Galois Groups and Fundamental Groups
MSRI Publications
Volume **41**, 2003

Monodromy Groups of Coverings of Curves

ROBERT GURALNICK

Abstract. We consider finite separable coverings of curves $f : X \to Y$ over a field of characteristic $p \geq 0$. We are interested in describing the possible monodromy groups of this cover if the genus of X is fixed. There has been much progress on this problem over the past decade in characteristic zero. Recently Frohardt and Magaard completed the final step in resolving the Guralnick–Thompson conjecture showing that only finitely many nonabelian simple groups other than alternating groups occur as composition factors for a fixed genus. There is an ongoing project to get a complete list of the monodromy groups of indecomposable rational functions with only tame ramification. In this article, we focus on positive characteristic. There are more possible groups but we show that many simple groups do not occur as composition factors for a fixed genus. We also give a reduction theorem reducing the problem to the case of almost simple groups. We also obtain some results on bounding the size of automorphism groups of curves in positive characteristic and discuss the relationship with the first problem. We note that prior to these results there was not a single example of a finite simple group which could be ruled out as a composition factor of the monodromy group of a rational function in any positive characteristic.

Contents

Mathematics Subject Classification: 14H30, 14H37, 20B15, 20B25.

Keywords: curves, coverings of curves, permutation group, automorphisms of curves, genus.

The author gratefully acknowledges support from MSRI and NSF grant DMS 9970305.

1. Introduction

Let k be a perfect field of characteristic $p \geq 0$. Suppose that X and Y are smooth projective curves over k and $f : X \to Y$ is a nonconstant separable rational map. The (arithmetic) monodromy group A of this cover is defined to be the Galois group of the Galois closure of the extension of function fields $k(X)/k(Y)$. Let Z denote the curve corresponding to the Galois closure. Let H be the subgroup of A corresponding to X, i.e. $X = Z/H$. It is possible that k', the constant field of Z, properly contains k. Let G be the normal subgroup of A consisting of those automorphisms which are the identity on k'. We call G the geometric monodromy group of the cover. Then A/G is isomorphic to the Galois group of k'/k.

The general theme that we wish to stress is that many arithmetic and geometric properties of the cover f can be recast in properties of A and G and their permutation representation on the cosets of H. This program has proved very successful in attacking several problems — in particular, exceptional polynomials [16], [42], [34], covers with a totally ramified point [35], exceptional rational functions [31] and the genus question. This approach has three parts. The first is the translation of the arithmetic or geometric problem to a group theoretic one. The second is the solution of the group theoretic problem. Finally, the third problem is to determine which group theoretic solutions correspond to an actual geometric solution. All three parts may be difficult and interesting. In particular, the classification of finite simple groups and results about primitive permutation groups have been used to solve several outstanding problems (for example, see the above mentioned references).

The main focus of this article is to study in more detail the problem of describing the covers if we bound the genus of X. For this problem, we may assume that k is algebraically closed and in particular $A = G$. There has been great progress when $p = 0$ or more generally if the cover is tame. See [22]. We will develop approaches here that are valid even in the presence of wild ramification.

If the cover is Galois, then there are classical results bounding the order of $\mathrm{Aut}(X)$. By a classical result of Hurwitz, if the cover is tame and $g(X) > 1$, then $|G| \leq 84(g-1)$. If $p > 0$, Stichtenoth [64] showed that $|G| < 16g^4$ with one explicit family of exceptions — see also [56], [57].

The other extreme case is when the cover is indecomposable (or equivalently, the field extension $k(X)/k(Y)$ is minimal). Since every cover is a composition of indecomposable covers, this is a critical case. There is in fact a very close connection between the Galois and non-Galois cases. In particular, if G has no genus zero representations, then it cannot act on a curve of small genus (relative to the size of G). This is already apparent in [64].

Let S be a (nonabelian) simple group. We say that S is a genus g group (in characteristic p), if S is a composition factor of the monodromy group of a cover $f : X \to Y$ with X of genus at most g. Since there exist covers from $X \to \mathbb{P}^1$ of

degree n with monodromy group S_n (or A_n) for $g = 0$, we will concentrate on Chevalley groups.

Thus, we let $\mathbf{E}_p(g)$ denote the set of genus g groups (in characteristic p) other than alternating groups. Similarly, let $\mathbf{E}_p^{\mathrm{ta}}(g)$ denote the set of simple groups (other than alternating groups) which are composition factors of monodromy groups of tamely ramified covers $X \to Y$ with X of genus at most g.

By [40], this problem reduces to the case where f is indecomposable. It is also easy to see that the critical case is when Y has genus 0. If $p = 0$, there is a recent result answering a question posed in [40] (the final paper proving this result was done by Frohardt and Magaard [22]; other papers involved in the proof include [21], [32], [40], [58], [6], [49] and [51]) — since the proof really only uses the assumption that the cover is tame, the result can be stated as follows:

THEOREM 1.1. *$\mathbf{E}_p^{\mathrm{ta}}(g)$ is finite for each g.*

Indeed, much more precise information is known and hopefully a complete determination of the monodromy groups of the tamely ramified indecomposable covers of genus zero (and in particular, indecomposable rational functions) will be available in the near future. In particular, there will be several infinite families and a finite list of other examples. There will be a similar result for any fixed genus g.

We mention two results which involve special cases of this analysis.

The first is a special case in [31]:

THEOREM 1.2. *Let $f(x) \in \mathbb{Q}(x)$ be an indecomposable rational function. Suppose that f is bijective modulo p for infinitely many primes p. Aside from finitely many possibilities, the genus of the Galois closure of $\mathbb{Q}(x)/\mathbb{Q}(f)$ is at most 1.*

A much more precise version of the theorem is in [31], where an essentially complete list of possibilities is given. After one solves the group theory problem, it is left to determine which possibilities actually arise. This involves a careful analysis of elliptic curves and results about torsion points and isogenies of elliptic curves over $\mathbb{Q}$.

The second result is a consequence of [32], [30] and [39].

THEOREM 1.3. *Let $g \geq 4$ and $p = 0$. Let X be a generic curve of genus g. If $f : X \to \mathbb{P}^1$ is an indecomposable cover of degree n, then the monodromy group of f is either S_n with $n > (g+1)/2$ or A_n with $n > 2g$.*

This was a problem originally studied by Zariski who proved that if $g > 6$ and $f : X \to \mathbb{P}^1$ with X generic of genus g, then the monodromy group of f is not solvable (this is a special case of the result above — using the observation of Zariski that any such cover is a composition of an indecomposable cover and covers from $\mathbb{P}^1$ to $\mathbb{P}^1$). A more precise statement of the theorem above is to say that the set of Riemann surfaces of genus $g \geq 4$ which have indecomposable covers of degree n to $\mathbb{P}^1$ with monodromy group other than A_n or S_n is contained

in a proper closed subvariety of the moduli space of genus g curves. It is well known that S_n does occur as the monodromy group of the generic curve (for $n > (g+1)/2$). It has been recently shown [17] that A_n actually does occur for $n > 2g$, thus giving a fairly complete picture of the situation when $g > 3$.

If $g < 4$, there are more group theoretic possibilities. In unpublished work, Fried and Guralnick have considered some possibilities for $g = 2$. The recent work of Frey, Magaard and Völklein show that there are other examples when $g = 3$ (all the group theoretic possibilities for $g = 3$ are known by the results cited above).

Until now, it was not known that a single simple group in any positive characteristic could be shown not to be a genus 0 group. In this article, we show that there are infinitely many such groups. In particular, we show that:

THEOREM 1.4. *If p does not divide the order of $|S|$, then $S \in \mathbf{E}_p(g)$ implies that $S \in \mathbf{E}_p^{\mathrm{ta}}(g+2) \subseteq \mathbf{E}_0(g+2)$. In particular, for any odd prime p and any g, there are infinitely many simple groups not in $\mathbf{E}_p(g)$.*

We also show that there are infinitely many simple groups whose order is divisible by p which are not in contained in $\mathbf{E}_p(g)$ for a fixed p and g. Let $\mu_p(S)$ be the smallest g such that $S \in \mathbf{E}_p(g)$. Let $\mathrm{Chev}(r)$ denote the family of simple groups which are Chevalley groups in characteristic r. Let $\mathrm{Chev}_b(r)$ denote the groups in $\mathrm{Chev}(r)$ which have rank at most b. Indeed, we prove the following result.

THEOREM 1.5. *Let X be a fixed type of Chevalley group. Fix a nonnegative integer g. There are only finitely many pairs (p,q) with p a prime and q a prime power not divisible by p such that $X(q) \in \mathbf{E}_p(g)$. More precisely, $\mu_p(X(q)) \to \infty$ as $q \to \infty$ for $(p,q) = 1$ and $\mathbf{E}_p(g) \cap \left(\bigcup_{r \neq p} \mathrm{Chev}_b(r)\right)$ is finite for each g.*

The proof shows that typically $\mu_p(X(q))$ grows like a polynomial of degree close to b in q (as long as p does not divide q).

Abhyankar ([1], [2], [3], [4], [5]) has shown that many finite groups of Lie type (particularly the classical groups) are genus 0 groups in the natural characteristic and so the exclusion $p \neq r$ is necessary.

This led the author to make the following conjecture several years ago—the positive characteristic analog of the Guralnick–Thompson Let $\mathrm{Chev}(r)$ denote the set of finite simple groups which are finite groups of Lie type over a field of characteristic r.

CONJECTURE 1.6. $\mathbf{E}_p(g) \cap \left(\bigcup_{r \neq p} \mathrm{Chev}(r)\right)$ *is finite.*

Given the classification of finite simple groups, this conjecture says that there are only finitely many simple groups in $\mathbf{E}_p(g)$ other than Chevalley groups in characteristic p.

The previous theorem goes a long way towards proving the conjecture. Namely, the conjecture is true if we consider Chevalley groups of bounded dimension. The next step would be to prove the same result for fixed q and then finally to prove

that the genus increases as the rank of the Chevalley group increases irrespective of field size (all under the assumption that we are considering Chevalley groups in characteristic different from the characteristic of the field).

It is not clear what the right answer for exceptional groups in the natural characteristic is. It will also be quite difficult to handle the case of small fields — this was already evident in the case for tame covers. Some of the techniques developed here should be useful.

We prove two main results and then apply them to obtain the previous theorem. The first is to show that one can check these questions by reducing to a few minimal configurations and in particular, if p does not divide $|\operatorname{Aut}(S)|$, it reduces to the tame case. The results we obtain here give a much easier reduction for the genus problem even in characteristic zero (but do give less precise information). The analog of the reduction theorem in the tamely ramified case seems out of reach when wild ramification is present.

The second is to show that there is a close connection between the genus of the Galois closure of the cover and the genus of X. In particular, let $\gamma_p(S)$ be the minimal genus $h > 1$ of a curve Z (in characteristic p) so that S is a subgroup of $\operatorname{Aut}(Z)$. We show that if $\gamma_p(S)/|S|$ is large compared to fixed point ratios of elements in primitive permutation representations of S (and related groups), then S cannot be a genus g group for g small.

This is used in conjunction with the following theorem.

THEOREM 1.7. *Let X be a type of Chevalley group. Let p and r be distinct primes. There exists a constant $c = c(X)$ such that if $X(r^a)$ acts on a curve of genus $g > 1$, then $g \geq c|X(r^a)|$.*

Using patching constructions, one can show that the constant $c(X) \to 0$ as the rank of X goes to infinity and also that the characteristic assumptions are necessary.

Of course if $g \leq 1$, we know the automorphism groups. For tame covers, a more specific version of the previous result is the Hurwitz bound on the size of $\operatorname{Aut}(X)$. We will explore other bounds on automorphism groups of curves in future work.

The paper is organized as follows. In section 2, we discuss the Riemann–Hurwitz formula and show the connection between fixed points in permutation representations and the genus.

In section 3, we indicate the connection between the ℓ-torsion in the Jacobian (and more generally the Tate module) and the genus and use some elementary representation theory to obtain some inequalities on the genus.

In section 4, we give upper bounds for $\mu(S)$ and also show how to reduce to the case that the cover is indecomposable and the map is to $\mathbb{P}^1$.

In section 5, we deal with the case of regular normal subgroups and show how one can reduce to a smaller case (at the expense of possibly slightly increasing the minimal genus).

In section 6, using the previous sections, we prove our main reduction result and prove Theorem 1.4.

In section 8, we obtain estimates for the Riemann–Hurwitz formula when we have certain conditions on the inertia groups.

In section 9, we indicate the relationship between the genus of the Galois closure and $\mu(S)$ and prove our main result about Chevalley groups.

In sections 10, 11 and 12, we introduce some group theoretic notation and machinery. In particular, we prove a simple version of the Aschbacher–O'Nan–Scott theorem that we use in the paper. There is a nice proof of this in the literature (see [48]), but our proof is quite short and elementary and gives the result precisely in the form we require. We also include a proof of a version of Aschbacher's theorem on subgroups of classical groups. This has been of fundamental importance in studying primitive permutation groups.

In the final section, we turn to a different topic. It does show how group theory plays an important role in studying covers of curves. It gives a simpler example of a group G such that G/Q is an abelian p'-group on two generators where Q is a quasi-p group (i.e. is generated by its Sylow p-subgroups) but $G \neq QA$ where A is abelian. In the case that G/Q is cyclic, clearly cyclic supplements always exist and this easy fact is used in the proof of the Abhyankar conjecture for curves.

This example in conjunction with work of Harbater and Van der Put [44] shows that the strongest form of a conjecture of Abhyankar about covers unramified outside a normal crossing in the affine plane is not true. A much more general but more complicated construction is given by the author in the appendix of [44].

Some of the results stated above do depend on the classification of finite simple groups and we do use that theorem in a few places in this paper. However, for the most part, the results about Chevalley groups do not depend on the classification. In particular, one can give a proof of the minimal genus result for Chevalley groups without reference to the classification.

The author wishes to thank MSRI for its generous hospitality. Much of this work was done while the author was a Research Professor at MSRI during the Fall 1999 program on Galois groups and fundamental groups. He would also like to thank the referee for a careful reading of the manuscript.

2. The Riemann–Hurwitz Formula

Let G be a finite group and Ω a G-set of size n. If $I \leq G$, define $\mathrm{ind}(I) = \mathrm{ind}(I, \Omega) = n - \mathrm{orb}(I)$, where $\mathrm{orb}(I)$ is the number of orbits of I on Ω. Let $f(x) = f(x, \Omega)$ denote the size of the set of fixed points of $x \in G$.

It follows by a result of Burnside (or by Frobenius reciprocity) that

$$\operatorname{orb}(I) = |I|^{-1} \sum_{x \in I} f(x).$$

If $\mathcal{I}$ is a descending sequence of normal subgroups of $I = I_0 \geq I_1 \geq I_2 \geq \ldots \geq I_m$, define

$$\rho(\mathcal{I}, \Omega) = \sum_{i=0} [I : I_i]^{-1} \operatorname{ind}(I_i).$$

We will often abuse notation and write $\rho(I)$ for $\rho(\mathcal{I}, \Omega)$. This notation will be used in the case that I is the inertia group of a point on a curve and $\mathcal{I}$ is the sequence of higher ramification groups.

We can now express the Riemann–Hurwitz formula in group theoretic notation.

Let k be an algebraically closed field of characteristic $p \geq 0$ and X, Y smooth projective curves over k with the genus of X, $g(X) = g$ and $g(Y) = h$. Let $f : X \to Y$ be a separable nonconstant rational map of degree n. Let Z denote the curve corresponding to the Galois closure and G the monodromy group of the cover.

Let $B \subset Y$ denote the (finite) set of branch points of the cover. If $y \in B$, let $I = I(y)$ denote the inertia group of some point in Z over y and let $I_i(y)$ denote the ith higher ramification group. See [61] for details about higher ramification groups. The Riemann–Hurwitz formula can now be stated:

THEOREM 2.1.

$$2(g-1) = 2n(h-1) + \sum_{y \in B} \rho(I(y)).$$

In particular, we record:

COROLLARY 2.2. *If $h > 1$, then $n \leq (g-1)/(h-1) \leq (g-1)$.*

Thus, for a fixed g, given n and $h > 1$, there are only finitely many possibilities for G.

If $h = 1$, we have a similar result. This is stated in [32] for characteristic 0; however the proof is identical using the Riemann–Hurwitz formula. For the second corollary, just note that $\operatorname{ind}(I) \geq n/2$ for any nontrivial I in the regular representation.

COROLLARY 2.3. *If the cover $f : X \to Y$ is indecomposable of degree n and $h = 1$, then one of the following holds*:

(i) *n is prime, G is cyclic of order n, $g = 1$ and the cover is unramified.*
(ii) *$G \cong A_n$ or S_n.*
(iii) *$2(g-1) \geq \sqrt{n} - 1$.*

COROLLARY 2.4. *If the cover $f : X \to Y$ is Galois and $h = 1$, then one of the following holds*:

(i) *G is abelian and the cover is unramified.*
(ii) $2(g-1) \geq n/2$.

So the critical case is when $h = 0$.

