Pacific Journal of Mathematics

GROUPS WHICH HAVE A FAITHFUL REPRESENTATION OF DEGREE LESS THAN $(p-1/2)$

WALTER FEIT AND JOHN GRIGGS THOMPSON

Vol. 11, No. 4 1961

GROUPS WHICH HAVE A FAITHFUL REPRESENTATION OF DEGREE LESS THAN $(p - 1/2)$

WALTER FEIT AND JOHN G. THOMPSON

1. Introduction. Let G be a finite group which has a faithful representation over the complex numbers of degree n. H. F. Blichfeldt has shown that if p is a prime such that $p > (2n + 1)(n - 1)$, then the Sylow p-group of G is an abelian normal subgroup of G [1]. The purpose of this paper is to prove the following refinement of Blichfeldt's result.

THEOREM 1. *Let p be a prime. If the finite group G has a faithful representation of degree n over the complex numbers and if $p > 2n + 1$, then the Sylow p-subgroup of G is an abelian normal subgroup of G.*

Using the powerful methods of the theory of modular characters which he developed, R. Brauer was able to prove Theorem 1 in case p^2 does not divide the order of G [2]. In case G is a solvable group, N. Ito proved Theorem 1 [4]. We will use these results in our proof.

Since the group $SL(2, p)$ has a representation of degree $n = (p - 1)/2$, the inequality in Theorem 1 is the best possible.

It is easily seen that the following result is equivalent to Theorem 1.

THEOREM 2. *Let A, B be n by n matrices over the complex numbers. If $A^r = I = B^s$, where every prime divisor of rs is strictly greater than $2n + 1$, then either $AB = BA$ or the group generated by A and B is infinite.*

For any subset S of a group G, $C_G(S)$, $N_G(S)$, $|S|$ will mean respectively the centralizer, normalizer and number of elements in S. For any complex valued functions ζ, ξ on G we define

$$(\zeta, \xi)_G = \frac{1}{|G|} \sum_G \zeta(x)\overline{\xi(x)} ,$$

and $\| \zeta \|_G^2 = (\zeta, \zeta)_G$. Whenever it is clear from the context which group is involved, the subscript G will be omitted. $H \lhd G$ will mean that H is a normal subgroup of G. For any two subsets A, B of G, $A - B$ will denote the set of all elements in A which are not in B. If a subgroup of a group is the kernel of a representation, then we will also say that it is the kernel of the character of the given representation. All groups

Received November 25, 1960. The first author was partly supported by O. O. R. and an NSF Grant. The second author was partly supported by the Esso Research Foundation.

considered are assumed to be finite.

2. Proof of Theorem 1. We will first prove the following preliminary result.

LEMMA 1. *Assume that the Sylow p-group P of N is a normal subgroup of N. If x is any element of N such that $C_N(x) \cap P = \{1\}$, then $\lambda(x) = 0$ for any irreducible character λ of N which does not contain P in its kernel.*

Proof. Since $|C_N(x)|$ is not divisible by p, it is easily seen that $C_N(x)$ is mapped isomorphically into $C_{N/P}(\bar{x})$, where $\bar{x}$ denotes the image of x in N/P under the natural projection. Let $\mu_1, \mu_2, \cdots$ be all the irreducible characters of N which contain P in their kernel and let $\lambda_1, \lambda_2, \cdots$ be all the other irreducible characters of N. The orthogonality relations yield that

$$\sum_i |\mu_i(x)|^2 = |C_{N/P}(\bar{x})| \geqq |C_N(x)| = \sum_i |\mu_i(x)|^2 + \sum_i |\lambda_i(x)|^2 .$$

This implies the required result.

From now assume that G is a counter example to Theorem 1 of minimal order. We will show that p^2 does not divide $|G|$, then Brauer's theorem may be applied to complete the proof. The proof is given in a series of short steps.

Clearly every subgroup of G satisfies the assumption of Theorem 1, hence we have

(I) *The Sylow p-group of any proper subgroup H of G is an abelian normal subgroup of H.*

Let P be a fixed Sylow p-group of G. Let Z be the center of G.

(II) *P is abelian.*

As P has a faithful representation of degree $n < p$, each irreducible constituent of this representation has degree one. Therefore in completely reduced form, the representation of P consists of diagonal matrices. Consequently these matrices form an abelian group which is isomorphic to P.

