Groups of Square-Free Order, An Algorithm

By J. Alonso

Abstract. An abstract definition of the groups of square-free order is given that leads naturally to a programmable computation of their number. O. Hölder's alternative description of the groups of square-free order is incidentally derived.

Throughout this paper $G$ will be a group of order $h = \Pi_{i=1}^{n} p_i$, where $p_1 > p_2 > \cdots > p_n$ are given prime numbers. O. Hölder proved in 1895 that the number of groups of order $h$ is

$$\sum_{S} \left( \prod_{j=1}^{r} \frac{(p_{S(j)})^{c_{S(j)}} - 1}{p_{S(j)} - 1} \right),$$

where the sum extends to all the subsets $S = \{S(1), S(2), \ldots, S(r)\}$ of the set $\{2, 3, \ldots, n\}$; and $c_{S(j)}$ is the number of differences $p_i - 1$, $i \in S$, which are divisible by $p_j$. The number of terms in (1) is very large even for small values of $n$; and therefore, it seems desirable to have a computer program that for each set of primes $\{p_1, p_2, \ldots, p_n\}$ skips the zero terms in (1).

The present paper makes no use of formula (1); it is an alternative approach to the description of the groups of order $h$ and the determination of their number.

1. If $n = 2$, by the Sylow theorems $G$ has a normal subgroup $\langle a \rangle$ of order $q = p_1$ and a subgroup $\langle b \rangle$ of order $p = p_2$; therefore, $bab^{-1} = a^k$; and since $a = b^pab^{-p} = a^{kp}$, $k$ is a solution of the congruence equation

$$x^p = 1 \pmod{q}.$$

If $p\mid (q - 1)$, (2) has exactly $p$ distinct solutions mod $q$, say $1, K, K^2, \ldots, K^{p-1}$ forming a cyclic group under multiplication mod $q$; and $G$ is one of the two metacyclic groups [4, p. 462]

$$\langle a, b; a^q, b^p, bab^{-1} = a \rangle,$$

$$\langle a, b; a^q, b^p, bab^{-1} = a^K \rangle.$$

(3) is a cyclic group generated by $ab$. Observe that the metacyclic group $\langle a, b; a^q, b^p, bab^{-1} = a^{kr} \rangle$ with $1 < r < p$ has also presentation (4) if we use the generators $a, b^r$ instead of $a, b$. If $p\mid (q - 1)$, then we only have the cyclic group (3).

2. In the general case, $n \geq 2$, we will use the following theorems whose proofs can be found in [3, 2.6.7, p. 39, 6.2.11, p. 138, 9.3.11, p. 229 and 9.3.10, p. 228].

**Theorem 1.** If $H$ and $A/H$ are solvable groups, so is $A$.

**Theorem 2.** If $A$ is a finite group, $p$ the smallest prime dividing $o(A)$, and a Sylow $p$-subgroup $P$ of $A$ is cyclic, then $P$ has a normal complement in $A$.

---

Received July 8, 1975; revised November 24, 1975.


Copyright © 1976, American Mathematical Society
Definition. A Sylow basis $B$ of a finite group $A$ is a set of Sylow subgroups $P_i$ of $A$, one for each prime divisor of $o(A)$, such that if $P_1, P_2, \ldots, P_r$ are elements of $B$ then $P_1P_2 \cdots P_r$ is a subgroup of $A$ of order $\prod_{i=1}^{r} o(P_i)$.

Theorem 3. If $A$ is a finite solvable group, then $A$ has a Sylow basis.

Theorem 4 (Hall). If $A$ is a finite solvable group of order $uv$, and $(u, v) = 1$, then: (i) $A$ has at least one subgroup of order $u$, (ii) all the subgroups of $A$ of order $u$ are conjugate.

