n are labelled by M_n. In this section we prove

Theorem. *Let G be the monodromy group of a polynomial $f \in \mathbb{C}[X]$. Then G is one of the following groups. Conversely, each of these groups occurs.*

(i) C_p *of type* $(p : p)$*, p a prime.*
D_p *of type* $(2, 2 : p)$*, p an odd prime.*
(ii) $PSL_2(11)$ *of type* $(2, 3 : 11)$
$PGL_3(2)$ *of types* $(2, 3 : 7)$*,* $(2, 4 : 7)$*, and* $(2, 2, 2 : 7)$
$PGL_3(3)$ *of types* $(2, 3 : 13)$*,* $(2, 4 : 13)$*,* $(2, 6, 13)$*, and* $(2, 2, 2 : 13)$
$PGL_4(2)$ *of types* $(2, 4 : 15)$*,* $(2, 6 : 15)$*, and* $(2, 2, 2 : 15)$
$P\Gamma L_3(4)$ *of type* $(2, 4 : 21)$
$PGL_5(2)$ *of type* $(2, 4 : 31)$
(iii) A_n *(n odd) and* S_n *of many, not reasonably classifiable types.*

M_{11} *of type* $(2,4:11)$
M_{23} *of type* $(2,4:23)$
$PGL_2(5)$ *of type* $(2,4:6)$
$PGL_2(7)$ *of type* $(2,3:8)$
$P\Gamma L_2(8)$ *of types* $(2,3:9)$ *and* $(3,3:9)$
$P\Gamma L_2(9)$ *of type* $(2,4:10)$

Remark. In [**19, 2.6.10**] we get, as a side product to the Hilbert–Siegel problem, a classification of the monodromy groups of the rational functions $f(X)/X$ where f is an arbitrary polynomial $f \in \mathbb{C}[X]$ with $f(0) \neq 0$. The list is as follows: $\mathrm{AGL}_1(p)$ with $p \in \{2,3,5,7\}$, $\mathrm{A\Gamma L}_1(8)$, $\mathrm{AGL}_3(2)$, $\mathrm{A\Gamma L}_2(4)$, $\mathrm{AGL}_4(2)$, $\mathrm{AGL}_5(2)$, $\mathrm{A\Gamma L}_1(9)$, $\mathrm{AGL}_2(3)$, A_n (n even), S_n, $\mathrm{PSL}_2(5)$, $\mathrm{PGL}_2(5)$, $\mathrm{PSL}_2(7)$, $\mathrm{PGL}_2(7)$, $\mathrm{PSL}_2(13)$, M_{11} with $n = 12$, M_{12}, M_{24}.

There are also results about monodromy groups of indecomposable polynomials with coefficients in a finite field or in an algebraically closed field of positive characteristic. In [**14**] is a classification of the primitive groups which meet a necessary condition for being the monodromy group of a polynomial. The main constraint comes from the ramification at infinity. The genus condition however is hardly to use.

2.3 About the Proof. Let $f \in \mathbb{C}[X]$ be a polynomial and G its monodromy group. As a consequence of Lüroth's Theorem, f is indecomposable if and only if G is a primitive group (i.e. G does not act on a non–trivial partition of the underlying set), see [**12, 3.4**].

Now let f be indecomposable and $\sigma_1, \dots, \sigma_s$ a generating system of G fulfilling (*). Set $Z = \langle \sigma_1\sigma_2 \cdots \sigma_s \rangle$, then Z is a transitive cyclic subgroup of G. Together with the primitivity of G, we get by classical results of Schur and Burnside (see [**22, 11.7 and 25.2**]) that $G \leq \mathrm{AGL}_1(p)$ (p a prime) or G is doubly transitive.

Let A be a minimal normal subgroup of G. If A is elementary abelian, then $G \leq \mathrm{AGL}_1(p)$ or $G \leq \mathrm{S}_4$, see the proof of [**16, Satz 5**]. The non–solvable doubly transitive groups with a cyclic transitive subgroup are known by the classification of the finite simple groups and listed in [**5, 4.1**]. Thus we have to investigate the following groups G.

> $C_p \leq G \leq \mathrm{AGL}_1(p)$, A_n (n odd), S_n, M_{11}, M_{23}, $\mathrm{PSL}_2(11)$ of degree 11, and (not all) groups between $\mathrm{PSL}_m(q)$ and $\mathrm{P\Gamma L}_m(q)$ (with $m \geq 2$, q a prime power) in its action on the projective space.

The cases $G = \mathrm{PSL}_2(11)$ with $n = 11$ and the semi–projective linear groups with $m \geq 3$ have been investigated by Feit in [**4**]. (These are just the cases where G admits two inequivalent doubly transitive representations with Z acting transitively in both of them.) However, his proof needs to be modified, as [**4, 3.4**] is wrong. In the following we supply an alternative treatment in the case when [**4, 3.4**] does not work. I thank Feit for a discussion about this.

We will discuss the different classes of groups separately. The case $C_p \leq G \leq \mathrm{AGL}_1(p)$ is quite easy and left to the reader.

2.4 Counting Orbits. Some more notation: For $\sigma \in G$ denote by $o(\sigma)$ the number of cycles of σ (thus $n = o(\sigma) + \operatorname{ind}\sigma$). Let $f(\sigma)$ be the number of elements fixed by σ. For later use we derive an elementary relation between $o(\sigma)$ and the number of fixed points of powers of σ: For this denote by a_i the number of i-cycles of σ. Clearly

$$f(\sigma^r) = \sum_{i|r} i \cdot a_i$$

for every positive integer r. Möbius inversion yields

$$r \cdot a_r = \sum_{k|r} \mu(\frac{r}{k}) f(\sigma^k) \quad .$$

Using $\sum_{t|m} \frac{\mu(t)}{t} = \frac{\varphi(m)}{m}$ and $o(\sigma) = a_1 + a_2 + \dots$ we get the basic relation

$$o(\sigma) = \frac{1}{|\sigma|} \sum_{k|\,|\sigma|} f(\sigma^k)\varphi(\frac{|\sigma|}{k}) \quad . \tag{1}$$

