

DAVENPORT PAIRS OVER FINITE FIELDS

WAYNE AITKEN, MICHAEL D. FRIED AND LINDA M. HOLT

We call a pair of polynomials $f, g \in \mathbb{F}_q[T]$ a *Davenport pair* (DP) if their value sets are equal, $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$, for *infinitely* many extensions of \mathbb{F}_q . If they are equal for *all* extensions of \mathbb{F}_q (for all $t \geq 1$), then we say (f, g) is a *strong Davenport pair* (SDP). Exceptional polynomials and SDP's are special cases of DP's. Monodromy/Galois-theoretic methods have successfully given much information on exceptional polynomials and SDP's. We use these methods to study DP's in general, and analogous situations for inclusions of value sets.

For example, if (f, g) is an SDP, then $f(T) - g(S) \in \mathbb{F}_q[T, S]$ is known to be reducible. This has interesting consequences. We extend this to DP's (that are not pairs of exceptional polynomials) and use reducibility to study the relationship between DP's and SDP's when f is indecomposable. Additionally, we show that DP's satisfy $(\deg f, q^t - 1) = (\deg g, q^t - 1)$ for all sufficiently large t with $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$. This extends Lenstra's theorem (Carlitz–Wan conjecture) concerning exceptional polynomials.

1. Introduction

Let \mathbb{F}_q be a finite field with q elements, and let p denote its characteristic. For any $f \in \mathbb{F}_q[T]$ and finite extension \mathbb{F}_{q^t} of \mathbb{F}_q , define the *value set* $\mathcal{V}_f(\mathbb{F}_{q^t})$ to be $\{f(a) \mid a \in \mathbb{F}_{q^t}\}$. Call (f, g) a *Davenport pair* over \mathbb{F}_q if $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$ for *infinitely* many values of t . For brevity, we use the acronym DP. We will see that (f, g) is automatically a Davenport pair (DP) if $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$ for one sufficiently large value of t . Call (f, g) a *strong Davenport pair* (SDP) over \mathbb{F}_q if $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$ for all $t \geq 1$.

The name *Davenport pair* honors a problem formulated by H. Davenport in the 1960's on a characteristic zero analogue of what we call SDP's. He asked which pairs $(f, g) \in \mathbb{Q}[T]$ have equal value sets mod l , for almost all primes l . (See Section 3.2 below for more details.)

1.1. Examples, summary of results, and problems. Call $f \in \mathbb{F}_q[T]$ an *exceptional polynomial* if $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathbb{F}_{q^t}$ for infinitely many values of t . So f is exceptional if and only if (f, T) is a DP. Thus both SDP's and exceptional polynomials are special types of Davenport pairs. One way to

create a DP which is not an SDP is to compose an SDP with exceptional polynomials.

Definition 1.1. Suppose (f, g) is an SDP and (h_1, h_2) is a pair of exceptional polynomials. Then $(f \circ h_1, g \circ h_2)$ is a DP, which we call an SDP-Ex composition.

SDP-Ex compositions have equal value sets over the base field \mathbb{F}_q , a property not possessed by all DP's.

Problem 1.2. Suppose (f, g) is a DP over \mathbb{F}_q , where

(1.1) q is sufficiently large and $\mathcal{V}_f(\mathbb{F}_q) = \mathcal{V}_g(\mathbb{F}_q)$.

When is (f, g) an SDP-Ex composition?

Here *sufficiently large* means larger than a bound depending on the degrees of f and g . Condition (1.1) can be replaced with a condition not requiring large q . By Corollary 4.4 there is a natural union of arithmetic progressions, defined Galois theoretically, containing all but finitely many of the values t for which $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$. We can replace (1.1) with the hypothesis that 1 is in this union of arithmetic progressions: $\bar{1} \in \mathcal{D}_{f,g}$ (see Definition 4.3).

Examples of Müller (see Remark 3.16) illustrate the phenomenon of *masking*, which suggests an approach for finding DP's satisfying (1.1) which are not SDP-Ex compositions.

Definition 1.3. Let $f, g, h \in \mathbb{F}_q[x]$. We say that h *masks* differences between value sets of f and g if $\mathcal{V}_f(\mathbb{F}_{q^t}) \neq \mathcal{V}_g(\mathbb{F}_{q^t})$ but $\mathcal{V}_{h \circ f}(\mathbb{F}_{q^t}) = \mathcal{V}_{h \circ g}(\mathbb{F}_{q^t})$ for an infinite number of t .

We now describe the key results of this paper from the point of view that several properties held by SDP-Ex compositions extend to DP's in general.

For example, if (f, g) is an SDP with $\deg f > 1$, then $f(T) - g(S)$ is known to be reducible in $\mathbb{F}_q[S, T]$. It follows that, $f \circ h_1(T) - g \circ h_2(S)$ is also reducible in $\mathbb{F}_q[S, T]$ for any pair (h_1, h_2) . This gives a property of SDP-Ex composition which extends: *If (f, g) is a DP satisfying (1.1), and f is not an exceptional polynomial, then $f(T) - g(S) \in \mathbb{F}_q[S, T]$ is reducible over \mathbb{F}_q (Corollary 4.12).*

As another example, consider this theorem of Lenstra [CF95], conjectured by Carlitz and Wan: *If $h \in \mathbb{F}_q[T]$ is exceptional, then $\deg h$ is relatively prime to $q - 1$.* It is also known that if (f, g) is an SDP, and if the degrees of f and g are prime to the characteristic p , then $\deg f = \deg g$. Thus if $f = f' \circ h_1$ and $g = g' \circ h_2$ where (f', g') is an SDP, (h_1, h_2) is a pair of exceptional polynomials, and $\deg f$ and $\deg g$ are prime to p , then $\gcd(\deg f, q - 1) = \gcd(\deg g, q - 1)$. This property of SDP-Ex composition holds for all DP's satisfying (1.1). It is a consequence of Theorem 5.4 (which is stronger since it makes no assumption on the degrees of f and g).

Finally, consider our Theorem 8.1, a result consistent with SDP-Ex composition. *Suppose that (f, g) is a DP and that f is indecomposable. Suppose also that f has degree prime to the characteristic p , and is neither an exceptional polynomial nor linearly related to a cyclic polynomial. Then $g = g' \circ h$ for some SDP (f, g') .*

We end this introduction with other problems related to DP's.

Problem 1.4. If (h_1, h_2) is a pair of polynomials such that $(f \circ h_1, g \circ h_2)$ is a DP for all SDP's (f, g) , must h_1 and h_2 be exceptional polynomials?

Other problems involve *multiplicities* of values. Call (f, g) a DP *with multiplicity* if there are an infinite number of t so that f and g not only have the same value sets over \mathbb{F}_{q^t} , but the values occur with the same multiplicities. That is, $f(T) - b$ and $g(T) - b$ have the same number of zeros in \mathbb{F}_{q^t} for each $b \in \mathbb{F}_{q^t}$. Similarly, call (f, g) an SDP *with multiplicity* if the multiplicity condition occurs for all values of t .

Problem 1.5. Are there SDP's which are not SDP's with multiplicity? Are there DP's which are not DP's with multiplicity?

[Mül98, Conjecture 5.2] considered the characteristic zero analogue of the first part of this question. Müller conjectures that Kronecker conjugate polynomials (the analogue of SDP's) are arithmetically equivalent (i.e., have the same multiplicities).

1.2. A bigger context for DP's. A polynomial $f \in \mathbb{F}_q[T]$ gives an algebraic map $f : \mathbb{A}^1 \rightarrow \mathbb{A}^1$, or, by adding points at infinity, an algebraic map $f : \mathbb{P}^1 \rightarrow \mathbb{P}^1$. Our approach, via the arithmetic and geometric monodromy groups associated with the map f , or pairs of maps (f, g) , extends considerably to include maps between algebraic curves defined over \mathbb{F}_q , and even to finite maps between higher-dimensional varieties. We concentrate on polynomial maps, as these offer a sufficient challenge while showing us their considerable structure without forcing excessive notation. Also, more can be proven for such maps since they have a totally ramified point, infinity, and the maps are between curves of genus zero. Still, we now briefly discuss a natural program that will benefit from the investigations of this paper, but requires considering the challenges of extending beyond polynomial maps.

We describe, in particular, the link between Davenport pairs and such topics as Weil vectors, Galois stratification, and Chow motives. Here, a *Weil vector* is the sequence of coefficients of a Poincaré series associated to a number-theoretic counting problem. For example, if V is a projective variety over \mathbb{F}_q , we get the familiar Weil vector $\mathcal{N} = (N_1, N_2, \dots)$ where N_t is the number of \mathbb{F}_{q^t} -rational points of V . The associated Poincaré series is $P_V(X) = \sum_{t=1}^{\infty} N_t X^t$, and the associated zeta function is $Z_V(X) = \exp\left(\sum_{t=1}^{\infty} N_t X^t / t\right)$.

Weil vectors also arise from other counting problems. For example, let V be a scheme (reduced, separated) of finite type over \mathbb{Z} . Consider the Weil vector $\mathcal{N} = (N_1, N_2, \dots)$, where N_t is the number of \mathbb{Z}/p^t -rational points which lift to \mathbb{Z}_p -rational points. The rationality of the associated Poincaré series was established by Denef [Den84].

Galois stratification is a tool for studying Weil vectors in a wide variety of counting problems (see [FS76] and [FJ86]). Denef and Loeser [DL] link Galois stratification and *Chow motives*. Given two Weil vectors $\mathcal{N} = (N_1, N_2, \dots)$ and $\mathcal{N}' = (N'_1, N'_2, \dots)$, the *characteristic set* $\chi(\mathcal{N}, \mathcal{N}')$ is $\{t \in \mathbb{N}^+ \mid N_t = N'_t\}$. Such characteristic sets, when the Weil vectors arise from Galois stratification, form Frobenius progressions (Definition 4.5).

To consider the link between DP's and these topics, consider your favorite equation $\Phi(T, \mathbf{U}) = 0$, where $\Phi \in \mathbb{F}_q[T, \mathbf{U}]$ and $\mathbf{U} = (U_1, \dots, U_s)$. Consider also the Weil vector $\mathcal{N}(\Phi) = (N_1(\Phi), N_2(\Phi), \dots)$, where $N_t(\Phi)$ is the number of solutions over \mathbb{F}_{q^t} . You often substitute a polynomial or rational function $f(T)$ for T to get the related equation $\Phi(f(T), \mathbf{U}) = 0$. Write Φ_f for $\Phi(f(T), \mathbf{U})$. Let (f, g) be a pair of polynomials, and let $\chi(f, g)$ be the set of t with the property that $\mathcal{V}_f(\mathbb{F}_{q^t})$ and $\mathcal{V}_g(\mathbb{F}_{q^t})$ are equal, and every value occurs with the same multiplicity. We assume $\chi(f, g)$ is infinite. In other words, (f, g) is a DP with multiplicity. Observe that $\chi(f, g) \subseteq \chi(\mathcal{N}(\Phi_f), \mathcal{N}(\Phi_g))$.

This gives us a procedure for generating nontrivial (nonfinite) characteristic sets relating many different pairs of Weil vectors. The resulting characteristic sets must contain a common Frobenius progression $\chi(f, g)$ regardless of your choice of *favorite equation*. This suggests the importance of the study of Frobenius progressions of the form $\chi(f, g)$ from the more general Weil vector viewpoint.

For any pair of Weil vectors, attached to any elementary problem (as in [FS76]), there is a characteristic set at which the two Weil vectors are equal. The argument of [Fri94, Riem. Hyp. Lem. 2.2] extends to show that such a characteristic set is always, modulo finite sets, a union of Frobenius progressions. We consider such a characteristic set a *relation* among Weil vectors. It is a fundamental problem to consider how such relations arise and to what extent they arise from sets $\chi(f, g)$ as in our problem above.

2. Notations and conventions

Note that $(f(T), f(T^p))$ is an SDP (as above, $f \in \mathbb{F}_q[T]$ and p is the characteristic of \mathbb{F}_q). So, for value set problems, it is harmless to replace any polynomial of the form $f(T^p)$ by $f(T)$. By repeating this process starting with a given polynomial, we obtain a polynomial whose derivative is not the zero polynomial, and whose value set, in all finite extensions, is the same as the original polynomial. This justifies the following convention. *Assume all polynomials appearing in this paper have nonzero derivatives.*

Let F be a field. We are most interested in $F = \mathbb{F}_q$, especially when we are considering value sets, but many of our results hold for more general F . Fix an algebraic closure $\overline{F(z)}$ of $F(z)$, where z is a fixed transcendental element over F , and regard \overline{F} as a subfield of $\overline{F(z)}$. We use the letter T (as above) for a general transcendental element not in $\overline{F(z)}$. We use S and T when we need two independent transcendental elements (neither in $\overline{F(z)}$).

For any $f \in F[T]$, let $\Omega_f \subseteq \overline{F(z)}$ be the splitting field of $f(T) - z$. Since $f(T) - z$ has z -degree 1, it is irreducible in $F(z)[T]$. It is also separable (the derivative f' is not the zero polynomial). Call

$$\widehat{G}_f = \text{Gal}(\Omega_f/F(z))$$

the *arithmetic monodromy group* of f . Let $\widehat{F}_f = \Omega_f \cap \overline{F}$. Call

$$G_f = \text{Gal}(\Omega_f/\widehat{F}_f(z)) \subseteq \widehat{G}_f$$

the *geometric monodromy group*. Let $n = \deg f$, and let $\{x_1, x_2, \dots, x_n\}$ be the zeros of $f(T) - z$ in Ω_f . If H is \widehat{G}_f or a subgroup, denote the elements of H which fix x_i by $H(x_i)$. For example, $\widehat{G}_f(x_i) = \text{Gal}(\Omega_f/F(x_i))$.

Think of $f \in F[T]$ as an algebraic map $f : \mathbb{A}^1 \rightarrow \mathbb{A}^1$. By adding a point at infinity, also regard a polynomial (or rational function) as an algebraic covering map $f : \mathbb{P}^1 \rightarrow \mathbb{P}^1$.

Now consider the case $F = \mathbb{F}_q$. Here we abuse notation and write $\widehat{\mathbb{F}}_f$ for \widehat{F}_f . The quotient \widehat{G}_f/G_f is isomorphic to the cyclic group $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$, where $d = [\widehat{\mathbb{F}}_f : \mathbb{F}_q]$. Not only is $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ cyclic, but it is *canonically* isomorphic to \mathbb{Z}/d by the map sending the Frobenius automorphism $a \mapsto a^q$ to 1. Let $\widehat{G}_{f,t}$ be the G_f -coset of elements $\sigma \in \widehat{G}_f$ for which $\sigma|_{\widehat{\mathbb{F}}_f}$ is the map $a \mapsto a^{q^t}$. So $\widehat{G}_{f,t}$ consists of elements of \widehat{G}_f whose image in \mathbb{Z}/d is congruent to t . Thus $\widehat{G}_{f,t}$ depends only on t modulo d .

Now consider analogous definitions for pairs of polynomials (f, g) , first for a general field F . Let $\Omega_{f,g} = \Omega_f \cdot \Omega_g \subseteq \overline{F(z)}$ be the splitting field of the product $(f(T) - z)(g(T) - z)$. Let $\widehat{F}_{f,g} = \Omega_{f,g} \cap \overline{F}$. Define the arithmetic monodromy group of the pair as $\widehat{G}_{f,g} = \text{Gal}(\Omega_{f,g}/F(z))$ and the geometric monodromy group as $G_{f,g} = \text{Gal}(\Omega_{f,g}/\widehat{F}_{f,g}(z))$.

Let $\{x_1, x_2, \dots, x_n\}$ be the zeros of $f(T) - z$, and $\{y_1, y_2, \dots, y_m\}$ those of $g(T) - z$. Then $\widehat{G}_{f,g}$ acts on $\{x_i\}$, on $\{y_j\}$, and on the Cartesian product $\{x_i\} \times \{y_j\}$. For H equal to $\widehat{G}_{f,g}$ or a subgroup, $H(x_i)$, $H(y_j)$, and $H(x_i, y_j)$ have the usual meanings as stabilizer subgroups.

Note that $\widehat{G}_{f,g}$ is the fiber product of \widehat{G}_f and \widehat{G}_g over the common quotient group $\text{Gal}(\Omega_f \cap \Omega_g/F(z))$.

