HALF-FACTORIAL SUBSETS IN INFINITE ABELIAN GROUPS

ALFRED GEROLDINGER AND RÜDIGER GÖBEL

Communicated by Klaus Kaiser

Abstract. Let G be an abelian group. A subset S of G is said to be half-factorial, if the block monoid over S is a half-factorial monoid. We show that every Warfield group has a half-factorial subset which generates the group in the monoid theoretical sense. In particular, this implies that for every Warfield group G there exists a half-factorial Dedekind domain whose divisor class group is isomorphic to G. We also provide torsion-free abelian groups with prescribed endomorphism ring (for any ring with free additive group) which have half-factorial generating sets but surely are not Warfield groups. The corresponding question about the existence of non totally projective abelian p-groups with a half-factorial set of generators remains open.

1. Introduction

By a monoid we always mean a multiplicative, commutative semigroup with unit element satisfying the cancellation law. A monoid is said to be atomic, if every element may be written as a product of atoms (irreducible elements). The main examples we have in mind are the multiplicative monoids of noetherian domains. An atomic monoid is said to be half-factorial, if for every element \(a \in H\) the following holds: if \(a = u_1 \cdots u_k\) and \(a = v_1 \cdots v_l\) are two factorizations of \(a\) into irreducibles, then \(k = l\). Clearly, every factorial monoid is half-factorial.

Since the very beginning of the theory of non-unique factorization the property of half-factoriality has been in the centre of interest. In 1960 L. Carlitz proved that the ring of integers of an algebraic number field is half-factorial if and only if the ideal class group has at most two elements. Motivated by a question of W.

2000 Mathematics Subject Classification. 13F05; 20K99.

Key words and phrases. Abelian groups, factorization, half-factorial.

We would like to thank L. Fuchs for reading this paper and suggesting many improvements.
Narkiewicz, L. Skula and A. Zaks started the investigation of general half-factorial Dedekind domains (cf. [Sku76] and [Zak76]). Since that time half-factoriality has been studied in a great variety of atomic monoids and (not necessarily integrally closed) noetherian domains (cf. [HK83], [AP97], [ACS94b], [ACS95], [PL00], [KL00] and many others; for a recent survey cf. [CC00]).

Let $H$ be a Krull monoid (cf. [HK98], §23) with divisor class group $G$ and let $G_0 \subseteq G$ denote the set of classes containing prime divisors. Then $G_0$ generates $G$ (as a monoid) and the question whether or not $H$ is half-factorial depends only on $G_0$ (cf. [Ger88], Proposition 1). We say that $G_0$ is half-factorial, if the corresponding Krull monoid $H$ is half-factorial (cf. Definition 3.1). Conversely, for every abelian group $G$ and every generating subset $G_0 \subseteq G$ there exists a Krull monoid $H$ (even a Dedekind domain) whose divisor class group is isomorphic to $G$ such that $G_0$ corresponds to the set of classes containing prime divisors (These results go back to L. Claborn, A. Grams, L. Skula and F. Halter-Koch; see Theorem 1.4 in [Gra74], Theorem 2.4 in [Sku76], Satz 5 in [HK90] and Theorem 23.7 in [HK98]; for a survey cf. [CG97]). Thus studying half-factoriality in Krull monoids is exactly the same as studying pairs $(G, G_0)$ of abelian groups $G$ and generating subsets $G_0$.

Let $G$ be an abelian group and $G_0 \subseteq G$ a generating subset. If $G_0 = G$, then the result of L. Carlitz carries over immediately whence $G$ is half-factorial if and only if $|G| \leq 2$. The situation is completely different, if $G_0$ is a proper subset of $G$. It is easy to see that every finite abelian group has a half-factorial generating subset. Furthermore, half-factorial subsets play an important role in the investigation of various arithmetical properties in (not necessarily half-factorial) Krull monoids (cf. [Ger90], [GG98], [GG00]). However, up to now only little is known about their structure or about their maximal possible size.

Half-factorial subsets (and other arithmetical properties) in infinite abelian groups have been studied in [ACS94c] and [ACS94a]. The question, whether every infinite abelian group has a half-factorial generating set, was first tackled by D. Michel and J.L. Steffan (see [MS86]) and is still open. The existence of half-factorial generating sets $G_0$ is in sharp contrast to a result of F. Kainrath, who showed that, if $G_0 = G$ is an infinite abelian group, then every finite set $L \subseteq \mathbb{N}_{\geq 2}$ appears as a set of lengths (see [Kai99]). We continue the investigation of half-factorial subsets in infinite abelian groups. As a main result we show that every Warfield group has a half-factorial generating set (Theorem 5.1). In particular, all countable abelian groups have a half-factorial generating set. Moreover, we will provide examples of groups with half-factorial generating sets which are not Warfield groups (cf. the Remark after Corollary 5.4).
2. Preliminaries

Our terminology in factorization theory is consistent with the one used in the survey articles in [And97] and concerning group theory we refer to the books of L. Fuchs and P. Loth ([Fuc70], [Fuc73] and [Lot98]). For convenience and to fix notations we briefly recall some central notions.

Let \( \mathbb{N} \) denote the positive integers, \( \mathbb{N}_0 = \mathbb{N} \cup \{0\} \), \( \mathbb{P} \subset \mathbb{N} \) the set of prime numbers and for \( a, b \in \mathbb{Z} \) we set \([a, b] = \{m \in \mathbb{Z} \mid a \leq m \leq b\}\).

Throughout, a monoid is a commutative, cancellative semigroup with unit element. Let \( H \) be a (multiplicatively written) monoid with unit element \( 1 \in H \).

We denote by \( H^\times \) the invertible elements of \( H \) and say that \( H \) is reduced, if \( H^\times = \{1\} \). Let \( \mathcal{A}(H) \) denote the atoms (irreducible elements) of \( H \), and \( H \) is said to be atomic, if every \( a \in H \setminus H^\times \) allows a factorization

\[
a = u_1 \cdots u_k
\]

with atoms \( u_1, \ldots, u_k \in \mathcal{A}(H) \). In this case \( k \) is called the length of the factorization and

\[
L_H(a) = L(a) = \{k \in \mathbb{N} \mid a \text{ has a factorization of length } k\} \subseteq \mathbb{N}
\]
denotes the set of lengths of \( a \). For convenience we set \( L(a) = \{0\} \) for all \( a \in H^\times \).

