On a Product of Finite Subsets in a Torsion-Free Group

L. V. Braidovsky and G. A. Freiman

School of Mathematical Sciences, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel-Aviv University, Ramat-Aviv, 69978, Israel

Communicated by Walter Feit
Received November 8, 1988

1. INTRODUCTION

Let $G$ be a torsion-free group, and $K$ and $M$ finite subsets of $G$ with $|K| \geq 2$ and $|M| \geq 2$. We denote by $KM$ the set of the elements $g \in G$ which have at least one representation of the form $g = km$, where $k \in K$ and $m \in M$. It is known [Ke] that in the described situation the following inequality always holds:

$$|KM| \geq |K| + |M| - 1.$$  \hfill (1.1)

The purpose of this paper is to determine the structure of $K$ and $M$ when the order of $KM$ happens to be the minimal possible, namely, when $|KM| = |K| + |M| - 1$. We prove the following

THEOREM 1. If $G$ is a torsion-free group, $K$ and $M$ are subsets of $G$ satisfying

$$2 \leq |K|, |M| < \infty$$  \hfill (1.2)

and

$$|KM| = |K| + |M| - 1.$$  \hfill (1.3)

Then the subsets $K$ and $M$ have the form

$$K = \{a, aq, ..., aq^{t-1}\}$$  \hfill (1.4)

and

$$M = \{b, qb, ..., q^{n-1}b\},$$  \hfill (1.5)
where

\[ a, b, q \in G, \quad q \neq 1. \]

A special case of Theorem 1 with the additional restriction \(|K| \geq 3(|M| / 1)^5\) was proved in [FS]. The present work gives the proof for the general case. The authors are grateful to Graham Higman for mentioning to them the relation of the problem discussed to the question of the absence of zero divisors in the group ring of a torsion-free group over an integral domain.

2. Preliminaries

The condition and the statement of Theorem 1 are unchanged if \(K, M\) are replaced by \(gK, Mh\) for any \(g, h \in G\), whence we will always assume that

\[ 1 \in K, \quad 1 \in M. \tag{2.1} \]

We will also assume that

\[ |K| \geq |M|, \tag{2.2} \]

replacing, if the need arises, \(K\) and \(M\) by \(K^{-1} = \{ g \in G \mid g^{-1} \in K \}\) and \(M^{-1}\) correspondingly. We introduce now a notion of a segment. If \(x \in G, x \neq 1\) and \(A\) is a finite subset of \(G\) then a right \(x\)-segment of \(A\) is a subset \(P \subseteq A\) having the form

\[ P = \{ p, px, \ldots, px^{s-1} \}, \quad p \in G, \quad s \geq 1 \tag{2.3} \]

and satisfying

\[ Px \not\subseteq A, \quad Px^{-1} \not\subseteq A. \tag{2.4} \]

The number \(s\) will be called the length of the segment \(P\), \(p\) - the lower element of \(P\), and \(px^{s-1}\) - the upper element of \(P\). The left \(x\)-segment \(Q\) of some finite subset \(B \subseteq G\) is defined similarly:

\[ B \supseteq Q = \{ q, xq, \ldots, x^{t-1}q \}, \]

where

\[ xQ \not\subseteq B, \quad x^{-1}Q \not\subseteq B, \quad q \in G, \quad t \geq 1. \]

The number of right \(x\)-segments of \(A\) will be denoted by \(\beta_x(A)\), and the number of left \(x\)-segments of \(B\) will be denoted by \(\beta_x(B)\).
Speaking of some product set $AB$, $A \subseteq G$, $B \subseteq G$, by segments of $A$ we will always mean right segments, and by segments of $B$ we mean left segments.

In this notation Theorem 1 states that there exist $q \in G$, $q \neq 1$, such that

$$\beta_q(K) = \beta_q(M) = 1.$$ 

Obviously, if for some finite subset $A \subseteq G$, $\beta_q(A) = n$, then

$$|Ax \setminus A| = n,$$ 

(2.5)

and, particularly, we obtain

**Proposition 2.1 [FS].** Theorem 1 holds when $|M| = 2$.

**Proof.** By (2.1) we assume that

$$M = \{1, q\}, \quad q \in G.$$ 

Then (1.3) implies

$$|KM| = |K \cup Kq| = |K| + 1,$$

whence $|Kq \setminus K| = 1$ and by (2.3), $\beta_q(K) = 1$. Obviously, $\beta_q(M) = 1$ as well.

