PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 140, Number 9, September 2012, Pages 2967–2980
S 0002-9939(2012)11199-2
Article electronically published on January 12, 2012

POLYNOMIALS WITH AGL-MONODROMY

FLORIAN MÖLLER

(Communicated by Ted Chinburg)

ABSTRACT. Let p be a prime and r, e positive integers. In this paper we prove that the full affine group $\mathrm{AGL}(r, p^e)$ of dimension r over the field with p^e elements can be realized as the geometric monodromy group of a polynomial in characteristic p. We also determine the arithmetic monodromy group of this polynomial and the ramification structure it induces.

1. INTRODUCTION

Let p be a prime, K a fixed algebraic closure of the field with p elements, $f \in K[X]$ a polynomial with coefficients in K, and k the subfield of K that is generated by the coefficients of f. Denote with t a transcendental over K. Suppose that f is not a p-th power of some other polynomial. Then $f(X) - t \in K(t)[X]$ is separable and, hence, we can define the two Galois groups

$$A_f := \mathrm{Gal}\big(f(X) - t \mid k(t)\big) \qquad \text{and} \qquad G_f := \mathrm{Gal}\big(f(X) - t \mid K(t)\big).$$

A_f is called the *arithmetic monodromy group of* f; G_f is called the *geometric monodromy group of* f.

Monodromy groups of a polynomial encode many properties of the polynomial. In fact, some questions about polynomials can be entirely stated in terms of their monodromy groups. A prominent example of such a question was motivated by Dickson [12] in 1896:

Call a polynomial f over a finite field k of characteristic $p > 0$ *exceptional over* k if the mapping $\kappa \to \kappa$, $x \mapsto f(x)$ is bijective for infinitely many finite extensions κ of k. Now, given a finite field k, which polynomials are exceptional over k?

Clearly, f is exceptional if and only if the p-th power of f is. Hence, we can restrict ourselves to exceptional polynomials that are not p-th powers of other polynomials. This allows us to give a translation of the question after exceptionality in terms of pure group theory: Fix a root x of $f(X) - t$ and denote the stabilizer of x in G_f resp. A_f with H resp. U. Then f is exceptional if and only if H and U only have the orbit $\{x\}$ in common.

Albeit interesting advances have been made (cf. [14] and thereupon [15, 16, 18]) the exceptionality problem is still open, mainly, because up to now we cannot decide whether a given group G is a monodromy group or not — except by constructing an appropriate polynomial. However, there is a necessary condition on G: the infinite place of $K(t)$ ramifies totally in a root field of $f(X) - t$. Hence, G must contain a subgroup that can serve as an inertia group of the infinite place. Using

Received by the editors August 11, 2009 and, in revised form, December 8, 2010 and March 23, 2011.

2010 *Mathematics Subject Classification.* Primary 12F05, 12F10.

this restriction, Guralnick and Saxl [17] produced a list of possible candidates for monodromy groups. But it is still unclear which groups of this list actually occur.

In a long series of papers, Abhyankar found many polynomials realizing groups on the Guralnick-Saxl list; among them are various simple groups, projective groups, and linear groups; cf. [1, 2, 3]. An expository summary about Abhyankar's work on monodromy groups with many references is given in [5, Sec. 15 ff.]. Recently, Conway, McKay, and Trojan [9] simplified some of Abhyankar's proofs and, additionally, gave particularly nice polynomials with monodromy groups including several Mathieu groups.

Also, in dealing with the exceptionality problem many interesting monodromy groups have been found, for instance, some affine groups, dihedral groups, and $\mathrm{PSL}(2,q)$; cf. [15, 16, 18].

It seems that a classification of affine monodromy groups is especially challenging. This is caused by the fact that an affine group naturally fulfills the necessary condition on monodromy groups stated above: simply choose some extension of the translation subgroup as a candidate for an inertia group of the infinite place.

Therefore the affine monodromy case is wide and open. For instance, the Guralnick-Saxl list [17, Thm. A] subsumes this case under the statement "G_f has degree a prime power". Under strong additional assumptions one can prove more; cf. [17, Thms. 6.3, 6.4]. But the general affine case is far from being settled.

In this paper we present a new class of polynomials realizing the full affine groups $\mathrm{AGL}(n,q)$ as geometric monodromy groups. We also determine which arithmetic monodromy groups occur. Additionally, we explicitly describe the ramification structure induced by this class.

Our polynomials can essentially be seen as a generalization of the polynomial $X^{p^r}+X^{p^r-1}$ whose geometric monodromy was proved to be $\mathrm{AGL}(1,p^r)$ by Abhyankar [4] in 1994. One obtains Abhyankar's polynomials by setting $s=0$ in (1). An alternative and probably simpler proof of Abhyankar's result is given in Corollary 8.

Definitions and notation. Throughout this paper p is a prime, $\mathbb{F}_p$ the field with p elements, and K a fixed algebraic closure of $\mathbb{F}_p$. Every algebraic extension of $\mathbb{F}_p$ is regarded as a subfield of K. For q a power of p we denote the field with q elements by $\mathbb{F}_q$. t is a transcendental element over K. We write $F^\times$ for the set of invertible elements of a field F.

$f\in K[X]$ always denotes a polynomial of the form

$$f(X):=X^{p^r}+\sum_{i=0}^{s}a_iX^{p^r-p^i}\qquad\text{with}\qquad a_i\in K,\ s<r,\ \text{and } a_0a_s\neq 0. \tag{1}$$

Sometimes we write n instead of p^r for the degree of f.

k is the smallest field over which f is defined, i.e., $k=\mathbb{F}_p(a_0,\dots,a_s)$. Note that $f'\neq 0$. Hence, $f(X)-t\in K(t)[X]$ is separable and the monodromy groups

$$A_f=\mathrm{Gal}\big(f(X)-t|k(t)\big)\qquad\text{and}\qquad G_f=\mathrm{Gal}\big(f(X)-t|K(t)\big)$$

are defined. The roots of $f(X)-t$ in some algebraic closure of $K(t)$ are denoted by $x_1,\dots,x_n$. x is a fixed root of $f(X)-t$. Define

$$L:=K(x_1,\dots,x_n)\qquad\text{and}\qquad\lambda:=k(x_1,\dots,x_n);$$

L resp. λ is the splitting field of $f(X)-t$ over $K(t)$ resp. $k(t)$.

We always consider A_f and G_f as permutation groups acting naturally on the set of roots $\{x_1, \dots, x_n\}$. Note that both monodromy groups are transitive since the polynomial $f(X) - t$ is irreducible (its negative is a monic polynomial of degree 1 in t).

