Exceptional polynomials and monodromy groups in positive characteristic

Dissertation zur Erlangung des
naturwissenschaftlichen Doktorgrades
der Julius-Maximilians-Universität Würzburg

vorgelegt von

Florian Möller

Institut für Mathematik der Universität Würzburg

Würzburg, März 2009

Danksagung
Ich möchte mich herzlich bei Professor Peter Müller für seine Unterstützung in allen Phasen meiner Promotion bedanken.

Als Betreuer meiner Dissertation lastete auf Herrn Müller die Aufgabe, mir einerseits zu zeigen wie schön freie und eigenständige Forschungstätigkeit sein kann, mir andererseits aber auch Probleme vorzulegen, die mich in meiner Promotion voranbrachten. Dies ist Herrn Müller ausgezeichnet gelungen.

Besonders erwähnen möchte ich noch, dass Professor Müller mehrere komplizierte mathematische Situationen, mit denen ich mich konfrontiert sah, stark vereinfachte. Erst durch seine Hilfe sind mir einige Beweise gelungen oder in ihre jetzige lesbare(re) Form gebracht worden.

Weiterhin danke ich Professor Theo Grundhöfer, der für meine Fragen immer ein offenes Ohr hatte und mir an mancher Stelle mit wertvollen Literaturhinweisen half. Weiter habe ich ihm eine zusätzliche Anstellung am Lehrstuhl für Mathematik III zu verdanken. Ohne die Unterstützung von Herrn Grundhöfer wäre mir meine Promotion erheblich schwerer gefallen.

Mein besonderer Dank gilt meiner Familie, die mich in meinem Vorhaben stets bestärkte und mir einen Ausgleich zur mathematischen Beschäftigung bot.

Contents

1. Introduction

In 1923 Schur [43] requested a description of all polynomials $f \in \mathbb{Z}[X]$ that induce a bijection on $\mathbb{Z}/p\mathbb{Z}$ for infinitely many primes p. He proved that if f is of prime degree, then it is – up to linear changes over the algebraic closure of $\mathbb{Q}$ – either a cyclic polynomial X^q or a Chebychev polynomial $T_q(X)$ (defined implicitly by $T_q(X + 1/X) = X^q + \frac{1}{X^q}$). He conjectured that in the general case f is a composition of such polynomials. This was proved by Fried [13] in 1970.

Schur's original question has been generalized in several ways: Turnwald [48] discusses the problem over integral domains, Guralnick, Müller, and Saxl [19] characterize rational functions r over number fields K so that r induces a bijection on the residue field $K_\mathfrak{p}$ for infinitely many places $\mathfrak{p} \in \mathcal{P}(K)$.

There is a different generalization of interest to us: we assume the base field to be of positive characteristic and search for *exceptional polynomials*, i.e. polynomials that fulfill the following

Definition (Exceptionality) *Assume k is a finite field. Let $f \in k[X]$ be a polynomial with coefficients in k. If K is an extension field of k, then f is called a* permutation polynomial over K *if f induces a bijection on K.*

$f \in k[X]$ is called exceptional over k *if it is a permutation polynomial over infinitely many finite extensions of k.*

The classification of permutation polynomials has a long tradition and goes back to Hermite [24] who noticed that any function $k \to k$ with k a finite field can be represented by a polynomial. A broad survey of permutation polynomials can be found in Lidl and Niederreiter [35].

An important step forward concerning the theory of exceptional polynomials was the reformulation of the original definition in terms of Galois theory and covering theory in positive characteristic. A first consequence was the proof of the following

Exceptionality Lemma (cf. [14]) *Let k be a finite field of characteristic p and t a transcendental over k. Let $f \in k[X]$ be a polynomial. Denote the set of zeros of $f(X) - t$ by Z. Fix a zero $x \in Z$. Then:*

(1) Suppose f is not a p-th power in $k[X]$. Then f is exceptional over k if and only if the x-stabilizer of the arithmetic monodromy group of f fixes no orbit of the x-stabilizer of the geometric monodromy group of f on $Z \setminus \{x\}$. (A definition of monodromy groups is given on page 7.)

(2) Suppose f is a composition $f = f_1 \circ f_2$ with $f_1, f_2 \in k[X]$. Then f is exceptional over k if and only if both f_1 and f_2 are exceptional over k.

In 1993 Fried, Guralnick, and Saxl [14] realized that this result reduces the classification of exceptional polynomials essentially to a question about primitive groups. They used the

Theorem of O'Nan-Scott and the classification of finite simple groups to obtain

Theorem *Let k be a finite field of characteristic p. Assume $f \in k[X]$ is an indecomposable and exceptional polynomial of degree n. Denote the geometric monodromy group of f by G. Then one of the following holds:*

(1) n is an odd prime different from the characteristic p. The group G is cyclic or dihedral of degree n.

(2) $n = p^r$ and $G = \mathbb{F}_p^r \rtimes H$ is an affine group with $H \leq \mathrm{GL}(r, p)$ acting naturally on $\mathbb{F}_p^r$.

(3) $p \in \{2, 3\}$, there exists an odd integer $a \geq 3$ with $\mathrm{PSL}(2, p^a) \leq G \leq \mathrm{P\Gamma L}(2, p^a)$, and $n = \frac{1}{2}p^a(p^a - 1)$.

This classification solved in particular Carlitz's conjecture (1966): if p is an odd prime, then the degree of f is odd.

The three cases of the above theorem are understood with different degrees of completeness:

Case (1) is classical; up to linear changes only cyclic or Chebychev polynomials of degree n arise here, cf. [38, Appendix]. This is the equivalent to Schur's original conjecture.

The first examples in case (3) were given by Müller [39] for $p = 2$ and $a = 3$. Cohen and Matthews [10] generalized these to an infinite series in even characteristic. Lenstra and Zieve [34] found a similar series for $p = 3$. Recently, Guralnick, Zieve, and Rosenberg [22, 20] gave a complete discussion of case (3). The polynomials occurring fulfill either $G = \mathrm{PSL}(2, p^a)$ or $G = \mathrm{PGL}(2, p^a)$.

Case (2) is still open. The main problem is the difficulty to find restrictions for the group H; even the smallest possible case $\deg f = p$ requires some work, cf. [14, §5]. For some time the only examples of this case were additive polynomials and certain twists of them. In 1997 Guralnick and Müller [17] found a completely new series. Guralnick and Zieve [22] conjecture that there are no more polynomials belonging to this case. Up to the present every example fulfills the following

Observation. The fixed field E of the affine kernel of the geometric monodromy group of f is rational.

This observation motivates a classification of exceptional polynomials with primitive affine arithmetic monodromy group in terms of the genus g of E. This is done in chapter 4 up to $g = 2$. As a result, E is rational if and only if f belongs to a family of known polynomials. Moreover there are no exceptional polynomials with primitive affine arithmetic monodromy group for $g \in \{1, 2\}$. However, Theorem 4.25 shows that in case $g = 2$ the affine group $\mathrm{AGL}(2, 3)$ can be realized as the geometric monodromy group of a polynomial.

Chapter 5 generalizes this $\mathrm{AGL}(2, 3)$-polynomial; Theorem 5.7 eventually shows that every affine group $\mathrm{AGL}(r, p^e)$ can be realized as the geometric monodromy group of a polynomial of degree p^{re}. Unfortunately, these groups are 2-transitive on the r-dimensional $\mathbb{F}_{p^e}$-vector space; hence, this chapter does not offer exceptional polynomials at all.

The last three chapters continue the classification of [14, §5]. In chapter 6 polynomials of degree p^2 with primitive and affine arithmetic monodromy group are discussed. Theorem 6.1 shows that such a polynomial either belongs to a class of known affine polynomials or has a "big" geometric monodromy group. Chapter 7 classifies exceptional polynomials of degree

p^3 with primitive arithmetic monodromy group. Again only known exceptional polynomials are obtained. In chapter 8 we study exceptional polynomials of degree p^r where r is an odd prime. We assume additionally that the arithmetic monodromy group of f is 2-transitive. Theorem 8.1 shows that this chapter does not offer new classes of exceptional polynomials.

Notation and terminology

Mostly we use standard notation. In the following we give terminology about which an explanation may be needed.

For an integer $m \in \mathbb{N}$ we denote by C_m resp. D_m a cyclic group of order m resp. a dihedral group of order $2m$.

Assume that E is a function field. Then $g(E)$ is the genus of E. The set of places of E is denoted by $\mathcal{P}(E)$.

Page 23 gives a survey of frequently used definitions.

Part I.

General Results

2. Monodromy groups and affine polynomials

In this chapter we give the basic ideas how Galois theory and ramification theory can be used to translate properties of polynomials into properties of certain field extensions. Most of the following results are classical.

2.1. Polynomials and monodromy groups

Monodromy groups

Let k denote a finite field of characteristic p, and let $f \in k[X] \setminus k[X^p]$ be a polynomial of degree n which is not a p-th power in $k[X]$. Suppose t is transcendental over k. Denote by K an algebraic closure of k.

Set ℓ the splitting field of $f(X) - t|k(t)$. As $f(X) - t \in k(t)[X]$ is separable, the extension $\ell|k(t)$ is Galois. Its Galois group $A := \mathrm{Gal}\big(\ell|k(t)\big)$ is called the *arithmetic monodromy group of* f.

Let $k' \subseteq K$ denote an algebraic extension of k; obviously t is also transcendental over k'. The splitting field of $f(X) - t|k'(t)$ coincides with the compositum $k'\ell$. Set $M := \mathrm{Gal}\big(k'\ell|k'(t)\big)$.

The restriction of any Galois automorphism $\sigma \in M$ to ℓ yields a Galois automorphism $\sigma|_\ell \in A$. Since the mapping $M \to A$, $\sigma \mapsto \sigma|_\ell$ is injective, we obtain an embedding of M into A; hence, we can consider M to be a subgroup of A.

Denote the exact field of constants of ℓ by $\tilde{k}$. As $k(t) \subseteq \ell \cap k'(t) \subseteq k'(t)$, Lüroth shows that $\ell \cap k'(t) = (\tilde{k} \cap k')(t)$. Since the extension $(\tilde{k} \cap k')(t)|k(t)$ is Galois with Galois group $\mathrm{Gal}\big((\tilde{k} \cap k')(t)|k(t)\big) \cong \mathrm{Gal}(\tilde{k} \cap k'|k)$, it follows in particular that M is a normal subgroup of A with A/M being cyclic of order $[(\tilde{k} \cap k') : k]$.

All in all, we have proved the following fact: For every choice of k' the group M contains the group $G := \mathrm{Gal}\big(\ell|\tilde{k}(t)\big)$ as a normal subgroup with M/G being cyclic. G is called the *geometric monodromy group of* f.

Note that M is isomorphic to G in particular if $k' = K$. As we work later on mostly with function fields whose fields of constants are algebraically closed, this easy consequence becomes important.

Since $f(X) - t$ is absolutely irreducible, the groups G, M, and A act transitively on the zeros of $f(X) - t$.

Functional decomposability

Definition 2.1 *With the above notation we call* f functionally decomposable over k' *if there exist nonlinear polynomials* $g, h \in k'[X]$ *with* $f = g \circ h$.

If f *is not functionally decomposable over* k'*, we call* f functionally indecomposable over k'.

Let $x \in \ell$ be a zero of $f(X) - t$. We state some consequences of the functional indecomposability of f over k'.

Lemma 2.2 *The following statements are equivalent:*

(1) f is functionally indecomposable over k'.

(2) The monodromy group M acts primitively on the zeros of $f(X) - t$.

(3) There is no proper intermediate field between $k'(t)$ and $k'(x)$.

Proof. We show first that (2) and (3) are equivalent: By Galois duality the field $k'(x)$ is the fixed field of the stabilizer M_x of x. Both the primitivity of M and the non-existence of proper intermediate fields between $k'(t)$ and $k'(x)$ translate into the maximality of M_x in M.

Now, suppose $f = g \circ h$ to be decomposed over k'. Let $Z := x^M$ denote the set of zeros of $f(X) - t$. Set $Y := h(Z)$ and define $\Delta_y := h^{-1}(y) \subseteq Z$ for $y \in Y$. It is easy to verify that $\{\Delta_y \mid y \in Y\}$ is a system of imprimitivity for M.

Next, assume there is a proper intermediate field between $k'(t)$ and $k'(x)$. As this field is rational by Lüroth, there exists $y \in k'(x)$ with $k'(t) \subset k'(y) \subset k'(x)$. Since x resp. y is algebraic over $k'(y)$ resp. $k'(t)$, we can find nonlinear polynomials $g, h \in k'[X]$ such that $h(x) = y$ and $g(y) = t$. Thus, x is a zero of $(g \circ h)(X) - t$. Consider $f(X) - t$ and $(g \circ h)(X) - t$ as polynomials in t. Then both are irreducible and have the same leading coefficient. This gives the equality $f = g \circ h$. ■

2.2. Affine groups and affine polynomials

Definition 2.3 *Let G be a permutation group on a finite nonempty set Ω. We call G an* affine group *if G contains a normal subgroup N that fulfills the following two conditions:*

- *N is elementary abelian.*
- *N is regular on Ω, i.e. for every $(\omega_i, \omega_j) \in \Omega^2$ there exists exactly one $n \in N$ with $\omega_i^n = \omega_j$.*

Remark 2.4 The elementary abelian regular normal subgroup in the above definition is not unique in general. For instance, in the affine group $\mathrm{AGL}(2, 3)$ there exists an affine subgroup of order 27 containing three regular elementary abelian normal subgroups. ⋆

We state some basic facts about affine groups:

Lemma 2.5 *Let G be an affine group with $N \trianglelefteq G$ being elementary abelian and regular. Then:*

(1) A point stabilizer H of G is a complement of N, $G = N \rtimes H$.

(2) There exist a prime p and an integer r such that N is isomorphic to the r-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_p^r$.

(3) For $g \in G$ write $g = n_g h_g$ with $n_g \in N$ and $h_g \in H$. Then the action of G on Ω and of G on N defined by

$$n^g := h_g^{-1} n n_g h_g$$

are equivalent. In particular, G can be embedded into $\mathrm{AGL}(r,p)$, the group of all affine transformations of $\mathbb{F}_p^r$. H acts on N as a subgroup of $\mathrm{GL}(r,p)$.

Proof. (1) is a direct consequence of the transitivity of N, cf. [32, 3.1.4]. (2) is merely another formulation of N being elementary abelian. (3) follows from Huppert [25, II 2.2]. ■

The next definition connects affine groups with polynomials. It is central for our further considerations:

Definition 2.6 *With the above notation we call $f \in k[X] \setminus k[X^p]$ an* affine polynomial *if its geometric monodromy group is an affine group.*

A consequence of Dixon and Mortimer [12, Sec. 4.7] and Huppert [25, II 3.2] is

Definition/Lemma 2.7 *With the above notation G is primitive if and only if H acts irreducibly on N. If G is primitive, then N is the unique minimal normal subgroup of G. In this case we call N* the affine kernel of G.

Huppert [25, II 3.2] also gives the important

Proposition 2.8 (Galois) *Suppose G is a primitive affine group whose affine kernel has order p^r. Then a point stabilizer H of G does not contain a nontrivial normal p-subgroup.*

As a first application we classify all affine polynomials having a regular geometric monodromy group.

Proposition 2.9 *Let K be an algebraic closure of the field $\mathbb{F}_p$. Denote by t a transcendental element over K.*

(1) Assume f is a semi-additive polynomial of degree $n = p^r$, i.e.

$$f(X) = a + \sum_{i=0}^{r} a_i X^{p^i} \qquad \text{with } a, a_i \in K \text{ and } a_0 a_r \neq 0. \tag{2.1}$$

Then the geometric monodromy group G of f is elementary abelian and regular. In particular, f is affine.

(2) Suppose f is affine and the geometric monodromy group G of f is a p-group. Then f is semi-additive of the form (2.1).

Proof.

(1) Set $g := f - a$ the linearization of f. Denote the set of zeros of g by $Z := \{z_1, \ldots, z_n\} \subseteq K$ and fix a zero x of $f(X) - t$. Since $g(z_i + z_j) = g(z_i) + g(z_j) = 0$, Z is an $\mathbb{F}_p$-vector space.

The set of zeros of $f(X) - t$ is given by $x + Z$; in particular, $K(x)$ is the splitting field of $f(X) - t$ and $|G| = [K(x) : K(t)] = \deg f = |Z|$.

It follows together with the transitivity of G that for every $z \in Z$ there exists a unique $g_z \in G$ with $x^{g_z} = x + z$. The map $g_z \mapsto z$ gives an isomorphism between G and Z. This is the claim.

(2) Let x denote a zero of $f(X) - t$ and set $H := G_x$ the stabilizer of x. As G is a p-group, there exist subgroups G_i with $H = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_r = G$ and $G_{i+1}/G_i \cong C_p$. By Lemma 2.2 f is a composition of degree-p polynomials f_i with monodromy group $G_{f_i} \cong C_p$.

As G_{f_i} is abelian of order p, it is regular. Turnwald [49, Theorem 2.10] proves that there exist elements $a, b, c \in K$ such that $f_i = aX^p + bX + c$.

A simple induction shows that f being a composition of semi-additive polynomials is semi-additive, too.

■

Remark 2.10 Part (2) of the above proposition can also be proved by using Corollary 3.16.

We see that only the infinite place of $K(t)$ ramifies in the extension $K(x)|K(t)$; its ramification index equals $[K(x) : K(t)]$. The fixed field of G_i is rational by Lüroth; thus, $\mathrm{Fix}(G_i) = K(y_i)$ where y_i can be chosen such that the infinite place of $K(y_i)$ lies over the infinite place of $K(t)$.

Hence, the extensions $K(y_i)|K(y_{i+1})$ are of degree p and without finite ramification. This shows that y_i fulfills an equation of the form $ay_i^p + by_i + c = y_{i+1}$ with $a, b, c \in K$. Therefore the polynomials f_i are semi-additive of degree p. ⋆

2.3. Generic polynomials

In this section we give an alternative approach to affine polynomials. Our main idea is to find a primitive element z for the extension $k(x)|k(t)$ that has a simple minimal polynomial. Our main tool will be the following result of Kemper and Mattig [31]:

Proposition 2.11 *Let k be an algebraic extension of $\mathbb{F}_p$. Suppose $t_1, \ldots, t_{r+1}$ are algebraically independent transcendentals over k. Then*

$$g(t_1, \ldots, t_{r+1}; X) := X^{p^r} + \sum_{i=1}^{r} t_i X^{p^{r-i}} + t_{r+1} \in k(t_1, \ldots, t_{r+1})[X] \tag{2.2}$$

is generic for $\mathrm{AGL}(r, p)$ over k, i.e. g fulfills the following two conditions:

(1) The Galois group of g (as a polynomial in X) is $\mathrm{AGL}(r, p)$.

(2) If K is an infinite field containing k and $L|K$ is a Galois field extension with Galois group $H \leq \mathrm{AGL}(r, p)$, then there exist $\lambda_1, \ldots, \lambda_{r+1} \in K$ such that L is the splitting field of $g(\lambda_1, \ldots, \lambda_{r+1}; X)$ over K.

The next lemma describes how the Galois group of g acts on the zeros of g.

Lemma 2.12 *Let g be defined as in (2.2). Denote by L the splitting field and by $G \cong \mathrm{AGL}(r, p)$ the Galois group of g. Fix a zero z of g. Then the set Z of zeros of g is given by $Z = z + V$ where $V \subset L$ is an $\mathbb{F}_p$-vector space. Elements of the stabilizer G_z of z act on V as automorphisms of V. Elements of the affine kernel N of G stabilize V pointwise and act on Z by translation.*

Proof. V is given as the set of zeros of the linearization of g, i.e. as the set of zeros of $g(t_1, \ldots, t_r, 0; X)$. As this polynomial is additive, it follows at once that V is an $\mathbb{F}_p$-vector space.

We prove that G acts on V. Let $\sigma \in G$. As $z^\sigma \in Z$, there exists $v' \in V$ with $z^\sigma = z + v'$. This gives for any $v \in V$

$$(z+v)^\sigma = z + v' + v^\sigma \in Z \iff v' + v^\sigma \in V \iff v^\sigma \in V.$$

Since we have

$$(\lambda v_1)^\sigma = \lambda v_1^\sigma \quad \text{and} \quad (v_1 + v_2)^\sigma = v_1^\sigma + v_2^\sigma \qquad \text{for all } \lambda \in \mathbb{F}_p \text{ and } v_1, v_2 \in V,$$

G acts on V as a subgroup of $\mathrm{GL}(V) \cong \mathrm{GL}(r, p)$.

Set $\varphi : G \to \mathrm{GL}(V)$ the homomorphism that maps σ to the V-automorphism induced by σ. Then $\ker\varphi \cap G_z = 1$. Since $G_z \cong \mathrm{GL}(r, p)$, the mapping φ is an epimorphism with $|\ker\varphi| = p^r$. As $\mathrm{AGL}(r, p)$ is primitive and, hence, N is the unique normal subgroup of order p^r, $N = G_{(V)}$ is the pointwise stabilizer of V. The remaining assertions follow. ∎

Remark 2.13 Let t be a transcendental over k. Consider the polynomial

$$h(X) := g(a_1, \ldots, a_{r+1}; X) \in k(t)[X]. \tag{2.3}$$

h results from g by specializing elements $a_i \in k(t)$ for the transcendentals t_i. Suppose h is separable. Then the Galois group of h is a subgroup of the Galois group of g, cf. [33, VII §2]. Hence, our results from the above lemma can be transferred to describe the action of the Galois group of h. ⋆

Remark 2.14 Note that the Galois group of a polynomial of the form (2.3) is merely a *subgroup* of $\mathrm{AGL}(r, p)$; it need not be an affine group.

For instance, consider the polynomial

$$f(X) := X^8 + tX^2 + tX + t^2 \in \mathbb{F}_2(t)[X].$$

Huppert [25, p. 161] proves that $\mathrm{AGL}(3, 2)$ contains a transitive complement C of its affine kernel. We show that the Galois group $G := \mathrm{Gal}\big(f|\mathbb{F}_2(t)\big)$ of f is conjugate to C.

The action of G on the zeros $x_1, \ldots, x_8$ of f gives a natural embedding of G into S_8, the symmetric group on the set $\Omega := \{1, \ldots, 8\}$. Specialization of elements of $\mathbb{F}_8$ for the parameter t and factorization of the resulting polynomial over $\mathbb{F}_8$ show that G contains permutations of type $[1, 1, 3, 3]$, $[1, 7]$, and $[4, 4]$. A survey of the subgroups of $\mathrm{AGL}(3, 2)$ proves that this condition enforces either $G = \mathrm{AGL}(3, 2)$ or $G = C^g$ for some $g \in \mathrm{AGL}(3, 2)$.

Define $\Omega_4 := \{M \subseteq \Omega \mid |M| = 4\}$ to be the set of all subsets of Ω of cardinality 4. The definition $M^g := \{m^g \mid m \in M\}$ for $g \in G$ and $m \in M$ gives an action of G on Ω_4. If $G = \mathrm{AGL}(3, 2)$, then Ω_4 splits into two G-orbits; in the other case Ω_4 splits into three G-orbits.

The `MAPLE`-function `‘galois/rsetpol‘` allows us to compute the polynomial

$$f_4(X) := \prod_{M \in \Omega_4} \Big(X - \prod_{i \in M} x_i\Big) \in \mathbb{F}_2(t)[X]$$

whose zeros are the products of four pairwise different zeros of f. As f_4 has three irreducible factors over $\mathbb{F}_2(t)$, the claim follows. ⋆

Lemma 2.15 *Let p be a prime and $r \in \mathbb{N}$ be an integer. Let $E_1, E_2 \leq S_{p^r}$ be elementary abelian regular subgroups of S_{p^r}. Then there exists an element $g \in S_{p^r}$ such that $E_1^g = E_2$. In particular, all subgroups of S_{p^r} that are isomorphic to $\mathrm{AGL}(r,p)$ are conjugate.*

Proof. The action of E_1 resp. E_2 is equivalent to the natural action of E_1 on the coset space $E_1/1$ resp. of E_2 on the coset space $E_2/1$. As $E_1/1 \cong E_2/1$, these actions are equivalent, too. Hence, E_1 acts equivalently to E_2. This shows that E_1 and E_2 are conjugate.

Let $A, A' \leq S_{p^r}$ with $A \cong A' \cong \mathrm{AGL}(r,p)$. Denote the affine kernel of A with N and the affine kernel of A' with N'. Then $A = N_{S_{p^r}}(N)$ and $A' = N_{S_{p^r}}(N')$. As N and N' are conjugate, the same holds for A and A'. ∎

Now we prove the main result of this section.

Proposition 2.16 *Let k be an algebraic extension of $\mathbb{F}_p$, denote by t a transcendental over k, and let g be defined as in (2.2). Suppose $f \in k[X] \setminus k[X^p]$ is an affine polynomial of degree $n = p^r$. Fix a zero x of $f(X) - t$. Then there exists an element $z \in k(x)$ such that $k(t,z) = k(x)$ and the minimal polynomial μ of z over $k(t)$ is separable with*

$$\mu(X) = g\big(a_1, \ldots, a_{r+1}; X\big) \qquad \text{and} \qquad a_i \in k[t]. \tag{2.4}$$

Proof. Identify the zeros of $f(X)-t$ with integers $1, \ldots, n$ and set $G \leq S_n$ the permutation representation of $\mathrm{Gal}\big(f(X)-t|k(t)\big)$ on the zeros of $f(X)-t$. Let $N \leq G$ denote an elementary abelian regular normal subgroup of G. Then $A := N_{S_n}(N) \cong \mathrm{AGL}(r,p)$, the affine kernel of A coincides with N, and for every integer $i \in \{1, \ldots, n\}$ the stabilizer G_i of i fulfills

$$G_i = A_i \cap G.$$

The previous lemma shows that there exists an identification of the zeros of g with the integers $1, \ldots, n$ such that the action of the Galois group of g on the zeros of g is given by A. Due to Proposition 2.11 and the proof of Kemper [30, Theorem 1] we can find elements $a_i \in k(t)$ such that the polynomial $h(X) := g(a_1, \ldots, a_{r+1}; X)$ is separable, the splitting field of h over $k(t)$ coincides with the splitting field of $f(X) - t$ over $k(t)$, and the action of the Galois group of h on the zeros of h is equivalent to the action of G. Hence, we can find a zero $z' \in k(x)$ of h with $k(x) = k(t,z')$.

Set d the least common multiple of the denominators of the a_i. Define $z := dz'$. Then $k(t,z') = k(t,z)$ and a simple calculation shows that the minimal polynomial of dz over $k(t)$ is of the form (2.4). ∎

Example 2.17 Use the notation from the above proof.

Suppose f is a sublinearized polynomial of the form (4.2), cf. page 28. Then we can write

$$f(X) = X \cdot g^m(X) \qquad \text{with} \qquad g(X) = \sum_{\substack{m \mid p^i - 1 \\ p^i \mid n}} g_{\frac{p^i-1}{m}} X^{\frac{p^i-1}{m}} \in k[X].$$

Some calculation shows that we can set $z' := \big(g(x)\big)^{-1}$.

Suppose f fulfills the conclusion of Guralnick/Müller [17, Theorem 1.4]. Then we can set $z' := \frac{1}{f'(x)}$. This follows from [17, §3]. ⋆

3. Calculation of differents and the genus-0 condition

In this chapter we present several techniques to calculate the different exponent of an extension of a place. For the convenience of the reader we first state some classical results that will help us with the following computations.