Also, note that the each of the groups $I(y)$ has a normal Sylow p-subgroup, $I_1(y)$, and that $I(y)/I_1(y)$ is a cyclic p'-group.

Let N denote the normal subgroup of G generated by the subgroups $I_1(y), y \in B$. Then G/N is a p'-group and is the monodromy group of the cover $Z \to Z/N$. Moreover G/N generated by the images of the $I(y)$ and choosing appropriate generators for the (cyclic) images of the $I(y)$, the product of these generators is 1—i.e. we have the description of the monodromy group G/N as in characteristic zero.

3. The Tate Module

Let Z be a smooth projective curve of genus g over an algebraically closed field k of characteristic $p \geq 0$. Let $J = J(Z)$ be the Jacobian of Z. So J is the set of formal finite sums of points of Z with weight zero modulo those elements which correspond to divisors of functions on Z.

If m is a positive integer, let $J[m]$ denote the m-torsion points on J. If ℓ is a prime, let $T_\ell(Z)$ denote the inverse limit of $J[\ell^a]$. So this is a $\mathbb{Z}_\ell$-module and of course, $\mathrm{Aut}(Z)$ acts on this module as well. Let $T'_\ell(Z) = T_\ell(Z) \otimes \mathbb{Q}_\ell$.

The following result is classical.

LEMMA 3.1. *Let H be a finite subgroup of $\mathrm{Aut}(Z)$. Let $V = T'_\ell$ for any $\ell \neq p$. Then $2g(Z/H) = \dim C_V(H)$. If $p \neq \ell$ and ℓ does not divide the order of H, then $2g(Z/H) = \dim C_{J[\ell]}(H)$.*

PROOF. The Jacobian is a g-dimensional abelian variety. Thus, for any m not divisible by p, $J[m]$ has order m^{2g}. Let $d = |H|$ and $f : Z \to Z/H$ the covering map of degree d. Let f_* denote the induced map from $J(Z) \to J(Z/H)$. If $y \in Z/H$, let $f^*(y) = n_y \sum z$, where the sum runs over x with $f(z) = y$ and n_y is the order of the inertia group of any such z (note this is independent of z). Then f_* induces a map from $J(Z/H) \to Y$. In particular, note that the image of f^* is contained in $J(Z)^H$. It follows immediately from the definitions that $f^* f_*(D) = dD$ for element $D \in J(Z)^H$ and similarly that $f_* f^*(D) = dD$ for element $D \in J(Z/H)$. In particular, this shows that $T'_\ell(Z)^H \cong T'_\ell(Z/H)$ for all $\ell \neq p$.

If ℓ does not divide the order of H, then the fixed points on the Tate module have the same dimension as the fixed on points on the ℓ-torsion subgroup of the Jacobian. □

We could replace V by the ℓ-torsion subgroup for some ℓ not dividing $|H|$. We remark that it is well known that the Tate module is really independent of ℓ. Also if ℓ does not divide the order of H and the genus is at least 2, then H acts faithfully on the ℓ-torsion subgroup.

The case $\ell = p$ is also interesting but in fact in that case V can be 0 (and in general $0 \leq \dim V \leq g(Z)$).

If $p = 0$, we could also use the module of holomorphic differentials on Z and remove the 2 in the formula.

We point out an interesting consequence. If H is a subgroup of G, let 1_H^G denote the permutation module for G over $\mathbb{C}$.

COROLLARY 3.2. *Let Z be a curve over k with G a finite group of automorphisms of Z. Suppose that H and K are subgroups of G such that 1_H^G is isomorphic to a submodule of 1_K^G. Then $g(Z/H) \leq g(Z/K)$.*

PROOF. Let V denote the Tate module for some sufficiently large prime ℓ other than the characteristic of the curve. By Frobenius reciprocity, $\dim C_V(H) = \dim \mathrm{Hom}_G(1_H^G, V)$ and $\dim C_V(K) = \dim \mathrm{Hom}_G(1_K^G, V)$. Since 1_H^G is a direct summand of 1_K^G, $\dim \mathrm{Hom}_G(1_H^G, V) \leq \dim \mathrm{Hom}_G(1_K^G, V)$, whence the result. □

Here are some well known situations where the previous result applies.

(i) $G = S_n$ or A_n. Let H be the stabilizer of a subset of size j and K the stabilizer of a set of size j' with $1 \leq j \leq j' \leq n/2$.
(ii) $PSL(n,q) \leq G \leq P\Gamma L(n,q)$. Let H be the stabilizer of a subspace of dimension j and K the stabilizer of the a subspace of dimension j' with $1 \leq j \leq j' \leq n/2$.
(iii) G is a classical group and H is the stabilizer of a totally singular 1-space. Then we can take K to be the stabilizer of any totally singular space of less than maximal rank or usually the stabilizer of a nonsingular space as well. See [19] for a precise statement.

We now prove some easy representation theoretic facts that will be useful in estimating genera.

LEMMA 3.3. *Let G be a finite group with a normal subgroup E. Let H be a maximal subgroup of G which does not contain any normal subgroup of G contained in E. Assume that $E = X_1 \times \ldots \times X_t$ with the $X_i = X^{g_i}$ being the set of G-conjugates of $X := X_1$. Set $Y = X_2 \times \ldots \times X_t$. Let $N = N_G(X) = N_G(Y)$. If V is a finite dimensional $\mathbb{C}G$-module, then* $\dim C_V(H) \geq \dim C_V(N_H(X)Y) - \dim C_V(N_G(X))$.

PROOF. Since both sides of the inequality we are proving are additive over direct sums and since V is a completely reducible $\mathbb{C}G$-module, it suffices to prove the result for V irreducible. If V is trivial, there is nothing to prove. Suppose that E does not act faithfully on V. Let K denote the kernel of E on V. Since H is maximal and does not contain K, $G = HK$ and $N_G(X) = N_H(X)K$ and similarly for Y. In this case $0 = C_V(G) = C_V(HK) = C_V(H)$ and $C_V(N_G(X)) = C_V(N_H(X))$ whence we have equality.

So we may assume that E acts faithfully on V. Note that since $N_G(X) \geq E$, $C_V(N_G(X)) = 0$.

We may assume that $C_V(Y) = W$ is nonzero (or the result obviously holds). Let $Y_i = Y^{g_i}$. Note that $\sum_i C_V(Y_i)$ is a direct sum (for if $\sum v_i = 0$ with $0 \neq v_1$ and $v_i \in C_V(Y_i)$, then $v_1 \in C_V(Y) \cap \bigcap_{i>1} C_V(Y_i) = C_V(Y) \cap C_V(X) = C_V(E) = 0$).

Now $N_G(X)$ leaves W invariant (since $N_G(X)$ normalizes Y). As we have seen above the distinct images of W under G form a direct sum Also the stabilizer of W is $N_G(X)$ (for if $gW = W$ and g is not in $N_G(X)$, then $\langle Y, Y^g \rangle = E$ would imply that $W = C_V(E) = 0$). It follows that $V \cong W^G_{N_G(X)}$ and so $V \cong W^H_{N_H(X)}$ as H-modules (since as noted $G = HN_G(X)$). So by Frobenius reciprocity, $C_V(H) \cong C_W(N_H(X)) = C_V(N_H(X)Y)$. □

The following variant of the previous result will also be useful.

LEMMA 3.4. *Let G be a finite group with a normal subgroup E. Let H be a maximal subgroup of G which does not contain any normal subgroup of G contained in E. Assume that $E = X_1 \times \ldots \times X_t$ with the $X_i = X^{g_i}$ being the set of G-conjugates of $X := X_1$. Let $\Delta = \{1, \ldots, t\}$. Let $\delta \subset \Delta$ and set $X_\delta = \prod_{i \in \delta} X_i$. Let $Y_\delta = X_{\delta'}$ where δ' is the complement of δ. Let $N_\delta = N_G(X_\delta)$. Let V be an irreducible $\mathbb{C}G$-module containing an E-submodule W of the form $W_1 \otimes \ldots \otimes W_t$ with W_i an irreducible X_i module with W_j trivial if and only if $j \in \delta'$. Then* $\dim C_V(H) \geq \dim C_V(N_H(X_\delta)Y_\delta) - \dim C_V(N_G(X_\delta))$.

PROOF. Note that $N_H(X_\delta)Y_\delta \leq N_G(X_\delta)$ and so each term on the righthand side of our desired inequality is non-negative.

First suppose that E does not act faithfully on V. Let K denote the kernel of E on V. Since K is normal in G, $G = KH$. Then $C_V(H) = C_V(HK) = C_V(G)$. If G acts trivially, then the lefthand side is 1 and the righthand side is 0.

Otherwise, the lefthand side is 0. Since $G = HK$, $N_G(X_\delta) = KN_H(X_\delta)$, whence the righthand side is also 0.

So we may assume that E acts faithfully on V. If $W = V$, Y_δ has no fixed points on V for δ any proper subset of Δ (for Y_δ contains some X_j and V restricted to X_j is a direct sum of copies of V_j). Thus, the righthand side of the equation is 0.

Let $U := U_\delta = C_V(Y_\delta)$. So $W \subseteq U$. By irreducibility, $V = \sum U_\gamma$ where γ is the orbit of δ. Note that this sum is in fact direct, since the terms are direct sums of irreducible E-modules which are not isomorphic (as they have different kernels). Moreover, the stabilizer in G of U_δ is precisely $N_G(X_\delta)$ (because of the permutation action on the X_i). Thus, V is isomorphic to the induced module, $U^G_{N_G(X_\delta)}$. Since $G = N_G(X_\delta)H$, this implies that $V_H \cong U^H_{N_H(X_\delta)}$ and so by Frobenius reciprocity, $\dim C_V(H) = \dim C_U(N_H(X_\delta))$. Since $U = C_V(Y_\delta)$, it follows tht $C_V(N_H(X_\delta))(Y_\delta) = C_U(N_H(X_\delta))$, whence the result. □

We next deal with diagonal subgroups (see section 11 for terminology). The result is actually more general than we state — the condition that X is simple is not necessary.

LEMMA 3.5. *Let G be a finite group with a minimal normal subgroup $E = X_1 \times \ldots \times X_t$ with the X_i the set of G-conjugates of the nonabelian simple group $X = X_1$ and $t > 1$. Let H be a maximal subgroup of G not containing E such that $H \cap E$ is a diagonal subgroup of E. Let $\Delta = \{1, \ldots, t\}$. If $\delta \subset \Delta$, set $X_\delta = \prod_{i \in \delta} X_i$. Let $Y_\delta = X_{\delta'}$ where δ' is the complement of δ. Let $N_\delta = N_G(X_\delta)$. If V is a finite dimensional $\mathbb{C}G$-module, then* $\dim C_V(H) \geq \dim C_V(N_H(X_{12})Y_{12}) - \dim C_V(N_G(X_{12}))$.

PROOF. It suffices to assume that V is irreducible. Note that the righthand side is always non-negative (since $N_G(X_{12}) \geq N_H(X_{12})Y_{12}$).

If V is a trivial G-module, there is nothing to prove.

If E acts trivially on V, then $C_V(H) = C_V(HE) = 0$. On the other hand, since $G = HE$, we have $N_G(X_{12}) = EN_H(X_{12})$ and so $C_V(N_H(X_{12})Y_{12}) = C_V(N_G(X_{12}))$.

So assume that E acts nontrivially on V. In particular, this implies that $C_V(N_G(X_{12})) = 0$. If Y_{12} has no fixed points on V, then clearly the result holds (since the right hand side of the inequality is 0).

Suppose first that $C_V(Y_1)$ is nonzero. Then as in the previous result, V is the direct sum of the $C_V(Y_i) = [X_i, V]$. Since $H \cap E$ is a diagonal subgroup, this implies that $(H \cap E)Y_i \geq E$ and so $H \cap E$ has no fixed points on $[X_i, V]$ and so none on V. Since $H \cap E \leq N_H(X_{12})$, the right hand side is 0, whence the result.

Finally, assume that $W := C_V(Y_{12}) \neq 0$, but $C_V(Y_1) = 0$. This implies that every irreducible E-submodule of V is of the form $U_1 \otimes \ldots \otimes U_t$ with U_i an irreducible X_i-module with U_i nontrivial for precisely 2 terms. In particular, it follows that W is a sum of E-homogeneous components. Let $W_{ij} = C_V(Y_{ij})$. Since W_{ij} is also a sum of E-homogeneous components and there are no common irreducibles among the distinct W_{ij}, it follows that $V = \oplus W_{ij}$ and the nontrivial W_{ij} must be a single G-orbit. Clearly, W is invariant under $N_G(X_{12})$ and indeed, we see that this is the full stabilizer of W. Since $G = HE = HN_G(X_{12})$, H acts transitively on the W_{ij} as well. Thus, $V \cong W^H_{N_H(X_{12})}$ and so by Frobenius reciprocity, $C_V(H) = C_W(N_H(X_{12})) = C_V(N_H(X_{12})Y_{12})$. □

The next lemma gives a bound in certain additional cases.

LEMMA 3.6. *Let A be a finite group and G a normal subgroup. Let $M = N_A(M)$ be a maximal subgroup of A such that $M \cap G$ is properly contained in the maximal subgroup J of G. Assume moreover that the intersection of any proper subset of M-conjugates of J properly contains $M \cap G$. Let V be an irreducible $\mathbb{C}A$-module. Then either G acts trivially on V or* $\dim C_V(J) \leq \dim C_V(M)$.

PROOF. Since M does not contain G, it follows that $A = GM$. Let $W = C_V(J)$. Choose a transversal $1 = x_1, \ldots x_t$ in M for A/G. We claim that $\sum x_i W$ is a direct sum. If not, then there exists a nonzero vector $v \in W$ with $v \in \sum_{I>1} x_i W$. Thus, $v \in C_V(J) \cap C_V\left(\bigcap_{i>1} J^{x_i}\right)$. By assumption, $\bigcap_{i>1} J^{x_i}$ is not contained in

J and so $G = \langle J, \bigcap_{i>1} J^{x_i} \rangle$. Hence $v \in C_V(G) = 0$. Thus, the map $w \mapsto \sum x_i w$ is an injection from W to $C_V(M)$. □

Note that if $M \cap G$ is not maximal in G and J is a maximal self-normalizing subgroup of G containing $M \cap G$ and A/G has order 2, the hypotheses are always satisfied.

4. Upper Bounds for Genus

The first result is classical. Let k be an algebraically closed field of characteristic $p \geq 0$. All covers refer to curves over k.

LEMMA 4.1. *There exist covers $f : \mathbb{P}^1 \to \mathbb{P}^1$ of degree n with monodromy group S_n.*

PROOF. Let $f(x) = x^2 h(x)$, where h is a polynomial of degree $n-2$ with distinct nonzero roots. Choose h in addition so that f is separable and indecomposable (these are both open conditions on the coefficients of h). Then the monodromy group is a primitive group of degree n containing a transposition (consider the inertia group over 0). It is elementary to prove that a primitive permutation group of degree n containing a transposition is S_n. □

LEMMA 4.2. *Let S be a nonabelian simple group and let n be the minimal index of a maximal subgroup of S. Then there exists a cover $f : X \to \mathbb{P}^1$ of degree n with X of genus $n+1$. In particular, $\mu(S) \leq n+1$.*

PROOF. By [63], there exists an unramified S-cover of a genus 2 curve Y. Thus, there exists a degree n cover X of Y with monodromy group S. By the Riemann–Hurwitz formula, X has genus $n+1$. □

With some effort, one should be able show that $\mu(S) < n/2$ at least for $p \neq 2$. One would need a slight generalization of a the generation result from [29] given below — something like given $1 \neq x \in S$, there exists $y \in S$ with $S = \langle x, y \rangle$ such that y and xy have order prime to p. If $p \neq 2$, this would give $\mu(S) \leq (n-1)/2$ and a slightly weaker bound for $p = 2$.

We give the proof of a slightly better result in characteristic zero only. One can do a bit better for most simple groups because they can be generated by elements of order 2 and 3, we can require in this case that (in characteristic 0) X has genus at most $n/6 + 1$ (and asymptotically for many families that is the best that can be done).

LEMMA 4.3. *Let G be an almost simple group with socle S acting faithfully on a set of cardinality m. If x is a nontrivial element of G, then there exists a Riemann surface X and $f : X \to \mathbb{P}^1$ of degree at most m with X of genus $g \leq \mathrm{ind}(x)/2$ and monodromy group G_0 with $S \leq G_0 \leq G$. In particular, if n is the minimal degree of a permutation representation of S, then there exists a Riemann surface $f : X \to \mathbb{P}^1$ of degree m with X of genus $g \leq n/4$.*

PROOF. By [29], there exists an element $y \in G$ so that $G_0 := \langle x, y\rangle \geq S$. By passing to a G_0-orbit if necessary we may assume that $G = G_0$. By Riemann's existence theorem, there exists a 3 branch point cover $f : X \to \mathbb{P}^1$ with inertia groups generated by x, y and $z := (xy)^{-1}$. Since $\mathrm{ind}(y), \mathrm{ind}(z) < m$, it follows that $g(X) \leq \mathrm{ind}(x)/2$.

