Acta Math. Univ. Comenianae
Vol. LXI, 2(1992), pp. 193–208

ARITHMETICAL CHARACTERIZATIONS OF DIVISOR CLASS GROUPS II

A. GEROLDINGER

1. Introduction

Almost 20 years ago, W. Narkiewicz posed the problem to give an arithmetical characterization of the ideal class group of an algebraic number field ([**13,** problem 32]). In the meantime there are various answers to this question if the ideal class group has a special form. (cf. [**4**], [**5**], [**12**] and the literature cited there).

The general case was treated by J. Koczorowski [**11**], F. Halter-Koch [**8**], [**9,** §5] and D. E. Rush [**16**]. In principle they proceed in the following way: they consider a finite sequence $(a_i)_{i=1\dots r}$ of algebraic integers, requiring a condition of independence and a condition of maximality. Thereby the condition of independence guarantees that the ideal classes g_i of one respectively all prime ideals g_i appearing in the prime ideal decomposition of a_i are independent in a group theoretical sense. The invariants of the class group are extracted from arithmetical properties of the a_i's, and the condition of maximality ensures that one arrives at the full class group but not at a subgroup.

We study the problem in the general context of semigroups with divisor theory where every divisor class contains a prime divisor (cf. [**1**], [**17**]). Semigroups with divisor theory have turned out to be not only the appropriate setting for investigations on the arithmetic of rings of integers but to be of independent interest (cf. [**6**], [**9**], [**10**]). But contrary to the case of algebraic number fields, where the class group is always finite, every abelian group can be realized as a divisor class group of a semigroup with divisor theory ([**17,** Theorem 3.7] and [**9,** Satz 5]).

The condition, that every divisor class has to contain at least one prime divisor, means a quite natural restriction. It is just this condition, which ensures that the relationship between the arithmetic of the semigroup and the class group in close enough, to allow a reasonable answer to the present problem. However, there are Dedekind domains which do not satisfy this condition, as can be seen from L. Skula's paper [**18**].

We achieve the various descriptions of invariants of the class group by using only properties, which are satisfied by the semigroup if and only if they are satisfied by

Received May 18, 1992.
1980 *Mathematics Subject Classification* (1991 *Revision*). Primary 11R04.

the corresponding block semigroup. Therefore, when clearing up the relationship between arithmetical properties and properties of the class group, we may restrict to block semigroups, which are the central tool in this paper.

After some preliminaries in Section 3, where we discuss arithmetical properties of elements, we deal with the rank of a divisor class group. We introduce independent systems in the semigroup (Definition 7b) which correspond to independent systems in the class group (Corollary 1). The rank of the class group turns out to be the supremum of the cardinals of independent systems in the semigroup (Theorem 1). In addition, and this seems essential to us, the notion of independence is made in such a way that it satisfies the following universal property: every minimal independent system from which the rank of the class group can be extracted is an independent one (Proposition 1). In particular this implies that the sequences considered by Kaczorowski, Halter-Koch and Rush are independent in the present sense. In Section 5 we consider torsion class groups, develop an arithmetical analogue to pure subgroups (Definition 9b) and give an arithmetical characterization of the type of a basic subgroup of the class group (Theorem 2).

2. Preliminaries

Throughout this paper, let S be a semigroup with divisor theory $\partial\colon S \to \mathcal{F}(P)$ and divisor class group G; $\mathcal{F}(P)$ means the free abelian semigroup with basis P. Every divisor class should contain at least one prime divisor $\mathfrak{p} \in P$ and for the sake of simplicity we exclude the trivial cases $\operatorname{card}(G) \leq 2$, where S is half-factorial, and assume $\operatorname{card}(G) \geq 3$.

We write G additively, and for $\alpha \in \mathcal{F}(P)$ we denote by $[\alpha] \in G$ the divisor class containing α. For a subset $G_0 \subset G$ let $\langle G_0 \rangle$ be the subgroup generated by G_0. In S we have the usual notions of divisibility theory as developed in [**7**]. In particular $S^{\times}$ means the group of units, and for a system S_0 of elements of S we denote by $[S_0]$ the subsemigroup generated by the elements of S_0. We shall make use of the fact that an element $a \in S$ is prime if and only if $\partial a = \mathfrak{p}$ for some $\mathfrak{p} \in P$ ([**9**, Satz 10]). If for a non-unit $a \in S$, $a = u_1 \dots u_k$ is a factorization into irreducibles $u_1, \dots, u_k \in S$, then k is called length of the factorization and $L(a)$ denotes the set of lengths of possible factorizations of a.