3.1. The general case

The first theorem describes how the different exponent $d(\mathfrak{P}|\mathfrak{p})$ of an extension $\mathfrak{P}|\mathfrak{p}$ is related to its ramification groups. Since these groups are only defined in Galois extensions, we have to assume the field extension $E|F$ to be Galois. A proof of the theorem can be found in Stichtenoth [47, III.8.8].

Theorem 3.1 (Hilbert's Different Formula) *Let $L|E$ be a finite Galois extension of function fields, $\mathfrak{p} \in \mathcal{P}(E)$, and $\mathfrak{P} \in \mathcal{P}(L)$ lying over $\mathfrak{p}$. Let $I_{\mathfrak{p}}(i)$ denote the i-th ramification group of $\mathfrak{P}|\mathfrak{p}$. Then the different exponent $d(\mathfrak{P}|\mathfrak{p})$ is given by*

$$d(\mathfrak{P}|\mathfrak{p}) = \sum_{i=0}^{\infty} \big(|I_{\mathfrak{p}}(i)| - 1\big).$$

Next, we state a "transitivity formula" for different exponents, cf. [47, III.4.11].

Lemma 3.2 *Let $E \subseteq F \subseteq L$ be a tower of separable extensions of function fields. Suppose $\mathfrak{p}''$ resp. $\mathfrak{p}'$ resp. $\mathfrak{p}$ is a place of L resp. F resp. E with $\mathfrak{p}''|\mathfrak{p}'$ and $\mathfrak{p}'|\mathfrak{p}$. If $e(\mathfrak{p}''|\mathfrak{p}')$ denotes the ramification index of $\mathfrak{p}''|\mathfrak{p}'$, then*

$$d(\mathfrak{p}''|\mathfrak{p}) = e(\mathfrak{p}''|\mathfrak{p}') \cdot d(\mathfrak{p}'|\mathfrak{p}) + d(\mathfrak{p}''|\mathfrak{p}').$$

The following theorem gives a lower bound for the different exponent; moreover, tame extensions are characterized. Again, a proof can be found in Stichtenoth [47].

Theorem 3.3 (Dedekind's Different Theorem) *Let $L|E$ be a separable extension of function fields, $\mathfrak{p} \in \mathcal{P}(E)$, and $\mathfrak{P} \in \mathcal{P}(L)$ lying over $\mathfrak{p}$. Let $e(\mathfrak{P}|\mathfrak{p})$ denote the ramification index of $\mathfrak{P}|\mathfrak{p}$. Then $d(\mathfrak{P}|\mathfrak{p}) \geq e(\mathfrak{P}|\mathfrak{p}) - 1$ and*

$$d(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p}) - 1 \iff \mathfrak{P}|\mathfrak{p} \text{ is tame.}$$

We are still missing a comfortable tool to compute the degree of the different in non-Galois extensions. It seems that the following proposition is widely known and often used, but the author does not know any reference for it. Hence, we will prove

Proposition 3.4 *Let $L|E$ be a Galois extension of function fields with Galois group G. Let $H \leq G$ be a subgroup of G and set $F := \mathrm{Fix}(H)$ the fixed field of H. Define $n := [G : H]$. Consider G as a permutation group on n points via the natural action of G on the left-coset space G/H. Denote by $o(S)$ the number of orbits of a subgroup $S \leq G$.*

Let $\mathfrak{p} \in \mathcal{P}(E)$ be a place of E. Fix an arbitrary place $\pi \in \mathcal{P}(L)$ lying over $\mathfrak{p}$, denote by $I(i)$ the i-th ramification group of the extension $\pi|\mathfrak{p}$, and define

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

Then

$$\mathrm{ind}(\mathfrak{p}) = \sum_{\mathfrak{q}|\mathfrak{p},\ \mathfrak{q}\in\mathcal{P}(F)} d(\mathfrak{q}|\mathfrak{p}) \deg(\mathfrak{q}) \in \mathbb{N}_0$$

equals the degree of the different in the extension $F|E$ coming from the ramification of $\mathfrak{p}$. In particular, $\sum_{\mathfrak{p}\in\mathcal{P}(E)} \mathrm{ind}(\mathfrak{p})$ equals the degree of the different of the extension $F|E$.

Proof. For a place $\mathfrak{q} \in \mathcal{P}(F)$ denote by $n_{\mathfrak{q}}$ the number of places of L lying over $\mathfrak{q}$. If $\mathfrak{P} \in \mathcal{P}(L)$ is a place of L, denote by $\mathfrak{P}_F := \mathfrak{P} \cap F$ the well-defined restriction of $\mathfrak{P}$ to F and by $I_{\mathfrak{P}|\mathfrak{P}_F}(i)$ the i-th ramification group of the extension $\mathfrak{P}|\mathfrak{P}_F$.

If $\mathfrak{q}$ resp. $\mathfrak{P}$ appears as an index of summation, then the sum extends over all places of F resp. L.

We use the notation from Stichtenoth [47]. We get

$$\begin{aligned}
\sum_{\mathfrak{q}|\mathfrak{p}} d(\mathfrak{q}|\mathfrak{p}) \deg(\mathfrak{q}) &\overset{(a)}{=} \sum_{\mathfrak{P}|\mathfrak{p}} \frac{1}{n_{\mathfrak{P}_F}} d(\mathfrak{P}_F|\mathfrak{p}) \deg(\mathfrak{P}_F) \\
&\overset{(b)}{=} \sum_{\mathfrak{P}|\mathfrak{p}} \frac{e(\mathfrak{P}|\mathfrak{P}_F) f(\mathfrak{P}|\mathfrak{P}_F)}{|H|} d(\mathfrak{P}_F|\mathfrak{p}) \deg(\mathfrak{P}_F) \\
&= \frac{\deg(\pi)}{|H|} \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}|\mathfrak{P}_F) d(\mathfrak{P}_F|\mathfrak{p}) \\
&\overset{(c)}{=} \frac{\deg(\pi)}{|H|} \sum_{\mathfrak{P}|\mathfrak{p}} \big(d(\mathfrak{P}|\mathfrak{p}) - d(\mathfrak{P}|\mathfrak{P}_F)\big) \\
&\overset{(d)}{=} \frac{\deg(\pi)}{|H|} \sum_{\mathfrak{P}|\mathfrak{p}} \sum_{i\geq 0} \big(|I(i)| - |I_{\mathfrak{P}|\mathfrak{P}_F}(i)|\big) \\
&\overset{(e)}{=} \frac{\deg(\pi)}{|H|} \sum_{i\geq 0} \sum_{\mathfrak{P}|\mathfrak{p}} \big(|I(i)| - |I_{\mathfrak{P}|\mathfrak{P}_F}(i)|\big) \\
&\overset{(f)}{=} \frac{\deg(\pi)}{|H|} \sum_{i\geq 0} \left(|I(i)| \frac{|G|}{|I(-1)|} - \sum_{\mathfrak{P}|\mathfrak{p}} |I_{\mathfrak{P}|\mathfrak{P}_F}(i)| \right).
\end{aligned}$$

Here are some hints for the above equations:

(a): Exactly $n_{\mathfrak{P}_F}$ places of L induce the same summand $d(\mathfrak{P}_F|\mathfrak{p}) \deg(\mathfrak{P}_F)$.

(b): Since $L|F$ is Galois, we have $|H| = n_{\mathfrak{P}_F} e(\mathfrak{P}|\mathfrak{P}_F) f(\mathfrak{P}|\mathfrak{P}_F)$.

(c): cf. Lemma 3.2

(d): cf. Hilbert's Different Formula

(e): Both sums are finite.

(f): The number of places of L above $\mathfrak{p}$ is $\frac{|G|}{|I(-1)|}$, cf. Stichtenoth [47, III.8.2].

Next we transform the expression $\sum_{\mathfrak{P}|\mathfrak{p}} |I_{\mathfrak{P}|\mathfrak{P}_F}(i)|$. Let T be a left-transversal for H in G. We have

$$\begin{aligned}
\sum_{\mathfrak{P}|\mathfrak{p}} |I_{\mathfrak{P}|\mathfrak{P}_F}(i)| &\overset{(A)}{=} \frac{1}{|I(-1)|} \sum_{g\in G} \big|I_{\pi^g|(\pi^g)_F}(i)\big| \\
&\overset{(B)}{=} \frac{|H|}{|I(-1)|} \sum_{t\in T} \big|I_{\pi^t|(\pi^t)_F}(i)\big| \\
&\overset{(C)}{=} \frac{|H|}{|I(-1)|} \sum_{t\in T} \big|I(i)\cap tHt^{-1}\big| \\
&\overset{(D)}{=} \frac{|H|}{|I(-1)|} |I(i)| \cdot o\big(I(i)\big).
\end{aligned}$$

Here again some hints, that explain the transformations in detail:

(A): G acts transitively on the set of places of L lying above $\mathfrak{p}$. By definition the decomposition group $I(-1)$ equals the stabilizer of π. Thus, there exist exactly $|I(-1)|$ elements in G that map π to a fixed place $\mathfrak{P}$ lying over $\mathfrak{p}$.

(B): Let $h \in H$ be an element of H. As h fixes F pointwise, the definitions immediately give $(\pi^{th})_F = \big((\pi^t)_F\big)^h = (\pi^t)_F$. Since $L|F$ is Galois, the equality $\big|I_{\pi^{th}|(\pi^{th})_F}(i)\big| = \big|I_{\pi^t|(\pi^t)_F}(i)\big|$ holds.

(C): Because of $I_{\pi^t|\mathfrak{p}}(i) = I_{\pi|\mathfrak{p}}(i)^t = I(i)^t$ and $I_{\pi^t|(\pi^t)_F}(i) = I_{\pi^t|\mathfrak{p}}(i) \cap H$ it follows

$$\big|I_{\pi^t|(\pi^t)_F}(i)\big| = \big|I_{\pi^t|\mathfrak{p}}(i)\cap H\big| = \big|I(i)^t \cap H\big| = \big|I(i)\cap tHt^{-1}\big|.$$

(D): Let $g \in I(i)$. g fixes the coset tH if and only if

$$(tH)^g = g^{-1}tH = tH \iff t^{-1}g^{-1}t \in H \iff g^{-1} \in tHt^{-1} \iff g \in tHt^{-1}.$$

Thus, the stabilizer of tH in $I(i)$ coincides with $I(i)\cap tHt^{-1}$ and $\sum_{t\in T}\big|I(i)\cap tHt^{-1}\big|$ equals the sum of the number of fixed points of all elements of $I(i)$. Therefore the orbit-counting theorem yields

$$\sum_{t\in T}\big|I(i)\cap tHt^{-1}\big| = |I(i)|\cdot o\big(I(i)\big).$$

Putting all together we obtain

$$\begin{aligned}
\sum_{\mathfrak{q}|\mathfrak{p}} d(\mathfrak{q}|\mathfrak{p})\deg(\mathfrak{p}) &= \frac{\deg(\pi)}{|H|}\sum_{i\geq 0}\left(|I(i)|\frac{|G|}{|I(-1)|} - \sum_{\mathfrak{P}|\mathfrak{p}}|I_{\mathfrak{P}|\mathfrak{P}_F}(i)|\right) \\
&= \frac{\deg(\pi)}{|H|}\sum_{i\geq 0}\left(|I(i)|\frac{|G|}{|I(-1)|} - \frac{|H|}{|I(-1)|}|I(i)|\cdot o\big(I(i)\big)\right) \\
&= \frac{\deg(\pi)}{|I(-1)|}\sum_{i\geq 0}|I(i)|\Big(n - o\big(I(i)\big)\Big) \\
&= \deg(\mathfrak{p})\sum_{i\geq 0}\frac{n - o\big(I(i)\big)}{[I:I(i)]} = \operatorname{ind}(\mathfrak{p})
\end{aligned}$$

The remaining assertions follow from the general definitions, cf. [47, III.4.3]. ∎

The next lemma gives a lower bound for the function "ind". An obvious idea is to discard all summands with $i > 0$; this method yields $\mathrm{ind}(\mathfrak{p}) \geq n - o(I)$. However, the following estimation is stronger.

Lemma 3.5 *With the notation from Proposition 3.4 set p the characteristic of E and define $o'(I)$ the number of orbits of the inertia group $I := I(0)$ with length not divisible by p. Then*

$$\mathrm{ind}(\mathfrak{p}) \geq n - o'(I).$$

Proof. Denote by $\ell(t) := |(tH)^I|$ the length of the I-orbit through tH. [47, III.1.6] and the identity $\mathrm{Fix}(t^{-1}Ht) = F^t$ show

$$\ell(t) = \frac{|I|}{|I \cap tHt^{-1}|} = \frac{e(\pi|\mathfrak{p})}{e(\pi|\pi_{F^{t^{-1}}})} = e(\pi_{F^{t^{-1}}}|\mathfrak{p}).$$

Dedekind's Different Theorem yields

$$\ell(t) = d(\pi_{F^{t^{-1}}}|\mathfrak{p}) + \delta_t$$

where δ_t is an integer with $\delta_t \leq 1$ and $\delta_t = 1$ if and only if $p \nmid e(\pi_{F^{t^{-1}}}|\mathfrak{p})$. Set

$$\delta'(t) := \begin{cases} 0 & \text{if } p \mid e(\pi_{F^{t^{-1}}}|\mathfrak{p}), \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$\begin{aligned}
\mathrm{ind}(\mathfrak{p}) &= \frac{\deg(\pi)}{|H|} \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}|\mathfrak{P}_F) d(\mathfrak{P}_F|\mathfrak{p}) \\
&= \frac{\deg(\pi) \cdot |I|}{|H|} \sum_{\mathfrak{P}|\mathfrak{p}} \frac{d(\mathfrak{P}_F|\mathfrak{p})}{e(\mathfrak{P}_F|\mathfrak{p})} \\
&\overset{(\alpha)}{=} \frac{\deg(\pi) \cdot |I|}{|H| \cdot |I(-1)|} \sum_{g \in G} \frac{d\big((\pi^g)_F|\mathfrak{p}\big)}{e\big((\pi^g)_F|\mathfrak{p}\big)} \\
&\overset{(\beta)}{=} \frac{\deg(\pi) \cdot |I|}{|I(-1)|} \sum_{t \in T} \frac{d\big((\pi^t)_F|\mathfrak{p}\big)}{e\big((\pi^t)_F|\mathfrak{p}\big)} \\
&\overset{(\gamma)}{=} \deg(\mathfrak{p}) \sum_{t \in T} \frac{d\big(\pi_{F^{t^{-1}}}|\mathfrak{p}\big)}{e\big(\pi_{F^{t^{-1}}}|\mathfrak{p}\big)} \\
&\geq \deg(\mathfrak{p}) \sum_{t \in T} \frac{\ell(t) - \delta'_t}{\ell(t)} \\
&\geq \deg(\mathfrak{p}) \Big(n - \sum_{t \in T} \delta'_t\Big) \\
&\overset{(\delta)}{=} \deg(\mathfrak{p}) \big(n - o'(I)\big)
\end{aligned}$$

Again some hints for the above equations:

(α): cf. hint (A)

(β): cf. hint (B)

(γ): Hint (C) shows that $e\big(\pi^t|(\pi^t)_F\big) = |I \cap tHt^{-1}| = e\big(\pi|\pi \cap \mathrm{Fix}(tHt^{-1})\big) = e\big(\pi|\pi_{F^{t^{-1}}}\big)$; thus,

$$e\big((\pi^t)_F|\mathfrak{p}\big) = \frac{e\big(\pi^t|\mathfrak{p}\big)}{e\big(\pi^t|(\pi^t)_F\big)} = \frac{e(\pi|\mathfrak{p})}{e\big(\pi|\pi_{F^{t^{-1}}}\big)} = e\big(\pi_{F^{t^{-1}}}|\mathfrak{p}\big).$$

The equality $d\big((\pi^t)_F|\mathfrak{p}\big) = d\big(\pi_{F^{t^{-1}}}|\mathfrak{p}\big)$ is due to Lemma 3.2 and Hilbert's Different Formula.

(δ): δ'_t vanishes if and only if p divides the length of the I-orbit through tH. Therefore $\sum_{t\in T}\delta'_t$ and $o'(I)$ are equal by definition.

■

Now we state two important theorems that allow us to give severe restrictions for the decrease in the orders of the higher ramification groups.

We continue to assume $L|E$ to be Galois and suppose the constant field of E to be algebraically closed. $\mathfrak{p} \in \mathcal{P}(E)$ is a place of E and $\mathfrak{P} \in \mathcal{P}(L)$ lies over $\mathfrak{p}$. For an integer i set $I(i)$ the i-th ramification group of $\mathfrak{P}|\mathfrak{p}$. For a real number $u \in \mathbb{R}$ define

$$I_u := \begin{cases} I(-1) & \text{if } u < -1, \\ I(\lceil u \rceil) & \text{if } u \geq -1. \end{cases}$$

Let $\varphi_{\mathfrak{P}|\mathfrak{p}} : \mathbb{R}_0^+ \to \mathbb{R}$ be the function defined by

$$\varphi_{\mathfrak{P}|\mathfrak{p}}(u) := \int_0^u \frac{dt}{[I_0 : I_t]}.$$

Since its derivative is always positive, $\varphi_{\mathfrak{P}|\mathfrak{p}}$ is injective.

The Theorem of Hasse-Arf [44, IV §3] now reads as follows

Theorem 3.6 (Hasse-Arf) *If $I(0)$ is an abelian group and $i \in \mathbb{N}_0$ is an integer with $I(i) > I(i+1)$, then $\varphi_{\mathfrak{P}|\mathfrak{p}}(i) \in \mathbb{Z}$.*

Suppose N is a normal subgroup of $\mathrm{Gal}(L|E)$. Set $F := \mathrm{Fix}(N)$ and $\mathfrak{p}' := \mathfrak{P} \cap F$. Denote the ramification groups of $\mathfrak{P}|\mathfrak{p}'$ with $J(i)$ resp. J_u and the ramification groups of $\mathfrak{p}'|\mathfrak{p}$ with $F(i)$ resp. F_u.

It is easy to express J_u in terms of I_u; the definitions directly give

$$J_u = I_u \cap N.$$

The computation of F_u is more difficult; however, [44, IV §3] shows

Theorem 3.7 (Herbrand) *With the above notation it follows*

$$F_{\varphi_{\mathfrak{P}|\mathfrak{p}'}(u)} \cong I_u N/N \cong I_u/J_u.$$

Remark 3.8 Although Serre [44] proves the above results only in case of *local* function fields, they are correct in the global case, too. This is seen as follows: Completion at the place $\mathfrak{P}$ gives an Galois extension $L'|E'$ with Galois group $I(0)$. The normal subgroup N of $\mathrm{Gal}(L|E)$ corresponds to the group $J(0) = I(0) \cap N$. In particular, the function φ is invariant under completion as it only depends on subgroups of $I(0)$ resp. $J(0)$. Since, moreover, completion at $\mathfrak{P}$ does not change the ramification behavior of $\mathfrak{P}|\mathfrak{p}$, the assertions of the Theorems of Hasse-Arf and Herbrand can be transferred unmodified to the case of global function fields. ⋆

3.2. Applications to the case of affine Galois groups

In this section $p \in \mathbb{P}$ is a prime, k an algebraic extension of $\mathbb{F}_p$, t a transcendental over k, and $f \in k[X]$ an affine polynomial of degree $n = p^r$ that is functionally indecomposable over k. Set ℓ the splitting field of $f(X) - t|k(t)$. Denote by K an algebraic closure of k and set $L := K\ell$. Then $L|K(t)$ is a Galois extension with affine Galois group $G = N \rtimes H$; here N denotes the affine kernel of $\mathrm{Gal}\big(\ell|k(t)\big)$ and H is the stabilizer of a root x of $f(X) - t$.

As the fixed field $\mathrm{Fix}(H)$ of H coincides with $K(t, x) = K(x)$ and the action of G on the roots of $f(X) - t$ is equivalent to the natural action of G on the left-coset space G/H, Proposition 3.4 and the Riemann-Hurwitz genus formula imply the important

Corollary 3.9 (Genus-0 Condition) *With the notation from Proposition 3.4 the equality* $\sum_{\mathfrak{p}} \mathrm{ind}(\mathfrak{p}) = 2n - 2$ *holds.*

For a place $\mathfrak{p} \in \mathcal{P}\big(K(t)\big)$ of $K(t)$ the integer $\mathrm{ind}(\mathfrak{p})$ only depends on the series of higher ramification groups of $\mathfrak{p}$ and the way how these groups act on the set of zeros of $f(X) - t$.

In the following sections we present methods that give estimations for these information.

3.2.1. Consequences of Hasse-Arf and Herbrand

Set $E := \mathrm{Fix}(N)$, fix a place $\mathfrak{P} \in \mathcal{P}(L)$, and define $\mathfrak{p}' := \mathfrak{P} \cap E$.

Let I_u resp. J_u resp. F_u denote the ramification groups of $\mathfrak{P}|\mathfrak{p}$ resp. $\mathfrak{P}|\mathfrak{p}'$ resp. $\mathfrak{p}'|\mathfrak{p}$. Define $I := I_0$, $J := J_0$, and $F := F_0$. For an integer $i \in \mathbb{N}_0$ set

$$u_i := \varphi^{-1}_{\mathfrak{P}|\mathfrak{p}'}(i).$$

Important facts concerning the elements u_i are given by the following

Lemma 3.10 *u_i is an integer. For a real number $x \in \mathbb{R}$ with $u_i < x \leq u_{i+1}$ the equalities*

$$J_x = J(u_{i+1}) \qquad \text{and} \qquad I_x = I(u_{i+1})$$

hold. Furthermore

$$u_{i+1} - u_i = \frac{|J|}{|J(u_{i+1})|}.$$

Proof. Let $m \in \mathbb{N}_0$ be an integer and $u \in \mathbb{R}$ a real number with $m < u \leq m + 1$. Since $\varphi_{\mathfrak{P}|\mathfrak{p}'}$ is continuous and piecewise linear by definition, it follows

$$\varphi_{\mathfrak{P}|\mathfrak{p}'}(u) = \frac{|J(m+1)|}{|J|}(u - m) + \sum_{k=1}^{m} \frac{|J(k)|}{|J|}.$$

Thus, assuming $m < u_i \leq m + 1$ yields

$$\varphi_{\mathfrak{P}|\mathfrak{p}'}(u_i) = i = \frac{|J(m+1)|}{|J|}(u_i - m) + \sum_{k=1}^{m} \frac{|J(k)|}{|J|}$$

which is equivalent to

$$i|J| = |J(m+1)|(u_i - m) + \sum_{k=1}^{m} |J(k)|.$$

Since $|J(m+1)|$ divides $|J(k)|$ for all $k \in \{0, 1, \ldots, m+1\}$, $u_i - m$ is an integer and, hence, $u_i \in \mathbb{N}_0$.

The ramification groups of $\mathfrak{P}|\mathfrak{p}'$ are subgroups of $J \leq N$ and, thus, abelian. As $i < \varphi_{\mathfrak{P}|\mathfrak{p}'}(x) \leq i+1$ and $\varphi_{\mathfrak{P}|\mathfrak{p}'}(x) = i+1$ if and only if $x = u_{i+1}$, Hasse-Arf gives

$$J_x = J(u_{i+1}).$$

The definition of u_i gives $F_{\varphi_{\mathfrak{P}|\mathfrak{p}'}(x)} = F(\lceil \varphi_{\mathfrak{P}|\mathfrak{p}'}(x) \rceil) = F(i+1)$. Herbrand states

$$I_x/J_x = I_x/J(u_{i+1}) \cong F_{\varphi_{\mathfrak{P}|\mathfrak{p}'}(x)} = F(i+1);$$

this shows $|I_x| = |I(u_{i+1})|$ for all possible x. Hence, $I_x = I(u_{i+1})$.

As $\varphi'_{\mathfrak{P}|\mathfrak{p}'}(x) = \frac{|J(u_{i+1})|}{|J|}$, the definitions of u_i and x give

$$\varphi_{\mathfrak{P}|\mathfrak{p}'}(x) = i + \frac{|J(u_{i+1})|}{|J|}(x - u_i).$$

The remaining assertions follow easily. ∎

Corollary 3.11 *The equality*

$$\operatorname{ind}(\mathfrak{p}) = \sum_{i=0}^{\infty} \frac{|F(i)|}{|F|}\Big(n - o\big(I(u_i)\big)\Big)$$

holds.

Proof. By Lemma 3.10 the $u_{i+1} - u_i = \frac{|J|}{|J(u_{i+1})|}$ groups

$$I(u_i + 1),\ I(u_i + 2),\ \ldots,\ I(u_{i+1})$$

are equal. J being a p-group gives $J = J(0) = J(1)$, $u_0 = 0$, and $u_1 = 1$. Therefore

$$\begin{aligned}
\operatorname{ind}(\mathfrak{p}) &= \sum_{i=0}^{\infty} \frac{n - o\big(I(i)\big)}{[I : I(i)]} \\
&= \frac{n - \big(I(u_0)\big)}{[I : I(u_0)]} + \sum_{i=1}^{\infty} \frac{n - o\big(I(u_i)\big)}{[I : I(u_i)]}(u_i - u_{i-1}) \\
&= \frac{n - \big(I(u_0)\big)}{[I : I(u_0)]} + \sum_{i=1}^{\infty} \Big(n - o\big(I(u_i)\big)\Big) \frac{|I(u_i)| \cdot |J|}{|I| \cdot |J(u_i)|}.
\end{aligned}$$

Herbrand shows that $I/J \cong F$ and $I(u_i)/J(u_i) \cong F(i)$. Thus,

$$\begin{aligned}
\operatorname{ind}(\mathfrak{p}) &= \frac{n - \big(I(u_0)\big)}{[I : I(u_0)]} + \sum_{i=1}^{\infty} \Big(n - o\big(I(u_i)\big)\Big) \frac{|F(i)|}{|F|} \\
&= \sum_{i=0}^{\infty} \frac{|F(i)|}{|F|}\Big(n - o\big(I(u_i)\big)\Big).
\end{aligned}$$

This is the claim. ∎

3.2.2. Bounds for the number of fixed points for elements of G

We have seen in the previous paragraphs that we need information about the number of orbits $o\big(I(i)\big)$ of a series of ramification groups $I(i)$ in order to calculate degrees of differents in the extension $K(x)|K(t)$. As the orbit-counting theorem relates the number of orbits of a group with the number of fixed points of each group element, we have to develop good bounds for this latter number. For an arbitrarily given permutation group this is a difficult problem.

In our case G is an affine group; we have geometric interpretations of the action of G. This allows us to give severe restrictions for the number of fixed points of an element of G.

Every element $g \in G$ can uniquely expressed in the form $g = nh$ with $n \in N$ and $h \in H$. Define the H-projection mapping $\mathcal{L} : G \to H$ (the letter "$\mathcal{L}$" stands for "linearization") via

$$(nh)^{\mathcal{L}} := h.$$

$\mathcal{L}$ is an epimorphism with kernel N. We state an important observation.