An atomic monoid \( H \) is said to be

- factorial, if every irreducible element is prime (equivalently, every element has a factorization, which is unique up to associates and up to the order of factors),
- half-factorial, if \( |L(a)| = 1 \) for every \( a \in H \).

Clearly, every factorial monoid is half-factorial.

Let \( G \) be an abelian group and \( \emptyset \neq G_0 \subseteq G \) a subset. We set \( -G_0 = \{-g \mid g \in G_0\} \) and denote by

\[
\langle G_0 \rangle = \left\{ \sum_{e \in E} m_e g_e \mid m_e \in \mathbb{N}, \ g_e \in G_0, \ E \text{ a finite set} \right\} \subseteq G
\]

the submonoid generated by \( G_0 \), and we say that \( G_0 \) is a generating set of \( G \), if \( [G_0] = G \). As usual let \( \langle G_0 \rangle \) denote the subgroup generated by \( G_0 \). Obviously, if \( G \) is a torsion group, then \( \langle G_0 \rangle = \langle G_0 \rangle \).

\( G_0 \) is called independent, if \( 0 \notin G_0 \) and given distinct elements \( g_1, \ldots, g_l \in G_0 \) and integers \( m_1, \ldots, m_l \in \mathbb{Z} \), then \( \sum_{i=1}^{l} m_i g_i = 0 \) implies that \( m_1 g_1 = \cdots = m_l g_l = 0 \). Clearly, \( G_0 \) is independent if and only if every finite subset of \( G_0 \) is
independent. Any equation of the form
\[ m_1 g_1 + \cdots + m_l g_l = 0 \]
where \( g_1, \ldots, g_l \in G \) and \( m_1, \ldots, m_l \in \mathbb{N} \) is called a \textit{minimal relation}, if \( \sum_{i=1}^{l} n_i g_i \neq 0 \) for all \( 0 \leq n_i \leq m_i \) with \( 0 < \sum_{i=1}^{l} n_i < \sum_{i=1}^{l} m_i \).

We denote by \( \mathcal{F}(G_0) \) the free abelian monoid with basis \( G_0 \). The elements \( S \in \mathcal{F}(G_0) \) have a unique representation of the form
\[ S = \prod_{g \in G_0} g^{v_g(S)} \]
with \( v_g(S) \in \mathbb{N}_0 \) and \( v_g(S) = 0 \) for all but finitely many \( g \in G_0 \).

Let \( S = \prod_{g \in G_0} g^{v_g(S)} = \prod_{i=1}^{l} g_i \in \mathcal{F}(G_0) \). We denote by
\[ |S| = \sum_{g \in G_0} v_g(S) = l \in \mathbb{N}_0 \]
the \textit{length} of \( S \),
\[ \text{supp}(S) = \{ g \in G_0 \mid v_g(S) > 0 \} = \{ g_i \mid i \in [1, l] \} \subseteq G_0 \]
the \textit{support} of \( S \),
\[ k(S) = \sum_{g \in G_0} \frac{v_g(S)}{\text{ord}(g)} = \sum_{i=1}^{l} \frac{1}{\text{ord}(g_i)} \in \mathbb{Q} \]
the \textit{cross number} of \( S \)
and by
\[ \sigma(S) = \sum_{g \in G_0} v_g(S) g = \sum_{i=1}^{l} g_i \in G \]
the \textit{sum} of \( S \).

Clearly, the sum gives rise to a monoid homomorphism \( \sigma : \mathcal{F}(G_0) \to G \) and
\[ B(G_0) = \ker(\sigma) \]
is the \textit{block monoid} over \( G_0 \). The block monoid is a reduced atomic monoid with unit element \( 1 = \prod_{g \in G_0} g^0 \) and we set \( A(G_0) = A(B(G_0)) \). An element \( S = \prod_{i=1}^{l} g_i^{m_i} \in \mathcal{F}(G_0) \) if and only if \( \sigma(S) = \sum_{i=1}^{l} m_i g_i = 0 \) and this is a minimal relation in \( G \). The relevance of block monoids stems from its relationship to Krull monoids: Let \( H \) be a Krull monoid with divisor class group \( G \) and let \( G_0 \) denote the set of classes containing prime divisors. Then \( H \) is a half-factorial monoid if and only if \( B(G_0) \) is half-factorial (cf. [Ger88], Proposition 1 or [CG97]).

3. \textbf{Half-factorial subsets}

\textbf{Definition 3.1.} A non-empty subset \( G_0 \) of an abelian group \( G \) is said to be \textit{factorial} (resp. \textit{half-factorial}), if the block monoid \( B(G_0) \) is factorial (resp. half-factorial).

We start with some simple observations.

\textbf{Lemma 3.2.} Let \( G \) be an abelian group.

(1) For every \( g \in G \) the set \( \{ g \} \) is factorial.

(2) For a non-empty subset \( G_0 \subseteq G \) the following are equivalent:
(a) $G_0$ is a factorial (resp. half-factorial) subset of $G$.
(b) $G_0 \cup \{0\}$ is factorial (resp. half-factorial) in $G$.
(c) Every finite subset of $G_0$ is factorial (resp. half-factorial) in $G$.

(3) There exists a maximal (with respect to set-theoretical inclusion) half-factorial subset.

**Proof.** 1. If $g$ has infinite order, then $B(\{g\}) = \{1\}$ is the trivial monoid. If $g$ has order $n \in \mathbb{N}$, then $A(\{g\}) = \{g^n\}$, whence $B(\{g\})$ is a reduced monoid having exactly one prime element.

2. The sequence $0 \in F(G)$ is a prime element in $B(G)$ whence $B(G_0 \cup \{0\}) = B(\{0\}) \times B(G_0 \setminus \{0\})$ whence a) and b) are equivalent. $G_0$ is half-factorial if and only if $|L(B)| = 1$ for every $B \in B(G_0)$ which holds if and only if $B(\text{supp}(B))$ is half-factorial for every $B \in B(G_0)$. An analogue statement holds for factorial subsets whence a) and c) are equivalent.