Now consider the case $F = \mathbb{F}_q$. We abuse notation and write $\widehat{\mathbb{F}}_{f,g}$ for $\widehat{F}_{f,g}$. As before, we have the exact sequence

$$1 \rightarrow G_{f,g} \rightarrow \widehat{G}_{f,g} \rightarrow \mathbb{Z}/d \rightarrow 1,$$

where $d = [\widehat{\mathbb{F}}_{f,g} : \mathbb{F}_q]$. Denote the elements of $\widehat{G}_{f,g}$ mapping to $t \bmod d$ by $\widehat{G}_{f,g,t}$. So $\widehat{G}_{f,g,t}$ is the $G_{f,g}$ -coset of all σ that restrict on \mathbb{F}_{q^d} to the automorphism $x \mapsto x^{q^t}$.

Again consider a general field F . Call $f \in F[T]$ *decomposable* over F if $f = f_1 \circ f_2$ with $f_1, f_2 \in F[T]$, $\deg f_i > 1$, $i = 1, 2$. Otherwise, f is *indecomposable* over F .

If $f, l_1, l_2 \in F[T]$ are polynomials with $\deg l_1 = \deg l_2 = 1$, then we say f and $l_1 \circ f \circ l_2$ are *linearly related over F* . Linearly related polynomials have isomorphic monodromy groups and equivalent actions of their monodromy groups on their respective zero sets.

When comparing value sets, we are interested in a special type of linearly related polynomial pairs. If $f, l \in F[T]$ are polynomials such that $\deg l = 1$, then we say that f and $f \circ l$ are *linearly related on the inside over F* . For example, a pair of polynomials $f, g \in \mathbb{F}_q[T]$ linearly related on the inside over \mathbb{F}_q clearly forms an SDP. We call such SDP's *trivial*. As explained in the next section, there are examples of nontrivial SDP's.

If n is a positive integer, we consider the statement n is *prime to the characteristic of F* to be vacuously true if F has characteristic zero.

3. Review of earlier results

We summarize some of what is known concerning value sets, exceptional polynomials, SDP's, and DP's.

3.1. Value sets from the monodromy point of view. Consider a polynomial map as a covering map $f : \mathbb{P}^1 \rightarrow \mathbb{P}^1$. Suppose $b \in \mathbb{F}_{q^t} = \mathbb{A}^1(\mathbb{F}_{q^t})$ is not a branch point for this map. Then $b \in \mathcal{V}_f(\mathbb{F}_{q^t})$ if and only if the associated Frobenius element $\text{Frob}_t(b) \in \widehat{G}_f$ fixes at least one zero of $f(T) - z$. Further, the number of $a \in \mathbb{F}_{q^t}$ satisfying $f(a) = b$ is equal to the number of fixed points of $\text{Frob}_t(b)$ acting on the zeros $\{x_i\}$. We call this the *Frobenius Principle*. It follows from an early result of Artin [Art23, §2]. Here

$$\text{Frob}_t(b) = i \left(\frac{\Omega_f \cdot \mathbb{F}_{q^t}/\mathbb{F}_{q^t}(z)}{P_b} \right),$$

where P_b is the place of $\mathbb{F}_{q^t}(z)$ associated to $b \in \mathbb{A}^1(\mathbb{F}_{q^t})$, $(\frac{L/K}{P})$ is the Artin symbol, and $i : \text{Gal}(\Omega_f \cdot \mathbb{F}_{q^t}/\mathbb{F}_{q^t}(z)) \rightarrow \widehat{G}_f$ is the natural inclusion induced by restriction. The Artin symbol is defined up to conjugacy, so the number of fixed points of $\text{Frob}_t(b)$ is well-defined.

Observe that $\text{Frob}_t(b) \in \widehat{G}_{f,t}$. Conversely, the nonregular analog of the Chebotarev Density Theorem implies the proportion of $b \in \mathbb{F}_{q^t}$ with $\text{Frob}_t(b)$

in a given conjugacy class $C \subseteq \widehat{G}_{f,t}$ is approximately $|C|/|\widehat{G}_{f,t}|$. More precisely, if $p(C)$ is the proportion of $b \in \mathbb{F}_{q^t}$ such that $\text{Frob}_t(b) \in C$ and b is not a branch point, then

$$\left| p(C) - \frac{|C|}{|\widehat{G}_{f,t}|} \right| < B|C|q^{-t/2}.$$

The best B depends on f , but we can find a B depending only on $n = \deg f$. For example, the bound of Proposition 5.16 of [FJ86], specialized to the current situation, gives $B = 4(g+2)$, where g is the genus of Ω_f . There is a bound in n for this genus g , and hence for B . (From Riemann–Hurwitz, bounding higher ramification group orders bounds the $\Omega/\widehat{\mathbb{F}}_f(z)$ different divisor degree. To bound the nontrivial higher ramification groups in G_f , combine an obvious bound on the $\widehat{\mathbb{F}}_f(x_i)/\widehat{\mathbb{F}}_f(z)$ different degree with the corollary to Proposition 4, Chapter IV, §1, of [Ser79].)

Let $N(\sigma)$ be the cardinality of those $\{x_1, \dots, x_n\}$ fixed by $\sigma \in \widehat{G}_{f,t}$. Then

$$(3.1) \quad \sum_{\sigma \in \widehat{G}_{f,t}} N(\sigma) = |\widehat{G}_{f,t}|.$$

This is a corollary of the Chebotarev Density Theorem, taking $t' \equiv t \pmod{d}$, where $d = [\widehat{\mathbb{F}}_f : \mathbb{F}_q]$ and t' is large. It is also a consequence of the following group-theoretical lemma [GW97, Lemma 3.1], taking $H = G_f$, $H^* = \widehat{G}_{f,t}$, $G \subseteq \widehat{G}_f$ the group generated by G_f and $\widehat{G}_{f,t}$, and $r = 1$.

Lemma 3.1. *Let G be a finite group acting on a finite set S . Let H be a normal subgroup of G such that G/H is cyclic. Finally, let H^* be a coset whose image generates G/H . Then*

$$\frac{1}{|H^*|} \sum_{\sigma \in H^*} N(\sigma) = r,$$

where r is the number of H -orbits in S which are also G -orbits, and where $N(\sigma)$ is the number of points in S that $\sigma \in G$ fixes.

(The case when $H = G$ is well-known; see Lemma 7.1.)

From (3.1), the following are equivalent:

- (3.2) Every element of $\widehat{G}_{f,t}$ fixes at least one element of $\{x_i\}$.
- (3.3) Every element of $\widehat{G}_{f,t}$ fixes at most one element of $\{x_i\}$.
- (3.4) Every element of $\widehat{G}_{f,t}$ fixes exactly one element of $\{x_i\}$.

Remark 3.2. Suppose any of (3.2), (3.3) or (3.4) hold. Then, for any $b \in \mathbb{F}_{q^t}$ not a branch point, $\text{Frob}_t(b)$ fixes exactly one zero. So, by the Frobenius Principle, $f : \mathbb{F}_{q^t} \rightarrow \mathbb{F}_{q^t}$ is bijective on the set of points mapping to nonbranch points.

When $b \in \mathbb{F}_{q^t}$ is a branch point, one has a *Frobenius coset* instead of a Frobenius element. To determine the number of $a \in \mathbb{F}_{q^t}$ satisfying $f(a) = b$, consider the action of the associated decomposition group D and inertia group I on the zeros $\{x_i\}$. It is well-known that one counts I -orbits which are also D -orbits (for example, [vdW35]). Lemma 3.1, with $G = D$, $H = I$, and H^* the Frobenius coset, shows that *the number of $a \in \mathbb{F}_{q^t}$ mapping to b is the average number of $\{x_i\}$ fixed by σ as σ varies over the Frobenius coset*. We call this the *Strong Frobenius Principle*. So, (3.4) implies bijectivity even when we allow points above branch points. (Note: in the Frobenius Principle or the Strong Frobenius Principle, we can replace \widehat{G}_f with the Galois group of any normal extension of $\mathbb{F}_q(z)$ containing Ω_f .)

Definition 3.3. Let $0 \leq \epsilon \leq 1$. Call a polynomial map $f : \mathbb{F}_{q^t} \rightarrow \mathbb{F}_{q^t}$ ϵ -almost injective if the proportion of points $b \in \mathbb{F}_{q^t}$ which either have at most one $a \in \mathbb{F}_{q^t}$ satisfying $f(a) = b$ or are branch points is at least $1 - \epsilon$. Similarly, call $f : \mathbb{F}_{q^t} \rightarrow \mathbb{F}_{q^t}$ ϵ -almost surjective if the proportion of points $b \in \mathbb{F}_{q^t}$ which are either in the value set $\mathcal{V}_f(\mathbb{F}_{q^t})$ or are branch points is at least $1 - \epsilon$.

The above considerations lead easily to the following theorem.

Theorem 3.4. Let $0 \leq \epsilon < 1/|\widehat{G}_{f,t}|$, and let $\delta = 1/|\widehat{G}_{f,t}| - \epsilon$. If $q^t \geq (B/\delta)^2$, where B is the constant in the Chebotarev Density Theorem, then the following are equivalent:

- (3.5) $f : \mathbb{F}_{q^t} \rightarrow \mathbb{F}_{q^t}$ is ϵ -almost surjective.
- (3.6) $f : \mathbb{F}_{q^t} \rightarrow \mathbb{F}_{q^t}$ is ϵ -almost injective.
- (3.7) $f : \mathbb{F}_{q^t} \rightarrow \mathbb{F}_{q^t}$ is bijective.
- (3.8) Every element of $\widehat{G}_{f,t}$ fixes exactly one zero of $f(T) - z$.

For general q^t , large or small, (3.8) implies (3.7).

Remark 3.5. See [Fri74, Lemma 2 and Theorem 1] for a generalization to multivariable polynomial maps $\mathbb{A}^n \rightarrow \mathbb{A}^n$. This theorem has also been generalized [FGS93, p. 186] to covering maps $X \rightarrow Y$ between absolutely irreducible curves over \mathbb{F}_q . (The statement in [FGS93] is essentially the case where $\epsilon = 0$, but the methods clearly work for small $\epsilon > 0$.)

The upper bound for ϵ in the implication (3.5) \Rightarrow (3.8) can be replaced by $1/\deg f$. With *a priori* restrictions on the monodromy groups involved, one can often do better (see [GW97]).

Corollary 3.6. A polynomial $f \in \mathbb{F}_q[T]$ is exceptional if and only if any of the equivalent conditions (3.2) to (3.7) hold for a suitable value of t and ϵ .

If (3.7) holds for t , then it holds for any divisor of t . This yields:

Corollary 3.7. If $f \in \mathbb{F}_q[T]$ is an exceptional polynomial and any of the (equivalent) conditions (3.2) to (3.4) are true of $t = t_0$, then these conditions are true of any t satisfying $\gcd(t, d) \mid \gcd(t_0, d)$ where $d = [\widehat{\mathbb{F}}_f : \mathbb{F}_q]$.

A similar analysis gives a monodromy interpretation for $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$.

Theorem 3.8. *Let $f, g \in \mathbb{F}_q[T]$. Suppose that, for some t ,*

- (3.9) *every $\sigma \in \widehat{G}_{f,g,t}$ fixes an element of $\{x_i\}$ if and only if it fixes an element of $\{y_j\}$ (as usual, $\{x_i\}$ are the zeros of $f(T) - z$ and $\{y_j\}$ are the zeros of $g(T) - z$).*

Then $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$.

Conversely, if $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$ for t sufficiently large, then (3.9) holds.

Remark 3.9. The Chebotarev Density Theorem together with the Frobenius Principle gives the converse above, even generalizing it by replacing the hypothesis $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$ with an ϵ -almost equality (analogous to Theorem 3.4).

To prove that (3.9) implies $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$ one can use the Strong Frobenius Principle (as in Remark 3.2) to cover both branch points and nonbranch points. Alternatively, one can use the following argument, a straightforward adaptation to the current situation of the second part of the proof of [FJ86, Lem. 19.27]. Let $b \in \mathcal{V}_f(\mathbb{F}_{q^t})$, and let $a \in \mathbb{F}_{q^t}$ be a zero of $f(T) - b$. Consider the homomorphism $\mathbb{F}_q[x_1] \rightarrow \mathbb{F}_{q^t}$ with $x_1 \mapsto a$ (and so $z \mapsto b$). Extend this to a homomorphism $\varphi : R \rightarrow \overline{\mathbb{F}_q}$, where R is the integral closure of $\mathbb{F}_q[z]$ in $\Omega_{f,g}$. Let $D(\varphi) \subseteq \widehat{G}_{f,g}(x_1)$ be the decomposition group associated to φ (the subgroup fixing $\ker \varphi$). Since $D(\varphi)$ is a decomposition group, the homomorphism $D(\varphi) \rightarrow \text{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q(a))$ associated to the residue maps is surjective, where \mathbb{F}_{q^s} is the image of φ . Thus, some $\tau \in D(\varphi)$ has image in $\text{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q(a))$ the q^t -power Frobenius map $u \mapsto u^{q^t}$. Note that τ fixes x_1 and that $\tau \in \widehat{G}_{f,g,t}$. From (3.9), τ fixes some y_j . Let $c = \varphi(y_j)$. The image of τ acting on \mathbb{F}_{q^s} fixes c . Thus, $c \in \mathbb{F}_{q^t}$. Since $g(c) = b$, conclude $b \in \mathcal{V}_g(\mathbb{F}_{q^t})$.

For inclusions of value sets we have:

Theorem 3.10. *Let $f, g \in \mathbb{F}_q[T]$. Suppose that, for some t ,*

- (3.10) *every $\sigma \in \widehat{G}_{f,g,t}$ that fixes some x_i also fixes some y_j .*

Then $\mathcal{V}_f(\mathbb{F}_{q^t}) \subseteq \mathcal{V}_g(\mathbb{F}_{q^t})$.

Conversely, if $\mathcal{V}_f(\mathbb{F}_{q^t}) \subseteq \mathcal{V}_g(\mathbb{F}_{q^t})$ for t sufficiently large, then (3.10) holds.

Remark 3.11. We can replace (3.10) with:

- (3.11) Every $\sigma \in \widehat{G}_{f,g,t}(x_1)$ fixes an element of $\{y_j\}$.

3.2. Strong Davenport pairs. [Fri99] discusses the theory of SDP's starting with the following characterization (a corollary of Theorem 3.8).

Corollary 3.12. *The pair (f, g) in $\mathbb{F}_q[T]$ is an SDP if and only if*

- (3.12) *for $\sigma \in \widehat{G}_{f,g}$, fixing an element of $\{x_i\}$ is equivalent to fixing an element of $\{y_j\}$.*

An analogous result holds for polynomials over number fields ([FJ86, Lemma 19.27] or [Mül98, Theorem 2.3]). Then (3.12) is equivalent to f and g being *Kronecker conjugate* over a number field K : their value sets are equal modulo all but a finite number of nonzero prime ideals of K .

We generalize the following well-known result ([Fri73, Proposition 3], [FJ86, Lemma 19.31], and [Fri99]) to DP's (see Corollary 4.12).

Theorem 3.13. *Let $f, g \in \mathbb{F}_q[T]$. If (f, g) is an SDP where $\deg f > 1$, then $f(T) - g(S) \in \mathbb{F}_q[S, T]$ is reducible.*

This gives several immediate corollaries. For example, if f and g have relatively prime degrees, then (f, g) is not an SDP. As another example, if (f, g) is an SDP with each degree at most 3, then (f, g) is a trivial SDP: reducibility implies the existence of a linear factor, which implies that f and g are linearly related on the inside.

When $f : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ and $g : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ are tamely ramified, the results in [Fri73] in characteristic 0 are relevant, implying major restrictions on the pair (f, g) . We now review these results.

Let K be a number field and let $f, g \in K[T]$. If f and g are Kronecker conjugate and $\deg f > 1$, the analogue of Theorem 3.13 holds: $f(T) - g(S)$ is reducible. When f is indecomposable, the reducibility of $f(T) - g(S)$ forces the geometric monodromy group of f to be one of a small list, and $\deg f$ to be one of 7, 11, 13, 15, 21, and 31. That f and g are Kronecker conjugate also forces $\deg f = \deg g$. This together with the Grothendieck Lifting Theorem gives the following theorem in positive characteristic.

