FACTORIZING SMALL 2-GROUPS

SÁNDOR SZABÓ

Let $G$ be a finite abelian group and let $G = A_1 \cdots A_n$ be a factorization of $G$ into its subsets $A_1, \ldots, A_n$. For a given $G$ certain choices of the orders $|A_1|, \ldots, |A_n|$ guarantee that one of the factors is periodic. In connection with an open problem we determine such choices of orders of factors in two special cases. In these cases $|G|$ is either $2^5$ or $2^6$.

1. Introduction

Let $G$ be a finite abelian group. Let $A_1, \ldots, A_n$ be subsets of $G$. If the product $A_1 \cdots A_n$ is direct and is equal to $G$, then we say that $A_1 \cdots A_n$ is a factorization of $G$. In other words $A_1 \cdots A_n$ is a factorization of $G$ if each element $g$ of $G$ is uniquely expressible in the form

$$g = a_1 \cdots a_n, \quad a_1 \in A_n, \ldots, a_n \in A_n.$$ 

If $|A_1| = q_1, \ldots, |A_n| = q_n$, then $(q_1, \ldots, q_n)$ is called the type of the factorization $A_1 \cdots A_n$.

By the fundamental theorem of finite abelian groups each finite abelian group is a direct product of cyclic groups. This decomposition into cyclic groups is not necessarily unique. However, if $G$ is the direct product of cyclic groups of orders $t_1, \ldots, t_r$ respectively, then we say that $G$ is of type $(t_1, \ldots, t_r)$. We use

Entrato in redazione: 15 giugno 2004

AMS 2000 Subject Classification: 20K01, 52C22.
Keywords: factorization of finite abelian groups, Hajós-Rédei theory.
group types only to identify groups and so it does not cause any problem that a
given group may belong to different types.

Let \( e \) be the identity element of \( G \). A subset \( A \) of \( G \) is called periodic if
there is an element \( g \in G \) such that \( Ag = A \) and \( g \neq e \). Sometimes we express
this fact saying that \( A \) is periodic with period \( g \) or \( g \) is a period of \( A \). Note that
\( Ag = A \) implies \( Ag^m = A \) for all natural numbers \( m \). Thus we may assume that
the period \( g \) of a periodic subset \( A \) has prime order.

In 1965 L. Rédei [6] proved that if \( G = A_1 \cdots A_n \) is a factorization of the finite
abelian group \( G \) and \( |A_1|, \ldots, |A_n| \) are primes, then at least one of the factors is
periodic.

Let \( G \) be a finite abelian group. If from each factorization \( G = A_1 \cdots A_n \) of
type \( (q_1, \ldots, q_n) \) it follows that at least one of the factors is always periodic,
then we say that the factorization type \( (q_1, \ldots, q_n) \) is periodicity forcing for \( G \).
Motivated by Rédei’s theorem we set forth the following problem. Given a
group classify all the possible factorization types that force periodicity for this

It looks natural to try to solve this problem for \( p \)-groups first. K. Corrádi
and S. Szabó [3], [4], [5] are focused on the special case \( p = 2 \). Let \( (q_1, \ldots, q_n) \)
be a factorization type for the finite abelian 2-group \( G \) with \( q_1 \geq \cdots \geq q_n \geq 2 \).
It is still not known whether \( (q_1, \ldots, q_n) \) forces periodicity for \( G \) when \( n \geq 3,
q_1 \mid 4, \ldots, q_n \mid 4 \) and \( G \) is not of type \((2^\lambda, 2, \ldots, 2)\) or \((2^\lambda, 2^\mu)\). The main result
is that the factorization types listed in Table 1 force periodicity for groups of the
corresponding types.