2.5 The Mathieu Groups. For the two candidates M_{11} and M_{23} we use the Atlas of the finite simple groups [**2**] and its notation. Besides other things the character tables in this source allow us to compute the ind–function. Let us start with $G = M_{11}$: First we get $\operatorname{ind}\sigma_i \geq 4$, hence $s = 2$ by (*). We see that $\sigma_1 \in 2A$ and $\sigma_2 \in \{3A, 4A\}$. Let χ_1, χ_2,…,χ_h be the irreducible characters of G and C_1, C_2,…,C_h be the conjugacy classes of G. For an $x \in C_k$ denote by $N(i,j;k)$ the number of solutions of $x = uv$ with $u \in C_i$ and $v \in C_j$. It is well–known (see e.g. [**13, 4.2.12**]) that

$$N(i,j;k) = \frac{|C_i| \cdot |C_j|}{|G|} \sum_{m=1}^{h} \frac{\chi_m(C_i)\chi_m(C_j)\overline{\chi_m(C_k)}}{\chi_m(1)} \tag{2}$$

We want to exclude the case $\sigma_2 \in 3A$: Pick an element $g \in G$ of order 11. Using (2) we see that there are exactly 11 solutions of $g = uv$ with $u \in 2A$, $v \in 3A$. Since $\langle g \rangle$ is transitive and abelian g does not centralize u (and v). Thus $\langle g \rangle$ acts fixed–point–freely on the pairs (u,v) with $g = uv$. So there is essentially one solution to $g = uv$ with $u \in 2A$ and $v \in 3A$. Now [**2**] tells us that G contains a transitive subgroup isomorphic to $H \cong \mathrm{PSL}_2(11)$. Again using (2) and [**2**] we see that there are elements g, u, and v in H of orders 11, 2, and 3 respectively with $g = uv$. The previous consideration shows that a conjugate of $\langle \sigma_1, \sigma_2 \rangle$ is a subgroup of H, therefore σ_1 and σ_2 do not generate G.

Now consider the case $\sigma_2 \in 4A$. Set $H = \langle \sigma_1, \sigma_2 \rangle$. If $H \neq G$ then $H \leq \mathrm{PSL}_2(11)$, as $\mathrm{PSL}_2(11)$ is the only maximal and transitive subgroup of M_{11} by [**2**]. However, $\mathrm{PSL}_2(11)$ does not contain an element of order 4. Thus σ_1 and σ_2 generate G. An explicit example is
$\sigma_1 = (4,5)(6,7)(8,9)(11,11)$, $\sigma_2 = (1,11,2,9)(8,3,5,7)$.

We treat the case $G = M_{23}$ quite similarly: Here we get $\sigma_1 \in 2A$, $\sigma_2 \in 4A$, and $H = \langle \sigma_1, \sigma_2 \rangle$ with $\sigma_1\sigma_2$ an 23-cycle. The only transitive and maximal subgroup of G has order 253, see [**2**]. Thus σ_1 and σ_2 generate G. Again we give one explicit example:
$\sigma_1 = (8,9)(10,11)(12,13)(14,15)(16,17)(18,19)(20,21)(22,23)$,
$\sigma_2 = (2,14)(17,19)(1,10,16,4)(8,13,15,6)(12,20,11,7)(3,9,5,22)$

2.6 $\mathbf{PSL}_2(q) \le G \le \mathbf{PGL}_2(q)$. The distinction between the projective case and the non–projective semilinear case simplifies the somewhat tedious way through the estimations. We assume $q \ge 5$ (because $\mathrm{PGL}_2(4) \cong \mathrm{A}_5$). Let p be the prime divisor of q.

For the case $q = 11$ and G of degree 11 see [**4, 4.3**]. Thus assume from now on that G acts naturally on the projective line.

Pick a $\sigma \in G$. There are three cases:

(i) σ has at least 2 fixed points. Then $\operatorname{ind}\sigma = (q-1)(1-\frac{1}{|\sigma|})$ by simple linear algebra.

(ii) σ has exactly one fixed point. Then $\operatorname{ind}\sigma = q(1-\frac{1}{|\sigma|})$ and $|\sigma| = p$.

(iii) σ has no fixed points. Denote by $\hat\sigma$ a preimage of σ in $\mathrm{GL}_2(q)$. Then $\langle\hat\sigma\rangle$ acts irreducibly on $\mathbb{F}_q^2$, hence $\mathbb{F}_q[\hat\sigma]$ is a quadratic field extension of $\mathbb{F}_q$ by Schur's Lemma. We deduce that $\langle\sigma\rangle$ acts fixed–point–freely on $\mathbf{P}^1(q)$, thus $\operatorname{ind}\sigma = (q+1)(1-\frac{1}{|\sigma|})$.

In all three cases we obtain $\operatorname{ind}\sigma \ge (q-1)(1-\frac{1}{|\sigma|}) \ge \frac{1}{2}(q-1)$. Therefore $s = 2$ by (*). As G contains the non–solvable group $\mathrm{PSL}_2(q)$, σ_2 cannot be an involution (recall the monotony of the orders of σ_i). This shows (again using (*)) $(q-1)(1-\frac{1}{2}+1-\frac{1}{3}) \le q$, hence $q \le 7$.

Suppose $q = 5$. We have $\operatorname{ind}\sigma \in \{2,3\}$, $\operatorname{ind}\sigma = 4$, or $\operatorname{ind}\sigma \in \{3,4\}$ if σ is of type (i), type (ii), or type (iii) respectively. Thus both σ_1 and σ_2 are of type (i) with $|\sigma_1| = 2$, $|\sigma_2| = 4$. One readily checks (see the arguments in the Mathieu group case) that σ_1 and σ_2 generate a group containing $\mathrm{PSL}_2(5)$. Since σ_2 is an odd permutation, they actually generate $\mathrm{PGL}_2(5)$. An explicit example is $\sigma_1 = (1,2)(3,4)$, $\sigma_2 = (3,2,5,6)$.

Now suppose $q = 7$. Similarly as above we get $|\sigma_1| = 2$, $|\sigma_2| = 3$, and $f(\sigma_1) = f(\sigma_2) = 2$. So σ_1 is an odd permutation, hence $G = \mathrm{PGL}_2(7)$. This case occurs as well, an example is provided by $\sigma_1 = (1,2)(3,4)(5,6)$, $\sigma_2 = (1,3,6)(2,7,8)$.

2.7 $\mathbf{PSL}_m(q) \le G \le \mathbf{P\Gamma L}_m(q)$. Set $q = p^e$ with a prime p. This case is even for $m = 2$ more complicated than the projective linear case since there are many more types of possible cycle decompositions. In particular a fixed–point–free element need not generate a fixed–point–free group.