We will also use another fact proved in [FS]:

**Proposition 2.2 [FS].** Theorem 1 holds for linearly orderable groups.

The number of $\langle q \rangle$-cosets having non-empty intersection with some finite subset $A \subseteq G$ may, generally speaking, differ from the number of $q$-segments of $A$. For the present we note the following

**Proposition 2.3.** Theorem 1 holds if one of the subsets $K$, $M$ is contained in one $\langle q \rangle$-coset (right or left correspondingly) for some $q \in G$, $q \neq 1$.

**Proof.** We give the proof for $K$, and the other case is similar. By (2.1) we may assume $K \subseteq \langle q \rangle$. Let

$$M = \bigcup_{i=1}^{n} M_i$$

be the representation of $M$ as a disjoint union of subsets $M_i$, each contained in a different (left) $\langle q \rangle$-coset. Suppose $n \geq 2$. Then

$$|KM| = \sum_{i=1}^{n} |KM_i|.$$
Observe, (1.1) holds for one-element subsets as well, whence

\[ |KM| \geq n |K| + \sum_{i=1}^{n} |M_i| - n = |K| + |M| + |K| (n - 1) - n \]

so

\[ |KM| \geq |K| + |M|, \]

which contradicts assumption (1.3) of Theorem 1. Hence M is also contained in one \( \langle q \rangle \)-coset, and by (2.1) we may assume that \( M \subseteq \langle q \rangle \). The proof is completed by applying Proposition 2.2 to the linearly orderable group \( Q = \langle q \rangle \).

3. SET TRANSFORMATION

In the proof of Theorem 1 we will use the set transformation introduced in [Ke]. The transformation is applied to a pair of sets \( K, M \). If an \( x \in G, x \neq 1 \) is given, then the transformation increases by one element upward all the \( x \)-segments of one of the two sets, say \( K \), and takes off the upper elements of all the \( x \)-segments of the second set, \( M \). As a result, two new sets are obtained, correspondingly \( K_1 \) and \( M_1 \), with

\[ K_1 \supseteq K, \quad M_1 \subseteq M. \quad (3.1) \]

We will not consider the case \( M_1 = \emptyset \) that occurs if \( |M| = \beta_x(M) \) and all the \( x \)-segments in \( M \) are of length 1. It is always possible to choose \( x \in G, x \neq 1 \) such that \( |M| > \beta_x(M) \). Indeed, if \( M = \{ b_1, b_2, \ldots, b_n \} \) then taking \( x = b_2 b_1^{-1} \) will provide us with at least one \( x \)-segment \( P \subseteq M \) of length not less than 2: \( P \{ b_1, xb_1, \ldots \} \).

More formally, let \( x \in G, x \neq 1 \). Consider the sets of the upper elements of the \( x \)-segments in \( K \) and \( M \):

\[ K_x = \{ a \in K \mid ax \notin K \} \]
\[ M_x = \{ b \in M \mid xb \notin M \}. \quad (3.2) \]

The sets \( K_x \) and \( M_x \) are non-empty since \( K \) and \( M \) are finite and \( G \) is torsion-free. Subsets \( K_1 \) and \( M_1 \) are defined as

\[ K_1 = K \cup K_x x \]
\[ M_1 = M \setminus M_x. \quad (3.3) \]

**Proposition 3.1.** If \( K \) and \( M \) are subsets of \( G \), satisfying (1.2) and (1.3), while \( x \) is an element of \( G \) such that \( x \neq 1 \) and \( |M| > \beta_x(M) \), then

\[ \beta_x(K) = \beta_x(M) \quad (3.4) \]
and

\[ KM = K_1M_1, \quad (3.5) \]

where \( K_1 \) and \( M_1 \) are defined in (3.3).

