PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 107, Number 1, September 1989

ON ABELIAN QUOTIENTS OF PRIMITIVE GROUPS

MICHAEL ASCHBACHER AND ROBERT M. GURALNICK

(Communicated by Warren J. Wong)

ABSTRACT. It is shown that if G is a primitive permutation group on a set of size n, then any abelian quotient of G has order at most n. This was motivated by a question in Galois theory. The field theoretic interpretation of the result is that if M/K is a minimal extension and L/K is an abelian extension contained in the normal closure of M, then the degree of L/K is at most the degree of M/K.

1. INTRODUCTION

In this note, we prove the following results:

Theorem 1. *Let G be a primitive permutation group on a set of finite order n. Then $|G: G'| \leq n$.*

Theorem 2. *Let G be a permutation group on a finite set of order n. Then $|G: G'| \leq 3^{n/3} \leq 2^{n-1}$.*

Theorem 3. *Let V be a finite dimensional vector space over a finite field of characteristic ℓ and G a subgroup of $\mathrm{GL}(V)$. If $O_\ell(G) = 1$, then $|G: G'| < |V|$.*

Theorem 1 answers a question of Tamagawa, which was prompted by [I]. A minor modification of the argument in [I] shows that $|G: G'(H \cap H^g)| \leq |G: H|$. This was first observed by D. Cantor in the following form: If α and β are conjugate over a field K, then any abelian extension L/K with $L \subset K(\alpha, \beta)$ satisfies $|L: K| \leq |K(\alpha): K|$. The field theoretic version of Theorem 1 is:

Corollary 4. *Let K be a field with M/K a minimal extension. If L/K is an abelian extension with L contained in the normal closure of M, then $|L: K| \leq |M: K|$.*

Theorems 2 and 3 are needed to prove Theorem 1. Theorem 3 depends on the classification of simple groups (one needs to know the relative sizes of outer

Received by the editors November 10, 1988 and, in revised form, February 8, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20B15; Secondary 20C20, 20B05.
Both authors were partially supported by NSF grants. The first author was partially supported by NSA.

0002-9939/89 $1.00 + $.25 per page

automorphism groups, degrees of permutation representations, and dimensions of modules). See also [KP] in regard to Theorem 2.

It is not very difficult to see that primitive cannot be replaced by transitive in Theorem 1. We shall give an example to show that the bound in Theorem 2 is not too far off even in the transitive case.

2. Transitive groups

(2.1). *Let G be a group, $\pi: G \to A$ a homomorphism, and $K = \ker \pi$. Suppose $H = M \leq G$. Then*

$$|H: [M, H]| = |H\pi: [M, H]\pi||H \cap K: [M, H] \cap K|.$$

Proof. First $[M\pi, H\pi] = [M, H]\pi \cong [M, H]K/K$. Therefore, $H\pi/[M\pi, H\pi] \cong HK/[M, H]K \cong H/(H \cap [M, H]K) = H/[M, H](H \cap K)$. Then as $|H: [M, H]| = |H: (H \cap K)[M, H]||(H \cap K)[M, H]: [M, H]|$, it remains only to observe that $(H \cap K)[M, H]/[M, H] \cong (H \cap K)/[M, H] \cap K)$.

(2.2). *Let $\pi: G \to A$ be a surjective group homomorphism and $K = \operatorname{Ker} \pi$. Then $|G: G'| = |A: A'||K \cap G'| \leq |A: A'||K: K'|$.*

Proof. Apply (2.1) with $G = M = H$.

Theorem 2.3. *Let G be a group of permutations on a set X of order n. Then*

(a) $|G: G'| \leq 3^{n/3} \leq 2^{n-1}$, *and*

(b) $|G: G'| \leq p^{n/p}$ *for G a p-group.*

The proof is by induction on $|G|$. So assume G is a minimal counterexample to (a) or (b).

(2.4). *G is nilpotent.*

Proof. If not, choose M maximal in G with $G = MG'$. Then $|G: G'| = |M: M \cap G'| \leq |M: M'| \leq 3^{n/3}$ by induction.

(2.5). *G is transitive on X.*

Proof. If G acts on a proper subset Y of X with $0 \neq m = |Y| < n$, then apply (2.2) with π the representation of G on Y to obtain $|G: G'| \leq 3^{m/3}3^{(n-m)/3} = 3^{n/3}$. Similarly, if G is a p-group, we see that G is transitive.