Write $\Gamma\mathrm{L}_m(q) = \mathrm{GL}_m(q) \rtimes \Gamma$ with $\Gamma = \mathrm{Aut}(\mathbb{F}_q)$. Let $\Gamma\mathrm{L}_m(q)$ act from the left on $\mathbb{F}_q^m$. For $\sigma \in \mathrm{P\Gamma L}_m(q)$ denote by $\hat\sigma$ a preimage of σ in $\Gamma\mathrm{L}_m(q)$. Feit [**6**] told me a special case of the following lemma.

Lemma. *Write $\hat\sigma = g\gamma$ with $g \in GL_m(q)$ and $\gamma \in \Gamma$. Let e/i be the order of*

γ. Then $f(\sigma) \leq \frac{p^{im}-1}{p^i-1}$.

Proof. Set $\hat{\sigma}^{e/i} = h \in \mathrm{GL}_m(q)$. If $\hat{\sigma}v = \alpha v$ for $v \in \mathbb{F}_q^m \setminus \{0\}$, $\alpha \in \mathbb{F}_q$, then $hv = N(\alpha)v$, where $N : \mathbb{F}_q \to \mathbb{F}_{p^i}$ denotes the norm.

First suppose that h is a scalar. If $\hat{\sigma}w = \beta w$ for some $w \in \mathbb{F}_q^m \setminus \{0\}$, $\beta \in \mathbb{F}_q$, then $hw = N(\beta)w$ and therefore $N(\alpha) = N(\beta)$. By Hilbert's Theorem 90 there is a $\zeta \in \mathbb{F}_q^\times$ with $\alpha/\beta = \zeta^\gamma/\zeta$. From $\hat{\sigma}\zeta w = \zeta^\gamma \hat{\sigma} w = \zeta^\gamma \beta w = \alpha\zeta w$ we conclude that every $\hat{\sigma}$–invariant $\mathbb{F}_q$–line L contains an element $u \neq 0$ with $\hat{\sigma}u = \alpha u$. There are exactly $p^i - 1$ such points on L. One easily sees that a basis of the $\mathbb{F}_{p^i}$–space $\{v \in \mathbb{F}_q^m \,|\, \hat{\sigma}v = \alpha v\}$ is linearly independent over $\mathbb{F}_q$. This proves the assertion.

Now suppose that h is not a scalar. Let $\eta_1, \ldots, \eta_s$ be those elements in $\mathbb{F}_{p^i}$ which are eigenvalues of h. Let V_k be the eigenspace of h with eigenvalue η_k. Note that $h|_{V_k}$ is the smallest power of $\hat{\sigma}|_{V_k}$ which lies in $\mathrm{Aut}_{\mathbb{F}_q}(V_k)$. Set $d_k = \dim_{\mathbb{F}_q}(V_k)$. Every $\hat{\sigma}$–invariant line lies in one of these subspaces. The preceding consideration yields

$$f(\sigma) \leq \sum \frac{p^{id_k} - 1}{p^i - 1}.$$

From $(x^{\delta_1} - 1) + (x^{\delta_2} - 1) \leq x^{\delta_1+\delta_2} - 1$ for $x \geq 1$ and $\delta_1, \delta_2 \geq 0$ and $\sum d_k \leq m$ we get the assertion.

Proposition. *Set $\hat{\sigma} = g\gamma$ with $g \in GL_m(q)$ and $\gamma \in \Gamma$. Let e/i be the order of γ. Set $r = 1$ if $e = i$. Otherwise let r be the smallest prime divisor of e/i. Then*

$$\operatorname{ind} \sigma \geq (1 - \frac{1}{|\sigma|})(q^{m-1} - 1) + (1 - \frac{1}{e/i})(\frac{q^{m-1} - 1}{q - 1} - \frac{q^{m/r} - 1}{q^{1/r} - 1} + 1).$$

Proof. We use the formula in 2.4, together with the well–known relation $\sum_{t|m} \varphi(t) = m$. If $\sigma^k \notin \mathrm{PGL}_m(q)$, then we estimate the number of fixed points with the preceding lemma. Note that γ^k has the order $\frac{e}{i(e/i,k)} = \frac{e}{(e,ik)}$, where (a, b) denotes the greatest common divisor of a and b. If however $1 \neq \sigma^k \in \mathrm{PGL}_m(q)$, then clearly $f(\sigma) \leq \frac{1}{q-1}(q^{m-1} - 1 + q - 1) = \frac{q^{m-1}-1}{q-1} + 1$.

$$
\begin{aligned}
|\sigma|\cdot o(\sigma) &= \sum_{\substack{k \big| |\sigma| \\ \frac{e}{i}|k}} f(\sigma^k)\varphi(\frac{|\sigma|}{k}) + \sum_{\substack{k \big| |\sigma| \\ \frac{e}{i}\nmid k}} f(\sigma^k)\varphi(\frac{|\sigma|}{k}) \\
&\le \sum_{\substack{k \big| |\sigma| \\ \frac{e}{i}|k}} (\frac{q^{m-1}-1}{q-1}+1)\cdot\varphi(\frac{|\sigma|}{k}) + (\frac{q^m-1}{q-1} - \frac{q^{m-1}-1}{q-1} - 1)\varphi(1) + \\
&\quad \sum_{\substack{k \big| |\sigma| \\ \frac{e}{i}\nmid k}} \frac{p^{(e,ik)m}-1}{p^{(e,ik)}-1}\varphi(\frac{|\sigma|}{k}) \\
&\le \sum_{\substack{k \big| |\sigma| \\ \frac{e}{i}|k}} (\frac{q^{m-1}-1}{q-1}+1)\cdot\varphi(\frac{|\sigma|}{k}) + q^{m-1} - 1 + \sum_{\substack{k \big| |\sigma| \\ \frac{e}{i}\nmid k}} \frac{p^{em/r}-1}{p^{e/r}-1}\varphi(\frac{|\sigma|}{k}) \\
&= \sum_{\substack{k \big| |\sigma| \\ \frac{e}{i}|k}} (\frac{q^{m-1}-1}{q-1} + 1 - \frac{q^{m/r}-1}{q^{1/r}-1})\cdot\varphi(\frac{|\sigma|}{k}) + \frac{q^{m/r}-1}{q^{1/r}-1} + q^{m-1} - 1 \\
&= \sum_{t|\frac{|\sigma|}{e/i}} (\frac{q^{m-1}-1}{q-1} + 1 - \frac{q^{m/r}-1}{q^{1/r}-1})\cdot\varphi(t) + \frac{q^{m/r}-1}{q^{1/r}-1} + q^{m-1} - 1 \\
&= (\frac{q^{m-1}-1}{q-1} + 1 - \frac{q^{m/r}-1}{q^{1/r}-1})\frac{|\sigma|}{e/i} + \frac{q^{m/r}-1}{q^{1/r}-1} + q^{m-1} - 1,
\end{aligned}
$$

from which the assertion follows.

