ON BASES FOR $\sigma$-FINITE GROUPS

Y. O. HAMIDOUNE and Ö. J. RÖDSETH

Abstract.

Let $A$ be a subset of a $\sigma$-finite group $G$, such that $A$ contains the identity element. Let $d$ and $\delta$ denote the lower density of $A$ and the upper asymptotic density of $A$, respectively. Let $K$ be the subgroup generated by $A$. We show that $A$ is a $\sigma$-basis for $K$ of exact order at most $\max\{2, 2/\delta - 1\}$, and that $A$ is a basis for $K$ of exact order at most $\max\{2, 2/\delta - 1\}$. Also some sharper results are obtained under more restrictive conditions.

1. Introduction.

Let $G$ be a multiplicative group with identity element $1$. Let $A$ and $B$ be nonempty subsets of $G$. We denote the cardinality of $A$ by $|A|$, and the subgroup generated by $A$ is denoted by $\langle A \rangle$. The product $AB$ is the set of all element of the form $ab$, where $a \in A$ and $b \in B$. The product of more than two sets is defined similarly. In particular, for a positive integer $r$, we write $A^r$ for the set of all products of $r$ elements of $A$. For a positive integer $h$ the set $A$ is a basis of order $h$ for $G$, if $A^h = G$. The least $h$ possessing this property is the exact order of $A$.

Let $G_1 \subseteq G_2 \subseteq \ldots$ be an increasing sequence of finite subgroups of $G$. Then $G$ is $\sigma$-finite with respect to the sequence $\{G_i\}$ if $G = \bigcup_{i=1}^{\infty} G_i$. Clearly, if $G$ is $\sigma$-finite, then $G$ is a countable torsion group.

We further put $A_i = A \cap G_i$ for $i = 1, 2, \ldots$. Suppose that there is an $h$ (independent of $i$) such that $A_i$ is a basis of order $h$ for $G_i$ for $i = 1, 2, \ldots$ Then $A$ is a $\sigma$-basis of order $h$ for $G$ with respect to the sequence $\{G_i\}$. Again, the least $h$ possessing this property is the exact order of $A$. Clearly, every $\sigma$-basis for $G$ of order $h$ is a basis for $G$ of order $h$. The converse is not true; see Exercise 4 in Nathanson [12, Section 4.6].

For $G$ $\sigma$-finite with respect to the sequence $\{G_i\}$, we define the lower density $d(A)$ of the set $A$ with respect to $\{G_i\}$ by

$$d(A) = \inf_{i \geq 1} \frac{|A_i|}{|G_i|}.$$
and the upper asymptotic density \( \delta(A) \) of the set \( A \) with respect to \( \{G_i\} \) by

\[
\delta(A) = \limsup_{i \to \infty} \frac{|A_i|}{|G_i|}
\]

The additive group of polynomials over the finite field \( \mathbb{F}_q \) is \( \sigma \)-finite with respect to \( \{G_i\} \), if \( G_i \) is the additive group of polynomials over \( \mathbb{F}_q \) of degree less than \( i \). Denoting the set of all sums of two irreducible polynomials in \( \mathbb{F}_q[x] \) by \( 2P \), it was shown by Cherly [1] that \( 2P \) generates \( \mathbb{F}_q[x] \) and \( d(2P) > 0 \). Motivated by these facts, Cherly [2] and later Cherly and Deshouillers [3] considered the case of a generating subset \( A \) of \( \mathbb{F}_q[x] \) satisfying \( d(A) > 0 \). In [3] it was shown that such an \( A \) is a basis for \( \mathbb{F}_q[x] \) of exact order at most \( 4/d(A) \).

The result of Cherly and Deshouillers was strengthened by Jia and Nathanson [6], who showed that if \( A \) is a subset of a \( \sigma \)-finite abelian group \( G \) such that \( 1 \in A \) and \( \delta(A) > 0 \), then \( A \) is a basis for \( K = \langle A \rangle \) of exact order at most \( 4/\delta(A) \).