Apply this result to the case that $G = S$ and x is an involution to obtain the last statement. □

LEMMA 4.4. [40] *If $f : X \to Y$ is a branched covering and $f = f_1 \circ f_2$, then any composition factor of the monodromy group of f is a composition factor of the monodromy group of f_i for $i = 1$ or 2.*

We will need the following result about minimal permutation representations of a groups with a given composition factor.

LEMMA 4.5. *Let S be a nonabelian simple group. Let n be the smallest cardinality of a faithful G-set for any group G with S as a composition factor of G. Then $F^*(G) = S$ and n is the index of the largest proper subgroup of S.*

PROOF. Let Ω be the given G-set of size n. Note first that G is transitive (for otherwise S is a composition factor in G/K or K where K is the subgroup acting trivially on some G-orbit and either group acts faithfully on a smaller G-set). We claim also that G is primitive on Ω. Otherwise, S is a composition factor of the stabilizer of a block or a composition factor of G acting on the blocks. In either case, we would have a smaller action with S as a composition factor.

Let H be a point stabilizer. If G has a normal abelian subgroup or 2 minimal normal subgroups, then H has a smaller faithful orbit and has S as a composition factor. So let L be a simple component of G and let $L_i, 1 \leq i \leq t$ be the G-conjugates of L. Thus, G has a unique minimal normal subgroup.

Suppose that S is not a component of G. Then S embeds in G/K where K is the subgroup normalizing each L_i. Thus, $t \geq n$, but (cf. section 11), $n \geq 5^t$, a contradiction.

So S is a component of G and G has a unique minimal normal subgroup. Let m be the index of the largest proper subgroup of S. By section 11, one of the following holds: $n \geq m^t$ or $n \geq |S| > m$. Thus, $t = 1$ (as claimed). □

It is convenient to define $\mathrm{md}(S)$ to be the smallest index of a proper subgroup of S. We remark that $\mathrm{md}(S)$ is known for all S — cf [45].

LEMMA 4.6. *Let $f : X \to Y$ be a branched covering of degree n with S a nonabelian composition factor of the monodromy group G of f. Assume that Y has genus at least 1.*

(i) *If Y has genus at least 2, then $g(X) - 1 \geq n \geq \mathrm{md}(S)$;*
(ii) *If S is not an alternating group, then $g(X) - 1 > n/12 \geq \mathrm{md}(S)/12$.*

PROOF. By Lemma 4.4, we may assume that f is indecomposable. Let $h = g(Y)$. If $h > 1$, then the Riemann–Hurwitz formula yields $g - 1 \geq n(h-1) \geq n$. By the previous lemma, $n \geq \mathrm{md}(S)$.

Suppose that $h = 1$. Since S is nonabelian, the cover must be ramified. Then the Riemann–Hurwitz formula yields that $g - 1 \geq (1/2)\rho(J)$ where J is a nontrivial inertia group. Clearly, $\rho(J) \geq \mathrm{ind}(J)$ and so by [49], $\mathrm{ind}(J) \geq n/6$ whence the second statement. □

5. Regular Normal Subgroups

In this section, we show that the affine case can be reduced to the other cases. We first prove two general results.

LEMMA 5.1. *If G is a finite primitive permutation group with point stabilizer H and N is a regular normal subgroup, then $H \cap H^g$ contains no nontrivial normal subgroup of H for g any nontrivial element of $G \setminus N$.*

PROOF. Let K be a nontrivial normal subgroup of H in $H \cap H^g$. Since $G = HN$, we may assume that $g \in N$. Then $H \cap H^g = C_H(g)$ and so $N_G(K) \geq \langle H, g\rangle = G$ (by the maximality of H). This contradicts the fact that H contains no nontrivial normal subgroup of G. □

LEMMA 5.2. *Let H be a group of automorphisms of a finite group N which is transitive on the set of all nontrivial elements of N. If H is not solvable, then H contains a normal cyclic subgroup C with $F^*(H/C)$ simple.*

PROOF. N is characteristically simple and must have all elements of the same order, whence N is an elementary abelian p-group for some prime p. The result follows easily from Aschbacher's theorem on subgroups of classical groups (see the appendix). □

We now fix some notation. Fix a prime p. All curves will be smooth projective curves over an algebraically closed field of characteristic p. Let S be a finite nonabelian simple group. Fix a non-negative integer d. Let $\lambda(S,d)$ denote the smallest positive n such that there exists an indecomposable separable branched cover $f : X \to Y$ of degree n with monodromy group G such that S is a composition factor of G and X has genus at most d (if the characteristic is not clear, we write $\lambda_p(S,d)$).

Similarly, let $\lambda'(S,d)$ denote the smallest positive n' such that there exists an indecomposable separable branched cover of degree $f : X \to Y$ of degree n with monodromy group G such that S is a component of G and X has genus at most d.

Let $\lambda''(S,d)$ denote the smallest positive n such that there exists an indecomposable separable branched cover $f : X \to Y$ of degree n with monodromy group G such that $F(G) = 1$, X has genus at most d and S is a composition factor of G.

In particular, to say that any of these quantities is finite is to say that such covers exist.

THEOREM 5.3. *Let $f : X \to Y$ be an indecomposable separable nonconstant map of degree $n = \lambda(S, d)$ with X of genus $g \leq d$. Assume that S is a nonabelian composition factor of the monodromy group G of f. Assume that G contains a regular normal abelian subgroup N. Then Y has genus zero and one of the following holds*:

(i) $g = 0$ *and* $\lambda'(S, 2) < n$;
(ii) $g = 0$ *and* $\lambda''(S, 1) < n$;
(iii) $g = d$, G *acts transitively on the nontrivial elements of* N *via conjugation and* $\lambda'(S, d + 1) < \lambda(S, d)$.

PROOF. Let Ω denote the G-set of degree n corresponding to the cover. Let H be the stabilizer of a point ω and let Ω_i be the nontrivial H-orbits on Ω. Let H_i be the stabilizer of a point in Ω_i. Identifying H with G/N, we may identify Ω_i with the G-set G/NH_i.

Let Z denote the Galois closure of X/Y and consider the curves $X_i := Z/NH_i$ and let g_i denote the genus of X_i.

If $x \in G$, then write $x = yz$ with $y \in H$ and $z \in N$. Let $\mathrm{fix}(x, \Omega)$ denote the cardinality of the set of fixed points of x on Ω. We note that $\mathrm{fix}(x, \Omega) \leq 1 + \sum \mathrm{fix}(y, \Omega_i)$. For if x is conjugate to y, this is clear while if x is not conjugate to y, then $\mathrm{fix}(x, \Omega) = 0$.

Then $\mathrm{ind}(J, \Omega_i) = \mathrm{ind}(JN/N, \Omega_i)$. The previous paragraph shows that for any subgroup J of G, $\mathrm{ind}(J, \Omega) \leq 1 + \sum_i \mathrm{ind}(J, \Omega_i)$.

Let h denote the genus of Y. Now applying the Riemann–Hurwitz formula to the curves X and X_i, we obtain:

$$2(g-1) = 2n(h-1) + \sum_J \rho(J, \Omega) \geq 2n(h-1) + \sum_{J,i} \rho(J, \Omega_i).$$

Here the sum is over the inertia groups (and higher ramification groups) J of the cover $X \to Y$.

Now

$$2(g_i - 1) = 2n_i(h-1) + \sum_J \rho(J, \Omega_i),$$

and so since $n = 1 + \sum n_i$,

$$(g-1) \geq (h-1) + \sum (g_i - 1).$$

Note that the monodromy group of the cover of $X_i \to Y$ is $G/N \cong H$ (by Lemma 5.1). By minimality, it follows that $g_i > d \geq g$ for each i and so $h = 0$.

This implies that either $g = 0$ and each $g_i = 1$ or H has only one nontrivial orbit on Ω in which case $g = g_1 - 1 \geq d$ and so $g = d$.

Suppose that the second case occurs and $g \neq 0$. Now apply Lemma 5.2 to conclude that (3) holds.

Now suppose the first case holds. So $g = 0$. Now start over and choose an indecomposable cover $\phi : W \to \mathbb{P}^1$ of degree m with W of genus 1 and m minimal with S as a composition factor. Note that $m < n$. So this gives a primitive permutation group. If this group has a normal elementary abelian group, then we repeat the argument and obtain a cover as in the second case (with the genus at most 2) and so $\lambda'(S, 2) < n$. If not, then we conclude that $\lambda''(S, 1) < n$. □

LEMMA 5.4. *Let $f : X \to Y$ be an indecomposable separable nonconstant map of degree $n = \lambda''(S, d)$ with X of genus $g \leq d$. Assume that S is a nonabelian composition factor of the monodromy group G of f. Then G has a unique minimal normal subgroup or $d = 0$ and $\lambda''(S, 1) < \lambda''(S, 0)$.*

PROOF. Assume that G has more than one minimal normal subgroup. Let Ω be the G-set of size n associated with the cover. Let H be a point stabilizer. Let N be a minimal normal subgroup of G. Since there are 2 minimal normal subgroups of G, N is a regular normal nonabelian subgroup. So $G = HN$ is a semidirect product.

Define the curves X_i as in the previous proof. Arguing precisely as above, we have the same possibilities (and note that S is a composition factor of G/N and G/N has no normal abelian subgroups). In this case, H has more than one orbit on the nontrivial elements of N, eliminating that possibility. So it follows that $g = 0$ and $g_i = 1$ for each i. □

We note that for most S, the situations in the lemma cannot occur. For example, if $S = A_m, m \geq 5$, then there is a degree m cover from $\mathbb{P}^1$ to $\mathbb{P}^1$ and so $\lambda(S, d) = \lambda'(S, d) = \lambda''(S, d) = m$.

6. Minimal Genus for Composition Factors

Let S be a finite nonabelian simple group. As in the previous section, all curves considered are over an algebraically closed field of characteristic p. Let $\mu'_p(S) = \mu'(S)$ denote the minimal genus g of a curve X so that there exists a cover $f : X \to Y$ with f indecomposable and S is a component of the monodromy group of f.

Let $\mu''(S)$ denote the minimal genus g of a cover $f : X \to Y$ with f indecomposable such that the monodromy group has no normal abelian subgroup and S is a composition factor. Clearly, we have:

LEMMA 6.1. $\mu(S) \leq \mu''(S) \leq \mu'(S)$.

We rephrase Theorem 5.3 in this notation.

LEMMA 6.2. *Assume that $\mu(S) < \mu''(S)$. Then one of the following holds*:

(i) $\mu(S) = 0$ *and* $\mu'(S) \leq 2$;
(ii) $\mu(S) = 0$ *and* $\mu''(S) = 1$;
(iii) $\mu(S) > 0$, *and* $\mu'(S) = \mu(S) + 1$.

PROPOSITION 6.3. $\mu''(S) = \mu'(S)$ *or* $\mu'(S) \leq 2$.

PROOF. Let $f : X \to Y$ be a separable branched covering of degree $n = \lambda''(S, g)$ with X of genus $g = \mu''(S)$, S a composition factor of the monodromy group G of the cover. We may assume that G has no normal abelian subgroup and that $\mu'(S) > 2$.

Let Z denote the curve corresponding to the Galois closure. Let H be the subgroup with $X = Z/H$. If S is a component of G, $\mu''(S) = \mu'(S)$. So assume that this is not the case. It follows that S is a composition factor of $G/F^*(G)$.

Since G has no normal abelian subgroup, we can write $E = F^*(G)$ as a direct product of conjugates of a subgroup J. Let J' be the direct product of all the other distinct conjugates of J.

Let V denote a the complexification of a Tate module for Z. By Lemmas 3.3 and 3.4, $\dim C_V(H) \geq \dim C_V(N_H(J)J') - \dim C_V(N_G(J))$.

Note that S is a composition factor of the monodromy group of the cover $Z/N_G(J) \to Y$. It follows that $Z/N_G(J)$ has genus g' which is at least $\mu(S)$.

First suppose that $g' > 1$. Then the genus of $Z/(N_H(J)J')$ is at least $5(g' - 1) + 1$ (by the Riemann–Hurwitz formula and the fact that the degree of $Z/(N_H(J)J') \to Z/N_G(J)$ is at least 5). Hence $2g = \dim C_V(H) \geq 8(g' - 1)$.

Thus, $g = \mu''(S) \geq 4(g' - 1) \geq 4(\mu(S) - 1)$. Thus $\mu''(S) > \mu(S)$ and so the previous lemma applies. If $\mu(S) = 0$, then $\mu''(S) \leq 2$, contradicting the fact that $g \geq 4(g' - 1) \geq 4$. Otherwise, $\mu''(S) \leq \mu(S) + 1$ and so $\mu(S) + 1 \geq 4(\mu(S) - 1)$, whence $\mu(S) = 1$ and $g = \mu''(S) \leq 2$, contradicting the fact that $g \geq 4$.

Next consider the case that $g' \leq 1$. If $g' = 1$, since $Z/(N_H(X)Y) \to Z/N_G(X)$ is not an abelian, $Z/(N_H(J)J')$ has genus $g'' \geq 2$. Again, by Lemmas 3.3 and 3.4, $g \geq g'' - 1 \geq 1$.

It follows that $\mu(S) < \mu''(S)$ and $\lambda(S, \mu(S)) < \lambda''(S, \mu''(S))$ (because there is a smaller degree cover which yields a cover with composition factor S and genus no larger than g). Thus, the minimal degree cover achieving $\mu(S)$ must have an abelian normal subgroup. It follows by the proof of Theorem 5.3 that $\lambda''(S, \mu(S) + 1) < \lambda(S, \mu(S))$ or $\mu'(S) \leq 2$.

The first condition does not hold by the inequality at the start of the paragraph and the second does not hold by assumption. This completes the proof. □

COROLLARY 6.4. *Either* $\mu(S) \leq \mu'(S) \leq 2$ *or* $\mu'(S) \leq \mu(S) + 1$.

PROOF. Assume $\mu'(S) > 2$. Then $\mu'(S) = \mu''(S)$. By Lemma 6.2 $\mu''(S) \leq \mu(S) + 1$. □

The previous result allows us to concentrate on computing $\mu'(S)$—i.e. a lower bound for $\mu'(S)$ is very close to the lower bound for $\mu(S)$. The next result essentially reduces this to the almost simple case.

THEOREM 6.5. *Let $f : X \to Y$ be an indecomposable degree n cover with monodromy group G with S a component of G. Assume that X has genus $g = \mu'(S)$. Moreover, assume that n is minimal with respect to these conditions. Then one of the following holds*:

(i) $F^*(G) = S$; *or*
(ii) $F^*(G) = S \times S$ *and* $H \cap F^*(G)$ *is a diagonal subgroup of* $F^*(G)$; *or*
(iii) $\mu'(S) \geq \mathrm{md}(S)/12 + 1$.

PROOF. Let $E = F^*(G)$. Let Z be the curve corresponding to the Galois closure of the cover. Let H be the subgroup of G of index n with $X = Z/H$.

Suppose that we can write $E = A_1 \times \ldots \times A_t$, where the A_i are all the conjugates of $A = A_1 \cong S^m$, $H \cap E$ is the direct product of the subgroups $H \cap A_i$ and $N_H(A)C(A)$ does not contain A. By Lemmas 3.3 and 3.4, $g \geq g(Z/(N_H(A)C(A)) - g(Z/N_G(A))$. If $h := g(X/N_G(A)) \geq 2$, then by the Riemann–Hurwitz formula, $g(Z/(N_H(A)C(A)) - 1 \geq \mathrm{md}(S)(h-1)$ and so $g \geq (\mathrm{md}(S) - 1)(h-1) \geq (\mathrm{md}(S) - 1)$.

If $h = 1$, then the same argument (together with Lemma 2.3 and the fact that we may assume that S is not an alternating group), implies that $g \geq \mathrm{md}(S)/12 + 1$.

So we may assume that $h = 0$ and so $g \geq g(Z/(N_H(A)C(A))$. Note that the monodromy group of the cover $Z/(N_H(A)C(A)) \to Z/N_G(A)$ is $N_G(A)/C_G(A)$ and so has S has a composition factor (since $C(A)N_H(A)$ does not contain A). Thus, by minimality, $A = E$. So we cannot decompose E in such a manner.

By the Aschbacher–O'Nan–Scott Theorem, this implies that either $F^*(G) = S$ or E is the unique minimal normal subgroup of G and $H \cap E$ is a full diagonal subgroup of E.

In the latter case, we apply Lemma 3.5. Arguing exactly as above, by minimality, we see that $F^*(G) = S \times S$. □

Putting together the previous results, we obtain:

THEOREM 6.6. *Let S be a nonabelian simple group. If $\mu'(S) < (\mathrm{md}(S))/12 + 1$, then there exists an indecomposable cover $f : X \to \mathbb{P}^1$ with X of genus g and with S a composition factor of the monodromy group J of f such that $g \leq \mu(S) + 1$ or $g = 2$ and one of the following holds*:

(i) $F^*(J) = S$; *or*
(ii) $F^*(J) = S \times S$ *and* $H \cap F^*(J)$ *is a full diagonal subgroup of* $F^*(J)$.