Table 1: The main result

<table>
<thead>
<tr>
<th>factorization type</th>
<th>group type</th>
</tr>
</thead>
<tbody>
<tr>
<td>(4,4,2)</td>
<td>(4,4,2)</td>
</tr>
<tr>
<td>(4,4,2,2)</td>
<td>(4,4,2,2)</td>
</tr>
</tbody>
</table>

The first row in the table represents the only case of groups of order \( 2^5 \) that was
not decided in [1], [3], [4], and [5]. Thus the classification problem is solved for
2-groups of order not greater than \( 2^5 \). Namely, for an abelian 2-group with order
less than or equal to \( 2^5 \) every factorization type is periodicity forcing except the
four cases depicted in Table 2.
Table 2: Groups of order $2^5$

<table>
<thead>
<tr>
<th>factorization type</th>
<th>group type</th>
</tr>
</thead>
<tbody>
<tr>
<td>(8,4)</td>
<td>(8,4)</td>
</tr>
<tr>
<td>(8,4)</td>
<td>(8,2,2)</td>
</tr>
<tr>
<td>(8,2,2)</td>
<td>(8,4)</td>
</tr>
<tr>
<td>(8,2,2)</td>
<td>(8,2,2)</td>
</tr>
</tbody>
</table>

2. Preliminaries

Let $G$ be a finite abelian group. A subset $A$ of $G$ is called normalized if $e \in A$. A factorization $G = A_1 \cdots A_n$ of $G$ is called normalized if the factors $A_1, \ldots, A_n$ are normalized.

Let $G = A_1 \cdots A_n$ be a factorization of $G$ and let $a_1, \ldots, a_n$ be elements of $A_1, \ldots, A_n$ respectively. Multiplying the factorization $G = A_1 \cdots A_n$ by $a = a_1^{-1} \cdots a_n^{-1}$ leads to the factorization $G = Ga = (A_1 a_1^{-1}) \cdots (A_n a_n^{-1})$. Note that the new factorization is normalized and if one of the new factors is periodic then so is the corresponding original one. This means that when we deal with periodicity forcing factorizations types we may restrict our attention to normalized factorizations.

Let $A$ and $A'$ be subsets of $G$. We say that $A$ can be replaced by $A'$ if $G = A'B$ is a factorization of $G$ whenever $G = AB$ is a factorization of $G$. For example $A$ can be replaced by $Ag$ for each $g \in G$. For a subset $A$ of $G$ and an integer $t$ let us define $A'$ to be $\{a' : a \in A\}$. By Proposition 3 of [8], $A$ can be replaced by $A'$, whenever $t$ is relatively prime to $|A|$.

If $A$ is a subset and $\chi$ is a character of $G$, then we use $\chi(A)$ to denote the sum

$$\sum_{a \in A} \chi(a).$$

If $\chi(A) = 0$, then we say that $\chi$ annihilates $A$. The set of all characters for which $\chi(A) = 0$ will be called the annihilator set of $A$ and will be denoted by $\text{Ann}(A)$. L. Rédei [6] developed a character test for the replaceability of factors which reads as follows. The factor $A$ can be replaced by $A'$ if $|A| = |A'|$ and $\text{Ann}(A) \subseteq \text{Ann}(A')$. In this paper character always means an irreducible linear character.

From time to time we will work in the group ring $\mathbb{Z}[G]$. The elements of $\mathbb{Z}[G]$ are formal linear combinations of elements of $G$ with integer coefficients. The addition and multiplication of these elements are defined in a way which
resembles the addition and multiplication of multivariate polynomials. A character of $G$ can be extended to be a character of $Z[G]$. To a subset $A$ of $G$ we assign the element

$$\overline{A} = \sum_{a \in A} a$$

of $Z[G]$. The fact that $A_1 \cdots A_n$ is a factorization of $G$ can be expressed equivalently by saying that the equation $G = \overline{A_1} \cdots \overline{A_n}$ holds in $Z[G]$.

