PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 65, Number 1, July 1977

GROUPS OF ORDER pq^m WITH ELEMENTARY ABELIAN SYLOW q-SUBGROUPS

J. ALONSO

ABSTRACT. Characterization and number of the groups of order pq^m with elementary Abelian Sylow q-subgroups. Old methods of O. Hölder and A. E. Western are simplified and generalized.

O. Hölder [1, pp. 340–357] and A. E. Western [2, pp. 230–244] determined the number of groups of order pq^2 and pq^3; the method they used for this purpose can be substantially simplified and generalized to the order pq^m, where m is any positive integer.

We consider first the groups with normal Sylow q-subgroup. Let p, q be distinct primes, G a group of order pq^m with elementary Abelian normal Sylow q-subgroup Q, and $P = \langle d \rangle$ a Sylow p-subgroup of G. If $a = (a_1, \ldots, a_m)$ is a basis of Q, we write the elements of Q in the form

$$a^v = a_1^{v_1} a_2^{v_2} \cdots a_m^{v_m}$$

where $v_i \in Z_q$ (the field of numbers modulo q). G has a presentation of the form

$$\big(a, d;\, a_i^q,\, a_i a_j = a_j a_i,\, d^p,\, d a^v d^{-1} = A^{Mv}\big) \tag{1}$$

where M is a matrix of rank m and order dividing p with entries in Z_q; we will refer to M as 'the matrix of d over Q relative to the basis a'.

THEOREM. *Let p, q be distinct primes, let n be the smallest positive integer such that p divides $q^n - 1$, and put $p - 1 = nh$. For any positive integer m, let H be the set of all h-tuples $e = (e_1, \ldots, e_h)$ of nonnegative integers with $(e_1 + \cdots + e_h)n \leq m$. Then the number of groups of order pq^m with elementary Abelian normal Sylow q-subgroup, is the number of classes of the equivalence relation $\sim$ on H, where $e \sim e'$ if and only if $e'_j = e_{j+i}$, $1 \leq j \leq h$, for some i (the sum of subindexes is carried modulo h).*

For the proof of this theorem we make use of the following well-known lemmas which we state without proof.

LEMMA 1. *In $Z_q[\lambda]$, $\lambda^p - 1 = (\lambda - 1) f_1(\lambda) \cdots f_h(\lambda)$, here $f_i(\lambda)$ is irreducible in $Z_q[\lambda]$ and*

$$f_i(\lambda) = \prod_{j=0}^{n-1} \left(\lambda - z^{x^{i-1} q^j}\right),$$

Received by the editors May 14, 1976.
AMS (MOS) subject classifications (1970). Primary 20D99; Secondary 15A33.

where z is a primitive pth root of unity in $GF(q^n)$ and x is a primitive root modulo p.

Let

$$M_i, \quad 1 \leq i \leq h, \tag{2}$$

be the companion matrix of the polynomial $f_i(\lambda)$.

LEMMA 2. *$(M_i)^j$ is similar to M_{i+j} (the sum of subindexes is carried modulo h).*

PROOF OF THE THEOREM. By the Sylow theorems, $n_p(G) = q^{rn}$ with $0 \leq r$, $nr \leq m$, and correspondingly $o(N(P)) = pq^{m-rn}$; therefore, we can write $Q = U \times W$, with $U \subset N(P)$, U of order q^{m-nr}, and $W \cap N(P) = E$, W of order q^{rn}. Since P and U are both normal in $N(P)$, $N(P) = C(P) = U \times P$, that is, the matrix of d over U is the identity matrix I_{m-rn}. On the other hand, by a known theorem on canonical forms of matrices, we may assume that $W = Q_1 \times \cdots \times Q_r$, such that $o(Q_u) = q^n$ and the matrix A_u of d over Q_u is one of the matrices (2); therefore in (1)

$$M = I_{m-rn} \oplus A_1 \oplus \cdots \oplus A_r \tag{3}$$

where each A_u is one of the M_i.