If p is a prime that does not divide the order of $\mathrm{Aut}(S)$, the previous theorem essentially asserts that the minimal genus of any group involving S does not have order divisible by p, whence we can apply the results about tame covers and so we obtain the following result. Note this says nothing about characteristic 2.

THEOREM 6.7. *Let S be a nonabelian simple group. If p does not divide the order of* $\mathrm{Aut}(S)$, *then one of the following holds*:

(i) $\mu_p(S) \geq \mathrm{md}(S)/12 + 1$; *or*
(ii) $\mu_0(S) \leq 2$; *or*
(iii) $\mu_p(S) = \mu^{\mathrm{ta}}(S)$.

We can extend this result to the case that p does not divide the order of S (rather than $\mathrm{Aut}(S)$) by observing if that holds, then the Sylow p-subgroup P of $\mathrm{Aut}(S)$ is cyclic and $\mathrm{Aut}(S) = PG_0$ with G_0 being a p'-group. An easy analysis of this situation together with the results of this section yield Theorem 1.4.

Since for any odd prime there are infinitely many simple groups not divisible by p (for $p > 3$, consider $L_2(r)$ with r prime and p not dividing $r(r^2 - 1)$; for $p = 3$, consider the Suzuki groups), we have the following corollary.

COROLLARY 6.8. *If p is an odd prime and g is fixed, then there are infinitely many simple groups with $\mu_p(S) > g$.*

We will obtain much more precise results in the next few sections including results that hold for $p = 2$.

7. Composition Factors of Genus g Covers

We will use Theorem 6.6 to show that there are many groups which are not composition factors of genus g in characteristic p.

If G is a finite group, define $\gamma(G) := \min\{g(X) - 1 | G \leq \mathrm{Aut}(X)\}$. Of course, $\gamma(G)$ depends on the characteristic (although if p does not divide the order of G, then by Grothendieck, the description of G-covers is independent of characteristic).

We need the following result. There should be a more conceptual proof but we use the classification of finite simple groups. If S is a finite simple group, let $\mathrm{fpr}(S)$ be minimum of $\mathrm{fix}(x, \Omega)/|\Omega|$ as where Ω is a faithful G-set for some group G with $F^*(G) = S$ and $1 \neq x \in G$.

LEMMA 7.1. *Let S be a finite simple nonabelian group. If $x \in \mathrm{Aut}(S)$, the number of elements y in the coset xS with $y^2 = 1$ is at most $|S| \mathrm{fpr}(S)$.*

PROOF. If S is alternating, this is clear (since $\mathrm{fpr}(S)$ is very close to 1). The result follows by inspection for the sporadic groups.

So assume that S is a Chevalley group. The number of involutions in S (or xS) is at most $|S|/d$ where d is the smallest degree of a nontrivial complex representation of S. These degrees are known (see [66] and [52]). If S is a classical group, then $\mathrm{fpr}(S)$ is approximately $1/q$ whence we are not even close. If S is an exceptional group, all conjugacy classes of involutions are known and we can get an exact formula for the number of involutions and again the result holds easily. □

THEOREM 7.2. *Let S be a finite nonabelian simple group. Then one of the following holds*:

(i) $\mu(S) \geq 1 + \mathrm{md}(S)/12$; *or*
(ii) $\mu(S) \geq -2\,\mathrm{md}(G)\,\mathrm{fpr}(G) + \mathrm{md}(G)(\gamma(G))/|G|)(1-\mathrm{fpr}(G))$ *for some group* G *with* $F^*(G) = S$.

Proof. We may assume that $\mu(S) < (\mathrm{md}(S)-1)/6$. Then by Theorem 6.6, there exists an indecomposable cover $f : X \to \mathbb{P}^1$ with X either of genus 2 or genus at most $\mu(S)+1$ such that the monodromy group G of the cover satisfies (1) or (2) of Theorem 6.6. Let n denote the degree of f.

Let Z denote the Galois closure of the cover and let H be such that $Z/H = X$. Let h denote the genus of Z.

Consider case (1) of 6.6 first.

Then $F^*(G) = S$ and $2 + (h-1)/|G| = \sum_J \rho(J,G)/|G|$ and $2 + (g-1)/n = \sum_J \rho(J,\Omega)/n$. Here the sum is over the inertia groups corresponding to branch points of the cover.

Now $\mathrm{ind}(J,\Omega)/n = 1 - |J|^{-1} - |J|^{-1}\sum_{g\in J^\#} f(g,\Omega))/n) \geq (1-|J|^{-1})(1-\mathrm{fpr}(G))$.

It follows that $\rho(J,\Omega)/n \geq (\rho(J,G)/|G|)(1-\mathrm{fpr}(G))$.

Thus, $(1-\mathrm{fpr}(G))[2 + (h-1)/|G|] \leq 2 + (g-1)/n$, or

$$g - 1 \geq -2n\,\mathrm{fpr}(G) + n(\gamma(G))/|G|)(1-\mathrm{fpr}(S)).$$

Since $n \geq \mathrm{md}(G)$ and $g \leq \mu(S)+1$ or $\mu(S) = 0$ and $g = 2$, the result follows in this case.

Consider case (2). So $n = |S|$. In this case $f(g,\Omega)/n \leq \mathrm{fpr}(S)$ (by the previous lemma and [6]). By Lemma 5.4, we may assume that G does not normalize either component. Precisely as above, it follows that

$$(1-\mathrm{fpr}(S))(h-1)/|G| \leq -2\,\mathrm{fpr}(S) + (g-1)/n.$$

Consider the curve Z/S where S is one of the components of G. Then $R := N_G(S)/S$ acts on this curve, whence it has genus at least $\gamma(R)$. Note that R is almost simple with socle S. Thus, $2(h-1) \geq 2|S|\gamma(R)$ and so

$$(1-\mathrm{fpr}(S))n\gamma(R)/|G| = (1-\mathrm{fpr}(S))\gamma(R)/|R| \leq -2\,\mathrm{fpr}(S) + (g-1)/n.$$

As above, this implies (ii) holds. □

We restate this:

Corollary 7.3. *Let* S *be a nonabelian finite simple group with* $n = \mathrm{md}(S)$. *Then* $(\mu(S)-1) \geq n/12$ *or* $\mu(S)/n \geq -2\,\mathrm{fpr}(G) + (\gamma(G))/|G|)(1-\mathrm{fpr}(G))$ *for some group* G *with* $F^*(G) = S$.

In particular, if $\mathrm{fpr}(G)$ is small and $\gamma(G)$ is large, then $\mu(S)$ is large. We shall apply this to Chevalley groups of characteristic different from p. Here $\mathrm{fpr}(G)$ is roughly $1/q$ and $\gamma(G)$ is a constant times $|G|\log(q)$ (where the constant depends only on the type of G).

8. Estimates on Inertia Groups

Let k be an algebraically closed field of characteristic p. Let $f : X \to Y$ be a Galois cover with Galois group G. Let I be the inertia group of a point of X and let I_i be the higher ramification groups. We write $I = I_1 D$ with D cyclic. Let $C = C_D(I_1)$ and set $r = |D : C|$ and $s = |C|$. In this section, we obtain estimates for $\rho(I)/|G|$. The permutation representation is the regular representation for G since we have a Galois cover. Restricting this representation to I gives $|G : I|$ copies of the regular representation. Thus, $\rho(I)/|G|$ is independent of G and can be computed by considering any such cover with the same I (and higher ramification groups).

In particular, we want to reduce to the case that $I = G$. This can be done in several ways. We could just replace G by I and consider the cover $X \to X/I$ (and so the point with inertia group I is totally ramified). Alternatively, by Katz–Gabber [46], there exists a Galois cover $\psi : L \to \mathbb{P}^1$ ramified at precisely 2 points with inertia groups I (and the same higher ramification groups) and D. Let $g(L)$ denote the genus of L. Thus, $2(g(L) - 1)/|I| + 2 = \rho(I)/|I| + (|D| - 1)/|D|$ or $\rho(I)/|I| = 1 + 2(g(L) - 1)/|I| - 1/|D|$.

For the remainder of this section, we assume that $G = I$; i.e. there is a totally ramified point.

LEMMA 8.1. *If $I_j \neq I_{j+1}$, then $j \equiv 0 \pmod{s}$.*

PROOF. We may assume $j > 0$. Choose an element $x \in I_j$ with x not in I_{j+1} and pass to the abelian subgroup $C \times \langle x \rangle$. Now apply Hasse–Arf [61]. □

LEMMA 8.2. $\rho(I)/|I| \geq 1 + 1/r - (s+1)/|I|$.

PROOF. By the previous result, $I_1 = \ldots = I_s$. Thus, $\rho(I)/|I| \geq 1 - 1/|I| + \sum_{i=1}^{s}(1/rs)(1 - 1/|I_i|)$, whence the result. □

Assume now that I_1 is abelian. We change our numbering scheme to keep track of distinct terms among the higher ramification subgroups and count multiplicities. Let $I_1 = J_1 > J_2 > \ldots > J_m = 1$ with the J_j being the *distinct* higher ramification groups. Let r_i denote the number of higher ramification groups equal to J_i. It follows from Hasse–Arf [61] that if $I_j \neq I_{j+1}$, then $|CI_1|$ divides $\sum_{i=1}^{j} |I_i|$ and in particular, r_{i+1} is a multiple of $|CI_1 : I_{i+1}|$.

Thus (recall our permutation representation is the regular representation)

$$\rho(I)/|I| = 1 - 1/|I| + |C|/|D| \sum_{i=1} \lambda_i (1 - 1/|J_i|),$$

where the λ_i are positive integers. In particular, we see that

$$\begin{aligned}\rho(I)/|I| &> 1 + |C|/|D| - 1/|I| - |C|/|D||I_1| \\ &\geq 1 + |C|/|D| - 1/|D||I_1| - |C|/|D||I_1| \\ &\geq 1 + |C|/2|D|,\end{aligned}$$

unless possibly $|I_1| = 2$ or $|I_1| = 3$ and $C = 1$.

If $|I_1| = 2$, then $C = D$. If $D = 1$, then $\rho(I)/|I|$ is a positive integer. If $D \neq 1$, then $|I| \geq 6$ and so $\rho(I)/|G| \geq 4/3$.

If $|I_1| = 3$ and $C = 1$, then either $D = 1 = I_2$ and $\rho(I)/|I| = 4/3$ or $\rho(I)/|I| \geq 1 + 1/|D| = 1 + |C|/|D|$. Summarizing we have the following:

LEMMA 8.3. *If I_1 is a nontrivial abelian group, then one of the following holds:*

(i) $\rho(I)/|I| \geq 1 + |C|/2|D|$;
(ii) $I = I_1$ *has order* 2, $I_2 = 1$ *and* $\rho(I)/|I| = 1$;
(iii) $|I_1| = 2$ *and* $\rho(I)/|I| \geq 4/3$; *or*
(iv) $I = I_1$ *has order* 3, $I_2 = 1$ *and* $\rho(I)/|I| = 4/3$.

Keep the assumption that I_1 is abelian. Set $\lambda = \sum \lambda_i$. Then

$$1 - 1/|I| + (|C|/|D|)(1 - 1/p)\lambda \leq \rho(I)/|I| < 1 - 1/|I| + |C|/|D|\lambda.$$

LEMMA 8.4. *Fix $r = |D/C|$. Assume that I_1 is abelian and $p > 3$.*

(i) *If $\lambda \geq 2|D|/|C|$, then $\rho(I)/|I| \geq 12/5$;*
(ii) *If p is sufficiently large, then $\rho(I)/|I| > 1 + 1/3r$;*
(iii) *Let $d > 1$ be a positive integer with $\rho(I)/|I| > 1 + 1/d$. If $|I| \geq 8r^2$ and p is sufficiently large, then $\rho(I)/|I| > 1 + 1/d + 1/(9r^2)$; and*
(iv) *If $\rho(I)/|I| > 2$, $|I| \geq 8r^2$ and p is sufficiently large, then $\rho(I)/|I| > 2 + 1/(9r^2)$.*

PROOF. The first statement follows immediately from the inequality above.

So we may assume that $\lambda \leq 2r$. Note that D/C is a cyclic group acting faithfully on I_1. Thus, $|I_1| > r$ and so $r - 1/|I| \geq 1/r - 1/r(r+1) \geq 1/2r$. Thus, for p sufficiently large, $\rho(I)/|I| > 1 + 1/3r$.

Suppose that $\rho(I)/|I| > 1 + 1/d$ for $d > 1$ an integer. If $d > 4r$, then $\rho(I)/|I| + 1 - 1/d > 2 + 1/(12r)$.

So assume that $d \leq 4r$ and $\rho(I)/|I| + 1 - 1/d > 2$. Thus, $1 - 1/|I| + \lambda/r > 1 + 1/d$, and $\lambda/r - 1/d \geq 1/rd \geq 1/(4r^2)$. Hence $\lambda/r - 1/d - 1/|I| \geq 1/(8r^2)$ and so for p sufficiently large, $\rho(I)/|I| > 1 + 1/d + 1/(9r^2)$.

The same argument yields the last statement. □

If p is small or to get better bounds, one needs to analyze the above case more closely. However, we will not need this in this article.

We need to handle the remaining primes. We first show that $\rho(I)/|I|$ cannot be too close to $1 - 1/d$ if $|I_1|$ is small. If $|I|$ itself is small, this is clear since we have bounded the denominator and we can also bound d easily.

First note that an easy consequence of Hasse–Arf is the following:

LEMMA 8.5. *Each r_i is a multiple of $|C|$. Indeed, r_i is a multiple of $|C_i|$, where $C_i = C_D(J_i/J_{i+1})$.*

PROOF. By passing to the subgroup C_iJ_i, we may assume that $I = C_1I_1$ and prove the result for r_1. We can then pass to I/I_2 and assume that $I_2 = 1$, whence I is abelian and now Hasse–Arf applies. □

LEMMA 8.6. *Fix $r = |D/C|$. Assume that I_1 contains an abelian subgroup I' of index at most m. Suppose that there are at least $t \geq 5rm$ distinct terms among the $I'_j = I_j \cap I'$. Then $\rho(I)/|I| > 5/2$.*

PROOF. Let $J_1, \ldots, J_t$ denote the smallest subgroups among the higher ramification groups with fixed intersection with I'. Let m_i denote the number of terms among the higher ramification groups which intersect I' in J_i. Then the Riemann–Hurwitz formula yields:

$$\rho(I)/|I| \geq 1 - 1/|I| + (1/|I|) \sum m_i(|J_i| - 1).$$

Now m_i is a multiple of $|C|$ and also by Hasse–Arf m_i is a multiple of $|I' : I'_j|$. Thus,

$$\rho(I)/|I| \geq 1 - 1/|I| + (1/rm) \sum (1 - 1/|J_i|) \geq 1 - 1/|I| + t/(2rm),$$

whence the result. □

LEMMA 8.7. *Fix $r = |D/C|$. Assume that $|I_1| < N$.*

(i) *Let $d > 1$ be a positive integer with $\rho(I)/|I| > 1 + 1/d$. Then $\rho(I)/|I| > 1 + 1/d + 1/(32r^3N^2)$; and*
(ii) *If $\rho(I)/|I| > 2$, then $\rho(I)/|I| > 2 + 1/(2rN)$;*
(iii) *If $\rho(I)/|I| > 1$, then $\rho(I)/|I| > 1 + 1/(2rN)$.*

PROOF. By the previous lemma and the Riemann–Hurwitz formula, it follows that

$$\rho(I) = |I| - 1 + a_i \sum (|J_i| - 1),$$

with the a_i being positive integers that are multiples of s. Thus,

$$\rho(I)/|I| = 1 - 1/|I| + b/r|I_1|,$$

for some positive integer b.

We assume that $s > 1$. If $s = 1$, then $|I| = r|I_1|$ and $\rho(I)/|I| = 1 + b/r|I_1|$ and the argument we give below will also be valid.

If $\rho(I)/|I| > 2$, it follows that $b > r|I_1|$ and so $\rho(I)/|I| > 2 + 1/r|I_1| - 1/|I| \geq 2 + 1/(2r|I_1|)$. We get precisely the same estimate if $\rho(I)/|I| > 1$.

If $d \geq 4rN$ and $\rho(I)/|I| > 1 + 1/d > 1$, then $\rho(I)/|I| > 1 + 1/(2rN) \geq 1/d + 1/(4rN)$.

So assume that $d < 4rN$ and $\rho(I)/|I| > 1 + 1/d$. Thus, $b/r|I_1| > 1/d + 1/|I|$. It follows that $b/r|I_1| - 1/|I| \geq 1/d|I|$ and so $\rho(I)/|I| \geq 1 + 1/d + 1/d|I|$. If $s < 2d$, this implies that $\rho(I) > 1 + 1/d + 1/(32r^3N^2)$.

Also, $\rho(I) \geq 1 + 1/d + 1/rd|I_1| - 1/|I|$. If $s \geq 2d$, this implies $\rho(I) \geq 1 + 1/d + 1/2rd|I_1| > 1 + 1/(8r^2N^2)$.