(III) *G contains no proper normal subgroup whose index in G is a power of p.*

Suppose this is false. Let H be a normal subgroup of G of minimum

order such that $[G:H]$ is a power of p. Let P_0 be a Sylow p-group of H. By (I) $P_0 \lhd H$, hence $P_0 \lhd G$. Thus $C_G(P_0) \lhd G$. If $C_G(P_0) \neq G$, then by (I) and (II), $P \lhd C_G(P_0)$, thus $P \lhd G$ contrary to assumption. Therefore $C_G(P_0) = G$. Burnside's Theorem ([3], p. 203) implies that H contains a normal p-complement which must necessarily be normal in G. The minimal nature of H now yields that p does not divide $|H|$.

If q is any prime dividing $|H|$, then it is a well known consequence of the Sylow theorems that it is possible to find a Sylow q-group Q of H such that $P \subseteqq N(Q)$. Hence PQ is a solvable group which satisfies the hypotheses of Theorem 1. Ito's Theorem [4] now implies that $P \lhd PQ$, thus $Q \subseteqq N(P)$. As q was an arbitrary prime dividing $|H|$, we get that $|H|$ divides $|N(P)|$. Consequently $N(P) = G$, contrary to assumption.

(IV) *Z is the unique maximal normal subgroup of G. G/Z is a non-cyclic simple group. $|Z|$ is not divisible by p.*

Let H be a maximal normal subgroup of G, hence G/H is simple. Let P_0 be a Sylow p-group of H. Then by (I) $P_0 \lhd H$, hence $P_0 \lhd G$, thus $C(P_0) \lhd G$. If $C(P_0) \neq G$, then by (I) and (II) $P \lhd C(P_0)$, hence $P \lhd G$ contrary to assumption. Therefore $C(P_0) = G$. If $P_0 \neq \{1\}$, then it is a simple consequence of Grün's Theorem ([3], p. 214) that G contains a proper normal subgroup whose index is a power p. This contradicts (III). Hence $P_0 = \{1\}$ and p does not divide $|H|$.

By (III) $PH \neq G$, hence by (I) $P \lhd PH$. Consequently $PH = P \times H$, and $P \subseteqq C(H) \lhd G$. If $C(H) \neq G$, then (I) yields that $P \lhd C(H)$. Hence once again $P \lhd G$, contrary to assumption. Consequently $C(H) = G$. Therefore $H \subseteqq Z$. As G is not solvable, neither is G/H. Now the maximal nature of H yields that $H = Z$ and suffices to complete the proof.

(V) $P \cap xPx^{-1} = \{1\}$ *unless* x *is in* $N(P)$.

Let $D = P \cap xPx^{-1}$ be a maximal intersection of Sylow p-groups of G. Then P is not normal in $N(D)$. Hence by (I) $N(D) = G$, or $D \lhd G$. However (IV) now implies that $D \subseteqq Z$. Hence (IV) also yields that $D = \{1\}$ as was to be shown.

Define the subset N_0 of $N(P)$ by

$$N_0 = \{x \mid x \in N(P),\ C(x) \cap P \neq \{1\}\}\ .$$

Clearly $\{P, Z\} \subseteqq N_0$.

(VI) $N(N_0) = N(P)$. $(N_0 - Z) \cap x(N_0 - Z)x^{-1}$ *is empty unless* $x \in N(P)$.

Clearly $N(P) \subseteqq N(N_0)$. Since P consists of all elements in N_0 whose

order is a power of p, it follows that $N(N_0) \subseteqq N(P)$.

Suppose $y \in (N_0 - Z) \cap x(N_0 - Z)x^{-1}$. Then y and $x^{-1}yx$ are both contained in $(N_0 - Z)$. Let $P_0 = C(y) \cap P$, $P_1 = C(x^{-1}yx) \cap P$. By assumption $P_0 \neq \{1\} \neq P_1$. It follows from the definitions that P_0 and xP_1x^{-1} are both contained in $C(y)$. Since y is not in Z, $C(y) \neq G$. Hence (I) yields that P_0 and xP_1x^{-1} generate a p-group. Thus by (II) $xP_1x^{-1} \subseteqq C(P_0)$. Now (V) implies that $xP_1x^{-1} \subseteqq N(P)$. Consequently $xP_1x^{-1} \subseteqq P$. By (V), this yields that $x \in N(P)$ as was to be shown.

From now on we will use the following notation:

$$|P| = p^e\,, \quad |Z| = z\,, \quad |N(P)| = p^e z t\,.$$

Let $\chi_0 = 1, \chi_1, \cdots$ be all the irreducible characters of G. Define α_i, β_i, b_i by

$$\chi_{i|N(P)} = \alpha_i + \beta_i\,, \qquad b_i = \beta_i(1)$$

where α_i is a sum of irreducible characters of $N(P)$, none of which contain P in their kernel and β_i is a character of $N(P)$ which contains P in its kernel.