Let $A$ be a subset of $G$ such that $|A| = 4$. If $A$ contains two elements with a common square we say that $A$ is a type 1 subset of $G$. If $A$ is normalized and $A$ contains an involution, then $A$ is clearly a type 1 subset. On the other hand if $A$ is a type 1 subset, then it can be replaced by a normalized subset that contains an involution. In order to verify this claim let $A = \{a, b, c, d\}$, where $a^2 = b^2$. Now $A$ is replaceable by $Aa^{-1} = \{e, ba^{-1}, ca^{-1}, da^{-1}\}$. Clearly $Aa^{-1}$ is normalized and $ba^{-1}$ is an involution.

To a subset $A$ of $G$ we assign the companion subgroup

$$K = \bigcap_{\chi(A) = 0} \text{Ker}\chi$$

of $G$, where $\chi$ runs over all the (irreducible) characters of $G$. The reader can easily verify that if $A$ has two elements, then $K = \{e\}$ implies the periodicity of $A$. By Lemma 1 of [3], if $A$ is a type 1 subset, then $K = \{e\}$ implies that $A$ is periodic.

By Theorem 2 of [2], if $G = A_1 \cdots A_n$ is a factorization of $G$, $K_1, \ldots, K_n$ are the companion subgroups assigned to the factors $A_1, \ldots, A_n$ respectively and $n \leq 4$, then there is an $i, 1 \leq i \leq n$ such that $K_i = \{e\}$.

We would like to state explicitly the following corollary of the above theorem as we will refer to it later. If $G = A_1 \cdots A_n$ is a factorization of $G$, where each factor $A_i$ either has two elements or it is a type 1 subsets and $n \leq 4$, then at least one of the factors is periodic.

### 3. Lemmas

In this section we present two lemmas. The first is about vanishing products in the group ring $Z[G]$ and the second is about the annihilator of a subset.

**Lemma 3.1.** Let $G$ be a finite abelian group and $d_1, d_2, d_3$ involutions of $G$ with $d_1 d_2 d_3 \neq e$. If

$$\overline{A}(e - d_1)(e - d_2)(e - d_3) = 0,$$  \hspace{1cm} (1)

where $A$ is a nonempty subset of $G$, then $A$ contains two elements with a common square.
Proof. From the equation (1) by multiplying out and rearranging the terms we get
\[ A + Ad_1 d_2 + Ad_1 d_3 + Ad_2 d_3 = Ad_1 + Ad_2 + Ad_3 + Ad_1 d_2 d_3. \]

It follows that
\[ A \cup Ad_1 d_2 \cup Ad_1 d_3 \cup Ad_2 d_3 = Ad_1 \cup Ad_2 \cup Ad_3 \cup Ad_1 d_2 d_3. \]

Hence one of
\[ A \cap Ad_1, \quad A \cap Ad_2, \quad A \cap Ad_3, \quad A \cap Ad_1 d_2 d_3 \]

is not empty. So there are elements \( a_1, a_2 \in A \) and \( d \in G \) such that \( a_1 = a_2 d \) and \( d \neq e, d^2 = e \). Thus \( a_1 \neq a_2 \) and \( a_1^2 = a_2^2 \).

This completes the proof. \( \square \)

**Lemma 3.2.** Let \( G \) be a finite abelian group and \( x, y \in G \) such that \( |x| = |y| = 4 \) and \( x, y \) are independent. If \( A = \{e, x, y, x^3 y^3\} \) and \( \chi \) is an irreducible character of \( G \), then \( \chi(A) = 0 \) implies \( \chi(x^2) = 1 \) and \( \chi(y^2) = 1 \).

**Proof.** Assume that \( \chi(x) = \rho \), where \( \rho \) is a primitive 4th root of 1. Then \( \chi(y) = \rho^k \), for some \( k, 0 \leq k \leq 3 \). From \( \chi(x^3 y^3) = \rho^{3+3k} = (-\rho)^{1+k} \) it follows that \( \chi(A) \in \{2, 2\rho\} \). Hence the assumption \( \chi(A) = 0 \) implies \( \chi(x) = \pm 1 \), which gives \( \chi(x^2) = 1 \). A similar argument gives that \( \chi(y^2) = 1 \) and this completes the proof. \( \square \)

The proof above is from the anonymous referee of the paper. The original proof was longer. We will use only the following consequence of Lemma 3.2. If \( G = AB \) is a factorization of \( G \), then by Theorem 1 of [9] it follows that \( B \) is periodic with periods \( x^2 \) and \( y^2 \).

