CAMBRIDGE

Cambridge University Press
978-0-521-17457-2 - Galois Groups and Fundamental Groups
Edited by Leila Schneps
Excerpt
More information

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.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-17457-2 - Galois Groups and Fundamental Groups
Edited by Leila Schneps
Excerpt
More information

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-17457-2 - Galois Groups and Fundamental Groups
Edited by Leila Schneps
Excerpt
More information

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 this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-17457-2 - Galois Groups and Fundamental Groups
Edited by Leila Schneps
Excerpt
More information

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-17457-2 - Galois Groups and Fundamental Groups
Edited by Leila Schneps
Excerpt
More information

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 this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-17457-2 - Galois Groups and Fundamental Groups
Edited by Leila Schneps
Excerpt
More information

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

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-17457-2 - Galois Groups and Fundamental Groups
Edited by Leila Schneps
Excerpt
More information

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

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:*

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-17457-2 - Galois Groups and Fundamental Groups
Edited by Leila Schneps
Excerpt
More information

(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.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-17457-2 - Galois Groups and Fundamental Groups
Edited by Leila Schneps
Excerpt
More information

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 $N_G(X) \geq E$, $C_V(N_G(X)) = 0$.

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-17457-2 - Galois Groups and Fundamental Groups
Edited by Leila Schneps
Excerpt
More information

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.

© in this web service Cambridge University Press www.cambridge.org