ON p-GROUPS OF CLASS THREE GENERATED BY THREE ELEMENTS[1,2]

J. R. BOEN

1. **Introduction.** Let $f(n, p)$ be the number of nonisomorphic groups of order p^n, p a prime. G. Higman [1, p. 24] has suggested that $f(n, p)$ has the following form: there exists a positive integer N and polynomials $f_i(p)$ with integer coefficients independent of p such that $f(n, p) = f_i$ for $p \equiv i \pmod{N}$. He has proved this for p-groups of Φ-class two [2]; the tables of p-groups show that it is correct for $n \leqq 5$. In this paper we shall be concerned with p-groups of exponent $p > 3$ of class three generated by three elements and shall refer to them as "groups of our class".

Let a, b, c be elements of a group, and let H, K, L be subgroups. Define

$$\begin{aligned}
(a, b) &= a^{-1}b^{-1}ab, \\
(a, b, c) &= ((a, b), c), \\
(H, K) &= \text{the subgroup generated by } \{(h, k) \mid h \in H, k \in K\}, \\
(H, H) &= H', \\
(H, K, L) &= ((H, K), L), \\
a^b &= b^{-1}ab.
\end{aligned}$$

We also need the easily-verified Witt identity,

$$(a, b^{-1}, c)^b(b, c^{-1}, a)^c(c, a^{-1}, b)^a = 1.$$

2. **The classification.**

THEOREM. *There is exactly one group of order p^{14} of our class and none of larger order. There are $p+7$ and $p+5$ groups of our class of order p^{13} for $p \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$, respectively.*

PROOF. The first part is straightforward. Let F be the free group on three generators and let R be the normal subgroup generated by all pth powers and elements of the forms $((x, y, w), z)$, $((x, y), (w, z))$ where $x, y, z, w \in F$. Clearly $F/R = G$ is a group of our class. A theorem

Presented to the Society, January 28, 1960; received by the editors December 5, 1960.

[1] We regret the error appearing in the abstract in Notices Amer. Math. Soc. vol. 6 (1959) pp. 817–818. The error was due to an oversight of the Witt identity.

[2] Partly supported by the National Science Foundation through the Summer Institute on Finite Groups, Pasadena, 1960.

of P. Hall [4, p. 56] and the formulae of Witt [3, p. 169] imply that G is of order p^{14}. More precisely, they imply that G/G', $G'/(G', G)$ and (G', G) are elementary abelian of orders p^3, p^3, and p^8, respectively. It follows easily that G is unique and is the only group of our class of order $>p^{13}$.

Let $G=\{u_1, u_2, u_3\}$ and define $s_1=(u_2, u_3)$, $s_2=(u_3, u_1)$, $s_3=(u_1, u_2)$, $t_{ij}=(s_j, u_i)$ for $i, j=1, 2, 3$. The t_{ij}'s are not independent, for the Witt identity implies that $t_{11}t_{22}t_{33}=1$. Since G is of class three, G is metabelian and (G', G) is central. In fact, it is easy to see that $(G', G)=Z$, the center of G.

Every group of our class is isomorphic to a quotient group of G. Define two subsets of G to be of equal type if they are conjugate under the automorphism group of G. We now argue that the task of classifying quotient groups of G of order p^{13} is equivalent to that of counting equal-type classes of normal subgroups of G of order p. Let H_1 and H_2 be two such subgroups. If $H_2=\alpha(H_1)$ where α is an automorphism of G, then clearly $G/H_1\cong G/H_2$. To show the converse, we notice first that H_1 and H_2 are central, since minimal normal subgroups of a p-group are central. Clearly H_1 and H_2 are in $\Phi(G)$, the Frattini subgroup of G. Since G is relatively free, i.e., the quotient group of a free group by a fully invariant subgroup, $G/H_1\cong G/H_2$ implies that $H_2=\alpha(H_1)$ for H_1, H_2 in $\Phi(G)$ [1].

The following characterizes the central cyclic kernels of equal type.

LEMMA. *Consider $A=(a_{ij})$, a 3-square matrix over $GF(p)$. Define the map ϕ: $A\to t=\prod_{i,j} t_{ij}^{a_{ij}}$. Let $t_1=\phi(A_1)$ and $t_2=\phi(A_2)$. Then $\{t_1\}$ and $\{t_2\}$ are of equal type if and only if there exist elements of $GF(p)$ $\rho\neq 0$, λ, and a matrix B such that $A_1=B(\rho A_2+\lambda I)B^{-1}$.*

PROOF. Recalling that G' is abelian and that the t_{ij}'s are central, the following identities may be verified.

(i) $(\prod u_i^{x_i}st, \prod u_i^{y_i}s't')=(\prod u_i^{x_i}, \prod u_i^{y_i})=\prod s_i^{z_i}t''$ where s, $s'\in G'$, t, t', $t''\in Z$ and $z_1=x_2y_3-x_3y_2$, $z_2=x_3y_1-x_1y_3$, $z_3=x_1y_2-x_2y_1$.

(ii) $(\prod s_i^{y_i}t, \prod u_i^{x_i}s't')=(\prod s_i^{y_i}, \prod u_i^{x_i})=\prod_{i,j} t_{ij}^{x_iy_j}$ where $s'\in G'$ and t, $t'\in Z$.

Let α be an automorphism of G and suppose $\alpha(u_1)=\prod u_i^{x_i}st$, $\alpha(u_2)=\prod u_i^{y_i}s't'$. Then (i) implies that $\alpha(s_1)=\prod s_i^{z_i}t''$ and (ii) implies that $\alpha(t_{11})=\prod_{i,j} t_{ij}^{x_iz_j}$. The other $\alpha(s_i)$'s and $\alpha(t_{ij})$'s are obtained similarly. Thus α induces an automorphism of Z which is completely determined by the automorphism α induces on G/G'.