In this paper we improve the bound of Jia and Nathanson to \( \max \{2, 2/\delta(A) - 1\} \) without assuming \( G \) to be abelian. We also show that \( A \) is a \( \sigma \)-basis for \( K \) of exact order at most \( \max \{2, 2/d(A) - 1\} \) with respect to a certain increasing sequence of finite subgroups of \( K \). Both these results are deduced from the result that if \( K \) is finite, then \( A \) is a basis for \( K \) of exact order at most \( \max \{2, 2/|K|/|A| - 1\} \), and this result is in turn deduced from a theorem of Olson [13]. In Section 4 some sharper results are obtained under more restrictive conditions.

2. Preliminaries.

Let \( A, B \) be finite nonempty subsets of \( G \). We write \( B^{-1} \) for the set of elements \( b^{-1} \), \( b \in B \), and \( xB \) for \( \{x\}B \), \( x \in G \). Also, put \( |AB| = |A| + |B| - k \).

It is known that every element \( c \in AB \) has at least \( k \) representations as a product \( c = ab \) with \( a \in A \), \( b \in B \). This result goes back to L. Moser and P. Scherk in the case of abelian \( G \), and was proved for nonabelian groups by J. H. B. Kemperman and (independently) D. F. Wehn. A proof can be found in Kemperman's paper [7]. Based on this result Olson [13] gave a simple proof of the theorem below. Olson [14] later gave a more general result, but the result cited below is all we shall need in this paper.

**Olson's Theorem.** If \( 1 \in A \) and \( r \) is a positive integer, then \( A^r = \langle A \rangle \) or

\[
|A^r| \geq |A| + (r - 1) \left\lfloor \frac{|A|}{2} \right\rfloor.
\]
We shall on some occasions need the following fact:

\begin{equation}
G = AB \text{ or } |G| \geq |A| + |B|.
\end{equation}

This is easy to see. For if \( x \in G \setminus AB \), then \( A \cap xB^{-1} = \emptyset \). Hence \( |G| \geq |A| + |xB^{-1}| = |A| + |B| \).

Olson's theorem now gives us Lemma 1 below; cf. Theorem 7.2 in Hamidoune [5] and the proposition in Rödseth [15].

**Lemma 1.** Let \( G \) be a finite group, and let \( A \) be a subset of \( G \). Subset that \( 1 \in A \) and that \( A \) generates \( G \). Then \( A \) is a basis for \( G \) of exact order at most

\[ \max \left\{ 2, 2 \frac{|G|}{|A|} - 1 \right\}. \]

**Proof.** Suppose that \( A \) has exact order \( h \geq 3 \). Then \( G = AA^{h-2} \), so that by (1),

\[ |G| \geq |A| + |A^{h-2}|. \]

By Olson's theorem,

\[ |A^{h-2}| \geq |A| + (h - 3) \frac{|A|}{2}, \]

and Lemma 1 follows.

3. **Bases for \( \sigma \)-finite groups.**

Let \( G \) be \( \sigma \)-finite with respect to the sequence \( \{G_i\} \). Let \( A \) be subset of \( G \), and put \( K = \langle A \rangle \).

As in Section 1, we put \( A_i = A \cap G_i, i = 1, 2, \ldots \) Then \( A_1 \subseteq A_2 \subseteq \cdots \) Putting \( K_i = \langle A_i \rangle \), we have that \( K_1 \subseteq K_2 \subseteq \cdots \) is an increasing sequence of subgroups of \( K \). Each \( K_i \) is finite since \( K_i \subseteq G_i \), and it is easily seen that \( A_i = A \cap K_i, i = 1, 2, \ldots \) We also have

\begin{equation}
K = \bigcup_{i=1}^{\infty} K_i,
\end{equation}

so that \( K \) is \( \sigma \)-finite with respect to the sequence \( \{K_i\} \).

To see that (2) holds, it is sufficient to show that \( K \) is contained in the right hand side. First, suppose that \( a \in A \). Then \( a \in G \), so that there is an \( i \) such that \( a \in G_i \). Hence \( a \in A \cap G_i = A_i \). Now let \( k \in K \). Since \( K = \langle A \rangle \), we then have

\[ k = a_{i_1}^{\pm 1} \cdots a_{i_m}^{\pm 1}, a_{j_i} \in A_{j_i}. \]

Putting \( j = \max_{1 \leq i \leq m} j_i \), we have \( a_{j_i} \in A_j \) for \( i = 1, \ldots, m \). Hence \( k \in \langle A_j \rangle = K_j \), which completes the proof of (2).
We also put

\[ \delta_{K}(A) = \limsup_{i \to \infty} \frac{|A_i|}{|K_i|}. \]