If $i < e$, then we get, using $2 \le r \le e/i \le |\sigma|$,

Corollary. *Let $\sigma \in P\Gamma L_m(q) \setminus PGL_m(q)$.*
If $m \ge 4$, then

$$ind\sigma \ge (1 - \frac{1}{|\sigma|})(q^{m-1}-1) + \frac{1}{2}(\frac{q^{m-1}-1}{q-1} - \frac{q^{m/2}-1}{q^{1/2}-1} + 1).$$

If $m \in \{2,3\}$, then

$$ind\sigma \ge (1 - \frac{1}{|\sigma|})(q^{m-1} - q^{1/2}).$$

Now we are prepared to discuss condition (*). Let $\sigma'_1, \dots, \sigma'_s \in G \le \mathrm{P\Gamma L}_m(q)$ be a system as in (*).

If not all the σ'_i are involutions, then assume without loss that σ'_s is not an involution, and set $\sigma_1 = \sigma'_1\sigma'_2\dots\sigma'_{s-1}$, $\sigma_2 = \sigma'_s$.

If all the σ'_i are involutions, then $s \ge 3$, as G is not dihedral. By conjugation and operations of the kind $\dots, a, b, \dots \mapsto \dots, b, a^b, \dots$ we may assume that

σ'_{s-1} and σ'_s do not commute. Then $\sigma'_{s-1}\sigma'_s$ is not an involution, and we set $\sigma_1 = \sigma'_1\sigma'_2 \cdots \sigma'_{s-2}$, $\sigma_2 = \sigma'_{s-1}\sigma'_s$.

In either case we have $\sigma_1, \sigma_2 \in G$ which not both are involutions, such that $\operatorname{ind}\sigma_1 + \operatorname{ind}\sigma_2 \leq n-1$ (with $n = (q^m-1)/(q-1)$) and such that $\sigma_1\sigma_2$ is an n–cycle. (As to the inequality for the index note that $\operatorname{ind}\sigma$ is also the minimal number of transpostions required to write σ as a product with. Thus $\operatorname{ind}\sigma\tau \leq \operatorname{ind}\sigma + \operatorname{ind}\tau$. From this we actually get $\operatorname{ind}\sigma_1 + \operatorname{ind}\sigma_2 = n-1$.)

If $\sigma_1, \sigma_2 \in \mathrm{PGL}_2(q)$, then $q = 5$ or 7 as in section 2.6. If $\sigma_1, \sigma_2 \in \mathrm{PGL}_m(q)$ for $m \geq 3$, then proceed as in [**4**]. The key tool [**4, 3.4**] is correct in this case.

From now on suppose that one of the elements σ_1, σ_2 is not contained in $\mathrm{PGL}_m(q)$. As a consequence of Zsigmondy's Theorem and Schur's Lemma, we get that the n–cycle $\sigma_1\sigma_2$ is contained in $\mathrm{PGL}_m(q)$ except possibly for $m = 2, q = 8$, see the proof of [**4, 5.1**]. The case $m = 2, q = 8$ is excluded until otherwise stated.

Thus σ_1 and σ_2 have the same order $e/i \geq 2$ modulo $\mathrm{PGL}_m(q)$. In particular $|\sigma_1|$ and $|\sigma_2|$ have a common divisor > 1.

First suppose $m \geq 4$. Using $n - 1 \geq \operatorname{ind}\sigma_1 + \operatorname{ind}\sigma_2$ and the Corollary we get

$$(2)\quad q\frac{q^{m-1}-1}{q-1} \geq ((1-\frac{1}{2}) + (1-\frac{1}{4}))(q^{m-1}-1) + (\frac{q^{m-1}-1}{q-1} - \frac{q^{m/2}-1}{q^{1/2}-1} + 1).$$

As the last summand on the right side is positive, we get

$$q\frac{q^{m-1}-1}{q-1} \geq \frac{5}{4}(q^{m-1}-1),$$

hence $q = 4$. Now we use $q = 4$ in (2), and easily get the contradiction $m \leq 3$.

Now suppose $m = 3$. Similarly as above we get

$$q(q+1) \geq \frac{5}{4}(q^2 - q^{1/2}),$$

hence $q = 4$. For a treatment of $G \leq \mathrm{P\Gamma L}_3(4)$ confer [**4**].

From now on suppose $m = 2$. Without loss we assume $|\sigma_1| \leq |\sigma_2|$. As above we get

$$q \geq \frac{5}{4}(q - q^{1/2}),$$

hence $q \leq 25$.

If $q = 25$, then $|\sigma_1| = 2$, $|\sigma_2| = 4$, and $\sigma_2^2 \in \mathrm{PGL}_2(25)$, hence $f(\sigma_2) \leq f(\sigma_2^2) \leq 2$. From 2.4 we get $\operatorname{ind}\sigma_2 \geq 18$, hence $\operatorname{ind}\sigma_1 \leq 7$, contrary to the Corollary.

Now suppose $q = 16$. We quickly get $|\sigma_1| = 2$ and $|\sigma_2| = 4$. As σ_1 and σ_2 have the same order modulo $\mathrm{PGL}_2(16)$, we get $\sigma_2^2 \in \mathrm{PGL}_2(16)$. Now σ_2^2 has exactly one fixed point, hence so does σ_2. It follows $\operatorname{ind}\sigma_2 = 12$, hence $\operatorname{ind}\sigma_1 = 4$, contrary to the Corollary.

Now suppose $q = 9$. We get $s = 2$, for if $s \geq 3$ then $s = 3$ and the σ_i are fixed–point–free involutions. However $\mathrm{PGL}_2(9)$ does not contain fixed–point–free involutions, contrary to $\sigma_1\sigma_2\sigma_3 \in \mathrm{PGL}_2(9)$.

