MATH. SCAND. 78 (1996), 246–254

ON BASES FOR σ-FINITE GROUPS

Y. O. HAMIDOUNE and Ö. J. RÖDSETH

Abstract.

Let A be a subset of a σ-finite group G, such that A contains the identity element. Let d and δ 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 σ-basis for K of exact order at most $\max\{2, 2/d - 1\}$, 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 $G_1 \subseteq G_2 \subseteq \dots$ be an increasing sequence of finite subgroups of G. Then G is *σ-finite with respect to the sequence* $\{G_i\}$ if $G = \bigcup_{i=1}^{\infty} G_i$. Clearly, if G is σ-finite, then G is a countable torsion group.

We further put $A_i = A \cap G_i$ for $i = 1, 2, \dots$ Suppose that there is an h (independent of i) such that A_i is a basis of order h for G_i for $i = 1, 2, \dots$ Then A is a *σ-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 σ-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 σ-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

$$d(A) = \inf_{i \geq 1} \frac{|A_i|}{|G_i|},$$

Received October 3, 1994.

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 F_q is σ-finite with respect to $\{G_i\}$, if G_i is the additive group of polynomials over F_q of degree less than i. Denoting the set of all sums of two irreducible polynomials in $\mathsf{F}_q[x]$ by $2P$, it was shown by Cherly [1] that $2P$ generates $\mathsf{F}_q[x]$ 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 $\mathsf{F}_q[x]$ satisfying $d(A) > 0$. In [3] it was shown that such an A is a basis for $\mathsf{F}_q[x]$ 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 σ-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 σ-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*

$$|A^r| \geqq |A| + (r-1)\left\lceil \frac{|A|}{2} \right\rceil.$$

We shall on some occasions need the following fact:

(1) $$G = AB \text{ or } |G| \geqq |A| + |B|.$$

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

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 $h \geqq 3$. Then $G \neq AA^{h-2}$, so that by (1),

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

By Olson's theorem,

$$|A^{h-2}| \geqq |A| + (h-3)\frac{|A|}{2},$$

and Lemma 1 follows.

3. Bases for σ-finite groups.

Let G be σ-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 $K_1 \subseteq K_2 \subseteq \ldots$ 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

(2) $$K = \bigcup_{i=1}^{\infty} K_i,$$

so that K is σ-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

$$k = a_{j_1}^{\pm 1} \cdots a_{j_m}^{\pm 1}, \; a_{j_i} \in A_{j_i}.$$

Putting $j = \max_{1 \leqq i \leqq m} j_i$, 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

$$\delta_K(A) = \limsup_{i\to\infty} \frac{|A_i|}{|K_i|}. \tag{3}$$

Since $|G_i| \geqq |K_i|$ for all i, we then have

$$\delta_K(A) \geqq \delta(A). \tag{4}$$

THEOREM 1. *Let G be a group which is σ-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 σ-finite, and A is a σ-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 $\max\{2, 2|K_i|/|A_i| - 1\}$. Hence A is a σ-basis for K of exact order at most

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

which completes the proof of Theorem 1.

THEOREM 2. *Let G be a group which is σ-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 ε 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

$$\frac{|A_i|}{|K_i|} \geqq \delta_K(A) - \varepsilon.$$

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

$$h \leqq \max\left\{2, 2\frac{|K_i|}{|A_i|} - 1\right\},$$

so that

$$h \leqq \max\left\{2, \frac{2}{\delta_K(A) - \varepsilon} - 1\right\}. \tag{5}$$

We thus have that for an arbitrary ε in the interval $0 < \varepsilon < \delta_K(A)$, there is an h satisfying (5) such that $A^h = K$. Hence,

$$h \leqq \max\left\{2, \frac{2}{\delta_K(A)} - 1\right\} \leqq \max\left\{2, \frac{2}{\delta(A)} - 1\right\},$$

where we also used (4).