Our notation for the classical linear groups and their projective and affine incarnations is standard. Unless explicitly stated these groups always act naturally on their modules. Throughout, we denote the translation subgroup of a primitive affine group by N. Note that N is the unique minimal normal subgroup of this group.

Outline of the paper. Section 2 deals with the determination of the monodromy groups of f.

We first show that the polynomials in question are closely related to linear polynomials, i.e., polynomials of the shape $\sum_{i=0}^{r} a_i X^{p^i}$. This yields upper bounds on the monodromy groups. A consideration of some permutation properties of G_f proves that G_f is almost always a Jordan group (a definition and a classification result about Jordan groups are stated in Section 2.2). This gives a lower bound on G_f and eventually proves

Theorem 1. *Let f be a polynomial of the form* (1). *Define e to be the greatest common divisor of r and all $0 \le i \le s$ with $a_i \neq 0$, $e := \gcd(r, i \mid a_i \neq 0)$. Then $G_f = \mathrm{AGL}(r/e, p^e)$.*

An investigation of constant field extensions of $\lambda|k(t)$ in Section 2.4 yields

Corollary 2. *Let f be a polynomial of the form* (1) *and define the integer e as in the theorem above. Then A_f is the unique intermediate group between $G_f = \mathrm{AGL}(r/e, p^e)$ and $\mathrm{A\Gamma L}(r/e, p^e)$ with*

$$[A_f : G_f] = [k\mathbb{F}_{p^e} : k].$$

Here, $k\mathbb{F}_{p^e}$ denotes the compositum of k and $\mathbb{F}_{p^e}$, i.e., the smallest subfield (of K) that contains both k and the field with p^e elements.

An interesting consequence of these two results is that G_f only depends on the degrees of the terms of f but not on the actual values of the coefficients. However, this is not true for A_f. For instance, denote by ξ an element of K with multiplicative order $p^2 - 1$ and define

$$f_1 := X^{p^4} + X^{p^4-1} + X^{p^4-p^2} \qquad \text{and} \qquad f_2 := X^{p^4} + X^{p^4-1} + \xi X^{p^4-p^2}.$$

Then, by Theorem 1,

$$G_{f_1} = G_{f_2} = \mathrm{AGL}(2, p^2).$$

But Corollary 2 yields

$$A_{f_1} = \mathrm{A\Gamma L}(2, p^2) \qquad \text{and} \qquad A_{f_2} = \mathrm{AGL}(2, p^2).$$

This discrepancy comes from the fact that the minimal fields of definition of the polynomials differ: f_1 can be defined over $\mathbb{F}_p$, whereas f_2 can only be defined over $\mathbb{F}_{p^2}$. Thus, in contrast to A_{f_2}, the group A_{f_1} permits an additional field automorphism of order 2.

In Section 3 we discuss the ramification structure of the extension $L|K(t)$. Our main result is Theorem 20, which gives the isomorphism types of the inertia groups of all branch points as well as a full description of the higher ramification.

We can use these results to explicitly calculate the genus γ of the fixed field E of the translation subgroup N in $L|K(t)$. The family (1) of polynomials can be used to construct examples of nonrational fields E. This is interesting insofar as there is little known about which function fields may occur for E.

For instance, consider the polynomial $f(X) = X^{p^2} + X^{p^2-1} + X^{p^2-p}$. Theorem 1 and the Riemann-Hurwitz genus formula yield

$$G_f = \mathrm{AGL}(2,p) \qquad \text{and} \qquad \gamma = \frac{1}{2}(p^3 - 3p^2 + 4).$$

This proves that γ is not bounded. The case $p = 3$ shows additionally that even if G_f is solvable E need not be rational.

2. Determination of the monodromy groups G_f and A_f

2.1. **An upper bound.** We first state a central but easy observation. Define $Z := X^{-1}$ and $z_i := x_i^{-1}$. Then the equation $f(X) - t = 0$ can be rewritten as

$$Z^{p^r} - \sum_{i=0}^{s} \frac{1}{t} a_i Z^{p^i} - \frac{1}{t} = 0. \tag{2}$$

Its zeros are exactly the z_i. Moreover, $L = K(z_1, \dots, z_n)$ and the action of A_f and G_f on $\{x_1, \dots, x_n\}$ is equivalent to the action on $\{z_1, \dots, z_n\}$.

Equations of type (2) have been intensively studied at least since Dickson [11]. A more contemporary approach can be found in Elkies [13], who proved the following.

Theorem 3 (based on Elkies [13, Thm. 3])**.** *Let $q := p^f$ be a power of p and denote by k the field with q elements. Let $c_0, \dots, c_n, t$ be algebraically independent transcendentals over k. Then the Galois group of*

$$\sum_{i=0}^{n} c_i X^{q^i} - t \tag{3}$$

over $k(c_0, \dots, c_n, t)$ is $\mathrm{AGL}(n, q)$.

Since equation (2) is a specialization of (3), we obtain the following lemma.

Lemma 4. *Both A_f and G_f are subgroups of* $\mathrm{AGL}(r, p)$.

Let e denote the greatest common divisor of r and all $0 \le i \le s$ with $a_i \neq 0$, $e := \gcd(r, a_i \mid a_i \neq 0)$. If κ is an algebraic extension of k containing $\mathbb{F}_{p^e}$, then

$$\mathrm{Gal}\big(f(X) - t | \kappa(t)\big) \le \mathrm{AGL}(r/e, p^e).$$

In particular, G_f is a subgroup of $\mathrm{AGL}(r/e, p^e)$.

Proof. The first claim follows from Theorem 3 by setting the parameter q of the theorem to p and the observation that equation (2) then results from a separable specialization of (3).

The second part of the lemma is due to the definition of e. The polynomial f can be written as

$$f(X) = X^{p^{e \cdot r/e}} + \sum_{i=0}^{m} \alpha_i X^{p^{e \cdot r/e} - p^{e \cdot i}},$$

where the α_i are elements of k, the integer $e \cdot m$ equals s, and $\alpha_0\alpha_m = a_0a_s \neq 0$. Setting $q := p^e$ and rewriting the equation $f(X) - t = 0$ according to (2) yield

$$Z^{q^{r/e}} - \sum_{i=0}^{m} \frac{1}{t}\alpha_i Z^{q^i} - \frac{1}{t} = 0.$$

Since we consider this equation over a field containing $\mathbb{F}_q$, Theorem 3 gives the claim. □

Remark 5. We shall describe the action of $\mathrm{AGL}(n, q)$ on the roots of (3) and, subsequently, the action of the monodromy groups of f.