So we get $|\sigma_1| = 2$ and $|\sigma_2| = 4$. An explicit example is $\sigma_1 = (2,7)(5,6)(8,10)$, $\sigma_2 = (1,4,9,2)(3,5,7,10)$.

For the last case $G = \mathrm{P\Gamma L}_2(8)$ we get from the index estimations $s = 2$ and $(|\sigma_1|, |\sigma_2|) = (2,3)$ or $(3,3)$. Explicit examples are $\sigma_1 = (2,3)(4,5)(6,7)(8,9)$, $\sigma_2 = (7,5,8)(1,9,3)$ and $\sigma_1 = (4,5,6)(7,8,9)$, $\sigma_2 = (5,9,2)(6,3,1)$.

As $\mathrm{P\Gamma L}_2(4) \cong \mathrm{S}_5$ we do not discuss $q = 4$.

3. Rationality Questions

3.1. Using a special case of the so–called branch cycle argument (for a short proof see [**10**]), we get the following

Lemma. *Let $f \in \mathbb{Q}[X]$ be a polynomial of degree n. Let G be the monodromy group of f, and let σ be an n–cycle as in (*). Let $\hat{G}$ be the normalizer of G in S_n. Then any two generators of $Z = \langle\sigma\rangle$ are conjugate in $\hat{G}$.*

We now prove the Theorem from the Introduction.

We note that f is indecomposable even over $\mathbb{C}$ by [**12, 3.5**]. Thus we apply our result from section 2.2. As for type (i), consider the polynomials $f(x) = x^p$ or $f \in \mathbb{Q}[X]$ defined by $f(z + \frac{1}{z}) = z^p + \frac{1}{z^p}$ to get the cyclic group or the dihedral group, both of degree p.

If f is of type (ii), then Fried showed ([**8, Section 3**]) that $f \notin \mathbb{Q}[X]$. We remark that Fried did this without actually knowing the occurring groups (even to prove that there are only finitely many examples seems to require the classification of the finite simple groups).

Now we discuss the type (iii). The group S_n is in some sense the generic case. To get this group take for instance $f(X) = X^n - X$. The discriminant of $f(X) - t$ is a polynomial of degree $n-1$ in t, and the roots of the discriminant are precisely the finite branch points of $f: \mathbb{P}^1 \to \mathbb{P}^1$. In this case the discriminant has $n-1$ different simple roots, therefore σ_i is a transposition for $i = 1, \ldots, r-1$, see 2.1. Thus G is a transitive group generated by transpositions, and such a group is symmetric.

Similarly we get the alternating group. Choose f such that its derivative equals $(X^m - 1)^2$, thereby $2m + 1 = n$. Denote by S the set of m^{th} roots of unity. Then the discriminant of $f(X) - t$ equals, up to a multiplicative constant, $\Delta(t) = \prod_{\zeta \in S}(t - f(\zeta))^2$. Note that Δ has m different roots, each of multiplicity 2. Now $f'(\zeta) = f''(\zeta) = 0 \neq f'''(\zeta)$ for each $\zeta \in S$. This shows that (in the notation of 2.1) $r = m + 1$ and each σ_i $(i = 1, \ldots, r-1)$ is a 3-cycle. So the transitive group G is generated by 3-cycles, thus $G = \mathrm{A}_n$ (see [**18, lemme 1 in 4.**]).

Next we exclude M_{11}, M_{23} and $\mathrm{PGL}_2(7)$ using the Lemma from above. Observe that every automorphism of these groups is inner, hence $\hat{G} = G$ in these cases. To exclude the two Mathieu groups it suffices to see that no element of order 11 (resp. 23) is conjugate to its inverse. This can be deduced from [**2**].

Suppose that $\mathrm{PGL}_2(7)$ meets the conclusion of the Theorem. As Z has 4 generators, $8 \cdot 4 = |\mathrm{N}_G(Z)|$ does divide $7 \cdot 48 = |G|$, a contradiction.

For the group $\mathrm{P\Gamma L}_2(8)$ we got two different types of branch cycle descriptions. We show that the case with $|\sigma_1| = 2$, $|\sigma_2| = 3$ does not occur. Of course $\sigma_1 \in \mathrm{PGL}_2(8)$ and $\sigma_2 \notin \mathrm{PGL}_2(8)$. Thus the 9–cycle $\sigma = \sigma_1\sigma_2$ is not contained in $\mathrm{PGL}_2(8)$. Thus σ has order 3 modulo $\mathrm{PGL}_2(8)$, and therefore cannot be conjugate to its inverse.

It remains to show that $\mathrm{PGL}_2(5)$, $\mathrm{P\Gamma L}_2(8)$ of type $(3, 3 : 9)$, and $\mathrm{P\Gamma L}_2(9)$ are monodromy groups of polynomials with rational coefficients and to exhibit the corresponding polynomials.

3.2 The group $\mathbf{PGL}_2(5)$. We know from our result in section 2, that there is a polynomial $f \in \mathbb{C}[X]$ with monodromy group $\mathrm{PGL}_2(5)$. We just compute it, and it will turn out that it can be chosen with rational coefficients. Recall the definition of the generators $\sigma_1, \dots, \sigma_s$ of the monodromy group. In our case we have (up to simultaneous conjugation with elements in S_6 and reordering the σ's) $\sigma_1 = (1, 2)(3, 4)$ and $\sigma_2 = (3, 2, 5, 6)$; that is a consequence of the considerations in 2.6.

Let f be monic, and let 0 be the branch point corresponding to σ_2. Without loss, above 0 lies the 4-fold point 0, and the simple points κ_1 and κ_2 ($\kappa_1, \kappa_2 \neq 0$). We have $\kappa_1 + \kappa_2 \neq 0$, for otherwise f were a composition with a quadratic polynomial. We may assume $\kappa_1 + \kappa_2 = -6$. Then $f(X) = X^4(X^2 + 6X + p)$ with $p \in \mathbb{C}$. The finite branch points of f are the zeroes of f'. We have $f'(X) = 2X^3(3X^2 + 15X + 2p)$. Let λ_1 and λ_2 be the zeroes of $h(X) = 3X^2 + 15X + 2p$. They are different, and have the same images under f. Write $f = q \cdot h + r$ with polynomials q and r, such that $\deg r \leq 1$. Then $f(\lambda_i) = r(\lambda_i)$, hence $r(\lambda_1) = r(\lambda_2)$. Thus r is a constant. On the other hand, by dividing the polynomials, we get that the coefficient of X in r is $8/3(p - 75/8)(p - 25)$. The choice $p = 75/8$ yields $3125/128$ as the second finite branch point. However, $f(X) - 3125/128 = 1/128(16X^3 - 24X^2 + 30X - 25)(2X + 5)^3$ shows that the ramification above this point is the wrong one. Thus $p = 25$.

