Computation of Isomorphism Classes of p-Groups

By Rodney James and John Cannon

Abstract. p-groups may be classified by splitting the groups up into classes having the same commutator relations (isoclinism classes) and then determining the non-isomorphic groups in each class. This paper reduces the problem of determining the isomorphism classes to that of finding the equivalence classes of a set of matrices under some equivalence relation. A computer is used to find the equivalence classes for the first few values of p, and these are then used as a guide for finding the solution for general p. ■

1. Introduction. Occasionally the solution of a research problem in algebra gives rise to large amounts of straightforward calculations of either a numerical or non-numerical nature. Sometimes the amount of calculation is so large as to preclude the solution of the problem. In such situations it is natural to consider the use of a computer and it is often surprising how much can be accomplished with the expenditure of relatively little programming effort. Such a computation, arising out of the problem of classifying the groups of order p^6 $(2 < p)$, is described here.

The groups of order p^n $(n \leqq 5)$ have been known for some time. These may all be found in a paper of Schreier [6] in which he determined the groups of order p^5 for the first time. Recently a catalogue of the groups of order 2^n $(n \leqq 6)$ has been published by Hall and Senior [3]. The usual method of classifying the groups of order p^n is to divide them into mutually exclusive families [isoclinism families] and to determine all the isomorphism classes of groups in each family separately. Easterfield [2] has found the isoclinism families of groups of order p^6 $(2 < p)$ and written down the groups for 10 of the 43 isoclinism families. James [5] has redetermined the isoclinism families for p^6 $(2 < p)$, written down the groups for 42 of the 43 families and found an expression for the number of groups of order p^6 $(2 < p)$.

This paper describes how, for p-groups, isomorphism classes of groups may be computed for each isoclinism family. We first show how the isomorphism classes of groups for each isoclinism family may be characterised by an equivalence relation on a set of matrices. The equivalence relation corresponding to each isoclinism family is found and a computer is used to calculate the equivalence classes for the first few primes p. Using these results as a guide one then attempts to write down equivalence class representatives for general p. Given an equivalence class representative one can immediately write down a set of generators and relations for the corresponding isomorphism class of groups.

2. Determination of the Equivalence Relations. Two groups G, G' with centres Z, Z' and derived groups H_2, H_2', respectively, are said to be isoclinic [4] if the following three properties hold:

(a) $G/Z \cong G'/Z'$;

Received March 5, 1968, revised August 12, 1968.

(b) $H_2 \cong H_2'$;

(c) for $\alpha, \beta \in G$ and $\alpha', \beta' \in G'$, there exist isomorphisms (a), (b) such that, if $\alpha'Z', \beta'Z'$ correspond to $\alpha Z, \beta Z$ in (a) then the commutator (α', β') corresponds to the commutator (α, β) in (b).

As we are not concerned here with the determination of isoclinism families, we shall not say anything further about it. The interested reader is referred to the paper by P. Hall [4]. Easterfield [2] has determined all the isoclinism families which contain groups of order p^6 $(2 < p)$.

For a given isoclinism family, the method of finding the isomorphism classes is essentially the same as that used by Blackburn [1] in determining p-groups of maximal class. We now give details of the method. Let G, G' (with centres Z, Z' respectively) be two isoclinic p-groups. By (a), (b) and (c) we may suppose without loss of generality that G and G' have the same relations modulo their centres and the same commutator relations. Thus, writing $\boldsymbol{\xi}$ for the m-tuple $(\xi_1, \xi_2, \cdots, \xi_m)$ and $w(\boldsymbol{\xi})$ for a word in $\xi_1, \xi_2, \cdots, \xi_m$, we may write

$$G = \langle \alpha_1, \alpha_2, \cdots, \alpha_m, Z \rangle \quad \text{for } \alpha_1, \alpha_2, \cdots, \alpha_m \in G$$

and

$$G' = \langle \alpha_1', \alpha_2', \cdots, \alpha_m', Z' \rangle \quad \text{for } \alpha_1', \alpha_2', \cdots, \alpha_m' \in G'$$

where $w(\boldsymbol{\alpha}) \equiv 1 \pmod{Z}$ if and only if $w(\boldsymbol{\alpha}') \equiv 1 \pmod{Z'}$ and $w'(\boldsymbol{\alpha}) = 1$ if and only if $w'(\boldsymbol{\alpha}') = 1$ for all commutator words w'.

