J. Aust. Math. Soc. **85** (2008), 191–196
doi:10.1017/S1446788708000840

FROBENIUS GROUPS AS MONODROMY GROUPS

ROBERT M. GURALNICK

(Received 3 February 2008; accepted 4 April 2008)

Communicated by Martin W. Liebeck

Dedicated to Cheryl Praeger for her sixtieth birthday

Abstract

We study Frobenius groups acting on curves.

2000 *Mathematics subject classification*: primary 14H30, 14H05; secondary 12F10, 20B25.
Keywords and phrases: Frobenius group, monodromy group, coverings of curves.

1. Introduction

Let k be an algebraically closed field of characteristic $p \geq 0$. Consider a separable nontrivial rational map $f : X \to Y$ between smooth projective curves X, Y defined over k. We call the Galois group of the Galois closure of $k(X)/k(Y)$ the monodromy group of f. A major tool in studying such covers is to translate arithmetic and geometric questions to questions about the monodromy group. This has been used very successfully in many instances. See [4] and [5] for examples and other references.

Recall that a Frobenius group is a finite permutation group G acting transitively on a set Ω with nontrivial point stabilizer such that no nonidentity element fixes two points. It follows that there is a Frobenius kernel N, a normal subgroup such that $N^\# = N \setminus (1)$ is precisely the set of fixed point free elements of G, and a Frobenius complement H (a point stabilizer). Rather surprisingly the only proof that the Frobenius kernel exists involves character theory (this was first proved by Frobenius).

This implies easily that N acts regularly on Ω. So we can identify Ω with N as an H-set, and so every nontrivial element of H acts on $N^\#$ by conjugation without fixed points. By a famous theorem of Thompson [7], this implies that N is nilpotent.

A rational function is a map from $\mathbb{P}^1$ to $\mathbb{P}^1$; similarly, a polynomial is a rational function that is totally ramified at ∞.

The author was partially supported by NSF Grant DMS 0653873.

In this note, we show that rational functions with monodromy group a Frobenius group have very special properties; in particular, the Galois closure has genus at most one. This was originally proved independently by the author [2] and Flynn [1]. These come up in many of the examples of interesting polynomials (for example, exceptional polynomials, subadditive polynomials) and also come up in a reduction theorem of the author (see [4, 5, 3]). The proofs given here are representation theoretic in nature and quite different from the earlier proofs.

In fact, we prove a much more general result for Frobenius groups acting on a curve X; see Theorem 3.1 for the precise statement. We also prove an analog under a weaker condition on fixed points of elements in inertia subgroups (see Theorem 4.2).

See [4] or [5] for basic results on monodromy groups and coverings of curves.

2. Basic properties of frobenius groups

We first point out an easy property of Frobenius groups. Recall that a group acts semiregularly on a set if no nonidentity element of the group fixes a point. If V is a G-module, let V^G denote the fixed points of G on V. If H is a subgroup of G and W is an H-module, let W_H^G denote the induced module.

LEMMA 2.1. *Let G be a Frobenius group with k a field.*

(1) *The subgroup H acts semiregularly on the set of isomorphism classes of nontrivial irreducible modules of N (by conjugation).*

(2) *If V is an irreducible kG-module, then either $V^N = V$ or $V \cong W_N^G$ for some (nontrivial) irreducible N-module W.*

(3) *If V is an irreducible kG-module, then either $V^N = V$ or V is a free module for H and $V^H \neq 0$.*

PROOF. Let V be an irreducible kN-module. Suppose that $1 \neq h \in H$ preserves V. Let M be the kernel of N on V. Since N is nilpotent, N/M has a nontrivial center and h must centralize this center (since it preserves the representation), whence $C_N(h) \neq 1$ (since the order of h is coprime to $|N|$). This contradicts the definition of Frobenius group.

Let V be an irreducible G-module with $V^N \neq V$. Let W be an irreducible N-submodule of V. By (1), W_N^G is a direct sum of nonisomorphic N-modules permuted freely by H and in particular is irreducible. Since $0 \neq \mathrm{Hom}_N(W, V) \cong \mathrm{Hom}_G(W_N^G, V)$ (by Frobenius reciprocity), it follows that $V \cong W_N^G$. This implies that V is a free H-module. Parts (2) and (3) follow. □

COROLLARY 2.2. *Let G be a Frobenius group with Frobenius kernel N and complement H. Let V be a finite-dimensional $\mathbb{C}G$-module with $V^G = 0$. Then* $\dim V = \dim V^N + |H| \dim V^H$.