Note that the cyclic subgroups of G/G' form a projective plane U over $GF(p)$ and that the cyclic subgroups of Z form a 7-dimensional

projective space T. Our problem thus becomes that of classifying points of T under collineations induced by collineations of U.

Let $\{\prod u_i^{x_i} \neq 1\}$ of G/G' correspond to the point $X=(x_1, x_2, x_3)$ of U and let $\{\prod s_i^{y_i} \neq 1\}$ of G/Z correspond to the line $Y=(y_1, y_2, y_3)$ of U. Choose $YX^T=0$ to be the incidence equation for points and lines of U and let the equation for the collineation matrix B acting on the points of U be $BX^T=(X')^T$. Then it is well known that the equation for B acting on the lines of U is $YB^{-1}=Y'$.

From (ii), $t \neq 1$ is a commutator if and only if $A=X^TY$ where $\phi(A)=t$; i.e., if and only if A is of rank one. If $A=X^TY$, then $A'=(X')^TY'=BX^TYB^{-1}=BAB^{-1}$. The similarity transformation is linear, however, so $A'=BAB^{-1}$ regardless of rank A. The Witt identity implies that the scalar matrices comprise the kernel of ϕ. Hence A and $\rho A+\lambda I(\rho \neq 0)$ represent the same point of T and the lemma follows. Q.E.D.

The remaining task is to find and count the canonical forms for the points of T. The method uses the fact that A_1 and $\rho A_2+\lambda I$ are similar if and only if they have the same invariant factors. If $A(x)=x^3+a_2x^2+a_1x+a_0=0$ is the characteristic equation of A, then $(x+\lambda)^3+\sigma a_2(x+\lambda)^2+\sigma^2a_1(x+\lambda)+\sigma^3a_0=0$, where $\sigma\rho=1$, is the characteristic equation of $\rho A+\lambda I$. Let K be the affine group in one variable over $GF(p)$. The canonical form for a cubic equation under K is x^3+bx+c where $b=0$, 1, or some fixed nonsquare. x^3+bx+c and $x^3+b'x+c'$ are conjugate under K if and only if $b=b'$ and $c^2=(c')^2$. Hence there are $p+5$ and $p+3$ characteristic equations for $p\equiv 1 \pmod 3$ and $p\equiv 2 \pmod 3$, respectively.

This almost completes the count of the classes of invariant factors under K. A (cubic) characteristic equation corresponds to more than one similarity class if and only if it has a repeated root in $GF(p)$. Since the points of T represented by scalar matrices are excluded, a characteristic equation with repeated roots in $GF(p)$ corresponds to exactly two similarity classes. It is easily shown that all our cubics with a double root in $GF(p)$ are conjugate under K; the same for triple roots. This gives two more classes of points of T for every $p>3$. Q.E.D.[3,4]

[3] This work is a revision of the author's Ph.D. thesis written under the supervision of H. R. Brahana, University of Illinois, Urbana, Illinois (1959). The author wishes to express his appreciation for the helpful suggestions of H. R. Brahana and G. Higman.

[4] The reader may notice that Theorem 1.2.2 [2, p. 568] implies that the number of classes of subspaces of T (according to the classification of our lemma) has the form described at the beginning of this paper. Theorem 1.2.2 does not, however, yield a specific number of classes.

The counting of groups of our class of order p^{12} by this method leads to the classification of similar pairs of matrices, an unsolved problem. The reader may check that our problem for two generators is easy, whereas for four generators seems unmanageable.

References

1. G. Higman, *Enumerating p-groups*, I: *Inequalities*, Proc. London Math. Soc. vol. 10 (1960) pp. 24–30.

2. ———, *Enumerating p-groups*, II: *Problems whose solution is* PORC, Proc. London Math. Soc. vol. 10 (1960) pp. 566–582.

3. M. Hall, Jr., *The theory of groups*, New York, Macmillan, 1959.

4. K. W. Gruenberg, *Residual properties of infinite soluble groups*, Proc. London Math. Soc. vol. 7 (1957) pp. 29–62.

Southern Illinois University and
The University of Chicago

AN INEQUALITY FOR HERMITE POLYNOMIALS

JACK INDRITZ

It is known that the Hermite polynomials

$$H_n(x) = (-1)^n e^{x^2} \frac{d^n}{dx^n} e^{-x^2}, \qquad n = 0, 1, \cdots, \quad -\infty < x < \infty \tag{1}$$

satisfy an inequality

$$H_n(x) \leqq c(2^n n!)^{1/2} e^{x^2/2}, \qquad c \text{ constant.} \tag{2}$$

Erdelyi [1] states that $c = 1.086435$ will serve. It has been conjectured that the best value for c is 1, and it is the purpose of this note to prove the conjecture.

As a basis for the discussion, we assume as known the following properties:

(3) $H_n(x)$ is a polynomial of degree n, having n distinct real zeros. The coefficient of x^n is 2^n.

(4) $H_{n+1}(x) = 2xH_n(x) - H_n'(x)$,

(5) $H_n(x) - 2xH_{n-1}(x) + 2(n-1)H_{n-2}(x) = 0, \qquad n \geqq 2,$

(6) $H_n''(x) - 2xH_n'(x) + 2nH_n(x) = 0$,

(7) $H_n(-x) = (-1)^n H_n(x)$,

(8) $H_n'(x) = 2nH_{n-1}(x)$.

Received by the editors October 28, 1960.