**Proof.** Obviously, \( |K_x| = \beta_x(K), \ |M_x| = \beta_x(M) \). Suppose \( |K_x| > |M_x| \).

Then

\[ |K_1| + |M_1| = |K| + |K_x| + |M| - |M_x| > |K| + |M|. \quad (3.6) \]

Let \( g \in K_1M_1 \). Then (3.3) implies that either \( g \in KM_1 \subseteq KM \), or \( g = a_1b_1 \), where \( a_1 \in K_x, b_1 \in M_1 \). In the latter case \( a_1 = a_0x, a_0 \in K \) and

\[ g = (a_0x)b_1 = a_0(xb_1) \in KM, \]

since \( b_1 \notin M_x \) and \( xb_1 \in M \). This implies

\[ K_1M_1 \subseteq KM. \quad (3.7) \]

Using (3.6) we derive from (3.7) that

\[ |K_1M_1| \leq |KM| = |K| + |M| - 1 < |K_1| + |M_1| - 1, \]

which contradicts (1.1). Hence \( |K_x| \leq |M_x| \). Supposing \( |K_x| < |M_x| \), we let

\[ K_1 = K \setminus K_x, \quad M_1 = M \cup xM \quad (3.8) \]

\((K_1 \neq \emptyset, \text{otherwise } |K| = |K_x| < |M_x| \leq |M| \) in contradiction with (2.2)) and get the contradiction in a similar way. Consequently, \( |K_x| = |M_x| \), which proves (3.4). It also follows that

\[ |K_1| + |M_1| = |K| + |M|. \]

Now, by (3.7), \( |K_1M_1| \leq |KM| \). Suppose \( |K_1M_1| < |KM| \). Then

\[ |K_1M_1| < |KM| = |K| + |M| - 1 = |K_1| + |M_1| - 1, \]

which again contradicts (1.1). This implies \( |K_1M_1| = |KM| \), and \( K_1M_1 = KM \). \[\square\]

We note also the following

**Corollary 3.1.** Let \( K, M \) be subsets of \( G \) satisfying (1.2), (1.3). Let \( K_1, M_1 \) be defined as in (3.3) Then

\[ |K_1M_1| = |K_1| + |M_1| - 1. \quad (3.9) \]

**Proof.** This is the immediate consequence of (3.4), (3.5). \[\square\]
We will call the transforming of $K$ and $M$ into $K_1$ and $M_1$, described by (3.3), as "increasing of $K$ by $x$" and "decreasing of $M$ by $x"). Similarly, we will speak of "decreasing of $K$" and "increasing of $M$" by $x$, when transformation is described by (3.8). In the latter case (3.4), (3.5), and (3.8) all hold as well, provided $|K| > \beta_x(K)$.

4. Proof of Theorem 1

4.1. Induction. Let $K, M$ satisfy (1.2) and (1.3). Let $|M| > 2$. Choose $q \in G$ such that

$$s = \beta_q(K) = \beta_q(M)$$

is minimal. Obviously, we can assume that $s < |M|$ and $s > 1$. The proof is by induction on $s$ with Proposition 2.3 proving the case $s = 1$. Suppose $s \geq 2$. The induction hypothesis is: for all finite subsets $A, B \subseteq G$, satisfying

$$|A|, |B| \geq 2,$$

and

$$|AB| = |A| + |B| - 1,$$

if $\beta_s(A) = \beta_s(B) < s$ for some $g \in G$, then an element $x \in G, x \neq 1$ can be found such that

$$\beta_s(A) = \beta_s(B) = 1.$$

Now, starting with $K_0 = K$ and $M_0 = M$ we begin by transforming $K_i, M_i$ into $K_{i+1}, M_{i+1} (i = 0, 1, ...)$, every time increasing $K_i$ and decreasing $M_i$ by $q$. The number of $q$-segments in $K_{i+1}, M_{i+1}$ is not greater than that of $K_i, M_i$ and by (3.9)

$$|K_i M_i| = |K_i| + |M_i| - 1.$$

We stop this process as soon as the number of $q$-segments in $K_n, M_n$ becomes less than $s$. Since $M$ is finite (3.1) guarantees the termination of the process which can create one of the following situations:

(i) The number of $q$-segments in $K_n, M_n$ becomes less than $s$, while $|M_n| \geq 2$. Then by induction

$$\exists x \in G, \ x \neq 1 \text{ such that: } \beta_x(M_n) = \beta_x(K_n) = 1.$$

But $K \subseteq K_n$ so $K$ is contained in one $\langle x \rangle$-coset and Proposition 2.3 completes the proof.
(ii) At some step \( n \) of the process \( M_n \) becomes empty. Then

\[ |M_{n-1}| - \beta_q(M_{n-1}) - s, \]

otherwise the process would have terminated earlier. We know, however, that

\[ \exists g \in G \text{ such that: } \beta_g(M_{n-1}) < |M_{n-1}|, \]

whence \( \beta_g(M_{n-1}) < s \) and induction may be applied to \( M_{n-1}, K_{n-1} \). The proof is completed similarly to (i).