3.3 The groups $\mathbf{P\Gamma L}_2(8)$ and $\mathbf{P\Gamma L}_2(9)$. The polynomials have been computed by Matzat. See [**17, 8.5**] for $\mathrm{P\Gamma L}_2(8)$ and [**17, 8.7**] for $\mathrm{P\Gamma L}_2(9)$.

Appendix: The Theorems of Ritt

The setup from section 2.1 allows for short proofs of the classical Theorems of Ritt about decompositions of polynomials. Throughout this section we deal with polynomials with complex coefficients. Via model theory the assertions hold for any algebraically closed field of characteristic 0. Using [**12, 3.5**] one readily gets that R.1 and R.2 hold for arbitrary fields of characteristic 0. By a maximal decomposition of a polynomial f we mean a decomposition $f = f_1 \circ f_2 \circ \cdots \circ f_r$ where the f_i are non–linear and indecomposable.

Theorem R.1 (Ritt). *Let $f = f_1 \circ \cdots \circ f_r = g_1 \circ \cdots \circ g_s$ be two maximal decompositions of a polynomial $f \in \mathbb{C}[X]$. Then $r = s$ and the degrees of the f_i's are a permutation of the degrees of the g_i's. Furthermore, one can pass from one decomposition to the other one by altering two adjacent polynomials in each step.*

From the latter part of this Theorem the question arises when $a \circ b = c \circ d$ with indecomposable polynomials a, b, c, and d. Recall that the Cebychev polynomial T_n is defined by $T_n(Z + 1/Z) = Z^n + 1/Z^n$.

Theorem R.2 (Ritt). *Let a, b, c, and d be non–linear indecomposable polynomials such that $a \circ b = c \circ d$. Assume without loss $\deg a \geq \deg c$. Then there exist linear polynomials L_1, L_2, L_3, and L_4 such that one of the following holds.*

(1)
$$a = c \circ L_1, b = L_1^{-1} \circ d, \text{ (the uninteresting case).}$$

(2)
$$L_1 \circ a \circ L_2^{-1} = X^k \cdot t(X)^m, \;\; L_2 \circ b \circ L_3 = X^m$$
$$L_1 \circ c \circ L_4^{-1} = X^m, \;\; L_4 \circ d \circ L_3 = X^k \cdot t(X^m)$$

for a polynomial t.

(3)
$$L_1 \circ a \circ L_2^{-1} = T_m, \;\; L_2 \circ b \circ L_3 = T_n$$
$$L_1 \circ c \circ L_4^{-1} = T_n, \;\; L_4 \circ d \circ L_3 = T_m \;.$$

for Cebychev polynomials T_m and T_n.

Let f be a polynomial with complex coefficients, and let x be a transcendental over $\mathbb{C}$. Set $t = f(x)$, and let Ω be the Galois closure of $\mathbb{C}(x)|\mathbb{C}(t)$. Let $G = \mathrm{Gal}(\Omega|\mathbb{C}(t))$ be the monodromy group of f, and let U be stabilizer of x. We view two decomposition of f as equivalent, if they differ just by linear twists (like (1) in R.2). As an easy consequence of Lüroth's theorem, we see that the equivalence classes of maximal decompositions of f correspond bijectively to the maximal chains of subgroups from U to G. If $f = f_1 \circ \cdots \circ f_r$ is such a decomposition, then the associated chain of subgroups is $U = U_0 < U_1 < \ldots < U_{r-1} < U_r = G$, where U_i is the stabilizer of $f_1(f_2(\cdots(f_i(x)\cdots))$. Then Theorem R.1 is a direct consequence of

Theorem R.3. *Let G be a finite group with subgroups U and C such that $G = UC$ and C is abelian. Then the maximal chains of subgroups from U to G have equal lengths and (up to permutation) the same relative indices. Furthermore, one can pass from one chain to an other one just by changing one group in the chain in each step.*

Proof of R.3. Choose a minimal counter–example subject to $U + [G : U]$ being minimal. Let $U = A_0 < A_1 < \ldots < A_r = G$ and $U = B_0 < B_1 < \ldots <$

$B_s = G$ be two chains failing the assertion. Then $A_1 \neq B_1$ and $\mathrm{core}_G(U) = 1$, where $\mathrm{core}_G(U)$ means the maximal normal subgroup of G, which is contained in U. Set $N_A = \mathrm{core}_G(A_1)$ and $N_B = \mathrm{core}_G(B_1)$. These groups are non–trivial, as $G = A_1C$, hence $1 \neq A_1 \cap C \leq \bigcap_{c\in C} A_1^c = \bigcap_{g\in G} A_1^g = N_A$. By maximality of U in A_1, and $N_A \not\leq U$, we get $A_1 = UN_A$. Likewise $B_1 = UN_B$. Set $D = \langle A_1, B_1\rangle$. The assumptions of the Theorem are fulfilled if we replace U by A_1 or B_1. We consider, in addition to the given chains, a maximal chain from D to G. Thus we are done once we know that A_1 and B_1 are maximal in D, $[D : A_1] = [B_1 : U]$, and $[D : B_1] = [A_1 : U]$. Note that $D = \langle N_AU, B_1\rangle = N_AB_1$. Suppose there is a group X properly between A_1 and $D = N_AB_1$. Then $X = N_A(X \cap B_1)$, hence $U < X \cap B_1 < B_1$, a contradiction. By symmetry B_1 is maximal in D as well.

Finally we have $N_A \cap B_1 \leq A_1 \cap B_1 = U$, hence $N_A \cap B_1 = N_A \cap U$. This yields $[D : B_1] = [N_A : N_A \cap B_1] = [N_A : N_A \cap U] = [A_1 : U]$. Again by symmetry we get $[D : A_1] = [B_1 : U]$. □

Proof of R.2. As in 2.1, let G be the Galois group of the Galois closure of $\mathbb{C}(X)|\mathbb{C}(t)$, where $a(b(X)) = c(d(X)) = t$.