□

9. Automorphism Groups of Curves

Let k be an algebraically closed field of characteristic $p \geq 0$. Let $f : Z \to Y$ be a G-Galois cover. Assume that Z has genus $h > 1$.

It is classical that $\mathrm{Aut}(Z)$ is finite. We sketch a slightly different proof of this than the standard ones. This proof came out of discussions with M. Zieve at MSRI. This topic will be more fully explored in further work by the author and Zieve.

First consider the case that Z is defined over a finite field. We first prove a weaker result that is valid for any genus curve.

THEOREM 9.1. *Let Z be a curve over k, the algebraic closure of a finite field. Then $\mathrm{Aut}(Z)$ is locally finite.*

PROOF. Let G be a finitely generated subgroup of $\mathrm{Aut}(Z)$. Then G is defined over some finite subfield k_0 of k. Let f be any nonconstant function on Z. We may enlarge k_0 and assume that f is defined over k_0 and all the poles and zeroes of f are k_0-rational points. Let H be the subgroup of G which fixes all k_0 rational points. Since there are only finitely many such points, H has finite index in G and so it suffices to prove that H is finite. Since $h \in H$ implies that h fixes the zeroes and poles of f, it follows that $f^h = a(h)f$ where $a : H \to k_0^*$ is a homomorphism. Thus, f^n is fixed by H for some n (for example, $n = |k_0^*|$). Thus, the fixed field F of H (acting on $k(Z)$) has transcendence degree 1 over k, whence $k(Z)/F$ is a finite extension and so H is finite. □

THEOREM 9.2. *There exists a positive valued integral monotonic function $c(g)$ such that if Z has genus at least 2, then $|\mathrm{Aut}(Z)| \leq c(g)$. In particular, $\mathrm{Aut}(Z)$ is finite.*

PROOF. Let G be a subgroup of $\mathrm{Aut}(Z)$. It suffices to show the bound holds when G is finitely generated (for if every finitely generated subgroup has order less than $c(g)$, so does the whole group). So assume that G is finitely generated.

First we define $c(g)$ and show that if G is finite, then $|G| \leq c(g)$.

We can now apply the Riemann–Hurwitz formula and some relatively easy computations as in [64] or the previous section to obtain some bound (one easily gets cg^5; Stichtenoth obtains cg^4 with some extra effort) to see that $c(g)$ can be taken to be a polynomial in g.

Alternatively, let $W := W_\ell$ denote the set of ℓ-torsion points on the Jacobian of Z. As we have observed, if ℓ does not divide the order of G, then $2g(Z/G) = \dim W^G$ (this is really the character formula version of the Riemann–Hurwitz formula — see [61]). In particular, if H is the kernel of the action of G on T, we see that $g(Z/H) = g(Z)$. If Z has genus greater than 1, then the Riemann–Hurwitz formula shows that Z has no nontrivial separable maps to a curve of genus $g(Z)$, whence $H = 1$. Thus, G acts faithfully on W for any sufficiently large prime ℓ. In particular, $|G|$ divides the greatest common divisor of the

orders of $\mathrm{GL}(2g,\ell)$ for all sufficiently large ℓ. Note that this does not depend on how large we need to let ℓ be (this was observed by Minkowski in his proof of the bound on the orders of finite subgroups of $\mathrm{GL}(n,\mathbb{Q})$ or more generally finite subgroups of $\mathrm{GL}(n,\mathbb{C})$ with all traces rational). We can take $c(g)$ to be this greatest common divisor.

In conjunction with this previous theorem, this proves the result for k the algebraic closure of a finite field.

Consider the general case. Suppose that G has infinite order. We may write the function field $k(Z) = k(u,v)$. Choose a finitely generated subring R of k such that both Z and G are defined over R and that G acts on $S = R(u,v)$. We note that if M is a maximal ideal of R, then R/M is finite (by the Nullstullensatz). Moreover, taking a plane model for Z over R, we see that any reduction will have genus at most some fixed g' (in fact, one knows that the reduction will have genus at most g). Enlarging R if necessary (by inverting a finite number of elements), we can also assume that there are $c > c(g')$ distinct elements of G that remain distinct on $(R/M)(u,v)$ for any maximal ideal M of R and that the genus of $(R/M)(u,v)$ is at least g (all we need is at least 2).

Now we have G acting on $F(u,v)$ with F a finite field. Moreover, the image H of G in this action has order greater than $c(g')$ since the x_i are still distinct. This is a contradiction, whence G is finite. Then $|G| \leq c(g)$ and the result follows. □

The standard Riemann–Roch argument shows that no nontrivial element of G fixes more than $2g+2$ elements. So if we are over a finite field, we can enlarge the field to guarantee the existence of at least $2g+3$ rational points and we see that G acts faithfully on these points and so is finite.

In this section, we consider subgroups of $\mathrm{Aut}(Z)$ that are isomorphic to Chevalley groups in a characteristic different from p and show that the genus of Z must be at least linear in the order of the group. The constant will depend only the type of Chevalley group and not the field. We will use the results of the previous section.

So fix a type of Chevalley group L. Let q be a prime power. Let $J(q)$ denote a group with $F^*(J(q)) = L(q)$ and $J(q)$ contained in the group of inner-diagonal automorphisms of $L(q)$ (for what we need we could just consider $L(q)$). Let W denote the Weyl group of L.

We need the following facts about $J(q)$.

LEMMA 9.3. *Let $G = J(q)$ and let U be a p-subgroup of G with p not dividing q.*

(i) *If p does not divide the order of the Weyl group of L, then the Sylow p-subgroup of G is abelian and if U has exponent p^d, then $|U| \leq p^{td}$ where t is the rank of the corresponding algebraic group.*

(ii) *If the exponent of U is at most p^d, then there exist constants e,t (depending only on L) such that $|U| \leq ep^{td}$.*

(iii) *There exists a constant δ (depending only on L) such that any p'-element of $N_G(U)/C_G(U)$ has order at most δ.*

PROOF. It suffices to prove this result for p-subgroups of the corresponding algebraic group $\mathbf{G}$.

If p does not divide the order of the Weyl group, then every p-subgroup of $\mathbf{G}$ is contained in maximal torus (see [24]). Thus, (i) and (ii) follow in this case. Similarly, it is known that W controls fusion in subgroups of tori and so $N(U)/C(U)$ embeds in W and (iii) holds as well for these primes.

Now consider a prime dividing the order of the Weyl group. There is no harm in embedding the simple algebraic $\mathbf{G}$ into $\mathrm{GL}(n, F)$ with F algebraically closed (over a finite field) and n depending only on L. Then every p-subgroup is conjugate to a subgroup of the monomial group M (since every absolutely irreducible representation of a p-group is induced from a 1-dimensional representation of a subgroup). So we may assume that $U \leq M$. If U has exponent p^d, then $U \cap T$ (with T the torus) has order at most p^{dn} and since $|U|$ divides $|U \cap T| n!$, (ii) follows.

Finally, we prove (iii). Again, it suffices to prove this for subgroups of $\mathrm{GL}(n, F) = \mathrm{GL}(V)$ and for primes dividing the order of the Weyl group. In particular, there are only finitely many primes (depending upon L) to consider. By a result of Thompson (see [23], 3.11), we may assume that $[U, U] \leq Z(U)$, $U/Z(U)$ is elementary abelian and the element is faithful on $U/Z(U)$. By elementary representation theory, we see that $U/Z(U)$ has rank at most n, whence the order of $U/Z(U)$ is bounded as a function of n. Thus (iii) holds. □

We will now prove:

THEOREM 9.4. *There exists a constant $c = c(L)$ such that if $J(q)$ is a subgroup of* Aut(Z) *for some curve Z of genus $g > 1$ defined over the algebraically closed field k of characteristic p with p not dividing q, then $g \geq c|J(q)|$.*

PROOF. Let $G = J(q)$. Consider Z/G. Let h be the genus of Z/G. If $h > 0$, the Riemann–Hurwitz formula together with the fact that $\mathrm{ind}(I) \geq |G|/2$ for any nontrivial inertia group I gives $g - 1 \geq |G|/4$. So we may assume that $h = 0$.

Let I be an inertia group with $I_1 \neq 1$. Write $I = DI_1$ with D a cyclic p'-group and let $C = C_D(I_1)$. By the previous results, we know that $|D/C| < r$ for some constant $r = r(L)$.

There are three possibilities for p.

First suppose that p is small (depending upon L) but $|I_1|$ is large (large enough so that it contains an abelian subgroup of exponent at least p^t with t satisfying the hypotheses of 8.6. Then $\rho(I)/|G| \geq 5/2$, whence $g - 1 \geq 5|G|/4$ and the result holds.

So assume either p is large (and in particular does not divide the order of the Weyl group, whence I_1 is abelian) or that $|I_1|$ is bounded.

If there is another wildly ramified point or at least 3 ramified branch points, then $2(g-1)/|G| \geq -1 + \rho(I)/|I|$. It follows by Lemma 8.4 for p large and by Lemma 8.7 if $|I_1|$ is small, that $\rho(I)/|I| > 1 + \delta$ for some positive δ (depending only upon r which in turn is bounded in terms of L and the bound on $|I_1|$).

Suppose that there is only one ramified point. Then $2(g-1)/|G| = -2 + \rho(I)/|I|$. In particular, $\rho(I)/|I| > 2$ and Lemma 8.4 for p large and Lemma 8.7 if $|I_1|$ is small, that $\rho(I)/|I| > 2 + \delta$ for some positive δ (again depending only upon r).

So we may assume that there is precisely one more ramified point in the cover and it is tamely ramified with inertia group cyclic of order d. Thus, $2(g-1)/|G| = -1 - 1/d + \rho(I)/|I|$. In particular, $\rho(I)/|I| > 1 + 1/d$. Again, Lemma 8.4 for p large and Lemma 8.7 if $|I_1|$ is small imply that $\rho(I)/|I| > 1 + 1/d + \delta$ for some positive δ depending only upon r

This completes the proof. □

COROLLARY 9.5. *Let L be a fixed type of Chevalley group. There exists a positive constant $c = c(L)$ such that $\mu_p(L(q)) \geq c\,\mathrm{md}(L(q))/\log q$ for q sufficiently large with q prime to p.*

PROOF. Let $f : X \to Y$ be a cover with monodromy group G involving $L(q)$ with X of genus $\mu_p(L(q))$. Let Z be the curve corresponding to the Galois closure. By Theorem 7.2, we may assume that $F^*(G) = L(q)$. Note that $|G| \leq 6|J(q)|\log(q)$, where $J(q)$ is the subgroup of G consisting of inner-diagonal automorphisms. By the previous result, this implies that $g(Z) \geq d(L)|G|/\log(q)$ for some constant $d(L)$. By [49] (excluding $L_2(q)$), $\mathrm{fpr}(G) \leq 4/3q$. There is an analogous result for $L_2(q)$. Now apply Corollary 7.3. □

10. The Generalized Fitting Subgroup

Let G be a finite group. A subgroup H of G is *subnormal* in G if there is a chain of subgroups $H = G_0 < G_1 \ldots < G_m = G$ with G_i normal in G_{i+1}. A group G is called *quasisimple* if $G/Z(G)$ is simple and G is equal to its own commutator subgroup. A component of G is a quasisimple subnormal subgroup. It is not difficult to show that any two distinct components of G commute (see the next two lemmas). Let $F(G)$ denote the Fitting subgroup of G (the maximal normal nilpotent subgroup). Let $E(G)$ be the subgroup of G generated by the components of G. The generalized Fitting subgroup of G is defined to be $E(G)F(G)$ and is denoted by $F^*(G)$.

We first need an elementary result about commutators. This follows from the three subgroup lemma (see [23]).

LEMMA 10.1. *Suppose that H is a perfect subgroup of G, N is a subgroup of G and $[H, N]$ is centralized by H. Then H commutes with N.*

PROOF. Since H is perfect, $[H, N] = [[H, H], N]$. The three subgroup lemma asserts that $[[H, H], N] \leq [[H, N], H] = 1$ as claimed. □

The next result is standard although the proof is not.

LEMMA 10.2. *Let H be a component of G.*

(i) *H commutes with every normal subgroup of G not containing H.*
(ii) *If H and K are distinct components, then H and K commute.*
(iii) *H commutes with $F(G)$.*

PROOF. Let M be a normal subgroup of G minimal with respect to containing H. So M is generated by the conjugates of H. If $M = G$, then H is normal in G. If M is proper in G, then by induction, H commutes with all other components of M (any component of M is a component of G). So in either case, M is a central product of the components it contains and $H \lhd M$. Also, we see that $F(M) = Z(M)$.

Let N be a normal subgroup of G not containing H. Then $[M, N] \leq M \cap N \lhd M$. So either $[M, N] \leq Z(M)$ or $M \leq N$, whence either $H \leq N$ or H commutes with N by the previous result.

Since H is not contained in $F(G)$, it follows that H commutes with $F(G)$.

All that remains to show is that H commutes with any other distinct component K. Let N be a minimal normal subgroup containing K. So N is a central product of all its components, whence if $H \leq N$, the result holds. If not, then we have seen that $[H, N] = 1$ and so also $[H, K] = 1$. □

We next give a different characterization of $E(G)$.

LEMMA 10.3. *Let $D = Z(F(G))$. Let X/D be the product of all the minimal normal subgroups of $C_G(F(G))/D$. Then $E(G) = [X, X]$.*

PROOF. Note that X/D has no normal abelian subgroups, for if Y/D is abelian, then since D is central in Y, Y is nilpotent and so $Y \leq F(G) \cap X = Z(F(G)) = D$.

Thus, X/D is a direct product of nonabelian simple groups. In particular, $X = [X, X]D$ with $D \leq Z(X)$ and so $[X, X]$ is perfect and modulo its center is a direct product of nonabelian simple groups $S_1 \times \ldots \times S_t$. Let Q_i be the preimage of S_i in X. Then as above, we see that $[Q_i, Q_i]$ is perfect and simple modulo its center — i.e. a component. We also see that $[X, X]$ is the product of the $[Q_i, Q_i]$, whence $[X, X] \leq E(G)$.

By the previous lemma, every component centralizes $F(G)$ and modulo D is simple. Moreover, as we have already seen, its normal closure is a direct product of simple groups, whence X contains every component of G. Thus, $E(G) = [X, X]$. □

The important property of this subgroup is the following (cf [8]) result which follows immediately.

THEOREM 10.4. *$C_G(F^*(G)) = Z(F(G)) = Z(F^*(G))$. In particular, $F^*(G) \geq C_G(F^*(G))$.*

PROOF. Note that $D := Z(F^*(G)) = Z(F(G))$ (since every component commutes with $F(G)$). Let $C = C_G(F^*(G))$. Suppose that C properly contains D. Consider a minimal normal subgroup of $C_G(F(G)/D$ contained in C/D. By the

previous result, this minimal normal subgroup is contained in $DE(G)$ and so is contained in the center of $DE(G)$, whence is contained in D, a contradiction. □

In particular, this shows that there are only finitely many groups with a given generalized Fitting subgroup (for $G/Z(F(G))$ embeds in $\mathrm{Aut}(F^*(G))$ and so we have a bound on $|G|$).

11. Aschbacher–O'Nan–Scott Theorem

In this section, we give a proof a version of the structure theorem for primitive permutation groups which we have used extensively. See [9] for a more detailed version.

Recall that a group G is said to act primitively on a set Ω of cardinality greater than 1 if G preserves no nontrivial equivalence relations on Ω. In particular, this implies that G is transitive on Ω (consider the equivalence relation of being in the same G-orbit). With this added assumption, it is equivalent to the condition that a point stabilizer is maximal. We include a proof of this well known elementary fact.

LEMMA 11.1. *Let G act transitively on Ω. Then G is primitive if and only if the stabilizer of a point ω is a maximal subgroup of G.*

PROOF. Let H be the stabilizer of the point ω. Then Ω can be identified with G/H, the set of left cosets of H. If H is not maximal, consider the natural map $\pi : G/H \to G/M$ for M a maximal subgroup containing H (here $\pi(gH) = gM$). The fibers of π define a G-invariant equivalence relation on G/H.