Since \( |G_i| \geq |K_i| \) for all \( i \), we then have

\[ \delta_{K}(A) \geq \delta(A). \]

**Theorem 1.** Let \( G \) be a group which is \( \sigma \)-finite with respect to the sequence of subgroups \( \{G_i\} \). Let \( A \) be a subset of \( G \) such that \( 1 \in A \) and \( d(A) > 0 \), where \( d(A) \) is the lower density of \( A \) with respect to \( \{G_i\} \). Then \( K = \langle A \rangle \) is \( \sigma \)-finite, and \( A \) is a \( \sigma \)-basis for \( K \) of exact order at most

\[ \max \left\{ 2, \frac{2}{d(A)} - 1 \right\}. \]

**Proof.** Since \( 1 \in A_i \) and \( A_i \) generates the finite group \( K_i \), Lemma 1 gives us that \( A_i \) is a basis for \( K_i \) of exact order at most \( \max \left\{ 2, \frac{|K_i|}{|A_i|} - 1 \right\} \). Hence \( A \) is a \( \sigma \)-basis for \( K \) of exact order at most

\[ \max \left\{ 2, 2 \sup_{i \geq 1} \frac{|K_i|}{|A_i|} - 1 \right\} \leq \max \left\{ 2, 2 \sup_{i \geq 1} \frac{|G_i|}{|A_i|} - 1 \right\} = \max \left\{ 2, \frac{2}{d(A)} - 1 \right\}, \]

which completes the proof of Theorem 1.

**Theorem 2.** Let \( G \) be a group which is \( \sigma \)-finite with respect to the sequence of subgroups \( \{G_i\} \). Let \( A \) be a subset of \( G \) such that \( 1 \in A \) and \( \delta(A) > 0 \), where \( \delta(A) \) is the upper asymptotic density of \( A \) with respect to \( \{G_i\} \). Then \( A \) is a basis for \( K = \langle A \rangle \) of exact order at most

\[ \max \left\{ 2, \frac{2}{\delta(A)} - 1 \right\}. \]

**Proof.** By (4) and the condition \( \delta(A) > 0 \), we have \( \delta_{K}(A) > 0 \). Given an arbitrary \( \varepsilon \) in the interval \( 0 < \varepsilon < \delta_{K}(A) \). Let \( k \in K = \langle A \rangle \). Then there exists an \( i \) such that \( k \in K_i \) and

\[ \frac{|A_i|}{|K_i|} \geq \delta_{K}(A) - \varepsilon. \]

By Lemma 1, there exists a positive integer \( h \) such that \( k \in A_i^h \) and

\[ h \leq \max \left\{ 2, 2 \frac{|K_i|}{|A_i|} - 1 \right\}, \]

so that

\[ h \leq \max \left\{ 2, \frac{2}{\delta_{K}(A)} - \varepsilon - 1 \right\}. \]
We thus have that for an arbitrary \( \varepsilon \) in the interval \( 0 < \varepsilon < \delta_k(A) \), there is an \( h \) satisfying (5) such that \( A^h = K \). Hence,
\[
h \leq \max \left\{ 2, \frac{2}{\delta_k(A)} - 1 \right\} \leq \max \left\{ 2, \frac{2}{\delta(A)} - 1 \right\},
\]
where we also used (4).

**Example 1.** For an integer \( n \geq 3 \), let \( G \) be the additive group \( \mathbb{Z}_n[X] \), and let \( G_i \) be the subgroup consisting of all polynomials of degree strictly less than \( i \). Let \( A \) be the set of polynomials with constant term 0 or 1. Then \( A \) is a basis for \( G \) of exact order \( n - 1 \). We also have \( d(A) = \delta(A) = 2/n \), and we see that both Theorem 1 and Theorem 2 are "sharp".

4. Further results.

It is possible to improve upon the bound given in Lemma 1 by imposing additional restrictions upon the set \( A \). Improvements of the bound in Lemma 1 give similar improvements of the bounds in Theorem 1 and Theorem 2.