Let A, B, and U be the fix groups of $b(X)$, $d(X)$, and X, respectively. The case $A = B$ yields (1) of the Theorem. From now on assume $A \neq B$. Then $U = A \cap B$ is core–free in G, and the chains of subgroups $U \subset A \subset G$ and $U \subset B \subset G$ are maximal. Let Z be a cyclic complement of U in G (c.f. 2.1).

Set $N_A = \mathrm{core}_G(A)$ ($\neq 1$, see the proof of R.3), $N_B = \mathrm{core}_G(B)$.

Then, by the maximality of the chains above, $G = AN_B = BN_A$, $A = UN_A$, and $B = UN_B$.

Set $m = [G : A] = [B : U]$, $n = [G : B] = [A : U]$.

Claim 1. *The monodromy groups of b and c are the same, as well as the ones of a and d.*

Proof. Set $N = \mathrm{core}_B(U)$. Of course $B \cap N_A = U \cap N_A \leq N$. On the other hand, the set of G-conjugates of A is the same as the set of B-conjugates of A. Therefore $N \leq N_A$, hence $N \leq B \cap N_A$. This shows $B \cap N_A = N$. Now $G/N_A = BN_A/N_A \cong B/B \cap N_A = B/N$ yields the assertion. □

Now we are going to study three different permutation representations of G. First let G act on the cosets of U. Then the set of cosets of A provides a system of imprimitivity, and so does the set of cosets of B. The intersection of a coset of A and a coset of B is a coset of U: Without loss consider A and Bg. We may assume $g \in N_A \subseteq A$ (as $G = BN_A$). Then $Ug \leq A \cap Bg$. If $Uh \leq A \cap Bg$, then $hg^{-1} \in A \cap B = U$, hence $Uh = Ug$. Therefore $Ug = A \cap Bg$.

Denote by π_A the canonical homomorphism $G \longrightarrow G/N_A \leq \mathrm{Sym}(G/A)$ of permutation groups, likewise for B. Note that $\pi_A(G)$ and $\pi_B(G)$ act primitively by the maximality of A and B in G.

Let $\mathrm{ind}(g)$, $o(g)$, and $\mathrm{f}(g)$ be the index of g, the number of cycles of g, and the number of fixed–points of g. Define $\mathrm{ind}_A(g)$, $o(g)$, and $\mathrm{f}_A(g)$ analogously for $\pi_A(g)$, likewise for B. From the considerations above we get $\mathrm{f}(g) = \mathrm{f}_A(g) \cdot \mathrm{f}_B(g)$.

For a fixed $g \in G$ let $[\nu_1, \nu_2, \cdots, \nu_k]$ be the cycle type of $\pi_A(g)$ (i.e. $\pi_A(g)$ has cycles of lengths ν_1, ν_2, …) and $[\mu_1, \mu_2, \cdots, \mu_l]$ be the cycle type of $\pi_B(g)$. Then

$$\sum_{i=1}^{k} \nu_i = m$$

$$\sum_{j=1}^{l} \mu_j = n$$

$$k = o_A(g) = m - \operatorname{ind}_A(g)$$

$$l = o_B(g) = n - \operatorname{ind}_B(g)$$

$$\sum_{i,j} (\nu_i, \mu_j) = o(g) = mn - \operatorname{ind}(g) \quad .$$

These relations imply

$$\operatorname{ind}(g) \geq n \cdot \operatorname{ind}_A(g)$$

$$\operatorname{ind}(g) \geq m \cdot \operatorname{ind}_B(g) \quad .$$

Let g_1, g_2,…,g_s be a generating system of G according to 2.2(*).

Claim 2. $\sum_{u=1}^{s} \operatorname{ind}_A(g_u) = m - 1$, $\sum_{u=1}^{s} \operatorname{ind}_B(g_u) = n - 1$.

Proof. $\sum \operatorname{ind}_A(g_u) \geq m - 1$ (for otherwise the elements $\pi_A(g_u)$ were a branch cycle description of a cover $X \to \mathbb{P}^1$ with X having negative genus). On the other hand, $\sum \operatorname{ind}_A(g_u) \leq \frac{1}{n} \sum \operatorname{ind}(g_u) = \frac{1}{n}(mn - 1) = m - \frac{1}{n}$. This proves the assertion. Here and in the following we use implicitly the symmetry of certain assertions in A and B. □

Claim 3. *If* $\pi_A(G)$ *is not cyclic, then* $\operatorname{ind}(g) \geq m \cdot \operatorname{ind}_B(g) + \operatorname{ind}_A(g)$ *for all* $g \in \{g_1, g_2, \cdots, g_s\}$.

Proof. Assume the contrary, which implies $o(g) > m \cdot o_B(g) + o_A(g) - m$ for some $g \in \{g_1, g_2, \cdots, g_s\}$. Assign to this g the ν's and μ's as above. Then

$$\sum_{i,j} (\nu_i, \mu_j) > \sum_{i,j} \nu_i + \sum_i 1 - \sum_i \nu_i$$

Thus there is an index i, without loss $i = 1$, such that

$$\sum_j (\nu_1, \mu_j) > \sum_j \nu_1 + 1 - \nu_1 \quad .$$

Let T be the number of j's such that ν_1 does not divide μ_j. Then

$$\nu_1/2 \cdot T \leq \sum_j (\nu_1 - (\nu_1, \mu_j)) < \nu_1 - 1 \ ,$$

hence $T \leq 1$. Thus there is at most one j_0 such that ν_1 does not divide μ_{j_0}. But $(\nu_1, \mu_{j_0}) = 1$ yields the contradiction $0 < 0$. Therefore the μ's have a common divisor $\delta > 1$. From Claim 2 we know that the elements $\pi_A(g_1), \ldots, \pi_A(g_s)$ provide a branch cycle description of a polynomial. A common divisor δ of the μ's means, that this polynomial has the form $h(X)^\delta + e$ for some polynomial h

and a constant e. However, this polynomial is decomposable, contrary to $\pi_A(G)$ being primitive. □

Claim 4. *If $\pi_A(G)$ is not cyclic, then* $\mathrm{ind}(g) = m \cdot \mathrm{ind}_B(g) + \mathrm{ind}_A(g)$ *for all* $g \in \{g_1, g_2, \dots, g_s\}$.