Lemma 3.12 *Let $g \in G$ be an element of G. Then either g fixes no element or g and $g^{\mathcal{L}}$ have the same number of fixed points.*

Proof. Suppose $f \in N$ is fixed by g. As N is a transitive subgroup of G, every element fixed by g can be written in the form fm with $m \in N$. Thus, let $m \in N$ be an arbitrary element of N and write $g = nh$ with $n \in N$ and $h \in H$. Then fm is fixed by nh if and only if

$$fm = (fm)^{nh} = (\underbrace{fm \cdot n}_{\in N})^h = (fn \cdot m)^h = f^{nh} \cdot m^h = f \cdot m^h \iff m = m^h.$$

It follows that g has as many fixed points as $g^{\mathcal{L}} = h$. ∎

Since an element $h \in H$ acts as an automorphism $A_h \in \mathrm{GL}(N)$ of the vector space N, the set of fixed points of h equals the eigenspace of A_h for the eigenvalue 1. As eigenspaces are vector spaces, we get

Corollary 3.13 *Suppose $g \in G$ has at least one fixed point. Then the number of fixed points of g is a power of p; in particular, $1 \neq g$ implies $|\operatorname{Fix}(g)| \mid \frac{n}{p}$.*

Next we state a criterion that guarantees the existence of fixed points.

Corollary 3.14 *Let $g \in G$ be a p-regular element. Then g has a fixed point.*

Proof. The group $U := \langle N, g\rangle$ can be written as $U = N \rtimes C$ with a cyclic group $C \leq H$ of order $|g|$. As N is solvable, Schur-Zassenhaus shows that g is conjugate to a generator of C. This element, however, fixes $0 \in N$. ∎

3.2.3. Bounds for $\mathrm{ind}(\infty)$

Let $\infty \in \mathcal{P}\big(K(t)\big)$ be the infinite place of $K(t)$ and denote with $\mathfrak{P} \in \mathcal{P}(L)$ a place of L lying over ∞. Set $I_\infty(i)$ the i-th ramification group of $\mathfrak{P}|\infty$ and define $I_\infty := I_\infty(0)$.

The next lemma is the basis for all estimations of $\mathrm{ind}(\infty)$.

Lemma 3.15 *Both I_∞ and $I_\infty(1)$ are transitive.*

Proof. As ∞ ramifies totally in the extension $K(x)|K(t)$, van der Waerden [51] gives the transitivity of I_∞.

$I_\infty(1)$ equals the normal p-Sylow subgroup of I_∞. Denote by $\Omega_1, \ldots, \Omega_r$ the orbits of $I_\infty(1)$. As $I_\infty(1)$ is normal in I_∞, all orbits Ω_i have the same cardinality ω. Since $|N| = \sum_{i=1}^{r} |\Omega_i|$ is a power of p, both ω and r are powers of p. I_∞ acts transitively on the set of orbits Ω_i. Hence, r divides $[I_\infty : I_\infty(1)]$; as this index is prime to p, we obtain $r = 1$ and, thus, the transitivity of $I_\infty(1)$. ∎

Easy consequences are

Corollary 3.16 *Suppose $|I_\infty| = p^r s$ with $p \nmid s$. Then $\mathrm{ind}(\infty) \geq (n-1)(1+s^{-1})$; equality holds if and only if $I_\infty(2) = 1$.*

In particular, $\mathrm{ind}(\infty) \geq n$ and, provided that $I_\infty > 1$ is a p-group, ∞ is the unique place ramifying in $L|K(t)$.

Corollary 3.17 *If $I_\infty(i) > 1$, then $o\big(I_\infty(i)\big) \mid \frac{n}{p}$. Use the notation from Corollary 3.11 and suppose $I_\infty(u_a) > I_\infty(u_{a+1}) = 1$. Then*

$$\mathrm{ind}(\infty) \geq (n-1)\Big(1 + \frac{|F_\infty(1)|}{|F_\infty|}\Big) + \big(n - \frac{n}{p}\big) \sum_{i=2}^{a} \frac{|F_\infty(i)|}{|F_\infty|}.$$

Proof. Every ramification group $I_\infty(i)$ is a normal subgroup of I_∞, cf. Maus [37]. Thus, the orbits of $I_\infty(i)$ all have the same length. The claim is due to n being a prime power. ∎

The previous results and our definition $E := \mathrm{Fix}(N)$ give

Lemma 3.18 *∞ ramifies in $E|K(t)$ if and only if $[E : K(t)] > 1$.*

Proof. Suppose ∞ does not ramify in the extension $E|K(t)$. Then $I_\infty \leq N$. Since ∞ ramifies totally in the extension $K(x)|K(t)$, the group I_∞ coincides with N. By Corollary 3.16 there is no finite ramification in $L|K(t)$. Therefore $E|K(t)$ is unramified. Stichtenoth [47, III.5.8] shows $E = K(t)$. ∎

3.2.4. Bounds for $\mathrm{ind}(\mathfrak{p})$ with $\mathfrak{p}$ a finite place

Let $\mathfrak{p} \in \mathcal{P}\big(K(t)\big)$ be a finite place of $K(t)$ and $\mathfrak{P} \in \mathcal{P}(L)$ lying over $\mathfrak{p}$. The symbols $\mathfrak{p}'$, $I_\mathfrak{p}$, $J_\mathfrak{p}$, and $F_\mathfrak{p}$ are defined as in section 3.2.1.

Lemma 3.5 allows us to prove an important

Corollary 3.19 *$J_\mathfrak{p} = 1$. $I_\mathfrak{p}(i) \cong F_\mathfrak{p}(i)$ and $o\big(I_\mathfrak{p}(i)\big) \leq o\big(I_\mathfrak{p}(i)^{\mathcal{L}}\big)$ for all i.*

Proof. Suppose $J_\mathfrak{p}$ is nontrivial. Then $p \mid |J_\mathfrak{p}|$ and every $J_\mathfrak{p}$-orbit has length a multiple of p. As $J_\mathfrak{p}$ is a subgroup of $I_\mathfrak{p}$, every $I_\mathfrak{p}$-orbit is the disjoint unit of some of the $J_\mathfrak{p}$-orbits. In particular, every $I_\mathfrak{p}$-orbit has length divisible by p. Lemma 3.5 shows

$$\mathrm{ind}(\mathfrak{p}) \geq n.$$

This contradicts the genus-0 condition as also $\mathrm{ind}(\infty) \geq n$.

Thus, $J_{\mathfrak{p}} = 1$ and $\varphi_{\mathfrak{P}|\mathfrak{p}'}$ is the identity. Herbrand gives

$$F_{\mathfrak{p}}(i) \cong I_{\mathfrak{p}}(i)/J_{\mathfrak{p}}(i) = I_{\mathfrak{p}}(i).$$

The remaining assertion follows from the orbit-counting theorem. ∎

We see that the knowledge of the ramification of $\mathfrak{p}$ in the extension $E|K(t)$ determines the ramification of $\mathfrak{p}$ in $L|K(t)$ completely. Furthermore the estimation

$$\operatorname{ind}(\mathfrak{p}) \geq \sum_{i\geq 0} \frac{n - o\big(I_{\mathfrak{p}}(i)^{\mathcal{L}}\big)}{[I_{\mathfrak{p}} : I_{\mathfrak{p}}(i)]}$$

holds.

A consequence of the orbit-counting theorem is

Lemma 3.20 *Set* $f := \max\{|\operatorname{Fix}(g)| \mid g \in I_{\mathfrak{p}}(i)\}$ *and suppose* $1 \leq r < |I_{\mathfrak{p}}(i)|$. *Then*

$$o\big(I_{\mathfrak{p}}(i)\big) \leq \frac{1}{|I_{\mathfrak{p}}(i)|}\Big(n + (|I_{\mathfrak{p}}(i)| - 1)f\Big) \leq \frac{1}{|I_{\mathfrak{p}}(i)|}\Big(n + (|I_{\mathfrak{p}}(i)| - 1)\frac{n}{p}\Big) \leq \frac{1}{r}\Big(n + (r-1)\frac{n}{p}\Big).$$

A simple but useful consequence of the previous estimations is the following lemma that gives a limit for the number of finite branch points for affine polynomials. This result is also proved in Guralnick/Müller [17, Lem. 2.1].

Lemma 3.21 *Suppose* f *is an affine polynomial of degree* p^r. *If* f *has* ≥ 2 *finite branch points, then* f *has exactly* 2 *finite branch points,* p *is odd, and the finite branch points are tamely ramified with corresponding inertia groups of order* 2.

Part II.

Application to specific problems

Notation used in this part

We continue the notation from the previous sections: k is a finite field of characteristic p. $f \in k[X]$ denotes an affine polynomial of degree $n = p^r$ that is functionally indecomposable over k. K is a fixed algebraic closure of k. t is a transcendental over K, x denotes a fixed zero of $f(X) - t$. The splitting field of $f(X) - t$ over $k(t)$ resp. $K(t)$ is denoted by ℓ resp. $L = K\ell$. The arithmetic monodromy group $\mathrm{Gal}\big(\ell|k(t)\big)$ of f is denoted by A, the geometric monodromy group $\mathrm{Gal}\big(L|K(t)\big)$ by G. N is the affine kernel of A. Set $U := A_x$ and $H := G_x$. The fixed field of N in the extension $L|K(t)$ is denoted by E.
∞ always stands for the infinite place of $K(t)$; the symbols $\mathfrak{p}$ and $\mathfrak{q}$ denote different finite places of $K(t)$.
Unless redefined, $I_\infty(i)$ is the i-th ramification group of a fixed place of L over ∞, $J_\infty(i) := I_\infty(i) \cap N$, and $F_\infty(i)$ denotes the i-th ramification group of the induced extension of ∞ in $E|K(t)$. Set $I_\infty := I_\infty(0)$, $J_\infty := J_\infty(0)$, and $F_\infty := F_\infty(0)$.
The groups $I_\mathfrak{p}$, $I_\mathfrak{q}$, etc. are defined analogously.

4. Affine polynomials with $g \leq 2$

In this chapter we restrict the genus $g := g(E)$ of E to certain values and classify all affine polynomials in question.

A first observation is

Lemma 4.1 *Suppose the extension $E|K(t)$ is tame. Then $g = 0$ and the possibilities for f are given in Theorem 4.2.*

Proof. The assertion is clear for $E = K(t)$.

Otherwise ∞ ramifies in $E|K(t)$ with index $e_\infty := |F_\infty| > 1$ by Lemma 3.18. Additionally at most two finite places $\mathfrak{p}$ and $\mathfrak{q}$ ramify; set $e_\mathfrak{p} := |F_\mathfrak{p}|$ and $e_\mathfrak{q} := |F_\mathfrak{q}|$.

Suppose $e_\mathfrak{q} = 1$. Then by Riemann-Hurwitz

$$2g - 2 = -2[E : K(t)] + \underbrace{\frac{e_\infty - 1}{e_\infty} \cdot [E : K(t)] + \frac{e_\mathfrak{p} - 1}{e_\mathfrak{p}} \cdot [E : K(t)]}_{<2[E:K(t)]} < 0;$$

hence $g = 0$.

Suppose $e_\mathfrak{p}$, $e_\mathfrak{q} > 1$. Then $e_\mathfrak{p} = e_\mathfrak{q} = 2$ by Lemma 3.21 and Riemann-Hurwitz shows

$$2g - 2 = -2[E : K(t)] + \frac{e_\infty - 1}{e_\infty} \cdot [E : K(t)] + 2 \cdot \frac{1}{2} \cdot [E : K(t)] < 0.$$

Thus, the claim follows in in this case, too. ∎

4.1. $g = 0$

In this section we assume the field E to be of genus 0. Our main result will be

Theorem 4.2 *With the notation from page 23 suppose $g = 0$. Then there exist linear polynomials $g_1, g_2 \in K[X]$ such that $F := g_1 \circ f \circ g_2 \in k[X]$ belongs to one of the following classes:*

(1) $H = 1$ and F is an additive polynomial, i.e. $F = \sum_{i=0}^{r} a_i X^{p^i}$. F is exceptional if and only if F has no nonzero root in k.

(2) Case (A) of Theorem 4.3 holds and F is sublinearized of the form (4.2), cf. page 28. F is exceptional if and only if the polynomial $\sqrt[m]{\frac{1}{X}F(X)}$ has no zero in k.

(3) Case (D) of Theorem 4.3 holds. In [18] F will be studied in detail.

(4) Case (E) of Theorem 4.3 holds. F fulfills the conclusion of [17, Theorem 1.4].

We start by describing the Galois theoretic structure of the extension $E|K(t)$. This is not difficult since the possible Galois groups and the corresponding ramification data of $E|K(t)$ are well known.

Theorem 4.3 *E is a rational function field. The following table gives all possible isomorphisms types for H with $E|K(t)$ having the associated ramification behavior.*

Case	$H \cong$	*Ramification data*	*Conditions*
(A)	C_m	(m, m)	$(p, m) = 1$
(B)	$C_p \times \cdots \times C_p$	$(\lvert H\rvert)$	
(C)	$(C_p \times \cdots \times C_p) \rtimes C_m$	(m, qm)	$\lvert H\rvert = qm$, $m \mid q-1$, $q \neq 1$
(D)	D_m	$(2, m)$	$p = 2$, $(2, m) = 1$
(E)	D_m	$(2, 2, m)$	$p \neq 2$, $(p, m) = 1$
(F)	A_5	$(5, 6)$	$p = 3$
(G)	$\mathrm{PSL}(2, q)$	$\left(\frac{q(q-1)}{2}, \frac{q+1}{2}\right)$	$p \neq 2$, $q = p^m$
(H)	$\mathrm{PGL}(2, q)$	$\big(q(q-1), q+1\big)$	$p \neq 2$, $q = p^m$
(I)	$\mathrm{PGL}(2, q)$	$\big(q(q-1), q+1\big)$	$p = 2$, $q = p^m$

Proof. As K is algebraically closed, the rationality of E is a direct consequence of Stichtenoth [47, I.6.3]. Thus, $E|K(t)$ is a Galois extension of rational function fields.

The ramification behavior and the Galois groups of such extensions were classified by Valentini and Madan in [50].

Some cases of the original classification cannot occur: on the one hand, $K(t)$ does not contain any place of degree > 1, on the other hand, an affine polynomial fulfills the conclusion of Lemma 3.21. This leads to the above cases. ∎

The case $H = 1$ is completely discussed by Proposition 2.9. The criterion for an additive polynomial to be exceptional is given for instance in Lidl/Niederreiter [35, Theorem 7.9]. Therefore we will assume $H > 1$ from now on.

4.1.1. Case (A): $H \cong C_m$ is cyclic

As ∞ ramifies totally in the extension $K(x)|K(t)$, mn is a divisor of $|I_\infty|$. Since G has order mn, the equality $I_\infty = G$ holds.

We show that no nontrivial element of H fixes an element of $N^\sharp$. Assume the contrary. Then there exist an element $a \in N^\sharp$ and a nontrivial subgroup $S \leq H$ such that a is fixed by every element of S. As H is cyclic, S is characteristic in H and, thus, normal in U. Set $M := \langle a \rangle$ the irreducible S-submodule of N generated by a. Then every element of M is fixed by S. Clifford allows us to decompose the S-module N in the form

$$N = \bigoplus_{i=1}^{s} M^{u_i}$$

where $u_i \in U$ are appropriate elements of U. It follows that S stabilizes every element of M^{u_i}. Hence, S is a subgroup of the kernel of the operation of H on N in contradiction to the faithfulness of this operation.

Corollary 3.14 shows

$$\mathrm{ind}(\mathfrak{p}) = n - \frac{1}{m}\big(n + (m-1)\cdot 1\big) = (n-1)\Big(1 - \frac{1}{m}\Big).$$

The above shows that a conjugate of $I_{\mathfrak{p}}$ either is a subgroup of H or intersects H trivially. Thus, places of $K(x)$ lying over $\mathfrak{p}$ either ramify with index m or index 1. Suppose there are a resp. b places of $K(x)$ lying over $\mathfrak{p}$ with index m resp. index 1. By solving the equations $am + b = n$ and $a(m-1) = \operatorname{ind}(\mathfrak{p})$ we obtain that $\mathfrak{p}$ decomposes in $K(x)$ in the form

$$\mathfrak{p} = \mathfrak{P} \cdot \mathfrak{P}_1^m \cdots \mathfrak{P}_{\frac{n-1}{m}}^m \qquad \text{with pairwise different places } \mathfrak{P}, \mathfrak{P}_i \in \mathcal{P}\big(K(x)\big). \tag{4.1}$$

The genus-0 condition enforces

$$\operatorname{ind}(\infty) = 2n - 2 - \operatorname{ind}(\mathfrak{p}) = (n-1)\Big(1 + \frac{1}{m}\Big) = n - o(I_\infty) + \frac{n - o\big(I_\infty(1)\big)}{[I_\infty : I_\infty(1)]};$$

this gives $I_\infty(2) = 1$.

Now we are able to compute the genus $g(L)$ of L. Our previous considerations prove that the ramification in the extension $L|K(x)$ comes from the infinite place of $K(x)$ and $\mathfrak{P}$; both places ramify totally. Hence, by Riemann-Hurwitz $g(L) = 0$ and L is a rational function field.

Construction of f

By a linear substitution of both t and x we may assume $\mathfrak{p}$ resp. $\mathfrak{P}$ to be the zero place of $K(t)$ resp. $K(x)$. The decomposition (4.1) of $\mathfrak{p}$ gives

$$f(X) = X \cdot g^m(X)$$

with a separable polynomial $g \in K[X]$ of degree $\frac{n-1}{m}$ and $g(0) \neq 0$. The derivative of f reads as

$$f'(X) = g^m(X) + mXg^{m-1}(X) \cdot g'(X) = g^{m-1}(X) \cdot \big(g(X) + mX \cdot g'(X)\big).$$

Since $\mathfrak{p}$ is the only finite place ramifying in $K(x)|K(t)$, every zero ξ of f' is also a zero of g. Assume $g(\xi) + m\xi g'(\xi) = 0$. Then $m\xi g'(\xi) = 0$. Since $m\xi \neq 0$, we get $g'(\xi) = 0$. But this is impossible as g does not have multiple roots. Hence, $g(X) + mXg'(X) \in K^\sharp$ is a nonzero element of K.

Write $g(X) = \sum_{i=0}^{\frac{n-1}{m}} g_i X^i$ with $g_i \in K$ and $g_0 \cdot g_{\frac{n-1}{m}} \neq 0$. We obtain the equivalence

$$g(X) + mX \cdot g'(X) = \sum_{i=0}^{\frac{n-1}{m}} g_i(1+mi)X^i \in K^\sharp \iff g_i(1+mi) = 0 \text{ for } i \geq 1.$$

This shows that for $i \geq 1$ a nonzero coefficient $g_i \neq 0$ is possible only if $1 + mi = 0$, i.e. $1 + mi = \alpha p$ with some $\alpha \in \mathbb{N}$. Hence,

$$f(X) = X\Big(g_0 + \sum_{\substack{m \mid \alpha p - 1 \\ 1 \leq \frac{\alpha p-1}{m} \leq \frac{n-1}{m}}} g_{\frac{\alpha p-1}{m}} X^{\frac{\alpha p-1}{m}}\Big)^m.$$

As L is a rational function field, it is possible to choose $z \in L$ such that $L = K(z)$ and the infinite resp. zero place of $K(z)$ lies over the infinite resp. zero place of $K(x)$. Hence, we may assume $z^m = x$. Then z is annihilated by

$$f \circ X^m - t = \overbrace{\Big(g_0 X + \sum_{\substack{m \mid \alpha p - 1 \\ 1 \leq \frac{\alpha p-1}{m} \leq \frac{n-1}{m}}} g_{\frac{\alpha p-1}{m}} X^{\alpha p}\Big)}^{:= F(X)}{}^m - t = X^m \circ F(X) - t.$$

Set $\tau := F(z)$. As $\tau^m = t$, the field $K(\tau)$ contains $K(t)$. Since $\deg F = n$, the extension $K(z)|K(\tau)$ has degree $[K(z) : K(\tau)] = n$. N is the unique subgroup of G of order n; thus, the equality $\mathrm{Fix}(N) = K(\tau)$ holds.

As the infinite place of $K(\tau)$ ramifies totally in the extension $K(z)|K(\tau)$ with the infinite place of $K(z)$ lying above, Proposition 2.9 shows that F is an additive polynomial. Thus, the indices α are powers of p. We obtain

$$f(X) = X\Big(g_0 + \sum_{\substack{m|\alpha p-1 \\ 1\leq\frac{\alpha p-1}{m}\leq\frac{n-1}{m}}} g_{\frac{\alpha p-1}{m}} X^{\frac{\alpha p-1}{m}}\Big)^m = X\Big(\sum_{\substack{m|p^i-1 \\ p^i|n}} g_{\frac{p^i-1}{m}} X^{\frac{p^i-1}{m}}\Big)^m. \tag{4.2}$$

This are exactly Cohen's *sublinearized polynomials*, cf. [9]. We state Cohen's criteria for f to be exceptional in Theorem 4.2.

4.1.2. Case (B): H is an elementary abelian p-group

H is a normal p-subgroup of U. Proposition 2.8 gives $H = 1$ which was previously excluded.

4.1.3. Case (C): $H \cong (C_p \times \cdots \times C_p) \rtimes C_m$ is a semidirect product

H contains a unique p-Sylow subgroup. Thus, the p-Sylow subgroup of H is normal in U. Hence, H is a p'-group in contradiction to Theorem 4.3

4.1.4. Case (D): H is dihedral in even characteristic

This case will be extensively studied in [18]. It will be proved that there exist exceptional polynomials realizing this case.

4.1.5. Case (E): H is dihedral in odd characteristic

As G/N is a p'-group and f has two finite branch points, Guralnick/Müller [17, Theorem 2.2] completely discusses the ramification of $L|K(t)$. It will be shown in [18] that this case leads to the class of polynomials described in [17, Theorem 1.4].

4.1.6. Case (F): $H \cong A_5$ in characteristic 3

We show that this case does not occur.

Suppose first that $\mathfrak{p}$ ramifies tamely. Then by Corollary 3.16 $\mathrm{ind}(\infty) \geq \frac{3}{2}(n-1)$ and

$$\mathrm{ind}(\mathfrak{p}) \geq n - \frac{1}{5}\big(n + 4 \cdot \frac{n}{3}\big).$$

This violates the genus-0 condition.

Now suppose that $\mathfrak{p}$ ramifies wildly. Then $I_\infty \cong N \rtimes C_5$ and $I_\mathfrak{p} \cong S_3$; the higher ramification groups of ∞ are subgroups of N and, thus, act semiregularly on N. It follows from section 3.2.1

$$\mathrm{ind}(\infty) = \sum_{i=0}^{\infty} \frac{|F(i)|}{|F(0)|}\Big(n - o\big(I_\infty(u_i)\big)\Big) = \frac{6}{5}(n-1) + \frac{n}{5}\sum_{i=2}^{\infty}\Big(1 - \frac{1}{|I_\infty(u_i)|}\Big).$$

Therefore

$$\operatorname{ind}(\infty) = \frac{6}{5}(n-1) \qquad \text{or} \qquad \operatorname{ind}(\infty) \geq \frac{4}{3}n - \frac{6}{5}$$

depending on whether $I_\infty(2) = 1$ or $I_\infty(2) \geq C_3 > 1$.

Since elements of the same order are conjugate in $I_\mathfrak{p}$, $\operatorname{ind}(\mathfrak{p})$ is given by

$$\operatorname{ind}(\mathfrak{p}) = n - \frac{1}{6}(n + 3f_2 + 2f_3) + s \cdot \frac{n - \frac{1}{3}(n + 2f_3)}{2}$$

where f_2 resp. f_3 denotes the number of fixed points of an element of $I_\mathfrak{p}$ of order 2 resp. 3 and s is the well-defined integer with $I_\mathfrak{p}(s) > I_\mathfrak{p}(s+1) = 1$. As both f_2 and f_3 are $\leq \frac{n}{3}$, the genus-0 condition immediately gives $\operatorname{ind}(\infty) = \frac{6}{5}(n-1)$, $s = 1$, and $f_2 = f_3 = \frac{n}{3}$. It follows

$$\operatorname{ind}(\infty) + \operatorname{ind}(\mathfrak{p}) - 2n + 2 = \frac{36 - n}{45};$$

hence, the genus-0 condition cannot be fulfilled.

4.1.7. Case (G): $H \cong \mathrm{PSL}(2, q)$ with $p \neq 2$

We prove that this case does not occur.

H is irreducible on N

We show first that we can construct a new affine polynomial $g \in K[X]$ from our given polynomial f such that g is indecomposable over K and the geometric point stabilizer of g is isomorphic to $\mathrm{PSL}(2, q)$.

Lemma 4.4 *Suppose H is a non-abelian group such that every normal subgroup of H is characteristic in H.*

Then there exists an affine polynomial $g \in K[X]$ that is indecomposable over K and whose geometric point stabilizer is isomorphic to a factor group of H. Moreover, the fixed field of the affine kernel of the geometric monodromy group of g is a rational function field.

Proof. If f is functionally indecomposable over K, then we can set $f = g$.

Otherwise H is reducible on N and we can find a proper H-submodule $M < N$. Since H is normal in U, N is a semisimple H-module and can be written in the form

$$N = \bigoplus_{i=1}^{s} M^{u_i} \qquad \text{with} \qquad u_1 = 1 \text{ and } u_i \in U^\sharp.$$

H is faithful on M because the kernel of the action of H on M is characteristic in H and, thus, a subgroup of the kernel of the action of H on N. As H is non-abelian, this shows in particular that M cannot be one-dimensional.

Set $N' := \bigoplus_{i \neq 1} M^{u_i}$; N' is an H-module with $H < N' \rtimes H < N \rtimes H$. By Galois duality $\mathrm{Fix}(N' \rtimes H) = K(y)$ is a proper intermediate field between $K(x)$ and $K(t)$. This field induces a decomposition $f = g \circ h$ over K with $h(x) = y$ and $g(y) = t$, cf. Lemma 2.2.

Set Z the Galois hull of $K(y)|K(t)$ and $J := \mathrm{Gal}(L|Z)$; by definition $J = \bigcap_{\sigma \in G} (N' \rtimes H)^\sigma$. N' is invariant under the action of H; hence, $N' \leq J \leq N' \rtimes H$. This shows that $J = N' \rtimes Q$ with Q a normal and, thus, characteristic subgroup of H.

The extension $Z|K(t)$ is Galois by construction; the Galois group of $Z|K(t)$ is given by

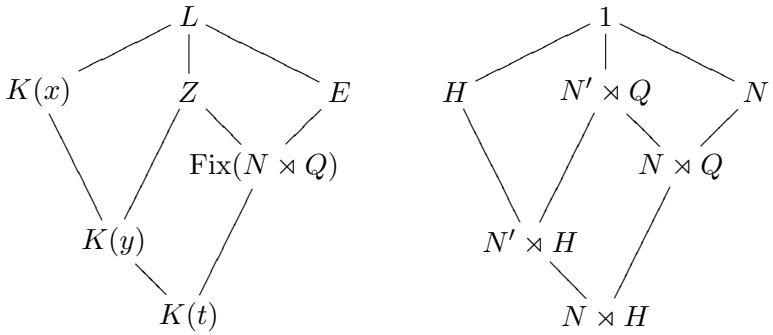
$$\mathrm{Gal}\big(Z|K(t)\big) \cong G/J = \frac{N \rtimes H}{N' \rtimes Q} \cong N/N' \rtimes H/Q \cong M \rtimes H/Q.$$

The isomorphism $\frac{N \rtimes H}{N' \rtimes Q} \cong N/N' \rtimes H/Q$ comes from the fact that every element $nhN'Q \in \frac{N \rtimes H}{N' \rtimes Q}$ can be written in the form $nN' \cdot hQ$ since $hN' = N'h$.