Denote the set of roots of (3) with $R := \{z_1, \ldots, z_n\}$. Fix an element $z \in R$. Then R can be written as

$$R = z + V,$$

where V is the set of roots of the linearization of (3), i.e., of the polynomial $L(X) := \sum_{i=0}^{n} c_i X^{q^i}$. This polynomial fulfills $L(X + Y) = L(X) + L(Y)$ for any two transcendentals X and Y. Furthermore, $L(\alpha X) = \alpha L(X)$ if and only if $\alpha \in \mathbb{F}_q$. This shows that V is an $\mathbb{F}_q$-vector space and R is an affine space over V.

The action of $\mathrm{AGL}(n, q)$ on R is the natural action; cf. [13, p. 79]. Denote with N the unique minimal normal subgroup of $\mathrm{AGL}(n, q)$ and with H the stabilizer of z. Then

$$\mathrm{AGL}(n, q) = N \rtimes H.$$

N is the translation subgroup of $\mathrm{AGL}(n, q)$; it comprises the maps

$$t_v : \ R \to R, \qquad r \mapsto v + r \qquad \text{with } v \in V,$$

acts fixed point freely on R, and fixes V pointwise. By definition, $H = \mathrm{GL}(n, q)$ fixes z and acts on V in its natural n-dimensional representation.

The action of A_f and G_f on the set of roots of $f(X) - t$ is essentially the same as the action above. The monodromy groups are not merely subgroups of $\mathrm{AGL}(r, p)$; they also inherit the same permutation representation.

A more detailed consideration of the structure of f yields

Lemma 6. *G_f is doubly transitive.*

Proof. Let X and Y be algebraically independent transcendentals over K. Set $\phi(X, Y) := f(X) - f(Y) \in K[X, Y]$. We prove in the sequel that the polynomial $\frac{\phi(X,Y)}{X-Y}$ is absolutely irreducible. The claim then follows from [21, 6.11].

Suppose ϕ is written as a product

$$\phi(X, Y) = \big(A_k(X, Y) + A_{k-1}(X, Y) + \ldots\big)\big(B_m(X, Y) + B_{m-1}(X, Y) + \ldots\big)$$

with $A_i, B_i \in K[X, Y]$ being homogeneous polynomials of degree i. Then

$$A_k B_m = X^{p^r} - Y^{p^r} = (X - Y)^{p^r};$$

this gives $A_k = a(X - Y)^k$ and $B_m = a^{-1}(X - Y)^m$ with an $a \in K^\times$. Hence,

$$a_0(X^{p^r-1} - Y^{p^r-1}) = A_k B_{m-1} + A_{k-1} B_m = a(X-Y)^k B_{m-1} + a^{-1}(X-Y)^m A_{k-1}.$$

As the left-hand side of this equation is separable in X, it follows that $k = 1$ or $m = 1$. □

Remark 7. Note that the above lemmas do not imply that G_f is an affine group. For instance, the group $\mathrm{AGL}(3, 2)$ contains a doubly transitive nonaffine complement of its translation subgroup; cf. Huppert [19, II 3.4 (b)].

Lemma 6 gives a proof of Abhyankar's original theorem without using Zassenhaus' classification of finite near-fields.

Corollary 8. *If $s = 0$, then $G_f = \mathrm{AGL}(1, n)$.*

Proof. By the double transitivity of G_f the integer $n(n-1)$ divides $|G_f|$. Since $s = 0$, G_f is a subgroup of $\mathrm{AGL}(1, n)$ by Lemma 4. □

2.2. **Jordan groups.** In this and the following section we heavily use the theory of Jordan groups. For the convenience of the reader we state some definitions and results. We omit the proofs. These and additional information about the subject can be found, for instance, in Neumann [22].

We start with

Definition 9 (Jordan group)**.** Let G be a transitive group on a finite set Ω.

(1) A subset $\Gamma \subseteq \Omega$ is said to be a *Jordan set (for G acting on Ω)* if $|\Gamma| > 1$ and the pointwise stabilizer
$$G_{(\Delta)} := \{g \in G \mid \forall \delta \in \Delta : \delta^g = \delta\}$$
of the complement $\Delta := \Omega \setminus \Gamma$ is transitive on Γ. The set Δ will then be called the *Jordan complement corresponding to* Γ.
(2) In the case $\Gamma = \Omega$, we call Γ and Δ *trivial*.
(3) Suppose G is k-transitive but not $(k+1)$-transitive. Let Γ be a Jordan set for G. If its Jordan complement Δ has order $|\Delta| > k$, then we call Γ a *proper* Jordan set.
(4) G is called a *Jordan group* if there exists a proper Jordan set for G.

The distinction between proper and improper Jordan sets in number (3) of the definition results from the fact that if G is $(k+1)$-transitive, then any subset $\Delta \subseteq \Omega$ of size $\leq k$ is a Jordan complement. Hence, improper Jordan sets do not reveal any additional information about G.

We also need the following classification.

Theorem 10 (Classification Theorem)**.** *Given that all finite simple groups are known, if G is a primitive Jordan group, then G is one of the groups in the following list.*

Affine groups: *Let q be a prime power, F the field with q elements, and $d \geq 2$. The group G with $\mathrm{ASL}(d, q) \leq G \leq \mathrm{A\Gamma L}(d, q)$ in its natural action on the d-dimensional affine F-space is a primitive Jordan group.*

Projective groups: *Let q be a prime power, F the field with q elements, and $d \geq 2$. The group G with $\mathrm{PSL}(d+1, q) \leq G \leq \mathrm{P\Gamma L}(d+1, q)$ in its natural action on the d-dimensional projective F-space $\mathrm{PG}(d, q)$ of order $(q^{d+1} - 1)/(q - 1)$ is a primitive Jordan group.*

Exceptional groups: *The alternating group A_7 occurs as a doubly transitive subgroup of $\mathrm{PGL}(4, 2)$. It is a Jordan group on the 15 points of $\mathrm{PG}(3, 2)$.*

This group has a transitive extension. If N is the translation group of the affine group $\mathrm{AGL}(4, 2)$, then $N \rtimes A_7$ is a triply transitive subgroup. It is a Jordan group on the 4-dimensional affine $\mathbb{F}_2$-space.

The Mathieu groups M_{22}, M_{23}, M_{24}, $\mathrm{Aut}(M_{22})$ are Jordan groups of degrees 22, 23, 24, 22, respectively. They act on their corresponding Steiner systems.

The next lemma is the basis for all further restrictions on G_f.