By Theorems 1 and 2 and induction on $n$, one can easily see that $G$ is solvable; and therefore by Theorem 3, there exist $a_i \in G$, $i = 1, 2, \ldots, n$, such that $o(a_i) = p_i$; and $(a_{S(1)}, a_{S(2)}, \ldots, a_{S(r)})$ is a subgroup of $G$ of order $\prod_{i=1}^{r} p_{S(i)}$ for every subset $S \subseteq \{1, 2, \ldots, n\}$. In particular, for $i < j$, we have, as in Section 1, $a_ia_ja_j^{-1} = a_i^{k(i,j)}$, so that $G$ has a presentation of the form

\[(a_i|1 \leq i \leq n); \{a_i^p|1 \leq i \leq n\}, \{a_ia_ja_j^{-1} = a_i^{k(i,j)}|1 \leq i < j \leq n\}\]

with

\[(k(i,j))^{p_j} = 1 \pmod{p_i}.\]  \hspace{1cm} (5)

For each pair $i < j$ such that $p_i|(p_j - 1)$, we will choose one $\neq 1$ solution $K(i, j)$ of the congruence equation (6); and therefore, $K(i, j)$ is a power of $K(i, j)$ (mod $p_i$).

If $i < j < t$, then $(a_i, a_j)$ is normal in $(a_i, a_j, a_t)$; and the relation $a_ia_ja_j^{-1} = a_i^{k(i,j)}$ is changed by conjugation by $a_t$ into $a_t^{k(j,i)}a_t^{k(i,t)}a_j^{-k(j,i)} = a_i^{k(i,j)k(i,t)}$, whence $a_i^{k(i,j)k(j,t)}a_i^{k(i,t)} = a_i^{k(i,j)k(j,t)},$ that is: $k(i,j)k(j,t) - 1 = 1 \pmod{p_i}$ which implies that:

\[k(i,j)k(j,t) - 1 = 1 \pmod{p_i} \]  \hspace{1cm} (7)

If $i < j < t$, then either $k(i, j) = 1$ or $k(j, t) = 1$.

Using a convenient power of $a_j$, $j > 1$, as generator instead of $a_j$, we may assume as in Section 1 that

\[k(1, j) \text{ equals either } 1 \text{ or } K(i, j). \]  \hspace{1cm} (8)

More generally, we may assume without loss of generality that:

\[k(1, j) = k(2, j) = \cdots = k(i - 1, j), \text{ then } k(i, j) \text{ is either } 1 \text{ or } K(i, j). \]  \hspace{1cm} (9)

Proposition 1. There exists a group $G$ with any given presentation of type (5) with exponents satisfying conditions (6)--(9).

Proof. For each $j$, $(a_1, a_2, \ldots, a_j, a_j+1)$ is the relative holomorph

\[\text{Hol}(a_1, a_2, \ldots, a_j, (f))\]

with $f(a_j) = a_i^{k(i,j+1)}$, $1 \leq i \leq j$ [3, 9.2.2, p. 214].

Proposition 2. Two presentations of type (5) with exponents satisfying conditions (6)--(9) that differ in one of the exponents $k(i, j)$ present morphically different groups. We postpone the proof of this proposition.

3. In the case of three factors we will call $r = p_1$, $q = p_2$ and $p = p_3$. By the previous section, $G$ has one of the following presentations:
In order to show that they present morphically different groups observe:

(i) The groups with presentations (10)—(15) have the following characteristics:

<table>
<thead>
<tr>
<th></th>
<th>Abelian</th>
<th>$\langle a \rangle$ central</th>
<th>$\langle b, c \rangle$ Abelian</th>
<th>$\langle b \rangle$ central</th>
<th>$\langle c \rangle$ central</th>
</tr>
</thead>
<tbody>
<tr>
<td>(10)</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>(11)</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>(12)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(13)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>(14)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>(15)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

(ii) If $G$ has two presentations of type (13), say, one with $k(2, 3) = K(2, 3)^s$ and the other with $k(2, 3) = K(2, 3)^t$, then $G$ has elements $a, b, c$ satisfying the relations of the first presentation, and elements $a', b', c'$ satisfying the relations of the second presentation; since $\langle a \rangle$ and $\langle b \rangle$ are normal in $G$, we have (Theorem 4) $a' = a^x$, $b' = b^y$ and $c' = a^u b^v c^w$. The relation $c'b'c'^{-1} = a^K(1,3)w$ implies $a^{xK(1,3)}w = a^{xK(1,3)}$, whence $w = 1$; and the relation $c'b'c'^{-1} = b'^{K(2,3)t}$ implies $b^{yK(2,3)}t = b^{yK(2,3)}$, whence $t = s \pmod{p}$; and therefore, the two presentations coincide.