(2.6). *G is a p-group for some prime p.*

Proof. If not then $G = P \times Q$ where P is a p-group and Q is a p'-group. Let $H = G_x$ be the stabilizer of x in X. Then $H = M \times N$ with $M = H \cap P$ and $N = H \cap Q$. Note that P acts faithfully on the cosets of M as does Q on the cosets of N. So

$$|G: G'| = |P: P'||Q: Q'| \leq 3^{a/3}3^{b/3} \leq 3^{n/3},$$

where $a = |P: M|$ and $b = |Q: N|$.

Proof of Theorem 2.3. By (2.6) and the fact that $p^{n/p} \leq 3^{n/3}$ for p a prime, it suffices to prove (2.3b). So G is a transitive p-group. Let Z be a central

subgroup of order p. If $G = Z$, then $n = p = |G: G'|$. Otherwise G acts transitively on the set Y of orbits of Z. Note $|Y| = n/p$. Let π be the representation of G as a permutation group on these orbits. By (2.2) and induction, $|G: G'| \leq p^{n/p^2}|K: K \cap G'|$, where $K = \operatorname{Ker}\pi$. Choose $g \in G$ with no fixed points on Y. Then $|K: K \cap G'| \leq |K: [g, K]| \leq |C_K(g)| \leq p^{n/p^2}$. Hence $|G: G'| \leq p^{2n/p^2} \leq p^{n/p}$.

By considering elementary abelian 3-subgroups of S_n, we see that (2.3b) cannot be improved.

We use the classification of finite simple groups in the following form:

Lemma 2.7. *Let L be a finite nonabelian simple group and M a proper subgroup of L with $|L: M| = k$.*

(i) *If $L \neq A_6$, then $2|\operatorname{Out} L| < k$.*
(ii) $4|\operatorname{Out} L| < |L|$.
(iii) *If $L \leq \mathrm{PSL}_d(q)$, then $2|\operatorname{Out} L| < q^d/(q-1)$.*

Proof. This follows easily by inspection. Note (ii) and (iii) follow from (i).

Proposition 2.8. *Let G be a primitive permutation group of degree n on a set X. Then either*

(i) $|G: G'| < n/2$, *or*
(ii) *G preserves an affine structure on X.*

Proof. Assume (2) does not hold. First consider the case where $F^*(G) = D = L_1 \times \cdots \times L_r$ is the product of r nonabelian simple groups L_i permuted transitively by G. It follows by [AS, Theorem 1] that either $n = k^r$ for $k = |L_1: M|$ for some proper subgroup M of L_1 or that $n = \ell^s \geq \ell^{r/2}$ where $\ell = |L_1|$ and $r \geq 2$. Let $K = \bigcap_i N_G(L_i)$. By Theorem 2, $|G: G'K| \leq 2^{r-1}$. Moreover, $K/D \leq \operatorname{Out} L_1 \times \cdots \times \operatorname{Out} L_r$. If $r = 1$, then $|G: G'| \leq |\operatorname{Out} L_1| < k/2$ by 2.7(i) unless $L_1 = A_6$. If $L_1 = A_6$, then either $k = 6$ and $|G: G'| \leq 2$ or $k > 8$ and $[G: G'] \leq 4$. If $r > 1$, then (3.1) implies $|K/D: [G, K/D]| \leq |\operatorname{Out} L_1|^{r/2}$. Thus $|G: G'| = |G: G'K||K: K \cap G'| \leq 2^{r-1}|\operatorname{Out} L_1|^{r/2}$. If $n = k^r$, then 2.7(i) implies $|G: G'| < n/2$. If $n = \ell^s$, $s \leq r/2$, then $|G: G'| \leq (4|\operatorname{Out} L|)^{r/2}/2 < n/2$ by 2.7(ii).

By [AS], the only case left is when $F^*(G) = Q = R \times D$, where $R \cong D$ and D is as above. Moreover, if H is a point stabilizer, then $G = HD$ and $H \cap Q = \{(x, \lambda(x)) | x \in R\}$ for some isomorphism λ of R and D. In particular, $n = |D| = \ell^r$ where $l = |L_1|$. Arguing as above, we see that $|G: G'| \leq \ell^{r/2}/2 < n/2$.

3. Induced modules

(3.1). *Let* $X = X_1 \times \cdots \times X_m$, $m > 1$, *be the direct product of finite groups* X_i *permuted transitively by* G. *If* V *is a* G*-invariant subgroup of* X, *then* $|V: [G, V]| \leq |X|^{1/2}$.