Lemma 11. *If $(p,r,s) \neq (2,1,0)$, then there exists a nontrivial Jordan complement Δ for G_f of size p^s.*

If $p \neq 2$ and $s > 0$, then the Jordan set corresponding to Δ is proper and G_f is a Jordan group. The same holds if $p = 2$ and $s > 1$.

If $(p,s) = (2,1)$, then G_f is triply transitive.

Proof. Rewrite the equation $f(X) - t = 0$ into

$$t = f(X) = X^{p^r - p^s} \cdot \Big(X^{p^s} + \sum_{i=0}^{s} a_i X^{p^s - p^i} \Big).$$

Since the right-hand factor is separable, the zero place $\mathbf{0} : \ t \mapsto 0$ of $K(t)$ decomposes in the root field $K(t,x) = K(x)$ in the following way:

$$\mathbf{0} = \mathfrak{P}_0^{p^r - p^s} \cdot \mathfrak{P}_1 \cdots \mathfrak{P}_{p^s} \qquad \text{with pairwise different places } \mathfrak{P}_i \text{ of } K(x). \tag{4}$$

Fix a place $\mathfrak{P}$ of L lying over $\mathbf{0}$ and denote the inertia group of the extension $\mathfrak{P}|\mathbf{0}$ with $I_{\mathbf{0}}$. By van der Waerden [25] $I_{\mathbf{0}}$ fixes a set $\Delta \subseteq \{x_1, \ldots, x_n\}$ of p^s elements pointwise and permutes the remaining $p^r - p^s$ elements transitively. Call this orbit Γ. As $(p,r,s) \neq (2,1,0)$, the length of Γ is at least 2. The pointwise stabilizer of Δ in G_f contains $I_{\mathbf{0}}$ and is a fortiori transitive on Γ. This proves that Δ is a nontrivial Jordan complement for G_f.

Suppose $p \neq 2$ and $s > 0$. As by Lemma 4, G_f is a subgroup of $\mathrm{AGL}(r,p)$ with $r \geq 2$, it is not triply transitive; cf. Huppert [19, II 2.3 (b)]. As $p^s = |\Delta| > 2$, the claim follows.

Now assume $p = 2$ and $s > 1$. Then $r > 2$, and G_f is not 4-transitive by Huppert [19, II 2.3 (c)]. Since $|\Delta| > 3$, G_f is a Jordan group in this case, too.

If $(p,s) = (2,1)$, then $|\Delta| = 2$, and since G_f is doubly transitive by Lemma 6, the 3-transitivity of G_f follows. □

Remark 12. In general, the above lemma becomes wrong for $s = 0$. In this case we have $G_f = \mathrm{AGL}(1, p^r)$. By the Classification Theorem this group is not a Jordan group; neither is it triply transitive (except for $\mathrm{AGL}(1,3) = S_3$).

Remark 13. We can give a different proof of the double transitivity of G_f based on Lemma 11.

In case $(p,r,s) = (2,1,0)$ the group G_f is a transitive group acting on $n = 2$ elements. Hence, G_f equals the doubly transitive group $\mathrm{AGL}(1,2) = S_2$.

In the remaining cases, G_f is a group possessing a nontrivial Jordan complement. A famous theorem of Jordan states that under these conditions, primitivity and double transitivity actually describe the same property of the group; cf. [22, Thm. J1]. Therefore we only have to show primitivity in the sequel.

It is a direct consequence of Lüroth's theorem on subfields of rational function fields that G_f is primitive if and only if f is functionally indecomposable; i.e., f cannot be written as a composition $f = g \circ h$ with nonlinear polynomials $g, h \in K[X]$. A proof of this result can be found for instance in [21, 6.10].

Suppose there exist nonlinear polynomials $g, h \in K[X]$ such that $f = g \circ h$. Note that any decomposition of f induces a set of "similar" decompositions via linear shifts in X; i.e., if $f = g \circ h$, then also $f = \tilde{g} \circ \tilde{h}$, where $\tilde{h}(X) := h(X) - c$, $\tilde{g}(X) := g(X + c)$, and $c \in K$. Hence, we are free to assume $h(0) = 0$ in our

original decomposition. Since $f(0) = 0$, this implies $g(0) = 0$, too. Observe that the derivative of f fulfills

$$g'\big(h(X)\big) \cdot h'(X) = f'(X) = -a_0 X^{p^r-2}.$$

First suppose $g'(0) \neq 0$. Then $X \nmid g' \circ h$ and it follows that $X^{p^r-2} \mid h'$. Hence, $\deg h \geq p^r - 1$. But then $p^r = \deg f = \deg g \cdot \deg h \geq 2(p^r - 1)$, a contradiction.

Thus, $g'(0) = 0$. As $0 \in K$ is the only zero of f', the polynomial h fulfills $h(\xi) \neq 0$ for all $\xi \in K^\times$; hence, $h(X) = h_0 X^\alpha$. But then every summand of f has degree divisible by α. Since p^r and $p^r - 1$ are relatively prime, this condition enforces $\alpha = 1$ and contradicts the nonlinearity of h.

2.3. **Determination of G_f.** We use the classification of primitive Jordan groups to obtain the following preliminary statement about G_f.

Lemma 14. *G_f is an affine group. Moreover, there exists a divisor d of r such that either*

$$\mathrm{ASL}(r/d, p^d) \leq G_f \leq \mathrm{A\Gamma L}(r/d, p^d) \qquad \text{or} \qquad \mathbb{F}_2^4 \rtimes A_7 \cong G_f \leq \mathrm{AGL}(4, 2).$$

In the latter case G_f belongs to the class of exceptional groups of Theorem 10 *and is unique in* $\mathrm{AGL}(4, 2)$ *up to conjugacy.*

Proof. The claim follows from Corollary 8 if $s = 0$. Hence, we assume $s > 0$ from now on.

Denote by

$$S := \mathrm{soc}(G_f) = \big\langle H \mid H \text{ is a minimal normal subgroup of } G_f \big\rangle$$

the socle of G_f. As G_f is doubly transitive, S is either elementary abelian or a nonabelian simple group; cf. Cameron [6, 5.2]. We prove that the latter case does not occur.

The proof proceeds in three steps. First, we assume that S is nonabelian simple. We show that this implies that S is a projective special linear group. Next, we discuss this case in detail and prove that it leads to a contradiction. Thus, we end up in the elementary abelian case, which we discuss last.

Step 1. Suppose S is nonabelian simple.