Theorem 3.14. *Consider an SDP (f, g) over \mathbb{F}_q with these properties:*

(3.13) *$f : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ is tamely ramified.*

(3.14) *f is indecomposable.*

Then $\deg f = \deg g$, and both $\deg f$ and G_f satisfy the above restrictions.

The following result from [Fri99, Thm 5.7] shows degrees are not bounded when we allow $f : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ to have wild ramification.

Theorem 3.15. *Over any field \mathbb{F}_q there are infinitely many n prime to the characteristic for which nontrivial SDP's (f, g) exist with $n = \deg f = \deg g$ and f indecomposable.*

The monodromy groups appearing in these examples are subgroups of the projective linear groups over finite fields of characteristic p .

Finally we mention what is known concerning Davenport's original question. If $K = \mathbb{Q}$ there are no nontrivial Kronecker conjugate polynomials with f indecomposable [Fri73], or with f and g each compositions of two indecomposable polynomials of degree at least 2 [Mül98]. Still, $f(T) = T^8$ and $g(T) = 16T^8$ are Kronecker conjugate polynomials, each the composition of *three* indecomposable polynomials. Over \mathbb{Q} , Müller suggests this is a singular anomaly.

Remark 3.16 (Müller’s work on masking). If (f, g) is an SDP, then the pair $(h \circ f, h \circ g)$ is also an SDP for all $h \in \mathbb{F}_q[T]$. More surprisingly, there are pairs (f, g) which are not SDP’s (not even DP’s) and $h \in \mathbb{F}_q[T]$ of positive degree such that $(h \circ f, h \circ g)$ is an SDP. That is, h *masks* (see Definition 1.3) the difference between f and g . Müller [Mül98, §4] gave examples of this over number fields and they apply over suitable \mathbb{F}_q . So this, in addition to the case where the pairs are indecomposable in Theorem 3.15 shows there are many nontrivial SDP’s. Müller’s examples give polynomials with equivalent permutation characters, so they yield SDP’s *with multiplicity*.

3.3. Other related value set work. Earlier related work (not exclusive to SDP’s or exceptional polynomials) did not concern DP’s *per se*, but rather polynomials with equal value sets over the ground field \mathbb{F}_q . Note: for q large, such pairs are DP’s (Corollary 4.2).

For example, [Coh81] studies pairs of rational functions $f, g \in \mathbb{F}_q(T)$ satisfying $\mathcal{V}_f(\mathbb{F}_q) \subseteq \mathcal{V}_g(\mathbb{F}_q)$. The main result is a classification of such f and g with $\deg g \leq 4$, where the characteristic is greater than 3 and q is large (lower bounds depending on $\deg f$). Other much earlier work: McCann and Williams (value set equalities for polynomials of degree 3), Mordell (also for degree 3), and Carlitz (value set inclusions with $g(T) = T^m$).

Finally, [Ait98] studies the overlap between $\mathcal{V}_f(\mathbb{F}_q)$ and $\mathcal{V}_g(\mathbb{F}_q)$ when the two sets are not equal, which, for large q , yields a criterion for whether or not two polynomials form a DP.

4. Basic results concerning Davenport pairs

Let $f, g \in \mathbb{F}_q[T]$, and let $d = [\widehat{\mathbb{F}}_{f,g} : \mathbb{F}_q]$. Below are corollaries of Theorem 3.8.

Corollary 4.1. *The pair (f, g) is a DP if and only if, for some t , (3.9) holds.*

Corollary 4.2. *The pair (f, g) is a DP if and only if $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$ for a sufficiently large t .*

Here, *sufficiently large* means that q^t exceeds some bound depending only on the maximum of the degrees of f and g .

Condition (3.9) depends only on $t \bmod d$. Thus, if (3.9) holds for one t , it holds for infinitely many t ; the set of such t forms a union of arithmetic progressions. For any integer t , denote its image in \mathbb{Z}/d by \bar{t} .

Definition 4.3. Let $\mathcal{D}_{f,g} = \{\bar{t} \in \mathbb{Z}/d \mid (3.9) \text{ holds for } t\}$. So (f, g) is a DP if and only if $\mathcal{D}_{f,g}$ is not empty, and (f, g) is an SDP if and only if $\mathcal{D}_{f,g} = \mathbb{Z}/d$.

Corollary 4.4. *For t sufficiently large, $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$ if and only if $\bar{t} \in \mathcal{D}_{f,g}$. For all t , large or small, $\bar{t} \in \mathcal{D}_{f,g}$ implies $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$.*

The set $\mathcal{D}_{f,g}$ is an example of a *Frobenius set*:

Definition 4.5. A *Frobenius set (mod d)* is a subset S of \mathbb{Z}/d with the following property. If $a \in S$, then so is ua , where u is a unit in \mathbb{Z}/d . Equivalently, if a, b have the same order in \mathbb{Z}/d , then $a \in S$ if and only if $b \in S$. So S is completely determined by the data (d, D) , where D is the set of divisors of d representing the orders in \mathbb{Z}/d of the elements in S .

Call a subset A of \mathbb{N}^+ (or \mathbb{N} or \mathbb{Z}) a *pure Frobenius progression* if there exists a Frobenius set $S \subseteq \mathbb{Z}/d$ so that $a \in A$ if and only if $\bar{a} \in S$. Finally, call a subset A of \mathbb{N}^+ a *Frobenius progression* if it differs from a pure Frobenius progression by only a finite number of elements.

Remark 4.6. If (f, g) is a pair of polynomials, then $\mathcal{D}_{f,g}$ is a Frobenius set. The set of t satisfying (3.9) forms a pure Frobenius progression. Finally, the set of t where $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$ is a Frobenius progression (containing the associated pure Frobenius progression).

For exceptional polynomials, the associated Frobenius set has additional structure: if $d_1 \in D$, where D is the set of divisors characterizing the Frobenius set, and k is a positive integer such that $kd_1 | d$, then $kd_1 \in D$. This follows from Corollary 3.7. One consequence is that $\mathcal{D}_{f,T}$ contains $(\mathbb{Z}/d)^*$. In particular, $1 \in \mathcal{D}_{f,T}$.

When we require $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$ with multiplicity, we also get Frobenius progressions. Later we discuss Frobenius progressions in the context of the reducibility of $f(T) - g(S)$.

The following lemma, a basic application of the Riemann Hypothesis, is needed to prove reducibility.

Lemma 4.7. Suppose $\Phi(S, T) \in \mathbb{F}_q[S, T]$ has A_t irreducible factors over $\mathbb{F}_{q^t}[S, T]$, of which N_t are absolutely irreducible. Then M_t , the number of \mathbb{F}_{q^t} -points in the algebraic set $\Phi(S, T) = 0$, is approximately $N_t \cdot q^t$. More precisely, $|M_t/q^t - N_t| < cq^{-t/2}$ for some constant c which depends only on the total degree of Φ .

Proof. Factor Φ over $\mathbb{F}_{q^t}[S, T]$ as $\Phi_1 \cdots \Phi_{A_t}$. Index the factors so $\Phi_1, \dots, \Phi_{N_t}$ are absolutely irreducible. Let M_i be the number of \mathbb{F}_{q^t} -points of the variety $\Phi_i = 0$. Bezout's Theorem bounds $|M_t - \sum M_i|$. For $i > N_t$, $|M_i|$ is bounded (use Bezout's Theorem here as well). For $i \leq N_t$ let \tilde{X}_i be the nonsingular projective curve corresponding to the affine curve $\Phi_i = 0$. Let \tilde{M}_i be the number of \mathbb{F}_{q^t} -points on \tilde{X}_i . Then $|M_i - \tilde{M}_i|$ is bounded. All these bounds depend on the total degree of Φ , not on q^t . Finally, the Riemann Hypothesis bounds $|\tilde{M}_i - q^t|$, giving the desired bound for $|M_t - N_t \cdot q^t|$. \square

Theorem 4.8. Suppose $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$ for sufficiently large t . Let N_t be the number of absolutely irreducible factors of $f(T) - g(S) \in \mathbb{F}_q[S, T]$ defined

over \mathbb{F}_{q^t} . Then $N_t \geq 1$. Furthermore, $N_t = 1$ if and only if

$$\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathbb{F}_{q^t} = \mathcal{V}_g(\mathbb{F}_{q^t}).$$

(So $N_t = 1$ implies that f and g are both exceptional polynomials.)

Here, t sufficiently large means that q^t is larger than an effectively computable bound which depends only on $\deg f$ and $\deg g$.

Proof. Let M_t be the number of \mathbb{F}_{q^t} -solutions of $f(T) - g(S) = 0$. Then $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$ implies $M_t \geq q^t$. Lemma 4.7 shows $N_t \geq 1$. Furthermore, if $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathbb{F}_{q^t}$, then $M_t = q^t$, so $N_t = 1$.

Now suppose $\mathcal{V}_f(\mathbb{F}_{q^t}) \neq \mathbb{F}_{q^t}$. Theorem 3.4 gives an $A > 0$ (independent of t) with at least $A \cdot q^t$ elements of $\mathcal{V}_f(\mathbb{F}_{q^t})$ having at least two elements of \mathbb{F}_{q^t} mapping to it under f . This implies $M_t \geq q^t \cdot (A + 1)$. Thus $N_t > 1$. \square

Remark 4.9. Let $f, g \in F[T]$. Gauss' Lemma implies that the factorization of $f(T) - g(S)$ into irreducibles in $F[S, T]$ gives a factorization of $f(T) - g(y_j)$ into irreducibles in $F(y_j)[T]$ (with all factors having positive T -degree). By basic Galois theory, these irreducible factors of $f(T) - g(y_j)$ over $\mathbb{F}_q(y_j)$ correspond to the orbits of $\{x_i\}$ under the action of $\widehat{G}_{f,g}(y_j)$.

Conclude that the F -irreducible factors of $f(T) - g(S)$ correspond to the orbits of $\{x_i\}$ under the action of $\widehat{G}_{f,g}(y_j)$. Further, if Φ is a factor associated with an orbit O then $|O| = \deg_T \Phi$. Similar statements apply for the $\widehat{G}_{f,g}(x_i)$ -action on $\{y_j\}$.

Remark 4.10. When $f, g \in \mathbb{F}_q[T]$, let G_t be the subgroup of $\widehat{G}_{f,g}$ generated by elements of $\widehat{G}_{f,g,t} \cup G_{f,g}$. In other words, G_t is the subgroup generated by $G_{f,g}$ and an element lifting the q^t -power Frobenius automorphism. Since G_t is canonically isomorphic to the Galois group of $\Omega_{f,g}\mathbb{F}_{q^t}$ over $\mathbb{F}_{q^t}(z)$, Remark 4.9 gives a natural correspondence between divisors $\Phi \in \mathbb{F}_{q^t}[S, T]$ of $f(T) - g(S)$ (up to multiplication by constants in $\mathbb{F}_{q^t}^\times$) and subsets $B \subseteq \{y_j\}$ on which $G_t(x_i)$ acts. Also, the divisor Φ is absolutely irreducible if and only if the corresponding subset B is an orbit under the action of $G_{f,g}(x_i)$. A similar statement applies, reversing the roles of $\{y_j\}$ vs. $\{x_j\}$ and S vs. T .

Remark 4.11. Suppose $\Phi \in \mathbb{F}_{q^t}[S, T]$ is a divisor of $f(T) - g(S)$. Since $G_t = G_{d'}$ with $d' = \gcd(d, t)$, the above shows that, up to multiplication by a nonzero constant, $\Phi \in \mathbb{F}_{q^{d'}}[S, T]$.

The above theorem and remarks give the following:

Corollary 4.12. For (f, g) a DP and f not exceptional, $f(T) - g(S)$ is reducible over $\overline{\mathbb{F}}_q$. In fact, if $\bar{t} \in \mathcal{D}_{f,g}$, then $f(T) - g(S)$ is reducible over $\mathbb{F}_{q^{\bar{t}}}$.

Proof. The first statement is clear. The second statement is clear for t sufficiently large, though the above remarks show that reducibility is not actually a property of t , large or small, but a property of $t \bmod d$. \square

Remark 4.13. The t such that $f(T) - g(S)$ is reducible over \mathbb{F}_{q^t} form a pure Frobenius progression, with associated Frobenius set a *subgroup* of \mathbb{Z}/d . Let (d, D) be the data defining this Frobenius set, where D is a set of divisors of d . Then, in contrast with the Frobenius set of an exceptional polynomial, if $d_1|d_2$ are divisors of d with $d_2 \in D$, then $d_1 \in D$.

Now we consider the analogous situation for inclusions $\mathcal{V}_f(\mathbb{F}_{q^t}) \subseteq \mathcal{V}_g(\mathbb{F}_{q^t})$.

Proposition 4.14. *Let $\mathcal{V}_f(\mathbb{F}_{q^t}) \subseteq \mathcal{V}_g(\mathbb{F}_{q^t})$ for t sufficiently large, and let N_t be the number of absolutely irreducible factors of $f(T) - g(S)$ defined over \mathbb{F}_{q^t} . Then $N_t \geq 1$. Furthermore, $N_t = 1$ if and only if g is bijective over $\mathcal{V}_f(\mathbb{F}_{q^t})$ in the sense that every nonbranch point $b \in \mathcal{V}_f(q^t)$ has exactly one $a \in \mathbb{F}_{q^t}$ mapping to it under g .*

Proof. Let G_t be as in Remark 4.10. Also from this remark, the number N_t of absolutely irreducible factors of $f(T) - G(S)$ defined over \mathbb{F}_{q^t} equals the number of $G_t(x_1)$ -orbits which are also $G_{f,g}(x_1)$ -orbits.

Use Lemma 3.1 to count such orbits. Conclude that $N_t = r$, where r is the average number of elements of $\{y_j\}$ fixed by σ , as σ varies in $\widehat{G}_{f,g,t}(x_1)$. By Theorem 3.10, $r \geq 1$, and $r = 1$ if and only if every $\sigma \in \widehat{G}_{f,g,t}$ fixing x_1 fixes exactly one element of $\{y_j\}$. So, by the Frobenius Principle and the Chebotarev Density Theorem, $r = 1$ is equivalent to every nonbranch point $b \in \mathcal{V}_f(\mathbb{F}_{q^t})$ being the image of exactly one $a \in \mathbb{F}_{q^t}$ under the map induced by g . \square

Remark 4.15. This generalizes Theorem 4.8 since, if $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_g(\mathbb{F}_{q^t})$, bijectivity of f over $\mathcal{V}_f(\mathbb{F}_{q^t})$ is equivalent to $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathbb{F}_{q^t}$ (use Theorem 3.4). In fact, we may view the above proof as an alternate proof of Theorem 4.8.

We end with a generalization of Theorem 3.13.

Proposition 4.16. *If $\mathcal{V}_f(\mathbb{F}_{q^t}) \subseteq \mathcal{V}_g(\mathbb{F}_{q^t})$ for all t , and $\deg g > 1$, then $f(T) - g(S)$ is reducible over \mathbb{F}_q .*

Proof. By Remark 4.9, the number of factors of $f(T) - g(S)$ is the number of $\widehat{G}_{f,g}(x_1)$ -orbits of $\{y_j\}$. By (3.10), each element of $\widehat{G}_{f,g}(x_1)$ fixes at least one element of $\{y_j\}$. If $\{y_j\}$ has only one $\widehat{G}_{f,g}(x_1)$ -orbit, then $\widehat{G}_{f,g}(x_1, y_j)$, as y_j varies, are conjugate subgroups of $\widehat{G}_{f,g}(x_1)$. The conjugates, however, of a proper subgroup of a finite group cannot cover the group. \square

Remark 4.17. Section 7 continues the topic of reducibility.

5. Behavior at infinity

Many results above generalize to nonpolynomial maps. The main distinction is that polynomial maps $f : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ totally ramify above the place at infinity. This section considers the consequences of total ramification.

We begin with a lemma concerning the special case of tame ramification. It is similar to results in the literature (for example [Mül98, Section 2.2]). However, for generality and the convenience of the reader, we give a proof. The setup is as follows. Let K be a field with discrete valuation v and associated residue field k , and let L be a degree n separable extension of K with valuation w extending v to L . Let M be the normal closure of L over K , and let ω be a valuation of M extending w with residue field $k(\omega)$. For a subgroup H of a group G , we denote the group of permutations of the n cosets G/H by $\text{Perm}(G/H)$.