Suppose that H is maximal. Let Γ be the equivalence class of ω in a nontrivial G-invariant equivalence relation. Since H fixes ω, H preserves Γ. The same is true for every point of Γ. Since G does not preserve Γ and H is maximal this implies that H preserves each point of Γ. Since G is transitive, this implies that $N_G(H)$ is transitive on Γ. Since H is maximal, this implies that H is normal in G and so is trivial. Thus, G has prime order, a contradiction. □

THEOREM 11.2. *Let G be a finite group acting primitively on a set Ω of cardinality n. Let H be the stabilizer of a point. Let A be the product of the minimal normal subgroups of G. Then $A = F^*(G)$ and one of the following holds*:

(i) *A is an elementary abelian p-group, $G = AH$ (semidirect) and H acts irreducibly on A via conjugation and $n = p^a = |A|$.*
(ii) *$A = A_1 \times A_2$ with $A_1 \cong A_2$ a direct product of $t \geq 1$ isomorphic nonabelian simple groups, $H \cap A = \{(a, \phi(a)) | a \in A_1\}$ for some isomorphism $\phi : A_1 \to A_2$. Moreover, A_1 and A_2 are the two minimal normal subgroups of G and $n = |A_1|$.*
(iii) *A is the unique minimal normal subgroup of G, $A = L_1 \times \ldots \times L_t$ is the direct product of t copies of isomorphic nonabelian simple groups and one of the following*:

(i) $1 \neq H \cap A = H \cap L_1 \times \ldots \times H \cap L_t$ *and* $n = m^t$ *with* $m = |L_1 : H \cap L_1|$ *and the* $H \cap L_i$ *all* H*-conjugate. Moreover,* $N_H(L_1)C_G(L_1)/C_G(L_1)$ *is maximal in* $N_G(L_1)/C_G(L_1)$.

(ii) *There exists a partition* $\{\Delta_1, \ldots \Delta_s\}$ *of* $\{1, \ldots, t\}$ *into* $s < t$ *subsets of size* t/s *and* $A \cap H = K_1 \times \ldots \times K_s$ *where* $K_i \cong L_1$ *is a full diagonal of the direct product of the* $A_i := L_j, j \in \Delta_i$. *In this case,* $n = |L_1|^{t-s}$.

(iii) $A \cap H = 1$, $t > 1$ *and* $n = |L_1|^t$.

Proof. Note that H contains no nontrivial normal subgroups (since a normal subgroup fixing 1 point fixes all points). Let B be any normal subgroup of G. Then $G = BH$ (since H is maximal). Thus, B is transitive, Now $C_H(B)$ is normal in H and normalized by B, whence is normal in G and trivial. Now let B be a minimal normal subgroup. Suppose that B is abelian. Then $B \leq C_G(B)$, so $C_G(B) = B$, and so B is the unique minimal normal subgroup. Thus we are in case (1).

So we may assume that there are no minimal normal abelian subgroups. So $F^*(G) = E(G)$. Let $A_1 = L_1 \times \ldots \times L_t$ be a minimal normal subgroup with L_i conjugate nonabelian simple groups (and components of G). Suppose that there is another minimal normal subgroup A_2. Then A_1 and A_2 commute. Then $G = HA_i$ and $H \cap A_i$ centralizes A_j for $j \neq i$. As noted above, $C_H(A_i) = 1$, whence $H \cap A_i = 1$ for $i = 1, 2$. On the other hand, $A_i \leq G = HA_j$ and so the projections of $H \cap A_1A_2$ into A_j are both onto and injective. Thus, $H \cap A_1A_2 = \{(a, \phi(a)) | a \in A_1\}$ for some isomorphism $\phi : A_1 \to A_2$ as required. Thus, we are in case (2).

So we may assume that A is the unique minimal normal subgroup of G and $A = L_1 \times \ldots \times L_t$ with the L_i conjugate nonabelian simple groups (and components). If $H \cap A = 1$, there is nothing more to say (except to show that $t > 1$ — this requires the classification of finite simple groups in the form of the Schreier conjecture that outer automorphism groups are solvable — see [9] for details).

Suppose that $H_1 = H \cap L_1 \neq 1$. Since $G = AH$ and A normalizes L_1, it follows that H permutes the L_i transitively, whence $H_j = H \cap L_j$ is conjugate to H_1 via H. The maximality of H implies that H is the normalizer of $H \cap A$ and all that remains to be shown in this case is that $N_H(L_1)C_G(L_1)$ is maximal in $N_G(L_1)$.

We note the following — H_1 is the maximal $N_H(L_1)$ invariant subgroup of L_1 (otherwise H normalizes the direct product of the conjugates of this $N_H(L_1)$ invariant overgroup of H_1 contradicting the maximality of H). Suppose that K is a maximal subgroup of $N_G(L_1)$ containing $N_H(L_1)C_G(L_1)$. Let $K_1 = K \cap L_1$. Since $AN_H(L_1) = N_G(L_1)$, it follows that $|N_G(L_1) : N_H(L_1)C_G(L_1)| = |L_1 : H_1|$ and similarly $|N_G(L_1) : K| = |L_1 : K_1|$. Clearly, K_1 contains H_1 and is normalized by $N_H(L_1)$ whence $K_1 = H_1$ and $K = N_H(L_1)C_G(L_1)$ as required.

In the remaining case, $H \cap A \neq 1 = H \cap L_i$. Let π_i denote the projection from onto L_i. Then H normalizes the direct product of these projections and by the

maximality of H, if these are proper H contains them. Thus, each projection is onto. Let K_i be the kernel of π_i. If $K_i = 1$, then $H \cap A \cong L_i$ and is a full diagonal subgroup (i.e. of the form $\{(x, \phi_2(x), \ldots, \phi_t(x)) | x \in L_1\}$ where ϕ_i an isomorphism from L_1 to L_i).

If $K_1 \neq 1$, let Δ_1 be those i such that $\pi_i(K_1) = 1$. All other projections of K_1 are surjective (because K_1 is normal in $H \cap A$ and the projections are surjective). By induction, there is a partition $\Delta_1, \ldots, \Delta_s$ such that K_1 is a direct product of full diagonal subgroups of $A_i, i = 2, \ldots, s$. Since K_1 is normal in $A \cap H$ and is self normalizing in $A_2 \times \ldots \times A_s$, it follows that the projection τ of $A \cap H$ into $A_2 \times \ldots \times A_s$ is the same as that of K_1. Thus, $A \cap H = \ker(\tau) \times K_1$. Since $(A \cap H)/K_1 \cong L_1$, this implies that $\ker(\tau)$ is a full diagonal subgroup of A_1. The only remaining point is to show that the Δ_i all have the same cardinality. This is clear since H normalizes $A \cap H$ and acts transitively on the L_j. □

Much more can be said particularly in case (3) of the theorem. See [9].

12. Aschbacher's Subgroup Theorem

In this section, we prove a version of Aschbacher's Theorem about subgroups of classical groups over finite fields. Roughly, the theorem is that if G is a classical group on a vector space over a finite field F, then any subgroup either is (modulo its intersection with the center) almost simple (i.e. has a unique minimal normal subgroup which is a nonabelian simple group) or preserves some natural geometric structure on the space. By a natural geometric structure on the space, we include such things as a tensor product decomposition, a subspace, a direct sum decomposition or a field extension structure. We will make this more precise below.

In Aschbacher's statement, there are 8 families of structures considered. In fact, there are different ways of organizing the possible structures that one wants to consider (or equivalently, the possible subgroups — the stabilizers of these structures). Aschbacher [7] proved a slightly more general theorem in that he considered subgroups of automorphism groups of classical groups. See also [50] for an approach using Lang's theorem.

This section is based on notes for a course given at USC in 1998.

This theorem has become a standard and important tool in the analysis of subgroups of classical groups. See [33] for one example of how it is used.

When one is using the theorem, it can be important to consider as fine a stratification of the possible geometric structures as possible. Indeed, one category that Aschbacher did not consider was the case of tensor decompositions over extension fields.

However, the proof of the theorem can be organized in different ways. In particular, one does not need to consider all the structures considered by Aschbacher.

The theorem is quite a bit simpler to prove in the case that all irreducible submodules for normal subgroups of G are absolutely irreducible (eg, if one works over the algebraic closure). If that fails, then either G preserves a field extension structure on the space or preserves a direct sum decomposition. Thus, one can give a proof as in the case of an algebraically closed field except for adding one additional class. One can then study this extra class separately. If there is no form involved, then essentially no extra work is required.

We now give a proof of the theorem. In the following subsections, we analyze and classify the groups preserving a field extension structure (in the case that there is no form preserved, there is essentially nothing more to add). In the last subsection, we give some elementary results about groups preserving forms and other representation theory facts which are used in the proof.

Recall that a group G is almost simple if and only if it has a unique minimal normal subgroup which is a nonabelian simple group S (this is equivalent to $S \leq G \leq \mathrm{Aut}(S)$).

Let F be a field of characteristic $p \geq 0$ which is either finite of algebraically closed (there are variations of this result over more general fields). Let G be a finite subgroup of $\mathrm{GL}(V)$ where V is a vector space of dimension d over F (the statement is valid for algebraic groups as well in the case F is algebraically closed with an identical proof where many of the details become quite a bit easier).

Suppose that q is a quadratic form, a unitary form or an alternating form on V. We assume that either $q = 0$ or that q is nondegenerate (i.e. except for the case of quadratic forms in characteristic 2, the radical of the form is 0). Let $X(V, q)$ denote the subgroup of $\mathrm{GL}(V)$ which preserves q up to scalar multiplication. The nondegeneracy condition implies that $X(V, q)$ acts irreducibly on V. So $X(V, q)$ is one of $\mathrm{GL}(V)$, $\mathrm{GO}(V, q)$, $\mathrm{GSp}(V)$ or $\mathrm{GU}(V)$ in the case $q = 0$, q is a quadratic form, alternating form or unitary form respectively. We let $I(V, q)$ denote the isometry group of q (i.e. the subgroup preserving the form). So $I(V, q)$ is one of $\mathrm{GL}(V)$, $O(V, q), Sp(V)$ or $U(V)$. Note that except for the case of quadratic forms, there is only one class of nondegenerate forms. In the case of quadratic forms, there are 2 classes if F is finite and 1 if F is algebraically closed. Moreover, if $\dim V$ is odd, the two classes of quadratic forms give rise to the same isometry groups.

We say that a group H acts homogeneously on V (over F) if V is a direct sum of isomorphic simple FH-modules. The homogeneous component corresponding to a simple FH-module W is the sum of all simple submodules isomorphic to W.

THEOREM 12.1. *Let G be a subgroup of $X(V, q)$ with V a vector space of dimension n over a field F which is either finite or algebraically closed. Let p denote the characteristic of F. Then one of the following holds*:

(R1) *G stabilizes a totally singular subspace*;

(R2) *G stabilizes a nondegenerate subspace*;

(R3) *if the characteristic is* 2 *and* q *is a quadratic form,* G *stabilizes a* 1*-dimensional nonsingular subspace*;

(D1) G *leaves invariant a decomposition* $V = \oplus_{i=1}^{2} V_i$ *with each* V_i *totally singular*;

(D2) G *leaves invariant a decomposition* $V = \oplus_{i=1}^{t} V_i$ *with each* V_i *nondegenerate*;

(T1) G *leaves invariant a tensor decomposition on* V; *i.e.* G *embeds in*

$$X(W_1, q_1) \otimes X(W_2, q_2)$$

where $n = w_1 w_2$ *with* $\dim W_i = w_i$ *and* $q = q_1 \otimes q_2$ *or* $p = 2$, *each* q_i *is a nondegenerate alternating form and* $X(W_1, q_1) \otimes X(W_2, q_2) \leq O(V, q)$ *for the unique* (*up to scalars*) *quadratic form vanishing on all simple tensors*;

(T2) G *leaves invariant a tensor structure on* V; *i.e.* G *embeds in* $X(W, q') \wr S_r$ *where* $n = w^r$, $q = q' \otimes \cdots \otimes q'$ (r *times*) *and* $\dim W = w$ *or* $p = 2$, q' *is alternating and* G *preserves a quadratic form on* V ;

(E) $F^*(G) = Z(G)E$ *where* E *is extraspecial of order* s^{1+2a} *with* s *prime,* $n = s^a$ *and* E *acts absolutely irreducibly* (*and so* G *is contained in the normalizer of* $EZ(G)$); *if* s *is odd,* G *preserves no alternating or quadratic form and if* $s = 2$, G *will preserve a form.*

(EXT) G *preserves an extension field structure*; *or*

(S) $G/Z(G)$ *is almost simple.*

Proof. Suppose that G acts reducibly. So let U be a proper invariant subspace of minimal dimension. Then $\mathrm{rad}(U)$ is also invariant under G—thus, either $U \subseteq \mathrm{Rad}(U)$ or U is nondegenerate (the radical is taken with respect to the corresponding form if it exists—in the case q is a quadratic form and F has characteristic 2, we compute the radical with respect to the corresponding alternating form). If U is nondegenerate, then (R2) holds.

If U is contained in $\mathrm{Rad}(U)$, then U is totally singular unless possibly $p = 2$. In the latter case, the set of vectors with $q(u) = 0$ forms a G-invariant hyperplane of U. By minimality, it follows that either U is totally singular or U is 1-dimensional. Thus (R1) or (R3) hold.

So we assume that G acts irreducibly. Let N be any normal noncentral subgroup of G.

Suppose that N does not act homogeneously on V. Let V_1 be a homogeneous component of V for N. If V_1 is nondegenerate (or there is no form), then so is every component and so (D1) holds. Otherwise, V_1 is totally singular (since $\oplus \mathrm{Rad}(V_i)$ is G-invariant). The irreducibility of G implies that there is a unique component V_i' so that V_i is not perpendicular to V_i'. Thus, G permutes the nondegenerate subspaces $V_i \oplus V_i'$. If this is a proper subspace, then (D1) holds. If not, then (D2) holds.

So we may assume that every normal subgroup of G acts homogeneously. Let W be an irreducible constituent of N. If W is not absolutely irreducible, then

the center of $\mathrm{End}_N(V)$ is a proper extension field E/F whence G preserves an extension field structure on V (this uses the fact that the Brauer group of F is trivial). We will consider this situation in more detail below.

So we may assume that every normal noncentral subgroup acts homogeneously and each irreducible constituent is absolutely irreducible. In particular, this means that we are assuming that G is absolutely irreducible.

Let G_0 be the normal subgroup of G which actually preserves the form (rather than up to a scalar multiple). Since $G/G_0Z(G)$ is cyclic, G_0 cannot consist of scalars (unless $n = 1$).

Let N be a normal noncentral subgroup and suppose that N does not act irreducibly. Moreover, if a form is involved, we assume that $N \leq G_0$. Let W be an irreducible constituent of V for N. Let G_1 be the normalizer in $\mathrm{GL}(W)$ of N. Then a straightforward computation (using the fact that the centralizer of N on W consists of scalars) shows the normalizer of N in $\mathrm{GL}(V)$ is $G_1 \times \mathrm{GL}_{n/d}(U)$ acting on $W \otimes U$ with U of dimension n/d. In particular, G embeds in this group.

If there is no form involved we are done (i.e. G preserves a tensor decomposition—and we note that there is a unique conjugacy class of such subgroups in GL depending only on the dimensions d and n/d). We now consider how the form behaves with respect to this tensor decomposition.

Case 1. q is a quadratic form.

Then V is self dual as an FN-module and hence so W is self-dual for N. Since N acts absolutely irreducibly on W, there is a unique (up to scalar multiple) bilinear form B on W which is N-invariant (if $p \neq 2$, this form is symmetric; if $p = 2$, the form is alternating).

An easy dimension computation shows that all the N-invariant bilinear forms on V are of the form $(W, B) \otimes (U, B')$.

Suppose that $p \neq 2$. If B is alternating, then $q = B \otimes B'$ where B' is an alternating form on B'. As we noted above, $G \leq G_1 \times \mathrm{GL}(U)$ acting on $V = W \otimes U$ where G_1 normalizes N on W. Thus, $G_1 \leq \mathrm{GSp}(W)$. It follows that $G \leq X(V, q) \cap G_1 \times \mathrm{GL}(U) = \mathrm{GSp}(W) \otimes \mathrm{GSp}(U) < \mathrm{GO}(q)$. Moreover, there is a unique conjugacy class of such subgroups.

If B is symmetric, then similarly, we see that $G \leq \mathrm{GO}(B) \otimes \mathrm{GO}(B') < \mathrm{GO}(q)$ with B' symmetric as well. There may be several conjugacy classes depending upon the dimension of W and the class of B.

If $p = 2$, we need to proceed in a slightly different manner and the answer is actually easier. Let Δ be the associated alternating bilinear form associated to q. As above, we see that $\Delta = B \otimes B'$ where B' is a bilinear form on U and $G \leq \mathrm{GSp}(W) \times \mathrm{GSp}(U)$. Let T denote the image of $\mathrm{GSp}(W) \otimes \mathrm{GSp}(U)$ in $\mathrm{GL}(V)$. In fact, T is contained in the orthogonal group and not just the symplectic group. Indeed, this last group preserves a unique (up to scalar mul-

tiplication) quadratic form. Since T is transitive on all nonzero vectors of the form $w \otimes u$, the quadratic form would have to be constant on such vectors. It is straightforward to compute that there exists a unique quadratic form which vanishes on all such vectors and has the corresponding associated alternating form $B \otimes B'$. The uniqueness shows that the form is T-invariant. Since G is absolutely irreducible, it preserves a unique quadratic form, whence q is the form described above.

Case 2. q is alternating.

As above, we see that N leaves an essentially unique form B on W. Thus, G_1 does as well. Arguing precisely, as above, we see that $G \leq X(W,B) \otimes X(U,B') \leq X(V,q)$. If $p \neq 2$, then we see that B is symmetric and B' alternating or vice versa. If $p = 2$, then we may take both B and B' alternating and we see that in fact G preserves a quadratic form (indeed, in Aschbacher's theorem, this is one of the geometric structures allowed — a subform).