Proof. Choose $g \in G$ that leaves no X_i invariant. Then $|C_X(g)| \leq |X|^{1/2}$. Hence $|V: [G, V]| \leq |V: [g, V]| \leq |C_V(g)| \leq |C_X(g)| \leq |X|^{1/2}$.

(3.2). *Let* F *be a finite field of order* q *and* G *the group of maps* $\tau(a, \sigma)\colon x \to a(x\sigma)$ *on* F, *where* $a \in F^{\#}$ *and* $\sigma \in \operatorname{Aut} F$. *Let* $B = \{\tau(a, 1) | a \in F^{\#}\}$ *and* $H \leq G$. *Then either*

(1) $|H: H'| \leq q/2$, *or*

(2) $H = B$ *has order* $q - 1$.

Proof. If $H \leq B$, the result is clear. So assume not. Then $e = |H: H \cap B| > 1$. Hence $q = r^e$ and $H = \langle \alpha, h \rangle$, where $\langle h \rangle = H \cap B$ and $\alpha(x) = ax^r$ for some $a \in F^{\#}$. Then $|C_B(\alpha)| = r - 1$. Thus $|H: H'| = |H: H \cap B||H \cap B: H'| = e|C_{H \cap B}(\alpha)| \leq e(r - 1) \leq q/2$.

4. Linear actions

In this section F is a finite field of characteristic l, V is a finite dimensional vector space over F, and $G \leq \mathrm{GL}(V)$. We prove:

Theorem 4.1. *Assume* $O_l(G) = 1$. *Then either*:

(a) $|G: G'| \leq |V|/2$, *or*

(b) G *is abelian and* $|G| < |V|$.

Let (G, V) be a minimal counterexample to (4.1). Clearly G is nonabelian.

(4.2). G *acts irreducibly on* V.

Proof. If not, choose $0 = V_0 < V_1 < \cdots < V_d = V$ with V_i G-invariant and $W_i = V_i/V_{i-1}$ G-irreducible. Since $O_l(G) = 1$, G acts faithfully on $W = W_1 \oplus \cdots \oplus W_d$. So we can assume V is a semisimple module. Since G is nonabelian, there exists an irreducible submodule U such that $\pi(G)$ is nonabelian, where π is the representation of G on U. Thus if $K = \ker \pi$, $|G: G'K| < |U|/2$. Since $O_l(K) = 1$, K acts faithfully on V/U. So by minimality, $|K: K'| \leq |V/U|$, whence $|G: G'| \leq |V|/2$.

(4.3). G *is primitive on* V.

Proof. If not, there is a nontrivial decomposition $V = \bigoplus_i V_i$ with G permuting $X = \{V_1, \ldots, V_r\}$ and $N_G(V_1)$ acting primitively on V_1. Let π be the permutation representation of G on X and $K = \ker \pi$. Set $K_0 = K$ and $K_{i+1} = \{g \in K_i | g \text{ acts trivially on } V_{i+1}\}$. By (2.2), $|G: G'| = k_0 k_1 \ldots k_r$, where $k_0 = |G: G'K|$ and $k_i = |K_{i-1}: (K_{i-1} \cap G')K_i| \leq |K_{i-1}: K'_{i-1}K_i|$ for $i \geq 1$. By Theorem 2, $k_0 \leq 2^{r-1}$.

Since $N_G(V_i)$ acts primitively on V_i and $K \trianglelefteq N_G(V_i)$, K acts homogeneously on each V_i. If K is not irreducible on V_1 (and so not on each V_i), then $k_i \leq |K_{i-1}: K'_{i-1}| < |W| \leq |V_i|/2$, where W is a K-irreducible subspace of V_1. Thus $|G: G'| < 2^{r-1}(|V|/2)^r = |V|/2$.

So assume K acts irreducibly on V_i. If K_{i-1}/K_i is not abelian for each i, then $k_i \leq |K_{i-1}: K'_{i-1}K_i| \leq |V_i|/2$ by induction, and $|G: G'| \leq |V|/2$ as above. So we can assume some K_{i-1}/K_i is abelian. Then $|K_{i-1}/K_i| < |V_i|$, whence $|K_{i-1}: (K_{i-1} \cap G')K_i| \leq |V_i|/2$ unless $K_{i-1} \cap G' \leq K_i$. Since K acts irreducibly on V_i and $K_{i-1} \trianglelefteq K$, this can happen only if K_{i-1}/K_i is cyclic of order $|V_i| - 1$ and $[K, K_{i-1}] \leq K_i$, whence K is abelian. If K is abelian, then $|K| \leq (|V_1| - 1)^r$, and so by (3.1), $|K: [G, K]| \leq |K|^{1/2}$. Thus $|G: G'| \leq 2^{r-1}(|V_1| - 1)^{r/2} < |V|/2$.