Lemma 5.1. *Let $G = \text{Gal}(M/K)$ and $H = \text{Gal}(M/L)$. Suppose (L, w) is tamely and totally ramified over (K, v) . Then:*

- (5.1) (M, ω) is tamely ramified over (K, v) and unramified over (L, w) .
- (5.2) The inertia group $I_\omega \subseteq G$ is cyclic and acts transitively and effectively on G/H ; any generator of I_ω corresponds to an n -cycle in $\text{Perm}(G/H)$.
- (5.3) $k(\omega) = k(\zeta_n)$, where ζ_n is a primitive n -th root of 1.
- (5.4) The decomposition group $G_\omega \subseteq G$ is isomorphic to the semidirect product $\mu_n \rtimes_\varphi \tilde{G}$ where $\mu_n \subseteq k(\omega)^\times$ is the group of n -th roots of 1, \tilde{G} is $\text{Gal}(k(\omega)/k)$, and $\varphi : \tilde{G} \rightarrow \text{Aut}(\mu_n)$ is the natural Galois action on the n -th roots of unity.
- (5.5) The isomorphism $G_\omega \rightarrow \mu_n \rtimes_\varphi \tilde{G}$ can be chosen so that the inertia group I_ω corresponds to μ_n , and $H \cap G_\omega$ corresponds to \tilde{G} .

Proof. Let $\pi = \pi_L$ be a uniformizer for (L, w) and let $h_1 \in K[T]$ be its minimal, monic polynomial. This polynomial is Eisenstein of degree n (its nonleading coefficients have positive valuation, and its constant term is a uniformizer for (K, v)).

Since (L, w) is totally ramified over (K, v) , I_ω acts transitively on G/H . The action is effective (G acts effectively on G/H). The property of tame ramification behaves well under composita, and (L, w) is tamely ramified over (K, v) . Thus (M, ω) is also tamely ramified over (K, v) . So I_ω is cyclic. It acts transitively and effectively on G/H , so its generator acts as an n -cycle. In particular $|I_\omega| = |G/H| = n$, forcing (M, ω) to be unramified over (L, w) .

Let K_v , L_w , and M_ω be the completions associated with (K, v) , (L, w) , and (M, ω) . So G_ω is canonically isomorphic to $\text{Gal}(M_\omega/K_v)$. Since h_1 remains irreducible over K_v , $L_w = K_v(\pi)$ and M_ω is the splitting field of h_1 over K_v . Let $h_2(T) = T^n - \pi_K$, where $\pi_K = -h_1(0)$. Note that π_K is a uniformizer for K_v . Let M' be the splitting field of h_2 over K_v . We show that $M_\omega = M'$.

Let $\beta \in M'$ be a zero of h_2 , and $\zeta \in M'$ a primitive n -th root of unity. Note that $h_3(T) \stackrel{\text{def}}{=} h_1(\beta T)/\pi_K$ is a monic polynomial in M' with coefficients

of nonnegative valuation. By Hensel's Lemma, all the zeros r_1, \dots, r_n of h_3 are in M' . Thus $\{r_i\beta\}$, the zeros of h_1 , are in M' . Conclude $M_\omega \subseteq M'$.

The zeros of h_1 correspond to the zeros of h_2 as follows. If α is a zero of h_1 , expand α in M' in terms of the uniformizer β as $\alpha = \zeta^i \beta$ plus higher-order terms. The correspondence sends α to $\zeta^i \beta$. This correspondence is compatible with the $\text{Gal}(M'/K_v)$ action. Conclude that $M_\omega = M'$.

Clearly $I_\omega = \text{Gal}(M_\omega/K_v(\zeta))$, and so $\text{Gal}(K_v(\zeta)/K_v)$ is canonically isomorphic to $\tilde{G} = \text{Gal}(k(\omega)/k)$. Conclude that $k(\omega) = k(\zeta_n)$.

Replace β by $\beta\zeta^i$, if necessary, so that π corresponds to β . So $H_\omega = H \cap G_\omega$ is the subgroup of G_ω fixing β , and $L_\omega = K_v(\beta)$. Clearly $H_\omega \cap I_\omega = 1$ and $|H_\omega| = |\tilde{G}|$. So, restricting the natural homomorphism $G_\omega \rightarrow \tilde{G}$ gives an isomorphism $H_\omega \rightarrow \tilde{G}$. The inverse isomorphism splits the exact sequence

$$1 \rightarrow I_\omega \rightarrow G_\omega \rightarrow \tilde{G} \rightarrow 1.$$

Thus G_ω is isomorphic to a semi-direct product $I_\omega \rtimes \tilde{G}$ with an isomorphism which sends H_ω to \tilde{G} .

The rule $\gamma \mapsto \gamma(\beta)/\beta$ defines a natural isomorphism $I_\omega \rightarrow \mu_n$ [Frö67, Section 8], where $a \mapsto \bar{a}$ is the residue map. If $\gamma \mapsto \zeta_n^i$, then clearly $\sigma\gamma\sigma^{-1} \mapsto \tilde{\sigma}(\zeta_n^i)$, where $\tilde{\sigma}$ is the image of σ in \tilde{G} . The result follows. \square

Example 5.2. Let $f \in F[T]$ be a polynomial of degree prime to the characteristic of F . The following imply the hypotheses of Lemma 5.1:

$K = F(z)$ with $v = \infty_z$, the place at infinity. (So $k = F$).

$L = F(x_1)$ with $w = \infty_{x_1}$. (Here, x_1 is a fixed zero of $f(T) - z$).

$M = \Omega_f$ with ω any place above ∞_{x_1} .

$G = \hat{G}_f$ and H is the subgroup fixing x_1 .

Note: We can identify the zeros $\{x_1, \dots, x_n\}$ with G/H , where a given zero x_j corresponds to the coset of elements sending x_1 to x_j .

Let $\zeta_n \in F$ be a primitive n -th root of 1, and $\mu_n \in F^\times$ the group of n -th roots of 1. Applying Lemma 5.1 to the above example yields:

Corollary 5.3. *Suppose $n = \deg f$ is prime to the characteristic of F .*

- *The geometric monodromy group G_f contains an element which acts on the set $\{x_i\}$ as an n -cycle.*
- *The field \hat{F}_f is a subfield of $F(\zeta_n)$. In particular, if $F = \mathbb{F}_q$ and $q \equiv 1 \pmod n$, then $\hat{\mathbb{F}}_f = \mathbb{F}_q$ and $\hat{G}_f = G_f$.*
- *The arithmetic monodromy group \hat{G}_f contains a subgroup isomorphic to $\mu_n \rtimes \text{Gal}(F(\mu_n)/F)$, and the geometric monodromy group G_f contains a subgroup isomorphic to $\mu_n \rtimes \text{Gal}(F(\mu_n)/\hat{F}_f)$.*

We now give the main theorem of this section. Here $\mathcal{D}_{f,g} \subseteq \mathbb{Z}/d$ is as in Definition 4.3 and $d = [\hat{\mathbb{F}}_{f,g} : \mathbb{F}_q]$.

Theorem 5.4. *Let $f, g \in \mathbb{F}_q[T]$ with $n = \deg f$ and $m = \deg g$. If (f, g) is a DP, then $\gcd(n, q^t - 1) = \gcd(m, q^t - 1)$ for all positive t with $t \in \mathcal{D}_{f,g}$.*

Proof. Let t be a positive integer with $t \in \mathcal{D}_{f,g}$. Let $n = n_0 p^u$ and $m = m_0 p^v$ with n_0 and m_0 prime to $p = \text{char}(\mathbb{F}_q)$. We must show

$$\gcd(n_0, q^t - 1) = \gcd(m_0, q^t - 1).$$

Let ∞_z be the infinite place of $\mathbb{F}_q(z)$ and K the completion. Fix a place ω of $\Omega_{f,g}$ above ∞_z . Let $\widehat{G}_\omega \subseteq \widehat{G}_{f,g}$ be the decomposition group associated to ω , and $I \subseteq \widehat{G}_\omega$ the inertia group. Thus \widehat{G}_ω is canonically isomorphic to $\text{Gal}(\Omega_\omega/K)$, where Ω_ω is the completion of $\Omega_{f,g}$ at ω . Choose $\phi_t \in \widehat{G}_\omega$ that induces the automorphism $x \mapsto x^{q^t}$ of the residue field. Since $\mathbb{F}_q(x_1)$ is totally ramified over $\mathbb{F}_q(z)$ at ∞_z , the group I acts transitively on $\{x_i\}$. So, after replacing ϕ_t by $\sigma\phi_t$ for a suitable $\sigma \in I$, we can assume ϕ_t fixes x_1 . Note: $\phi_t \in \widehat{G}_{f,g,t}(x_1)$, so ϕ_t must also fix an element of $\{y_j\}$.

Let $I_1 \subseteq I$ be the first higher ramification group. Thus I_1 is a normal p -Sylow subgroup of I with cyclic quotient. Let $\gamma \in I$ be an element whose image in I/I_1 is a generator.

Let R_x be $\widehat{G}_\omega/I_1\widehat{G}_\omega(x_1)$ and consider the map $\{x_i\} \rightarrow R_x$ sending x_i to the coset $\sigma I_1\widehat{G}_\omega(x_1)$, where $\sigma \in \widehat{G}_\omega$ is chosen so that $\sigma(x_1) = x_i$. The fibers of this map are exactly the I_1 -orbits of $\{x_i\}$. Since I_1 is normal in I and I acts transitively on $\{x_i\}$, the I_1 -orbits all have the same size; that size is a power of p , and the number of I_1 -orbits is prime to p . Since $n = |\{x_i\}|$ is the product of $|R_x|$ and the fiber size, it follows that R_x has n_0 elements, and the fibers have size p^u . Likewise, let R_y be $\widehat{G}_\omega/I_1\widehat{G}_\omega(y_1)$ and consider the corresponding map $\{y_j\} \rightarrow R_y$. Conclude that $|R_y| = m_0$ and the fibers have size p^v .

Let $L_x \subseteq \Omega_\omega$ be the fixed field of $I_1\widehat{G}_\omega(x_1)$ and L_y that of $I_1\widehat{G}_\omega(y_1)$. Let $M_x \subseteq \Omega_\omega$ be the normal closure of L_x over K and M_y that of L_y over K . We can identify R_x with

$$\text{Gal}(M_x/K)/\text{Gal}(M_x/L_x).$$

So $[L_x : K] = n_0$. Since I acts transitively on R_x , the extension L_x/K is totally and tamely ramified. A similar conclusion holds for L_y/K .

Apply Lemma 5.1 to L_x/K and L_y/K . For example, identify R_x with \mathbb{Z}/n_0 so ϕ_t fixes $0 \in \mathbb{Z}/n_0$ and γ acts as the map $c \mapsto c + 1$. Consequently, $\gamma^b\phi_t$ acts on \mathbb{Z}/n_0 as the map $c \mapsto q^t c + b$. Identify R_y with \mathbb{Z}/m_0 in a similar manner.

Now suppose $a = \gcd(q^t - 1, n_0)$ is not a multiple of $\gcd(q^t - 1, m_0)$. Then $\gamma^a\phi_t$, viewed as $c \mapsto q^t c + a$ modulo n_0 , clearly fixes an element of R_x . Yet $\gamma^a\phi_t$, viewed as $c \mapsto q^t c + a$ modulo m_0 , fixes no element of R_y . Suppose $\gamma^a\phi_t$ fixes $\rho \in R_x$. Let x_{i_0} be an element of the fiber of $\{x_i\} \rightarrow R_x$. Since fibers of this map are I_1 -orbits, there is a $\tau \in I_1$ such that $\tau\gamma^a\phi_t$ fixes x_{i_0} . As

$\tau\gamma^a\phi_t$ and $\gamma^a\phi_t$ act on R_y in the same way, neither has a fixed point in R_y . Thus, $\tau\gamma^a\phi_t$ fixes no element of $\{y_j\}$, contradicting $\bar{t} \in \mathcal{D}_{f,g}$. Conclude that a is a multiple of $\gcd(q^t - 1, m)$.

Similarly, conclude $\gcd(q^t - 1, m_0)$ is a multiple of $\gcd(q^t - 1, n_0)$. Therefore, $\gcd(q^t - 1, m_0) = \gcd(q^t - 1, n_0)$. \square

Remark 5.5. Although we have adopted the convention that polynomials in this paper have nonzero derivatives, the above theorem (and its corollaries) remain valid for polynomials with zero derivatives.

A corollary is Lenstra's theorem [CF95]:

Corollary 5.6. *Let $f \in \mathbb{F}_q[T]$ with $n = \deg f$. If f is an exceptional polynomial, then $\gcd(n, q - 1) = 1$.*

Proof. Apply the theorem to (f, g) , where $g(T) = T$. Take $t = 1$ and recall that $\bar{1} \in \mathcal{D}_{f,g}$ since f is exceptional. \square

Corollary 5.7. *Let $f, g \in \mathbb{F}_q[T]$, where $\deg f = n_0 p^u$ and $\deg g = m_0 p^v$ with n_0 and m_0 prime to the characteristic p . If (f, g) is an SDP, then $n_0 = m_0$.*

Proof. Let t be the order of q modulo $n_0 m_0$. Thus $n_0 m_0 \mid (q^t - 1)$. By Theorem 5.4,

$$n_0 = \gcd(q^t - 1, \deg f) = \gcd(q^t - 1, \deg g) = m_0. \quad \square$$

The above theorem and corollary easily generalize to value set inclusions.

Proposition 5.8. *Let $f, g \in \mathbb{F}_q[T]$, where $\deg f = n$ and $\deg g = m$. For all t such that (3.10) holds, $\gcd(q^t - 1, m)$ divides $\gcd(q^t - 1, n)$.*

Proposition 5.9. *Let $f, g \in \mathbb{F}_q[T]$, where $\deg f = n_0 p^u$ and $\deg g = m_0 p^v$ with n_0 and m_0 prime to the characteristic p . If $\mathcal{V}_f(\mathbb{F}_{q^t}) \subseteq \mathcal{V}_g(\mathbb{F}_{q^t})$ for all t , then m_0 divides n_0 .*

6. Factoring separated variable polynomials and rational functions

This section reviews properties of *induced decompositions* and how they affect factorizations of variables separated rational functions. For simplicity we stay with a notation where f and g are polynomials, until Remarks 6.4 and 6.9. Most results are in [Fri73] or are extensions of results there.

6.1. Statements on reducibility. This subsection concentrates on factorization, while the next concentrates on conclusions about SDPs and DPs.

Lemma 6.1. *Let $f, g \in F[T]$ be a pair of polynomials. There is a decomposition $f = f_1 \circ f_2$ with $f_1, f_2 \in F[T]$ having the following properties:*

$$(6.1) \quad F(x_i) \cap \Omega_g = F(f_2(x_i)) \text{ for all } x_i \text{ in } \{x_1, \dots, x_n\}.$$

(6.2) $\deg f_2 = 1$ if and only if $\Omega_f \subseteq \Omega_g$.

(6.3) For all x_i , $f_2(T) - f_2(x_i)$ is an irreducible polynomial over Ω_g .

These properties characterize f_1 and f_2 up to composition with linear polynomials (actually (6.1) suffices). More specifically, if $f = f_1 \circ f_2 = f'_1 \circ f'_2$ are two such decompositions, then $f'_1 = f_1 \circ l^{-1}$ and $f'_2 = l \circ f_2$, where $l \in F[T]$ is a linear polynomial.

Call this decomposition and the analogous decomposition of g the *induced decompositions* associated to the pair (f, g) .

Proof. Fix a particular zero x_i . By Lüroth's Theorem, $F(x_i) \cap \Omega_g = F(w_i)$ for some $w_i \in F(x_i)$. Adjust w_i by a suitable linear fractional transformation so that $w_i = f_2(x_i)$ and $z = f_1(w_i)$ for some $f_1, f_2 \in F[T]$. Thus $f = f_1 \circ f_2$. Any other choice w'_i has the form $aw_i + b$, where $a, b \in F$ and $a \neq 0$. So f_1 and f_2 are unique up to composition with a linear polynomial. Now let x_j be any element of $\{x_1, \dots, x_n\}$ and let $\sigma \in \widehat{G}_{f,g}$ send x_i to x_j . Then $F(x_j) \cap \Omega_g = F(\sigma(x_i)) \cap \Omega_g = F(f_2(\sigma(x_i))) = F(f_2(x_j))$. So (6.1) holds.

To see (6.2), note that $\deg f_2 = 1$ implies $F(x_i) \cap \Omega_g = F(x_i)$. Thus $F(x_i) \subseteq \Omega_g$, so $\Omega_f \subseteq \Omega_g$. The converse is clear.