The preceding discussion permits us to determine the number of groups of order $rqp$ as shown in the following table:

| $q(r - 1)$ | $p|(r - 1)$ | $p|(q - 1)$ | Number of groups |
|------------|-------------|-------------|------------------|
| No         | No          | No          | 1                |
| No         | No          | Yes         | 2                |
| No         | Yes         | No          | 2                |
| No         | Yes         | Yes         | $p + 2$          |
| Yes        | No          | No          | 2                |
| Yes        | No          | Yes         | 3                |
| Yes        | Yes         | No          | 4                |
| Yes        | Yes         | Yes         | $p + 4$          |
4. Proof of Proposition 2. Assume inductively that the proposition is true for \( n - 1 \), and let \( G \) and \( G' \) be groups with presentations of the type (5) satisfying conditions (6)–(9) and with \( k(i, j) \neq k'(i, j) \) for some pair \( i < j \). If \( j < n \), then by assumption \( \langle a_1, a_2, \ldots, a_{n-1} \rangle \neq \langle a'_1, a'_2, \ldots, a'_{n-1} \rangle \) and by Theorem 4 \( G \neq G' \); therefore, we may assume that \( k(i, j) = k'(i, j) \) for all \( 1 \leq i < j < n \). If \( k(1, n) \neq k'(1, n) \), then by (8) one of the two is 1 and the other is \( K(1, n) \), whence \( \langle a_1, a_n \rangle \neq \langle a'_1, a'_n \rangle \) and \( G \neq G' \); therefore, we may assume that \( k(1, n) = k'(1, n) \). Let \( j \) be the smallest subindex such that \( k(j, n) \neq k'(j, n) \); we may assume that \( k'(j, n) \neq 1 \) and by (7) \( k(i, j) = k'(i, j) = 1 \) for all \( i < j \). If \( k(i, n) = k'(i, n) = 1 \) for all \( i < j \), then by (9) \( k(i, n) = 1 \) and \( k'(j, n) = K(j, n) \); and therefore, \( \langle a_1, a_j, a_n \rangle \) is of type (10), whereas \( \langle a'_1, a'_j, a'_n \rangle \) is of type (11) and by Theorem 4 \( G \neq G' \). Else, let \( i \) be the least subindex such that \( k(i, n) = k'(i, n) \neq 1 \); by (9) \( k(i, n) = k'(i, n) = K(i, n) \); and therefore, \( \langle a_i, a_j, a_n \rangle \) is either of type (13) with different exponent or of type (12); again by Theorem 4 \( G \neq G' \).

5. O. Hölder’s Approach. It is easy to see that \( \langle a_j \rangle \) is normal in \( G \) if and only if \( k(i, j) = 1 \) for all \( i < j \), and \( H = \langle a_j \rangle \) normal in \( G \rangle \) is Abelian and therefore cyclic. Furthermore, condition (7) shows that \( G^1 \subseteq H \), and therefore, \( G/H \) is also cyclic, which implies [4, p. 462] that \( G \) is metacyclic with presentation of the form

\[ (a, b; a^2, b^t, bab^{-1} = a^k), \quad st = h. \]

<table>
<thead>
<tr>
<th>( k(1, 2) )</th>
<th>( k(1, 3) )</th>
<th>( k(2, 3) )</th>
<th>( k(1, 4) )</th>
<th>( k(2, 4) )</th>
<th>( k(3, 4) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( K )</td>
<td>( K )</td>
<td>( K )</td>
<td>( k )</td>
<td>( k )</td>
<td>( k )</td>
</tr>
<tr>
<td>( K )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( K )</td>
<td>( K )</td>
<td>( K )</td>
<td>( k )</td>
<td>( k )</td>
<td>( k )</td>
</tr>
<tr>
<td>( K )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( K )</td>
<td>( K )</td>
<td>( K )</td>
<td>( k )</td>
<td>( k )</td>
<td>( k )</td>
</tr>
<tr>
<td>( K )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Diagram 1
Definition. \( i \) is linked to \( j \) if there exist \( S(1) = i, S(2), \ldots, S(r) = j \) such that \( a_{S(t)} \) does not commute with \( a_{S(t+1)} \), \( t = 1, 2, \ldots, r - 1 \). The proof of the following proposition is trivial:

**PROPOSITION 3.** For each \( i, \langle a_{i}, \{a_{j} | i \text{ is linked to } j\} \rangle \) is the minimal direct summand of \( G \) containing \( a_{i} \).