Since there are no proper intermediate fields between $K(y)$ and $K(t)$, g is indecomposable over K and H/Q acts irreducibly on M.

$\mathrm{Gal}\big(Z|K(t)\big)$ is an affine group: the regularity of N on the set of zeros of $f(X) - t$ gives the regularity of N/N' on the set of zeros of $g(X) - t$. The fixed field of the geometric point stabilizer of g equals the fixed field of $N \rtimes Q$ and, thus, is a subfield of the rational function field E. Lüroth [47, III.5.9] shows that this field is rational, too.

The following diagram visualizes the above situation



■

For $q > 3$ the group $\mathrm{PSL}(2, q)$ is simple. Thus, the geometric monodromy group of g is $M \rtimes H/Q$ with $H/Q \in \{1, \mathrm{PSL}(2, q)\}$. The case $H/Q = 1$ is impossible because the irreducible H/Q-module M would be one-dimensional in contradiction to Lemma 4.4.

Suppose $q = p = 3$. Then $H \cong \mathrm{PSL}(2, 3) \cong A_4$ and every normal subgroup of H is also characteristic in H. We obtain $H/Q \in \{1, C_3, H\}$; this again yields $H/Q = H$.

Hence, in all cases we can construct a functionally indecomposable polynomial g from f that also belongs to case (G). Therefore we will assume from now on that the given polynomial f itself is functionally indecomposable. By showing that such an f does not exist we prove the impossibility of case (G).

Bounds for the number of fixed points for elements of H

The following concept allows us to obtain approximate upper bounds for the number of fixed points of elements of H.

Definition 4.5 *Let H be a group and $h \in H$. We say that h is* k-generating *in H if H can be generated by k conjugates of h, i.e. if there exist elements $g_1, \ldots, g_k \in H$ such that*

$$H = \langle h^{g_1}, \ldots, h^{g_k} \rangle.$$

This definition yields in case of the group $\mathrm{PSL}(2, q)$

Lemma 4.6 *Let $1 \neq x \in \mathrm{PSL}(2, q)$ with q any prime power (in particular, the case $q = 2^m$ is allowed). Then x is*

- 2*-generating if $q > 2$, $|x| > 2$, and $(|x|, q) \neq (3, 9)$,*

- 3-*generating if* $(|x|, q) = (3, 9)$,
- 3-*generating if* $|x| = 2$ *and* $q \neq 3$.

Proof. The case $(|x|, q) = (3, 9)$ follows directly from Guralnick/Saxl [21, Lem. 3.1].

Now suppose $|x| = 2$ and $q \neq 3$. [21] gives the assertion for $q \geq 4$. For $q = 2$ the claim follows by direct computation.

At last suppose $q > 2$, $|x| > 2$, and $(|x|, q) \neq (3, 9)$.

If $|x|$ is not a power of 2, then the assertion follows for $q \geq 4$ again from [21] and for $q = 3$ by direct computation.

Thus, assume $|x| = 2^i$ with $i \geq 2$. It is sufficient to show that an element $f \in \mathrm{PSL}(2, q)$ of order 4 is 2-generating.

An inspection of the list [25, II 8.27] of all subgroups of $\mathrm{PSL}(2, q)$ shows that for $q \notin \{7, 9\}$ the group $\mathrm{PSL}(2, q)$ contains a maximal subgroup D isomorphic to a dihedral group of order $2 \cdot \frac{q+1}{(2,q-1)}$. The well-known fact that $\mathrm{PSL}(2, q)$ contains exactly one conjugacy class of involutions allows to find elements $g, h \in \mathrm{PSL}(2, q)$ such that $D = \langle (f^2)^g, (f^2)^h \rangle$. Suppose $\langle f^g, f^h \rangle \neq \mathrm{PSL}(2, q)$. Then $\langle f^g, f^h \rangle \leq D$, and both f^g and f^h are elements of the normal cyclic subgroup of D of order $\frac{1}{2}|D|$. This implies $(f^g)^2 = (f^h)^2$ in contradiction to D being dihedral.

For $q \in \{7, 9\}$ the assertion follows by direct calculation. ∎

The next lemma gives an upper bound for the number of fixed points of a k-generating element.

Lemma 4.7 *Let $h \in H$ be an element of H. If h is k-generating in H, then*

$$\dim \mathrm{Fix}(h) \leq \frac{k-1}{k} \dim N \qquad \textit{and} \qquad |\mathrm{Fix}(h)| \leq \sqrt[k]{n^{k-1}}.$$

Proof. Let $h \in H$ be k-generating in H. Then there exist conjugates $h_1, \ldots, h_k$ of h that generate H. Set $F_i := \mathrm{Fix}(h_i)$, $f := \dim F_1$, and $d := \dim N$; obviously the equality $f = \dim F_i$ holds for all $i \in \{1, \ldots, k\}$. Consider the homomorphism

$$\varphi : N \to N/F_1 \oplus \cdots \oplus N/F_k, \quad n \mapsto (nF_1, \ldots, nF_k)$$

with kernel $\ker \varphi = \bigcap_{i=1}^k F_i$. As H is irreducible on N, the intersection $\bigcap_{i=1}^k F_i = \{0\}$ is trivial and φ is injective. Since $\dim N/F_i = d - f$, we obtain

$$d \leq k \cdot (d - f) \iff f \leq \frac{k-1}{k} d.$$

The remaining assertions follow easily. ∎

N is a "big" module: $n \geq q^4$

For this section we assume $n \geq q^4$.

Suppose $q \neq 9$ and $h \in H$. Lemmas 4.6 and 4.7 give the estimations

$$|\operatorname{Fix}(h)| \le \begin{cases} n & \text{for } h = 1, \\ \sqrt[3]{n^2} = \frac{n}{\sqrt[3]{n}} \le \frac{n}{q} & \text{for } |h| = 2 \text{ and } q \neq 3, \\ \sqrt{n} = \frac{n}{\sqrt{n}} \le \frac{n}{q^2} & \text{for } |h| > 2. \end{cases}$$

First we discuss the case where $\mathfrak{p}$ ramifies tamely with index $\frac{q+1}{2}$. Then $I_\infty = P \rtimes C_{\frac{q-1}{2}}$ with a transitive p-group P. Corollary 3.16 shows

$$\operatorname{ind}(\infty) \ge (n-1)\big(1 + \frac{2}{q-1}\big);$$

this contradicts the genus-0 condition if $q = 3$. $I_\mathfrak{p}$ is cyclic and, thus, contains at most one involution. Hence,

$$\operatorname{ind}(\mathfrak{p}) \ge n - \frac{2}{q+1}\Big(n + \frac{n}{q} + \big(\frac{q+1}{2} - 2\big)\frac{n}{q^2}\Big).$$

It follows

$$\operatorname{ind}(\infty) + \operatorname{ind}(\mathfrak{p}) - 2n + 2 \ge \frac{q^2(q+1)(q-3) + n\big(-3 + q(6+q)\big)}{q^4 - q^2} > 0;$$

so the genus-0 condition is violated for all q in question.

Next we consider the case where $\mathfrak{p}$ ramifies wildly with index $\frac{q(q-1)}{2}$. Here, $I_\infty \cong N \rtimes C_{\frac{q+1}{2}}$ and, thus, $\operatorname{ind}(\infty) \ge (n-1)\big(1 + \frac{2}{q+1}\big)$.

The following lemma allows us to estimate the number of involutions in $I_\mathfrak{p}$.

Lemma 4.8 *Suppose $G \cong A \rtimes B$ with $2 \nmid |A|$ and B cyclic. Let i be the number of involutions and f the number of elements of order 4 in B. Then the number of involutions resp. elements of order 4 in G is less or equal than $i \cdot |A|$ resp. $f \cdot |A|$.*

Proof. Let $a \in A$ and $b \in B$. As A is a normal $2'$-subgroup of G, it follows by some standard arguments that $ab \in G$ having order 2 resp. 4 implies b to be an involution resp. to be of order 4. The claim follows as a direct consequence of this fact. ∎

As $I_\mathfrak{p}$ is isomorphic to a product $P \rtimes C_{\frac{q-1}{2}}$ with a p-group P of order q, the above lemma shows that $I_\mathfrak{p}$ contains at most q involutions. Since $I_\mathfrak{p}$ is a $2'$-group for $q = 3$, we obtain in all cases

$$\operatorname{ind}(\mathfrak{p}) \ge n - \frac{2}{q(q-1)}\Big(n + q\frac{n}{q} + \big(\frac{q(q-1)}{2} - 1 - q\big)\frac{n}{q^2}\Big) + \frac{2}{q-1}\Big(n - \frac{1}{q}\big(n + (q-1)\frac{n}{q^2}\big)\Big).$$

These estimations succeed in disproving the genus-0 condition.

Now suppose $q = 9$.

If $\mathfrak{p}$ ramifies tamely, the same bounds as above hold and, hence, the same contradiction follows.

Otherwise $I_\mathfrak{p}$ contains exactly 9 involutions and 8 elements of order 3; this shows

$$o(I_\mathfrak{p}) \le \frac{1}{36}\big(n + 17\frac{n}{9} + 18\frac{n}{81}\big) \quad \text{and} \quad o\big(I_\mathfrak{p}(1)\big) \le \frac{1}{9}\big(n + 8\frac{n}{9}\big).$$

Again a contradiction to the genus-0 condition results.

N is a "small" module: $n < q^4$

Unfortunately, in this case the bounds from Lemma 4.7 are too weak to induce contradictions to the genus-0 condition. By classifying all irreducible representations of H on N we get much sharper estimations for the number of fixed points of elements of H, cf. Lemma 3.12. This method will eventually lead to the impossibility of this case.

The following presentation of p-modular representation theory of the groups $\mathrm{PSL}(2,q)$ and $\mathrm{PGL}(2,q)$ is based on Brauer and Nesbitt [5, §30].

Let κ be any field of characteristic p and u, v algebraically independent transcendentals over κ. Denote by V_n the vector space of homogeneous polynomials in u and v of degree n over κ. Obviously $B_n := (u^n, u^{n-1}v, \ldots, v^n)$ is a basis for V_n.

For an element $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,\kappa)$ define

$$u^A := au + bv \qquad \text{and} \qquad v^A := cu + dv.$$

Some calculation shows that for a second element $A' \in \mathrm{GL}(2,\kappa)$ the relations $(u^A)^{A'} = u^{AA'}$ and $(v^A)^{A'} = v^{AA'}$ hold.

This action of $\mathrm{GL}(2,\kappa)$ can be extended to an endomorphism φ_A of V_n by defining

$$(u^i v^{n-i})^{\varphi_A} := (u^A)^i (v^A)^{n-i} \quad \text{and, thus,} \quad \Big(\sum_{i=0}^{n} \kappa_i u^i v^{n-i}\Big)^{\varphi_A} = \sum_{i=0}^{n} \kappa_i (u^A)^i (v^A)^{n-i}.$$

The mapping $A \mapsto \varphi_A$ is a homomorphism $\mathrm{GL}(2,\kappa) \to \mathrm{Aut}(V_n)$. Set $\mathfrak{S}_n(A)$ the representation matrix of φ_A with respect to the basis B; we consider $\mathfrak{S}_n(A)$ always acting on the *row vector space* κ^{n+1}. Then

$$\mathrm{GL}(2,\kappa) \to \mathrm{GL}(n+1,\kappa), \quad A \mapsto \mathfrak{S}_n(A)$$

is a group homomorphism. The next lemma allows us to explicitly calculate $\mathfrak{S}_n(A)$.

Lemma 4.9 *Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,\kappa)$. Denote the entries of $\mathfrak{S}_n(A)$ by s_{ij} with $1 \le i, j \le n+1$. Then*

$$s_{ij} = \sum_{\lambda=\max(0,n+2-i-j)}^{\min(n+1-i,n+1-j)} \binom{n+1-i}{\lambda} \binom{i-1}{n+1-j-\lambda} a^\lambda b^{n+1-i-\lambda} c^{n+1-j-\lambda} d^{\lambda+i+j-n-2}.$$

Proof. For the sake of shortness set $n' := n+1$. The image of the i-th basis vector $u^{n+1-i}v^{i-1}$ of B under the mapping φ_A is

$$\begin{aligned}
(u^{n'-i}v^{i-1})^{\varphi_A} &= (au+bv)^{n'-i}(cu+dv)^{i-1} \\
&= \sum_{r=0}^{n'-i} \sum_{s=0}^{i-1} \binom{n'-i}{r} \binom{i-1}{s} a^r b^{n'-i-r} c^s d^{i-1-s} u^{r+s} v^{n-r-s} \\
&\overset{(\star)}{=} \sum_{\mu=0}^{n} \Bigg(\sum_{\lambda=\max(0,\mu+1-i)}^{\min(\mu,n'-i)} \binom{n'-i}{\lambda} \binom{i-1}{\mu-\lambda} a^\lambda b^{n'-i-\lambda} c^{\mu-\lambda} d^{i-1+\lambda-\mu} \Bigg) u^\mu v^{n-\mu}
\end{aligned}$$

In $(\star)$ we set $\mu = r+s$ and $\lambda = r$. The conditions for λ come from the fact that $0 \le r \le n+1-i$ and $0 \le s \le i-1$. This shows the assertion. ∎

Definition 4.10 (Kronecker Product) *Let $A = (a_{ij}) \in \kappa^{r\times s}$, $B \in \kappa^{t\times u}$. The* Kronecker product $A \otimes B$ of A with B *is the matrix*

$$A \otimes B := \begin{pmatrix} a_{11}B & \cdots & a_{1s}B \\ \cdots & \cdots & \cdots \\ a_{r1}B & \cdots & a_{rs}B \end{pmatrix} \in \kappa^{rt\times su}.$$

Now we are able to specify all irreducible p-modular representations of $\mathrm{PSL}(2,q)$ and $\mathrm{PGL}(2,q)$ over $\mathbb{F}_q$:

Theorem 4.11 (Brauer-Nesbitt) *Let $p \in \mathbb{P}$ be a prime and $q := p^m$ a power of p. Let φ_i denote the i-th power of the Frobenius-automorphism of $\mathbb{F}_q$, i.e.*

$$\varphi_i : \mathbb{F}_q \to \mathbb{F}_q, \quad x \mapsto x^{p^i}.$$

For a matrix $A = (a_{ij})$ with $a_{ij} \in \mathbb{F}_q$ set $A^{\varphi_i} := \big((a_{ij})^{\varphi_i}\big)$.

(1) Assume $p \geq 3$. For $A \in \mathrm{SL}(2,q)$ denote by $\overline{A}$ the image of A in $\mathrm{PSL}(2,q)$. Then, up to conjugation, the irreducible p-modular representations of $\mathrm{PSL}(2,q)$ over $\mathbb{F}_q$ correspond to mappings θ with

$$\theta : \mathrm{PSL}(2,q) \to \mathrm{GL}\big(\prod_{i=0}^{m-1}(r_i+1), q\big), \quad \overline{A} \mapsto \bigotimes_{i=0}^{m-1} \mathfrak{S}_{r_i}(A^{\varphi_i});$$

here $0 \leq r_i < p$ for all i and $2 \mid \sum_{i=0}^{m-1} r_i$. θ is faithful if and only if there exists at least one index i with $r_i \neq 0$.

(2) For $A \in \mathrm{GL}(2,q)$ denote by $\overline{A}$ the image of A in $\mathrm{PGL}(2,q)$. Then, up to conjugation, the irreducible p-modular representations of $\mathrm{PGL}(2,q)$ over $\mathbb{F}_q$ correspond to mappings θ with

$$\theta : \mathrm{PGL}(2,q) \to \mathrm{GL}\big(\prod_{i=0}^{m-1}(r_i+1), q\big), \quad \overline{A} \mapsto \det(A)^s \bigotimes_{i=0}^{m-1} \mathfrak{S}_{r_i}(A^{\varphi_i});$$

here $0 \leq r_i < p$ for all i, $0 \leq s < q-1$, and $q-1 \mid (2s + \sum_{i=0}^{m-1} r_i p^i)$.

$\mathbb{F}_q$ is a splitting field for both $\mathrm{PSL}(2,q)$ and $\mathrm{PGL}(2,q)$.

We proceed with our classification of irreducible H-modules N with $n < q^4$:

We interpret N as a $\mathbb{F}_p$-vector space; then H acts as a subgroup of $\mathrm{GL}(r,p)$. Isaacs [29, 9.21] and Theorem 4.11 show that $N^{\mathbb{F}_q} := N \otimes \mathbb{F}_q$ is completely reducible, i.e.

$$N^{\mathbb{F}_q} = V_1 \oplus \cdots \oplus V_f$$

with absolutely irreducible and pairwise non-similar H-modules V_i over $\mathbb{F}_q$. We further obtain from [11, 70.15] that the V_i form an orbit under the operation of the Galois group

$$X := \mathrm{Gal}(\mathbb{F}_q|\mathbb{F}_p) = \langle \xi : \mathbb{F}_q \to \mathbb{F}_q, \ z \mapsto z^p \rangle.$$

Set X_1 the stabilizer of V_1. Since $f = |V_1^X| = \frac{|X|}{|X_1|}$, we see that $X_1 = \langle \xi^f \rangle$.

Theorem 4.11 shows that V_1 is similar to a representation uniquely parametrized by an m-tuple of integers r_i with $0 \le r_i < p$; by abuse of notation set

$$V_1 = (r_0, \dots, r_{m-1}).$$

It follows from the definitions that

$$V_1^{\xi} = (r_{m-1}, r_0, \dots, r_{m-2});$$

thus, the operation of ξ on V_1 induces a cyclic right shift in the parametrization of V_1. If we consider the indices of the parameters r_i modulo m, the property of ξ^f stabilizing V_1 translates into $r_i = r_{i+f}$ for all i; setting $g := \gcd(f, m)$ this condition is equivalent to

$$r_i = r_j \quad \text{if} \quad i \equiv j \mod g.$$

So there exist elements $R_0, \dots, R_{g-1}$ with $0 \le R_i < p$ such that

$$\dim_{\mathbb{F}_q} V_1 = \prod_{i=0}^{m-1} (r_i + 1) = \prod_{i=0}^{g-1} (R_i + 1)^{\frac{m}{g}} = \Big(\underbrace{\prod_{i=0}^{g-1} (R_i + 1)}_{=:J} \Big)^{\frac{m}{g}}$$

and

$$\sum_{i=0}^{m-1} r_i = \frac{m}{g} \sum_{i=0}^{g-1} R_i.$$

Since $\dim_{\mathbb{F}_p} N = \dim_{\mathbb{F}_q} N^{\mathbb{F}_q} = f J^{\frac{m}{g}}$, the condition $n < q^4$ gives

$$n = p^{f J^{\frac{m}{g}}} < p^{4m} \iff f J^{\frac{m}{g}} < 4m \iff \frac{f}{g} J^{\frac{m}{g}} < 4 \frac{m}{g}.$$

Set $a := \frac{f}{g}$ and $b := \frac{m}{g}$; then we have to solve $aJ^b < 4b$. In particular $J > 1$ for otherwise V_1 would be trivial and H would not be faithful on N. Since $a \ge 1$, we get $b < 4$. Therefore only the following cases need to be discussed:

$b = 3$: We have to solve $aJ^3 < 12$; this is only possible for $(a, J) = (1, 2)$. But then

$$2 \nmid \sum r_i = b \sum R_i = b \cdot 1 = 3.$$

This shows that the case does not occur.

$b = 2$: We have to solve $aJ^2 < 8$; this is only possible for $(a, J) = (1, 2)$. It follows $f = g$ and

$$n = p^{f J^b} = p^{g J^b} = p^{4 \cdot \frac{m}{2}} = p^{2m} = q^2.$$

Since $J = 2$, there exists an index i, $0 \le i < \frac{m}{2} = g$, with $r_i = r_{i+g} = 1$ and $r_j = 0$ for all other indices j. Thus, V_1 is similar to the irreducible 4-dimensional representation

$$\psi : \mathrm{PSL}(2, q) \to \mathrm{GL}(4, \mathbb{F}_q), \quad \overline{A} \mapsto \mathfrak{S}_1(A^{\varphi_i}) \otimes \mathfrak{S}_1(A^{\varphi_{i+g}}).$$

Lemma 4.9 shows that for any $\overline{A} \in \mathrm{PSL}(2, q)$ the equality $\mathfrak{S}_1(\overline{A}) = A$ holds; therefore $\psi(\overline{A}) = A^{\varphi_i} \otimes A^{\varphi_{i+g}}$.

In the following we calculate for a given element $\overline{A}$ the dimension of the space of fixed points of $\psi(\overline{A})$. Huppert [25, II 8.1] shows that the centralizer $C_{\mathrm{PSL}(2,q)}(x)$ of any element $\overline{A}$ of order p is elementary abelian of order q. Hence, if $\overline{A} \neq 1$, then either $\overline{A}$ has order p or is p-regular.

First let $|\overline{A}| = p$. We may assume $|A| = p$. Then A is conjugate to $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ in $\mathrm{GL}(2,q)$. Thus, the dimension of the fixed point space of $\psi(\overline{A})$ equals the dimension of the fixed point space of $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \otimes \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ which is 2.

Now let $\overline{A}$ be p-regular. Then $A \in \mathrm{SL}(2,q)$ is also p-regular and can be diagonalized over a suitable extension field of $\mathbb{F}_q$. Denote by λ, λ^{-1} the eigenvalues of A. Due to Ortega [41, 6.3.1] eigenvalues of $\psi(\overline{A})$ are exactly given by the product of eigenvalues of A^{φ_i} with eigenvalues of $A^{\varphi_{i+g}}$; thus,

$$\left(\lambda^{\varphi_i}\lambda^{\varphi_{i+g}}\right)^{\pm 1} \quad \text{and} \quad \left((\lambda^{-1})^{\varphi_i}\lambda^{\varphi_{i+g}}\right)^{\pm 1}$$

are the eigenvalues of $\psi(\overline{A})$. We get

$$(\lambda^{\varphi_i}\lambda^{\varphi_{i+g}}) = 1 \iff (\lambda^{p^g+1})^{p^i} = 1 \iff \lambda^{p^g+1} = 1 \iff |A| \mid p^g + 1$$

and

$$(\lambda^{-1})^{\varphi_i}\lambda^{\varphi_{i+g}} = 1 \iff (\lambda^{p^g-1})^{p^i} = 1 \iff \lambda^{p^g-1} = 1 \iff |A| \mid p^g - 1.$$

Since $g = \frac{m}{2}$, we obtain

$$\dim_{\mathbb{F}_q} \mathrm{Fix}\left(\psi(\overline{A})\right) = \begin{cases} 4 & |\overline{A}| = 1, \\ 2 & |\overline{A}| = p, \\ 2 & \overline{A} \neq 1,\ A^{\sqrt{q}-1} = 1,\ \text{or } A^{\sqrt{q}+1} = 1, \\ 0 & \text{otherwise.} \end{cases}$$

As V_i and V_1 are Galois conjugate, in both modules the dimension of the space of fixed points of $\overline{A}$ is identical. Because $N^{\mathbb{F}_q}$ is the direct sum of all V_i, $h \in H$ fixes exactly one element of N unless

$$\begin{cases} h = 1; & \text{then } h \text{ fixes } q^2 = n \text{ points,} \\ |h| = p; & \text{then } h \text{ fixes } q = \sqrt{n} \text{ points,} \\ h \neq 1 \text{ and } |h| \mid \frac{\sqrt{q}-1}{2} \text{ or } |h| \mid \frac{\sqrt{q}+1}{2}; & \text{then } h \text{ fixes } q = \sqrt{n} \text{ points.} \end{cases}$$

These improved estimations succeed in disproving the genus-0 condition:

Suppose $\mathfrak{p}$ ramifies tamely. As $\gcd(\frac{q+1}{2}, \frac{\sqrt{q}+1}{2}) = \gcd(\frac{q+1}{2}, \frac{\sqrt{q}-1}{2}) = 1$,

$$\mathrm{ind}(\mathfrak{p}) \geq q^2 - \frac{2}{q+1}\Big(q^2 + \big(\frac{q+1}{2} - 1\big) \cdot 1\Big).$$

Together with the estimation for $\mathrm{ind}(\infty)$ from Corollary 3.16 a violation of the genus-0 condition follows.

If $\mathfrak{p}$ ramifies wildly, then the equation

$$\mathrm{ind}(\mathfrak{p}) \geq q^2 - \frac{2}{q(q-1)}\Big(q^2 + \big(\frac{q(q-1)}{2} - 1\big)q\Big) + \frac{2}{q-1}\Big(q^2 - \frac{1}{q}\big(q^2 + (q-1)q\big)\Big)$$

holds. We obtain again a contradiction to the genus-0 condition.

$b = 1$: We have to solve $aJ < 4$; this is only possible for $(a, J) \in \{(1, 2), (1, 3)\}$.

The case $(a, J) = (1, 2)$ cannot occur because $2 \nmid \sum_{i=0}^{m-1} r_i = b \sum_{i=0}^{g-1} R_i = 1$.

In the other case $r_i = 2$ for exactly one index i; all other r_j vanish. We get $m = g = f$ and

$$n = p^{fJ^b} = p^{3m} = q^3.$$

V_1 is similar to the irreducible 3-dimensional representation

$$\psi : \mathrm{PSL}(2, q) \mapsto \mathrm{GL}(3, q), \quad \overline{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \mathfrak{S}_2(A^{\varphi_i}) = \begin{pmatrix} a^2 & 2ab & b^2 \\ ac & ad + bc & bd \\ c^2 & 2cd & d^2 \end{pmatrix}^{\varphi_i}.$$

The dimension of the space of fixed points of $\psi(\overline{A})$ can be determined as shown in the case $b = 2$. We get

$$\dim_{\mathbb{F}_q} \mathrm{Fix}\big(\psi(\overline{A})\big) = \begin{cases} 3 & \overline{A} = 1, \\ 1 & \text{otherwise.} \end{cases} \tag{4.3}$$

Thus, any $h \in H^\sharp$ fixes exactly $\sqrt[3]{n} = q$ points.

These estimations are sufficient in disproving the genus-0 condition.

4.1.8. Case (H): $H \cong \mathrm{PGL}(2, q)$ with $p \neq 2$

This case does not occur, either. We use the same methods as in the previous case.

H is irreducible on N
We use the notation of the corresponding section of case (G).

If $q > 3$, then H contains a unique proper and nontrivial normal subgroup. This group has index 2 in H, is characteristic and isomorphic to $\mathrm{PSL}(2, q)$. We obtain

$$\mathrm{Gal}\big(Z|K(t)\big) \cong M \rtimes F$$

with $F \in \{1, C_2, \mathrm{PGL}(2, q)\}$. The cases $F \cong C_2$ and $F = 1$ are impossible; thus, $F \cong H$.

If $q = 3$, then H is isomorphic to S_4. Every normal subgroup of H is also characteristic in H. Quotient groups of H are isomorphic to 1, S_4, C_2, or S_3. Except for S_4, all of these groups enforce M to be of dimension one. Thus, $\mathrm{Gal}\big(Z|K(t)\big) \cong M \rtimes \mathrm{PGL}(2, 3)$.