PROOF. It suffices to prove this formula for an irreducible nontrivial G-module. If $V^N = V$, then $V^H = V^G = 0$ since V is nontrivial. If $V^N = 0$, then V is a free H-module, whence the result holds. □

https://doi.org/10.1017/S1446788708000840 Published online by Cambridge University Press

3. Frobenius groups acting on curves

We first recall some facts about the Tate module for a finite group acting on a curve X. The Tate module is a $\mathbb{C}G$-module of dimension $2g$ with g the genus of X. It can be constructed as follows. Let r be a prime different from the characteristic of X with r not dividing the order of G. Let W be the r-torsion points of the Jacobian of X. This has order r^{2g} and is a module for G. Its Brauer character is the character of G on the Tate module (this defines the Tate module; it does not depend upon the choice of r). The Tate module is uniquely determined by noting that its character is rational valued and that, if H is a subgroup of G, then $\dim V^H = 2g(X/H)$. This is the property that we require. Applying Corollary 2.2 to the Tate module gives the following corollary.

COROLLARY 3.1. *Let G be a Frobenius group acting on a curve X of genus g with X/G of genus zero. Let N be the Frobenius kernel and H a Frobenius complement. Then $g = g(X/N) + g(X/H)|H|$.*

The special case when $g(X/H) = 0$ had been proved much earlier independently by the author and Flynn [1, Theorem 9]. The previous result with $g(X/H) = 0$ says that $g = g(X/N)$. This implies that $g \leq 1$ (since if X is a curve of genus $g > 1$, there is no separable map of degree greater than one from X to another curve of genus g). Moreover, if $g = 1$, then $g(X/N) = 1$, and so the cover $X \to X/N$ must be unramified (and conversely). In particular, it follows that N is abelian of rank at most two. By considering subgroups of $\mathrm{Aut}(\mathbb{P}^1) = \mathrm{PGL}(2, k)$ and $\mathrm{Aut}(X)$ with X of genus one, we have the following result (see [6] for facts about automorphism groups of elliptic curves).

COROLLARY 3.2. *Let G be a Frobenius group acting on a curve X of genus g over a field k of characteristic $p \geq 0$. Let N be the Frobenius kernel and H a Frobenius complement of index n. If X/H has genus zero, then $g \leq 1$. Moreover, N is abelian. Furthermore:*

(1) *either $g = 0$, and*
  - (a) *G is dihedral of order $2n$, or*
  - (b) *$n = 4$, or*
  - (c) *$n = p^a$;*

(2) *or $g = 1$, $X \to X/N$ is unramified (X/N also has genus one) and H is cyclic of order two, three, four or six or $p \leq 3$.*

By considering the automorphism groups of curves of genus at most one, we can write down all such examples. We single out a special case.

COROLLARY 3.3. *Let $f(x)$ be a separable rational function in $k(x)$ of prime degree r. Assume that k is algebraically closed of characteristic p. Assume that the Galois group G of the Galois closure L of $k(x)/k(f(x))$ is solvable. Then G has a normal subgroup N of order r and one of the following holds:*

https://doi.org/10.1017/S1446788708000840 Published online by Cambridge University Press

(1) *there is a totally ramified point, L has genus zero, and*
   (a) *$r \neq p$ and G is cyclic of order r or dihedral of order $2r$, or*
   (b) *$r = p$ and $G \leq \mathrm{AGL}(1, p)$;*

(2) *there is no totally ramified point, $L = k(E)$ where E is an elliptic curve, $E \to E/N$ is unramified and G/N is a nontrivial cyclic subgroup of $\mathrm{Aut}(E)$; in particular, G/N has order two, three, four or six.*

PROOF. Observe that G is a solvable transitive subgroup of the symmetric group of degree r. Thus, G is a Frobenius group (or is cyclic of order r). Thus, our earlier results apply and it is straightforward to determine the possibilities. □

One can easily write down the rational functions (up to equivalence) that occur in the previous result. In particular, if $r \neq p$ and f is a polynomial, then L has genus zero and f is equivalent either to x^r or to a Dickson polynomial of degree r.

4. A variation on the theme

Now we consider another variation. Rather than consider the case where G is a Frobenius group, we just assume that:

($*$) G is a finite group acting on a curve X of genus g with a subgroup H of index $n > 1$. If $1 \neq x \in G$ fixes some point of X, then x fixes at most one point on G/H.

So we are only assuming the condition that nontrivial elements of inertia groups fix no more than one point on G/H. We first point out the following result. Recall that $O_p(J)$ is the largest normal p-subgroup of J.