To see (6.3), consider $f_2(T) - f_2(x_i)$. By (6.1), this polynomial is defined over Ω_g . We will show it is irreducible by showing $\text{Gal}(\overline{\Omega}_g/\Omega_g)$ acts transitively on its zeros. Any zero equals some x_j satisfying $f_2(x_i) = f_2(x_j)$. Let $\sigma \in \text{Gal}(\overline{F(z)}/F(z))$ satisfy $\sigma(x_i) = x_j$. Let $\tilde{\sigma}$ be the restriction of σ to Ω_g . Clearly, $\tilde{\sigma}(f_2(x_i)) = f_2(x_i)$, so $\tilde{\sigma} \in \text{Gal}(\Omega_g/\Omega_g \cap F(x_i))$. The restriction map

$$\text{Gal}(F(x_i) \cdot \Omega_g/F(x_i)) \rightarrow \text{Gal}(\Omega_g/\Omega_g \cap F(x_i))$$

is an isomorphism. Use this to lift $\tilde{\sigma}$ to $F(x_i) \cdot \Omega_g$, and then to $\overline{\Omega}_g$ so the lifting τ fixes x_i . Then $\sigma \circ \tau^{-1} \in \text{Gal}(\overline{\Omega}_g/\Omega_g)$ and $\sigma \circ \tau^{-1}(x_i) = \sigma(x_i) = x_j$. \square

An important feature of these induced decompositions is that they respect the factorization of $f(T) - g(S)$.

Lemma 6.2. *Suppose $f(T) - g(S)$ is reducible over F , and $f = f_1 \circ f_2$ is the induced decomposition. Then $f_1(T) - g(S)$ is reducible over F . Moreover, substituting $f_2(T)$ for T into the factorization of $f_1(T) - g(S)$ gives the factorization of $f(T) - g(S)$. In particular, $\deg f_1 > 1$.*

Proof. Fix x_i . As in Remark 4.9, factoring $g(S) - f(T)$ over $F[S, T]$ corresponds to finding the orbits of $\{y_j\}$ under the action of

$$G_{x_i} \stackrel{\text{def}}{=} \text{Gal}(\overline{F(z)}/F(x_i)).$$

Similarly, factoring $g(S) - f_1(T)$ over $F[S, T]$ corresponds to finding the orbits of $\{y_j\}$ under the action of

$$G_{f_2(x_i)} \stackrel{\text{def}}{=} \text{Gal}(\overline{F(z)}/F(f_2(x_i))).$$

Decompose $\{y_j\}$ into orbits with both groups. Clearly the $G_{f_2(x_i)}$ -orbits contain the G_{x_i} -orbits. We show, in fact, they are equal. Let $\sigma \in G_{f_2(x_i)}$ send y_j to y_k . If σ sends x_i to x_l , then x_i and x_l are both zeros of the polynomial $f_2(T) - f_2(x_i)$. By (6.3), there is a $\tau \in \text{Gal}(\overline{F(z)}/\Omega_g)$ sending x_i to x_l . Thus $\tau^{-1} \circ \sigma \in G_{x_i}$ sends y_j to y_k .

Let $O \subseteq \{y_j\}$ be such an orbit, $\Phi(S, T)$ the corresponding irreducible factor of $g(S) - f_1(T)$, and $\Phi'(S, T)$ the corresponding irreducible factor of $g(S) - f(T)$. The correspondence of Remark 4.9 yields the equation

$$\prod_{y_j \in O} (S - y_j) = c \Phi(S, x_i) = c' \Phi'(S, f_2(x_i))$$

for some $c, c' \in F$. Thus $c \Phi(S, T) = c' \Phi'(S, f_2(T))$. \square

Corollary 6.3 ([Fri73], Lemma 7). *Suppose $f(T) - g(S)$ is reducible over F . Then there are decompositions $f = f' \circ f''$ and $g = g' \circ g''$ with f', f'', g', g'' in $F[T]$ such that:*

- (i) $f'(T) - g'(S)$ is reducible.
- (ii) $\Omega_{f'} = \Omega_{g'}$.
- (iii) Substituting $f''(T)$ for T and $g''(S)$ for S into the factorization of $f'(T) - g'(S)$ gives the factorization of $f(T) - g(S)$.

Furthermore, if either $\deg f'$ or $\deg g'$ is prime to p , then $\deg f' = \deg g'$.

Proof. To prove this, repeatedly use the previous lemma applied to induced decompositions of f and g . (Replace f and g with the outer composites as you go along). Eventually you will obtain f_2 and g_2 of degree 1, which implies that $\Omega_f = \Omega_g$.

Now if $\deg f'$ or $\deg g'$ is prime to p , then the place at infinity is tamely ramified in $\Omega_{f'} = \Omega_{g'}$. Conclude that both $\deg f'$ and $\deg g'$ give the order of the inertia group at infinity, so they are equal. (See Lemma 5.1 above.) \square

Remark 6.4. Suppose $f = u_1/u_2$ and $g = v_1/v_2$, with $u_1, u_2, v_1, v_2 \in F[T]$ and $(u_1, u_2) = 1 = (v_1, v_2)$. We think of the factors of $f(T) - g(S)$ as being the factors of the polynomial $u_2 v_2 (f(T) - g(S))$. Geometrically, these are the components of the fiber product of the two maps $f : \mathbb{P}_t^1 \rightarrow \mathbb{P}_z^1$ and $g : \mathbb{P}_s^1 \rightarrow \mathbb{P}_z^1$ over the sphere \mathbb{P}_z^1 uniformized by z . Recall that the degree of f is the maximum of the degrees of u_1 and u_2 .

Lemma 6.1 and Lemma 6.2 hold exactly as stated for rational functions f and g (though in the proof one uses linear fractional changes of variables instead of just affine changes). In Corollary 6.3, the only result that doesn't hold for rational functions is the conclusion about $\deg f = \deg g$ when one of the degrees are prime to p . That requires using total tame ramification over ∞ .

6.2. Statements on value sets. Now we show that induced decompositions behave well in certain types of value set situations. Since we are dealing with value sets, we restrict to $F = \mathbb{F}_q$ for the remainder of this section.

Proposition 6.5. *Suppose $\mathcal{V}_f(\mathbb{F}_{q^t}) \subseteq \mathcal{V}_g(\mathbb{F}_{q^t})$ for all t . Let $f = f_1 \circ f_2$ be the induced decomposition associated to the pair (f, g) and let $g = g_1 \circ g_2$ be any decomposition (for example, the induced decomposition). Then*

$$\mathcal{V}_{f_1}(\mathbb{F}_{q^t}) \subseteq \mathcal{V}_{g_1}(\mathbb{F}_{q^t})$$

for all t .

Proof. All zeros of $f_1(T) - z$ have the form $f_2(x_i)$. By Theorem 3.10, we can show $\mathcal{V}_{f_1}(\mathbb{F}_{q^t}) \subseteq \mathcal{V}_g(\mathbb{F}_{q^t})$ for all t by showing that any $\sigma \in \text{Gal}(\overline{\mathbb{F}_q(z)}/\mathbb{F}_q(z))$ fixing $f_2(x_i)$ must also fix some y_j . If $\sigma \in \text{Gal}(\overline{\mathbb{F}_q(z)}/\mathbb{F}_q(z))$ fixes $f_2(x_i)$, then $x_l = \sigma(x_i)$ is a zero of $f_2(T) - f_2(x_i)$. By (6.3), there is a $\tau \in \text{Gal}(\overline{\mathbb{F}_q(z)}/\Omega_g)$ sending x_l to x_i . So $\tau \circ \sigma$ fixes x_i , and by hypothesis and Theorem 3.10, it must fix some y_j . Since τ fixes y_j , conclude that σ also fixes y_j .

Clearly, $\mathcal{V}_g(\mathbb{F}_{q^t}) \subseteq \mathcal{V}_{g_1}(\mathbb{F}_{q^t})$. \square

Corollary 6.6. *Suppose (f, g) is an SDP with $\deg g > 1$, so (as in Proposition 4.16) $f(T) - g(S)$ is reducible. Then the decompositions of Corollary 6.3 can be chosen so that (f', g') is an SDP.*

Suppose, instead, $\mathcal{V}_f(\mathbb{F}_{q^t}) \subseteq \mathcal{V}_g(\mathbb{F}_{q^t})$ for all t . Then the decompositions of Corollary 6.3 can be chosen so that $\mathcal{V}_{f'}(\mathbb{F}_{q^t}) \subseteq \mathcal{V}_{g'}(\mathbb{F}_{q^t})$ for all t .

Proposition 6.7. *Suppose (f, g) is an SDP with $n = \deg f$ and $m = \deg g$ prime to p . Then $\Omega_f = \Omega_g$ and $\deg f = \deg g$.*

Proof. By Corollary 5.7, $n = m$. Let $f = f_1 \circ f_2$ be the induced decomposition associated to the pair (f, g) . By Proposition 6.5, (f_1, g) is also an SDP. By Proposition 5.9 again, $\deg f_1 = m$. Hence, $\deg f_2 = 1$. Thus, by (6.2), $\Omega_f \subseteq \Omega_g$. A similar argument gives the other inclusion. \square

Finally, we show that in some circumstances the induced decompositions behave well for DP's.

Proposition 6.8. *Suppose (f, g) is a DP with $\widehat{\mathbb{F}}_{f,g} = \widehat{\mathbb{F}}_g$. Let $f = f_1 \circ f_2$ be the induced decomposition associated to the pair (f, g) . Then (f_1, g) is a DP. Furthermore, we have $\mathcal{D}_{f,g} \subseteq \mathcal{D}_{f_1,g}$, both being subsets of \mathbb{Z}/d where $d = [\widehat{\mathbb{F}}_g : \mathbb{F}_q]$. An analogous result holds for inclusions of value sets replacing the DP hypothesis.*

Proof. We need to verify (3.9) with (f_1, g) for all t such that $\bar{t} \in \mathcal{D}_{f,g}$ (Definition 4.3). So, let $\sigma \in \widehat{G}_{f_1,g,t}$ with $\bar{t} \in \mathcal{D}_{f,g}$, and let $\tilde{\sigma} \in \widehat{G}_{f,g,t}$ be an element restricting to σ . Note that the zeros of $f_1(T) - z$ have the form $f_2(x_i)$.

First, suppose σ fixes y_j . So $\tilde{\sigma}$ fixes y_j , and, by property (3.9), $\tilde{\sigma}$ fixes some x_i . Thus $\tilde{\sigma}$, and hence σ , fix $f_2(x_i)$.

Now suppose that σ fixes $f_2(x_i)$. Let $x_l = \tilde{\sigma}(x_i)$ (so that x_l is a zero of $f_2(T) - f_2(x_i)$). By (6.3) there is a $\tau \in \text{Gal}(\Omega_{f,g}/\Omega_g)$ sending x_i to x_l . Since τ fixes Ω_g , it also fixes $\widehat{\mathbb{F}}_g = \widehat{\mathbb{F}}_{f,g}$. Hence $\tau^{-1} \circ \tilde{\sigma} \in \widehat{G}_{f,g,t}(x_i)$. Since $\tilde{t} \in \mathcal{D}_{f,g}$, property (3.9) applies, and $\tau^{-1} \circ \tilde{\sigma}$ must fix some y_j . Since τ fixes $y_j \in \Omega_g$, conclude that σ also fixes y_j . \square

Remark 6.9. As with Remark 6.4, we may allow f and g to be rational functions, rather than polynomials. For the discussion of value sets this means we formally add ∞ to the domain and range. The only exception is in Proposition 6.7, where even the conclusion $\Omega_f = \Omega_g$ uses the total tame ramification over ∞ (as in the direct argument of [Fri73, Prop. 3]).

7. Reducibility and representations

This section links the reducibility of $f(T) - g(S)$ to the behavior of the associated Galois representations. It builds on the characteristic zero results of [Fri73] and the positive characteristic results of [Fri99].

7.1. Representation lemmas. Let G , a finite group, act on a set $\mathcal{S} = \{s_i\}$ with N elements. This permutation action of G has an associated linear action of G on a complex vector space $V_{\mathcal{S}}$ as follows. Let $V_{\mathcal{S}}$ be an N -dimensional complex vector space with a chosen basis (\mathbf{s}_i) . Have $\sigma \in G$ act on $V_{\mathcal{S}}$ by the unique linear transformation that sends \mathbf{s}_{i_1} to \mathbf{s}_{i_2} if and only if σ (acting on \mathcal{S}) sends s_{i_1} to s_{i_2} .

Let $\chi_{\mathcal{S}}$ be the character of the action of G on $V_{\mathcal{S}}$. The following lemma, a special case of Lemma 3.1, is easy and well-known.

Lemma 7.1. *For all $\sigma \in G$, the value of the character $\chi_{\mathcal{S}}(\sigma)$ is the number of elements of \mathcal{S} fixed by σ . Furthermore,*

$$\langle \chi_{\mathcal{S}}, 1 \rangle = \frac{1}{|G|} \sum_{\sigma \in G} \chi_{\mathcal{S}}(\sigma) = \text{number of orbits in } \mathcal{S}.$$

Here we use the standard Hermitian inner product on the vector space $\mathbb{C}^{|G|}$ of functions from G to \mathbb{C} :

$$\langle f_1, f_2 \rangle \stackrel{\text{def}}{=} \frac{1}{|G|} \sum_{\sigma \in G} f_1(\sigma) \overline{f_2(\sigma)}.$$

The irreducible characters form an orthogonal basis.

The $\mathbb{C}[G]$ -module $V_{\mathcal{S}}$ decomposes as $\mathbf{1}_{\mathcal{S}} \oplus V'_{\mathcal{S}}$, where $\mathbf{1}_{\mathcal{S}}$ is the submodule generated by $\sum_i \mathbf{s}_i$ and where $V'_{\mathcal{S}}$ is the kernel of the augmentation map $\eta : V_{\mathcal{S}} \rightarrow \mathbb{C}$ defined by $\sum_i \lambda_i \mathbf{s}_i \mapsto \sum \lambda_i$. Let $\chi'_{\mathcal{S}}$ be the character associated to $V'_{\mathcal{S}}$. In particular, $\chi_{\mathcal{S}} = 1 + \chi'_{\mathcal{S}}$.

Lemma 7.2. *If G acts transitively on \mathcal{S} , then $\mathbf{1}_{\mathcal{S}}$ consists of all elements of $V_{\mathcal{S}}$ fixed by G . Furthermore $\langle 1, \chi'_{\mathcal{S}} \rangle = 0$, and so $\langle \chi'_{\mathcal{S}}, \chi'_{\mathcal{S}} \rangle = \langle \chi_{\mathcal{S}}, \chi_{\mathcal{S}} \rangle - 1$.*

Proof. The identity character appears exactly once in the permutation representation of each orbit of G acting on S . So, transitivity means that $\mathbf{1}$ doesn't appear in χ'_S . Apply the inner product of $\mathbf{1} + \chi'_S$ to itself to get the given relation. \square

Remark 7.3. In general, $\langle \chi'_S, \chi'_S \rangle = \langle \chi_S, \chi_S \rangle - (2r - 1)$, where r is the number of orbits in S .

Now let the finite group G act transitively on two finite sets A and B . Consider also the associated G -action on $A \times B$. The following easy lemma is the starting point for our analysis of reducibility.

Lemma 7.4. *There are $\langle \chi_A, \chi_B \rangle$ orbits for G acting on the product $A \times B$.*

Proof. The character $\chi_{A \times B}$ associated to the action of G on $A \times B$ is $\chi_A \cdot \chi_B$. By Lemma 7.1, the number of orbits in $A \times B$ is

$$\frac{1}{|G|} \sum_{\sigma \in G} \chi_{A \times B}(\sigma) = \frac{1}{|G|} \sum_{\sigma \in G} \chi_A(\sigma) \chi_B(\sigma) = \langle \chi_A, \chi_B \rangle.$$

(Note: this proof does not require the transitivity assumption.) \square

The following well-known characterization of double transitivity is an immediate consequence of the above results.

Corollary 7.5. *Suppose the action of G on S is transitive where $|S| \geq 2$. Then the following are equivalent:*

- (7.1) *The action of G on S is doubly transitive.*
- (7.2) *There are exactly two orbits in $S \times S$ under the action of G .*
- (7.3) $\langle \chi_S, \chi_S \rangle = 2$.
- (7.4) $\langle \chi'_S, \chi'_S \rangle = 1$.
- (7.5) V'_S is an irreducible $\mathbb{C}[G]$ -module.