If $p \neq 2$, or $p = 2$ and $s > 1$, then G_f is a Jordan group by Lemma 11, and the Classification Theorem shows that either G_f is a projective or an exceptional group. Assume G_f is exceptional. Then $G_f = M_{23}$ because the degree of G_f is a prime power. But $M_{23} = G_f \not\leq \mathrm{AGL}(1, 23)$, a contradiction. Hence, G_f is projective.

Now assume $(p, s) = (2, 1)$. Then, again by Lemma 11, G_f is a triply transitive group of degree 2^r. The classification of nonaffine doubly transitive groups (a nice list is given in Cameron [6]) shows that S is either a projective group or the alternating group A_{2^r} with $2^r \geq 5$. In the latter case $S \leq \mathrm{AGL}(r, p)$ is at least $2^3 - 2 = 6$-transitive, which contradicts Huppert [19, II 2.3 (d)]. Hence, G_f is projective, too.

Step 2. Suppose S is nonabelian simple with $S = \mathrm{PSL}(d, q)$.

We first show that this implies that $(p^r, d, q) = (8, 2, 7)$.

S is a subgroup of the affine group $\mathrm{AGL}(r, p)$. Denote the translation subgroup of $\mathrm{AGL}(r, p)$ by N. The simplicity of S gives $S \cap N = 1$. Thus, S embeds into a

point stabilizer of $\mathrm{AGL}(r,p)$ which is $\mathrm{GL}(r,p)$. Since the degrees of S and G_f are equal, the integers p^r, d, and q fulfill the equation

$$p^r = \frac{q^d - 1}{q - 1}. \tag{5}$$

First assume $d > 2$, or $d = 2$ and q even. Then $q^d - 1$ has a primitive prime factor according to Zsigmondy's theorem (a nice proof of the theorem can be found in [23]). By (5) this prime factor is uniquely given by p; in particular, $\frac{q^d-1}{q-1}$ and $q-1$ are relatively prime. The group $\mathrm{PGL}(d,q)$ contains an element of order p^r by Huppert [19, II 7.3 (c)]. Since the order of the factor $\mathrm{PGL}(d,q)/S$ divides $q-1$, it is relatively prime to p^r. Hence, S also contains an element of order p^r. The same holds for $\mathrm{GL}(r,p)$ as S embeds into this group. But this contradicts the structure theorem of p-Sylow subgroups in $\mathrm{GL}(r,p)$; cf. Huppert [19, III 16.5 (a)].

Next assume $d = 2$ with odd q. Then $p = 2$ is even. Again, $\mathrm{PGL}(2,q)$ contains an element of order 2^r. Since $\mathrm{PGL}(2,q)/S$ is cyclic of order 2, there exists an element of order 2^{r-1} in S and, thus, in $\mathrm{GL}(r,2)$. As above, we use the structure theorem and obtain $r \in \{2,3\}$. The simplicity of S eventually yields $(p^r,d,q) = (8,2,7)$.

Now we show that $(p^r,d,q) = (8,2,7)$ is contradictory.

As $S = \mathrm{PSL}(2,7)$ is self-normalizing in $\mathrm{AGL}(3,2)$, it follows that $S = G_f$. An explicit computation shows that G_f does not have Jordan complements of size 2 or 4. This contradicts Lemma 11.

Step 3. Suppose S is elementary abelian.

Then S is regular by Huppert [19, II 1.5] and G_f is an affine group.

In the case of G_f being a Jordan group, the claim follows from the Classification Theorem. Otherwise G is a triply transitive affine group in even characteristic. The assertion then follows from the classification of these groups in Cameron/Kantor [7, Cor. 8.2]. □

Remark 15. Note that the classification statement of Cameron/Kantor [7, Cor. 8.2] we used above is correct although the given proof may not be; cf. [8]. A different proof of this result arises from the observation that for $n > 2$ a point stabilizer of a triply transitive affine subgroup of $\mathrm{AGL}(n,2)$ is not an affine group itself. One can then employ the classification of doubly transitive nonaffine groups. Alternatively, one could use Hering's classification of transitive linear groups.

By the above lemma, G_f is affine and, hence, contains the subgroup of translations. The next lemma investigates the fixed field of this group.

Lemma 16. *Denote by N the translation subgroup of G_f and set $E := \mathrm{Fix}(N)$, the fixed field of N in the extension $L|K(t)$. Fix a place $\mathfrak{P}$ of E lying over the infinite place ∞ of $K(t)$ and denote the inertia group of $\mathfrak{P}|\infty$ by F_∞. Then F_∞ is cyclic of order $n-1$.*

In particular, a point stabilizer of G_f contains a cyclic subgroup of order $n-1$.

Proof. Denote the set of roots of (2) with $R := \{z_1,\dots,z_n\}$ and fix an element $z \in R$. By Remark 5, R is an affine space. Its underlying vector space is given by

$$V := R - z = \{z_1 - z, \dots, z_n - z\}.$$

Remark 5 shows that N equals the kernel of the action of G on V. Therefore the fixed field E of N is given by $E = K(t,V)$.

V is the set of zeros of $Z^{p^r} - \sum_{i=0}^{s} \frac{1}{t} a_i Z^{p^i}$. Hence, all elements of $V^\times := V \setminus \{0\}$ are annihilated by $Z^{p^r-1} - \sum_{i=0}^{s} \frac{1}{t} a_i Z^{p^i-1}$. The identity $Z = X^{-1}$ shows that

$$Z^{p^r-1} - \sum_{i=0}^{s} \frac{1}{t} a_i Z^{p^i-1} = 0 \iff \sum_{i=0}^{s} a_i X^{p^r-p^i} - t = 0.$$

The latter polynomial is irreducible since its negative is a monic polynomial of degree 1 in t. We obtain an alternative description of E: The field E is the splitting field of the polynomial

$$F(X) := X^{p^r-1} + \sum_{i=1}^{s} \frac{a_i}{a_0} X^{p^r-p^i} - \frac{1}{a_0} t.$$

Fix an element $v \in V^\times$. Then F is the minimal polynomial of v. The structure of F shows that ∞ is tamely and totally ramified in $K(v)|K(t)$. As E is the compositum of all fields $K(w)$ with $w \in V^\times$, Abhyankar's Lemma shows that the extension $\mathfrak{P}|\big(\mathfrak{P} \cap K(v)\big)$ is unramified. Hence, $|F_\infty| = n-1$, and general ramification theory yields that F_∞ is cyclic.

Since the Galois group of $E|K(t)$ is isomorphic to a point stabilizer of G_f, the remaining statement follows, too. □

We can now prove the full result about the groups G_f.

Proof of Theorem 1. The claim follows from Corollary 8 if $s = 0$. Hence, assume $s > 0$.