(iii) At some step \( n \) of the process it happens that only one element is left in \( M_n \): \( |M_n| = 1 \). This means that all the \( q \)-segments of \( M \) but one are of equal length, while one segment is "one element longer." The rest of the work deals just with this case, which is finally proved to be impossible.

4.2. Nontrivial Case. We are now in the situation (iii) of 4.1. From now on we will work mainly with subsets \( K_{n-1} \) and \( M_{n-1} \) which will be henceforth denoted by \( K \) and \( M \). Thus

\[ |M| = s + 1, \quad (4.2.1) \]

and \( M \) consists of \( s - 1 \) \( q \)-segments of length 1 and one \( q \)-segment of length 2. Let \( M = \{b_1, qb_1 = b_2, b_3, \ldots \} \). Denoting \( y = b_3b_1^{-1} \) we notice that

\[ \beta_y(M) \leq |M| - 1 = s. \]

If \( \beta_y(M) < s \) then by induction \( M \) would be an \( x \)-segment for some \( x \in G \), which is a contradiction to the structure of \( M \). Therefore, assume

\[ \beta_y(M) = s. \]

Taking now the set \( M b_1^{-1} \) instead of \( M \), we obtain (denoting the new set also by \( M \))

\[ M = \{1, q, y, \ldots \}, \quad q \neq y \quad (4.2.2) \]

and, using the above argument,

\[ \beta_g(M) = s \quad \forall g \in M, \quad g \neq 1. \quad (4.2.3) \]

We have to clarify also the structure of \( K \). Let \( g \) be any non-trivial element of \( M \). Then (4.2.3) shows that \( |M| > \beta_g(M) \) so (3.4) implies

\[ \beta_g(K) = s, \quad \forall g \in M, \quad g \neq 1. \quad (4.2.4) \]
Let us organize now the transformation process, decreasing $K$ and increasing $M$ by $g$. If this process will terminate in the situations similar to (i) or (ii) of 4.1 then the arguments used there would yield that $K$ and $M$ are segments, which is a contradiction with the structure of $M$ again. Therefore assume that this transformation would also terminate in the situation similar to (iii) of 4.1. This means that $K$ consists of $s - 1$ $g$-segments of equal length $l$ and of one $g$-segment of length $l + 1$, so

$$|K| = ls + 1. \quad (4.2.5)$$

We will need later the two auxiliary results on the structure of $K$:

**Lemma 4.2.1.** $l \geq 2$, so $|K| \geq 2s + 1$.

**Proof.** Suppose the opposite and let $l = 1$, and $|K| = |M|$. For any $x \in G, x \neq 1$

$$|M \cap xM| \leq 1, \quad (4.2.6)$$

since otherwise $\beta_s(M)$ would be less than $|M| - 1 = s$ and $M$ would be a segment by induction. Let

$$K = \{a_1, \ldots, a_{s+1}\}, \quad M = \{b_1, \ldots, b_{s+1}\}.$$ 

The elements of $KM$ would then form a matrix

$$KM = \begin{pmatrix}
    a_1b_1 & a_1b_2 & \cdots & a_1b_{s+1} \\
    a_2b_1 & a_2b_2 & \cdots & a_2b_{s+1} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{s+1}b_1 & a_{s+1}b_2 & \cdots & a_{s+1}b_{s+1}
\end{pmatrix}.$$

No two rows of this matrix may have more than one pair of equal elements. Indeed, if, for example, it would not be so for the first two rows and

$$a_i b_j = a_2 b_j, \quad a_i b_k = a_2 b_k,$$

then, denoting $x = a_2^{-1} a_1$ we obtain

$$xb_j = b_j, \quad xb_k = b_k,$$

and $|M \cap xM| \geq 2$ in contradiction with (4.2.6). The number of distinct elements of $KM$ will therefore be not less than

$$(s + 1) + ((s + 1) - 1) \times ((s + 1) - 2) + \cdots + 1 = \frac{(s + 1)(s + 2)}{2},$$
implying

$$|KM| = 2s + 1 \geq \frac{s^2 + 3s + 2}{2}$$

whence $s = 1$, which is impossible.  ■

Let $g$ be any non-trivial element of $M$. Denote by $C_g(K)$ the number of right $\langle g \rangle$-cosets, having a non-empty intersection with $K$, and $C_g(M)$ the number of left $\langle g \rangle$-cosets, having a non-empty intersection with $M$.