Every element B of the free abelian semigroup $\mathcal{F}(G)$ with basis G is of the form

$$B = \prod_{g \in G} g^{v_g(B)}$$

where $v_g(B) \in \mathbb{N}$ and $v_g(B) = 0$ for all but finitely many $g \in G$. The subsemigroup

$$\mathcal{B}(G) = \{\, B \in \mathcal{F}(G) \mid \sum_{g \in G} v_g(B) g = 0 \in G \,\}$$

is called the block semigroup over G and the elements of $\mathcal{B}(G)$ are called blocks.

The embedding $\mathcal{B}(G) \hookrightarrow \mathcal{F}(G)$ is a divisor theory; G is the set of prime divisors; the divisor class group is isomorphic to G and every class contains exactly one prime divisor ([**9,** Beispiel 6]).

Let the block homomorphism $\beta\colon S \to \mathcal{B}(G)$ be defined by $\beta(a) = 1$, if $a \in S^\times$, and by

$$\beta(a) = [\mathfrak{p}_1] \dots [\mathfrak{p}_m]$$

if $\partial a = \mathfrak{p}_1 \dots \mathfrak{p}_m$. $\beta(a)$ is called the block of a, and we have the following fundamental correspondence between S and $\mathcal{B}(G)$:

1) a is irreducible, respectively a prime or a unit (in S) if and only if $\beta(a)$ is irreducible, respectively a prime or unit (in $\mathcal{B}(G)$).

2) If $a = u_1 \dots u_r$ is a factorization of a into irreducible elements of S, then $\beta(a) = \beta(u_1) \dots \beta(u_r)$ is a factorization of $\beta(a)$ into irreducible blocks, and every factorization in $\mathcal{B}(G)$ arises in this way; in particular $L(a) = L(\beta(a))$.

Finally we set, for $a \in S$ with $\beta(a) = \prod\limits_{i=1}^{k} g_i$,

$$\gamma(a) = \{\, g_i \mid 1 \le i \le k \,\} = \{\, g \in G \mid g|\beta(a) \,\} .$$

3. Arithmetical Properties of an Element

Our first aim is to describe arithmetically the number of prime divisors, counted with multiplicity, of ∂a for an element $a \in S$.

Definition 1. Let $a \in S$.
1) For $a \in S^\times$ let $\sigma(a) = 0$, and if a is irreducible, we set

$$\sigma(a) = \begin{cases} 1, & \text{if } a \text{ is prime.} \\ \max\{\max L(aa') \mid a' \in S \text{ irreducible}\}, & \text{otherwise.} \end{cases}$$

2) If $a = u_1 \dots u_k$ is any factorization of a into irreducibles, we set

$$\sigma(a) = \sum_{i=1}^{k} \sigma(u_i) .$$

By the following Lemma, this definition is independent of the particular factorization.

Lemma 1. *For every $a \in S$ we have*

$$\sigma(a) = \sigma(\beta(a)) = \sum_{\substack{\mathfrak{p} \in P \\ \mathfrak{p}^r \| \partial a}} r$$

Proof. Obviously it is sufficient to verify that for an irreducible block $0 \neq B = \prod_{i=1}^{k} g_i \in \mathcal{B}(G)$ we have $\sigma(B) = k$.

We set $B^* = \prod_{i=1}^{k}(-g_i)$; then B^* is irreducible and $k = \max L(BB^*) \leq \sigma(B)$. Since, on the other hand, for any irreducible block $\overline{B}$ we have $\max L(B\overline{B}) \leq k$, the assertion follows. $\square$

Definition 2. Let $a \in S \setminus S^\times$.

1) We say that a is of infinite type, if there exist an $M \in \mathbb{N}$ and, for every $n \in \mathbb{N}_+$, an $a_n \in S$ such that

$$a^n | a_n \quad \text{and} \quad \min L(a_n) \leq M .$$

2) We say that a is of finite type, if no irreducible $u \in S$ which divides some power of a is of infinite type.

Lemma 2. *Let* $a \in S \setminus S^\times$.

1) *The following conditions are equivalent:*

(i) a *is of infinite type.*

(ii) $\beta(a)$ *is of infinite type.*

(iii) $\mathrm{ord}\,(g) = \infty$ *for every* $g \in \gamma(a)$.

2) *The following conditions are equivalent:*

(i) a *is of finite type.*

(ii) $\beta(a)$ *is of finite type.*

(iii) $\mathrm{ord}\,(g) < \infty$ *for every* $g \in \gamma(a)$.

Proof. In both cases (i) and (ii) are obviously equivalent. Therefore we may restrict to block semigroups and it remains to proof the equivalence of (iii). Let $B = \prod_{i=1}^{k} g_i \in \mathcal{B}(G)$.