(VII) *If* $i \neq 0$, *then* $b_i < (1/p^{e/2})\ \chi_i(1)$.

By (VI) $(N_0 - Z)$ has $|G|/p^e zt$ distinct conjugates and no two of them have any elements in common. Since χ_i is a class function on G, this yields that

$$\begin{aligned} 1 = \|\chi_i\|^2 &> \frac{1}{|G|}\frac{|G|}{p^e zt}\,\Sigma_{(N_0-Z)}\,|\chi_i(x)|^2 \\ &= \frac{1}{p^e zt}\,\{-\Sigma_Z\,|\chi_i(x)|^2 + \Sigma_{N_0}\,|\alpha_i(x) + \beta_i(x)|^2\}\,. \end{aligned}$$

If $x \in Z$, then $|\chi_i(x)|^2 = |\chi_i(1)|^2$. As $P \subseteqq N_0$, we get that

$$1 > \frac{1}{p^e zt}\,[-|\chi_i(1)|^2 z + \Sigma_{N_0}\{|\alpha_i(x)|^2 + \alpha_i(x)\overline{\beta_i(x)} + \overline{\alpha_i(x)}\beta_i(x)\} + \Sigma_{PZ}|\beta_i(x)|^2]\,.$$

Since P is in the kernel of β_i, we get that $|\beta_i(x)| = b_i$ for $x \in PZ$. Lemma 1 implies that α vanishes on $N(P) - N_0$. Hence

$$1 > \frac{-|\chi_i(1)|^2}{p^e t} + \|\alpha_i\|^2_{N(P)} + (\alpha_i, \beta_i)_{N(P)} + \overline{(\alpha_i, \beta_i)}_{N(P)} + \frac{b_i^2}{t}\,.$$

By definition $(\alpha_i, \beta_i) = 0$, hence

$$\frac{|\chi_i(1)|^2}{p^e t} > \|\alpha_i\|^2_{N(P)} - 1 + \frac{b_i^2}{t}\,.$$

By (IV) the normal subgroup generated by P is all of G, hence $\alpha_i \neq 0$.

Therefore $\| \alpha_i \|^2_{N(P)} \geqq 1$. This finally yields that

$$\frac{|\chi_i(1)|^2}{p^e t} > \frac{b_i^2}{t},$$

which is equivalent to the statement to be proved.

(VIII) *If Γ is the character of G induced by the trivial character 1_P of P, then $(\Gamma, \chi_i) = b_i$.*

If λ is an irreducible character of $N(P)$ which does not contain P in its kernel, then λ is not a constituent of the character of $N(P)$ induced by 1_P. Hence by the Frobenius reciprocity theorem $(\lambda_{|P}, 1_P)_P = 0$. Consequently $(\alpha_{i|P}, 1_P)_P = 0$. The Frobenius reciprocity theorem now implies that

$$(\chi_i, \Gamma) = (\chi_{i|P}, 1_P)_P = (\beta_{i|P}, 1_P) = b_i .$$

From now on let χ be an irreducible character of minimum degree greater than one. Define the integers a_i by

$$a_i = (\chi_i, \chi\bar{\chi}) .$$

(IX) $\chi(1) - 1 \leqq \sum_{i \neq 0} a_i b_i$.

By (VIII)

$$a_0 b_0 + \sum_{i \neq 0} a_i b_i = (\Gamma, \chi\bar{\chi}) = \frac{\chi(1)^2}{p^e} + \frac{1}{p^e zt} \Sigma_{P-\{1\}} zt\chi\bar{\chi}(x)$$

$$= \frac{1}{p^e} \Sigma_P \chi\bar{\chi}(x) = \| \chi_{|P} \|^2_P .$$

By (II), $\chi_{|P}$ is a sum of $\chi(1)$ linear characters of P. Consequently

$$a_0 b_0 + \sum_{i \neq 0} a_i b_i \geqq \chi(1) .$$

As χ is irreducible, $a_0 = 1$. Clearly $b_0 = 1$. This yields the desired inequality.

We will now complete the proof of Theorem 1.

It follows from (IX) that

$$\chi(1) - 1 \leqq \sum_{i \neq 0} a_i b_i .$$

(VII) yields that

$$\sum_{i \neq 0} a_i b_i < \frac{1}{p^{e/2}} \sum_{i \neq 0} a_i \chi_i(1) .$$

The definition of the integers a_i implies that

$$\sum_{i \neq 0} a_i \chi_i(1) = \chi(1)^2 - 1 .$$

Combining these inequalities we get that

$$\chi(1) - 1 < \frac{\chi(1)^2 - 1}{p^{e/2}} ,$$

or

$$p^{e/2} < \chi(1) + 1 .$$

By assumption $\chi(1) < (p - 1)/2$, hence

$$p^{e/2} < \chi(1) + 1 < p .$$

This implies that $e < 2$. Thus $e \leqq 1$.