3. Let $\Omega = \{G_0 \subseteq G \mid G_0$ is half-factorial$\}$. Then 1. shows that $\Omega \neq \emptyset$. If $(G_i)_{i \in I}$ is a chain in $\Omega$, then $\bigcup_{i \in I} G_i \in \Omega$ by 2. Thus $\Omega$ has a maximal element by Zorn’s Lemma. □

Maximal half-factorial subsets $G_0$ do not necessarily generate the group $G$ (see the Remark at the end of section 4). For the special case of torsion groups the following result was first proved in [GG98].

**Proposition 3.3.** Let $G$ be an abelian group and $G_0 \subseteq G$ a half-factorial subset. Let $g_0 \in G_0$ and $g \in G \setminus \langle G_0 \rangle$ such that $pg = g_0$ for some $p \in \mathbb{P}$. Then $G_0 \cup \{g\}$ is half-factorial.

**Proof.** Let $B \in B(G_0 \cup \{g\})$ be given. We proceed in two steps.

First we show that $v_g(B)$ is a multiple of $p$. Suppose for contradiction that $B = g^k \cdot \prod_{i=1}^s g_i^{k_i}$ where $g_1, \ldots, g_s \in G_0$, $k \in \mathbb{Z} \setminus \{0\}$ and $p, k$ relatively prime. So there are $x, m \in \mathbb{Z}$ such that $1 = mp + kx$, hence $g = mpg + kxg$. From $\sigma(B) = 0$ it follows $kg + \sum_{i=1}^s k_i g_i = 0$, thus $kxg + \sum_{i=1}^s x k_i g_i = 0$. This implies that

$$g = mpg + kxg = mg_0 - \sum_{i=1}^s x k_i g_i \in \langle G_0 \rangle,$$

a contradiction.

In the second step we verify that $|L(B)| = 1$. To do so we proceed by induction on $v_g(B)$. If $v_g(B) = 0$, then $B \in B(G_0)$ and the assertion follows. If $v_g(B) > 0$, then $B' = (pg) \cdot g^{-p} \cdot B \in B(G_0)$ (by the first step) and by induction hypothesis we have $|L(B')| = 1$. For every factorization $U_1 \cdot \ldots \cdot U_k$ of $B$, say $v_g(U_1) \geq p$, there is some factorization $U'_1 \cdot U_2 \cdot \ldots \cdot U_k$ of $B'$ with the same length, where
\[ U'_1 = (pg) \cdot g^{-p} \cdot U_1. \] Thus we infer that that \( L(B) \subseteq L(B') \) whence the assertion follows. \qed

For torsion groups there is a simple but useful characterization of half-factorial subsets going back to L. Skula and J. Sliwa. For convenience we recall its short proof.

**Lemma 3.4.** Let \( G \) be a torsion group and \( G_0 \subseteq G \) a subset. Then the following statements are equivalent:

1. \( G_0 \) is half-factorial.
2. \( k(S) = 1 \) for every \( S \in \mathcal{A}(G_0) \).
3. For every minimal relation \( m_1 g_1 + \cdots + m_l g_l = 0 \) with \( g_1, \ldots, g_l \in G_0 \) and \( m_1, \ldots, m_l \in \mathbb{N} \) we have \( \sum_{i=1}^l \frac{m_i}{\text{ord}(g_i)} = 1 \).

**Proof.** 2. and 3. are equivalent by definition whence it remains to show the equivalence of 1. and 2.

If \( k(S) = 1 \) for all \( S \in \mathcal{A}(G_0) \) and \( U_1 \cdot \cdots \cdot U_s = V_1 \cdot \cdots \cdot V_t \) where \( U_i, V_j \in \mathcal{A}(G_0) \), then
\[ s = k(U_1 \cdot \cdots \cdot U_s) = k(V_1 \cdot \cdots \cdot V_t) = t \]
whence \( B(G_0) \) is half-factorial.

Let \( S = \prod_{i=1}^l g_i \in \mathcal{A}(G_0) \) with \( k(S) \neq 1 \). For every \( i \in [1, l] \) we set \( U_i = g_i^{\text{ord}(g_i)} \in \mathcal{A}(G_0) \) and \( m_i = \frac{m}{\text{ord}(g_i)} \) where \( m = \text{lcm}\{\text{ord}(g_1), \ldots, \text{ord}(g_l)\} \). Then it follows that
\[ S^m = U_1^{m_1} \cdots U_l^{m_l} \]
and since \( k(S) = \sum_{i=1}^l \frac{m_i}{m} \neq 1 \), these are factorizations of two different lengths. \qed

**Lemma 3.5.** Let \( G \) be an abelian group.

1. Suppose that \( G = \oplus_{i \in I} G_i \) and for every \( i \in I \) let \( H_i \subseteq G_i \setminus \{0\} \). Then \( B(\bigcup_{i \in I} H_i) = \prod_{i \in I} B(H_i) \). In particular, \( \bigcup_{i \in I} H_i \) is factorial (resp. half-factorial) if and only if all \( H_i \) are factorial (resp. half-factorial).
2. Every independent subset is factorial in \( G \).

**Proof.** 1. Since for each two distinct \( i, j \in I \) we have \( \langle H_i \rangle \cap \langle H_j \rangle = \{0\} \), it follows that \( \mathcal{A}(\bigcup_{i \in I} H_i) = \bigcup_{i \in I} \mathcal{A}(H_i) \) and hence \( B(\bigcup_{i \in I} H_i) = \prod_{i \in I} B(H_i) \).

2. If \( X \subseteq G \) is independent, then \( \langle X \rangle = \oplus_{x \in X} \langle x \rangle \). Hence the assertion follows from 1. and from Lemma 3.2.1. \qed

**Proposition 3.6.** Let \( G = \oplus_{x \in X} \mathbb{Z}x \) be a free abelian group with basis \( X \) and let \( Y \subseteq [X] \).
(1) If \( Y = G \), then \( [Y \cup (-X)] = G \).

(2) \( Y \cup (-X) \) is factorial in \( G \).