### 4. Groups of order \( 2^5 \)

In this section we show that the factorization type \( (4, 4, 2) \) forces periodicity for groups of type \( (4, 4, 2) \). With this result available all factorization types can be classified into periodicity forcing or not periodicity forcing for groups of order less than or equal to \( 2^5 \).

**Theorem 4.1.** Let \( G \) be a group of type \( (4, 4, 2) \) and \( G = ABC \) a normalized factorization of \( G \), where \( |A| = |B| = 4, |C| = 2 \). Then one of the factors is periodic.
**Proof.** Let

\[
A = \{e, a_1, a_2, a_3\}, \\
B = \{e, b_1, b_2, b_3\}, \\
C = \{e, c\}.
\]

If \(|c| = 2\), then \(C\) is periodic and we are done. So we may assume that \(|c| = 4\).

If \(A\) is a type 1 subset of \(G\), that is, if \(A\) contains two elements with a common square, then by Lemma 1 of [7], \(A\) or \(BC\) is periodic. If \(A\) is periodic, then we are done. So we may assume that \(BC\) is periodic with period \(g\) such that \(|g| = 2\).

This leads to the equation \(BC(e - g) = 0\) in the group ring \(Z[G]\). Multiplying by \((e - c)\) we get \(B(e - c^2)(e - g) = 0\). By Theorem 2 of [9], it follows that there are subsets \(U\) and \(V\) of \(G\) such that

\[
B = U \langle c^2 \rangle \cup V \langle g \rangle,
\]

where the products \(U \langle c^2 \rangle, V \langle g \rangle\) are direct and the union is disjoint. If \(U = \emptyset\), then \(B\) is periodic with period \(g\). If \(V = \emptyset\), then \(B\) is periodic with period \(c^2\).

Therefore we may assume that \(U \neq \emptyset\) and \(V \neq \emptyset\). So there is an element \(u\) in \(U\). Clearly, the elements \(ue\) and \(uc^2\) belong to \(B\) and they have a common square. Therefore \(B\) is a type 1 subset. As we are supposing that \(A\) is a type 1 subset, the corollary of Theorem 2 of [2] is applicable to the factorization \(G = ABC\) and gives that one of the factors is periodic.

Thus we may assume that \(A\) is not a type 1 subset. By symmetry we may assume that \(B\) is not a type 1 subset either. If \(BC\) is periodic, then \(BC(e - g) = 0\). Multiplying by \((e - c)\) we get \(B(e - c^2)(e - g) = 0\). Repeating the argument above it follows that \(B\) is a type 1 subset. This is an outright contradiction. So we may assume that \(BC\) is not periodic.

As \(A\) is not a type 1 subset, it follows that \(|a_i| = 4\) for each \(i, 1 \leq i \leq 3\). We claim that

\[
\langle a_1 \rangle \cap \langle a_2 \rangle = \langle a_1 \rangle \cap \langle a_3 \rangle = \langle a_2 \rangle \cap \langle a_3 \rangle = \{e\}. \tag{2}
\]

Indeed, for instance \(\langle a_1 \rangle \cap \langle a_2 \rangle \neq \{e\}\) implies the contradiction that \(a_1^2 = a_2^2\).

Let \(H = \langle a_1, a_2 \rangle\). Using (2) we can see that \(H\) is of type \(4, 4\). As \(H\) contains 3 involutions and \(G\) contains 7 involutions, it follows that there is an involution in \(G \setminus H\) which together with \(a_1, a_2\) form a basis for \(G\). We can choose a basis \(x, y, z\) of \(G\) with \(|x| = |y| = 4, |z| = 2, a_1 = x, a_2 = y\). Note that \(G^2 \subseteq \langle x^2, y^2 \rangle\).