EXAMPLE 1. For an integer $n \geqq 3$, let G be the additive group $\mathbf{Z}_n[X]$, 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*

$$|AB| \geqq |AH| + |BH| - |H|.$$

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 $A^rH = A^r$. Then*

$$|A^r| \geqq r|AH| - (r - 1)|H|.$$

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 $|A^r| \geqq r|A| - (r - 1)|H_r|$. 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 $h \geqq 3$. Let H be the largest subgroup of G satisfying $A^{h-2}H = A^{h-2}$. Then $(AH)A^{h-2} \neq G$, and (1) gives

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

By Lemma 2, we get

$$|G| \geqq (h-1)|AH| - (h-3)|H| \quad \text{for } h \geqq 3. \tag{6}$$

We have that AH is a disjoint union of $s \geqq 1$ 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 $s \geqq 2$.

By (6), we also have

$$|G| \geqq ((h-1)s - (h-3))|H|. \tag{7}$$

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

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

Since $s \geqq 2$, 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*

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

PROOF. Suppose that $h \geqq 3$. 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 $s \geqq 3$, and Lemma 3 follows immediately from (8).

THEOREM 3. *Let G be an abelian σ-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 $\lfloor n/2 \rfloor$, 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*

$$h \leqq \max\left\{\frac{|G|}{|A| - \frac{1}{2}} + 1, \frac{3}{2} \cdot \frac{|G|}{|A| - \frac{1}{2}} - 1\right\}. \tag{9}$$

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

Suppose that $h \geqq 3$. 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,

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

and by (7),

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

so that

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

and, since $s \geqq 2$,

$$h \leqq \frac{3}{2} \cdot \frac{|G|}{|A| - \frac{1}{2}} - 1 \quad \text{if } h \geqq 5.$$

This completes the proof of Lemma 4.

THEOREM 4. *Let G be a group which is abelian, infinite, and σ-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*

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

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 $1 \leqq c \leqq (n-1)/2$. 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 σ-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

1. J. Cherly, *Méthodes élémentaires dans l'arithmétique de* $\mathsf{F}_q[X]$, Thèse 3ème cycle, Bordeaux, 1976.
2. J. Cherly, *Addition theorems in* $\mathsf{F}_q[x]$, *J. reine angew. Math.* 293/294 (1977), 223–227.
3. J. Cherly and J.-M. Deshouillers, *Un théorème d'addition dans* $\mathsf{F}_q[x]$, J. Number Theory 34 (1990), 128–131.
4. J.-M. Deshouillers and E. Wirsing, *Untitled manuscript*, Undated.
5. Y. O. Hamidoune, *An application of connectivity theory in graphs to factorizations of elements in groups*, Europ. J. Comb. 2 (1981), 349–355.
6. X.-D. Jia and M. B. Nathanson, *Addition theorems for σ-finite groups*, In *Proc. Hans Rademacher Centenary Conference*, Contemp. Math., 1994.
7. J. H. B. Kemperman, *On complexes in a semigroup*, Indag. Math 18 (1956), 247–254.
8. J. H. B. Kemperman, *On small sumsets in an abelian group*, Acta Math. 103 (1960), 63–88.
9. M. Kneser, *Abschätzung der asymptotische Dichte von Summenmengen*, Math. Z. 58 (1953), 459–484.
10. M. Kneser, *Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen*, Math. Z. 61 (1955), 429–434.
11. M. Kneser, *Summenmengen in lokalkompakten abelschen Gruppen*, Math. Z. 66 (1956), 88–110.

12. M. B. Nathanson, *Additive Number Theory: 2. Inverse Problems and the Geometry of Sumsets*, Springer-Verlag, to appear.
13. J. E. Olson, *Sums of sets of group elements*, Acta Arith. 28 (1975), 147–156.
14. J. E. Olson, *On the sum of two sets in a group*, J. Number Theory 18 (1984), 110–120.
15. Ö. J. Rödseth, *Two remarks on linear forms in non-negative integers*, Math. Scand. 51 (1982), 193–198.
16. W. D. Wallis, A. P. Street, and J. S. Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices*, Lecture Notes in Math. 292 (1972).

UNIVERSITÉ P. ET M. CURIE
COMBINATOIRE, CASE 189
4 PLACE JUSSIEU
75005 PARIS
FRANCE
e-mail: yha@ccr.jussieu.fr

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF BERGEN
ALLEGT. 55
N-5007 BERGEN
NORWAY
e-mail: rodseth@mi.uib.no