**Proof.** 1. is obvious. To verify 2., note that every irreducible block \( B \in \mathcal{B}(Y \cup (-X)) \) has the form
\[
B = y \cdot \prod_{x \in E} (-x)^{m_x}
\]
for some \( y = \sum_{x \in E} m_x x \in Y \) where \( E \subseteq X \) is finite and all \( m_x \in \mathbb{N} \). Thus every \( B \in \mathcal{B}(Y \cup (-X)) \) has a unique factorization into irreducible blocks. \( \Box \)

Half-factorial subsets of \( \mathbb{Z} \) are studied in [ACS94a] and [ACS94c]. A special case of the following result goes back to D. Michel and J. Steffan (cf. [MS86], Proposition 7).

**Proposition 3.7.** Let \( G \) be an abelian group, \( X \subset G \) a maximal independent subset of elements of infinite order and \( \varphi : G \to G/\langle X \rangle = H \) the canonical epimorphism. Let \( H_0 = \{ h_i \mid i \in I \} \subseteq H \) be a subset and for every \( i \in I \) let \( g_i \in G \) such that \( \varphi(g_i) = h_i \) and \( n_i g_i \in [X] \) where \( n_i = \text{ord}_H(h_i) \in \mathbb{N} \). Then \( G_0 = \{ g_i, x, -x \mid i \in I, x \in X \} \) is a generating set of \( G \) if and only if \( H_0 \) is a generating set of \( H \) and we have

(1) \( \mathcal{B}(G_0) = \mathcal{B}(X \cup (-X)) \times \mathcal{B}(\{ g_i, -x \mid i \in I, x \in X \}) \).

(2) \[
f : \mathcal{B}(\{ g_i, -x \mid i \in I, x \in X \}) \to \mathcal{B}(H_0)\]
\[
\prod_{j \in J} g_j^{k_j} \cdot \prod_{x \in E_2} (-x)^{m_x} \mapsto \prod_{j \in J} h_j^{k_j}
\]
is an isomorphism. In particular, \( G_0 \) is (half-)factorial if and only if \( H_0 \) is (half-)factorial.

**Proof.** By construction, \( G_0 \) generates \( G \) if and only if \( H_0 \) generates \( H \). We proceed in several steps.

1. To study \( \mathcal{A}(G_0) \), let
\[
U = \prod_{j \in E} g_j^{k_j} \cdot \prod_{x \in E_1} x^{l_x} \cdot \prod_{x \in E_2} (-x)^{m_x} \in \mathcal{A}(G_0)
\]
be given with finite subsets \( E \subseteq I \), \( E_1, E_2 \subseteq X \) and positive integers \( k_j, l_x, m_x \). Then
\[
(*) \quad \sum_{j \in E} k_j g_j + \sum_{x \in E_1} l_x x = \sum_{x \in E_2} m_x x
\]
Case 1: \( E_1 \neq \emptyset \). Let \( y \in E_1 \). Multiplying (*) with \( n = \text{lcm}\{n_j \mid j \in E\} \) we obtain
\[
\sum_{j \in E} k_j (n g_j) + \sum_{x \in E_1} (l_x n) x = \sum_{x \in E_2} (m_x n) x.
\]
Since all summands on both sides of the equation are in \([X]\), it follows that \( m_g > 0 \) whence \( U = y \cdot (-y) \).

Case 2: \( E_1 = \emptyset \). We assert that
\[
V = \prod_{j \in E} \varphi(g_j)^{k_j} \in \mathcal{A}(H_0).
\]
Since \( |U| > 0 \) and \( |E_1| = 0 \), it follows that \( |E| > 0 \) and (*) implies that \( \sigma(V) = 0 \).

For every \( j \in E \) let \( k'_j \in [0, k_j] \) such that
\[
\sum_{j \in E} k'_j > 0 \quad \text{and} \quad \sum_{j \in E} k'_j \varphi(g_j) = 0 \in H.
\]

Hence there exist a finite subset \( E' \subseteq X \) and integers \( m'_x \in \mathbb{Z} \) such that
\[
(**) \quad \sum_{j \in E} k'_j g_j = \sum_{x \in E'} m'_x x
\]
and for \( n = \text{lcm}\{n_j \mid j \in E\} \) we obtain
\[
\sum_{x \in E'} (n m'_x) x = \sum_{j \in E} k'_j (n g_j) \in [X]
\]
\[
\sum_{x \in E_2} (n m_x) x = \sum_{j \in E} k_j (n g_j) \in [X].
\]
These equations imply that \( E' \subseteq E_2 \) and \( m'_x \in [0, m_x] \) for every \( x \in E' \). Since \( U \) is irreducible, (**) implies that \( k'_j = k_j \) for every \( j \in E \) whence \( V \) is irreducible.

2. Let \( B \in \mathcal{B}(G_0) \) be given. We have to show that \( B \) can be written uniquely in the form \( B = U \cdot V \) where \( U \in \mathcal{B}(X \cup (-X)) \) and \( V \in \mathcal{B}(\{g_i, -x \mid i \in I, x \in X\}) \).

Consider a factorization
\[
B = U_1 \cdots U_\rho \cdot V_1 \cdots V_\psi
\]
where \( U_i, V_j \in \mathcal{A}(G_0), \sum_{x \in X} v_x(U_i) > 0 \) for every \( i \in [1, \rho] \) and \( V_j = S_j T_j \) where \( 1 \neq S_j \in \mathcal{F}(\{g_i \mid i \in I\}) \) and \( T_j \in \mathcal{F}(\{-x \mid x \in X\}) \). The above considerations imply that \( |U_i| = 2 \) for every \( i \in [1, \rho] \) whence
\[
U = U_1 \cdots U_\rho = \prod_{x \in X} (-x \cdot x)^{v_x(B)}
\]
is uniquely determined. Thus \( V = U^{-1} \cdot B \) is uniquely determined and \( V = V_1 \cdots V_\psi \in \mathcal{B}(\{g_i, -x \mid i \in I, x \in X\}) \).
3. Obviously, \( f \) is a homomorphism. To show that \( f \) is bijective, let \( C = \prod_{j \in E} h_j^{k_j} \in \mathcal{B}(H_0) \) be given. We verify that there is exactly one \( B \in \mathcal{B}(\{g_i, -x \mid i \in I, x \in X\}) \) with \( f(B) = C \). Since
\[
\varphi(\sum_{j \in E} k_j g_j) = \sum_{j \in E} k_j h_j = \sigma(C) = 0,
\]
it follows that \( \sum_{j \in E} k_j g_j \in (X) \). If \( n = \text{lcm}\{n_j \mid j \in E\} \), then
\[
n \sum_{j \in E} k_j g_j = \sum_{j \in E} k_j \frac{n_j}{n}(n_j g_j) \in [X]
\]
whence \( \sum_{j \in E} k_j g_j \in [X] \). Thus there exist a uniquely determined finite subset \( F \subseteq X \) and uniquely determined positive integers \( (m_x)_{x \in F} \) such that
\[
\sum_{j \in E} k_j g_j = \sum_{x \in F} m_x x
\]
whence
\[
B = \prod_{j \in E} g_j^{k_j} \cdot \prod_{x \in F} (-x)^{m_x}
\]
is the unique block with \( f(B) = C \). \( \square \)