Remark 7.6. In Corollary 7.5, we can replace the hypothesis that G acts transitively on S with the alternate hypothesis $|S| > 2$.

The following is also an easy consequence of Lemma 7.4.

Lemma 7.7. *If G acts doubly transitively on A and $|A| \geq 2$, then the multiplicity of V'_A in the decomposition of V'_B is one less than the number of G -orbits of $A \times B$.*

Corollary 7.8. *Suppose $|A| \geq 2$ and G acts doubly transitively on A . Suppose also that $|A| = |B|$. Then the following are equivalent:*

- (7.6) $\chi_A = \chi_B$.
- (7.7) $A \times B$ has more than one orbit.
- (7.8) $A \times B$ has exactly two orbits.
- (7.9) V_A and V_B are isomorphic as $\mathbb{C}[G]$ -modules.

Remark 7.9. If (7.6) (or its equivalents) hold, then G must act doubly transitively on B as well (by Corollary 7.5).

We refine (7.9) above by explicitly constructing a natural isomorphism from V_A to V_B when the following hold:

- (i) G acts doubly transitively on A .
- (ii) $|A| = |B|$.
- (iii) $A \times B$ has more than one orbit.

We define some maps $V_A \rightarrow V_B$ without using hypotheses (i), (ii) or (iii). Then we show one gets an isomorphism when the hypotheses hold.

First choose a G -invariant subset Γ of $A \times B$, for example a G -orbit. For convenience, label elements: $A = \{a_i\}$, $B = \{b_j\}$. Consider the matrix $E = [\epsilon_{i,j}]$, where $\epsilon_{i,j}$ is 1 if $(a_i, b_j) \in \Gamma$, and 0 otherwise. Consider the linear map $\psi : V_A \rightarrow V_B$ defined by the matrix E :

$$\psi(\mathbf{a}_i) \stackrel{\text{def}}{=} \sum_j \epsilon_{i,j} \mathbf{b}_j, \quad \text{so} \quad \psi\left(\sum_i \lambda_i \mathbf{a}_i\right) = \sum_j \left(\sum_i \lambda_i \epsilon_{i,j}\right) \mathbf{b}_j.$$

Here and below, (\mathbf{a}_i) is the basis of V_A associated to $A = \{a_i\}$ and (\mathbf{b}_j) is the basis of V_B associated to $B = \{b_j\}$.

The following lemma follows directly from the definition (and does not depend on transitivity).

Lemma 7.10. *The map $\psi : V_A \rightarrow V_B$ is a $\mathbb{C}[G]$ -module morphism.*

Now we investigate some of the consequences of transitivity.

Lemma 7.11. *If Γ is nonempty, restricting ψ to $\mathbf{1}_A$ gives an isomorphism $\mathbf{1}_A \rightarrow \mathbf{1}_B$ of $\mathbb{C}[G]$ -modules.*

Proof. Check that ψ sends $\sum_i \mathbf{a}_i$ to $C \sum_j \mathbf{b}_j$, where, for each b_j , $C = C_j$ is the number of $a_i \in A$ with the property that $(a_i, b_j) \in \Gamma$. (C_j is independent of j by transitivity). \square

Lemma 7.12. *Restricting ψ to V'_A gives a $\mathbb{C}[G]$ -module morphism*

$$\psi' : V'_A \rightarrow V'_B.$$

Proof. Check that $\eta_B \circ \psi = D \cdot \eta_A$, where η_A and η_B are the augmentation maps and, for each a_i , $D = D_i$ is the number of $b_j \in B$ with the property that $(a_i, b_j) \in \Gamma$. (D_i is independent of i by transitivity). \square

Lemma 7.13. *If $\Gamma \subseteq A \times B$ is neither empty nor all of $A \times B$, then $\psi' : V'_A \rightarrow V'_B$ (defined above) has nontrivial image.*

Proof. Fix a basis vector \mathbf{a}_i of V_A . Since Γ is nonempty, $\epsilon_{i,j_1} = 1$ for some j_1 . Since Γ is a proper subset of $A \times B$, $\epsilon_{i,j_2} = 0$ for some j_2 . Let $\sigma \in G$ be an element such that $\sigma(b_{j_1}) = b_{j_2}$. Then $\psi'(\sigma(\mathbf{a}_i) - \mathbf{a}_i) \neq 0$. \square

Lemma 7.14. *Suppose that G acts doubly transitively on A and that Γ is neither empty nor all of $A \times B$. Then $\psi : V_A \rightarrow V_B$ is injective.*

Proof. By Corollary 7.5, V'_A is irreducible, and by the previous lemma, the map $\psi' : V'_A \rightarrow V'_B$ is not trivial. Thus ψ' is injective. By Lemma 7.11, the map $\mathbf{1}_A \rightarrow \mathbf{1}_B$ induced by ψ is an isomorphism. Thus $\psi : \mathbf{1}_A \oplus V'_A \rightarrow \mathbf{1}_B \oplus V'_B$ is injective. \square

Proposition 7.15. *Suppose that:*

- (i) G acts doubly transitively on A .
- (ii) $|A| = |B|$.
- (iii) Γ is a nonempty proper subset of $A \times B$ invariant under G .

Then $\psi : V_A \rightarrow V_B$ is an isomorphism.

Proof. By the previous lemma, ψ is injective. Since V_A and V_B have the same dimension, ψ is an isomorphism. \square

Also of interest is the following [Fri73, Lemma 2]:

Lemma 7.16. *Suppose G acts doubly transitively on A , and $|A| = |B| \geq 2$. Suppose also that, for all $\sigma \in G$, $\chi_A(\sigma) > 0$ if and only if $\chi_B(\sigma) > 0$. Then $\chi_A = \chi_B$.*

Proof. Recall $\chi'_A = \chi_A - 1$ and $\chi'_B = \chi_B - 1$. By hypothesis, for all $\sigma \in G$, $\chi'_A(\sigma) < 0$ if and only if $\chi'_B(\sigma) < 0$. If $\sigma = 1$ then $\chi'_A(\sigma) > 0$ and $\chi'_B(\sigma) > 0$. Thus $\langle \chi_A, \chi_B \rangle = \langle \chi'_A, \chi'_B \rangle + 1 \geq 2$. The result follows from Lemma 7.4 and Corollary 7.8. \square

Remark 7.17. This shows that if (f, g) is an SDP and if \widehat{G}_f acts doubly transitively on $\{x_i\}$, then (f, g) is actually an SDP with multiplicity. (This can also be seen as a corollary of Proposition 7.26 and Theorem 3.13.)

Remark 7.18. Lemma 7.16 uses this hypothesis: *For all $\sigma \in G$, $\chi_A(\sigma) > 0$ if and only if $\chi_B(\sigma) > 0$.* We can replace it with this hypothesis: *For all $\sigma \in G$, $\chi_A(\sigma) \leq 1$ if and only if $\chi_B(\sigma) \leq 1$.*

We end with one more consequence of double transitivity which we need later.

Lemma 7.19. *Let Γ be an orbit of $A \times B$ where G is transitive on A and B . Suppose that G acts doubly transitively on A , where $|A| \geq 2$. Then*

$$|A| |B| (|A| - 1) \mid |\Gamma| (|\Gamma| - |B|).$$

Proof. For $b \in B$, let $\Gamma_b \stackrel{\text{def}}{=} \{a \mid (a, b) \in \Gamma\}$. Note that $k \stackrel{\text{def}}{=} |\Gamma_b|$ is independent of $b \in B$ since G acts transitively on B .

Now consider the set

$$\Gamma' = \{(a, a', b) \mid (a, b), (a', b) \in \Gamma \text{ and } a \neq a'\}.$$

For distinct elements a, a' of A , let

$$\Gamma'_{a,a'} \stackrel{\text{def}}{=} \{b \mid (a, a', b) \in \Gamma'\}.$$

Note that $l \stackrel{\text{def}}{=} |\Gamma'_{a,a'}|$ is independent of a and a' since G acts doubly transitively on A .

We count the number of element of Γ' in two ways:

$$|\Gamma'| = |A|(|A| - 1)l = |B|k(k - 1).$$

Now multiply both sides by $|B|$ and use the equation $k|B| = |\Gamma|$. \square

7.2. Reducibility. In this section, unless otherwise stated, F is a general field and $f, g \in F[T]$. Remark 4.9 describes the factorization of $f(T) - g(S)$ in $F[S, T]$ in terms of $\widehat{G}_{f,g}(y_j)$ -orbits of $\{x_i\}$. There is, however, another description of the factorization of $f(T) - g(S)$ in $F[S, T]$ that follows from Remark 4.9.

Proposition 7.20. *Consider the action of $\widehat{G}_{f,g}$ on $\{x_i\} \times \{y_j\}$ induced by the natural actions of $\widehat{G}_{f,g}$ on $\{x_i\}$ and $\{y_j\}$. Irreducible factors of $f(T) - g(S)$ in $F[S, T]$ naturally correspond to the orbits of $\{x_i\} \times \{y_j\}$. This correspondence sends an irreducible factor Φ of $f(T) - g(S)$ to the orbit consisting of all pairs (x_i, y_j) satisfying $\Phi(x_i, y_j) = 0$ in $\Omega_{f,g}$. For $O \subseteq \{x_i\} \times \{y_j\}$ such an orbit, with $\Phi \in F[S, T]$ the corresponding factor of $f(T) - g(S)$:*

$$(7.10) \quad |O| = \deg f \cdot \deg_S \Phi = \deg g \cdot \deg_T \Phi.$$

Corollary 7.21. *Let $w = \gcd(\deg f, \deg g)$. The T -degree (resp. S -degree) of any irreducible factor of $f(T) - g(S)$ is a multiple of $(\deg f)/w$ (resp. of $(\deg g)/w$). So, w bounds the number of irreducible factors of $f(T) - g(S)$ in $F[S, T]$. This result holds even if f and g are rational functions (see Remark 6.4).*

Proof. By assumption, $\gcd(\deg(g)/w, \deg(f)/w) = 1$. So, (7.10) shows $\deg(f)/w$ divides the T -degree of any irreducible factor of $f(T) - g(S)$. Let r be the number of irreducible factors of $f(T) - g(S)$. Then, the sum of their respective T degrees (each a multiple of $\deg(f)/w$) adds up to $\deg f$. Therefore $r \leq w$. \square

Remark 7.22. The above corollary generalizes the well-known result of Ehrenfeucht that $\gcd(\deg f, \deg g) = 1$ implies $f(T) - g(S)$ is irreducible.

Corollary 7.23. *Let Φ be an irreducible divisor of $f(T) - g(S)$ in the ring $F[S, T]$. If $\deg f = \deg g$, then*

$$\deg \Phi = \deg_T \Phi = \deg_S \Phi,$$

where the first of these is the total degree of Φ .

Now consider the special case $F = \mathbb{F}_q$. Factoring $f(T) - g(S)$ over \mathbb{F}_q amounts to describing the orbits of $\{x_i\} \times \{y_j\}$ under the action of the arithmetic monodromy group $\widehat{G}_{f,g}$. Now use the canonical isomorphism between $\text{Gal}(\Omega_{f,g}\overline{\mathbb{F}_q}/\overline{\mathbb{F}_q}(T))$ and $G_{f,g}$, and then apply Proposition 7.20 with $F = \overline{\mathbb{F}_q}$. Conclude that factoring $f(T) - g(S)$ over $\overline{\mathbb{F}_q}$ amounts to describing the orbits of $\{x_i\} \times \{y_j\}$ under the action of the geometric monodromy group $G_{f,g}$.

In what follows, let $d = [\widehat{\mathbb{F}}_{f,g} : \mathbb{F}_q]$.

Proposition 7.24. *Let Φ be an irreducible factor of $f(T) - g(S)$ over $\overline{\mathbb{F}_q}[S, T]$, and let (x_{i_0}, y_{j_0}) be in the corresponding orbit under $G_{f,g}$. Then a nonzero constant multiple of Φ is defined over \mathbb{F}_{q^t} if and only if t is in the subgroup of \mathbb{Z}/d generated by the image of $\widehat{G}_{f,g}(x_{i_0}, y_{j_0})$ under $\widehat{G}_{f,g} \rightarrow \mathbb{Z}/d$.*

Proof. Let G_t consist of the elements in $\widehat{G}_{f,g}$ whose image in \mathbb{Z}/d is in the subgroup generated by \bar{t} . Note: G_t is isomorphic to $\text{Gal}(\mathbb{F}_{q^t}\Omega_{f,g}/\mathbb{F}_{q^t}(T))$ and the action on $\{x_i\}$ and $\{y_j\}$ are preserved by this isomorphism. Thus, by Proposition 7.20, irreducible factors of $f(T) - g(S)$ in $\mathbb{F}_{q^t}[S, T]$ correspond to G_t -orbits of $\{x_i\} \times \{y_j\}$.

Let $\Phi' \in \mathbb{F}_{q^t}[S, T]$ be the irreducible factor corresponding to the G_t -orbit containing (x_{i_0}, y_{j_0}) . The nature of the correspondence in Proposition 7.20 implies that Φ divides Φ' in $\overline{\mathbb{F}_q}[S, T]$. The degrees of Φ and Φ' are determined by the sizes of the associated orbits, so Φ' is a nonzero constant multiple of Φ if and only if these orbits are the same size. This in turn is equivalent to

$$\frac{|G_t|}{|G_t(x_{i_0}, y_{j_0})|} = \frac{|G_{f,g}|}{|G_{f,g}(x_{i_0}, y_{j_0})|},$$

or yet to

$$\frac{d}{a} = \frac{|G_t|}{|G_{f,g}|} = \frac{|G_t(x_{i_0}, y_{j_0})|}{|G_{f,g}(x_{i_0}, y_{j_0})|},$$

where $a = \gcd(d, t)$. The ratio $|G_t(x_{i_0}, y_{j_0})|/|G_{f,g}(x_{i_0}, y_{j_0})|$ determines the image of $G_t(x_{i_0}, y_{j_0})$ in \mathbb{Z}/d , and the above equation holds if and only if this image is the subgroup generated by \bar{t} . Finally, this occurs if and only if the image of $\widehat{G}_{f,g}(x_{i_0}, y_{j_0})$ in \mathbb{Z}/d contains \bar{t} . \square

We return to the case that F is a general field. Let V_f and V_g , respectively, be the $\mathbb{C}[\widehat{G}_{f,g}]$ -modules associated to the action of $\widehat{G}_{f,g}$ on $\{x_i\}$ and $\{y_j\}$. Let χ_f and χ_g be the associated characters. Lemma 7.4 and Proposition 7.20 give the following:

Proposition 7.25. *The number of irreducible factors of $f(T) - g(S)$ in $F[S, T]$ is equal to $\langle \chi_f, \chi_g \rangle$.*

Corollary 7.8 and Proposition 7.20 give the following:

Proposition 7.26. *Suppose that the degrees of f and g are equal and greater than one, and that the action of $\widehat{G}_{f,g}$ on $\{x_i\}$ is doubly transitive. Then the following are equivalent:*

- (7.11) $\chi_f = \chi_g$.
- (7.12) $f(T) - g(S)$ is reducible in $F[S, T]$.
- (7.13) $f(T) - g(S)$ factors into exactly two irreducible factors in $F[S, T]$.
- (7.14) V_f and V_g are isomorphic as $\mathbb{C}[\widehat{G}_{f,g}]$ -modules.

We note that if $F = \mathbb{F}_q$ and $\chi_f = \chi_g$, then Corollary 3.12 (together with the observation in Lemma 7.1) implies that (f, g) is an SDP. Thus we get:

Corollary 7.27. *Let $F = \mathbb{F}_q$. Suppose:*

- (i) *The degrees of f and g are equal.*
- (ii) *The action of $\widehat{G}_{f,g}$ on $\{x_i\}$ is doubly transitive.*
- (iii) *$f(T) - g(S)$ is reducible in $\mathbb{F}_q[S, T]$.*

Then (f, g) is an SDP with multiplicity.