Here we shall improve upon Theorem 2 in the two cases \( A \cap A^{-1} = \{1\} \) and \( A = A^{-1} \). For the sake of simplicity we shall deduce our results from a well-known theorem of Kneser [9], [10], [11]. Kneser's theorem holds, however, only for an abelian \( G \). In this section we therefore assume \( G \) to be abelian. For the nonabelian case we refer the reader to the paper [5].

**Kneser's theorem.** Let \( A, B \) be nonempty finite subsets of an abelian group \( G \). Let \( H \) be the largest subgroup of \( G \) satisfying \( ABH = AB \). Then
\[
|AB| \geq |AH| + |BH| - |H|.
\]

A nice proof of Kneser's theorem can be found in [8]. That proof is also presented in both [12] and [16].

**Lemma 2.** For a positive integer \( r \), let \( H \) be the largest subgroup of \( G \) satisfying \( A'H = A' \). Then
\[
|A'| \geq r|AH| - (r - 1)|H|.
\]

**Proof.** Putting \( H = H_r \), notice that \( H_1 \subseteq H_2 \subseteq \cdots \). Now, use Kneser's theorem and induction or \( r \) to prove that \( |A'| \geq r|A| - (r - 1)|H_r| \). Then apply this result with \( A \) replaced by \( AH_r \).

Now, suppose that \( 1 \in A \) and that \( A \) generates \( G \). Let \( h \) be the exact order of \( A \). Also, assume that \( h \geq 3 \). Let \( H \) be the largest subgroup of \( G \) satisfying \( A^{h-2}H = A^{h-2} \). Then \( (AH)A^{h-2} = G \), and (1) gives
ON BASES FOR $\sigma$-FINITE GROUPS

$|G| \geq |AH| + |A^{h-2}|.$

By Lemma 2, we get

(6) $|G| \geq (h - 1)|AH| - (h - 3)|H|$ for $h \geq 3$.

We have that $AH$ is a disjoint union of $s \geq 1$ $H$-cosets. Since $1 \in A$, one of these cosets is $H$ itself. If $s = 1$, then $A \subseteq H$, so that $G = \langle A \rangle \subseteq H$. This implies $A^{h-2} = G$, a contradiction. Hence $s \geq 2$.

By (6), we also have

(7) $|G| \geq ((h - 1)s - (h - 3))|H|.$

Further we have $|A| \leq |AH| = s|H|$, so that by (7),

(8) $|G| \geq \left(h - 1 - \frac{h - 3}{s}\right)|A|.$

Since $s \geq 2$, this inequality gives us immediately Lemma 1 for the special case of $G$ being abelian.

Here we use this method to prove Lemma 3 and Lemma 4 below.

**Lemma 3.** Let $A$ be a subset of the finite abelian group $G$. Suppose that $1 \in A$, $A = A^{-1}$, and that $A$ generates $G$. Then $A$ is a basis for $G$ of exact order $h$, where

$$ h \leq \max \left\{ 2, \frac{3|G|}{2|A|} \right\}. $$

**Proof.** Suppose that $h \geq 3$. For the number $s$ defined above, suppose that $s = 2$. Then $AH = H \cup aH$ for some $a \notin H$. Since $A = A^{-1}$, we have

$$ H \cup a^{-1}H = (AH)^{-1} = AH = H \cup aH, $$

so that $a \in a^{-1}H$. Hence $a^2 \in H$, and it follows that $(AH)^2 = AH$. Since $A$ generates $G$, we thus have $AH = G$, so that $A^{h-2} = A^{h-2}H = G$, a contradiction. Thus $s \geq 3$, and Lemma 3 follows immediately from (8).

**Theorem 3.** Let $G$ be an abelian $\sigma$-finite group. Let $A$ be a subset of $G$ such that $1 \in A$, $A = A^{-1}$, and $\delta(A) > 0$. Then $A$ is a basis for $K = \langle A \rangle$ of exact order at most

$$ \max \left\{ 2, \frac{3}{2\delta(A)} \right\}. $$

**Proof.** Clearly, $1 \in A_i$ and $A_i = A_i^{-1}$. Hence, by Lemma 3, $A_i$ is a basis for $K_i$ of exact order at most

$$ \max \left\{ 2, \frac{3|K_i|}{2|A_i|} \right\}. $$

Now, Theorem 3 follows in the same way as we deduced Theorem 2 from Lemma 1.
EXAMPLE 2. Let $n$, $G$, $G_i$ be as in Example 1. This time, let $A$ be the set of polynomials with constant term $-1, 0$, or $1$. Then $A$ satisfies the conditions of Theorem 3. We have that $A$ is a basis for $G$ of exact order $[n/2]$, and that $\delta(A) = 3/n$. This shows that Theorem 3 is sharp.