If $G \cong G'$ and θ is an isomorphism mapping G' onto G, then $Z \cong Z'$ and we may write

$$Z = \langle \gamma_1, \gamma_2, \cdots, \gamma_n \rangle \quad \text{for } \gamma_1, \gamma_2, \cdots, \gamma_n \in Z\,,$$

$$Z' = \langle \gamma_1', \gamma_2', \cdots, \gamma_n' \rangle \quad \text{for } \gamma_1', \gamma_2', \cdots, \gamma_n' \in Z'\,,$$

where the order of γ_j equals the order of γ_j' and each γ_j commutes with every element of G and each γ_j' with every element of G'. Also, since $G \cong G'$, $\gamma_j{}^{p^s j} = w_0(\boldsymbol{\alpha})$ if and only if $\gamma_j'{}^{p^s j} = w_0(\boldsymbol{\alpha}')$ where w_0 is a commutator word.

The only relations for G which have not been determined are those of the form

$$w(\boldsymbol{\alpha}) = \gamma_1{}^{a_1}\gamma_2{}^{a_2} \cdots \gamma_n{}^{a_n}$$

which we write more briefly $w(\boldsymbol{\alpha}) = \boldsymbol{\gamma}^{\mathbf{a}}$. Since G/H_2 is abelian, this reduces to equations of the form

$$\alpha_i{}^{p^r i} = w_1(\boldsymbol{\alpha})\boldsymbol{\gamma}^{\mathbf{a}\,i} \tag{1}$$

where $w_1(\boldsymbol{\alpha}) \in H_2$, $\boldsymbol{\gamma}^{\mathbf{a}\,i} \in Z$ and $i = 1, 2 \cdots m$.

For convenience, we may suppose that no term of $w_1(\boldsymbol{\alpha})$ is an element of $H_2 \cap Z$. Since $G/Z \cong G'/Z'$, we have (where $\mathbf{a}_1{}^*, \mathbf{a}_2{}^*, \cdots, \mathbf{a}_m{}^*$ are the parameters of G')

$$\alpha_i'{}^{p^r i} = w_1(\boldsymbol{\alpha}')\boldsymbol{\gamma}'^{\mathbf{a}_i{}^*}\,. \tag{1}'$$

Since $\theta: G' \to G$ is an isomorphism, we may write

$$G = \langle \alpha_1{}^*, \alpha_2{}^*, \cdots, \alpha_m{}^*, Z \rangle\,, \qquad Z = \langle \gamma_1{}^*, \gamma_2{}^*, \cdots, \gamma_n{}^* \rangle\,,$$

where

$$\alpha_i^* = \theta(\alpha_i') \equiv \boldsymbol{\alpha}^{\mathbf{x}_i} \pmod{H_2 Z} \tag{2}$$

(where $i = 1, 2 \cdots m$),

$$\gamma_j^* = \theta(\gamma_j') = \boldsymbol{\gamma}^{\mathbf{y}_j} \qquad (j = 1, 2, \cdots, n) \ . \tag{3}$$

γ_j^* commutes with every element of G and

$$\gamma_j^{p^{j_s}} = w_0(\boldsymbol{\alpha}) \ , \qquad \gamma_j^{*p^{j_s}} = w_0(\boldsymbol{\alpha}^*) \ . \tag{4}$$

Equations (1) and (4), together with the relations mod Z, the commutator relations and the structure of the abelian group Z are the defining relations for the group G.

Using (2) and (3), Eq. (4) yields

$$(\boldsymbol{\gamma}^{\mathbf{y}_j})^{p^s j} = w_0(\boldsymbol{\alpha}^{\mathbf{x}_1}, \boldsymbol{\alpha}^{\mathbf{x}_2} \cdots \boldsymbol{\alpha}^{\mathbf{x}_m}) \tag{5}$$

giving a restriction on $\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_m, \quad \mathbf{y}_1, \mathbf{y}_2, \cdots, \mathbf{y}_n$.

Also under the isomorphism θ, (1)′ becomes

$$\alpha_i^{*p^{r_i}} = w_1(\boldsymbol{\alpha}^*)\boldsymbol{\gamma}^{*\mathbf{a}_i^*} \ . \tag{1}^*$$

From (2) we get

$$\begin{aligned} \alpha_i^{*p^{r_i}} &\equiv \boldsymbol{\alpha}^{p^{r_i}\mathbf{x}_i} \pmod{H_2} \\ &\equiv \alpha_1^{p^{r_i}x_{i1}} \cdots \alpha_i^{p^{r_i}x_{ii}} \cdots \alpha_n^{p^{r_i}x_{in}} \pmod{H_2} \end{aligned}$$

(where x_{ij} is the jth component of the vector $\mathbf{x}_i$)

$$\begin{aligned} &\equiv \alpha_1^{p^{r_i}x_{ii}} \cdots \boldsymbol{\gamma}^{x_{ii}\mathbf{a}_i} \cdots \alpha_n^{p^{r_i}x_{in}} \pmod{H_2} \\ &\equiv \boldsymbol{\gamma}^{f(\mathbf{a}_i)} \pmod{H_2} \end{aligned}$$

for some function $f(\mathbf{a}_i)$, since $\boldsymbol{\gamma}^{\mathbf{a}_i}$ does not occur as any $\alpha_j^{p^{r_i}x_{ij}}$ $(j \neq i)$ and the term involving H_2 in (2) is independent of $\mathbf{a}_i$.