Bounds for the number of fixed points for elements of H
An analogue to Lemma 4.7 is

Lemma 4.12 *Suppose $1 \neq h \in H$. Then*

(1) $\dim \mathrm{Fix}(h) \leq \frac{1}{2} \dim N$ *if* $q > 2$, $|h| \neq \{2, 4\}$, *and* $(|h|, q) \neq (3, 9)$,

(2) $\dim \mathrm{Fix}(h) \leq \frac{2}{3} \dim N$ *if* $(|h|, q) = (3, 9)$,

(3) $\dim \mathrm{Fix}(h) \leq \frac{2}{3} \dim N$ *if* $|h| = 4$,

(4) $\dim \mathrm{Fix}(h) \leq \frac{2}{3} \dim N$ *if* $|h| = 2$ *and* $q \notin \{3, 5\}$.

Proof. The commutator subgroup H' of H is a characteristic subgroup of H with $H/H' \cong C_2$ and $H' \cong \mathrm{PSL}(2,q)$. Thus, N considered as a H'-module is semisimple. Let M denote an irreducible H'-submodule of N. Then either

$$N = M \qquad \text{or} \qquad N = M \oplus M^u \text{ with an appropriate } u \in H.$$

H' acts faithfully on M because the kernel of this operation is normal and, hence, characteristic in H' and would be a subgroup of the kernel of the action of H on N.

Lemma 4.7 shows that the bounds for fixed point spaces of H' are linear in the dimension of the module M; thus, these bounds also hold for the module N. Since $h \in H$ fixes less elements of N than $h^2 \in H'$, we can use the bounds for h^2 as bounds for h.

The assumption in case (1) gives $|h^2| > 2$. Therefore Lemma 4.6 yields $\dim \mathrm{Fix}(h) \leq \frac{1}{2} \dim N$. Case (2) can be proved analogously.

Case (4) is a direct consequence from [21]. Case (3) follows from case (4) and some explicit calculations for $q \in \{3,5\}$. ∎

N is a "big" H-module: $n \geq q^4$

Suppose $q \notin \{3,5,9\}$. Then we get from Lemma 4.12

$$|\mathrm{Fix}(h)| \leq \begin{cases} n & h = 1, \\ \frac{n}{q^{\frac{4}{3}}} \leq \frac{n}{q} & |h| \in \{2,4\}, \\ \frac{n}{q^2} & \text{otherwise.} \end{cases}$$

First we discuss the case where $\mathfrak{p}$ ramifies tamely with index $q+1$. Then

$$\mathrm{ind}(\infty) \geq (n-1)\big(1 + \frac{1}{q-1}\big).$$

$I_{\mathfrak{p}}$ is a cyclic group and contains therefore a unique involution and at most two elements of order 4. We get

$$\mathrm{ind}(\mathfrak{p}) \geq n - \frac{1}{q+1}\big(n + 3\frac{n}{q^{\frac{4}{3}}} + (q-3)\frac{n}{q^2}\big).$$

This gives

$$\mathrm{ind}(\infty) + \mathrm{ind}(\mathfrak{p}) - 2n + 2 \geq \frac{q^2(q+1)(q-2) + n(q^2 - 3q^{\frac{5}{3}} + 4q + 3q^{\frac{2}{3}} - 3)}{q^2(q^2-1)};$$

as $q^2 - 3q^{\frac{5}{3}} + 4q + 3q^{\frac{2}{3}} - 3$ is positive for all possible q, the genus-0 condition is violated.

Now suppose $\mathfrak{p}$ ramifies wildly. Then $I_\infty \cong N \rtimes C_{q+1}$. By Lemma 4.8 $I_{\mathfrak{p}}$ contains at most q involutions and $2q$ elements of order four. Using the same techniques as above gives again a contradiction.

The cases $q \in \{3,5\}$ can be disproved analogously; the number of fixed points of elements that is not dealt with in Lemma 4.12 can be estimated with $\frac{n}{p} = \frac{n}{q}$.

For $q = 9$ the same methods induce a contradiction to the genus-0 condition.

N is a "small" module: $n < q^4$

We use Theorem 4.11 to classify all possible H-modules N with $n < q^4$. In this section the same notation is used as in the corresponding section of case (G).

V_1 can be parametrized by

$$V_1 = (s; r_0, \dots, r_{m-1}).$$

The action of ξ on V_1 gives

$$V_1^\xi = (sp; r_{m-1}, r_0, \dots, r_{m-2}).$$

As ξ^f stabilizes V_1, the parameters must fulfill

$$sp^f \equiv s \mod (q-1) \qquad \text{and} \qquad r_i = r_j \quad \text{if} \quad i \equiv j \mod g.$$

Thus, there exist elements $R_0, \dots, R_{g-1}$ with $0 \le R_i < p$ such that

$$\dim_{\mathbb{F}_q} V_1 = J^{\frac{m}{g}} \quad \text{and} \qquad \sum_{i=0}^{m-1} r_i = \frac{m}{g} \sum_{i=0}^{g-1} R_i.$$

V_1 being a faithful H-module gives $J > 1$; the equation

$$p^{\dim_{\mathbb{F}_p} N} = p^{\dim_{\mathbb{F}_q} N^{\mathbb{F}_q}} = p^{fJ^{\frac{m}{g}}} < q^4 \iff aJ^b < 4b$$

enforces again $b < 4$. So, we have to discuss the following cases:

$b = 3$: We obtain the unique solution $(a, J) = (1, 2)$. This gives an index $0 \le i < g$ with $r_i = r_{i+g} = r_{i+2g} = 1$; all other r_j vanish. As p is odd, the sum $\sum_{i=0}^{m-1} r_i p^i$ is also odd. But the even number $q-1$ cannot divide $2s + \sum_{i=0}^{m-1} r_i p^i$. This contradiction to Theorem 4.11 shows that this case is impossible.

$b = 2$: We obtain the unique solution $(a, J) = (1, 2)$. We further get $f = g$ and $2g = m$. The condition for s translates to

$$p^{2g} - 1 \mid sp^g - s = s(p^g - 1) \iff p^g + 1 \mid s;$$

so, $s = \ell \cdot (p^g + 1)$. We further get the existence of an index $0 \le i < g$ with $r_i = r_{i+g} = 1$ and $r_j = 0$ for all other indices. The restriction from Theorem 4.11 shows

$$p^{2g} - 1 \mid 2\ell(p^g + 1) + p^i + p^{i+g} = (p^g + 1)(2\ell + p^i) \iff p^g - 1 \mid 2\ell + p^i.$$

This is impossible since $p^g - 1$ is even while $2\ell + p^i$ is not.

$b = 1$: In this case we have $a = 1$, $m = f = g$, and $J \in \{2, 3\}$.

$J = 2$ is impossible for $\sum r_i p^i$ is odd.

So the remaining case is $J = 3$. We obtain $n = q^3$; the action of $\mathrm{PGL}(2, q)$ on V_1 is given by

$$\psi : \mathrm{PGL}(2, q) \to \mathrm{GL}(3, q), \quad \overline{A} \mapsto (\det A)^s \mathfrak{S}_2(A^{\varphi_i}). \tag{4.4}$$

s has to fulfill

$$q - 1 \mid 2s + 2p^i \iff \frac{q-1}{2} \mid s + p^i \iff s \equiv -p^i \mod \frac{q-1}{2};$$

as $0 \leq s < q-1$, this congruence gives two different solutions for s.

Note that the restriction of ψ to $\mathrm{PSL}(2,q) \trianglelefteq \mathrm{PGL}(2,q)$ coincides with the irreducible representation of the corresponding section of case (G). We use this fact to transfer results from equation (4.3) on page 37 to this case.

An element of order p has a one-dimensional fixed point space because its image is similar to $\psi\left(\left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]\right)$.

Let $\overline{A} \in \mathrm{PGL}(2,q)$ be a p-regular element of order $\neq 2$. Then $1 \neq \overline{A}^2 \in \mathrm{PSL}(2,q)$; equation (4.3) shows that the fixed point space of $\psi(\overline{A})$ is at most one-dimensional.

At last suppose $\overline{A} \in \mathrm{PGL}(2,q)$ is an involution. As ψ is faithful, $\psi(\overline{A})$ is at most two-dimensional.

These bounds again induce contradictions to the genus-0 condition in all cases.

4.1.9. Case (I): $H \cong \mathrm{PGL}(2,2^m)$

Suppose $q = 2$. Then $H \cong D_3$ and the ramification data is $(2,3)$. This situation has already been described in case (D).

Hence, we will assume $q \neq 2$ from now on. Then H is simple with $H \cong \mathrm{SL}(2,2^m)$. By Lemma 4.4 N is an irreducible H-module.

The "big" cases can be disproved essentially the same way as in case (G) and (H). The "small" cases are more complicated. V_1 is an irreducible $\mathrm{PGL}(2,2^m)$-module induced by

$$\psi_1 : \mathrm{PGL}(2,2^m) \to \mathrm{GL}(2,2^m), \quad \overline{A} \mapsto (\det A)^s \cdot A^{\varphi_i},$$

here $n = q^2$; or

$$\psi_2 : \mathrm{PGL}(2,2^m) \to \mathrm{GL}(4,2^m), \quad \overline{A} \mapsto (\det A)^s \cdot \left(A^{\varphi_i} \otimes A^{\varphi_{i+\frac{m}{2}}}\right),$$

here $n = q^2$ and m is even with $0 \leq i < \frac{m}{2}$; or

$$\psi_3 : \mathrm{PGL}(2,2^m) \to \mathrm{GL}(8,2^m), \quad \overline{A} \mapsto (\det A)^s \cdot \left(A^{\varphi_i} \otimes A^{\varphi_{i+\frac{m}{3}}} \otimes A^{\varphi_{i+2\cdot\frac{m}{3}}}\right)$$

here $n = q^{\frac{8}{3}}$ and $3 \mid m$ with $0 \leq i < \frac{m}{3}$. In all cases s is uniquely determined; we have $\det\left(\psi_i(\overline{A})\right) = 1$ for all $\overline{A} \in \mathrm{PGL}(2,2^m)$.

With the same methods as before it is possible to determine the dimension of the space of fixed points of the image of $\overline{A} \in \mathrm{PGL}(2,2^m)$ under ψ_i. We obtain

$$\dim \mathrm{Fix}\left(\psi_1(\overline{A})\right) = \begin{cases} 2 & \psi_1(\overline{A}) = 1, \\ 1 & \psi_1(\overline{A}) \text{ is an involution}, \\ 0 & \text{otherwise}; \end{cases}$$

$$\dim \mathrm{Fix}\left(\psi_2(\overline{A})\right) = \begin{cases} 4 & \psi_2(\overline{A}) = 1, \\ 2 & |\psi_2(\overline{A})| = 2 \text{ or } |\psi_2(\overline{A})| \mid \sqrt{q}+1 \text{ or } |\psi_2(\overline{A})| \mid \sqrt{q}-1 \\ 0 & \text{otherwise}; \end{cases}$$

$$\dim \mathrm{Fix}\left(\psi_3(\overline{A})\right) \leq \begin{cases} 8 & \psi_3(\overline{A}) = 1, \\ 4 & \psi_3(\overline{A}) \text{ is an involution}, \\ 2 & \text{otherwise}. \end{cases}$$

These bounds imply a contradiction to the genus-0 condition in all cases.

4.2. $g = 1$

In this section we suppose E to be a genus-one function field. As the field of constants of E is algebraically closed, it is the function field of an elliptic curve. We will prove

Theorem 4.13 *With the notation from page 23 there is no affine polynomial f such that $g(E) = 1$.*

4.2.1. Ramification in $E|K(t)$

Before we describe the structure of $\mathrm{Aut}_K(E)$ we remind the reader that the set of places $\mathcal{P}(E)$ of E can be canonically interpreted as an abelian group; we will denote its zero element by $\mathfrak{o}$. Hasse [23] shows that every K-automorphism of E acts on $\mathcal{P}(E)$ and, conversely, if any operation on $\mathcal{P}(E)$ induces an automorphism of E, then this automorphism is uniquely determined. In particular, the translation mappings

$$\tau_{\mathfrak{a}} : \mathcal{P}(E) \to \mathcal{P}(E), \qquad \mathfrak{p} \mapsto \mathfrak{p} + \mathfrak{a}$$

induce *translation automorphisms* in $\mathrm{Aut}_K(E)$. We denote the set of translation automorphisms by $\mathfrak{T}$; this set is closed under composition and forms a normal subgroup in $\mathrm{Aut}_K(E)$.

Denote by $\mathfrak{I}$ the stabilizer of $\mathfrak{o}$ in $\mathrm{Aut}_K(E)$. Then $\mathfrak{I}$ is a finite group of homomorphisms $\mathcal{P}(E) \to \mathcal{P}(E)$ and the set of K-automorphisms of E can be written as

$$\mathrm{Aut}_K(E) = \mathfrak{T} \rtimes \mathfrak{I}. \tag{4.5}$$

A first consequence is

Lemma 4.14 *Suppose $\sigma = \tau_{\mathfrak{a}} \cdot \xi$ with $\tau_{\mathfrak{a}} \in \mathfrak{T}$ and $\xi \in \mathfrak{I}$ fixes a place $\mathfrak{P} \in \mathcal{P}(E)$. Then:*

(1) $\sigma \in \big(\mathrm{Aut}_K(E) \setminus \mathfrak{T}\big) \cup 1$.

(2) For any $\mathfrak{Q} \in \mathcal{P}(E)$ and $r \in \mathbb{N}$ we have $\mathfrak{Q}^{\sigma^r} = \mathfrak{Q}^{\xi^r} + \sum_{i=1}^{r} \mathfrak{a}^{\xi^i}$. In particular, σ has order $|\xi|$.

Proof. σ fixes $\mathfrak{P}$. No nontrivial translation automorphism has this property. This is (1).

The equation for $\mathfrak{Q}^{\sigma^r}$ follows by induction and the fact that elements of $\mathfrak{I}$ are homomorphisms of the group $\mathcal{P}(E)$.

$\sigma^{|\xi|}$ maps $\mathfrak{P}$ to $\mathfrak{P} + \sum_{i=1}^{|\xi|} \mathfrak{a}^{\xi^i}$. As every power of σ stabilizes $\mathfrak{P}$, it follows $\sum_{i=1}^{|\xi|} \mathfrak{a}^{\xi^i} = \mathfrak{o}$. Thus, $\sigma^{|\xi|} = 1$ and $|\xi|$ is the smallest positive integer with this property. ∎

The isomorphism types for $\mathfrak{I}$ are determined in Husemöller [27, Chapter 3]; the following cases occur:

$\mathfrak{I} \cong$	Conditions
C_2	
C_4	$p \notin \{2, 3\}$
C_6	$p \notin \{2, 3\}$
$C_3 \rtimes C_4$	$p = 3$, $\mathfrak{I}$ non-abelian
$\mathrm{SL}(2, 3)$	$p = 2$

This allows us to work out how places can ramify in the extension $E|K(t)$.

Lemma 4.15 *Let $\mathfrak{p} \in \mathcal{P}\big(K(t)\big)$ be any place of $K(t)$. Suppose $\mathfrak{P} \in \mathcal{P}(E)$ lies over $\mathfrak{p}$. Denote the inertia group of the extension $\mathfrak{P}|\mathfrak{p}$ with $F_\mathfrak{p}$ and the degree of the different coming from the ramification of $\mathfrak{p}$ with $\delta_\mathfrak{p}$. Set s resp. s_k the number of groups in the series $\big(F_\mathfrak{p}(i)\big)_{i\geq 1}$ of order $\neq 1$ resp. order $\frac{|F_\mathfrak{p}(1)|}{p^{k-1}}$. Suppose $|F_\mathfrak{p}| > 1$. Then:*

$\mathfrak{I} \cong$	$F_\mathfrak{p} \cong$	$\delta_\mathfrak{p} =$	*Conditions*
C_2	C_2	$\frac{1}{2}\lvert H\rvert$	$p \neq 2$
	C_2	$\frac{1}{2}\lvert H\rvert \cdot (1+s)$	$p = 2$
C_4	C_2	$\frac{1}{2}\lvert H\rvert$	
	C_4	$\frac{3}{4}\lvert H\rvert$	
C_6	C_2	$\frac{1}{2}\lvert H\rvert$	
	C_3	$\frac{2}{3}\lvert H\rvert$	
	C_6	$\frac{5}{6}\lvert H\rvert$	
$C_3 \rtimes C_4$	C_2	$\frac{1}{2}\lvert H\rvert$	
	C_4	$\frac{3}{4}\lvert H\rvert$	
	C_3	$\frac{1}{3}\lvert H\rvert \cdot (2+2s)$	
	C_6	$\frac{1}{6}\lvert H\rvert \cdot (5+2s)$	
	$C_3 \rtimes C_4$	$\frac{1}{12}\lvert H\rvert \cdot (11+2s)$	
$\mathrm{SL}(2,3)$	C_2	$\frac{1}{2}\lvert H\rvert \cdot (1+s)$	
	C_3	$\frac{2}{3}\lvert H\rvert$	
	C_4	$\frac{1}{4}\lvert H\rvert \cdot (3+3s_1+s_2)$	$s_1 \geq 1,\ s_2 \geq 1$
	C_6	$\frac{1}{6}\lvert H\rvert \cdot (5+s)$	
	Q_8	$\frac{1}{8}\lvert H\rvert \cdot (7+7s_1+3s_2+s_3)$	$s_1 \geq 1,\ s_2+s_3 \geq 1$
	$\mathrm{SL}(2,3)$	$\frac{1}{24}\lvert H\rvert \cdot (23+7s_1+3s_2+s_3)$	$s_1 \geq 1,\ s_2+s_3 \geq 1$

Proof. The decomposition (4.5) of $\mathrm{Aut}_K(E)$ proves the existence of a group $F \leq \mathfrak{I}$ such that $\mathfrak{T}F_\mathfrak{p} = \mathfrak{T}F$. By Lemma 4.14 $F_\mathfrak{p} \cap \mathfrak{T} = 1$; thus,

$$F_\mathfrak{p} \cong \mathfrak{T}F_\mathfrak{p}/\mathfrak{T} = \mathfrak{T}F/\mathfrak{T} \cong F.$$

Hence, $F_\mathfrak{p}$ embeds into $\mathfrak{I}$. ∎

We obtain an analogue to Theorem 4.3:

Theorem 4.16 *The following table gives the possible ramification behavior in the extension $E|K(t)$:*

Case	$\mathfrak{I} \cong$	*Ramification Data*	*Conditions*
(A1)	$C_3 \rtimes C_4$	*(2,6)*	$s = 2$
(A2)		*(4,12)*	$s = 2$
(B1)	$\mathrm{SL}(2,3)$	*(2,6)*	$s = 1$ *for both places*
(B2)		*(3,6)*	$s = 3$
(B3)		*(3,24)*	$s_1 = 1,\ s_2 = 0,\ s_3 = 2$
(B4)		*(6,6)*	$s = 1$ *for both places*
(B5)		*(6)*	$s = 7$
(B6)		*(24)*	$25 = 7s_1 + 3s_2 + s_3$

Proof. The proof is rather combinatorial; we use the genus formula of Riemann-Hurwitz together with the ramification data from Lemma 4.15 to ensure the correct genus of E.

Some combinations, however, cannot occur although they formally satisfy the different-condition. This is the case if too many places ramify (Lemma 3.21), or more than one place ramifies and all ramification groups are p-groups (Corollary 3.16), or only ∞ ramifies, I_∞ is a p-group, and the second ramification group of ∞ in the extension $E|K(t)$ does not vanish (Corollary 3.11). These criteria exclude in particular all cases where $\mathfrak{I}$ is a cyclic group.

As an example we discuss the case $\mathfrak{I} \cong C_2$. If $p \neq 2$ is odd, then the extension $E|K(t)$ is tame and the degree of the different of each branch point equals $\frac{1}{2}|H|$. Riemann-Hurwitz states

$$2g - 2 = 0 = -2|H| + a \cdot \frac{1}{2}|H|$$

with a being the number of branch points of $E|K(t)$. Hence, $a = 4$; but this contradicts Lemma 3.21.

Suppose $p = 2$. Lemma 3.18 shows that ∞ ramifies in the extension $E|K(t)$; Corollary 3.16 gives $F_\infty(0) = F_\infty(1) = C_2 > F_\infty(2) = 1$ and the nonexistence of any finite branch point. By Riemann-Hurwitz

$$2g - 2 = 0 = -2|H| + \frac{1}{2}|H| \cdot (1 + 1) = -|H| \iff |H| = 0;$$

but this is impossible. ∎

4.2.2. Cases in odd characteristic $p > 2$

We only disprove case (A2); the same methods also work for case (A1).

Suppose $\mathfrak{p}$ ramifies with index 12. Then $\operatorname{ind}(\infty) \geq \frac{5}{4}(n-1)$ and

$$\operatorname{ind}(\mathfrak{p}) \geq n - \frac{1}{12}\big(n + 11\frac{n}{3}\big) + 2 \cdot \frac{1}{4}\Big(n - \frac{1}{3}\big(n + 2 \cdot \frac{n}{3}\big)\Big) = \frac{5}{6}n.$$

But now $\operatorname{ind}(\infty) + \operatorname{ind}(\mathfrak{p}) > 2n - 2$.

Thus, $I_\mathfrak{p} \cong C_4$. Section 3.2.1 gives

$$\operatorname{ind}(\infty) \geq \frac{5}{4}(n-1) + \frac{1}{4}\big(n - \frac{n}{3}\big).$$

Furthermore

$$\operatorname{ind}(\mathfrak{p}) = n - \frac{1}{4}(n + f_2 + 2f_4)$$

where f_i denotes the number of fixed points of an element of order i in $I_\mathfrak{p}$. As $\operatorname{ind}(\mathfrak{p}) \in \mathbb{N}$, the impossibility of $f_2 = \frac{n}{3}$ follows. Hence, $f_2 \leq \frac{n}{9}$ and, thus, $f_4 \leq f_2 \leq \frac{n}{9}$.

These bounds induce a contradiction to the genus-0 condition.

4.2.3. Cases in even characteristic $p = 2$

Supersingularity

As $\operatorname{Aut}\big(\mathcal{P}(E)\big) \cong \mathrm{SL}(2,3)$, by Silverman [46, V §3] E is the function field of a supersingular elliptic curve. [46, V 3.1] gives some properties of such curves; for us most important is

Lemma 4.17 *There does not exist $\mathfrak{p} \in \mathcal{P}(E)$ with $\mathfrak{p} \neq \mathfrak{o}$ and $2 \cdot \mathfrak{p} = \mathfrak{o}$.*

For the following we identify H with the Galois group of $E|K(t)$. Then, a first consequence of the above lemma is

Lemma 4.18 *Suppose $h \in H$ is an involution. Then h fixes either no place or exactly one place of E.*

Proof. h can be written as a product $h = \tau\xi$ with $\tau \in \mathfrak{T}$ and $\xi \in \mathfrak{I}$.

If $\xi = 1$, then the assertion follows immediately.

Thus, by Lemma 4.14 $\xi \neq 1$ is the unique involution in $\mathfrak{I} \cong \mathrm{SL}(2,3)$. ξ acts on $\mathcal{P}(E)$ by inversion, i.e. every place $\mathfrak{p}$ of E is mapped to $-\mathfrak{p}$. Suppose h fixes the places $\mathfrak{p}, \mathfrak{q} \in \mathcal{P}(E)$. Then

$$\mathfrak{p}^h - \mathfrak{p} = \mathfrak{o} = \mathfrak{q}^h - \mathfrak{q} \iff \mathfrak{p}^\xi - \mathfrak{p} = \mathfrak{q}^\xi - \mathfrak{q} \iff 2 \cdot (\mathfrak{p} - \mathfrak{q}) = \mathfrak{o}$$

and we get $\mathfrak{p} = \mathfrak{q}$ by Lemma 4.17. ∎

Now we are able to state the main observation of this section

Proposition 4.19 *Let $i \in H$ be an involution that fixes the place $\mathfrak{P} \in \mathcal{P}(E)$. Then there exists a bijection between the set i^H of H-conjugates of i and the set $\mathfrak{P}^H$ of places over $\mathfrak{p} := \mathfrak{P} \cap K(t)$.*

In particular, the normalizer $N_H(\langle i \rangle)$ of $\langle i \rangle$ in H equals the inertia group $F_\mathfrak{p}$ of $\mathfrak{P}|\mathfrak{p}$.

Proof. As $F_\mathfrak{p}$ embeds into $\mathfrak{I} \cong \mathrm{SL}(2,3)$, i is the unique involution in $F_\mathfrak{p}$. Therefore $\langle i \rangle$ is normal in $F_\mathfrak{p}$; hence, $F_\mathfrak{p} \leq N_H(\langle i \rangle)$.

Let $\mathfrak{Q} \in \mathfrak{P}^H$ be another place lying over $\mathfrak{p}$. Then the inertia group of $\mathfrak{Q}|\mathfrak{p}$ is conjugate to $F_\mathfrak{p}$ and, thus, contains exactly one involution from the set i^H. Since every involution in i^H fixes exactly one place of E, the equality $|i^H| = |\mathfrak{P}^H|$ holds.

The equation

$$|i^H| = \frac{|H|}{|N_H(\langle i \rangle)|} = \frac{|H|}{|F_\mathfrak{p}|} = |\mathfrak{P}^H|$$

shows $|N_H(\langle i \rangle)| = |F_\mathfrak{p}|$. ∎

Corollary 4.20 *In cases (B3) and (B6) a 2-Sylow subgroup of H is isomorphic to a quaternion group of order 8. In the remaining cases a 2-Sylow subgroup of H is isomorphic to C_2.*

Proof. We start with cases (B3) and (B6). Let $F \leq H$ be an inertia group of order 24, $S \leq F$ the unique 2-Sylow subgroup of F, and $Z := Z(F) \leq S$ the center of F. Proposition 4.19 shows

$$F \leq N_H(S) \leq N_H(Z) = F;$$

as $2 \nmid [N_H(S) : S]$, S is a 2-Sylow subgroup of H. Since F is isomorphic to $\mathrm{SL}(2,3)$, the isomorphism type of S follows for instance from [32, 8.6.10].

The remaining cases can be proved similarly. ∎

Cases (B1) and (B4)
In both cases a 2-Sylow subgroup of H has order 2; thus, the set of involutions of H forms a conjugacy class of H. By Theorem 4.16 two different places of $K(t)$ ramify with even index; therefore an involution of H fixes more than one place of E. This contradicts Lemma 4.18.

Case (B2)
This case can be disproved by using the estimations for $\mathrm{ind}(\infty)$ and $\mathrm{ind}(\mathfrak{p})$.

Case (B3)
This case does not occur.

The estimations for $\mathrm{ind}(\infty)$ and $\mathrm{ind}(\mathfrak{p})$ show the impossibility of $I_\mathfrak{p} \cong \mathrm{SL}(2,3)$. Hence,

$$\mathrm{ind}(\infty) \geq \frac{4}{3}(n-1) + 2 \cdot \frac{2}{24}\Big(n - \frac{n}{2}\Big)$$

and $\mathrm{ind}(\mathfrak{p}) = n - \frac{1}{3}(n + 2f_3)$ with f_3 being the number of fixed points of a generator of the cyclic group $I_\mathfrak{p}$. The genus-0 condition and $\mathrm{ind}(\mathfrak{p})$ being an integer give $f_3 = \frac{n}{4}$.

A more detailed description of H is given by

Lemma 4.21 *H contains a characteristic and abelian subgroup J such that $H = J \rtimes F_\infty$ and $J \cap F_\mathfrak{p} = 1$. Let $Q \leq F_\infty$ denote a 2-Sylow subgroup of H. Then $F := \langle Q^h \mid h \in H\rangle = J \rtimes Q$ is a Frobenius group with Frobenius kernel J and complement Q; $[H : F] = 3$. F is also characteristic in H.*

Proof. Let J denote a maximal normal subgroup of H of odd order. As Q is isomorphic to a quaternion group of order 8, a theorem of Brauer/Suzuki ([25, V 22.9] or [4]) states that the center of H/J is cyclic of order two. Therefore H contains another normal subgroup $\tilde{J}$ with $[\tilde{J} : J] = 2$.