1) Suppose B is of infinite type and assume to the contrary, that $\mathrm{ord}\,(g_i) < \infty$ for some $i \in \{1, \ldots, k\}$. Let $n \in \mathbb{N}_+$; then for every B_n with $B^n | B_n$ $v_{g_i}(B_n) \geq v_{g_i}(B^n) \geq n$. If $B_n = C_1 \ldots C_s$ is any factorization of B_n into irreducible blocks C_j, then $v_{g_i}(C_j) \leq \mathrm{ord}\,(g_i)$, and this implies $s \geq \frac{n}{\mathrm{ord}\,(g_i)}$, a contradiction.

Conversely, assume $\mathrm{ord}\,(g_i) = \infty$ for $1 \leq i \leq k$ and let $n \in \mathbb{N}_+$. Then $B^n | \prod_{i=1}^{k} C_i$ with $C_i = (-ng_i)g_i^n$ and $\min L(\prod_{i=1}^{k} C_i) \leq k = \sigma(B)$.

2) Suppose B is of finite type and assume that property (iii) is violated. Then $M = \{g_i \,|\, 1 \leq i \leq k, \mathrm{ord}\,(g_i) < \infty\} \subsetneqq \{g_1, \ldots, g_k\}$. We set $m = \mathrm{lcm}\, M$ ($m = 1$ if $M = \emptyset$!) and obtain $B^m = (\prod_{g_i \notin M} g_i^m)(\prod_{g_i \in M} g_i^{\mathrm{ord}\,(g_i)})^{m/\mathrm{ord}\,(g_i)}$. Thus there is an irreducible block $B_m \in \mathcal{B}(G)$ dividing $\prod_{g_i \notin M} g_i^m$; B_m divides B^m and by 1) it is of infinite type, a contradiction.

Conversely, assume $\mathrm{ord}\,(g_i) < \infty$ for $1 \leq i \leq k$. Let $n \in \mathbb{N}_+$ and $C \in \mathcal{B}(G)$ an irreducible block with $C | B^n$. Thus $\mathrm{ord}\,(g) < \infty$ for every $g \in \gamma(C)$ and therefore by 1) C is not of infinite type; hence B is of finite type. $\square$

Definition 3. Two irreducible elements $\pi_1, \pi_2 \in S$ are called block equal, if $L(\pi_1 a) = L(\pi_2 a)$ for all $a \in S$.

Lemma 3. *For irreducible elements $\pi_1, \pi_2 \in S$ the following conditions are equivalent:*

1) *π_1 and π_2 are block equal.*
2) *$\beta(\pi_1)$ and $\beta(\pi_2)$ are block equal.*
3) *$\beta(\pi_1) = \beta(\pi_2)$.*

Proof. Obviously the only assertion to be proved is that two distinct irreducible blocks are not block equal. Let $B_1 = \prod_{i=1}^r g_i$ and $B_2 \in \mathcal{B}(G)$ be irreducible with $B_1 \neq B_2$, $\sigma(B_1) \geq \sigma(B_2)$ and if $\sigma(B_1) = \sigma(B_2)$, then

$$\max\{\operatorname{ord}(g) \mid g|B_1\} \geq \max\{\operatorname{ord}(g) \mid g|B_2\}\,.$$

We define a block $C \in \mathcal{B}(G)$, depending on the following cases:

$r \geq 3 \quad : \quad C = \prod_{i=1}^r (-g_i)$.

$r = 2$ and $\operatorname{ord}(g_1) \geq 3$: $C = B_1^{\operatorname{ord}(g_1)-1}$.

$r = 2$, $\operatorname{ord}(g_1) = 2$ and $B_2 = h^2$ for some $h \in G$: $C = (g_1 + h)^2 h^2$.

$r = 2$, $\operatorname{ord}(g_1) = 2$ and $B_2 = 0$: $C = (g_1 + h)(g_1 - h)h(-h)$ for an arbitrary $h \in G \setminus \{0, g_1\}$.

In each case it can be easily verified that $r \in L(B_1 C)$ but $r \notin L(B_2 C)$. □

Definition 4. Let $\pi \in S$ be an irreducible element of finite type. We say that π is homogenous if it is block equal with every irreducible $\pi' \in S$ dividing some power of π.

Lemma 4. *Let $\pi \in S$ be an irreducible element of finite type. Then the following conditions are equivalent:*

1) *π is homogenous.*
2) *$\beta(\pi)$ is homogenous.*
3) *$\beta(\pi) = g^{\operatorname{ord}(g)}$ for some $g \in G$.*

Proof. Obvious. □

Remark. π is homogenous, if and only if $\beta(\pi)$ is "absolut-unzerlegbar" in the sense of F. Halter-Koch ([**9,** Definition 8]).