Similarly, using (3) we obtain

$$\boldsymbol{\gamma}^{*\mathbf{a}_i^*} = \boldsymbol{\gamma}^{g(\mathbf{a}_1^*, \mathbf{a}_2^*, \cdots, \mathbf{a}_n^*)}$$

for some function g. Thus, by comparing indices of each γ_j on the left- and right-hand sides of (1)* we obtain a set of equations expressing the $\boldsymbol{\alpha}^*$'s in terms of the $\mathbf{a}$'s with restrictions on the variables $\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_m, \quad \mathbf{y}_1, \mathbf{y}_2, \cdots, \mathbf{y}_n$ given by (5). It may be verified that this system of equations actually defines an equivalence relation on the parameters $\mathbf{a}_i$ and so on the set of matrices $A = (\mathbf{a}_1, \cdots, \mathbf{a}_m)$.

Thus the isomorphism classes of an isoclinism family may be considered to correspond to equivalence classes of such matrices. For p-groups, the calculation of the isomorphism classes is simplified as the matrices are usually over $GF(p)$. However, the case of nonregular p-groups must be treated separately from the case of regular p-groups because of complications in calculating the $(\alpha_i^*)^p$.

3. Programming. For each isoclinism family of the groups of order p^n, such an equivalence relation is derived. One then requires a representative from each equivalence class of matrices for general p. If the solution is not obvious, a computer is used to calculate the equivalence classes for the first few values of p. Using the

equivalence class representatives found by the computer for the first few values of p, it is usually (but not always) a simple matter to write down equivalence class representatives for general p.

The matrices A generally consist of all $m \times n$ matrices over $GF(p)$ and may easily be generated in some order. As each new A is generated, all its distinct transforms under the equivalence relation are found and placed in a stack S_1. In this stack the matrix coefficients are packed several to a word. This set of matrices is the equivalence class containing A and so an equivalence class representative is chosen and printed. Now the matrices in S_1 are transferred to a stack S_2 containing all matrices which have occurred in any equivalence class already found. Now the whole process is repeated with the first matrix A that does not occur in S_2. If the computation runs out of store it tries to obtain more by deleting from S_2 all matrices coming before the present A. For some isoclinism families, the number of A's to be considered is reduced because of certain conditions the A's most satisfy.

Using a 32K English Electric KDF$_9$ it was found possible to calculate the equivalence classes for the primes up to and including 23 in a reasonable time.

4. An Example. We now give an example to illustrate how the equivalence relation for a particular isoclinism family is found. We shall consider one of the families of groups of order p^5. For this particular family, the groups are nonregular for $p = 3$ and regular for $p > 3$. So the case $p = 3$ must be treated separately from the case $p > 3$. Only the case $p = 3$ will be treated here.

This family will now be defined for $p = 3$. The groups G of order 3^5 in this family are generated by two elements α_1, α_2 satisfying the following conditions:

If $(a, b) = a^{-1}b^{-1}ab$ is the commutator of a and b, we have

$$(\alpha_1, \alpha_2) = \beta\,, \quad (\beta, \alpha_1) = \beta_1 \in Z(G)\,, \quad (\beta, \alpha_2) = \beta_2 \in Z(G)$$

and

$$\beta^3 = {\beta_1}^3 = {\beta_2}^3 = 1\,, \quad {\alpha_1}^3 \in Z(G)\,, \quad {\alpha_2}^3 \in Z(G)$$

where $Z(G) = \langle \beta_1, \beta_2 \rangle$ (i.e. β_1 and β_2 generate $Z(G)$).

(This family is the family Φ_6 in P. Hall [4].)

To determine the remaining relations, write ${\alpha_i}^3 = \mathfrak{B}^{\mathbf{a}_i}$, ${\alpha_i}^{*3} = \mathfrak{B}^{*\mathbf{a}_i^*}$, where

$$\alpha_1^* \equiv {\alpha_1}^{x_1}{\alpha_2}^{x_2}\beta^x \pmod{Z}, \qquad \alpha_2^* \equiv {\alpha_1}^{y_1}{\alpha_2}^{y_2}\beta^y \pmod{Z}$$

and so $\beta^* \equiv \beta^\Delta \pmod{Z}$, where $\Delta = x_1y_2 - x_2y_1 \not\equiv 0 \pmod{p}$. Also $\beta_1^* = \mathfrak{B}^{\Delta x}$, $\beta_2^* = \mathfrak{B}^{\Delta y}$. Now

$$\begin{aligned} {\beta_1^*}^{a_{11}^*}{\beta_2^*}^{a_{12}^*} &= {\alpha_1^*}^3 \\ &= ({\alpha_1}^{x_1}{\alpha_2}^{x_2})^3 \\ &= {\alpha_1}^{3x_1}{\alpha_2}^{3x_2}{\beta_1}^{-{x_1}^2x_2}{\beta_2}^{x_1{x_2}^2}\,. \end{aligned}$$