R. Brauer's theorem [2] now yields that $P \lhd G$ contrary to assumption. This completes the proof of Theorem 1.

BIBLIOGRAPHY

1. H. F. Blichfeldt, *On the order of linear homogeneous groups*, Trans. Amer. Math. Soc., **4** (1903), 387-397.
2. R. Brauer, *On groups whose order contains a prime number to the first power* II, Amer. J. of Math., **64** (1942), 421-440.
3. M. Hall, *The Theory of Groups*, The MacMillan Company, New York, 1959.
4. N. Ito, *On a theorem of H. F. Blichfeldt*, Nagoya Math. J., **5** (1954), 75-77.

CORNELL UNIVERSITY AND THE UNIVERSITY OF CHICAGO
HARVARD UNIVERSITY AND THE UNIVERSITY OF CHICAGO

PACIFIC JOURNAL OF MATHEMATICS

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, L. J. Paige at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50. Back numbers are available. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Reprinted 1966 in the United States of America

Pacific Journal of Mathematics
Vol. 11, No. 4 , 1961

A. V. Balakrishnan, *Prediction theory for Markoff processes* 1171
Dallas O. Banks, *Upper bounds for the eigenvalues of some vibrating systems* 1183
A. Białynicki-Birula, *On the field of rational functions of algebraic groups* 1205
Thomas Andrew Brown, *Simple paths on convex polyhedra* 1211
L. Carlitz, *Some congruences for the Bell polynomials* 1215
Paul Civin, *Extensions of homomorphisms* 1223
Paul Joseph Cohen and Milton Lees, *Asymptotic decay of solutions of differential inequalities* 1235
István Fáry, *Self-intersection of a sphere on a complex quadric* 1251
Walter Feit and John Griggs Thompson, *Groups which have a faithful representation of degree less than* $(p-1/2)$ 1257
William James Firey, *Mean cross-section measures of harmonic means of convex bodies* 1263
Avner Friedman, *The wave equation for differential forms* 1267
Bernard Russel Gelbaum and Jesus Gil De Lamadrid, *Bases of tensor products of Banach spaces* 1281
Ronald Kay Getoor, *Infinitely divisible probabilities on the hyperbolic plane* 1287
Basil Gordon, *Sequences in groups with distinct partial products* 1309
Magnus R. Hestenes, *Relative self-adjoint operators in Hilbert space* 1315
Fu Cheng Hsiang, *On a theorem of Fejér* 1359
John McCormick Irwin and Elbert A. Walker, *On N-high subgroups of Abelian groups* 1363
John McCormick Irwin, *High subgroups of Abelian torsion groups* 1375
R. E. Johnson, *Quotient rings of rings with zero singular ideal* 1385
David G. Kendall and John Leonard Mott, *The asymptotic distribution of the time-to-escape for comets strongly bound to the solar system* 1393
Kurt Kreith, *The spectrum of singular self-adjoint elliptic operators* 1401
Lionello Lombardi, *The semicontinuity of the most general integral of the calculus of variations in non-parametric form* 1407
Albert W. Marshall and Ingram Olkin, *Game theoretic proof that Chebyshev inequalities are sharp* 1421
Wallace Smith Martindale, III, *Primitive algebras with involution* 1431
William H. Mills, *Decomposition of holomorphs* 1443
James Donald Monk, *On the representation theory for cylindric algebras* 1447
Shu-Teh Chen Moy, *A note on generalizations of Shannon-McMillan theorem* 1459
Donald Earl Myers, *An imbedding space for Schwartz distributions* 1467
John R. Myhill, *Category methods in recursion theory* 1479
Paul Adrian Nickel, *On extremal properties for annular radial and circular slit mappings of bordered Riemann surfaces* 1487
Edward Scott O'Keefe, *Primal clusters of two-element algebras* 1505
Nelson Onuchic, *Applications of the topological method of Ważewski to certain problems of asymptotic behavior in ordinary differential equations* 1511
Peter Perkins, *A theorem on regular matrices* 1529
Clinton M. Petty, *Centroid surfaces* 1535
Charles Andrew Swanson, *Asymptotic estimates for limit circle problems* 1549
Robert James Thompson, *On essential absolute continuity* 1561
Harold H. Johnson, *Correction to "Terminating prolongation procedures"* 1571