Denote the stabilizer of x in G_f with H. By the above lemma there exists an element σ of order $n-1$ in H. This excludes the case $G_f \cong N \rtimes A_7$ from Lemma 14. Hence, there exists a divisor d of r such that

$$\mathrm{SL}(r/d, p^d) \le H \le \Gamma\mathrm{L}(r/d, p^d).$$

H (considered as a subgroup of the automorphism group of $L|K(t)$) fixes every element of $\mathbb{F}_{p^d} \le K$; therefore Remark 5 shows that H acts on the roots of (2) as a proper linear group. Thus, $H \le \mathrm{GL}(r/d, p^d)$. Huppert [19, II 7.3 (b)] shows that $|\langle\sigma\rangle \cap \mathrm{SL}(r/d, p^d)| = \frac{n-1}{p^d-1}$; we obtain

$$\begin{aligned} \big|H/\mathrm{SL}(r/d, p^d)\big| &\ge \big|\langle\sigma\rangle \mathrm{SL}(r/d, p^d)/\mathrm{SL}(r/d, p^d)\big| \\ &= \big|\langle\sigma\rangle/\big(\langle\sigma\rangle \cap \mathrm{SL}(r/d, p^d)\big)\big| = p^d - 1. \end{aligned}$$

Since $|\mathrm{GL}(r/d, p^d)/\mathrm{SL}(r/d, p^d)| = p^d - 1$, it follows that $H = \mathrm{GL}(r/d, p^d)$ and $G_f = \mathrm{AGL}(r/d, p^d)$.

Finally, we prove that the divisor d equals the integer e defined in the theorem. By Lemma 4, $G_f \le \mathrm{AGL}(r/e, p^e)$; hence, $e \mid d$. But by Remark 5, $\mathbb{F}_{p^d}$ is a subfield of $\mathbb{F}_{p^e}$; hence, $d \mid e$.

We obtain $G_f = \mathrm{AGL}(r/e, p^e)$. □

2.4. **Determination of A_f.** In this section we consider the behavior of the extension $\lambda|k(t)$ under constant field extensions. Stichtenoth [24, Sec. 3.6] is a good reference. We also employ the Translation Theorem of elementary Galois theory. Its statement and proof are given in Lang [20, VI Thm. 1.12].

First, we fix some notation. If A and B are subfields of a common field, then we write AB for the compositum of A and B, i.e., the field that is generated by A and B.

Throughout this section κ denotes an algebraic extension of k. We define $\overline{k}$ to be the exact constant field of λ, i.e., the field that contains every element of λ that is algebraic over $\mathbb{F}_p$. Clearly, $\overline{k} = \lambda \cap K$. It is a finite field by Stichtenoth [24, 1.1.16].

$M_f(\kappa)$ denotes the group

$$M_f(\kappa) := \mathrm{Gal}\big(f(X) - t|\kappa(t)\big) \cong \mathrm{Gal}\big(\kappa\lambda|\kappa(t)\big).$$

$M_f(\kappa)$ is closely connected to the monodromy groups of f; it is essentially the arithmetic monodromy group of f over an artificially enlarged base field. Obviously,

$$M_f(k) = A_f \qquad \text{and} \qquad M_f(K) = G_f.$$

$M_f(\kappa)$ always is a subgroup of A_f. This can be proved by restricting an element $g \in M_f(\kappa)$ which is an automorphism of $\kappa\lambda$ to λ. This restriction then is an element of A_f. A strict proof arises from the Translation Theorem. Moreover, this theorem shows that the fixed field of $M_f(\kappa)$ in $\lambda|k(t)$ is $\lambda \cap \kappa(t) = (\lambda \cap \kappa)(t)$. This yields our first result.

Lemma 17. (1) *$G_f \trianglelefteq M_f(\kappa) \trianglelefteq A_f$. The factor A_f/G_f is isomorphic to the Galois group of $\overline{k}|k$.*

(2) *$M_f(\kappa) = G_f \iff \overline{k} \le \kappa$.*

Proof. (1) The statement $M_f(\kappa) \le A_f$ follows from the preliminary remark. An analogous argument shows that $G_f \le M_f(\kappa)$. The fixed field of G_f in $\lambda|k(t)$ equals

$$\lambda \cap K(t) = (\lambda \cap K)(t) = \overline{k}(t).$$

The extension $\overline{k}(t)|k(t)$ is Galois, and its Galois group is isomorphic to the Galois group of $\overline{k}|k$. This proves $G_f \trianglelefteq A_f$ with A_f/G_f being cyclic. Hence, the claim follows.

(2) We use the theory of constant field extensions: If $\overline{k} \le \kappa$, then κ is the exact constant field of $\kappa\lambda = \kappa(x_1, \ldots, x_n)$ (by [24, 3.6.1 (a)]) and $\kappa(t)$. It follows from [24, 3.6.7] that $[L : K(t)] = [\kappa\lambda : \kappa(t)]$. Part (1) of this lemma gives $M_f(\kappa) = G_f$.

If $\overline{k} \not\le \kappa$, then κ is a proper subfield of the exact constant field of $\kappa\lambda$. By [24, 3.6.6] it follows that $[L : K(t)] < [\kappa\lambda : \kappa(t)]$. □

Lemma 18. *The field $\overline{k}$ equals the compositum of k and $\mathbb{F}_{p^e}$, $\overline{k} = k\mathbb{F}_{p^e}$.*

Proof. Since λ is defined over k, we have $k \le \overline{k}$. Moreover, λ is generated by an affine $\mathbb{F}_{p^e}$-vector space. Hence, $\mathbb{F}_{p^e} \le \overline{k}$. This shows that the compositum $k\mathbb{F}_{p^e}$ is also a subfield of the exact constant field of λ.

Set $\kappa := k\mathbb{F}_{p^e}$. Then $\mathbb{F}_{p^e}$ is a subfield of κ and Lemma 4 shows that $M_f(\kappa) \le \mathrm{AGL}(r/e, p^e) = G_f$. The above lemma gives $M_f(\kappa) = G_f$ and $\overline{k} \le \kappa$. This is the claim. □

We now state the main theorem of this section.

Theorem 19. *The group $M_f(\kappa)$ fulfills*

$$G_f \trianglelefteq M_f(\kappa) \trianglelefteq \mathrm{A\Gamma L}(r/e, p^e) \qquad \textit{and} \qquad [M_f(\kappa) : G_f] = [\kappa\mathbb{F}_{p^e} : \kappa].$$

These conditions uniquely determine $M_f(\kappa)$.

Proof. In view of the above lemmas there are only a few things left to prove.