4. **Simple subsets in modules over discrete valuation domains**

Throughout this section, let \( R \) be a discrete valuation domain over \( \mathbb{Z} \), with prime element \( \pi \) such that \( \pi R \cap \mathbb{Z} = p\mathbb{Z} \) for some prime \( p \in \mathbb{P} \) and residue class field \( k = R/\pi R \). Let \( v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\} \) the \( p \)-adic valuation. Then \( R \cap \mathbb{Q} = \mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid v_p(x) \geq 0\} \) denotes the corresponding valuation ring, \( p \) is a prime element and the residue class field is isomorphic to \( \mathbb{F}_p \).

A group \( G \) is called \( p \)-local, if for all \( q \in \mathbb{P} \setminus \{p\} \) multiplication with \( q \) is a group automorphism. Any \( p \)-local group can be given the structure of a \( \mathbb{Z}_{(p)} \)-module in a unique way and the \( \mathbb{Z}_{(p)} \)-submodules are the \( p \)-local subgroups. Conversely, note that \( \mathbb{Z}_{(p)} / \mathbb{Z} \) is a torsion divisible group with no \( p \)-torsion, whence, if \( G \) has a \( \mathbb{Z}_{(p)} \)-module structure, then all of its torsion is \( p \)-torsion. If \( G \) and \( H \) are \( p \)-local, then
\[
\]
Clearly, every \( R \)-module is a \( \mathbb{Z}_{(p)} \)-module and the main cases of interest are \( R = \mathbb{Z}_{(p)} \) or \( R \) the \( p \)-adic integers (for details cf. [War77] §2).

Let \( M \) be an \( R \)-module. For two elements \( g, h \in M \) we set
\[
g \leq h \quad \text{if} \quad \pi^k h = g \quad \text{for some} \quad k \in \mathbb{N}_0.
\]
This defines a natural partial order on \( M \) (for the antisymmetry, note that if \( \pi^k h = g \) and \( \pi^l g = h \) with \( k, l \in \mathbb{N} \), then \( (1 - \pi^{k+l})g = 0 \) whence \( g = h = 0 \).
because \(1 - \pi^{k+l} \in R^\times\). For a subset \(Y \subseteq G\) we denote by
\[
Y_g = \{ y \in Y \mid g \leq y \}
\]
the tree over \(g\) in \(Y\) and by
\[
\overline{Y} = \{ z \in M \mid \text{there is some } y \in Y \text{ with } z \leq y \}
\]
the \(\pi\)-closure of \(Y\). We say that \(Y\) is \(\pi\)-closed if \(\overline{Y} = Y\).

**Definition 4.1.** Let \(M\) be an \(R\)-module. We say that a subset \(Y \subseteq M\) is \(R\)-simple, if \(Y\) is \(\pi\)-closed and for every finite non-empty subset \(E \subseteq Y \setminus \{0\}\) and every maximal element \(e_0 \in E\) there exists some homomorphism \(\varphi : R(E) \rightarrow k\) such that \(\varphi(e_0) \neq 0\) and \(\varphi(e) = 0\) for all \(e \in E \setminus \{e_0\}\).

**Proposition 4.2.** Let \(M\) be a \(\mathbb{Z}_{(p)}\)-module for some prime \(p \in \mathbb{P}\) and \(G_0 \subseteq M\) a \(\mathbb{Z}_{(p)}\)-simple subset.

1. For every \(B \in \mathcal{B}(G_0)\) and every maximal element \(g \in \text{supp}(B)\) the multiplicity \(v_g(B)\) is a multiple of \(p\).
2. The support of every irreducible block in \(G_0\) lies in a tree and \(G_0\) is half-factorial.

**Proof.** 1. Suppose \(B = \prod_{i=1}^l g_i^{m_i} \in \mathcal{B}(G_0), E = \text{supp}(B) = \{g_1, \ldots, g_l\}\) and \(g_i\) is a maximal element in \(E\). Then there is some homomorphism \(\varphi : R(E) \rightarrow \mathbb{F}_p\) such that \(\text{ord}(\varphi(g_i)) = p\) and \(\varphi(g_i) = 0\) for every \(2 \leq i \leq l\). Since \(0 = \sigma(B) = \sum_{i=1}^l m_i g_i\), it follows that \(0 = \varphi(\sigma(B)) = m_1 \varphi(g_1)\) whence \(\text{ord}(\varphi(g_1)) = p\) divides \(m_1\).

2. We have to show that \(\text{supp}(B)\) lies in a tree for every \(B \in \mathcal{A}(G_0)\) and that \(|L(B)| = 1\) for every \(B \in \mathcal{B}(G_0)\). For both assertions we proceed by induction on \(|B|\).

If \(|B| = 1\), then \(B = 0\) whence \(B\) is prime and \(L(B) = \{1\}\). If \(1 < |B| \leq p\), then \(1\) implies that \(B = g^p\) for some \(g \in G_0\) whence \(L(B) = \{1\}\). In all these cases \(B\) is irreducible and its support lies in a tree.