Proof. Suppose wrong. Then Claim 2 and Claim 3 yield the contradiction

$$mn-1 = \sum_{u=1}^{s} \mathrm{ind}(g_u) > m \sum_{u=1}^{s} \mathrm{ind}_B(g_u) + \sum_{u=1}^{s} \mathrm{ind}_A(g_u) = m(n-1)+m-1 = mn-1 \ .$$

□

Claim 5. *Exactly one of the following holds.*

(1) *$\pi_A(G)$ or $\pi_B(G)$ is cyclic.*
(2) *G, $\pi_A(G)$, and $\pi_B(G)$ are dihedral and act naturally (i.e. the cyclic group of index 2 acts regularly in each case).*

Proof. Suppose that (1) doesn't hold. Choose any $g \in \{g_1, g_2, \dots, g_s\}$. Assign to g the cycle lengths ν_i and μ_j of $\pi_A(g)$ and $\pi_B(g)$ as in the proof of Claim 3.

The proof of Claim 3 shows that

$$\sum_j (\nu_i, \mu_j) = \sum_j \nu_i + 1 - \nu_j \quad \text{for each } i = 1, \dots, k \ .$$

Furthermore, also by this proof, the following holds: For each j there is at most one i such that μ_j does not divide ν_i. In particular, for fixed j, $\nu_i \geq \mu_j$ besides at most one index i. Thus

$$(o_A(g) - 1)\mu_j + 1 \leq m \ .$$

Now, for g_u in $\{g_1, g_2, \dots, g_s\}$, let w_u be the maximal associated cycle length μ_j. Then

$$(m - \mathrm{ind}_A(g_u) - 1)w_u + 1 \leq m \ .$$

Dividing by w_u and adding for $u = 1, 2, \dots, s$ yields

$$\sum_{u=1}^{s} (1 - \frac{1}{w_u}) \leq 1 \ .$$

Therefore all besides two w's are 1, and these two exceptions are 2. By the choice of the w's, this implies the existence of two indices u_1 and u_2 such that $\pi_B(g_{u_1})$ and $\pi_B(g_{u_2})$ are involutions, and the other $\pi_B(g_u)$'s are trivial. The same holds for the images of g_u in $\pi_A(G)$ for the same indices u, as can be seen (for instance) by Claim 4. Finally, as $G \longrightarrow \pi_A(G) \times \pi_B(G)$ is an injective homomorphism, the involutions g_{u_1} and g_{u_2} are the only non–trivial elements in $\{g_1, g_2, \dots, g_s\}$.

We get the assertion about the action as follows: $g_{u_1} g_{u_2}$ is an mn–cycle, hence the involutions g_{u_1} and g_{u_2} (neither of which is contained in $\langle g_{u_1} g_{u_2} \rangle$) generate a dihedral group of order $2mn$. □

The final step is to formulate our results in terms of polynomials: Suppose that (1) in Claim 5 holds. Then, by Claim 1, we need to study the decomposition $p(X^m) = q(X)^m$ for some polynomials p and q. Set $p(X) = X^k \cdot r(X)$ with r a polynomial such that $r(0) \neq 0$. Then $X^{km} \cdot r(X^m) = q(X)^m$. Thus X^k divides $q(X)$, hence $q(X) = X^k \cdot s(X)$ with a polynomial s such that $s(0) \neq 0$. We get $r(X^m) = s(X)^m$. Now every zero of r occurs with a multiplicity divisible by m, hence $r(X) = t(X)^m$ with a polynomial t. But then $s(X) = \zeta t(X^m)$ for some m-th root ζ of 1. Substituting back we get our result.

Now assume that case (2) of Claim 5 holds. Without loss of generality we assume $a \circ b = c \circ d = T_{mn} = T_m \circ T_n$. Then the fix groups of $T_n(X)$ and of $b(X)$ in G have the same order, thus they are equal (every group M between U and G is uniquely determined by its order, as $M = UZ \cap M = U(M \cap Z)$ and subgroups of cyclic groups are determined by their order). Thus $\mathbb{C}(T_n(X)) = \mathbb{C}(b(X))$, hence $b = L_2^{-1} \circ T_n$ for some linear polynomial L_2. Then $T_n \circ T_m = a \circ b = a \circ L_2^{-1} \circ T_n$, hence $a = T_n \circ L_2$.

Analogously express c and d in terms of T_m and T_n. The assertion follows. □

References

[1] M. Aschbacher, *On conjectures of Guralnick and Thompson*, J. Algebra **135** (1990), 277–343.

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

[3] F. Dorey, G. Whaples, *Prime and composite polynomials*, J. Algebra **28** (1974), 88–101.

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

[5] W. Feit, *Some consequences of the classification of finite simple groups*, The Santa Cruz conference on finite groups, Proc. Sympos. Pure Math., vol. 37, AMS, Providence, Rhode Island, 1980, pp. 175–181.

[6] W. Feit, *E-mail from 28. Jan 1992.*

[7] M. Fried, *On a conjecture of Schur*, Michigan Math. J **17** (1970), 41–55.

[8] ———, *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.

[9] ———, *Rigidity and applications of the classification of simple groups to monodromy, Part II – Applications of connectivity; Davenport and Hilbert-Siegel Problems*, Preprint.

[10] ———, *Review of Serre's 'Topics in Galois Theory'*, Bull. Amer. Math. Soc. **30(1)** (1994), 124–135.

[11] M. Fried, M. Jarden, *Field Arithmetic*, Springer, Berlin Heidelberg, 1986.

[12] M. Fried, R. E. MacRae, *On the invariance of chains of fields*, Illinois Journal of Mathematics **13** (1969), 165–171.

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

[14] R.M. Guralnick, J. Saxl, *Monodromy groups of polynomials*, Preprint (1993).

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

[16] B. Huppert, *Primitive, auflösbare Gruppen*, Arch. Math. **6** (1955), 303–310.

[17] B. H. Matzat, *Konstruktion von Zahl– und Funktionenkörpern mit vorgegebener Galoisgruppe*, J. Reine Angew. Math. **349** (1984), 179–220.

[18] J.-F. Mestre, *Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\tilde{A}_n$*, J. Alg. **131** (1990), 483–495.

[19] P. Müller, *Monodromiegruppen rationaler Funktionen und Irreduzibilität von Polynomen mit variablen Koeffizienten*, Thesis (1994).

[20] P. Müller, H. Völklein, *On a problem of Davenport*, submitted (1994).

[21] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51–66.

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

Mathematisches Institut, Universität Erlangen–Nürnberg, Bismarckstrasse $1\frac{1}{2}$, D–91054 Erlangen, Germany

E-mail address: mueller@mi.uni-erlangen.de