(4.4). *If $D \trianglelefteq G$, then D acts homogeneously. In particular, if D is abelian, then D is cyclic.*

Proof. Apply (4.3).

(4.5). *If D is a noncyclic normal subgroup of G, then D acts irreducibly on V and $C_G(D)$ is cyclic.*

Proof. By (4.4), D acts homogeneously. So assume $V = V_1 \oplus \cdots \oplus V_m$, $V_i \cong V_j$ as irreducible D-modules. Let $E = \mathrm{End}_{FD} V_1$ with $q = |E|$ and $m > 1$. Set $U = V_1$. Let $\alpha: D \to \mathrm{GL}(U)$ be the representation of D on U. Let Γ be the normalizer of $D\alpha$ in $\mathrm{GL}(U)$ and S the centralizer of $D\alpha$. Since $gV_1 \cong V_1$ as FD-modules for each $g \in G$, we can define $\pi: G \to \Gamma/S$ by $g\pi = Sx$ where $\alpha(g^{-1}hg) = x^{-1}\alpha(h)x$. Note $K = \ker \pi = C_G(D)$. Let M be the inverse image of $G\pi$ in $\Gamma \leq \mathrm{GL}(U)$. Since M contains a copy of D, M is nonabelian and so by minimality, $|G: G'K| \leq |M: M'| \leq |U|/2$. Since $K = C_G(D)$, there exists a faithful representation $\beta: K \to \mathrm{GL}_m(E)$. By minimality, $|K: K'| < q^m$. Thus $|G: G'| < |U|q^m/2 \leq |U|q^{2m-2}/2 \leq |U|^m/2 = |V|/2$.

Let T be a maximal normal cyclic subgroup of G.

(4.6). $T \neq C_G(T)$.

Proof. If so, then (3.2) applies.

Now choose D minimal subject to $D \leq C_G(T)$, $D \trianglelefteq G$, and D is nonabelian. Thus by (4.4), (4.5), and the maximality of T:

(4.7). *$Z(D)$ is the largest characteristic abelian subgroup of D, $Z(D)$ is cyclic, D acts irreducibly on V, and $T = C_G(D)$.*

(4.8). *Either*

(1) *D is the central product of quasisimple subgroups $L_1, \ldots, L_r$ permuted transitively by G, or*

(2) $D = PZ(D)$ *with* $|P| = p^{1+2w}$ *and* P *an extraspecial* p*-group and either* $Z(D) = Z(P)$ *or* $p = 2$ *and* $Z(D) \cong Z_4$. *Moreover,* G *is irreducible on* $\tilde{D} = D/Z(D)$.

Proof. This follows from (4.7) and the minimal choice of D.

(4.9). (4.8.2) *holds.*

Proof. Assume (4.8.1) holds. Let $X = \{L_1, \ldots, L_r\}$, π the permutation representation of G on X and $K = \ker \pi$. By (4.5), D acts irreducibly on V. Let $E = \mathrm{End}_D V$ and set $q = |E|$. Since V is absolutely irreducible over E, $V = V_1 \otimes_E \cdots \otimes_E V_r$ where V_i is an absolutely irreducible $\hat{L}_i$-module (where $\hat{L}_i$ is the covering group of L_i). Let $d = \dim_E V_i$. Then $|V| = q^{d^r}$ and $\mathrm{End}_{L_1} V_1 = E$. By Lemma 2.7(iii), $2k < q^d/(q-1)$, where $k = |\mathrm{Out}\, L_1|$. In particular, $(2k)^r(q-1) < q^{d^r} = |V|$. Since $T = C_G(D)$ by (4.7), it follows that $|T| < q$ and that $|K : K'(T \cap K)| \leq k^r$. By Theorem 2, $|G : G'K| \leq 2^{r-1}$. Thus

$$|G : G'| \leq 2^{r-1}k^r(q-1) = (2k)^r(q-1)/2 < |V|/2.$$

(4.10). *Let* $q = |\mathrm{End}_D V|$. *Then* $q > |C_G(D)|$, $|V| \geq q^{p^w}$, *and* $q \equiv 1 \bmod p$.