From (2) we know that \(a_1^2, a_2^2, a_3^2\) are distinct involutions of \(G\). Thus \(a_1^2, a_2^2, a_3^2\) is a permutation of \(x^2, y^2, x^2y^2\). Hence \(a_3^2 = x^2y^2\). Similarly, \(b_1^2, b_2^2, b_3^2\) is a permutation of \(x^2, y^2, x^2y^2\). By relabeling the elements of \(B\), we may assume that \(b_1^2 = x^2, b_2^2 = y^2, b_3^2 = x^2y^2\). This leaves 8 choices for \(a_3, b_3, b_1, \text{ and } b_2\).
independently. Namely,

\[
\begin{align*}
a_3, b_3 & \in xy(x^2, y^2, z), \\
b_1 & \in x(x^2, y^2, z), \\
b_2 & \in y(x^2, y^2, z).
\end{align*}
\]

Since \(B\) can be replaced by \(B^{-1} = \{e, b_1^{-1}, b_2^{-1}, b_3^{-1}\}\), it may be assumed that \(b_3 \in xy(x^2, z)\).

As \(|c| = 4\), it follows that \(c^2\) is one of \(x^2, y^2, x^2y^2\). This leaves us with \(c \in \{x, y, xy\}\langle x^2, y^2, z\rangle\). If \(a_3 = xy\), then \(A = \{e, x\}\{e, y\}\). In this case by Theorem 2 of [4], it follows that one of the factors is periodic. So we may assume that \(a_3 \neq xy\). If \(a_3 = x^3y\), then

\[
A = \{e, x, y, x^3y\} = \{e, x\}\{e, x^3y\}
\]

and so this case can be treated as the \(a_3 = xy\) case. Plainly, the \(a_3 = xy^3\) case can also be reduced to the \(a_3 = xy\) case. If \(a_3 = x^3y^3\), then by the remark after Lemma 3.2, \(BC\) is periodic with period \(x^2\). This is not the case. So we may assume that \(a_3 \neq x^3y^3\). When \(a_3 = x^3yz\), then setting \(x_1 = x, y_1 = x^3yz\) we get

\[
A = \{e, x, y, x^3yz\} = \{e, x_1, y_1, x_1y_1z\}.
\]

Thus the \(a_3 = x^3yz\) case can be reduced to the \(a_3 = xyz\) case. Similarly the \(a_3 = xy^3z\) case can be reduced to the \(a_3 = xyz\) case. In short only the \(a_3 = xyz\), \(a_3 = x^3y^3z\) cases need to be dealt with.

The directness of the products \(AB, AC, BC\) gives that

\[
AA^{-1} \cap BB^{-1} = AA^{-1} \cap CC^{-1} = BB^{-1} \cap CC^{-1} = \{e\}.
\]

Hence we may discard the cases

\[
\begin{align*}
b_1 & \in \{x, x^3\}, \\
b_2 & \in \{y, y^3\}, \\
b_3 & \in \{x^3y, xyz\}, \\
c & \in \{x, y, xyz, x^3y\}.
\end{align*}
\]

Table 3 summarizes the remaining choices for the elements \(a_1, a_2, a_3, b_1, b_2, b_3, c\). With the assistance of a computer we can inspect all the arising

\[
(1)(1)(2)(6)(6)(2)(8) = 1 \, 152
\]

cases. None of them provides a factorization for \(G\).

This completes the proof. \(\blacksquare\)
5. Groups of order $2^6$

We are not able to solve the classification problem of periodicity forcing factorization types for groups of order $2^6$. In this section we present a partial result. Namely, we show that the factorization type $(4,4,2,2)$ is periodicity forcing for the group of type $(4,4,2,2)$.

**Theorem 5.1.** Let $G$ be a group of type $(4,4,2,2)$ and $G = ABCD$ a normalized factorization, where $|A| = |B| = 4$, $|C| = |D| = 2$. Then one of the factors is periodic.