Remember our identification of H with the Galois group of $E|K(t)$ and set $Y := \mathrm{Fix}(J)$, $Z := \mathrm{Fix}(\tilde{J})$.

Suppose the extension $E|Y$ is ramified. Then $g(Y) = 0$ and Y is a rational function field. Since J has odd order, the inertia group of a place of Y lying over ∞ contains a quaternion group of order 8 in contradiction to the classification [50] of $\mathrm{Aut}_K\big(Y|K(t)\big)$.

Hence, $E|Y$ is unramified with $g(Y) = 1$; this shows in particular that $J \cap F_\mathfrak{p} = 1$. Furthermore by [46, III §4] we may assume J to be the set of automorphisms of E coming from the kernel of an isogeny $E \to Y$; thus, J is abelian. As $8 \nmid [H : \tilde{J}]$, the extension $Y|Z$ is ramified; every branch point of Z ramifies totally with index 2 and adds 4 to the degree of the different of $Y|Z$. Hence, exactly one place ramifies in $Y|Z$. As this place lies over ∞, the classification [50] of $\mathrm{Aut}_K\big(Z|K(t)\big)$ yields $\mathrm{Gal}\big(Z|K(t)\big) \cong A_4$. We obtain that ∞ ramifies totally in the extension $Y|K(t)$ with $\mathrm{Gal}\big(Y|K(t)\big) \cong \mathrm{SL}(2,3) \cong F_\infty$. By Herbrand F_∞ is a complement of J in H.

Proposition 4.19 shows that J is regular on the set of H-conjugates of Q (by conjugation); hence, $F \leq J \rtimes Q$. Since F is transitive on its 2-Sylow subgroups, the equality $F = J \rtimes Q$ holds. As $J > 1$ by Proposition 2.8, the remaining assertions follow as Q is selfnormalizing in F. ∎

Next we classify all absolutely irreducible $\mathbb{F}_2$-modules of F. Our main tool for this is the representation theory of Frobenius groups. The following proposition states the results for the convenience of the reader. A short and elegant proof can be found in Guralnick [16].

Proposition 4.22 *Let $F = J \rtimes Q$ be a Frobenius group with Frobenius kernel J and complement Q. Suppose K to be an algebraically closed field.*

(1) Q acts semiregularly on the set of isomorphism classes of nontrivial irreducible $K[J]$-modules.

(2) If V is an irreducible $K[F]$-module, then either $C_V(J) = V$ or there exists an absolutely irreducible nontrivial $K[J]$-module W such that $V \cong W^F$ is isomorphic to the induced $K[F]$-module W^F.

We use this proposition to get

Proposition 4.23 *Let V be an irreducible H-submodule of $N^K := N \otimes K$. Then V is 8-dimensional. If $t \in F_\mathfrak{p}$ has order 3, then the space of fixed points of t on V is at most 4-dimensional.*

Proof. Let Q, F, and J be defined as in Lemma 4.21.

Since $F \trianglelefteq H$, the F-module V is semisimple and can be written as a direct sum $V = \bigoplus_{i=1}^{s} V_i$ of irreducible F-modules $1 \neq V_i \leq V$. We use Proposition 4.22 to clarify the structure of V_1: As J is normal in U, the case $C_{V_1}(J) = V_1$ is impossible. Hence, V_1 is isomorphic to an absolutely irreducible and nontrivial J-module W induced to F. The commutativity of J gives $\dim_K W = 1$; since $[F : J] = 8$, it follows $\dim_K V_1 = 8$.

Because $\langle F, t\rangle = H$, the group $F_\mathfrak{p}$ is transitive on the V_i; therefore either $V = V_1$ is an irreducible F-module or $V = V_1 \oplus V_1^t \oplus V_1^{t^2}$. We show that the second case is impossible. V_1 intersects the space $\mathrm{Fix}(t)$ of fixed points of t trivially for otherwise $V_1 \cap V_1^t \neq 0$. But then the dimension formula for vector spaces gives

$$\underbrace{\dim_K \mathrm{Fix}(t)}_{=r-2} + \dim_K V_1 = \underbrace{\dim_K\big(\mathrm{Fix}(t) + V_1\big)}_{\leq r} + \underbrace{\dim_K\big(\mathrm{Fix}(t) \cap V_1\big)}_{=0};$$

hence, the contradiction $\dim_K V_1 \leq 2$ follows. This gives $\dim_K V = 8$.

By Lemma 4.21 t can be written as a product $t = jw$ with $j \in J$ and $w \in F_\infty$ being of order 3. As the abelian group J is normal in H, the J-module V is a direct sum of eight one-dimensional J-submodules $M_1, \ldots, M_8$ that are permuted transitively by F_∞. Hence, $Q \trianglelefteq F_\infty$ acts regularly on the modules M_i.

Suppose $n \in N^\sharp$ generates M_1. By proper identification of the integers $1, \ldots, 8$ with the modules M_i the action of w on the set $\{M_1, \ldots, M_8\}$ is described by the permutation $\omega := (1)(2)(3,4,5)(6,7,8)$. Set q_i the well-defined element of Q that maps M_1 to the module belonging to the integer i. Then

$$V = \bigoplus_{i=1}^{8} \langle n^{q_i}\rangle \qquad \text{and} \qquad \langle n^{q_i}\rangle^w = \langle n^{q_{i\omega}}\rangle.$$

It follows that there exist elements $c_i \in K^\sharp$ with $(n^{q_i})^{jw} = c_i \cdot n^{q_{i\omega}}$. Suppose $v := \sum_{i=1}^{8} \lambda_i n^{q_i} \in V$. Then

$$v^t = v^{jw} = \sum_{i=1}^{8} \lambda_i c_i n^{q_{i\omega}} = \sum_{i=1}^{8} \lambda_{i\omega^{-1}} c_{i\omega^{-1}} n^{q_i}.$$

Hence, v is fixed by t if and only if $\lambda_i = \lambda_{i^{\omega-1}} c_{i^{\omega-1}}$ for all $1 \le i \le 8$. Solving these equations shows that $\mathrm{Fix}(t)$ is at most 4-dimensional. ∎

The above proposition gives $r = 8s$ with $s \in \mathbb{N}$ and $\dim \mathrm{Fix}(t) \le \frac{r}{2}$; thus, $\dim \mathrm{Fix}(t) = r - 2$ is impossible.

Case (B5)
By Corollary 4.20 the order of H is $2u$ with $2 \nmid u$. Therefore H contains a normal subgroup J of index 2. In the extension $E|\mathrm{Fix}(J)$ exactly one place ramifies tamely with index 3. But this gives a contradiction to the Riemann-Hurwitz genus formula.

Case (B6)
This case is impossible, too.

The idea of Lemma 4.21 can be used to obtain a contradiction in this case. With the notation of this lemma we get eventually that $Z|K(t)$ is an Galois extension of rational function fields with the unique branch point ∞. The classification of Valentini and Madan [50] shows that the ramification index of ∞ in $Z|K(t)$ has to be a power of 2. This, however, is impossible as $E|Y$ is unramified.

Remark 4.24 This case can also be disproved without using the theorem of Brauer-Suzuki: A discussion of the ramification behavior of $E|\mathrm{Fix}(F_\infty)$ shows that in this extension exactly one place ramifies. Hence, the intersection of F_∞ with any different conjugate is trivial. Since F_∞ is selfnormalizing in H, the group H is a Frobenius group with Frobenius complement F_∞. Now, the same considerations as above lead to a contradiction. ⋆

4.3. $g = 2$

In this section we assume E to be a function field of genus two. Schmid [42] shows that $\mathrm{Aut}_K(E)$ is a finite group. Let F denote the fixed field of all K-automorphisms of E. Then $E|F$ is Galois with $\mathrm{Gal}(E|F) = \mathrm{Aut}_K(E)$.

Stichtenoth [47, VI.2] shows that E is the function field of a hyperelliptic curve. Thus, $E|F$ contains a unique intermediate rational field R with $[E : R] = 2$. The uniqueness of R shows that the extension $R|F$ is Galois. The central involution $\imath \in \mathrm{Aut}_K(E)$ that corresponds to R by Galois duality is called *the hyperelliptic involution of* E.

We will prove

Theorem 4.25 *With the notation from page 23 suppose $g = 2$. Then $p = 3$ and $A = G = \mathrm{AGL}(2, 3)$. f is not exceptional. Examples of f are given by the* AGL*-polynomials of chapter 5.*

4.3.1. Cases in odd characteristic $p > 2$

The K-automorphisms for genus-two hyperelliptic function fields are well-known. Due to Geyer [15], Igusa [28], or Shaska/Völklein [45] only the following isomorphism types can occur:

$\mathrm{Aut}_K(E) \cong$	Conditions
C_2	
C_{10}	$p \neq 5$
D_2	
D_4	
D_6	
$C_3 \rtimes D_4$	$p \notin \{3,5\}$, $\mathrm{Aut}_K(E)$ non-abelian
$\mathrm{GL}(2,3)$	$p \neq 5$
Σ_5	$p = 5$

Here Σ_5[1] denotes a non-split extension of C_2 by S_5 where the transpositions of S_5 lift to involutions, cf. [45]. Σ_5 is unique up to isomorphism.

Lemma 4.1 and our main assumption $p \neq 2$ show that $\mathrm{Aut}_K(E)$ cannot be isomorphic to C_2, C_{10}, D_2, D_4, or $C_3 \rtimes D_4$.

As a subgroup of D_6 either is a $3'$-group or contains a characteristic subgroup isomorphic to C_3, Proposition 2.8 gives the impossibility of $\mathrm{Aut}_K(E) \cong D_6$.

Case $\mathrm{Aut}_K(E) \cong \mathrm{GL}(2,3)$

Assume $\mathrm{Aut}_K(E) \cong \mathrm{GL}(2,3)$; then $p = 3$.

Lemma 4.1, Proposition 2.9, and Proposition 2.8 force H to be isomorphic to $\mathrm{SL}(2,3)$ or $\mathrm{GL}(2,3)$. A survey of the subgroups of these groups gives

Lemma 4.26 *Let $\mathfrak{p} \in \mathcal{P}\big(K(t)\big)$ be any place of $K(t)$. Suppose $\mathfrak{P} \in \mathcal{P}(E)$ lies over $\mathfrak{p}$. Denote the inertia group of the extension $\mathfrak{P}|\mathfrak{p}$ with $F_\mathfrak{p}$ and the degree of the different coming from the ramification of $\mathfrak{p}$ with $\delta_\mathfrak{p}$. Denote by s the well-defined integer with $F_\mathfrak{p}(s) > F_\mathfrak{p}(s+1) = 1$. Suppose $|F_\mathfrak{p}| > 1$. Then:*

$H \cong$	$F_\mathfrak{p} \cong$	$\delta_\mathfrak{p}$
$\mathrm{SL}(2,3)$	C_2	$\frac{1}{2}\lvert H\rvert$
	C_4	$\frac{3}{4}\lvert H\rvert$
	C_3	$\frac{1}{3}\lvert H\rvert \cdot (2+2s)$
	C_6	$\frac{1}{6}\lvert H\rvert \cdot (5+2s)$
$\mathrm{GL}(2,3)$	C_2	$\frac{1}{2}\lvert H\rvert$
	C_4	$\frac{3}{4}\lvert H\rvert$
	C_8	$\frac{7}{8}\lvert H\rvert$
	C_3	$\frac{1}{3}\lvert H\rvert \cdot (2+2s)$
	C_6 *or* D_3	$\frac{1}{6}\lvert H\rvert \cdot (5+2s)$

We use this lemma to solve the Riemann-Hurwitz equation

$$2 = -2|H| + \sum_{\mathfrak{p}} \delta_\mathfrak{p}$$

where $\mathfrak{p}$ runs through all places of $K(t)$ ramifying in $E|K(t)$. We obtain the following

Theorem 4.27 *The following table gives the possible ramification behavior in the extension $E|K(t)$:*

[1] `MAGMA` [3] knows this group as "`SmallGroup(240,90)`"

Case	$H \cong$	*Ramification Data*	*Conditions*
(A)	$\mathrm{SL}(2,3)$	*(4,3)*	$s = 1$
(B)	$\mathrm{GL}(2,3)$	*(8,6)*	$s = 1$

Case (A) can be easily disproved in the same manner as in the previous chapters. Case (B), however, is more interesting:

First it is easy to see that $\mathfrak{p}$ must ramify with index 6.

An inspection of the subgroups of H of order 8 shows that F_∞ contains the hyperelliptic involution $\imath$. Thus, $\imath \notin F_\mathfrak{p}$ because otherwise $\frac{48}{8} + \frac{48}{6} = 6 + 8 = 14$ places would ramify with index 2 in the extension $E|\operatorname{Fix}(\langle\imath\rangle)$, contrary to our assumption $g = 2$.

As all subgroups of H of order 6 not containing $\imath$ are isomorphic to S_3, we get $I_\mathfrak{p} \cong S_3$. Theorem 4.27 shows that $I_\mathfrak{p}(2) = 1$; thus,

$$\operatorname{ind}(\mathfrak{p}) = n - \frac{1}{6}(n + 3f_2 + 2f_3) + \frac{1}{2}\big(n - \frac{1}{3}(n + 2f_3)\big) = \frac{7n - 4f_3 - 3f_2}{6}$$

where f_2 resp. f_3 is the number of fixed points of an element of order 2 resp. 3 of $I_\mathfrak{p}$.

Since $\operatorname{ind}(\infty) \geq \frac{9}{8}(n-1)$, a simple calculation shows that the genus-0 condition is violated if $f_2 \neq \frac{n}{3} \neq f_3$. It follows $f_2 = f_3 = \frac{n}{3}$ and $\operatorname{ind}(\mathfrak{p}) = \frac{7}{9}n$.

Since $I_\infty(1) \leq N$, section 3.2.1 gives

$$\operatorname{ind}(\infty) = \frac{9}{8}(n-1) + \sum_{i=2}^{\infty} \frac{1}{8}\big(n - \frac{n}{|I_\infty(u_i)|}\big) = \frac{9}{8}(n-1) + \frac{1}{8}n\sum_{i=2}^{\infty}\big(1 - \frac{1}{|I_\infty(u_i)|}\big).$$

The genus-0 condition forces $I_\infty(u_3) = 1$. Therefore

$$\frac{7}{9}n + \frac{9}{8}(n-1) + \frac{1}{8}n\big(1 - \frac{1}{|I_\infty(u_2)|}\big) = 2n - 2 \iff n = \frac{63\,|I_\infty(u_2)|}{9 - 2\,|I_\infty(u_2)|}.$$

Thus, $I_\infty(u_2) = 1$, $n = 9$, and $\operatorname{ind}(\mathfrak{p}) = 3^2 - 2 = 7$.

The above situation is realized for instance by $f(X) = X^9 + X^8 + X^6 \in \mathbb{F}_3[X]$, cf. chapter 5. As $G = \mathrm{AGL}(2,3)$ is 2-transitive on N, this case never gives an exceptional polynomial.

Case $\operatorname{Aut}_K(E) \cong \Sigma_5$

An inspection of the subgroups and the conjugacy classes of Σ_5 shows that in case of tame ramification inertia groups are isomorphic to

$$C_2,\ C_3,\ C_4,\ C_6,\ \text{or } C_8,$$

in case of wild ramification to

$$C_5,\ C_{10},\ C_5 \rtimes C_4,\ \text{or } C_5 \rtimes C_8.$$

Since H may not contain a characteristic 5-Sylow subgroup by Proposition 2.8, it follows that H is isomorphic to either $\mathrm{SL}(2,5)$ or Σ_5.

As Σ_5 contains only one central involution, this involution coincides with the hyperelliptic involution $\imath$. Note that $\imath$ is the only involution in case $H \cong \mathrm{SL}(2,5)$.

It follows

Lemma 4.28 *Let $\mathfrak{p} \in \mathcal{P}\big(K(t)\big)$ be any place of $K(t)$. Suppose $\mathfrak{P} \in \mathcal{P}(E)$ lies over $\mathfrak{p}$. Denote the inertia group of the extension $\mathfrak{P}|\mathfrak{p}$ with $F_\mathfrak{p}$ and the degree of the different coming from the ramification of $\mathfrak{p}$ with $\delta_\mathfrak{p}$. Denote by s the well-defined integer with $F_\mathfrak{p}(s) > F_\mathfrak{p}(s+1) = 1$. Suppose $|F_\mathfrak{p}| > 1$. Then:*

$F_\mathfrak{p} \cong$	*can occur for* $H \cong$	$\delta_\mathfrak{p} =$
C_2	*all cases*	$\frac{1}{2}\lvert H\rvert$
C_3	*all cases*	$\frac{2}{3}\lvert H\rvert$
C_4	*all cases*	$\frac{3}{4}\lvert H\rvert$
C_6	*all cases*	$\frac{5}{6}\lvert H\rvert$
C_8	Σ_5	$\frac{7}{8}\lvert H\rvert$
C_5	*all cases*	$\frac{1}{5}\lvert H\rvert \cdot (4+4s)$
C_{10}	*all cases*	$\frac{1}{10}\lvert H\rvert \cdot (9+4s)$
$C_5 \rtimes C_4$	*all cases*	$\frac{1}{20}\lvert H\rvert \cdot (19+4s)$
$C_5 \rtimes C_8$	Σ_5	$\frac{1}{40}\lvert H\rvert \cdot (39+4s)$

We use this lemma to solve the Riemann-Hurwitz equation

$$2 = -2|H| + \sum_{\mathfrak{p}} \delta_\mathfrak{p}$$

where $\mathfrak{p}$ runs through all places of $K(t)$ ramifying in $E|K(t)$. We obtain

Theorem 4.29 *The following table gives the possible ramification behavior in the extension $E|K(t)$:*

Case	$H \cong$	*Ramification Data*	*Conditions*
(A)	$\mathrm{SL}(2,5)$	*(3,20)*	$s = 2$
(B)	Σ_5	*(6,40)*	$s = 2$

In case (A) $\mathfrak{p}$ cannot ramify with index 20; thus, we have $I_\mathfrak{p} \cong C_3$ and

$$\mathrm{ind}(\mathfrak{p}) = n - \frac{1}{3}(n+2f)$$

with f the number of fixed points of an element of order 3 in $I_\mathfrak{p}$. $\mathrm{ind}(\mathfrak{p})$ being an integer enforces $f \leq \frac{n}{25}$. Therefore $\mathrm{ind}(\mathfrak{p}) \geq \frac{16}{25}n$. As

$$\mathrm{ind}(\infty) \geq \frac{5}{4}(n-1) + \frac{5}{20}\big(n - \frac{n}{5}\big),$$

the genus-0 condition is violated.

In case (B) $\mathfrak{p}$ cannot ramify with index 40. Thus, we have $I_\mathfrak{p} \cong C_6$ and

$$\mathrm{ind}(\infty) \geq \frac{9}{8}(n-1) + \frac{5}{40}\big(n - \frac{n}{5}\big).$$

Let $\sigma \in I_\mathfrak{p}$ be a generator for $I_\mathfrak{p}$ and denote by $A \in \mathrm{GL}(r,5)$ the automorphism of N that is induced by the action of $\sigma \in H$ on the $\mathbb{F}_5$-vector space N; both σ and A have order 6. As $\mathbb{F}_{25}$ is a splitting field for the separable polynomial $X^6 - 1 \in \mathbb{F}_5[X]$, A is diagonalizable as an automorphism of $N' := N \otimes \mathbb{F}_{25}$.

First suppose that a primitive sixth root of unity is an eigenvalue of A. Then every Galois conjugate of this root of unity is also an eigenvalue of A; hence, A has two sixth roots of unity in its spectrum. Thus, every power A^s of A with $A^s \neq 1$ fixes at most $\frac{n}{25}$ points. We obtain

$$\operatorname{ind}(\mathfrak{p}) \geq n - \frac{1}{6}\big(n + 5\frac{n}{25}\big) = \frac{4}{5}n.$$

This violates the genus-0 condition with the above estimation for $\operatorname{ind}(\infty)$.

Next suppose that no primitive sixth root of unity is an eigenvalue of A. Then A has both a primitive third root of unity and $-1 \in \mathbb{F}_5$ in its spectrum. Again the inverse of the third root of unity is also an eigenvalue of A. This shows that A and A^5 have at most $\frac{n}{125}$, A^2 and A^4 at most $\frac{n}{25}$, and A^3 at most $\frac{n}{5}$ fixed points. We get

$$\operatorname{ind}(\mathfrak{p}) \geq n - \frac{1}{6}\big(n + 2\frac{n}{125} + 2\frac{n}{25} + \frac{n}{5}\big) = \frac{98}{125} \cdot n.$$

This is impossible, too.

4.3.2. Cases in even characteristic $p = 2$

Geyer [15] classifies all possible K-automorphism groups of genus-2 function fields; a nice list is also given in [8]. We obtain that $\operatorname{Aut}_K(E)$ is isomorphic to

$$C_2,\ C_2 \times C_2,\ D_6,\ G_{32},\ \text{or } G_{160}$$

where G_i is some group of order i. We will describe the groups G_i later when we need information about their internal structure.

Proposition 2.9 (2) reduces considerably the work in this section: only the cases $\operatorname{Aut}_K(E) \cong D_6$ or $\operatorname{Aut}_K(E) \cong G_{160}$ may occur.

Case $\operatorname{Aut}_K(E) \cong D_6$

By Lemma 4.1 and Proposition 2.8 it follows $H \cong D_3$ as $Z(D_6) \cong C_2$. Riemann-Hurwitz and Corollary 3.16 imply the impossibility of this case.

Case $\operatorname{Aut}_K(E) \cong G_{160}$

First we have to get some information about the group G_{160}. Due to [8, Sections 2.1, 3.1] G_{160} sits in the middle of the non-split exact sequence

$$1 \longrightarrow \langle \imath \rangle \longrightarrow G_{160} \longrightarrow C_2^4 \rtimes C_5 \longrightarrow 1$$

where C_5 acts non-trivially on C_2^4.

Up to isomorphism G_{160}[2] is uniquely determined by this sequence; we get

$$G_{160} \cong E_{32}^- \rtimes C_5$$

where E_{32}^- denotes the extraspecial group of order 32 being a central product of a quaternion group of order 8 and two copies of the dihedral group of order 8 (cf. [25, III 13.8]) and C_5

[2] `MAGMA` [3] knows this group as "`SmallGroup(160,199)`"

acts nontrivially on E_{32}^{-}.

An inspection of the subgroups of G_{160} and Proposition 2.9 prove that either $H \cong C_{10}$ or $H \cong G_{160}$. Hence, in every case H contains a characteristic nontrivial 2-subgroup. This contradicts Proposition 2.8.

5. AGL as a monodromy group

In this chapter f denotes a polynomial of the form

$$f(X) := X^{p^r} + \sum_{i=0}^{s} a_i X^{p^r - p^i} \qquad \text{with } s < r \text{ and } a_0 a_s \neq 0. \tag{5.1}$$

We are interested in the calculation of the geometric monodromy group of f. Abhyankar [1] already dealt with the case $s = 0$; he proved that f is affine with $G = \mathrm{AGL}(1, p^r)$. Thus, for the rest of this chapter we will always assume $s \neq 0$; this implies in particular $r \geq 2$. We use the notation from page 23.

Lemma 5.1 *(1) $f(X) - t$ is separable.*

(2) f is functionally indecomposable over K.

(3) $G \leq \mathrm{AGL}(r, p)$. (We do not *prove here that G is an affine group.)*

Proof.

(1) The derivative of f is given by $f'(X) = -a_0 X^{p^r - 2} \neq 0$. Therefore $f(X) - t$ does not have multiple roots.

(2) Suppose there exist nonlinear polynomials $g, h \in K[X]$ such that $f = g \circ h$. We may assume $h(0) = 0$. Since $f(0) = 0$, this yields $g(0) = 0$, too. It follows from (1) that $f'(X) = g'\big(h(X)\big) \cdot h'(X) = -a_0 X^{p^r - 2}$.

Suppose $g'(0) \neq 0$. Then $X \nmid g' \circ h$ and we get $X^{p^r - 2} | h'$. Hence, $\deg h \geq p^r - 1$. But then $p^r = \deg f = \deg g \cdot \deg h \geq 2(p^r - 1)$ which is impossible.

Thus, $g'(0) = 0$. As $0 \in K$ is the only zero of f', $h(\xi) \neq 0$ for all $\xi \in K^\sharp$. We obtain $h(X) = h_0 X^\alpha$. But then every summand of f has degree divisible by α. Since p^r and $p^r - 1$ are relatively prime, this enforces $\alpha = 1$ contrary to our assumption.

(3) Let $x_1, \ldots, x_n \in L$ be the roots of $f(X) - t$. Set $Z := X^{-1}$ and $z_i := x_i^{-1}$; this is well-defined as all x_i are different from zero. An easy calculation shows that the equation $f(X) - t = 0$ can be rewritten in the form

$$Z^{p^r} - \sum_{i=0}^{s} \frac{1}{t} a_i Z^{p^i} = \frac{1}{t}. \tag{5.2}$$

Since the zeros of this equation are precisely the elements $z_i \in L$, the splitting field of (5.2) is L. Section 2.3 gives the claim.

■

The following concept severely restricts the possibilities for G; we will prove for instance that G is 2-transitive.

Definition 5.2 (Jordan group) *Let G be a group acting transitively on the finite set Ω. A subset $\Gamma \subseteq \Omega$ is said to be a* Jordan set *if $|\Gamma| > 1$ and the pointwise stabilizer $G_{(\Omega\setminus\Gamma)}$ is transitive on Γ. The set $\Delta := \Omega \setminus \Gamma$ is called a* Jordan complement.

If G is k-transitive on Ω, every subset Δ of size $< k$ is a Jordan complement; in such a case we call Γ and Δ improper*, otherwise we call them* proper*. If $\Gamma = \Omega$, we call Γ and Δ trivial.*

G is called a Jordan group *if it has at least one proper Jordan complement.*

In our situation this definition yields

Proposition 5.3 *G is a 2-transitive group and contains a nontrivial Jordan complement Δ of size $|\Delta| = p^s$.*

If $p \neq 2$ or $p = 2$ and $s > 1$, then Δ is proper and G is a Jordan group.

Proof. We consider the ramification of the place $\mathbf{0}: t \mapsto 0$ in the extension $K(x)|K(t)$. Since

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

with $X^{p^s} + \sum_{i=0}^{s} a_i X^{p^s-p^i}$ being a separable polynomial, $\mathbf{0}$ decomposes over $K(x)$ in the following way:

$$\mathbf{0} = \mathfrak{P}_0^{p^r-p^s} \cdot \mathfrak{P}_1 \cdots \mathfrak{P}_{p^s} \qquad \text{with pairwise different places } \mathfrak{P}_i \in \mathcal{P}\big(K(x)\big). \tag{5.3}$$

Hence, by van der Waerden [51] $I_{\mathfrak{p}}$ fixes a set Δ of p^s elements pointwise and permutes the remaining $p^r - p^s$ elements transitively. Denote this orbit by Γ. Then the pointwise stabilizer $G_{(\Delta)}$ of Δ in G contains $I_{\mathfrak{p}}$; thus, $G_{(\Delta)}$ is a fortiori transitive on Γ.