6. The number of groups of order \( h \) can be determined by means of the tree diagram of the exponents in (5), as we illustrate here for the case of 4 factors. In Diagram 1 above we write \( K \) or \( k \) for \( K(i, j) \) or \( k(i, j) \) when it is not equal to 1; the branches with some \( K \) or \( k \) exist if and only if the corresponding \( p_{i} \) divides \( p_{t} - 1 \); a small \( k \) indicates that the offshoot originating at fork \((i, j)\) has multiplicity \( p_{t} - 1 \).

7. In the case of 4 factors we call \( s = p_{1}, r = p_{2}, q = p_{3} \) and \( p = p_{4} \). The number of groups of order \( srgq \) is easily determined by determining first the groups of order \( srg \), and pursuing in the tree diagram the number of extensions of each to groups of order \( srgq \). We obtain:

<table>
<thead>
<tr>
<th>Table 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of Groups of Order srgq, s &gt; r &gt; q &gt; p</strong></td>
</tr>
</tbody>
</table>

\[
\begin{array}{cccccccccc}
& p \cdot (s - 1) & p \cdot (r - 1) & p \cdot (q - 1) & p \cdot (t - 1) & p \cdot (s - 1) & p \cdot (r - 1) & p \cdot (q - 1) & p \cdot (t - 1) \\
\hline
r \cdot (s - 1) & 1 & 2 & 2 & p + 2 & 2 & p + 2 & p + 2 & p^2 + p + 2 \\
q \cdot (r - 1) & 2 & 3 & 4 & p + 4 & 4 & p + 4 & 2p + 4 & (p + 2)^2 \\
q \cdot (t - 1) & 2 & 3 & 4 & p + 4 & 4 & p + 4 & 2p + 4 & (p + 2)^2 \\
m \cdot (s - 1) & q + 2 & q + 3 & 2q + 4 & 2q + p + 4 & 2q + 4 & 2q + p + 4 & (q + 2)(p + 2) & + p^3 \\
m \cdot (r - 1) & 2 & 4 & 3 & p + 4 & 4 & 2p + 4 & p + 4 & (p + 2)^2 \\
m \cdot (q - 1) & 3 & 5 & 5 & p + 6 & 6 & 2p + 6 & 2p + 6 & p^2 + 3p + 6 \\
m \cdot (t - 1) & 4 & 6 & 6 & p + 7 & 8 & 2p + 8 & 2p + 8 & p^2 + 3p + 8 \\
\hline
s \cdot (s - 1) & q + 4 & q + 6 & 2q + 6 & 2q + p + 7 & 2q + 8 & 2(p + q + 4) & (q + 2)(p + 2) & + 4 & (q + 2)(p + 2) & + p^2 + p + 4 \\
s \cdot (r - 1) & 2 & 4 & 3 & p + 4 & 4 & 2p + 4 & p + 4 & (p + 2)^2 \\
s \cdot (q - 1) & q + 2 & q + 3 & 2q + 4 & 2q + p + 4 & 2q + 4 & 2q + p + 4 & (q + 2)(p + 2) & + p^3 \\
s \cdot (t - 1) & 2 & 3 & 4 & p + 4 & 4 & p + 4 & 2p + 4 & (p + 2)^2 \\
\hline
\end{array}
\]

8. A computer program to determine the number of groups of order \( h \) can be written using the tree diagram of Section 6:

(a) Set to 0 the number, NUM, of groups of order \( h \).

(b) As we proceed along one branch, each occurrence of \( k \) multiplies NU, the
number of groups originated by the branch, by \( p_j - 1 \). \( k \) occurs at the fork \((i, j)\) when the following conditions are satisfied simultaneously: (i) \( p_j | (p_l - 1) \), (ii) \( k(m, i) = 1 \) for all \( m < i \), and (iii) \( k(m, j) \neq 1 \) for some \( m < i \).

(c) When the end of one branch is reached, \( \text{NU} \) is accumulated to \( \text{NUM} \).

(d) The next branch is picked up at the last fork \((i, j)\) where \( p_j | (p_l - 1) \) and the \( k(i, j) \neq 1 \) has not been used.

Note. The FORTRAN program implementing the algorithm appears in the microfiche section.

Department of Mathematics
Bennett College
Greensboro, North Carolina 27420