**Proof.** Let $x, y, u, v$ be a basis of $G$ with $|x| = |y| = 4$, $|u| = |v| = 2$ and let

\[
A = \{e, a_1, a_2, a_3\}, \\
B = \{e, b_1, b_2, b_3\}, \\
C = \{e, c\}, \\
D = \{e, d\}.
\]

If $|c| = 2$, then $C$ is periodic. So we may assume that $|c| = 4$. Similarly, we may assume that $|d| = 4$.

If both $A$ and $B$ have two elements with a common square, then by the corollary of Theorem 2 of [2], one of the factors $A, B, C, D$ is periodic. In the remaining part of the proof we distinguish two cases.

Case 1: Neither $A$ nor $B$ is a type 1 subset.

Case 2: $A$ is not a type 1 subset and $B$ is a type 1 subset.

Let us turn to case 1 first. As we have seen in the proof of Theorem 4.1, the elements $a_1^2, a_2^2, a_3^2$ form a permutation of $x^2, y^2, x^2y^2$. Similarly the elements $b_1^2, b_2^2, b_3^2$ form a permutation of $x^2, y^2, x^2y^2$. We can choose the basis $x, y, u, v$ such

---

Table 3: The choices

<table>
<thead>
<tr>
<th>$a_1$</th>
<th>$a_2$</th>
<th>$a_3$</th>
<th>$b_1$</th>
<th>$b_2$</th>
<th>$b_3$</th>
<th>$c$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x$</td>
<td>$y$</td>
<td>$xyz$</td>
<td>$xy^2$</td>
<td>$x^2y$</td>
<td>$xy$</td>
<td>$xy$</td>
</tr>
<tr>
<td>$x^3$</td>
<td>$y^3$</td>
<td>$z$</td>
<td>$x^3$</td>
<td>$y^3$</td>
<td>$x^3z$</td>
<td>$x^2y$</td>
</tr>
<tr>
<td>$xz$</td>
<td>$yz$</td>
<td></td>
<td>$xy^2$</td>
<td>$x^2$</td>
<td>$x$</td>
<td></td>
</tr>
<tr>
<td>$x^3z$</td>
<td>$y^3z$</td>
<td>$x$</td>
<td>$x^3$</td>
<td>$y$</td>
<td>$z$</td>
<td></td>
</tr>
<tr>
<td>$x^3$</td>
<td>$y^3$</td>
<td>$z$</td>
<td></td>
<td>$x^3z$</td>
<td>$x^3y$</td>
<td></td>
</tr>
<tr>
<td>$x$</td>
<td>$y$</td>
<td>$xyz$</td>
<td>$x^2y$</td>
<td>$x^3$</td>
<td>$xy$</td>
<td></td>
</tr>
</tbody>
</table>

---
that $a_1 = x$, $a_2 = y$. Note that $G^2 \subseteq \langle x^2, y^2 \rangle$. By rearranging the elements of $B$, we may assume that $b_1^2 = x^2$, $b_2^2 = y^2$, $b_3^2 = x^2y^2$ and that $a_3, b_3 \in xy(x^2, y^2, u, v)$.

If $a_3 = xy$, then $A = \{e, x\} \{e, y\}$. In this case, by Theorem 2 of [4], one of the factors $\{e, x\}$, $\{e, y\}$, $B, C, D$ is periodic. So we may discard the choice $a_3 = xy$. By the argument used in the proof of Theorem 4.1 and using the symmetry of the elements $u, v, uv$, the following choices remain for $a_3$

$$xy, x^3y^3, x^3y^3u.$$ 

If $a_3 = x^3y^3$, then by the remark after Lemma 3.2, $BCD$ is periodic with period $x^2$ and so