**Lemma 4.** Let $A$ be a subset of the finite abelian group $G$. Suppose that $A \cap A^{-1} = \{1\}$ and that $A$ generates $G$. Then $A$ is a basis for $G$ of exact order $h$, where

$$h \leq \max \left\{ \frac{|G|}{|A| - \frac{1}{2}} + 1, \frac{3}{2} \cdot \frac{|G|}{|A| - \frac{1}{2}} - 1 \right\}.$$  

**Proof.** Since $A \cap A^{-1} = \{1\}$, we have $2|A| - 1 \leq |G|$. Therefore (9) holds if $h \leq 2$.

Suppose that $h \geq 3$. Since $A \cap A^{-1} = \{1\}$, at most one of the statements $x \in A$, $x^{-1} \in A$ holds for $1 \neq x \in H$. Hence,

$$s|H| = |AH| \geq |A \cup H| \geq |A| + \frac{|H| - 1}{2},$$

and by (7),

$$|G| \geq \left( h - 1 - \frac{h - 5}{2s - 1} \right) \left( |A| - \frac{1}{2} \right),$$

so that

$$h \leq \frac{|G|}{|A| - \frac{1}{2}} + 1 \text{ if } h \leq 5,$$

and, since $s \geq 2$,

$$h \leq \frac{3}{2} \cdot \frac{|G|}{|A| - \frac{1}{2}} - 1 \text{ if } h \geq 5.$$ 

This completes the proof of Lemma 4.

**Theorem 4.** Let $G$ be a group which is abelian, infinite, and $\sigma$-finite. Let $A$ be a subset of $G$ such that $A \cap A^{-1} = \{1\}$ and $\delta(A) > 0$. Then $A$ is a basis for $K = \langle A \rangle$ of exact order $h$, where

$$h \leq \max \left\{ \frac{1}{\delta(A)} + 1, \frac{3}{2\delta(A)} - 1 \right\}.$$  

**Proof.** The conditions $G$ infinite and $\delta(A) > 0$ imply that $|A_i| \to \infty$ as $i \to \infty$. Hence $|K_i| \to \infty$ as $i \to \infty$, so that for $\delta_k(A)$ given by (3), we also have
\[ \delta_k(A) = \limsup_{i \to \infty} \frac{|A_i| - \frac{1}{2}}{|K_i|}. \]

Further we have \( A_i \cap A_i^{-1} = \{1\} \), and Theorem 4 now follows from Lemma 4 in the same way as Theorem 2 followed from Lemma 1.

**Example 3.** Suppose that \( n > 3 \) is odd, and let \( G, G_i \) be as in Example 1. Let the set \( B \) consist of 0 and all polynomials with constant term 0 and leading coefficient congruent mod \( n \) to some integer in the interval \( 1 \leq c \leq (n - 1)/2 \). Let \( A \) be the union of \( B \) and the set of all polynomials with constant term 1. Then the conditions of Theorem 4 are satisfied. We see that \( A \) is a basis for \( G \) of exact order \( n - 1 \), and that \( |A_i| = (3n^{i-1} + 1)/2 \), so that \( \delta(A) = 3/2n \). This shows that Theorem 4 is sharp.

**5. Postscript.**

Professor Melvyn B. Nathanson has kindly drawn our attention to the fact that for abelian \( G \), the bound given in Theorem 2 can be found in a handwritten manuscript by Deshouillers and Wirsing [4]. In that manuscript this result is deduced from a more complicated and general theorem on sumsets in \( \sigma \)-finite abelian groups.

Most of the results in this paper were independently obtained by each of the two present authors, after we read a presentation of the paper [6] in a preliminary version of Nathanson’s book [12]. On the suggestion of Professor Nathanson we merged our results into the present joint paper.

**REFERENCES**

4. J.-M. Deshouillers and E. Wirsing, Untitled manuscript, Undated.