**Lemma 4.2.2.** Each $g$-segment of $K$ and $M$ belongs to a different $\langle g \rangle$-coset, so

$$C_g(K) = C_g(M) = s. \quad (4.2.7)$$

**Proof.** Obviously, $C_g(K) \leq s$, $C_g(M) \leq s$. First, we prove that $C_g(K) = s$.

Suppose that $C_g(K) < s$ and let

$$K = \bigcup_{i=1}^{C_g(K)} K^i$$

be the representation of $K$ as a disjoint union of its subsets, each belonging to a different $\langle g \rangle$-coset. Let

$$M = \bigcup_{i=1}^{C_g(M)} M^i$$

be a similar representation of $M$. We examine two cases.

(i) $C_g(K) \geq C_g(M)$. Then $C_g(M) \leq s - 1$ and (4.2.1), (4.2.3) allow us to pick $M^{m_i} \subseteq M$, $M^{m_i}$ not being a segment, and satisfying

$$|M^{m_i}| \geq |M^i|, \quad 1 \leq i \leq C_g(M).$$

Then

$$|KM| \geq |KM^{m_i}| = \sum_{i=1}^{C_g(K)} |K^i M^{m_i}|,$$

and since by Lemma 4.2.1, $|K'| \geq 2$, Proposition 2.3 implies

$$|K^i M^{m_i}| \geq |K'| + |M^{m_i}| \quad \forall i, 1 \leq i \leq C_g(K),$$

whence

$$|KM| \geq |K| + C_g(K) \cdot |M^{m_i}| \geq |K| + C_g(M) \cdot |M^{m_i}| \geq |K| + |M|,$$

which is a contradiction.
(ii) $C_g(K) < C_g(M)$. We decrease $K$ and increase $M$ by $g$, obtaining $K'$ and $M'$ correspondingly. Now every $g$-segment of $M'$ consists of at least two elements. Also, by Lemma 4.2.1, $|K'| \geq s + 1$ and we arrive at a contradiction similarly to (i), by choosing $K''$ as a subset of maximal order among all $K''$, which is not a segment, and multiplying $K''$ by $M'$. Thus, we proved that $C_g(K) = s$.

Suppose now that $C_g(M) < s$. Repeating arguments of (i) we once more get a contradiction that finally proves (4.2.7).

We know that $|KM| = |K| + |M| - 1 = |K| + s$ so, by (4.2.4),

$$KM = K \cup Kg \quad \forall g \in M, \quad g \neq 1.$$  \hspace{1cm} (4.2.8)

It means that the sets of the upper elements of (right) $g$-segments of $KM$ coincide for all non-trivial $g \in M$. We denote this set by

$$\overline{KM} = KM \setminus K.$$  \hspace{1cm} (4.2.9)

For the proof of Theorem 1 we will need the similar result for $K$, which is proved separately in Section 5:

**Proposition 4.2.** Let $q, y$ be two non-trivial elements of $M$. Then the sets of the upper elements of $q$-segments of $K$ and of $y$-segments of $K$ coincide.

Let us denote the set of Proposition 4.2 by $\overline{K}$. Then (4.2.8) implies

$$\overline{K} = (\overline{KM})q^{-1} = (\overline{KM})y^{-1}.$$  \hspace{1cm} (4.2.10)

Let $c$ be an arbitrary element of $K \subseteq K$. Then $cq \in KM$, $cq \notin K$, so $cq \in \overline{KM}$.