Case 3. q is unitary.

In this case F is a finite field of cardinality m^2. Let F_0 be the subfield of F of cardinality m. Since N acts absolutely irreducibly on W and homogeneously on V, it follows that N preserves a unique (up to F_0 multiple) unitary form h on W.

Arguing as above, we see that this implies that $q = h \otimes h'$ and $G \leq X(W,h) \otimes X(U,h') \leq X(V,q)$.

So now we may assume that every noncentral normal subgroup acts absolutely irreducibly. Let N be a minimal such subgroup. Thus, $C_G(N) = Z(G)$. It follows that $N/(N \cap Z(G))$ is characteristically simple (i.e. has no nontrivial characteristic subgroups). Thus $M := N/(N \cap Z(G)$ is either an elementary abelian s-group for some prime s or it is a direct product $L_1 \times \ldots \times L_t$ where $L_i \cong L$ is a nonabelian simple group.

Suppose that M is an elementary abelian s-group. Since N', the derived group of N, is contained in the center of N, it follows that N' is either trivial or has order s. In the first case, N is abelian and noncentral. Since it acts absolutely irreducibly, it follows that $n = 1$. So we may assume that N' has order s. Since N acts absolutely irreducibly, $Z(N) \leq Z(G)$.

It follows easily that if s is odd, then N is an extraspecial s-group of order s^{1+2a} and $n = s^a$. If s is even, then N is of symplectic type (i.e. either N is extraspecial or $Z(N)$ has order 4 and $N = Z(N)E$ with E extraspecial).

Thus, (E) holds.

So we may assume that M is a product of t isomorphic nonabelian simple groups. It follows that N is a central product of components $Q_1, \ldots, Q_t$. By

minimality, each of the Q_i are conjugate in G. Also, we may assume that every minimal normal noncentral subgroup has this form. Since $C_G(N) = Z(G)$, it follows that N is unique. So if $t = 1$, we see that (S) holds. So assume that $t > 1$.

Since N acts absolutely irreducibly on V, it follows that $V = W_1 \otimes \ldots \otimes W_t$ and N embeds in $\hat{Q}_1 \times \ldots \times \hat{Q}_t \leq \mathrm{GL}(W_1) \times \ldots \times \mathrm{GL}(W_t)$ where $\hat{Q}_i \cong \hat{Q}$ is a covering group of Q_i. Since the Q_i are conjugate, we may assume that W_i is an absolutely irreducible $\hat{Q}$-module and the W_i are isomorphic as $\hat{Q}$-modules. In particular, they have the same dimension. This is easily seen to be true over the algebraic closure. However, since the character of G is defined over F, the same is true for $\hat{Q}$ acting on W_i.

It follows that the normalizer of N in $\mathrm{GL}(V)$ is precisely $(R_1 \times \ldots \times R_t)\mathrm{Sym}_t$ where R_i is the normalizer of $\hat{Q}_i$ in $\mathrm{GL}(W_i)$ and Sym_t acts on $W_1 \otimes \ldots \otimes W_t$ by permuting the coordinates. In particular, G is contained in this product and so G preserves a tensor structure on V.

If G preserves a form on V, then so does N and since V restricted to Q_i is homogeneous (as $N = Q_i C_N(Q_i)$) and so $\hat{Q}_i$ preserves a form on W_i (and the type is the same for each i).

So if q is unitary, it follows that $G \leq X(W,h) \wr S_t \leq X(V,q)$ with h unitary. If V is self dual for N, then it follows that $G \leq X(W,f) \leq X(V,q)$. If $p \neq 2$, then for t even, necessarily q is symmetric. If t is odd, then q and f are either both symmetric or are both alternating. If $p = 2$, then we see that G does preserve a quadratic form (necessarily unique) and so we may always take f to be alternating.

This completes the proof. □

Note that one can state the previous theorem in a different manner. Namely, we have produced natural families of subgroups so that any finite subgroup of $X(V,q)$ is either contained in one of those subgroups or is almost simple (modulo the center). One can of course add to this family some almost simple groups and so when analyzing the subgroup structure of $X(V,q)$ (or related groups), one can use this result. See [45] for an analysis of which of these subgroups are maximal.

The theorem above gives a very specific list of possibilities and one can analyze the conjugacy classes of such subgroups quite easily and produce some natural invariants. In particular, we note that two irreducible subgroups of $X(V,q)$ are conjugate in $X(V,q)$ if and only if the representations are equivalent (up to an outer automorphism) if and only if the characters are the same (up to an outer automorphism).

The one family that we did not analyze so carefully in the proof above is the case where G preserves an extension field structure on V. If F is algebraically closed, this cannot occur. If $q = 0$, then it is straightforward to see that the group preserving a field extension structure corresponding to a field extension is precisely $\mathrm{GL}_{n/d}(E).\mathrm{Gal}(E/F)$ where $d = [E : F]$—i.e. the subgroup of E-

semilinear transformations on V. Note that the only invariant for the conjugacy class is d (and d must divide n).

In the next section, we will analyze the case where $q \neq 0$ and G preserves an extension field structure on V.

12.1. Field Extension Structures We now make more precise the family of overgroups occurring in the extension field case. We will break the proof up into the various cases depending upon the type of q.

So we assume that F is a finite field of order $m = p^a$ and that V is a vector space of dimension n over F. As usual, let q denote a form (zero, quadratic, alternating or unitary) on V and we assume that $G \leq X(V, q)$. We may also assume that G is irreducible on V and that G preserves a field extension structure on V. More precisely, there is an F-subalgebra $E \subset \mathrm{End}_F(V)$ so that G preserves E (and we have an homomorphism from G into $\mathrm{Gal}(E/F)$).

Note that if the isomorphism class of E is fixed, then E is uniquely determined up to conjugation in $\mathrm{GL}(V)$ (because E has a unique representation of fixed dimension). Since the norm map is surjective for finite fields, in fact this conjugation can always be realized in $SL(V)$. So in the case where $q = 0$, G preserves an E-structure on V if and only if G is a subgroup of $\mathrm{Aut}_E(V).\mathrm{Gal}(E/F)$.

So we assume that (V, q) is nondegenerate. We also make the blanket assumption throughout this section that every normal subgroup of G acts homogeneously on V (or G will satisfy (D1) or (D2)).

Let E/F be an extension of finite fields of degree $d > 1$. Suppose that B is a nondegenerate bilinear form on the vector space U over E. Let $V = U$ considered as a vector space over F. Then $q = \mathrm{tr} \circ B$ is a nondegenerate bilinear form on V and $X(U, B) \leq X(V, \mathrm{tr} \circ B)$.

We first discuss the case where q is either alternating or a quadratic form.

PROPOSITION 12.2. *Assume that q is a nondegenerate alternating or quadratic form on V where V is a vector space of dimension n over the finite field F. Let $G \leq X(V, q)$ be an irreducible subgroup. Assume that every normal subgroup of G acts homogeneously on V. Assume that G normalizes some proper field extension E/F where E is a subalgebra of* $\mathrm{End}_F(V)$. *Assume moreover that G preserves no additive decomposition of V. Then $G \leq X(U, q')$ where $U = V$ considered as a vector space over some nontrivial field extension E/F and q' is a form on U.*

PROOF. Let Z denote the subgroup of nonzero scalars in $GL(V)$. Let $H = G \cap I(X, q)$. Note that either $GZ = HZ$ or GZ/HZ has order 2. We claim that H acts irreducibly. If not, then $V = V_1 \oplus V_2$ with G permuting each of the H-invariant subspaces V_i. Since H is homogeneous on V, $V_1 \cong V_2$ as H-modules. Since V is self dual as an H-module, we may choose V_1 and V_2 nonsingular. Then G preserves the decomposition $V_1 \oplus V_2$, a contradiction.

Let $E = \mathrm{End}_H(V)$. So E/F is a proper field extension.

Let U denote V considered as an EH-module. Note that $V' := V \otimes_F E_0 \cong \oplus U^\sigma$ where the sum is taken over $\sigma \in \mathrm{Gal}(E/F)$. Since E is commutative, then centralizer of H in V' which is just $E \otimes_F E$ is also commutative. It follows that V' is multiplicity free, whence U^σ and U are nonisomorphic for all nontrivial σ. Since V' is self dual, it follows that $U^\tau \cong U^*$ for some τ. Thus, $U^{\tau^2} \cong U$ and so $\tau^2 = 1$.

Suppose first that $\tau = 1$, i.e. U is self dual. Then there exists a nondegenerate bilinear form B on U which is H-invariant. Moreover, B is unique up to scalar multiplication by E_0. Let $I = I(U, B)$. Note that this is independent of the choice of B. Since G acts naturally on the set of such forms, it normalizes I. Note that $I(U, B)$ preserves the form $\mathrm{tr}_{E/F} \circ B$. Note also that for $p \neq 2$, this form is the same type as q — i.e. B is alternating if and only if q is (because H and $I(U, B)$ have the same centralizer it follows that all forms stabilized by $I(U, B)$ are also stabilized by H and also are of the same type). Thus, $I(U, B) \leq I(X, q)$ and G is contained in the normalizer of $I(U, B)$ in $X(V, q)$.

If $p = 2$ and q is alternating, precisely the same argument suffices. All that remains to show is that if q is a quadratic form, then H preserves a quadratic form on U. Let B be an H-invariant alternating form on U. Then as above we may assume that $C = \mathrm{tr} \circ B$ where C is the alternating form on V associated to q.

Since the set of H-invariant forms on V has cardinality $|E|$ and the map $B \mapsto \mathrm{tr}_{E/F} \circ B$ is injective, we see that we may assume that $C := \mathrm{tr}_{E/F} \circ B$ is either q or if $p = 2$ and q is a quadratic form, C is the associated alternating form. Moreover, in the latter case, by considering $\mathrm{Sp}(B) \cap O(V, q)$, we see that $H \leq I(U, f)$ where f is a quadratic form on U whose associated alternating form is B. By a dimension argument, we may assume that $q = \mathrm{tr}_{E/F} \circ f$. Thus, we see that G is contained in the normalizer of $I(U, h)$ where h is a form of the same type as q (i.e. quadratic or alternating). Since $q = \mathrm{tr}_{E/F} \circ q$, it follows that $I(U, h) \leq I(X, q)$ and the result follows.

Next assume that $\tau \neq 1$. It follows that H preserves a unitary form h on U (note the assumption implies that $[E : F]$ is even). Let E_0 denote the fixed field of τ. Since H acts absolutely irreducibly on U, it is contained in precisely one unitary group on U, whence G normalizes this unitary group. □

A minor variant on the previous argument shows that:

PROPOSITION 12.3. *Assume that h is a nondegenerate hermitian form on V where V is a vector space of dimension n over the finite field F. Let $G \leq X(V, h)$ be an irreducible subgroup. Assume that every normal subgroup of G acts homogeneously on V. Assume that G normalizes some proper field extension of F where contained in $\mathrm{End}_F(V)$. Assume moreover that G preserves no additive decomposition of V. Then $G \leq X(U, h')$ where $U = V$ considered as a vector space over some nontrivial field extension E/F and h' is a hermitian form on U.*

12.2. Some Elementary Representation Theory

LEMMA 12.4. *Let H be a normal subgroup of finite index in G and assume that V is a homogeneous FH-module and an irreducible FG-module. Let W be an irreducible constituent of V for H.*
(a) *If W is absolutely irreducible, then G embeds in $\mathrm{GL}(W) \otimes \mathrm{GL}(U)$ acting on $W \otimes U \cong V$.*
(b) *If G/H is abelian and V is absolutely irreducibly as a G-module, then V is an irreducible FH-module.*
(c) *If G/H is abelian of exponent m and all mth roots of 1 are in F, then V irreducible as an FG-module implies that V is irreducible as an FH-module.*

PROOF. (a) is well known and is straightforward by computing the normalizer of H in $\mathrm{GL}(V)$.

We now prove (b). By Frobenius reciprocity, V embeds in the induced module W_H^G. This has the same composition factors as $W \otimes F[G/H]$ (for example, we can compute the Brauer character). Since G/H is abelian, over the algebraic closure, we can find a chain of G-submodules of W_H^G so that all quotients are isomorphic to W as H-modules. Since V is absolutely irreducible, this implies that $\dim V \leq \dim W$, whence $V = W$ as required.

If G/H has exponent m and F contains all mth roots of 1, then the same argument shows that each FG-composition factor of W_H^G has dimension at most $\dim W$, whence $V = W$. Thus, (c) holds. □

LEMMA 12.5. *Let G be a finite group.*

(i) *If V is an irreducible FG-module, then G preserves a nondegenerate symmetric or alternating form on V if and only if V is self dual. Moreover, any two forms are in the same C-orbit where C is the group of units in the centralizer of G in $\mathrm{End}(V)$.*
(ii) *If V is an irreducible FG-module and $p = 2$, then G preserves a nondegenerate alternating form if and only if V is self dual. If G preserves a nondegenerate quadratic form on V, then there is a single C-orbit of such quadratic forms.*
(iii) *If V is a homogeneous self dual module and W is an irreducible submodule of dimension m and $\dim \mathrm{End}_{FG}(W) = d$, then the dimension of the G-invariants on the space of bilinear forms is $d(n/m)^2$.*

PROOF. G leaves invariant a nonzero bilinear form on V if and only if there are nonzero fixed points on $V \otimes V$. Any nonzero invariant form must be nondegenerate (since $\mathrm{Rad}(V)$ would be invariant). Such a form gives an FG-isomorphism between V and V^*.

So we may assume that V is self dual. In that case $V \otimes V \cong V \otimes V^* \cong \mathrm{End}(V)$. The nonzero G invariants on $\mathrm{End}(V)$ are precisely C, whence there is a single C-orbit of invariants.

If $p \neq 2$, then $V \otimes V$ is the direct sum of alternating forms and symmetric forms so if G has a fixed point, there must be one that is either symmetric or alternating. Since C preserves both spaces (as $\mathrm{GL}(V)$ does), it follows that all invariant forms are either symmetric or alternating.

If $p = 2$, then the composition factors on $V \otimes V$ (as a $\mathrm{GL}(V)$-module) are $\wedge^2(V)$, V' and $\wedge^2(V)$ where V' is a twist of V (by the Frobenius automorphism). In any case, V' is an irreducible G-module, whence if G has fixed points, then G must have a fixed point on $\wedge^2(V)$. Thus, G always preserves an alternating form. Arguing as above, we see that the nontrivial G fixed points is a single C-orbit.

If G preserves a quadratic form q, we claim that the only quadratic forms which are G-invariant are Cq. Let B_q denote the associated alternating form (so $B_q(v, v') = q(v + v') + q(v) + q(v')$). We know that the set of G-invariant alternating forms is a single C-orbit. Suppose q' is G-invariant. Then replacing q' by an element in Cq', we may replace q' by something in its orbit so that $B_q = B_{q'}$. An elementary computation shows that the set of elements with $q(v) = q'(v)$ is a proper linear G-invariant subspace. Since G is irreducible, it must be 0, whence $q = q'$ and the result follows.

If V is homogeneous, then we compute the invariants as above. □

LEMMA 12.6. *Let F be the finite field of order q^2. Let V be an n-dimensional vector space over F such that V restricted to G is a homogeneous module with irreducible constituent W. Then G fixes a unitary form on W if and only if it does so on V if and only if $\chi(g^q) = \chi(g^{-1})$ for all $g \in G$ where χ is the Brauer character associated to W. If V is irreducible, these conditions are also equivalent to $\chi(g^q) = \chi(g^{-1})$ for all $g \in G$ where χ is the character associated to W. Moreover, if G preserves a unitary form on W, and W is absolutely irreducible, then the space of unitary forms on V which are G-invariant is a vector space over F_q of dimension m^2 where $m = \dim V / \dim W$ is the multiplicity of W.*

PROOF. Let ρ denote the field automorphism $x \to x^q$ on F. By definition of the unitary group, we know that $\rho(g)$ is similar to g^{-1}, viewing G as a subgroup of the unitary group on V. Since V is homogeneous as a G-module, this same condition holds in $\mathrm{GL}(W)$. Thus, to complete the first part of the proof, we need only show that if the character of W satisfies the hypothesis, then W supports a G-invariant form.

The easiest proof is to use Lang's Theorem. Let ϕ denote the given representation of G into $\mathrm{GL}(V)$. We need to find $S \in \mathrm{GL}_n(\bar{F})$ so that $S\phi(g)S^{-1}$ is in the unitary group. This is equivalent to the equation

$$(S\phi(g)S^{-1})^{-T} = \rho((S\phi(g)S^{-1})).$$

By hypothesis, there exists $U \in \mathrm{GL}_n(F)$ with $U\phi = \phi' U$. By Lang's Theorem, $U = S\rho(S^{-T})$ for some $S \in \mathrm{GL}_n(\bar{F})$. This implies that S satisfies the equation above. □

13. Abelian Supplements

Let p be a prime. Let $p(G)$ denote the normal subgroup of the finite group generated by all its Sylow p-subgroups. A finite group G is said to be a quasi p-group if $G = p(G)$ or equivalently if G has no nontrivial p'-quotients. This notion has become quite important in studying fundamental groups of varieties in characteristic p. See [43] and [60] for the solution of the Abhyankar conjecture about fundamental groups of affine curves.