We can also use Proposition 7.26 to prove the following:

Lemma 7.28. *Suppose $f, g \in F[T]$ are polynomials of degree at least three which are linearly related on the inside over the separable closure F^{sep} . Suppose also that the action of $\widehat{G}_{f,g}$ on $\{x_i\}$ is doubly transitive. Then f and g are linearly related on the inside over F .*

Proof. Let E be a finite Galois extension of F over which f and g are linearly related on the inside. This implies that $f(T) - g(S)$ has a linear factor defined over E . Proposition 7.26 implies $f(T) - g(S)$ has exactly two factors defined over E , one of which is linear, so the other must be of total degree greater than 1. Hence the factors are invariant under the natural $\text{Gal}(E/F)$ action. Since $f(T) - g(S)$ has a linear factor defined over F , the polynomials f and g are linearly related on the inside over F . \square

Lemma 7.19 gives the following:

Proposition 7.29. *Let Φ be a factor of $f(T) - g(S)$ of total degree $k > 1$ which is irreducible in $F[S, T]$. Suppose that the degrees of f and g are both equal to $n > 1$. Suppose also that the action of $\widehat{G}_{f,g}$ on $\{x_i\}$ is doubly transitive. Then*

$$n - 1 \mid k(k - 1).$$

Proof. Let O be the orbit corresponding to Φ via Proposition 7.20. Note that $\deg_S \Phi = \deg \Phi = k$ by Corollary 7.23. Apply Lemma 7.19 with $A = \{x_i\}$, $B = \{y_j\}$ and $\Gamma = O$. By Proposition 7.20, $|O| = nk$. \square

Corollary 7.30. *Suppose the degrees of f and g both equal $n > 2$, the action of $\widehat{G}_{f,g}$ on $\{x_i\}$ is doubly transitive, and $f(T) - g(S)$ is reducible over F . Then the two irreducible factors of $f(T) - g(S)$ have nonequal degrees.*

Proof. There are exactly two factors by Proposition 7.26. Suppose they both have degree k , i.e., $n = 2k$. Then $n - 1 = 2k - 1$ is prime to k and $k - 1$. Thus $n - 1$ cannot divide $k(k - 1)$, contradicting the previous proposition. \square

7.3. Polynomials with doubly transitive monodromy groups. Many of the above results (Proposition 7.26 to Corollary 7.30) depend on the double transitivity of monodromy groups. The classification of polynomials with doubly transitive geometric monodromy groups is well-known, at least when the degree is prime to the characteristic. We describe this classification. Throughout this section, let $f \in F[T]$ have degree n at least 2, and let V_f be the associated $\mathbb{C}[G_f]$ module with character χ_f .

Lemma 7.31. *Suppose the arithmetic monodromy group \widehat{G}_f acts doubly transitively on $\{x_i\}$. Then f is indecomposable over F .*

Proof. Assume $f = f_1 \circ f_2$ with $f_1, f_2 \in F[T]$ of degrees at least two. Then

$$f(T) - f(S) = (T - S) \Phi_1(f_2(S), f_2(T)) \Phi_2(S, T),$$

where

$$\Phi_i(S, T) \stackrel{\text{def}}{=} \frac{f_i(T) - f_i(S)}{T - S}.$$

Thus $f(T) - f(S)$ has at least three irreducible factors, contradicting Proposition 7.26. \square

The following argument of [Fri70] gives a partial converse.

Lemma 7.32. *Suppose $f \in F[T]$ is indecomposable over F with $n = \deg f$ composite and prime to the characteristic of F . Then the arithmetic and geometric monodromy groups of f act doubly transitively on $\{x_i\}$.*

Proof. A theorem of Fried and MacRae implies that, since n is prime to the characteristic of F , f is indecomposable over \bar{F} . Thus G_f acts primitively on $\{x_i\}$. By Corollary 5.3, there is an element of G_f which acts as an n -cycle on $\{x_i\}$. Schur proved that a finite group G acting on a set with N elements acts doubly transitively if:

- (i) The action is primitive.
- (ii) G contains an element acting as an N -cycle.
- (iii) N is composite. \square

The above lemmas allow us to concentrate on the case n a prime. In the case $n = 2$ the action is trivially doubly transitive, thus we can restrict $\deg f = n$ to odd primes (different from the characteristic of F). Before finishing the classification, we describe important families of polynomials whose geometric monodromy groups *do not* act doubly transitively on $\{x_i\}$.

Consider the cyclic polynomials $f(T) = T^n$. Here G_f is a cyclic group of order n with generator acting on the zeros $\{x_i\}$ as an n -cycle. Furthermore,

$\langle \chi_f, \chi_f \rangle = n$ and $f(T) - g(S)$ factors into n linear factors. So, when $n > 2$, the action of G_f on $\{x_i\}$ is not doubly transitive.

The other main family of examples is the Chebyshev polynomials:

Definition 7.33. The Chebyshev polynomial τ_n of degree n is defined to be the polynomial in $F[T]$ satisfying

$$\tau_n\left(T + \frac{1}{T}\right) = T^n + \frac{1}{T^n}.$$

The following well-known result is easily verified (the recursion can be used to prove existence).

Lemma 7.34. *For every $n \geq 1$ the n -th Chebyshev polynomial τ_n exists, is unique (for any given characteristic), and is monic. Moreover $\tau_1(T) = T$, $\tau_2(T) = T^2 - 2$, and*

$$\tau_{n+2}(T) = T \cdot \tau_{n+1}(T) - \tau_n(T) \quad \text{for all } n \geq 1.$$

Remark 7.35. When $F = \mathbb{Q}$ we get $\tau_n \in \mathbb{Z}[T]$. Such Chebyshev polynomials arise from the trigonometric identity $2 \cos(nT) = \tau_n(2 \cos(T))$.

The following is well-known, and the second part is easily verified.

Lemma 7.36. *Let n be an odd prime which is prime to the characteristic of F . Then the n -th Chebyshev polynomial $\tau_n \in F[T]$ has a dihedral geometric monodromy group of order $2n$, and this group acts on $\{x_i\}$ via the standard dihedral action.*

In particular, $\tau_n(T) - \tau_n(S)$ has $\langle \chi_{\tau_n}, \chi_{\tau_n} \rangle = (n+1)/2$ irreducible factors. All are quadratic, except for the linear factor $T - S$. So the action of the geometric monodromy group on $\{x_i\}$ is doubly transitive only for $n = 3$.

The following result of Burnside is an important piece in the classification.

Lemma 7.37. *Suppose G acts effectively and transitively, but not doubly transitively, on a set S of prime order l . Then G is isomorphic to a subgroup of the affine group $\mathbb{F}_l \rtimes \mathbb{F}_l^\times$.*

The last piece is provided by the following:

Lemma 7.38. *Let $f \in F[T]$ be a polynomial whose degree l is a prime distinct from the characteristic of F . If $G_f \subseteq \mathbb{F}_l \rtimes \mathbb{F}_l^\times$, then f is linearly related, over \bar{F} , to either a cyclic polynomial or a Chebyshev polynomial.*

Remark 7.39. See [Fri70] for the tame case. [FGS93] strengthens the result to general polynomials. See also [Mül97] (under the hypothesis that G_f is solvable).

Putting all this together gives the following classification.

Proposition 7.40. *Suppose $f \in F[T]$ has degree prime to the characteristic of F . Then the geometric monodromy group acts doubly transitively on the zeros $\{x_i\}$ if and only if one of the following hold:*

- (7.15) *f is indecomposable of composite degree.*
- (7.16) *f has degree 2.*
- (7.17) *f has degree 3 and is not linearly related to the cyclic polynomial T^3 .*
- (7.18) *f has prime degree $n > 3$ and is not linearly related over \bar{F} to either the cyclic polynomial or the Chebyshev polynomial of degree n .*

Remark 7.41. Suppose $f \in F[T]$ has degree n prime to the characteristic of F . It is easy to show that if f is linearly related over \bar{F} to a cyclic polynomial, then f is linearly related over F to a cyclic polynomial. However, $f \in F[T]$ can be linearly related over \bar{F} to the Chebyshev polynomial τ_n but not be linearly related over F .

This motivates the introduction of *Dickson polynomials*. For any $a \in F^\times$ and any positive integer n define the *Dickson polynomial*

$$D_{n,a}(T) = a^{n/2} \tau_n(a^{-1/2}T).$$

Then, for n odd, $f \in F[T]$ is linearly related over \bar{F} to the Chebyshev polynomial τ_n if and only if it is linearly related over F to a Dickson polynomial.

Note that if F is a finite field of odd characteristic then there are two nonlinearly related Dickson polynomials of each degree ($n > 2$); if F is a finite field of characteristic 2 there is only one.

Remark 7.42. The result quoted in the previous remark has been known for some time (see [Fri70] and [FGS93]; it can also be deduced from [Turn95, Lemma 1.9]). For the convenience of the reader we sketch an argument. Assume $n > 1$ since $n = 1$ is trivial.

First assume the characteristic of F is not 2, and check that the branch points of the covering map $\tau_n : \bar{F} \rightarrow \bar{F}$ (the elements $b \in \bar{F}$ where $\tau_n(T) - b$ has multiple roots) are $b_1 = 2$ and $b_2 = -2$. Next, check that the unique point unramified above $b_1 = 2$ is $a_1 = 2$ and the unique point unramified above $b_2 = -2$ is $a_2 = -2$. So, if f is linearly related over \bar{F} to τ_n , there are $a_1, a_2, b_1, b_2 \in \bar{F}$ such that b_1, b_2 are the branch points for the cover $f : \bar{F} \rightarrow \bar{F}$ and such that a_i is unramified over b_i .

If a_1 and a_2 are in the base field F , observe that the linear polynomials of $\bar{F}[T]$ sending $\{a_1, a_2\}$ to $\{-2, 2\}$ are in $F[T]$. If $a_i \in F$ then $b_i = f(a_i)$ is in F , so the linear polynomials of $\bar{F}[T]$ sending $\{b_1, b_2\}$ to $\{-2, 2\}$ are in $F[T]$. Conclude that f is linearly related over F to τ_n . So assume that some $a_i \notin F$. The derivative τ'_n has distinct roots of the form $\zeta + 1/\zeta$, where $\zeta \neq -1, 1$ is a $2n$ -th root of unity. Thus the derivative f' has distinct zeros. This implies that all ramification points are separable over F , and so a_1, a_2, b_1, b_2 are also in the separable closure of F . Since f has coefficients in F , a_1 and a_2 must be conjugate and contained in a quadratic extension F' of F . After

composing on the right by a linear polynomial in $F[T]$, we reduce to the case where $a_1 = \alpha$ and $a_2 = -\alpha$ where $\alpha^2 \in F$. Note that the images b_1, b_2 cannot be in F , and are in fact conjugate elements of F' . After composing on the left with an element of $F[T]$ we can assume f is monic and $b_2 = -b_1$. Finally, check that such f must be a Dickson polynomial.

Now, if the characteristic of F is 2, then $\tau_n : \bar{F} \rightarrow \bar{F}$ has a single branch point $b = 0$, and $a = 0$ is the unique point unramified above b . So any polynomial map $f : \bar{F} \rightarrow \bar{F}$ which is linearly related to τ_n must have a single branch point b , and a single point a unramified over b . Since f is defined over F , both a and b must be in the base field F . After linear compositions, we can assume $a = b = 0$ and f is monic. Thus $f = l_1 \circ \tau_n \circ l_2$ where $l_1(T) = c_1T$ and $l_2 = c_2T$. A simple consequence of the recursion for τ_n is that $\tau_n(T) = T^n + T^{n-2}$ plus lower order terms. This implies that $(c_2)^2 \in F$. Conclude that f is a Dickson polynomial.

7.4. A special class of Davenport pairs. Recall that one way to construct a DP (f, g) is as an SDP-Ex composition (Definition 1.1). Such DP's have the property that $1 \in \mathcal{D}_{f,g}$.

How does one construct DP's (f, g) with $1 \notin \mathcal{D}_{f,g}$? One strategy is to consider $f, g \in \mathbb{F}_q[T]$ with $g = f \circ l$ for some linear polynomial $l \in \mathbb{F}_q[T]$ not in \mathbb{F}_q . We see the only examples of this type, when f is indecomposable of degree prime to the characteristic of \mathbb{F}_q , are essentially of the form (T^n, aT^n) where $a \in \mathbb{F}_q$ is not an n -th power in \mathbb{F}_q (Corollary 7.45). In this case $f(T) = T^n$ and $l(T) = a^{1/n}T$.

Lemma 7.43. *Let $f \in F[T]$ be linearly related over \bar{F} to a Chebyshev polynomial of odd degree prime to the characteristic of F . Suppose that $f(\alpha T + \beta) \in F[T]$ for some $\alpha, \beta \in \bar{F}$, $\alpha \neq 0$. Then $\alpha, \beta \in F$.*

Proof. See [Turn95, Lemma 1.9]: Our $\tau_n(T)$ is equal to Turnwald's $D_n(1, T)$. \square

Proposition 7.44. *Let $f, g \in F[T]$ be indecomposable polynomials of degree n prime to the characteristic of F . Suppose F is a perfect field. If f and g are linearly related on the inside over \bar{F} then either:*

- (i) *f and g are linearly related on the inside over F , or*
- (ii) *f and g are both linearly related over F to the cyclic polynomial of degree n .*

In either case, f and g are linearly related over F .

Proof. Observe that $n < 3$ is trivial. If $G_{f,g}$ acts doubly transitively on $\{x_i\}$, use Lemma 7.28. Otherwise, use Proposition 7.40 to reduce to the Chebyshev or cyclic case. In the case where f and g are linearly related over \bar{F} to the Chebyshev polynomial and n is an odd prime, use the previous lemma. Finally, in the cyclic case, Remark 7.41 says that f and g are linearly related to T^n over the base field F . \square

Corollary 7.45. *Suppose that $f \in F[T]$ is indecomposable of degree n prime to the characteristic of F where F is a perfect field. If $g \in F[T]$ is linearly related to f on the inside over \bar{F} , but not over F , then there are linear $l_1, l_2, l_3 \in F[T]$ such that $l_1 \circ f \circ l_2 = T^n$ and $l_1 \circ g \circ l_3 = aT^n$ with $a \in F$ not an n -th power in F .*

8. Main results concerning indecomposability

The following results hold when one of the polynomials, f say, of the pair (f, g) is indecomposable with degree prime to the characteristic. There are essentially two cases, depending on whether or not f is linearly related to a cyclic polynomial. Recall f is linearly related to a cyclic polynomial over \mathbb{F}_q if and only if it is linearly related to a cyclic polynomial over $\bar{\mathbb{F}}_q$.

Theorem 8.1. *Let $f \in \mathbb{F}_q[T]$ be indecomposable over \mathbb{F}_q , nonexceptional, and of degree prime to the characteristic of \mathbb{F}_q . Let $g \in \mathbb{F}_q[T]$ be any polynomial where (f, g) forms a Davenport Pair, and let $g = g_1 \circ g_2$ be the induced decomposition over \mathbb{F}_q associated to (f, g) .*

If f is not linearly related to a cyclic polynomial, (f, g_1) is an SDP with multiplicity: the associated characters χ_f, χ_{g_1} are equal.

If f is linearly related to a cyclic polynomial, $g = f \circ h$ for some $h \in E[T]$ with E a finite extension of \mathbb{F}_q . Also, $g = l \circ f \circ h'$ for some $l, h' \in \mathbb{F}_q[T]$ with l linear, and f and $l \circ f$ are linearly related on the inside over $\bar{\mathbb{F}}_q$.

Proof. Let $g = h_1 \circ h_2$ be the induced decomposition over $\bar{\mathbb{F}}_q$ associated with the pair (f, g) . (It turns out, at least in the noncyclic cases, that the two induced decompositions, $g = g_1 \circ g_2$ and $g = h_1 \circ h_2$, are equivalent.)

Since (f, g) is a DP and f is nonexceptional, $f(T) - g(S)$ is reducible in $\bar{\mathbb{F}}_q[S, T]$ (Corollary 4.12). So $f(T) - h_1(S)$ is also reducible in $\bar{\mathbb{F}}_q[S, T]$ (Lemma 6.2). Since f is indecomposable over \mathbb{F}_q , f is indecomposable over $\bar{\mathbb{F}}_q$ (Theorem 3.5 of [FM69]). Thus the induced decompositions of both f and h_1 , associated to the pair (f, h_1) over $\bar{\mathbb{F}}_q$, are trivial. Lemma 6.1, especially property (6.2), implies $\bar{\mathbb{F}}_q\Omega_f = \bar{\mathbb{F}}_q\Omega_{h_1}$ and $G_f = G_{h_1} = G_{f, h_1}$. Finally, $\deg f = \deg h_1$ (Corollary 6.3).