Γ is a nontrivial Jordan subset of G. The indecomposability of f implies the primitivity of G; hence, Neumann [40, Theorem J1] gives the 2-transitivity of G.

Suppose $p > 2$. Lemma 5.1 and the classification in [32, 4.2.5] show that G is 2-transitive but not 3-transitive. Hence, Δ being proper comes down to $|\Delta| \geq 2$; but this condition is always fulfilled.

Suppose $p = 2$. [32, 4.2.5] shows that G is at most 4-transitive. The claim follows now easily. ∎

Remark 5.4 The 2-transitivity of G can be obtained in a different way, too. Unfortunately, the following proof does not show the important fact that G is a Jordan group in almost all cases.

Let X and Y be algebraically independent transcendentals over K. Set $\phi(X,Y) := f(X) - f(Y) \in K[X,Y]$. We prove that $\frac{\phi(X,Y)}{X-Y}$ is absolutely irreducible.

Suppose

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

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 $A_k = (X-Y)^k$ and $B_m = (X-Y)^m$. Hence,

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

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

The 2-transitivity of G follows for instance from [14, Exceptionality Lemma]. ⋆

For the following we need some information about the p-structure of $\mathrm{GL}(r, p)$.

Lemma 5.5 $\mathrm{GL}(r, p)$ *does not contain an element of order* p^r. $\mathrm{GL}(r, p)$ *contains an element of order* p^{r-1} *if and only if* $r \in \{1, 2\}$ *or* $(p, r) = (2, 3)$.

Proof. Let $P \leq \mathrm{GL}(r, p)$ be a p-Sylow subgroup of $\mathrm{GL}(r, p)$. Denote by J_s a Jordan block of dimension s for the eigenvalue 1. The minimal polynomial of J_s is given by $\mu_s(X) := (X-1)^s$. Every $A \in P$ is similar to a direct sum of Jordan blocks J_{s_i}, i.e. we find an element $T \in \mathrm{GL}(r, p)$ with

$$A^T = \bigoplus_{i=1}^{a} J_{s_i} \qquad \text{and} \qquad \sum_{i=1}^{a} s_i = r.$$

Let $s := \max\{s_i \mid 1 \leq i \leq a\}$ denote the maximum of the s_i. Then the minimal polynomial of A is given by μ_s. The order A is given by p^i where i is the smallest integer such that $\mu_s \mid (X-1)^{p^i}$.

This proves that J_r has the highest possible p-order in $\mathrm{GL}(r, p)$. We have

$$|J_r| = p^i \qquad \text{with} \qquad p^{i-1} < r \leq p^i.$$

As the equation $p^{r-1} < r$ is not solvable, $\mathrm{GL}(r, p)$ never contains an element of order p^r.

It follows by induction that the equation $p^{r-2} < r$ holds exactly for $r \in \{1, 2\}$ or $(p, r) = (2, 3)$. ■

Corollary 5.6 *G is an affine group. Moreover, there exists a divisor e of r such that either*

$$\mathrm{ASL}(e, p^{\frac{r}{e}}) \leq G \leq \mathrm{A\Gamma L}(e, p^{\frac{r}{e}}) \qquad \text{or} \qquad N \rtimes A_7 \cong G \leq \mathrm{AGL}(4, 2).$$

In the latter case $A_7 \hookrightarrow \mathrm{GL}(4, 2)$ acts 2-transitively on the nonzero elements of $\mathbb{F}_2^4$.

Proof. Let $S := \mathrm{soc}(G)$ be the socle of G. As G is 2-transitive, S is either elementary abelian and regular or isomorphic to a non-abelian simple group.

We start with the latter case. Suppose S is non-abelian and simple.

We show first that S can only be isomorphic to a projective special linear group.

Assume G is a Jordan group. The primitivity of G and Neumann [40, Classification Theorem] immediately show that $S \cong \mathrm{PSL}(d, q)$ acts 2-transitively on the projective plane $\mathrm{PG}(d-1, q)$ with $|\mathrm{PG}(d-1, q)| = \frac{q^d-1}{q-1} = p^r$.

If G is not a Jordan group, then by Proposition 5.3 $(p, s) = (2, 1)$ and – with the notation from this proposition – the two-point stabilizer $G_{(\Delta)}$ is transitive on Γ. Hence G is even 3-transitive. The classification of 2-transitive groups (a nice list is given in Cameron [6]) shows that $\mathrm{soc}(G)$ is isomorphic to $\mathrm{PSL}(2, q)$ acting on $\mathrm{PG}(1, q)$ with $|\mathrm{PG}(1, q)| = q+1 = 2^r$.

Suppose $S \cong \mathrm{PSL}(d, q)$. We prove that this implies $(p^r, d, q) = (8, 2, 7)$.

S is a subgroup of the affine group $\mathrm{AGL}(r, p)$. Denote the affine kernel of $\mathrm{AGL}(r, p)$ with N. The simplicity of S gives $S \cap N = 1$. Hence, a point stabilizer of the group $N \rtimes S$ is

isomorphic to S. Thus, S can be considered a subgroup of $\mathrm{GL}(r,p)$. The integers p^r, d, and q fulfill the equation

$$p^r = \frac{q^d - 1}{q - 1}. \tag{5.4}$$

First assume that $q^d - 1$ has a primitive prime factor. In our case as a consequence of Zsigmondy [52] this is true if $d > 2$, or $d = 2$ and q is even. By (5.4) this prime factor is uniquely given by p; in particular, $\frac{q^d-1}{q-1}$ and $(q-1)$ are relatively prime. Let x be a Singer-element of $\mathrm{PGL}(d,q)$. Then x has order $\frac{q^d-1}{q-1}$, cf. Huppert [25, II 7.3]. As $\mathrm{PSL}(d,q) \trianglelefteq \mathrm{PGL}(d,q)$ with $\mathrm{PGL}(d,q)/\mathrm{PSL}(d,q) \leq C_{q-1}$ cyclic, x^{q-1} is an element of $\mathrm{PSL}(d,q)$ with $|x| = |x^{q-1}| = p^r$. We obtain that $\mathrm{GL}(r,p)$ contains an element of order p^r. This contradicts Lemma 5.5.

Now assume $d = 2$ with odd q. Then $p = 2$ is even. The same idea as above shows $x^2 \in \mathrm{PSL}(2,q)$. Hence, $\mathrm{GL}(r,2)$ contains an element of order 2^{r-1}. Lemma 5.5 and Huppert [25, II 6.14] show that this is only possible for $r = 3$. Thus, we obtain $(p^r, d, q) = (8, 2, 7)$.

But this is impossible: As S is selfnormalizing in $\mathrm{AGL}(3,2)$, we obtain $S = G$. An explicit calculation shows that the Jordan complements of S have order 1 or 7 contrary to Proposition 5.3.

Thus, we end up in the affine case. If G is a Jordan group, Neumann [40] gives the assumption. Otherwise G is a 3-transitive affine group in even characteristic. Our claim follows directly from Cameron/Kantor [7, Sec. 8]. ∎

Now we are able to state our main theorem:

Theorem 5.7 *Define e the greatest common divisor of r and all $0 \leq i \leq s$ with $a_i \neq 0$, $e := \gcd(r, i \mid a_i \neq 0)$. Then $G = \mathrm{AGL}(\frac{r}{e}, p^e)$.*

Proof. We use the notation from Lemma 5.1 and Lemma 2.12.

Let $v \in V^\sharp$ be a nonzero element of V. Then the equation

$$v^{p^r-1} - \sum_{i=0}^{s} \frac{1}{t} a_i v^{p^i-1} = 0$$

holds; in fact, the set of zeros of this equation coincides with $V^\sharp$. Using the identity $Z = X^{-1}$ we obtain

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

Since the latter polynomial is irreducible, we see that the elements $1, v, v^2, \ldots, v^{p^r-2}$ are linearly independent over K. Thus, any representation of v^{p^r-1} by smaller powers of v is uniquely given by $\sum_{i=0}^{s} \frac{1}{t} a_i v^{p^i-1}$.

Let c be an element of $K^\times$. Then the following holds:

$$\begin{aligned} cv \in V^\sharp &\iff c^{p^r-1}v^{p^r-1} = \sum_{i=0}^{s} \frac{1}{t} a_i c^{p^i-1} v^{p^i-1} = c^{p^r-1} \sum_{i=0}^{s} \frac{1}{t} a_i v^{p^i-1} \\ &\iff a_i c^{p^r} = a_i c^{p^i} \quad \text{for all } 0 \le i \le s \\ &\iff c^{p^r} = c^{p^i} \quad \text{for all } 0 \le i \le s \text{ with } a_i \neq 0 \\ &\overset{a_0 \neq 0}{\iff} c^{p^r} = c \wedge c^{p^i} = c \quad \text{for all } 1 \le i \le s \text{ with } a_i \neq 0 \\ &\iff c \in \mathbb{F}_{p^r} \cap \bigcap_{a_i \neq 0, i \neq 0} \mathbb{F}_{p^i} = \mathbb{F}_{p^e} \le K. \end{aligned}$$

Thus, we can consider V to be an $\mathbb{F}_{p^e}$-vector space and $H \le \Gamma\mathrm{L}(\frac{r}{e}, p^e)$ is a subgroup of $\Gamma\mathrm{L}(\frac{r}{e}, p^e)$. But H acts as a proper linear group since $(cv)^h = cv^h$ for all $h \in H$ and $c \in \mathbb{F}_{p^e} \le K$. Hence, $H \le \mathrm{GL}(\frac{r}{e}, p^e)$.

In the following we prove that the equality $H = \mathrm{GL}(\frac{r}{e}, p^e)$ holds.

By Lemma 2.12 N equals the kernel of the operation of G on V. Therefore we have $E = K(V)$; but we can also think of E as the splitting field of the irreducible polynomial $F(X) := \sum_{i=0}^{s} a_i X^{p^r - p^i} - t$.

Let $v \in E$ be any root of F. Denote by F_∞ the inertia group of a fixed place of E lying over ∞. The structure of F shows that ∞ ramifies totally in the extension $K(v)|K(t)$. Hence, by van der Waerden [51] F_∞ is transitive on $V^\sharp$.

Let P be the normal p-Sylow subgroup of F_∞. As the p-group P fixes at least one element of $V^\sharp$, P fixes every element of $V^\sharp$ because all P-orbits on $V^\sharp$ have the same length. We obtain $P = 1$; F_∞ is a cyclic and transitive p'-group of linear transformations of V of order a multiple of $\deg F = p^r - 1$. It follows from Huppert [25, II 3.10 and 7.3] that F_∞ is a full Singer cycle in $\mathrm{GL}(\frac{r}{e}, p^e)$.

Using the classification from Corollary 5.6 we see that $N \rtimes A_7 \cong G \le \mathrm{AGL}(4,2)$ is impossible as this group does not contain a cyclic subgroup of order 15. Hence, $\mathrm{SL}(\frac{r}{e}, p^e)$ is a subgroup of H. By Huppert [25, II 7.3 (b)]

$$H/\operatorname{SL}\Big(\frac{r}{e}, p^e\Big) \ge \operatorname{SL}\Big(\frac{r}{e}, p^e\Big) F_\infty / \operatorname{SL}\Big(\frac{r}{e}, p^e\Big) \cong C_{p^e-1} \cong \operatorname{GL}\Big(\frac{r}{e}, p^e\Big) / \operatorname{SL}\Big(\frac{r}{e}, p^e\Big);$$

as $H \le \mathrm{GL}(\frac{r}{e}, p^e)$, it follows $H = \mathrm{GL}(\frac{r}{e}, p^e)$. ∎

Higher ramification in $L|K(t)$

Proposition 5.8 *The normal p-Sylow subgroup of I_∞ equals N. Moreover*

$$\operatorname{ind}(\infty) = n \qquad \textit{and} \qquad I_\infty(2) = 1.$$

$I_{\mathbf{0}}$ is isomorphic to $P \rtimes C_{p^{r-s}-1}$ with $|P| = p^s$. Moreover

$$\operatorname{ind}(\mathbf{0}) = n - 2 \qquad \textit{and} \qquad I_{\mathbf{0}}(2) = 1.$$

Proof. Theorem 5.7 gives $I_\infty \cong N \rtimes C_{n-1}$; therefore we have

$$\operatorname{ind}(\infty) \ge (n-1)\Big(1 + \frac{1}{n-1}\Big) = n \quad \text{and} \quad \operatorname{ind}(\infty) = n \iff I_\infty(2) = 1.$$

We use the notation from the proof of Proposition 5.3. Let $\mathfrak{P}$ be a place of L lying over $\mathfrak{P}_0$. Denote by I the inertia group of the extension $\mathfrak{P}|\mathbf{0}$. We know that I is isomorphic to a semidirect product $P \rtimes C$ with a p-group P and a cyclic p'-group C.

By van der Waerden [51] we obtain $o(I) = s + 1$. Denote by Γ the I-orbit consisting of $p^r - p^s$ elements. As $I(1)$ is normal in I, Γ splits into a different $I(1)$-orbits γ_i, each of length b. Since C acts transitively on the γ_i, it follows

$$a \mid |C| \qquad \text{and} \qquad b \mid |P|. \tag{5.5}$$

Because $ab = |\Gamma| = p^s(p^{r-s} - 1)$, we get at once $a = p^{r-s} - 1$, $b = p^s$, and $o\big(I(1)\big) = p^s + p^{r-s} - 1$.

Next we show that $|I| = p^r - p^s$. Suppose $|I| > p^r - p^s$. Then there exists an element $1 \neq h \in I \cap H$. Since the inertia group of any place of L over $\mathbf{0}$ is G-conjugate to I, the decomposition (5.3) of $\mathbf{0}$ in $K(x)$ shows $h^G \subseteq H$. But then the contradiction $h \in \bigcap_{g\in G} H^g = 1$ follows.

Hence, $|P| = p^s$, $|C| = p^{r-s} - 1$, and

$$\operatorname{ind}(\mathbf{0}) \geq n - o(I) + \frac{1}{|C|}\Big(n - o\big(I(1)\big)\Big) = n - 2.$$

The remaining assertions follow directly from the genus-0 condition. ∎

Now we show that an affine polynomial of degree p^2 is an AGL-polynomial of the form (5.1) if it fulfills the conclusion of Proposition 5.8.

Proposition 5.9 *Let $f \in K[X]$ be a monic affine polynomial of degree p^2. Let x be a zero of $f(X) - t$ and denote by $\mathbf{0}$ resp. $\mathfrak{P}_0$ the zero place of $K(t)$ resp. $K(x)$. Suppose $\mathbf{0}$ decomposes in $K(x)$ in the form*

$$\mathbf{0} = \mathfrak{P}_0^{p^2-p} \cdot \mathfrak{P}_1 \cdots \mathfrak{P}_p \qquad \textit{with pairwise different places } \mathfrak{P}_i \in \mathcal{P}\big(K(x)\big).$$

Moreover assume that $\operatorname{ind}(\mathbf{0}) = p^2 - 2$ holds. Then $f = X^{p^2} + aX^{p^2-1} + cX^{p^2-p}$ with $a, c \in K^\sharp$ and both arithmetic and geometric monodromy group of f are equal to $\mathrm{AGL}(2, p)$.

Proof. Corollary 3.16 gives $\operatorname{ind}(\infty) \geq p^2$. The genus-0 condition shows immediately that no other finite place of $K(t)$ ramifies. We obtain

$$f(X) = X^{p^2-p} \cdot g(X) \qquad \text{with a polynomial } g \in K[X] \text{ of degree } p,\ g(0) \neq 0.$$

Since $\mathbf{0}$ is the unique finite place ramifying in $K(x)|K(t)$, the polynomial $f(X) - c$ is separable for all $c \in K^\times$. This shows that $0 \in K$ is the only root of f'.

The derivative of f is given by $f'(X) = X^{p^2-p} g'(X)$. Thus, g' is a monomial. We obtain

$$g(X) = X^p + aX^b + c \qquad \text{with } 0 < b < p \text{ and } ac \neq 0.$$

As $\mathfrak{P}_i|\mathbf{0}$ is unramified for $i \in \{1, \ldots, p\}$, the degree of the different $d(\mathfrak{P}_i|\mathbf{0})$ vanishes; by our assumption $d(\mathfrak{P}_0|\mathbf{0}) = p^2 - 2$. Stichtenoth [47, III.5.10(a)] gives

$$p^2 - 2 = d(\mathfrak{P}_0|\mathbf{0}) \leq v_{\mathfrak{P}_0}\big(f'(x)\big) = v_{\mathfrak{P}_0}\big(abx^{p^2-p+b-1}\big) = p^2 - p + b - 1;$$

hence, $b = p - 1$. The claim follows. ∎

The results of this chapter allow us to give some properties of the fixed field E:

Remark 5.10 The genus $g(E)$ is not bounded.

Denote by K_p an algebraic closure of $\mathbb{F}_p$ and set $f_p(X) := X^{p^2} + X^{p^2-1} + X^{p^2-p} - t$. Then $\mathrm{Gal}\big(f_p|K_p(t)\big) = \mathrm{AGL}(2,p)$; Riemann-Hurwitz shows $g(E) = \frac{1}{2}\big(p^3 - 3p^2 + 4\big)$. This proves $g(E) \to \infty$ for $p \to \infty$.

Let $r \geq 2$ be an integer and set $g_p(X) := X^{p^r} + X^{p^r-1} + X^{p^r-p}$. Then $\mathrm{Gal}\big(g_p|K_p(t)\big) = \mathrm{AGL}(r,p)$. Again, by Riemann-Hurwitz $g(E) \to \infty$ for $r \to \infty$. $\star$

Remark 5.11 Even if G is solvable, E need not be a rational function field.

Let K denote an algebraic closure of $\mathbb{F}_3$ and define $f(X) := X^9 + X^8 + X^6 - t$. Then $\mathrm{Gal}\big(f|K(t)\big) \cong \mathrm{AGL}(2,3)$ is solvable with $g(E) = 2$. $\star$

6. Affine polynomials of degree p^2

In this chapter we classify all affine polynomials of degree p^2 with primitive arithmetic monodromy group. Our result will be

Theorem 6.1 *With the notation from page 23 suppose* $\deg f = p^2$. *Then either* $E|K(t)$ *is tame and* f *fulfills the conclusion of Theorem 4.2 or one of the following cases holds:*

- $H = \mathrm{GL}(2,p)$, $I_\infty \cong N \rtimes C_{n-1}$ *with* $I_\infty(2) = 1$ *and* $\mathrm{ind}(\infty) = n$, $I_\mathfrak{p} \cong C_p \rtimes C_{p-1}$ *with* $I_\mathfrak{p}(2) = 1$, $\mathrm{ind}(\mathfrak{p}) = n-2$, *and* $o(I_\mathfrak{p}) = p+1$. *This case is realized for example by the* AGL*-polynomial* $X^{p^2} + aX^{p^2-1} + bX^{p^2-p}$, *cf. chapter 5.*
- $\mathrm{SL}(2,p) \leq H$ *and* $F_\mathfrak{p}$ *is a cyclic* p'*-group.*

If $E|K(t)$ *is wild, then* f *is not exceptional.*

We know from Lemma 4.1 that $E|K(t)$ being a tame extension implies $g = 0$. Hence, this case only gives polynomials satisfying the conclusion of Theorem 4.2. Therefore we will suppose $E|K(t)$ to be wild from now on.

We state a first observation

Lemma 6.2 *Suppose* f *has degree* p^r *with* r *being a prime. Assume further that* f *is functionally indecomposable over* k *but decomposable over* K. *Then* $p \nmid [E : K(t)]$. *In particular, the extension* $E|K(t)$ *is tame.*

Proof. As U is irreducible on N, the H-module N is semisimple by Clifford. As H acts reducibly, we can write $N = \bigoplus_{i=1}^{r} N_i$ where the N_i are irreducible H-submodules of N of order p. Since the automorphism group of N_i is abelian, the commutator subgroup H' of H lies in the kernel of the action of H on N_i. Thus, H' is a subgroup of the kernel of H on N; hence, $H' = 1$ and H is abelian.

Let P be a p-Sylow subgroup of H. Then P is characteristic in H and, thus, normal in U. Proposition 2.8 gives $P = 1$; hence, $p \nmid [E : K(t)]$. ∎

The above lemma allows us to reduce our classification to polynomials that are indecomposable over K, or, equivalently, groups $H \leq \mathrm{GL}(2,p)$ acting irreducibly. These groups fulfill

Proposition 6.3 *Suppose* H *is an irreducible subgroup of* $\mathrm{GL}(2,p)$. *If* p *divides* $|H|$, *then* $\mathrm{SL}(2,p) \leq H$.

Proof. Let $P \cong C_p$ denote a p-Sylow subgroup of $\mathrm{GL}(2,p)$. As $p \mid |H|$, we may assume $P \leq H$. Proposition 2.8 shows that P is not normal in H. Hence, there exists $h \in H$ with $P \neq P^h$. [32, 8.6.7] gives $\langle P, P^h \rangle = \mathrm{SL}(2,p) \leq H$. ∎

The next lemma states some well-known properties of $\mathrm{GL}(2,p)$:

Lemma 6.4 *(1) Let P denote a p-Sylow subgroup of $\mathrm{GL}(2,p)$. Then the order of a p-regular element in $N_{\mathrm{GL}(2,p)}(P)$ divides $p-1$.*

(2) Let $g \in \mathrm{SL}(2,p) \le H$ be p-regular. Then g fixes only $0 \in N$.

6.1. Cases in odd characteristic $p \neq 2$

By Proposition 6.3 we may assume $H = \mathrm{SL}(2,p) \rtimes C$ where C is a cyclic group of order $r|p-1$. Set $Z := \mathrm{Fix}\big(N \rtimes \mathrm{SL}(2,p)\big)$. Then $Z|K(t)$ is a tame Galois extension of degree r. For the following s and t denote integers relatively prime to p.

Two finite places ramify

Suppose $\mathfrak{p}$ and $\mathfrak{q}$ ramify. By Lemma 3.21 we get $F_\mathfrak{p} \cong F_\mathfrak{q} \cong C_2$. Since an involution in $\mathrm{GL}(2,p)$ fixes either exactly one point or exactly p points, $\mathrm{ind}(\mathfrak{p})$ and $\mathrm{ind}(\mathfrak{q})$ can only have the values

$$p^2 - \frac{1}{2}(p^2+1) = \frac{p^2-1}{2} \qquad \text{or} \qquad p^2 - \frac{1}{2}(p^2+p) = \frac{p(p-1)}{2}.$$

As $E|K(t)$ is wild, ∞ ramifies in this extension with index ps. Lemma 6.4 shows $s \mid p-1$; thus,

$$\mathrm{ind}(\infty) \ge (p^2-1)\Big(1 + \frac{1}{p-1}\Big) = p(p+1).$$

We obtain a violation of the genus-0 condition.

Only one finite place ramifies

By Riemann-Hurwitz Z is a rational function field. The classification of Valentini and Madan [50] shows that $Z|K(t)$ has exactly two branch points, both ramifying totally. Thus, r divides $|F_\infty|$ and $|F_\mathfrak{p}|$.

Suppose $\mathfrak{p}$ ramifies wildly. We have $F_\mathfrak{p} \cong C_p \rtimes C_{rt}$ with $rt \mid p-1$. Set $S := F_\mathfrak{p} \cap \mathrm{SL}(2,p)$. Then S has order pt and by Lemma 6.4 $I_\mathfrak{p}$ contains $(pt-p)$ elements that fix at most one point. Thus,

$$\mathrm{ind}(\mathfrak{p}) \ge p^2 - \frac{1}{prt}\big(\underbrace{p^2 + (p-1)p + pt - p}_{\text{induced by } S} + (prt - pt)p\big) + \frac{1}{rt}\Big(p^2 - \frac{1}{p}\big(p^2 + (p-1)p\big)\Big).$$

If ∞ ramifies wildly in the extension $E|K(t)$, then $\mathrm{ind}(\infty) \ge p(p+1)$. This induces a contradiction to the genus-0 condition.

Hence, $F_\infty \cong C_{rs}$ with $\mathrm{ind}(\infty) \ge (p^2-1)\big(1+\frac{1}{rs}\big)$. We obtain

$$\mathrm{ind}(\infty) + \mathrm{ind}(\mathfrak{p}) - 2p^2 + 2 \ge \frac{(p-1)\big(t + pt + s(p+t-3-rt)\big)}{rst}.$$

Since $rt \mid p-1$, the genus-0 condition is violated for $t \neq 1$. Thus, suppose $t = 1$. The genus-0 condition forces $r = p-1$ and $s = p+1$. This gives $H \cong \mathrm{GL}(2,p)$, $I_\mathfrak{p}(2) = I_\infty(2) = 1$, and $|\mathrm{Fix}(g)| = p$ for all $g \in I_\mathfrak{p}^\sharp$. It follows $\mathrm{ind}(\infty) = p^2$, $\mathrm{ind}(\mathfrak{p}) = p^2 - 2$, and $o(I_\mathfrak{p}) = p+1$.

There exist polynomials f that realize this case, cf. chapter 5. As H is transitive on $N^\sharp$, such an f cannot be exceptional.

If $\mathfrak{p}$ ramifies tamely, then our estimations for the degree of the different of $K(x)|K(t)$ are too weak to induce contradictions to the genus-0 condition. Hence, we only obtain $\mathrm{SL}(2,p) \leq H$ with $F_{\mathfrak{p}}$ being a cyclic p'-group.

No finite ramification
A discussion of the extension $Z|K(t)$ shows $r = 1$. Hence, $H \cong \mathrm{SL}(2,p)$ and ∞ ramifies with $F_\infty \cong C_p \rtimes C_s$ where $s \mid p-1$. Set $a \in \mathbb{N}$ the well-defined integer with $F_\infty(a) > F_\infty(a+1) = 1$. Riemann-Hurwitz states

$$2g(E) - 2 = -2|H| + \frac{|H|}{ps}\big(ps - 1 + a \cdot (p-1)\big).$$

As $g(E) \geq 0$, we obtain $a \geq \frac{p^2-1+s(p^3-p-2)}{(1+p)(p-1)^2}$. Section 3.2.1 shows

$$\mathrm{ind}(\infty) \geq (p^2-1)\Big(1 + \frac{1}{s}\Big) + \frac{1}{s}(a-1)(p^2-p);$$

this gives a contradiction to the genus-0 condition.

6.2. Cases in even characteristic $p = 2$

Proposition 6.3 gives $H = \mathrm{GL}(2,2) = \mathrm{SL}(2,2) \cong S_3$. Denote by C the normal cyclic subgroup of H of order 3. Set $Z := \mathrm{Fix}(N \rtimes C)$. Then $E|Z$ resp. $Z|K(t)$ is Galois of degree 3 resp. 2. As all subgroups of H of order 2 are selfnormalizing, ramification groups in the extension $E|K(t)$ are either isomorphic to C_3 or to C_2.

Only one finite place ramifies
By Corollary 3.16 $F_\infty \cong C_3$ and $I_{\mathfrak{p}} \cong C_2$. Van der Waerden [51] shows that $\mathfrak{p}$ decomposes in $K(x)$ in the form

$$\mathfrak{p} = \mathfrak{P}^2 \cdot \mathfrak{P}_1 \cdot \mathfrak{P}_2 \quad \text{with pairwise different places of } K(x).$$

Proposition 5.9 proves that the extension $L|K(t)$ comes from a polynomial belonging to the class of AGL-polynomials described in chapter 5.