It means, by (4.2.10), that

$$(cq)y^{-1} \in \overline{K}.$$  

Taking $cqy^{-1}$ instead of $c$ yields

$$(cqy^{-1})qy^{-1} \in \overline{K}.$$  

Continuing in this way we will obtain an infinite number of elements, belonging to $\overline{K}$:

$$c(qy)^{-1} \in \overline{K}, \quad i = 1, 2, ....$$  

$\overline{K}$ is finite, so for some $n > 0$

$$(qy^{-1})^n = 1,$$
but $G$ is torsion-free, so

$$q = v,$$

which is a contradiction. This proves that case (iii) of 4.1 is impossible and completes the proof of Theorem 1.

5. PROOF OF PROPOSITION 4.2

Proposition 4.2 states that $K_y = K_y$ (see (3.2)). Suppose the contrary. Let us decrease $K$ and increase $M$ by $q$, obtaining $K'$ and $M'$. Then (4.2.3) implies

$$|M'| = |M| + s = 2s + 1$$

and (4.2.4) together with Lemma 4.2.1 yields

$$|K'| = |K| - s \geq 2.$$ 

We will try now to determine $\beta_y(M')$. Obviously,

$$\beta_y(M') \leq |M'| - 1 = 2s,$$ 

(5.1)

since in $M'$ there is at least one $y$-segment of length not less than 2, namely $\{1, y, \ldots\}$. Also, $C_y(M') \geq C_y(M)$ and by Lemma 4.2.1, $C_y(M') \geq s$, whence $\beta_y(M') \geq s$. Now, if

$$s + 1 \leq \beta_y(M') \leq 2s - 1$$ 

(5.2)

then decrease $M'$ and increase $K'$ by $y$, obtaining $M''$ and $K''$. But

$$|M''| = |M'| - \beta_y(M'),$$

so (5.2) implies that

$$s \geq |M''| \geq 2.$$ 

(5.3)

We know that there exist $g \in G, g \neq 1$, such that

$$\beta_g(M'') < |M''|,$$

so (5.3) allows us to apply induction again and conclude that $K$ and $M$ are segments, which is a contradiction. In view of (5.1) only two cases are left for consideration:

Case (i): $\beta_y(M') = s$,

Case (ii): $\beta_y(M') = 2s$. 

Case (i). Assume $\beta_s(M') = s$. We state that there are no $y$-segments of length 1 in $M'$. Indeed, if there were such segments, then, decreasing $M'$ and increasing $K'$ by $y$, we would obtain $M''$ and $K''$ with $\beta_s(M'') < s$ and $|M''| = s + 1 \geq 2$, so applying induction we get a contradiction as before. Assume, therefore, that $M'$ consists of $s - 1$ $y$-segments of length 2 and one $y$-segment of length 3. Since we supposed Proposition 4.2 to be wrong, let

$$x \in K' \cap K_y.$$  

(5.4)

We need two simple lemmas.

**Lemma 5.1.** Let $b$ be any non-trivial element of $M$. Then $yb \notin M'$.

**Proof.** Suppose $yb \in M'$. Then

$$x(yb) \in K'M' = KM,$$

according to the set transformation property (3.5). But (5.4) implies $xy \in KM$ and $xy \notin K$, so (see (4.2.9))

$$xy \in \overline{KM},$$

and $xy$ is an upper element of some $b$-segment of $KM$. Applying now Lemma 4.2.2 we see that every $\langle b \rangle$-coset contains at most one $b$-segment, so

$$(xy)b \notin KM,$$

which is a contradiction. 

**Lemma 5.2.** If $b_1$, $b_2$, and $b_3$ are any non-trivial elements of $M$ then

$$b_1 \neq b_2b_3.$$

**Proof.** If $b_1 = b_2b_3$ then we obtain two $b_2$-segments of length at least 2 in $M$: $Q_1 = \{1, b_2, \ldots\}$ and $Q_2 = \{b_3, b_1, \ldots\}$, which is a contradiction to (4.2.3).