Certain two dimensional varieties are considered in [44]. For these varieties, Abhyankar observed that for any finite image of the fundamental group we have

$$1 \to p(G) \to G \to A \to 1,$$

where A is abelian generated by 2 elements. Abhyankar also conjectured that these conditions were sufficient. Harbater and Van der Put [44] showed that in fact it must also be the case that $G = p(G)B$ for some abelian subgroup B of G. In the appendix of [44], we developed a theory about this situation and gave examples. Combining the examples with the results of [44] shows that the Abhyankar conjecture does not hold.

In this section, we give a simpler form of the example. We also give some examples of a similar phenomenon when A is cyclic of bounded order. Recall that if $H \leq G$, then B is called a supplement to H in G if $G = HB$ and a complement to B if in addition $H \cap B = 1$.

Of course, if $G/p(G)$ is cyclic, we can always write $G = p(G)B$ where B is a cyclic p'-group. If $p(G)$ is a p-group (i.e. there is a unique Sylow p-subgroup of G), then the short exact sequence above splits and so abelian supplements will always exist. The apparent hope was that quasi p-groups have cohomological properties similar to p-groups. However, that is not the case as the examples in the appendix of [44] show.

If $G/p(G)$ is abelian of rank larger than 2, it is quite easy to write down a plethora of examples where there is no abelian supplement to $p(G)$. It is a bit harder to find such examples with the quotient that is abelian of rank 2.

A generalization of the following result appears in the thesis of the author. See also [25].

LEMMA 13.1. *Let r be an odd prime. Let $R := R_d$ be the free group on $2d$ generators subject to $x^r = 1 = [[x, y], z]$ for all $x, y, z \in R$. Then there exist elements in $[R, R]$ which are a product of d commutators but no fewer. Moreover, $Z(R) = [R, R]$ is elementary abelian of order $p^{d(2d-1)}$ and $R/Z(R)$ is elementary abelian of order p^{2d}.*

PROOF. It is straightforward to verify that $|R| = r^{d(2d+1)}$ and that $Z(R) = [R, R]$ and $R/Z(R)$ are elementary abelian. If we choose generators $x_i, 1 \leq i \leq 2d$ for R and set $y_{ij} = [x_i, x_j]$ for $i < j$, then any element in $w \in [R, R]$ can be expressed uniquely as $\prod_{i<j} y_{ij}^{c_{ij}}$ where c_{ij} may be viewed as an element of $\mathbb{F}_r$.

This gives a bijection between $[R,R]$ and the set of $2d \times 2d$ skew symmetric matrices over $\mathbb{F}_r$ (by sending w to the unique skew symmetric matrix whose i,j entry to be c_{ij} for $i<j$). On the other hand, a commutator will correspond to a rank two skew symmetric matrix. So if w corresponds to a nonsingular skew symmetric matrix, w is a product of d commutators but no fewer. This also shows that $[R,R]$ has the order mentioned above. □

We first give the example when $p=2$ because it is so simple.

PROPOSITION 13.2. *Let $p=2$ and r be any odd prime. Let H be the semidirect product of R_2 and a cyclic group generated by an involution τ, where τ inverts each generator x_i. Note that τ centralizes $Z := Z(R_2)$. Pick a subgroup $Y = \langle y \rangle$ of Z of order r which contains noncommutators. Let E be the extraspecial group of order r^3 and exponent r. Let G be the central product of H and E identifying $Z(E)$ and Y (precisely, $G = (H \times E)/\langle (y,w) \rangle$ where w generates $Z(E)$). Then*

(i) *$p(G) = H$;*
(ii) *$G/p(G)$ is elementary abelian of order r^2; and*
(iii) *there is no abelian supplement to H in G.*

PROOF. Since $R = [\tau, R]$, it follows that the normal closure of τ is H and so the first assertion holds. Clearly $G/H \cong E/W$ is elementary abelian of order r^2, whence the second statement holds.

Suppose that B is an abelian supplement to H in G. There is no harm in assuming that B is an r-group (pass to the Sylow r-subgroup of B) and is generated by two elements u,v (pass the subgroup generated by a pair of elements which generate modulo H). Then $u = ah_1$ and $v = bh_2$ where a,b generate E/W and $h_i \in R$ (clearly, we can take $h_i \in H$ but since u and v are r-elements, so are the h_i). Then $1 = [u,v] = [ah_1, bh_2] = [a,b][h_1,h_2]$. This implies that $y^j = [h_1,h_2]$ for some nontrivial j (since $[a,b]$ is a nontrivial power of w which we identify with that same power of y). However, y^j is not a commutator in R. This contradiction completes the proof. □

We now show how to modify the construction for an arbitrary p. Let r be a prime congruent to 1 modulo p. Let $c,d \in F_r^*$ of order p with $cd=1$. Then there is an automorphism τ of order p of R_2 which sends x_i to x_i^c if i is even and x_i^d if i is odd. Moreover, τ centralizes $y = y_{14}y_{23}$. Note that $y \in Z(R)$ and y is not a commutator in R. Let H be the semidirect product R and the group generated by τ. Let E be as above and define G to be the central product of H and E — identify y with a nontrivial central element of E. The proof of the previous result shows that:

PROPOSITION 13.3. (i) *$p(G) = H$;*
(ii) *$G/p(G)$ is elementary abelian of order r^2; and*
(iii) *there is no abelian supplement to H in G.*

More recently, Harbater has become interested in another fundamental group problem. In this case, G is a group with $G/p(G)$ cyclic of order dividing a fixed m (with m prime to p). The question is whether there is a cyclic supplement of order dividing m. If $G/p(G)$ cyclic of order exactly m, then any cyclic supplement of order dividing m would have to be a complement of order m. If m is infinite, then of course one can also find such a supplement (just choose any cyclic subgroup which generates $G/p(G)$). It is not hard to show that for any fixed m there are examples with no cyclic supplement of order dividing m.

The first example that comes to mind is $G = M_{10}$ and $m = 2$. Let p be 3 or 5. Then $p(G) = A_6$ and $G/p(G)$ has order 2. However, $p(G)$ contains all involutions of G and so there is no supplement of order 2.

For convenience, let us take m an odd prime (different from p). An obvious modification of the construction gives examples for any m prime to p. Let S be an extraspecial m-group of order m^{1+2d} such that S admits an automorphism τ of order p with $C_S(\tau) = Z(S)$. The existence of such an automorphism amounts to finding an element of order p in $Sp(V)$ that has no trivial eigenvalues. Let H be the semidirect product of S and τ. Let G be the central product of H and $J = \langle w \rangle$ with J cyclic of order m^2 (where we identify the center of S with the subgroup of J of order m). Any cyclic supplement of order m is generated by an element of the form wh for some $h \in S$. Since m is odd, it is straightforward to compute that $(wh)^m = w^m$ for all $h \in S$, whence any cyclic supplement has order a multiple of m^2. Clearly $p(G) = H$ and G/H is cyclic of order m.

References

[1] S. Abhyankar, Nice equations for nice groups. Israel J. Math. 88 (1994), 1–23.

[2] S. Abhyankar, Symplectic groups and permutation polynomials, Part I, preprint.

[3] S. Abhyankar, Symplectic groups and permutation polynomials, II, Finite Fields Appl. 8 (2002), 233–255.

[4] S. Abhyankar, Orthogonal groups and permutation polynomials, preprint.

[5] S. Abhyankar and N. Inglis, Galois groups of some vectorial polynomials, Trans. Amer. Math. Soc. 353 (2001), no. 7, 2941–2869.

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

[7] M. Aschbacher, On the maximal subgroups of the finite classical groups. Invent. Math. 76 (1984), 469–514.

[8] M. Aschbacher, Finite Group Theory, Cambridge University Press, Cambridge, 1986.

[9] M. Aschbacher and L. Scott, Maximal subgroups of finite groups, J. Algebra 92 (1985), 44–80.

[10] S. Cohen, Permutation Polynomials in Shum, Kar-Ping (ed.) et al. Algebras and combinatorics, Papers from the international congress, ICAC'97, Hong Kong, August 1997, Singapore, Springer, 133–146 (1999).

[11] S. Cohen, and R. Matthews, A class of exceptional polynomials, Trans. Amer. Math. Soc. 345 (1994), no. 2, 897–909.

[12] N. Elkies, Linearized algebra and finite groups of Lie type. I. Linear and symplectic groups. Applications of curves over finite fields (Seattle, WA, 1997), 77–107, Contemp. Math., 245, Amer. Math. Soc., Providence, RI, 1999.

[13] W. Feit, On symmetric balanced incomplete block designs with doubly transitive automorphism groups, J. Combinatorial Theory Ser. A 14 (1973), 221–247.

[14] M. D. Fried, Galois groups and complex multiplication, Trans. Amer. Math. Soc. 235 (1978), 141–162.

[15] M. D. Fried, On a Theorem of MacCluer, Acta Arith. XXV (1974), 122–127.

[16] M. Fried, R. Guralnick, and J. Saxl, Schur covers and Carlitz's conjecture, Israel J. Math. 82 (1993), 157–225.

[17] G. Frey, K. Magaard and H. Voelklein, The monodromy group of a function on a general curve, preprint.

[18] M. Fried and H. Völklein, Unramified abelian extensions of Galois covers, Proceedings of the Summer Research Institute on Theta Functions (Gunning and Ehrenpreis, editors), Proceedings of Symposia in Pure Mathematics 49 (1989), 675–693.

[19] D. Frohardt, R. Guralnick and K. Magaard, Incidence matrices, permutation characters, and the minimal genus of a permutation group. J. Combin. Theory Ser. A 98 (2002), 87–105.

[20] D. Frohardt and K. Magaard, Monodromy composition factors among exceptional groups of Lie type in Group Theory, Proceedings of the Biennial Ohio State-Denison Conference, 134–143(eds. Sehgal and Solomon), World Scientific, Singapore, 1993.

[21] D. Frohardt and K. Magaard, Grassmanian fixed point ratios, Geometriae Dedicata 82 (2000), 21–104.

[22] D. Frohardt and K. Magaard, Composition factors of monodromy groups, Ann. of Math. 154 (2001), 327–345.

[23] D. Gorenstein, Finite Groups, Harper and Row, New York, 1968.

[24] D. Gorenstein, R. Solomon and R. Lyons, The classification of finite simple groups. Number 3, Part 1. Chapter A, Almost simple K-groups, Amer. Math. Soc., Providence, RI, 1998.

[25] R. Guralnick, On a result of Schur, J. Algebra 59 (1979), 302–310.

[26] R. Guralnick, Subgroups of prime power index in a simple group. J. Algebra 81 (1983), 304–311.

[27] R. Guralnick, Monodromy groups of rational functions which are Frobenius groups, preprint (1998).

[28] R. Guralnick, The genus of a permutation group, in Groups, Combinatorics and Geometry, edited by M. Liebeck and J. Saxl, LMS Lecture Note Series 165, Cambridge University Press, London, 1992.

[29] R. Guralnick and W. Kantor, Probabilistic generation of finite simple groups. Special issue in honor of Helmut Wielandt. J. Algebra 234 (2000), 743–792.

[30] R. Guralnick and P. Müller, Exceptional polynomials of affine type. J. Algebra 194 (1997), 429–454.

[31] R. Guralnick, P. Müller, and J. Saxl, The rational function analogue of a question of Schur and exceptionality of permutation representations, Mem. Amer. Math. Soc., to appear.

[32] R. Guralnick and M. Neubauer, Monodromy groups of branched coverings: The generic case, in Recent developments in the inverse Galois problem (Seattle, WA 1993) 325–352, Comtemp. Math.,186, Amer. Math. Soc., Providence, RI, 1995.

[33] R. Guralnick, T. Pentilla, C. Praeger, and J. Saxl, Linear groups with orders having certain large prime divisors. Proc. London Math. Soc. (3) 78 (1999), 167–214.

[34] R. Guralnick, J. Rosenberg, and M. Zieve, A new class of exceptional polynomials in characteristic 2, preprint (2000).

[35] R. Guralnick and J. Saxl, Monodromy groups of polynomials. Groups of Lie type and their geometries (Como, 1993), 125–150, London Math. Soc. Lecture Note Ser., 207, Cambridge Univ. Press, Cambridge, 1995.

[36] R. Guralnick and J. Saxl, Exceptional polynomials over arbitary fields, to appear.

[37] R. Guralnick, J. Saxl and M. Zieve, in preparation.

[38] R. Guralnick and K. Stevenson, Prescribing ramification in Arithmetic fundamental groups and noncommutative algebra, Proceedings of Symposia in Pure Mathematics, 70 (2002) editors M. Fried and Y. Ihara, 1999 von Neumann Conference on Arithmetic Fundamental Groups and Noncommutative Algebra, August 16–27, 1999 MSRI.

[39] R. Guralnick and J. Shareshian, Genus of symmetric and alternating groups actions I., preprint (2002).

[40] R. Guralnick and J. Thompson, Finite Groups of Genus Zero, J. Algebra 131 (1990) 303–341.

[41] 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.

[42] R. Guralnick and M. Zieve, Polynomials with monodromy $PSL(2,q)$, preprint (2000).

[43] D. Harbater, Abhyankar's conjecture on Galois groups over curves, Inventiones Math., 117 (1994), 1–25.

[44] D. Harbater and M. van der Put with an appendix by R. Guralnick, Valued fields and covers in characteristic p, in "Valuation Theory and its Applications", Fields Institute Communications, vol. 32, edited by F.-V. Kuhlmann, S. Kuhlmann and M. Marshall, 2002, 175–204.

[45] P. Kleidman and M. Liebeck, The subgroup structure of the finite classical groups. London Mathematical Society Lecture Note Series, 129. Cambridge University Press, Cambridge, 1990.

[46] N. Katz, Local-to-global extensions of representations of fundamental groups, Ann. Inst. Fourier (Grenoble) 36 (1986), 69–106.

[47] H. Lenstra, H. W., Jr. and M. Zieve, A family of exceptional polynomials in characteristic three, Finite fields and applications (Glasgow, 1995), 209–218, London Math. Soc. Lecture Note Ser., 233, Cambridge Univ. Press, Cambridge, 1996.

[48] M. Liebeck, C. Praeger and J. Saxl, On the O'Nan-Scott theorem for finite primitive permutation groups, J. Austral. Math. Soc. Ser. A 44 (1988), 389–396.

[49] M. Liebeck and J. Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces, Proc. London Math. Soc. (3) 63 (1991), 266–314.

[50] M. W. Liebeck and G. Seitz, On the subgroup structure of classical groups, Invent. Math. 134 (1998), 427–453.

[51] M. Liebeck and A. Shalev, Simple groups, permutation groups and probability, J. Amer. Math. Soc. 12 (1999), 497–520.

[52] F. Lübeck, F., Smallest degrees of representations of exceptional groups of Lie type, Comm. Algebra 29 (2001), 2147–2169.

[53] K. Magaard, Monodromy and Sporadic Groups, Comm. Algebra 21 (1993), 4271–4297.

[54] G. Malle, Explicit realization of the Dickson groups $G_2(q)$ as Galois groups in their defining characteristic, Pacific J. Math., to appear.

[55] P. Müller, Primitive monodromy groups of polynomials, Recent developments in the inverse Galois problem (Seattle, WA, 1993), 385–401, Contemp. Math., 186, Amer. Math. Soc., Providence, RI, 1995.

[56] S. Nakajima, p-ranks and automorphism groups of algebraic curves, Trans. Amer. Math. Soc. 303 (1987), 595–607.

[57] S. Nakajima, On abelian automorphism groups of algebraic curves, J. London Math. Soc. (2) 36 (1987), 23–32.

[58] M. Neubauer, On monodromy groups of fixed genus, J. Algebra 153 (1992), 215–261.

[59] M. Neubauer, On primitive monodromy groups of genus zero and one. I. Comm. Algebra 21 (1993), 711–746.

[60] M. Raynaud, Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar, Invent. Math. 116 (1994), 425–462.

[61] J.-P. Serre, Local fields. Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.

[62] Shih, T., A note on groups of genus zero, Comm. in Alg. 19 (1991), 2813–2826.

[63] K. Stevenson, Galois groups of unramified covers of projective curves in characteristic p, J. Algebra 182 (1996), 770–804.

[64] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe, Arch. Math. (Basel) 24 (1973), 527–544.

[65] H. Stichtenoth, Algebraic function fields and codes. Universitext. Springer-Verlag, Berlin, 1993.

[66] P. H. Tiep and A. Zalesskii, Minimal characters of the finite classical groups, Comm. Algebra 24 (1996), 2093–2167.

Robert Guralnick
Department of Mathematics
University of Southern California
Los Angeles, CA 90089-1113
United States
guralnic@math.usc.edu