It can be seen that, if the matrix of d over Q_u relative to some basis is M_i, and a_1 is a nonidentity element of Q_u, then $(a_1, \ldots, a_n)$ with $a_k = da_{k-1}d^{-1}$, $2 \leq k \leq n$, is a basis of Q_u, and the matrix of d over Q_u relative to this basis is the same M_i.

Let e_i be number of occurrences of M_i among the A_u. Clearly $e = (e_1, \ldots, e_h) \in H$, and the presentations (1) with M as in (3) are in one-to-one correspondence with the elements of H.

By Lemma 2, equivalent h-tuples determine presentations (1) of the same group. It remains to show that nonequivalent h-tuples determine presentations of morphically different groups; we do this by proving that, for a given h-tuple e, the number of n-tuples $(c_1, \ldots, c_n)$ of linearly independent elements of Q such that M_i, $1 \leq i \leq h$, is the matrix of d over $\langle c_1, \ldots, c_n \rangle$ relative to the basis $(c_1, \ldots, c_n)$ is $q^{ne_i} - 1$. (Observe that the use of d^j for d as generator of P preserves the equivalence classes and the use of gd, $g \in Q$, for d introduces no novelty, since d and gd determine, by conjugation, the same automorphism in Q.)

A change of names and order permits to assume that $i = 1$ and

$$A_1 = A_2 = \ldots = A_{e_1} = M_1 = \begin{bmatrix} 0 & 0 & . & . & . & 0 & j_0 \\ 1 & 0 & . & . & . & 0 & j_1 \\ 0 & 1 & . & . & . & 0 & j_2 \\ . & . & . & . & . & . & . \\ 0 & 0 & . & . & . & 1 & j_{n-1} \end{bmatrix},$$

$$A_u \neq M_1, e_1 < u \leq r.$$

If $(c_1, \ldots, c_n)$ is one of the n-tuples under consideration, then $c_1 \neq 1$, and, under conjugation by d,

$$c_1 \to c_2 \to \cdots \to c_n \to c_1^{j_0} c_2^{j_1} \cdots c_n^{j_{n-1}};$$

c_i can be uniquely expressed as a product $c_i = b_i a_{i1} a_{i2} \cdots a_{ir}$ with $b_i \in U$ and $a_{iu} \in Q_u$, $1 \leqslant u \leqslant r$; therefore, under conjugation by d,

$$b_1 \to b_2 \to \cdots \to b_n \to b_1^{j_0} b_2^{j_1} \cdots b_n^{j_{n-1}} = b_1^{j_0 + j_1 + \cdots + j_{n-1}} = b_1^{1 - f_1(1)}$$

and

$$a_{1u} \to a_{2u} \to \cdots \to a_{nu} \to a_{1u}^{j_0} a_{2u}^{j_1} \cdots a_{nu}^{j_{n-1}}$$

whence $b_1 = 1$ and $a_{1u} = 1$ for $e_1 < u \leqslant r$; therefore, $c_1 \in Q_1 \times Q_2 \times \cdots \times Q_{e_1}$ which allows $q^{ne_1} - 1$ choices for c_1 and consequently for the n-tuple. This concludes the proof of the theorem.

If Q is not normal in G, then $N(Q) = Q = C(Q)$, and by Burnside's theorem, P is normal in G; since $N(P)/C(P) \subseteq \mathrm{Aut}(P)$, the group $G/C(P)$ is cyclic, which implies that $o(C(P)) = pq^{m-1}$; it easily follows that:

If $q \nmid (p-1)$, there are no groups in this category, and

If $q \mid (p-1)$, there is only one group with presentation

$$\left(a, d;\ a_i^q, a_i a_j = a_j a_i,\ d^p,\ a_1 d a_1^{-1} = d^k,\ a_i d a_i^{-1} = d \text{ for } 1 < i \leqslant m\right),$$
$$k^q = 1 \neq k \pmod{p}.$$

The results of Hölder and Western follow at once from the preceding discussion.

References

1. O. Hölder, *Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4*, Math. Ann. **43** (1893), 300–412.
2. A. E. Western, *On groups of order p^3q*, Proc. London Math. Soc. **30** (1899), 209–269.

Department of Mathematics, Bennett College, Greensboro, North Carolina 27420