$$\overline{B}(e + c)(e + d)(e - x^2) = 0.$$ 

Multiplying by $(e - c)(e - d)$ gives that

$$\overline{B}(e - c^2)(e - d^2)(e - x^2) = 0.$$ 

If $c^2d^2x^2 \neq e$, then by Lemma 3.1, $B$ is a type 1 subset. This is not the case and so it follows that $c^2d^2x^2 = e$, that is, $c^2d^2 = x^2$. Repeating the argument with $y^2$ in place of $x^2$ gives that $c^2d^2 = y^2$. But this is not possible since $\langle x \rangle \cap \langle y \rangle = \{e\}$. Thus we may assume that $a_3 \neq x^3y^3$. Now $b_1 \in x(x^2, y^2, u, v)$. We can discard the choices $b_1 = x$ and $b_1 = x^3$ as $AA^{-1} \cap BB^{-1} = \{e\}$. Similarly, $b_2 \in y(x^2, y^2, u, v)$. We can discard the choices $b_2 = y$ and $b_2 = y^3$ as $AA^{-1} \cap BB^{-1} = \{e\}$. Since $B$ can be replaced by $B^{-1} = \{e, b_1^{-1}, b_2^{-1}, b_3^{-1}\}$ it follows that $b_3 \in xy(x^2, u, v)$. We can discard the choices $b_3 = x^3y$, $b_3 = xyu$ as $AA^{-1} \cap BB^{-1} = \{e\}$.

We know that $|c| = |d| = 4$ and that $C, D$ can be replaced by $C^{-1} = \{e, c^{-1}\}$, $D^{-1} = \{e, d^{-1}\}$. This leaves us with $c, d \in \{x, y, xy, xy^2, xy^3, x^2y\}\langle u, v \rangle$. The choices when $c$ or $d$ is equal to one of $x, y, xy^3, xyu$ can be discarded.

There are

$$(1)(1)(2)(14)(14)(6)[(1/2)(20)(19)] = 446880$$

choices for the elements $a_1, a_2, a_3, b_1, b_2, b_3, c, d$. With the help of a computer we can inspect all the arising cases. None of them provides a factorization for $G$.

Let us turn to case 2. We can write $b_3$ in the form $b_3 = b_1b_2d_3$ with a suitable $d_3 \in G$. By Lemma 1 of [3], we may assume that $|d_3| = 2$. So we may assume that $B$ is in form $B = \{e, b_1, b_2, b_1b_2d_3\}$. We claim that $d_3 \in \langle x^2, y^2 \rangle$. In order to prove the claim note that by Lemma 1 of [3], $ACD$ is periodic with period $d_3$. This leads to the equation

$$\overline{A}(e - d_3)(e - c^2)(e - d^2) = 0.$$
in the group ring \( Z[G] \). Write \( d_3 \) in the form \( d_3 = x^{2\alpha} y^{2\beta} u^\gamma v^\delta \), where \( 0 \leq \alpha, \beta, \gamma, \delta \leq 1 \). If \( u^\gamma v^\delta = e \), then \( d_3 \in \langle x^2, y^2 \rangle \) and we are done. So we may assume that \( u^\gamma v^\delta \neq e \). Now \( d_3^2d^2 \neq e \) and Lemma 1 is applicable and it gives that \( A \) contains two elements with a common square. Thus \( A \) is a type 1 subset contrary to our assumption.

Next we claim that \( \{b_1, b_2, b_3\} \cap \langle x^2, y^2 \rangle \neq \emptyset \). In order to prove the claim we distinguish two subcases.

Subcase 2(a): \( B \) contains two involutions.

Subcase 2(b): \( B \) contains only one involution.

Let us deal first with subcase 2(a). Suppose that \( B \) contains two involutions, say \( b_1 \) and \( b_2 \). In this case, by Lemma 1 of [3], \( B \) can be replaced by \( H = \langle b_1, b_2 \rangle \). From the factorization \( G = AH \) we get the factorization \( G/H = (AH)/H \cdot (CH)/H \cdot (DH)/H \) of the factor group \( G/H \), where
\[
(AH)/H = \{H, a_1H, a_2H, a_3H\}, \\
(CH)/H = \{H, cH\}, \\
(DH)/H = \{H, dH\}.
\]

As \( G/H \) is of type \((4,4)\) or \((4,2,2)\) or \((2,2,2,2)\), by [4] it follows that one of the factors is periodic. So \( (gH)^2 = g^2H = H \) holds, where \( g \in \{a_1, a_2, a_3, c, d\} \).