No finite ramification
As $E|K(t)$ is wild, we get $F_\infty \cong C_2$. By Section 3.2.1 $F_\infty(2) = 1$; but this gives a contradiction to the Riemann-Hurwitz genus formula.

7. Exceptional polynomials of degree p^3

In this chapter we classify all exceptional polynomials of degree p^3 with primitive arithmetic monodromy group. Our result will be

Theorem 7.1 *With the notation from page 23 suppose* $\deg f = p^3$. *If f is exceptional, then the extension $E|K(t)$ is tame.*

In particular, $g = 0$ and Theorem 4.2 lists all possibilities for f.

We will suppose the extension $E|K(t)$ to be wild from now on. Lemma 6.2 gives the irreducibility of H on N. We start with the discussion of the case $p > 3$.

7.1. The cases in characteristic $p > 3$

Suppose $p > 3$. We first classify all irreducible subgroups $H \leq \mathrm{GL}(3,p)$ in question.

Lemma 7.2 *Suppose $H \leq \mathrm{GL}(3,p)$ with $p \mid |H|$. Define $S := H \cap \mathrm{SL}(3,p)$ and $Z := Z\big(\mathrm{SL}(3,p)\big)$. Set $\overline{S} := SZ/Z \leq \mathrm{PSL}(3,p)$ the image of S in $\mathrm{PSL}(3,p)$. Then:*

(1) H acts irreducibly on $N \iff S$ acts irreducibly on N.

(2) If S is irreducible on N, then $\overline{S} \cong \mathrm{PSL}(3,p)$, $\overline{S} \cong \mathrm{PSL}(2,p)$, or $\overline{S} \cong \mathrm{PGL}(2,p)$.

(3) If H is irreducible on N but not transitive on $N^\sharp$, then

$$H_0' \leq H \leq H_0 \times Z\big(\mathrm{GL}(3,p)\big)$$

where H_0 is isomorphic to $\mathrm{PGL}(2,p)$ and acts irreducibly on N. H_0 is conjugate to the image of $\mathrm{PGL}(2,p)$ under the mapping (4.4) on page 39.

Proof.

(1) S is a subgroup of H; if S is irreducible, then H is a fortiori irreducible.

Suppose H is irreducible and S acts reducibly. Let $1 \neq P \leq H$ be a p-Sylow subgroup of H. As $H/S \leq C_{p-1}$, the group $P \leq S$ is also a p-Sylow subgroup of S. Thus, we obtain the same contradiction as in the proof of Lemma 6.2.

(2) We use Bloom's [2] classification of the subgroups of $\mathrm{PSL}(3,p)$.

First assume that $\overline{S}$ does not have any nontrivial elementary abelian normal subgroup. Then [2, Thm. 1.1] and the condition $p \mid |\overline{S}|$ give $\overline{S} \cong \mathrm{PSL}(3,p)$, $\overline{S} \cong \mathrm{PSL}(2,p)$, or $\overline{S} \cong \mathrm{PGL}(3,p)$. We show in part (3) of this proof that these cases really induce an irreducible group S.

Now assume $\overline{S}$ has a nontrivial normal elementary abelian subgroup; this case is dealt with in [2, Theorem 7.1]. The cases (1), (2), (4), and (5) of this theorem cannot occur for $\overline{S}$ would be a p'-group. In the remaining case (3) the group S contains a normal

elementary abelian p-subgroup P. By Proposition 2.8 $P = 1$. Bloom [2] shows that S – up to conjugacy and/or the inverse-transpose isomorphism – embeds into the subgroup of $\mathrm{GL}(3,p)$ consisting of elements of the form $\left(\begin{smallmatrix} * & 0 & 0 \\ * & * & * \\ * & * & * \end{smallmatrix}\right)$. This shows that S does not act irreducibly.

(3) $\overline{S} \cong \mathrm{PSL}(3,p)$ enforces $S = \mathrm{SL}(3,p)$. But then S would be 2-transitive, a contradiction to our assumption.

In the remaining cases $\overline{S}$ contains a normal subgroup isomorphic to $\mathrm{PSL}(2,p)$. Bloom [2, Lemma 6.3] shows that the commutator subgroup S' of S is conjugate to the image of $\mathrm{PSL}(2,p)$ under the mapping ψ on page 37. In particular we obtain the irreducibility of S.

As S' is characteristic in H, we see that H is a subgroup of $N_{\mathrm{GL}(3,p)}(S')$. Bloom proves that $N_{\mathrm{SL}(3,p)}(S') = H_0 \times Z$ where $H_0 \cong \mathrm{PGL}(2,p)$ is irreducible with $H_0' = S'$. This shows that H_0 is conjugate to the image of $\mathrm{PGL}(2,p)$ under the mapping (4.4) on page 39. Certainly $H_0 \times Z\big(\mathrm{GL}(3,p)\big) \leq N_{\mathrm{GL}(3,p)}(H_0')$. Some calculation shows that $C_{\mathrm{GL}(3,p)}(H_0') = Z\big(\mathrm{GL}(3,p)\big)$. As $\mathrm{Aut}(H_0') \cong \mathrm{Aut}\big(\mathrm{PSL}(2,p)\big) \cong \mathrm{PGL}(2,p)$, the N/C theorem gives

$$H_0 \times Z\big(\mathrm{GL}(3,p)\big) = N_{\mathrm{GL}(3,p)}(H_0').$$

■

Remark 7.3 The assumption $p \mid |H|$ in statement (1) of the previous lemma is necessary. Consider for instance the group

$$H := \left\langle \left(\begin{smallmatrix} 0 & 1 & 0 \\ 3 & 5 & 3 \\ 1 & 0 & 2 \end{smallmatrix}\right) \right\rangle \leq \mathrm{GL}(3,7).$$

H is isomorphic to C_9 and acts irreducibly. But $S := H \cap \mathrm{SL}(3,7) = Z(\mathrm{SL}(3,7)) \cong C_3$ is reducible. ⋆

As we are interested in exceptional polynomials f, H is primitive on N but may not be transitive on $N^\sharp$. Hence, all possibilities for H are given by Lemma 7.2 (3). As a consequence we get

Lemma 7.4 *(1) The fixed field $Z := \mathrm{Fix}(N \rtimes H')$ is rational. Either H/H' is isomorphic to the Klein four-group; then exactly three places of $K(t)$ ramify in the extension $Z|K(t)$, each one with index $r = 2$. Or H/H' is cyclic of order $r \mid p-1$; then exactly two places of $K(t)$ ramify in the extension $Z|K(t)$, each one with index r.*

(2) Let $h \in H$ be of order > 2. Then h has at most p fixed points.

(3) Let I be a subgroup of H being isomorphic to $C_p \rtimes C_s$. If $\gcd(s,p) = 1$, then $s \mid p-1$.

Proof.

(1) Lemma 7.2 shows that H/H' is a p'-group. Thus, the extension $Z|K(t)$ is tame with $g(Z) = 0$. As K is algebraically closed, it follows that Z is a rational function field.

The ramification data and the group structure of H/H' can be obtained directly from the classification of Valentini and Madan [50].

H/H' embeds into $C_2 \times C_{p-1}$; thus, every cyclic subgroup of $C_2 \times C_{p-1}$ has order a divisor of $p-1$. This shows $r \mid p-1$.

(2) With the notation from Lemma 7.2 write $h = gz$ with $g \in H_0$ and $z \in Z\big(\mathrm{GL}(3,p)\big)$. Then $h^2 = g^2z^2 \neq 1$ and $g^2 \in H_0'$. If $g^2 = 1$, then h^2 and, hence, h do not have any nontrivial fixed point. Thus, suppose $g^2 \neq 1$. Then either g^2 has order p; here the assertion follows from equation 4.3 on page 37. Or g^2 is p-regular; but then the representation ψ on page 37 shows that g^2 has three pairwise different eigenvalues. Hence, the assertion is valid in this case, too.

(3) We use the notation from Lemma 7.2. Suppose $H \cong H_0 \times Z\big(\mathrm{GL}(3,p)\big)$. Let P be a p-Sylow subgroup of H. Then $P \leq H_0$ and $N_H(P) = N_{H_0}(P) \times Z\big(\mathrm{GL}(3,p)\big)$. Huppert [25, II 7.1] shows $N_{H_0}(P) \cong C_p \rtimes C_{p-1}$. As also $Z\big(\mathrm{GL}(3,p)\big) \cong C_{p-1}$, every p-regular element of $N_H(P)$ has order a divisor of $p-1$. This is the claim.

■

For the following s and t denote integers relatively prime to p.

Two finite places ramify
Both $\mathfrak{p}$ and $\mathfrak{q}$ ramify tamely with index 2. Therefore we obtain

$$\mathrm{ind}(\mathfrak{p}) + \mathrm{ind}(\mathfrak{q}) \geq 2 \cdot \Big(p^3 - \frac{1}{2}(p^3 + p^2)\Big) = p^3 - p^2.$$

Lemma 7.4 gives $\mathrm{ind}(\infty) \geq (p^3-1)\big(1+\frac{1}{p-1}\big)$. These estimations violate the genus-0 condition.

No finite ramification
Lemma 7.4 yields $H = H' \cong \mathrm{PSL}(2,p)$. Suppose $|F_\infty| = ps$. Let $a \in \mathbb{N}$ be the well-defined integer with $F_\infty(a) > F_\infty(a+1) = 1$. Riemann-Hurwitz states

$$2g(E) - 2 = -2|H| + \frac{|H|}{ps}\big(ps - 1 + a(p-1)\big).$$

As $g(E) \geq 0$, we obtain

$$a \geq \frac{p^2 - 1 + s(p^3 - p - 4)}{(p+1)(p-1)^2}.$$

Section 3.2.1 shows

$$\mathrm{ind}(\infty) \geq (p^3-1)\Big(1 + \frac{1}{s}\Big) + \frac{1}{s}(a-1)(p^3-p);$$

this gives a contradiction to the genus-0 condition.

Exactly one finite place ramifies
As at most two places ramify in $Z|K(t)$, Lemma 7.4 shows that $\mathrm{Gal}(Z|K(t))$ is cyclic of order $r \mid p-1$ and both ∞ and $\mathfrak{p}$ ramify totally in this extension.

Suppose first that $\mathfrak{p}$ ramifies wildly. Then $F_\mathfrak{p} \cong C_p \rtimes C_{rt}$ with $rt \mid p-1$. Lemma 4.8 shows that $I_\mathfrak{p}$ contains at most p involutions. Thus,

$$\mathrm{ind}(\mathfrak{p}) \geq p^3 - \frac{1}{prt}\big(p^3 + p \cdot p^2 + (prt - p - 1)p\big) + \frac{1}{rt}\Big(p^3 - \frac{1}{p}\big(p^3 + (p-1)p\big)\Big).$$

The p'-part of the ramification index of ∞ is given by rs. We have $\mathrm{ind}(\infty) \geq (p^3-1)\Big(1+\frac{1}{rs}\Big)$. This yields

$$\mathrm{ind}(\infty) + \mathrm{ind}(\mathfrak{p}) - 2p^3 + 2 \geq \frac{t(p^3-1) + s(p-1)\big(p(p-2) - rt - 2\big)}{rst}.$$

As $p(p-2)-rt-2 \geq p(p-3)-1 > 0$, this case is impossible.

Now suppose that $\mathfrak{p}$ ramifies tamely. Then $F_{\mathfrak{p}} \cong C_{rt}$ and $F_\infty \cong C_p \rtimes C_{rs}$ with $rs \mid p-1$. Let a denote the well-defined integer with $F_\infty(a) > F_\infty(a+1) = 1$. For the following we use additionally the notation from section 3.2.1.

We show first that $I_\infty(u_a) \cong C_p$ is impossible. Suppose $I_\infty(u_a) \cong C_p$. Maus [37] gives $I_\infty(u_a) \trianglelefteq I_\infty(1)$; thus,

$$N_{I_\infty(1)}\big(I_\infty(u_a)\big)/C_{I_\infty(1)}\big(I_\infty(u_a)\big) \hookrightarrow \mathrm{Aut}\big(I_\infty(u_a)\big) \cong C_{p-1}.$$

As $\mathrm{Aut}(I_\infty(u_a))$ is a p'-group, it follows

$$I_\infty(1) = N_{I_\infty(1)}\big(I_\infty(u_a)\big) = C_{I_\infty(1)}\big(I_\infty(u_a)\big).$$

The total ramification of ∞ in $K(x)|K(t)$ shows $p^3 \mid |I_\infty|$. As a p-Sylow subgroup of H is cyclic of order p, it follows $p^2 \mid |J_\infty(1)|$. As $I_\infty(u_a) \not\leq N$, there exist $n \in N$ and $h \in H^\sharp$ such that $I_\infty(u_a) = \langle nh \rangle$. Moreover h cannot be an involution; hence, h fixes at most p points. But for all $m \in J_\infty(1)$

$$nh \cdot m = m \cdot nh \iff nhm = mnh = nmh \iff hm = mh \iff m = m^h.$$

But this is impossible.

Hence, $|I_\infty(u_a)| \geq p^2$ and $o\big(I_\infty(u_a)\big) \leq \frac{1}{p^2}\big(p^3 + (p^2-1)p\big) = 2p - \frac{1}{p}$. Since $2p - \frac{1}{p} < p^2$, Corollary 3.17 gives $o(I_\infty(u_a)) \leq p$.

Due to our classification in chapter 4 we may assume the genus of E to be ≥ 3. The above estimations together with the estimation for a coming from the Riemann-Hurwitz genus formula succeed in disproving the genus-0 condition.

7.2. The cases in characteristic $p \in \{2, 3\}$

In this section we use the computational algebra system `MAGMA` [3] to classify all pairs (A, G) being exceptional with A a primitive group of degree 8 or 27.

We obtain only one pair in characteristic 3 with H being elementary abelian of order 4. Hence, even in this case the extension $E|K(t)$ is tame.

8. Exceptional polynomials of degree p^r, r an odd prime, with 2-transitive group A

In this chapter we classify all exceptional polynomials of degree p^r, r an odd prime, such that the arithmetic monodromy group of f is 2-transitive. Our result will be

Theorem 8.1 *With the notation from page 23 suppose* $\deg f = p^r$. *Assume the arithmetic monodromy group of* f *is* 2*-transitive. If* f *is exceptional, then the extension* $E|K(t)$ *is tame.*
In particular, $g = 0$ *and Theorem 4.2 lists all possibilities for* f.

The 2-transitivity of A on N gives the transitivity of U on $N^\sharp$. The following lemma is based on Hering's classification of transitive subgroups of $\mathrm{GL}(r,p)$. A complete treatment of these groups can be found in Liebeck [36, Appendix 1].

Lemma 8.2 N *can be considered a one-dimensional* $\mathbb{F}_{p^r}$ *vector space.* U *acts on* N *as a subgroup of* $\Gamma\mathrm{L}(1,p^r)$.

Proof. r being an odd prime enforces either $U \leq \Gamma\mathrm{L}(1,p^r)$ or $\mathrm{SL}(r,p) \leq U$. Suppose the latter case holds. Huppert [25, II 6.10] shows the perfectness of $\mathrm{SL}(r,p)$; thus, we have $\mathrm{SL}(r,p) \leq H$. However, the transitivity of $\mathrm{SL}(r,p)$ on $N^\sharp$ is a contradiction to the exceptionality of f. ∎

We assume the extension $E|K(t)$ to be wild from now on. As the order of $\Gamma\mathrm{L}(1,p^r)$ is $|\Gamma\mathrm{L}(1,p^r)| = (p^r-1)\cdot r$, this immediately yields $p = r$. The next lemma gives some estimations for the number of fixed points of elements of A.

Lemma 8.3 *(1) Let* $1 \neq g \in A \leq \mathrm{A}\Gamma\mathrm{L}(1,p^p)$. *Then* g *fixes at most* p *elements. If* g *is* p*-regular, then it fixes exactly one point.*

(2) Let P *be a* p*-Sylow subgroup of* $\Gamma\mathrm{L}(1,p^p)$. *Then the normalizer* $N_{\Gamma\mathrm{L}(1,p^p)}(P)$ *is cyclic of order* $p(p-1)$.

Proof.

(1) As we are interested in the maximal number of fixed points of an element $1 \neq g \in A$, Lemma 3.12 allows us to assume $g \in U$. Lemma 8.2 gives the identification $N \cong \mathbb{F}_{p^p}$. Thus, the action of g on N is given by a tuple (a,b) with $0 \leq a < p$ and $b \in \mathbb{F}_{p^p}^\times$ such that

$$n^g = n^{p^a} \cdot b \qquad \text{for all } n \in N.$$

Suppose $n \in N^\sharp$ is fixed by g. Then n fulfills $n^{p^a-1} = b^{-1}$. If $m \in N^\sharp$ is also fixed by g, then we have $m = d \cdot n$ with $d \in N^\sharp$ and $d^{p^a-1} = 1$. Thus, $d \in \mathbb{F}_p^\times$ and $\mathrm{Fix}(g) = n \cdot \mathbb{F}_p$.

Suppose g is p-regular. A simple induction shows that the action of g^p is given by $(1,\beta)$ with $\beta \neq 1$. It follows that the unique fixed point of g^p and, thus, of g is the zero element of N. The assertion is due to Corollary 3.14.

(2) Since P is cyclic of order p, we may assume P to be generated by an element $g \in \Gamma\mathrm{L}(1,p^p)$ whose action is given by $(1,1)$. A simple calculation shows that $N_{\Gamma\mathrm{L}(1,p^p)}(P)$ is generated by g and the $(0,\beta)$-element h where β denotes a primitive element of $\mathbb{F}_p^\times$. As g and h commute, we get

$$N_{\Gamma\mathrm{L}(1,p^p)}(P) = \langle g,h\rangle \cong C_p \times C_{p-1} \cong C_{p(p-1)}.$$

■

Now we discuss the ramification behavior of the extension $E|K(t)$ in detail. As in the previous two chapters s and t denote integers relatively prime to p.

Two finite places ramify
Lemma 3.21 shows that both $\mathfrak{p}$ and $\mathfrak{q}$ ramify tamely with index 2. By Lemma 8.3 we have

$$\mathrm{ind}(\mathfrak{p}) + \mathrm{ind}(\mathfrak{q}) \geq 2\Big(n - \frac{1}{2}\big(n+1\big)\Big) = n-1.$$

Since $\mathrm{ind}(\infty) \geq n$, this is a contradiction to the genus-0 condition.

One finite place ramifies
Suppose $\mathfrak{p}$ ramifies wildly. Then $I_\mathfrak{p}$ embeds into the normalizer of a p-Sylow subgroup of $\Gamma\mathrm{L}(1,p^p)$; hence, $I_\mathfrak{p} \cong C_p \times C_t$ with $t \mid p-1$. If $g \in I_\mathfrak{p}$ does not have order 1 or p, the p-th power of g is p-regular. Thus, by Lemma 8.3 only elements of order 1 or p can have more than one fixed point. This shows

$$\mathrm{ind}(\mathfrak{p}) \geq n - \frac{1}{pt}\Big(n + (p-1)p + (pt-p)\Big) + \frac{1}{t}\Big(n - \frac{1}{p}\big(n+(p-1)p\big)\Big).$$

Together with $\mathrm{ind}(\infty) \geq n$ we get

$$\mathrm{ind}(\infty) + \mathrm{ind}(\mathfrak{p}) - 2n + 2 \geq \frac{n(p-2) + p(t+3-2p)}{pt};$$

as $p > 2$ and $n = p^p > 2p^2$, this case cannot occur.

Suppose $\mathfrak{p}$ ramifies tamely with index t. Then $\mathrm{ind}(\mathfrak{p}) \geq (n-1)\frac{t-1}{t}$. The group F_∞ is cyclic of order ps. Let $a \in \mathbb{N}$ denote the well-defined integer with $F_\infty(a) > F_\infty(a+1) = 1$. Then Riemann-Hurwitz gives

$$2g(E) - 2 = -2|H| + \frac{|H|}{t}(t-1) + \frac{|H|}{ps}\big(ps - 1 + a(p-1)\big).$$

Due to the classification in chapter 4 we may assume $g \geq 3$. This gives

$$a \geq \frac{4pst + |H|(ps+t)}{|H|t(p-1)}.$$

Together with the estimation of section 3.2.1 for $\mathrm{ind}(\infty)$ a a violation of the genus-0 condition results.

Only ∞ ramifies
We use the same idea as above. We obtain

$$a \geq \frac{ps(|H|+4) + |H|}{|H|(p-1)}.$$

This again induces a contradiction to the genus-0 condition.

Bibliography

[1] S. S. Abhyankar, *Nice equations for nice groups*, Isr. J. Math., **88** (1994), 1–23.

[2] D. M. Bloom, *The subgroups of* PSL$(3, q)$ *for odd* q, Trans. Am. Math. Soc., **127** (1967), 150–178.

[3] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I: The user language*, J. Symb. Comput., **24** (1997), 235–265.

[4] R. Brauer, *Some applications of the theory of blocks of characters of finite groups. II*, J. Algebra, **1** (1964), 307–334.

[5] R. Brauer, C. Nesbitt, *On the Modular Characters of Groups*, Ann. Math. (2), **42** (1941), 556–590.

[6] P. J. Cameron, *Finite permutation groups and finite simple groups*, Bull. Lond. Math. Soc., **13** (1981), 1–22.

[7] P. J. Cameron, W. M. Kantor, 2*-transitive and antiflag transitive collineation groups of finite projective spaces*, J. Algebra, **60** (1979), 384–422.

[8] G. Cardona, E. Nart, J. Pujolàs, *Curves of genus two over fields of even characteristic*, Math. Z., **250** (2005), 177–201.

[9] S. D. Cohen, *Exceptional polynomials and the reducibility of substitution polynomials*, Enseign. Math., II Sér., **36** (1990), 53–65.

[10] S. D. Cohen, R. W. Matthews, *A class of exceptional polynomials*, Trans. Am. Math. Soc., **345** (1994), 897–909.

[11] C. W. Curtis, I. Reiner, *Representation theory of finite groups and associative algebras*, John Wiley & Sons, Ltd., 1962.

[12] J. D. Dixon, B. Mortimer, *Permutation groups*, Springer-Verlag New York, Inc., 1996.

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

[14] M. D. Fried, R. M. Guralnick, J. Saxl, *Schur covers and Carlitz's conjecture*, Isr. J. Math., **82** (1993), 157–225.

[15] W. D. Geyer, *Invarianten binärer Formen*, in: H. Popp: *Classification of Algebraic Varieties and Compact Complex Manifolds*, Lecture Notes in Mathematics, **412** (1974), 36–39.

[16] R. M. Guralnick, *Frobenius groups as monodromy groups*, J. Aust. Math. Soc. Ser. A, **85** (2008), 191–196.

[17] R. M. Guralnick, P. Müller, *Exceptional polynomials of affine type*, J. Algebra, **194** (1997), 429–454.

[18] R. M. Guralnick, P. Müller, M. E. Zieve, *Exceptional polynomials of affine type, revisited*, *in preparation*.

[19] R. M. Guralnick, P. Müller, J. Saxl, *The rational function analogue of a question of Schur and exceptionality of permutation representations*, Mem. Am. Math. Soc., **773**, 2003.

[20] R. M. Guralnick, J. E. Rosenberg, M. E. Zieve, *A new family of exceptional polynomials in characteristic two*, Annals of Math., *to appear*.

[21] R. M. Guralnick, J. Saxl, *Generation of finite almost simple groups by conjugates*, J. Algebra, **268** (2003), 519–571.

[22] R. M. Guralnick, M. E. Zieve, *Polynomials with* PSL(2) *monodromy*, Annals of Math., *to appear*.

[23] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper II*, J. Reine Angew. Math., **175** (1936), 69–88.

[24] C. Hermite, *Sur les fonctions de sept lettres*, C. R. Acad. Sci. Paris, **57** (1863), 750–757.

[25] B. Huppert, *Endliche Gruppen I*, Springer-Verlag Berlin Heidelberg New York, 1967.

[26] B. Huppert, N. Blackburn, *Finite Groups III*, Springer-Verlag Berlin Heidelberg New York, 1982.

[27] D. Husemöller, *Elliptic Curves*, Springer-Verlag New York Inc., 1987.

[28] J. Igusa, *Arithmetic variety of moduli for genus two*, Ann. Math., **72** (1960), 612–649.

[29] I. M. Isaacs, *Character Theory of Finite Groups*, Academic Press, Inc., 1976.

[30] G. Kemper, *Generic polynomials are descent-generic*, Manuscr. Math., **105** (2001), 139-141.

[31] G. Kemper, E. Mattig, *Generic polynomials with few parameters*, J. Symb. Comput., **30** (2000), 843–857.

[32] H. Kurzweil, B. Stellmacher, *Theorie der endlichen Gruppen*, Springer-Verlag Berlin Heidelberg, 1998.

[33] S. Lang, *Algebra*, Springer Science+Business Media Inc., 2002.

[34] H. W. Lenstra, Jr., M. Zieve, *A family of exceptional polynomials in characteristic three*, in: S. Cohen (Ed.) et al., Finite fields and applications, Cambridge University Press. Lond. Math. Soc. Lect. Note, **233** (1996), 209–218.

[35] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, vol. 20, Addison-Wesley Publishing Company, Inc., 1983.

[36] M. W. Liebeck, *The affine permutation groups of rank three*, Proc. Lond. Math. Soc., III. Ser., **54** (1987), 477–516.

[37] E. Maus, *Die gruppentheoretische Struktur der Verzweigungsgruppenreihen*, J. Reine Angew. Math., **230** (1968), 1–28.

[38] P. Müller, *A Weil-bound free proof of Schur's conjecture*, Finite Fields Appl, **3** (1997), 25–32.

[39] P. Müller, *New examples of exceptional polynomials*, *in* "Finite Fields: Theory, Applications and Algorithms" (G. L. Mullen and P. J. Shiue, Eds.), Contemp. Math., **168** (1994), 245–249.

[40] P. M. Neumann, *Some primitive permutation groups*, Proc. Lond. Math. Soc., III. Ser., **50** (1985), 265–281.

[41] J. M. Ortega, *Matrix theory*, Plenum Press, New York, 1987.

[42] H. L. Schmid, *Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik*, J. Reine Angew. Math., **179** (1938), 5–15.

[43] I. Schur, *Über den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen*, Berl. Ber. (1923), 123–134.

[44] J.-P. Serre, *Local fields*, Springer-Verlag New York, Inc., 1979.

[45] T. Shaska, H. Völklein, *Elliptic subfields and automorphisms of genus 2 function fields*, Christensen, Chris (ed.) et al., Algebra, arithmetic and geometry with applications, July 19–26, 2000. Berlin: Springer.

[46] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag New York Inc, 1986.

[47] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag Berlin Heidelberg, 1993.

[48] G. Turnwald, *On Schur's conjecture*, J. Aust. Math. Soc. Ser. A, **58** (1995), 312–357.

[49] G. Turnwald, *Some notes on monodromy groups of polynomials*, in: Kálmán et al., *Number theory in progress*, vol. 1, Berlin: de Gruyter, 1999, 539–552.

[50] R. C. Valentini, M. L. Madan, *A Hauptsatz of L. E. Dickson and Artin-Schreier extensions*, J. Reine Angew. Math., **318** (1980), 156–177.

[51] B. L. van der Waerden, *Die Zerlegungs- und Trägheitsgruppe als Permutationsgruppen*, Math. Ann., **111** (1935), 731–733.

[52] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. f. Math., **III** (1892), 265–284.