First, we have to show that $[M_f(\kappa) : G_f] = [\kappa\mathbb{F}_{p^e} : \kappa]$. The fixed field of G_f in $\kappa\lambda|\kappa(t)$ is

$$(\kappa\lambda \cap K)(t) = \kappa\overline{k}(t) = \kappa\mathbb{F}_{p^e}(t).$$

Hence,

$$M_f(\kappa)/G_f \cong \mathrm{Gal}\big(\kappa\mathbb{F}_{p^e}(t)|\kappa(t)\big) \cong \mathrm{Gal}(\kappa\mathbb{F}_{p^e}|\kappa) \cong \mathrm{Gal}\big(\mathbb{F}_{p^e}|(\mathbb{F}_{p^e} \cap \kappa)\big).$$

In particular, $[M_f(\kappa) : G_f] \mid e$.

Next, we have to prove that the above conditions uniquely determine $M_f(\kappa)$. As the normalizer of $\mathrm{GL}(r/e, p^e)$ in $\mathrm{GL}(r, p)$ is $\Gamma\mathrm{L}(r/e, p^e)$, it follows that $M_f(\kappa) \leq \mathrm{A}\Gamma\mathrm{L}(r/e, p^e)$. Since $\mathrm{GL}(r/e, p^e)$ is a normal subgroup of $\Gamma\mathrm{L}(r/e, p^e)$ with cyclic quotient, for every divisor d of $[\mathrm{A}\Gamma\mathrm{L}(r/e, p^e) : \mathrm{AGL}(r/e, p^e)] = e$ there exists a unique group U with

$$\mathrm{AGL}(r/e, p^e) \leq U \leq \mathrm{A}\Gamma\mathrm{L}(r/e, p^e) \qquad \text{and} \qquad [U : \mathrm{AGL}(r/e, p^e)] = d.$$

□

Corollary 2 on page 2969 is a direct consequence of this theorem; simply set $\kappa = k$.

3. Ramification in $L|K(t)$

In this section we describe the ramification structure of the extension $L|K(t)$. This requires some additional notation.

Given a place $\mathfrak{p}$ of $K(t)$ fix some place $\mathfrak{P}$ of L lying over $\mathfrak{p}$ and write $I_\mathfrak{p}$ for the inertia group of the extension $\mathfrak{P}|\mathfrak{p}$. The i-th ramification group (in the usual "lower numbering") is denoted by $I_\mathfrak{p}(i)$. By definition, $I_\mathfrak{p} = I_\mathfrak{p}(0)$. Since $\mathfrak{P}$ is freely chosen, the $I_\mathfrak{p}(i)$ are unique up to conjugacy in G_f. Let $o\big(I_\mathfrak{p}(i)\big)$ denote the number of orbits of $I_\mathfrak{p}(i)$ and define

$$\mathrm{ind}(\mathfrak{p}) := \sum_{i=0}^{\infty} \frac{n - o\big(I_\mathfrak{p}(i)\big)}{[I_\mathfrak{p} : I_\mathfrak{p}(i)]}.$$

Note that $\mathrm{ind}(\mathfrak{p})$ is a finite sum since $I_\mathfrak{p}(i) = 1$ if i is sufficiently large. It can be shown that

$$\mathrm{ind}(\mathfrak{p}) = \sum_{\mathfrak{q}|\mathfrak{p}} d(\mathfrak{q}|\mathfrak{p}), \tag{6}$$

where the sum runs over all places $\mathfrak{q}$ of $K(x)$ lying over $\mathfrak{p}$ and $d(\mathfrak{q}|\mathfrak{p})$ denotes the different exponent of $\mathfrak{q}$ over $\mathfrak{p}$. It follows in particular that $\mathrm{ind}(\mathfrak{p})$ is an integer not depending on the specific choice of $\mathfrak{P}$.

The Riemann-Hurwitz Genus Formula for the extension $K(x)|K(t)$ gives

$$-2 = -2[K(x) : K(t)] + \mathrm{degdiff}\big(K(x)|K(t)\big),$$

where the last summand is the degree of the different of $K(x)|K(t)$. Using (6) this can be rewritten into the useful

Genus-0 condition. $\quad 2n - 2 = \sum_\mathfrak{p} \mathrm{ind}(\mathfrak{p})$.

Now we can prove the main result of this section.

Theorem 20. *$K(t)$ contains exactly two branch points, the zero place $\mathbf{0} : t \mapsto 0$ and the infinite place $\infty : 1/t \mapsto 0$. Set N to be the translation subgroup of G_f. Then*

(1) *$I_\infty(0) \cong N \rtimes C_{n-1}$, $I_\infty(1) = N$, $I_\infty(2) = 1$, and $\mathrm{ind}(\infty) = n$.*

(2) $I_{\mathbf{0}}(0) \cong P \rtimes C_{p^{r-s}-1}$, $I_{\mathbf{0}}(1) = P$, $I_{\mathbf{0}}(2) = 1$, *and* $\operatorname{ind}(\mathbf{0}) = n-2$. *Here,* P *is an elementary abelian subgroup of* G_f *of order* p^s. $I_{\mathbf{0}}(0)$ *intersects* N *trivially.*

Proof. The statement about the branch points of $K(t)$ follows as $0 \in K$ is the only zero of f'.

Let E denote the fixed field of N in the extension $L|K(t)$. We know from Lemma 16 that ∞ ramifies with index $n-1$ in $E|K(t)$. Since ∞ is totally ramified in $K(x)|K(t)$ with index n, every place of E lying over ∞ ramifies totally in $L|E$. As $\operatorname{Gal}(L|E) = N$, we obtain $I_\infty \cong N \rtimes C_{n-1}$. Because I_∞ and $I_\infty(1)$ are transitive,

$$\operatorname{ind}(\infty) \geq (n-1) + \frac{n-1}{n-1} = n.$$

The genus-0 condition implies that $\operatorname{ind}(\mathbf{0}) \leq n-2$.