Let \(B = \prod_{i=1}^l g_i^{m_i} \in \mathcal{B}(G_0)\) with \(|B| > p\). If \(l = 1\), then \(\text{ord}(g) < \infty, m_1\) is a multiple of \(\text{ord}(g_1)\) and \(L(B) = \{ \frac{m_1}{\text{ord}(g_1)} \}\). Suppose that \(l > 1\). After a suitable renumbering we may suppose that \(g_1\) is a maximal element of \(\text{supp}(B)\) whence \(p \mid m_1\). Since \(G_0\) is \(p\)-closed it follows that \(g_0 = pg_1 \in G_0\). We consider the block \(B' = g_0 \cdot g_1^{m_1-p} \cdot \prod_{i=2}^l g_i^{m_i}\). Clearly \(|B'| < |B|\), whence by induction hypothesis both assertions hold for \(B'\).

If \(B\) is irreducible, then \(B'\) is irreducible and if \(\text{supp}(B')\) lies in a tree over some element \(g\), then \(\text{supp}(B)\) lies in the tree over \(g\).
Suppose that $B$ is not irreducible. We show that for every factorization $z$ of $B$ there exists some factorization $z'$ of $B'$ with $|z| = |z'|$ which implies the assertion. Let $z = U_1 \cdots U_k$ be a factorization of $B$. Without restriction we may suppose that $g_1 | U_1$. Then $g_1$ is maximal in $\text{supp}(U_1)$ whence 1. implies that $p | v_{g_1}(U_1)$. Thus $U_1' = g_0 \cdot g_1 \cdot \ldots \cdot U_k$ is a factorization of $B'$ with $k = |z'| = |z|$. 

Let $M$ be an $R$-module. Following R. Warfield ([War81], p. 329) we say that $M$ is \textit{simply presented}, if it has a presentation of the following form: let $F$ be a free $R$-module with basis $X$, $L \subseteq F$ a subset and $\Phi : F \to M$ a surjective homomorphism with $\ker(\Phi) = _R(L)$ such that $Y = \Phi(X)$ satisfies the following properties:

- $\Pi(Y) = M$
- $0 \notin Y$
- if $y \in Y$ and $\pi y \neq 0$, then $\pi y \in Y$
- for every $y \in Y$ we have $y \notin \Pi\{z \in Y \mid \pi^nz \neq y \text{ for all } n \in \mathbb{N}_0\}$.

Every subset $Y \subseteq G$ satisfying the above properties is called a \textit{T-basis} of $M$. In [Hal77] simple presentations are exactly those representations having "relational complexity" two and it is proved that every group has a presentation with relational complexity at most three.

\textbf{Theorem 4.3.} Let $M$ be a simply presented $R$-module and $Y \subseteq M$ a T-basis. Then $Y$ is $R$-simple and hence half-factorial.

\textbf{Proof.} The set $Y$ is $\pi$-closed by definition. Let $E \subseteq Y$ be finite and $y \in E$ maximal. Let $Z = \{z \in Y \mid \pi^n z \neq y \text{ for all } n \in \mathbb{N}_0\}$ whence $E \setminus \{y\} \subseteq Z$. By the proof of Lemma 2.1 in [War81] there exists an $R$-module homomorphism $\sigma : M \to k$ with $\sigma(y) \neq 0$ and $\sigma(Z) = \{0\}$. Thus $Y$ is $R$-simple (and hence $Z_{(y)}$-simple) in the sense of Definition 4.1, since $\sigma \mid _{\pi(E)}$ has the required property. Proposition 4.2 implies that $Y$ is half-factorial. \qed

\textbf{Remark.} 1. For every $n \in \mathbb{N}$ the set $Y = \{p^i + p^n \mathbb{Z} \mid i \in [1, n - 1]\}$ is a T-basis of $\mathbb{Z}/p^n \mathbb{Z}$. The set $Y = \\{1/p^i + \mathbb{Z} \mid i \in \mathbb{N}\}$ is a T-basis of $\mathbb{Z}(p^\infty) = \{a/p^i + \mathbb{Z} \mid a \in \mathbb{Z}, i \in \mathbb{N}\} \subseteq \mathbb{Q}/\mathbb{Z}$. T-bases of generalized Prüfer groups are given in [Fuc73], §83, Example 3.

2. Let $G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} = \langle e_1 \rangle \oplus \langle e_2 \rangle$ with $\text{ord}(e_1) = 2$ and $\text{ord}(e_2) = 4$. Then $G_0 = \{0, e_1, e_1 + 2e_2\}$ is a 2-closed, $\mathbb{Z}(2)$-simple subset of $G$ and it is a maximal half-factorial subset. However, $G_0$ does not generate $G$. 

HALF-FACTORIAL SUBSETS 851
3. Let $G = \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} = \langle e_1 \rangle \oplus \langle e_2 \rangle$ with $\text{ord}(e_1) = \text{ord}(e_2) = n$ for some $n \in \mathbb{N}$ with $n \geq 3$. Then $G_0 = \{ie_1 + e_2 \mid i \in [1, n]\}$ is a half-factorial subset which is not simple (cf. also Theorem 6.3 and Corollary 6.5 in [GG98]).

4. There is also a definition of simple presentations in the global case (cf. [Lot98], Definition 1.19). However, if $g \in G$ with $\text{ord}(g) = p^km$ for some prime $p$, positive integers $k, m$ with $p \nmid m$ and $m \geq 3$, then the $p$-closed set $G_0 = \{p^ng \mid i \in \mathbb{N}_0\}$ is not half-factorial.

To verify this, we set $h = p^kg$. Then $\text{ord}(h) = m$ and multiplication with $p$ is an automorphism on $\langle h \rangle$. Thus $\langle h \rangle \subseteq G_0$, $U = (-h) \cdot h$ is an irreducible block in $G_0$ with $k(U) = \frac{2}{m} \neq 1$ whence $G_0$ is not half-factorial by Lemma 3.4.

5. **Abelian groups having half-factorial generating sets**

We recall some basic facts on Warfield groups. All of them may be found in the book of P. Loth [Lot98].

An abelian group $G$ is called a **Warfield group**, if there exists a subset $X \subseteq G$ such that the following conditions are satisfied:

1. $X \subseteq G$ is a maximal independent subset of elements of infinite order.
2. $G/\langle X \rangle$ is a torsion group whose $p$-subgroups are simply presented as $\mathbb{Z}(p)$-modules.
3. $\langle X \rangle$ is a nice valuated coproduct in $G$.