LEMMA 4.1. *Let G be a finite transitive permutation group on the a Ω of cardinality n. Let I be a subgroup of G with $I/O_p(G)$ cyclic. Assume that, if $1 \neq g \in I$, then g fixes at most one point on Ω. Then every orbit except perhaps one is regular for I. In particular, the number of orbits of I on Ω is at most $(n-1)/|I| + 1$. Moreover, equality holds precisely when I fixes a point of Ω.*

PROOF. We may assume that I has at least one nonregular orbit. Let w be a point in that orbit, and let $x \in I$ be an element of prime order r fixing w. Note that the centralizer of x in G must also fix w (since w is the unique point fixed by x). In particular, if $r = p$, then the center Z of $O_p(I)$ fixes w as does the normalizer. Since w is also the unique fixed point of Z and I normalizes Z, I also fixes w. In this case I has a fixed point, and all other orbits are regular. Thus the number of orbits is $1 + (n-1)/|I|$.

So we may assume that no nontrivial element of $O_p(I)$ fixes a point of Ω and $r \neq p$. In particular, it follows that any element of I of order prime to p fixes a point in Iw, and so has no fixed points in any other I-orbit. In this case, there is one orbit of size $|O_p(I)|$ and all other orbits are regular. □

https://doi.org/10.1017/S1446788708000840 Published online by Cambridge University Press

THEOREM 4.2. *Assume that* $(*)$ *holds. Let* h *be the genus of* X/H *and* $|G| = m$.

(1) *Then* $g - 1 \le hm/(n-1)$, *with equality if and only if each inertia subgroup is conjugate to a subgroup of* H.

(2) *In particular, if* $h = 0$, *then* X *has genus at most one. Moreover,* X *has genus one if and only if each inertia group is conjugate to a subgroup of* H.

PROOF. Let g be the genus of X and h the genus of X/G. Let J be any subgroup of an inertia group. Set $n = [G : H]$ and $m = |G|$.

By the Riemann–Hurwitz formula,

$$2(g-1)/m = -2 + \sum a_J(1 - 1/|J|)$$

and

$$2(h-1)/n = -2 + \sum a_J(1 - \mathrm{orb}(J, G/H))n.$$

Here the sum runs over some family of subgroups each contained in an inertia group and the a_J are positive rational numbers. Also $\mathrm{orb}(J, G/H)$ is the number of orbits of J on G/H. By the previous lemma, $\mathrm{orb}(J, G/H) \le 1 + (n-1)/|J|$ and so

$$1 - \mathrm{orb}(J, G/H)/n \ge (n-1)/n - (n-1)/n|J| = [(n-1)/n](1 - 1/J|).$$

Thus, multiplying the second equation by $n/(n-1)$ and using equality in the third equation, we see that

$$2(h-1)/(n-1) \ge -2n/(n-1) + \sum a_J(1 - 1/|J|) = 2(g-1)/m - 2/(n-1).$$

So $h/(n-1) \ge (g-1)/m$ or $g - 1 \le hm/(n-1)$. In particular, $h = 0$ implies that $g \le 1$. The same argument shows that we have a strict inequality above unless each inertia group has one orbit of size one and all other orbits regular (and in this case, we have equality, forcing $g = 1$). □

References

[1] John Flynn, 'Near-exceptionality over finite fields', PhD Thesis, University of California Berkeley, 2001.

[2] Robert M. Guralnick, 'Rational functions with monodromy group a Frobenius group', Preprint, 2000.

[3] ———, 'Solvable monodromy groups of low genus covers', Preprint.

[4] ———, *Monodromy Groups of Coverings of Curves, Galois Groups and Fundamental Groups*, Mathematical Sciences Research Institute Publications, 41 (Cambridge University Press, Cambridge, 2003), pp. 1–46.

[5] Robert M. Guralnick, Peter Müller and Jan Saxl, 'The rational function analogue of a question of Schur and exceptionality of permutation representations', *Mem. Amer. Math. Soc.* **162**(773) (2003).

[6] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106 (Springer, New York, 1992).

[7] J. G. Thompson, 'Finite groups with fixed-point-free automorphisms of prime order', *Proc. Natl. Acad. Sci. USA* **45** (1959), 578–581.

ROBERT M. GURALNICK, Department of Mathematics, University of
Southern California, Los Angeles, CA 90089-2532, USA
e-mail: guralnic@usc.edu

https://doi.org/10.1017/S1446788708000840 Published online by Cambridge University Press