In particular \( g \) is not an involution, that is, \( g^2 \neq e \). In addition we know that \( g^2 \in H = \{e, b_1, b_2, b_1b_2\} \). Thus \( g^2 \in \{b_1, b_2, b_1b_2\} \). It means that one of \( b_1, b_2, b_1b_2 \) is a square that is an involution too and so it can only be one of \( x^2, y^2, x^2y^2 \).

Clearly \( \{b_1, b_2, b_3\} \cap \langle x^2, y^2 \rangle \neq \emptyset \) holds unless \( b_1b_2 \in \langle x^2, y^2 \rangle \). So we assume that \( b_1b_2 \in \langle x^2, y^2 \rangle \). As \( d_3 \in \langle x^2, y^2 \rangle \), it follows that \( b_3 = b_1b_2d_3 \in \langle x^2, y^2 \rangle \). Thus \( \{b_1, b_2, b_3\} \cap \langle x^2, y^2 \rangle \neq \emptyset \) as claimed.

Let us turn to subcase 2(b). Assume that \( B \) contains only one involution, say \( |b_1| = 2, |b_2| = |b_3| = 4 \). By Lemma 1 of [3], \( B \) can be replaced by \( HB_2 \), where \( H = \{e, b_1\} \), \( B_2 = \{e, b_2\} \). From the factorization \( G = AB_2HCD \) we get the factorization \( G/H = (AH)/H \cdot (B_2H)/H \cdot (CH)/H \cdot (DH)/H \) of the factor group \( G/H \), where
\[
(AH)/H = \{H, a_1H, a_2H, a_3H\}, \\
(B_2H)/H = \{H, b_2H\}, \\
(CH)/H = \{H, cH\}, \\
(DH)/H = \{H, dH\}.
\]

As \( G/H \) is of type \((4,4,2)\) or \((4,2,2,2)\), it follows that one of the factors is periodic. So \( (gH)^2 = g^2H = H \) holds, where \( g \in \{b_2, a_1, a_2, a_3, c, d\} \). In particular \( g \) cannot be an involution, that is, \( g^2 \neq e \) In addition we know that
Thus we left with the \( g^2 = b_1 \) possibility. This in turn means that \( b_1 \in \langle x^2, y^2 \rangle \).

Summing up our argument we may assume that \( \{b_1, b_2, b_3\} \cap \langle x^2, y^2 \rangle \neq \emptyset \) By reordering the elements of \( B \) we may assume that \( b_1 \in \langle x^2, y^2 \rangle \).

The choices for \( a_1, a_2, a_3, c, d \) are the same as in case 1. The choices for \( b_1, d_3 \) are

\[
x^2, y^2, x^2 y^2.
\]

As \( B \) can be replaced by \( B^{-1} = \{e, b_1^{-1}, b_2^{-1}, b_3^{-1}\} \) the choices for \( b_2 \) are the elements of

\[
\{x, y, xy, xy^2, xy^3, x^2, x^2 y, x^2 y^2, y^2, x^2 y^2, \langle u, v \rangle \}.
\]

We can discard the choices \( x, y, xy^3, xyu \) as \( AA^{-1} \cap BB^{-1} = \{e\} \). There are

\[
(1)(1)(2)(3)(32)(3) \left[\left(\frac{1}{2}\right)(20)(19)\right] = 109,440
\]

choices for the elements \( a_1, a_2, a_3, b_1, b_2, d_3, c, d \). With some assistance of a computer we can inspect all the arising cases. None of them provides a factorization for \( G \).

This completes the proof. \( \square \)

REFERENCES


SÁNDOR SZABÓ

Institute of Mathematics and Informatics
University of Pécs
Ifjúság u. 6.

e-mail: sszabo7@hotmail.com