We know from the decomposition (4) that $I_{\mathbf{0}}$ stabilizes p^s points and is transitive on the remaining $p^r - p^s = p^s(p^{r-s}-1)$ points. Elementary group theory shows that this $I_{\mathbf{0}}$-orbit decomposes into $p^{r-s}-1$ different $I_{\mathbf{0}}(1)$-orbits, each of length p^s. We obtain

$$p^{r-s}-1 \mid [I_{\mathbf{0}} : I_{\mathbf{0}}(1)], \quad o(I_{\mathbf{0}}) = p^s + 1, \quad \text{and} \quad o\big(I_{\mathbf{0}}(1)\big) = p^s + p^{r-s} - 1. \tag{7}$$

As N is regular, the intersection of $I_{\mathbf{0}}$ with N is trivial. Thus, we can consider $I_{\mathbf{0}}$ as a subgroup of $\mathrm{GL}(r,p)$. Let $c \in I_{\mathbf{0}}$ be an element that generates a cyclic complement of $I_{\mathbf{0}}(1)$ and denote the matrix induced by c with $A \in \mathrm{GL}(r,p)$. Since A is p-regular, it is diagonalizable over K,

$$A \sim \operatorname{diag}(\underbrace{1,\dots,1}_{s \text{ times}}, \lambda_1, \dots, \lambda_{r-s}) \qquad \text{with the } \lambda_i \in K^\times.$$

This proves that A actually can be considered as an element of $\mathrm{GL}(r-s,p)$. The maximal order of an element in this group is $p^{r-s}-1$ by [10, Cor. 2]. Together with (7) the order of A and, thus, of c is $p^{r-s}-1$. We obtain

$$\operatorname{ind}(\mathbf{0}) \geq n - (p^s - 1) + \frac{n - (p^s + p^{r-s} - 1)}{p^{r-s}-1} = n - 2.$$

It follows that $I_\infty(2) = 1$ and $I_{\mathbf{0}}(2) = 1$, which implies that $I_{\mathbf{0}}(1)$ is elementary abelian. The statement about the order of $I_{\mathbf{0}}(1)$ follows as there exists an $I_{\mathbf{0}}(1)$-orbit of length p^s. □

Acknowledgement

The author is very indebted to the referee for introducing him to Elkies's paper. The author further appreciates the detailed report that helped him to improve the paper significantly.

References

[1] S. S. Abhyankar, *Fundamental group of the affine line in positive characteristic*, in *Geometry and analysis*, Oxford Univ. Press, Oxford, 1995, pp. 1–26. MR1351500 (97b:14034)

[2] S. S. Abhyankar, *Galois theory on the line in nonzero characteristic*, Bull. AMS, **27**, No. 1 (1992), pp. 68–133. MR1118002 (94a:12004)

[3] S. S. Abhyankar, *Mathieu group coverings and linear group coverings*, in *Recent developments in the inverse Galois problem*, Contemp. Math., **186**, Amer. Math. Soc., 1995, pp. 17–23. MR1352279 (97e:14038)

[4] S. S. Abhyankar, *Nice equations for nice groups*, Israel J. Math., **88** (1994), pp. 1–23. MR1303488 (96f:12003)
[5] S. S. Abhyankar, *Resolution of singularities and modular Galois theory*, Bull. AMS, **38**, No. 2 (2001), pp. 131–169. MR1816069 (2002a:14013)
[6] P. J. Cameron, *Finite permutation groups and finite simple groups*, Bull. Lond. Math. Soc., **13** (1981), pp. 1–22. MR599634 (83m:20008)
[7] P. J. Cameron, W. M. Kantor, 2-*transitive and antiflag transitive collineation groups of finite projective spaces*, J. Algebra, **60** (1979), pp. 384–422. MR549937 (81c:20032)
[8] P. J. Cameron, W. M. Kantor, *Antiflag transitive collineation groups revisited*, http://www.maths.qmul.ac.uk/∼pjc/odds/antiflag.pdf, unpublished and incomplete draft, February 2002.
[9] J. Conway, J. McKay, A. Trojan, *Galois groups over function fields of positive characteristic*, Proc. Amer. Math. Soc., **132**, No. 8 (2010), pp. 1205–1212. MR2578514
[10] M. R. Darafsheh, *Order of elements in the groups related to the general linear group*, Finite Fields Appl., **11**, No. 4 (2005), pp. 738–747. MR2181417 (2006g:20085)
[11] L. E. Dickson, *A fundamental system of invariants of the general modular linear group with a solution of the form problem*, Trans. Amer. Math. Soc., **12** (1911), pp. 75–98. MR1500882
[12] L. E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Ann. of Math., **11** (1896), pp. 65–120, 161–183. MR1502214; MR1502221
[13] N. Elkies, *Linearized algebra and finite groups of Lie type. I: Linear and symplectic groups*, in *Applications of curves over finite fields*, AMS Contemp. Math., **245**, 1999, pp. 77–107. MR1732230 (2001a:20082)
[14] M. D. Fried, R. M. Guralnick, J. Saxl, *Schur covers and Carlitz's conjecture*, Israel J. Math., **82** (1993), pp. 157–225. MR1239049 (94j:12007)
[15] R. M. Guralnick, P. Müller, *Exceptional polynomials of affine type*, J. Algebra, **194**, No. 2 (1997), pp. 429–454. MR1467161 (98i:12006)
[16] R. M. Guralnick, J. Rosenberg, M. E. Zieve, *A new family of exceptional polynomials in characteristic two*, Ann. of Math. (2), **172**, No. 2 (2010), pp. 1361–1390. MR2680493
[17] R. M. Guralnick, J. Saxl, *Monodromy groups of polynomials*, in *Groups of Lie type and their geometries*, Cambridge Univ. Press, Cambridge, 1995, pp. 125–150. MR1320519 (96b:20003)
[18] R. M. Guralnick, M. E. Zieve, *Polynomials with* PSL(2) *monodromy*, Ann. of Math. (2), **172**, No. 2 (2010), pp. 1315–1359. MR2680492
[19] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin-Heidelberg-New York, 1967. MR0224703 (37:302)
[20] S. Lang, *Algebra*, Springer-Verlag, New York, 2002. MR1878556 (2003e:00003)
[21] R. Lidl, G. L. Mullen, G. Turnwald, *Dickson polynomials*, Longman, Harlow, 1993. MR1237403 (94i:11097)
[22] P. M. Neumann, *Some primitive permutation groups*, Proc. Lond. Math. Soc., III. Ser., **50** (1985), pp. 265–281. MR772713 (86d:20005)
[23] M. Roitman, *On Zsigmondy primes*, Proc. AMS, **125**, No. 7 (1997), pp. 1913–1919. MR1402885 (97i:11005)
[24] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin-Heidelberg, 2009. MR2464941 (2010d:14034)
[25] B. L. van der Waerden, *Die Zerlegungs-und Trägheitsgruppe als Permutationsgruppen*, Math. Ann., **111** (1935), pp. 731–733. MR1513024

Institut für Mathematik, Universität Würzburg, Hubland Nord, 97074 Würzburg, Germany

E-mail address: fmoeller@mathematik.uni-wuerzburg.de