Now we show, assuming that $f(T) - g(S)$ is reducible over \mathbb{F}_q , that we can take h_i to be g_i for $i = 1, 2$. Note: The argument that $\deg f = \deg h_1$ modifies to show $\deg f = \deg g_1$ under this reducibility assumption. Now, by Lemma 6.1,

$$\mathbb{F}_q(y_1) \cap \Omega_f = \mathbb{F}_q(g_2(y_1)) \quad \text{and} \quad \bar{\mathbb{F}}_q(y_1) \cap (\bar{\mathbb{F}}_q\Omega_f) = \bar{\mathbb{F}}_q(h_2(y_1)).$$

Since $\bar{\mathbb{F}}_q(\mathbb{F}_q(y_1) \cap \Omega_f) \subseteq \bar{\mathbb{F}}_q(y_1) \cap (\bar{\mathbb{F}}_q\Omega_f)$,

$$\bar{\mathbb{F}}_q(g_2(y_1)) \subseteq \bar{\mathbb{F}}_q(h_2(y_1)).$$

In particular, $g_2 = h' \circ h_2$ for some polynomial $h' \in \bar{\mathbb{F}}_q$. Since $\deg h_1 = \deg g_1$, $\deg h' = 1$. So, after adjusting h_1 and h_2 by a linear map, $h_i = g_i$, for $i = 1, 2$.

We divide the remaining proof into three cases, using Proposition 7.40.

Case 1: G_f acts doubly transitively on the zeros $\{x_i\}$ and $\deg f > 2$. By Proposition 7.26 and Corollary 7.30, $f(T) - h_1(S)$ has exactly two irreducible factors over $\overline{\mathbb{F}}_q$, and these factors have nonequal degrees. Substitute $h_2(S)$ for S in the factorization of $f(T) - h_1(S)$ to get the factorization of $f(T) - g(S)$ (Lemma 6.2). Thus the two irreducible factors of $f(T) - g(S)$ have nonequal T -degrees, so the action of $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ fixes them. Conclude that the factorization of $f(T) - g(S)$ is defined over \mathbb{F}_q . As above, this means we can take $h_1 = g_1$. The result follows from Proposition 7.26 and Corollary 7.27.

Case 2: f is linearly related over $\overline{\mathbb{F}}_q$ to a Chebyshev polynomial and $n = \deg f$ is an odd prime. Let $G = G_f = G_{h_1}$. By Lemma 7.36, G is isomorphic to a dihedral group of order $2n$. Note: G acts transitively on both $\{x_i\}$ and on the zeros $\{u_j\}$ of $h_1(T) - z$. Clearly, any two transitive actions of such a dihedral group on sets of order n are equivalent as permutation representations. Thus $G(x_1)$ is $G(u_j)$ for some j . Use the description of factorization of Remark 4.9 applied to $G(u_j) = G(x_1)$ acting on $\{x_i\}$ to conclude that the factorization of $f(T) - h_1(S)$ has exactly one linear factor Φ and $(n-1)/2$ irreducible quadratic factors in $\overline{\mathbb{F}}_q[S, T]$.

Recover the factorization of $f(T) - g(S)$ by substituting $h_2(S)$ for S in the factorization of $f(T) - h_1(S)$ (Lemma 6.2). Since $\Phi(T, h_2(S))$ is the unique irreducible factor of $f(T) - g(S)$ of T -degree one, the action of $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ fixes it. So $f(T) - g(S)$ is reducible in $\mathbb{F}_q[S, T]$. As discussed above, we can conclude that $h_1 = g_1$. Also, Φ , the only linear factor of $f(T) - g_1(S)$, must be defined over \mathbb{F}_q . The existence of Φ implies f and g_1 are linearly related on the inside over \mathbb{F}_q . Thus (f, g_1) forms a trivial SDP.

Case 3: f is linearly related over $\overline{\mathbb{F}}_q$ to a cyclic polynomial. (This automatically includes the case $\deg f = 2$.) Let $G = G_f = G_{h_1}$. So G is isomorphic to a cyclic group of order n acting transitively on both $\{x_i\}$ and on zeros $\{u_j\}$ of $h_1(T) - z$. Clearly, any two transitive actions of G on sets of order n are equivalent as permutation representations. Thus $G(x_1)$ is $G(u_j)$ for some j . Use Remark 4.9 to conclude that $f(T) - h_1(S)$ factors over $\overline{\mathbb{F}}_q$ as the product of n linear factors. This implies that $h_1 = f \circ l_0$ for some $l_0 \in \overline{\mathbb{F}}_q[T]$ of degree 1. So $g = f \circ h$, where $h = l_0 \circ h_2$.

Using [FGS93, Lemma 4.1] and that $\deg f$ is prime to p , we get a linear polynomial $l' \in \overline{\mathbb{F}}_q[T]$ such that $f' = f \circ l'$ and $h' = (l')^{-1} \circ h$ are in $\mathbb{F}_q[T]$, giving a decomposition $g = f' \circ h'$ over \mathbb{F}_q . By Proposition 7.44, $f' = l \circ f \circ l''$ for some linear $l, l'' \in \mathbb{F}_q[T]$. By replacing h' with $l'' \circ h'$, we obtain the decomposition $g = l \circ f \circ h'$. \square

Remark 8.2. If we replace the hypotheses (f, g) is a DP and f is not exceptional with the alternate hypothesis $f(T) - g(S)$ reducible over \mathbb{F}_q (keeping all the other hypotheses as they are) we get a variant of Theorem 8.1.

Remark 8.3. This paper has adopted the convention that polynomials have nonzero derivatives. Theorems 8.1 and 8.4 hold for g with zero derivative (with a suitable definition of *induced decomposition*).

Theorem 8.4. Let $f, g \in \mathbb{F}_q[T]$ be two polynomials with $\mathcal{V}_g(\mathbb{F}_{q^t}) \subseteq \mathcal{V}_f(\mathbb{F}_{q^t})$ for all t . Suppose f is indecomposable over \mathbb{F}_q and has degree prime to the characteristic of \mathbb{F}_q . Then there are $g_1, g_2 \in \mathbb{F}_q[T]$ with $g = g_1 \circ g_2$ and (f, g_1) is an SDP with multiplicity.

Proof. Consider Remark 8.2 together with Proposition 4.16. The case where f is not linearly related to a cyclic polynomial follows immediately.

In the cyclic case, consider the decomposition $g = l \circ f \circ h'$ of Theorem 8.1, where f and $f' = l \circ f$ are linearly related on the inside over \mathbb{F}_q . We claim f and f' are linearly related on the inside over \mathbb{F}_q , and so we can take $g_1 = f$. Suppose otherwise and use Corollary 7.45 to reduce to the case $f = T^n$ and $f' = aT^n$, where $a \in \mathbb{F}_q$ is not an n -th power. Choose t so that $q^t > \deg h'$ and a is not an n -th power in \mathbb{F}_{q^t} . Then $\mathcal{V}_f(\mathbb{F}_{q^t})$ contains only n -th powers, but if $c \in \mathbb{F}_{q^t}$ is not a zero of h' then $g(c)$ is not an n -th power, a contradiction. \square

Remark 8.5. In the above theorems, we can often conclude that (f, g_1) is actually a trivial SDP. In other words, we can choose the decomposition $g = g_1 \circ g_2$ in such a way that $g_1 = f$ itself.

For example, in case 2 of the above proof we concluded that (f, g_1) is a trivial SDP if $n = \deg f$ is an odd prime, and f is linearly related to a Chebyshev polynomial. In this case G_f is dihedral. In fact, from Proposition 7.44, having (f, g_1) a nontrivial SDP requires G_f to have two nonequivalent permutation representations on n elements whose associated characters are equal. This excludes most G_f .

Part of the classification of finite simple groups includes the classification of doubly transitive representations [CKS76]. This applies to classify groups G with two nonequivalent faithful permutation representations acting on a set with n elements such that:

- (i) The characters of the two actions are equal.
- (ii) The actions are doubly transitive.
- (iii) Some element of G acts as an n -cycle under the two actions.

The conclusion is that

$$G = \mathrm{PSL}_2(\mathbb{F}_{11}) \quad \text{and} \quad n = 11, \quad \text{or} \\ \mathrm{PSL}_k(\mathbb{F}_s) \subseteq G \subseteq \mathrm{P\Gamma L}_k(\mathbb{F}_s) \quad \text{and} \quad n = (s^k - 1)/(s - 1) \text{ for some } k \geq 3.$$

[Fri73] conjectured this; [Fri99, Thm. 2.7 and §9] has complete details, including historical information. The field \mathbb{F}_s appearing in the above list is called the *characteristic field* of the Chevalley group G .

This result allows us to strengthen the above theorems: if $G = G_f$ and n are not of the above form, then the conclusion (f, g_1) is an SDP, can be replaced by the stronger conclusion $g = f \circ h$ for some $h \in \mathbb{F}_q[T]$.

Not all of the above groups are expected to occur as geometric monodromy groups of polynomials for a given \mathbb{F}_q . Guralnick has conjectured the following: the finite simple groups appearing as composition factors of geometric monodromy groups G_f as f varies over all polynomials, or even all rational functions, are, with finitely many exceptions (depending on the characteristic), the cyclic groups, the alternating groups, and the Chevalley groups with characteristic field containing \mathbb{F}_p . Thus, we can expect among $f \in \mathbb{F}_q[T]$ with \mathbb{F}_q of fixed characteristic p , that the fields \mathbb{F}_s appearing as G_f as in the above classification should, with a finite number of exceptions depending on p , also be of characteristic p .

By way of contrast, in the case where \mathbb{F}_q and \mathbb{F}_s have the same characteristic, examples abound. [Fri99, Thm. 5.2] (dependent on [Abh97]) states that, for any finite field \mathbb{F}_q , any s a power of the characteristic of \mathbb{F}_q , and any $k \geq 3$, there is a nontrivial SDP (f, g) with $\chi_f = \chi_g$ whose geometric monodromy group is $G_f = G_g = \mathrm{PSL}_k(\mathbb{F}_s)$.

References

- [Abh97] S.S. Abhyankar, *Projective polynomials*, Proc. Amer. Math. Soc., **125** (1997), 1643–1650, [MR 1403111](#) (98a:12001), [Zbl 0912.12004](#).
- [Ait98] W. Aitken, *On value sets of polynomials over a finite field*, Finite Fields Appl., **4** (1998), 441–449, [MR 1648581](#) (99h:11138), [Zbl 0929.11059](#).
- [Art23] E. Artin, *Über die Zetafunktionen gewisser algebraischer Zahlkörper*, Math. Ann., **89** (1923), 147–156, [Zbl 49.0123.02](#).
- [Coh81] S.D. Cohen, *Value sets of functions over finite fields*, Acta Arith., **39** (1981), 339–359, [MR 0640921](#) (83e:12015), [Zbl 0399.12005](#).
- [CF95] S.D. Cohen and M.D. Fried, *Lenstra’s proof of the Carlitz–Wan conjecture on exceptional polynomials: an elementary version*, Finite Fields Appl., **1** (1995), 372–375, [MR 1341953](#) (96d:11127), [Zbl 0839.11063](#).
- [CKS76] C.W. Curtis, W.M. Kantor and G.M. Seitz, *The 2-transitive permutation representations of the finite Chevalley groups*, Trans. Amer. Math. Soc., **218** (1976), 1–59, [MR 0422440](#) (54 #10429), [Zbl 0374.20002](#).
- [Den84] J. Denef, *The rationality of the Poincaré series associated to the p -adic points on a variety*, Invent. Math., **77**(1) (1984), 1–23, [MR 0751129](#) (86c:11043), [Zbl 0537.12011](#).
- [DL] J. Denef and F. Loeser, *Definable sets, motives and p -adic integrals*, J. Amer. Math. Soc., **14**(2) (2001), 429–469, [MR 1815218](#) (2002k:14033), [Zbl 01566267](#).
- [Fri70] M.D. Fried, *On a conjecture of Schur*, Michigan Math. J., **17** (1970), 41–45, [MR 0257033](#) (41 #1688), [Zbl 0169.37702](#).

- [Fri73] M.D. Fried, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Illinois J. Math., **17** (1973), 128–146, [MR 0347828](#) (50 #329), [Zbl 0266.14013](#).
- [Fri74] M.D. Fried, *On a theorem of MacCluer*, Acta Arith., **25** (1974), 122–126, [MR 0337911](#) (49 #2680), [Zbl 0229.12021](#).
- [Fri94] M.D. Fried, *Global construction of general exceptional covers, with motivation for applications to coding*, G.L. Mullen and P.J. Shiue, Finite Fields: Theory, Applications and Algorithms, Contemp. Math., **168**, Amer. Math. Soc., Providence, 1994, 69–100, [MR 1291419](#) (95f:12005), [Zbl 0849.12002](#).
- [Fri99] M.D. Fried, *Variables separated polynomials, the genus 0 problem and moduli spaces*, Number Theory in Progress (Berlin-New York) (J. Urbanowicz, K. Gyory, H. Iwaniec, eds.), Walter de Gruyter, 1999, Proceedings of the Schinzel Festschrift, Summer 1997, 169–228, <http://www.math.uci.edu/~mfried/#math>, [MR 1689506](#) (2000g:14033), [Zbl 01305290](#).
- [FGS93] M.D. Fried, R. Guralnick and J. Saxl, *Schur covers and Carlitz's conjecture*, Israel J. Math., **82** (1993), 157–225, [MR 1239049](#) (94j:12007), [Zbl 0855.11063](#).
- [FJ86] M.D. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik III, **11**, Springer-Verlag, 1986, [MR 0868860](#) (89b:12010), [Zbl 0625.12001](#).
- [FM69] M.D. Fried and R.E. MacRae, *On the invariance of chains of fields*, Illinois J. Math., **13** (1969), 165–171, [MR 0238815](#) (39 #179), [Zbl 0174.07302](#).
- [FS76] M.D. Fried and G. Sacerdote, *Solving diophantine problems over all residue class fields of a number field and all finite fields*, Ann. of Math., **104**(2) (1976), 203–233, [MR 0491477](#) (58 #10722), [Zbl 0376.02042](#).
- [Frö67] A. Frölich, *Local Fields*, Algebraic Number Theory (ed. J. W. S. Cassels, A. Frölich), Academic Press, London, 1967, 1–41, [MR 0236145](#) (38 #4443).
- [GW97] R. Guralnick and D. Wan, *Bounds for fixed point free elements in a transitive group and applications to curves over finite fields*, Israel J. Math., **101** (1997), 255–287, [MR 1484879](#) (98j:12002), [Zbl 0910.11053](#).
- [Mül97] P. Müller, *A Weil-bound free proof of Schur's conjecture*, Finite Fields Appl., **3**(1) (1997), 25–32, [MR 1429041](#) (98d:11143), [Zbl 0904.11040](#).
- [Mül98] P. Müller, *Kronecker conjugacy of polynomials*, Trans. Amer. Math. Soc., **350**(5) (1998), 1823–1850, [MR 1458331](#) (98h:11032), [Zbl 0894.11006](#).
- [Ser79] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, 1979, [MR 0554237](#) (82e:12016), [Zbl 0423.12016](#).
- [Turn95] G. Turnwald, *On Schur's conjecture*, J. Austral. Math. Soc. Ser. A, **58**(3) (1995), 312–357, [MR 1329867](#) (96a:11135), [Zbl 0834.11052](#).
- [vdW35] B. L. van der Waerden, *Die Zerlegungs- und Trägheitsgruppe als Permutationsgruppen*, Math. Ann., **111** (1935), 731–733, [Zbl 0012.24402](#).

Received December 20, 2001 and revised June 13, 2002. The second author was partially supported by #DMS-9970676, #DMS-0202259 and a senior research Alexander von Humboldt award. The first author would like to thank M. Zieve and R. Guralnick for helpful discussions, and MSRI and UCI for their support and hospitality.

CAL. STATE SAN MARCOS
 SAN MARCOS, CA 92096
E-mail address: waitken@csusm.edu

UC IRVINE
IRVINE, CA 92697
E-mail address: mfried@math.uci.edu

CAL. STATE SAN MARCOS
SAN MARCOS, CA 92096
E-mail address: lholt@csusm.edu

This paper is available via <http://www.pacjmath.org/2004/iii-i-i.html>.