Proof. Clearly $q > |T|$. Since V is a faithful D-module, the second inequality holds. Since $\mathrm{Aut}_P V \geq Z(D)$, $q \equiv 1 \bmod p$.

(4.11). $C_G(\tilde{D}) = DC_G(D)$.

Proof. Any automorphism of D which is trivial on $\tilde{D}$ must be inner.

Proof of Theorem 4.1. Now G acts irreducibly on $\tilde{D}$. Since $D \leq G'Z(D)$, it follows by the minimality of (G, V) that $|G : G'C_G(\tilde{D})| < |\tilde{D}|$. Thus $|G : G'| < |\tilde{D}||C_G(D) : C_G(D) \cap G'| \leq p^{2w}(q-1)/p < q^{p^w}/2 \leq |V|/2$ unless $q = 3$, $p = 2$, $w = 1$, and $|V| = 9$. The result follows by inspection in this case.

5. Primitive groups

In this section we prove the following result:

Theorem 1. *Let* G *be a primitive group of permutations on a set* X *of order* n. *Then* $|G : G'| \leq n$.

The proof is by induction on n. So choose a counterexample with n minimal. By (2.7):

(5.1). G *preserves an affine space structure on* X.

By (5.1) $F^*(G) = V$ is an m-dimensional vector space over $F = \mathrm{GF}(p)$ for some prime p, with V regular on X and $G = HV$, where $H = G_x$ is the stabilizer of some $x \in X$ and H is an irreducible subgroup of $\mathrm{GL}(V)$. Then $n = |V|$. We can assume $H \neq 1$. Also as H is irreducible on V, $V = [V, H] \leq G'$. So $|G : G'| = |H : H'|$. Finally by Theorem 3, $|H : H'| < |V|$. This contradiction completes the proof of Theorem 1.

Note that in fact one has the slightly stronger result that either $|G: G'| \leq n/2$ or G' is abelian and G/G' is cyclic.

6. Transitive subgroups II

We would like to know whether the bound in Theorem 2.3 is a good one for transitive subgroups. Observe that the proof of (2.3) actually shows:

(6.1). *If P is a p-group acting transitively on a set X of size p^a, $a \geq 3$, then $|P: P'| \leq p^{g(a)}$, where $g(a) = 2 + p + p^2 + \cdots + p^{a-2} = 1 + (p^{a-1} - 1)/(p-1)$.*

Thus for p large, $|P: P'|$ cannot be much larger than p^{n/p^2}. So we shall look for a 2-group for an example.

Let E be an elementary abelian group of order 2^d. Let $X = \mathbf{Z}_2[E]$ as an E-module. Then X has a filtration $X = X_0 \geq X_1 \geq X_2 \geq \cdots \geq X_d = 0$, such that $(g-1)X_i \leq X_{i+1}$ for all $g \in E$. Moreover, $\dim X_i/X_{i-1} = \binom{d}{i}$. For convenience let us assume $d = 2f$ is even.

Set $V = X_f$ and $G = VE$. Note that $G \leq XE \cong \mathbf{Z}_2 wr E \leq S_n$, $n = 2^{d+1}$, and that G acts transitively. Also

$$|G: G'| = |G: V||V: [G, V]| = 2^{d+\binom{d}{f}}.$$

Since $\binom{d}{f}$ is the largest of the binomial coefficients, it is clear that $\binom{d}{f} \geq 2^d/(d+1) = n/(2\log_2 n)$. Thus we have shown:

(6.2). *If n is an odd power of 2, there exists a transitive 2-group G of degree n such that $|G: G'| \geq 2^{n/2\log_2 n}$.*

If one uses a better approximation for the binomial coefficient, the $\log_2 n$ can be replaced by $(\log_2 n)^{1/2}$ for n sufficiently large. See also [A] and [KN] for similar examples.

References

[A] M. S. Audu, *Transitive permutation groups of prime-power order*, Ph. D. Thesis, Oxford, 1983.

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

[KN] L. G. Kovacs and M. F. Newman, *Generating transitive permutation groups*, Quart J. Math Oxford (2) **39** (1988), 361–372.

[KP] L. Kovacs and C. Praeger, *Finite permutation groups with large abelian quotients*, Pacific J. Math., **136** (1989), 283–292.

[I] I. M. Isaacs, *Solution of problem* 6523, Amer. Math. Monthly **95** (1988), 561–562.

Department of Mathematics, California Institute of Technology, Pasadena, California 91125

Department of Mathematics, University of Southern California, Los Angeles, California 90089