Consider now the $y$-segment of $M'$ that contains $q$. By the argument given above, it has length not less than 2, so either $yq \in M'$ or $y^{-1}q \in M'$. The former case is impossible according to Lemma 5.1, so

$$y^{-1}q \in M'.$$

Since $M' = M \cup qM$ we obtain that either

$$y^{-1}q = b_i,$$

(5.5)
or

\[ y^{-1}q = qb_i, \quad (5.6) \]

where \( b_i \) is some non-trivial element of \( M \). However, (5.5) implies \( q = yb_i \), which is impossible by Lemma 5.2, so (5.6) holds. Recall now that \( M' \) contains also a \( y \)-segment of length \( 3 - \{ h, yh, y^2h \} \), where \( h \) is some element of \( M' \). Again, either

\[ h = b_j, \quad (5.7) \]

or

\[ h = qb_j, \quad (5.8) \]

where \( b_j \in M \). If (5.7) takes place then \( M' \) contains elements of the form \( yb_j \) and Lemma 5.1 implies that \( x = b_j = 1 \). But then \( y^2 \in M' \), which contradicts Lemma 5.1. Thus, (5.8) holds. We now use the same arguments regarding another element from this segment, \( yh \in M' \). Either

\[ yh = b_i, \quad (5.9) \]

or

\[ yh = qb_i, \quad (5.10) \]

where \( b_i \in M \). Suppose (5.9) holds, then \( y^2h = yb_i \in M' \) and Lemma 5.1 implies that \( b_i = 1 \) and \( y^{-1} = h \). Then (5.8) and (5.6) yield

\[ y^{-1} = qb_i q^{-1} = qb_j, \]

and \( b_i = qb_j \). Lemma 5.2 would then imply that \( b_j = 1 \), which was proved to be impossible earlier. Thus (5.10) holds, and together with (5.6), (5.8) yields

\[ yh = y(qb_j) = qb_i^{-1}b_j = qb_j, \]

and

\[ b_j = b_ib_i. \]

Lemma 5.2 shows that \( b_i = 1 \), so \( yh = q \) and

\[ y^2h = yq \in M', \]

which is a contradiction according to Lemma 5.2. Thus, we got a contradiction in Case (i).
Case (ii). Assume now $\beta_y(M') = 2s$. Lemma 4.2.1 shows that there exists a $y$-segment $P$ of length not less than 2 in $K'$ and we may assume $P = \{1, y, \ldots\}$. Then

$$|K'M'| \geq |PM'| \geq |M'| + \beta_y(M') = 4s + 1,$$

so

$$|K'| + |M'| - 1 = |K'| + (2s + 1) - 1 \geq 4s + 1,$$

and

$$|K'| \geq 2s + 1.$$

Let us determine $\beta_y(K')$. We know that $\beta_y(K) = s$ and that $K'$ is obtained by extracting $s$ elements out of $K$, so

$$\beta_y(K') \leq 2s,$$

since taking out an element we add at most one segment to a set. Thus, $|K'| > \beta_y(K')$ and Proposition 3.1 implies

$$\beta_y(K') = 2s. \quad (5.11)$$

By Lemma 4.2.2, $C_y(K) = s$. Let

$$K' = \bigcup_{i=1}^{C_y(K')} K'i$$

be the representation of $K'$ as a disjoint union of its subsets, each belonging to a different $\langle y \rangle$-coset. Then, since $C_y(K') \leq C_y(K)$, there exist $K''^m \subseteq K'$, $1 \leq m \leq C_y(K')$, such that

$$|K''^m| \geq l$$

(see (4.2.5)). Let

$$M' = \bigcup_{i=1}^{C_y(M')} M'^i$$

be a corresponding representation of $M'$. Suppose that there exist $M''^n \subseteq M'$ with

$$|M''^n| \geq 3.$$

Then, according to (5.11), at least one of $K'^i$ is bound not to be a segment, and

$$|K'M'| \geq |K'M''^n| = \sum_{i=1}^{C_y(K')} |K'^i M''^n| > \sum_{i=1}^{C_y(K')} |K'^i| + 2s.$$
Hence,
\[ |K'M'| > |K'| + |M'| - 1, \]
which is a contradiction. Hence
\[ |M''_i| \leq 2, \quad \forall i, 1 \leq i \leq C_j(M'), \]
so \( C_j(M') \geq s + 1 \). Multiplying again \( K''m \) by \( M' \) we obtain
\[ |K'M'| \geq |K''mM'| \geq |M'| + (l - 1)(s + 1) = |M'| + |K'| - 1 + (l - 1), \]
whence \( l = 1 \). Thus, Case (ii) also implies a contradiction. This completes the proof of Proposition 4.2.

REFERENCES