Equating indices of β_1, β_2 we have

$$\begin{aligned} \Delta(x_1a_{11}^* + y_1a_{12}^*) &= x_1a_{11} + x_2a_{21} - {x_1}^2x_2\,, \\ \Delta(x_2a_{11}^* + y_2a_{12}^*) &= x_1a_{12} + x_2a_{22} + x_1{x_2}^2\,. \end{aligned}$$

Similarly,

$$\Delta(x_1a_{21}^* + y_1a_{22}^*) = y_1a_{11} + y_2a_{21} - y_1^2y_2,$$
$$\Delta(x_2a_{21}^* + y_2a_{22}^*) = y_1a_{12} + y_2a_{22} + y_1y_2^2.$$

Writing

$$A = (\mathbf{a}_1, \mathbf{a}_2), \quad A^* = (\mathbf{a}_1^*, \mathbf{a}_2^*), \quad X = (\mathbf{x}, \mathbf{y})$$

we have

$$\Delta XA^* = AX + \begin{pmatrix} -x_1^2x_2 & -y_1^2y_2 \\ x_1x_2^2 & y_1y_2^2 \end{pmatrix}$$

i.e.,

$$A^* = \Delta(X^{-1}AX + X') \cdots \tag{6}$$

is the required equivalence relation, where

$$X' = \Delta\begin{pmatrix} -x_1x_2(x_1y_2 + x_2y_1) & y_1^2y_2 \\ -x_1^2x_2 & y_1y_2(x_1y_2 + x_2y_1) \end{pmatrix}.$$

Here A ranges over all 2×2 matrices over $GF(3)$ and X over all 2×2 non-singular matrices over $GF(3)$. The computer is now used to find the equivalence classes of the matrices A under the equivalence relation (6), and it prints the following equivalence class representatives:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Thus there are seven isomorphism classes of groups of order 3^5 in this family and we may suppose the remaining relations are

$$\alpha_1^3 = 1, \beta_1, \beta_2, \beta_1, \beta_2, \beta_2, 1.$$
$$\alpha_2^3 = 1, 1, \beta_2, \beta_2, \beta_1, \beta_1^2, \beta_1.$$

5. Discussion. Using similar methods for each isoclinism class, the groups of order p^5 ($p > 2$), as given by Schreier [6], were checked and the nonisomorphic groups of order p^6 ($p > 2$) found for 42 of the 43 isoclinism classes for p^6. For the remaining class the nonisomorphic groups have been found by the computer for the primes up to and including 23. The number of groups in this class for general p was derived using the computer results for the early primes as a guide.

The number of nonabelian groups of order 3^6 is 481, and the number of order p^6 ($p > 3$) is given by the following expression:

$$\tfrac{1}{4}\{13p^2 + 133p + 1346 + 80(p-1,3) + 45(p-1,4) + 8(p-1,5) + 8(p-1,6)\},$$

where (l, m) denotes the greatest common divisor of l and m. The details of these results may be found in [5].

Acknowledgment. The authors wish to express their gratitude to Professor G. E. Wall for his valuable assistance during the preparation of this paper.

Department of Pure Mathematics
University of Sydney
Sydney, Australia

1. N. BLACKBURN, "On a special class of p-groups," *Acta Math.*, v. 100, 1958, pp. 45–92. MR **21** #1349.
2. T. EASTERFIELD, *A Classification of Groups of Order* p^6, Ph.D. Dissertation, Cambridge Univ., Cambridge, 1940.
3. M. HALL & J. SENIOR, *The Groups of Order* 2^n $(n \leqq 6)$, Macmillan, New York, 1964. MR **29** #5889.
4. P. HALL, "Classification of prime-power groups," *J. Reine Angew. Math.*, v. 182, 1940, pp. 130–141. MR **2**, 211.
5. R. JAMES, *The Groups of Order* p^6 $(p \geqq 3)$, Ph.D. Thesis, Univ. of Sydney, 1968.
6. O. SCHREIER, "Über die Erweiterung von Gruppen. II," *Abh. Math. Sem. Univ. Hamburg*, v. 4, 1926, pp. 321–346.