Indeed, in Theorem 3.83 in [Lot98] there are given 10 equivalent characterization for Warfield groups and the above definition coincides with condition 3 (cf. also Definition 3.25). The class of Warfield groups is closed under arbitrary direct sums and summands. Every Warfield group is balanced projective. A torsion-free group is balanced projective if and only if it is completely decomposable (i.e., a direct sum of groups of rank one). A torsion $p$-group is balanced projective if and only if it is a direct sum of a divisible $p$-group (which is a direct sum of groups isomorphic to $\mathbb{Z}(p^\infty)$) and of a totally projective $p$-group (these are defined in [Fuc73] and include generalized Prüfer groups and countable reduced $p$-groups) (cf. [War76]).

**Theorem 5.1.** Every Warfield group has a half-factorial generating set.

**Proof.** Let $G$ be a Warfield group, $X \subseteq G$ as in the above definition and $G/\langle X \rangle = H = \oplus_{p \in \mathbb{P}} H_p$. Let $p \in \mathbb{P}$, $R = \mathbb{Z}(p)$ and consider $H_p$ as an $R$-module. If $Y \subseteq H_p$ is a $T$-basis of $H_p$, then $Y$ is half-factorial by Theorem 4.3, and since $R(Y) = \langle Y \rangle = [Y]$, it follows that $Y$ is a half-factorial generating set of $H_p$. By Lemma 3.5 $H$ has a half-factorial generating set whence by Proposition 3.7.2 $G$ has a half-factorial generating set. □
Corollary 5.2. Let $G$ be an abelian group and $X \subseteq G$ a maximal independent subset of elements of infinite order such that $G/\langle X \rangle$ is a Warfield group. Then $G$ has a half-factorial generating set.

Proof. Let $X \subseteq G$ be a maximal independent subset of elements of infinite order, $F$ the free abelian group with basis $X$ and $\varphi : G \to H = G/F$ the canonical epimorphism. Since $H$ is a Warfield group, it has a half-factorial generating subset by Theorem 5.1. Since $X$ is maximal, $H$ is a torsion group whence $G$ has a half-factorial generating set by Proposition 3.7. □

Theorem 5.3. Let $G$ be an abelian group and $F \subseteq G$ a free abelian subgroup such that $G/F$ is either countable or divisible. Then $G$ has a half-factorial generating set.

Proof. Let $X$ denote a basis of $F$. By Zorn’s Lemma we extend $X$ to a maximal independent subset $X'$ of elements (of infinite order). If $G/\langle X' \rangle$ is countable, then $G/\langle X' \rangle$ is a countable group whence a Warfield group and the assertion follows from Corollary 5.2. If $G/\langle X' \rangle$ is divisible, then $G/\langle X' \rangle$ is divisible (as an epimorphic image of a divisible group) whence it is Warfield group and the assertion follows from Proposition 3.7 as well as from Corollary 5.2. □

We want to apply Theorem 5.3 to topological groups and to do so we repeat some basic facts (for details we refer to [CG85], [GM89], [FS01], Chapter 8 and [Mat97], §8). Let $R$ be a commutative ring with identity and characteristic zero, $S \subseteq R \setminus \{0\}$ a multiplicative subsemigroup consisting of non-zero divisors, $1 \in S$ and $M$ an $R$-module. Then $M$ is called $S$-divisible if $sM = M$ for every $s \in S$ and a submodule $N \subseteq M$ is called $S$-pure if $sM \cap N = sN$ for every $s \in S$. The $S$-topology on $M$ is defined by taking $\{x + sM \mid s \in S\}$ as a basis of neighbourhoods for every $x \in M$. Then addition in $M$ and (equipping $R$ with the discrete topology) scalar multiplication are continuous whence $M$ is a topological $R$-module. If $R$ is noetherian and $\{0\} \neq I \triangleleft R$ an ideal, then the $I$-adic topology (where $(I^nM)_{n \geq 0}$ is a basis of neighbourhoods of $0$) coincides with the $S$-topology where $S = (I \setminus \{0\}) \cup \{1\}$ (We provide the short argument: i) let $s \in S$ be given; then $sR \subseteq I \subseteq \sqrt{I}$ whence there is some $n \in \mathbb{N}$ with $I^n \subseteq sR$ whence $I^nM \subseteq sM$. ii) let $n \in \mathbb{N}$ be given; if $s \in I$ then $s^nR \subseteq I^n$ whence $s^nM \subseteq I^nM$).

Let $T \subseteq R$ such that for every $t \in T$ multiplication with $t$ is an automorphism on $M$. If $S_T$ denotes the multiplicative subsemigroup generated by $S$ and $T$, then the $S$-topology coincides with the $S_T$-topology and $M$ is $S$-divisible if and only if $M$ is $S_T$-divisible. In particular, if $M$ is a $\mathbb{Z}_(p)$-module, then the $p$-adic topology
The $S$-topology coincides with the $\mathbb{Z}$-adic topology (i.e., the $S$-topology with $S = \{p^k \mid k \in \mathbb{N}\}$) if and only if $\bigcap_{s \in S} sM = \{0\}$. Note that, if $M$ is a free $\mathbb{Z}$-module, then the $S$-topology is Hausdorff. From now on we suppose that the $S$-topology is Hausdorff and that $S$ is countable.

Let $\hat{M}$ denote the completion of $M$ in the $S$-topology. Then the completion topology on $\hat{M}$ coincides with the $S$-topology on $\hat{M}$ and $M$ is dense and $S$-pure in $\hat{M}$.

Let $N \subseteq M$ be a submodule. If $N \subseteq M$ is dense in the $S$-topology, then $M/N$ is $S$-divisible (here is the argument: let $x + N \in M/N$ and $s \in S$ be given; since $N$ is $S$-dense, there is some $y \in N$ with $x - y \in sM$, say $x - y = sz$ whence $s(z + N) = sz + N = x - y + N = x + N$). If $N \subseteq M$ is $S$-pure, then, by definition of purity, the $S$-topology on $N$ (having $(sN)_{s \in S}$ as a basis of neighbourhoods of 0) coincides with the induced $S$-topology of $M$ ( having $(sM \cap N)_{s \in S}$ as a basis of neighbourhoods of 0).

Let $G$ be any $R$-module between $M$ and $\hat{M}$ such that $G \subseteq \hat{M}$ is $S$-pure. Then $M$ is dense in $G$ in the $S$-topology whence $G/M$ is $S$-divisible.

**Corollary 5.4.** Let $R$ be a commutative ring with identity and characteristic zero, $S \subseteq (R \setminus \{0\}, \cdot)$ as above such that $nR \cap S \neq \emptyset$ for all $n \in \mathbb{N}$ and $G$ a Hausdorff $R$-module. If $G$ has a submodule $M$, which is a free abelian group and dense in the $S$-topology, then $G$ has a half-factorial generating set.

**Proof.** Let $M \subseteq G$ be a submodule having the above properties. Since $M \subseteq G$ is dense, the factor module $G/M$ is $S$-divisible. If $n \in \mathbb{N}$ and $a \in R$ such that $na = s \in S$, then

$$n(G/M) \subseteq G/M = s(G/M) = n(aG/M) \subseteq n(G/M)$$

whence $G/M$ is divisible as an abelian group. Thus the assertion follows from Theorem 5.3. \qed

Note that, if $R$ is an integral domain, $\{0\} \neq I \triangleleft R$ an ideal and $S = (I \setminus \{0\}) \cup \{1\}$, then

$$nR \cap S = nR \cap ((I \setminus \{0\}) \cup \{1\}) \supseteq (nR) \cdot (I \setminus \{0\}) \neq \emptyset$$

for every $n \in \mathbb{N}$. In the following remark we discuss some groups to which Corollary 5.4 applies. All of them are torsion-free.

**Remark.** 1. Consider $\mathbb{Z}$ together with the $\mathbb{Z}$-adic topology and let $\hat{\mathbb{Z}}$ denote its completion. Since $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$, it follows that $\hat{\mathbb{Z}}$ has a half-factorial generating set.
2. Let $R$ be a ring which is a free $\mathbb{Z}$-module, $I \triangleleft R$ an ideal and $G = \widehat{R}$ the $I$-adic completion. Then $G$ has a half-factorial generating set. We would like to point out two special situations.

If $A$ is a ring which is a free $\mathbb{Z}$-module, then $R = A[X_1, \ldots, X_n]$ is a free $\mathbb{Z}$-module and if $I = R(X_1, \ldots, X_n)$, then $\widehat{R} = A[[X_1, \ldots, X_n]]$ is the power series ring.

If $K$ is an algebraic number field with ring of integers $\mathfrak{o}$ and $\{0\} \neq \mathfrak{p}$ a prime ideal. Then $R = \mathfrak{o}$ is a free $\mathbb{Z}$-module and $\widehat{R}$ are the $\mathfrak{p}$-adic integers.

3. There are two standard construction principles for pathological abelian groups $G$, which satisfy the assumption of Corollary 5.4. They are based on A.L.S. Corner, M. Dugas, R. Göbel and S. Shelah.

Let $R$ be a ring which is a free $\mathbb{Z}$-module and $\lambda$ a cardinal number. Then there always exists a torsion-free abelian group $G$ and some multiplicatively closed subset $S \subseteq R \setminus \{0\}$ such that

- $M = \bigoplus_{\tau \in T} \tau R \subseteq G$ and $G \subseteq \widehat{M}$ is $S$-pure, whence $M$ is a free abelian group, dense in the $S$-topology and by Corollary 5.4 $G$ has a half-factorial generating set.
- $\text{End}(G) \cong R$.

provided that one of the following conditions holds:

1. $|R| < 2^{\aleph_0}$ and $2 \text{rk}(R) \leq \lambda \leq 2^{\aleph_0}$ see [Cor63] and [GM89].
2. $|R| \cdot 2^{\aleph_0} \leq \lambda = \lambda^{\aleph_0}$ see [CG85].
3. $|R| = \aleph_0$ and $\lambda = \aleph_1$ see [GS98].

In 2) and 3) $G$ may be assumed to be $\aleph_1$-free i.e., all its countable subgroups are free. Surely these examples are not Warfield groups, so we do have a large supply of torsion-free groups with half-factorial systems of generators besides all Warfield groups. However the question whether every abelian group has a half-factorial generating set remains open. In particular, we do not know whether this is true for the torsion-completion $\overline{B}$ of $B = \bigoplus_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z}$. We close with an observation stating that the case of general abelian groups might be reduced to the case of reduced uncountable, unbounded $p$-groups.

Remark. If every reduced unbounded uncountable $p$-group has a half-factorial generating set, then every abelian group has a half-factorial generating set.

Proof. First we show that all $p$-groups have a half-factorial generating set. Let $G$ be a $p$-group. Then $G = D \oplus C$ for some divisible group $D$ and some reduced group $C$. By Theorem 5.1 $D$ has a half-factorial generating set. If $C$ is bounded
or countable it is Warfield. If $C$ is unbounded and uncountable, it has a half-factorial generating set by assumption. Thus $G = D \oplus C$ has a half-factorial generating set by Lemma 3.5.

If $G$ is a torsion group, it is a direct sum of its $p$-components whence it has a half-factorial generating set by Lemma 3.5.

Let $G$ be an abelian group and $X \subseteq G$ a maximal independent subset of elements with infinite order. Then $F = \langle X \rangle$ is a free abelian group and $H = G/F$ a torsion group. Since $H$ has a half-factorial generating set, Proposition 3.7 implies that $G$ has a half-factorial generating set. \qed

References


HALF-FACTORIAL SUBSETS


Received August 1, 2001

(Alfred Geroldinger) INSTITUT FÜR MATHEMATIK, KARL-FRANZENS UNIVERSITÄT, HEINRICH-STRASSE 36, 8010 GRAZ, AUSTRIA

E-mail address: alfred.geroldinger@uni-graz.at
(Rüdiger Göbel) Universität Essen, Fachbereich 6, Mathematik und Informatik, 45117 Essen, Germany
E-mail address: r.goebel@uni-essen.de