Definition 5. Let $\pi \in S$ be an irreducible element of finite type with $\sigma(\pi) = n + 1$ for some $2 \leq n \in \mathbb{N}_+$. Then π is called n-simple, if it is either homogenous or if there exists a homogenous $\overline{\pi} \in S$ satisfying the following two conditions:

1) $\overline{\pi}$ divides some power of π and $\sigma(\overline{\pi}) = \min\{k \in \mathbb{N}_+ \mid \overline{\pi}|\pi^k\}$.

2) all homogenous elements, which divide some power of π and which are not associated with $\overline{\pi}$, are pairwise block equal.

If π is homogenous, we set $\overline{\pi} = \pi$.

Lemma 5. *For $2 \le n \in \mathbb{N}_+$ and an irreducible element $\pi \in S$ of finite type the following conditions are equivalent:*

1) *π is n-simple.*
2) *$\beta(\pi)$ is n-simple.*
3) *$\beta(\pi) = (-g)^n(ng)$ for some $g \in G$.*

In addition, if $\beta(\pi) = (-g)^n(ng)$ for some $g \in G$, then $\beta(\overline{\pi}) = \overline{\beta(\pi)} = (ng)^{\mathrm{ord}\,(ng)}$ and $\overline{\pi}$ is unique up to associates.

Proof. If π is homogenous then all three conditions are satisfied and the additional statement is true.

So suppose π to be not homogenous. Because $\beta(\beta(\pi)) = \beta(\pi)$ it is sufficient to prove the equivalence of 1) and 3).

1) $\implies$ 3) Let $\partial\pi = \mathfrak{p}_0 \dots \mathfrak{p}_n$ and $\beta(\pi) = g_0 \dots g_n$ with $\mathfrak{p}_i \in g_i$ for $0 \le i \le n$. Assume $\partial\overline{\pi} \ne \mathfrak{p}_i^{\mathrm{ord}\,(g_i)}$ for all $i \in \{0, \dots, n\}$; then by condition 2) in Def. 5 all g_i are equal and π would be homogenous, a contradiction. So without restriction let $\partial\overline{\pi} = \mathfrak{p}_0^{\mathrm{ord}\,(g_0)}$. By condition 1) in Def. 5 we infer that $\mathfrak{p}_0 \ne \mathfrak{p}_i$ for all $1 \le i \le n$. Therefore by condition 2) all $\pi_i \in S$ with $\partial\pi_i = \mathfrak{p}_i^{\mathrm{ord}\,(g_i)}$ are pairwise block equal. Thus $g_1 = \dots = g_n = -g$ for some $g \in G$ and $\beta(\pi)$ has the required form.

3) $\implies$ 1) Let $\beta(\pi) = (-g)^n(ng)$ and $\partial\pi = \mathfrak{p}_0 \dots \mathfrak{p}_n$ with $\mathfrak{p}_0 \in ng$ and $\mathfrak{p}_i \in -g$ for $1 \le i \le n$. Then every $\overline{\pi} \in S$ with $\partial\overline{\pi} = \mathfrak{p}_0^{\mathrm{ord}\,(ng)}$ satisfies condition 1) of Def. 5 and obviously condition 2) holds.

In addition, if $\beta(\pi) = (-g)^n(ng)$, then it follows from the proof of 3) $\implies$ 1) that $\beta(\overline{\pi}) = (ng)^{\mathrm{ord}\,(ng)}$; $\partial\overline{\pi}$ is unique and it can be seen directly that $\overline{\beta(\pi)} = (ng)^{\mathrm{ord}\,(ng)}$. □

Definition 6. Let $a \in S$ be of finite type and let $p \in \mathbb{N}$ be prime. We say that a is of type p, if $\sigma(u)$ is a power of p for every homogenous $u \in S$ which divides some power of a.

Lemma 6. *Let $a \in S$ be of finite type and let $p \in \mathbb{N}$ be prime. Then the following conditions are equivalent:*

1) *a is of type p.*
2) *$\beta(a)$ is of type p.*
3) *$\mathrm{ord}\,(g)$ is a power of p for every $g \in \gamma(a)$.*

Proof. It suffices to verify the equivalence of 3) for block semigroups. For this we take a block $B = \prod_{i=1}^k g_i \in \mathcal{B}(G)$.

Suppose B is of type p. Then for every $i \in \{1, \dots, k\} g_i^{\mathrm{ord}\,(g_i)}$ is homogenous and divides $B^{\mathrm{ord}\,(g_i)}$. Thus $\sigma(g_i^{\mathrm{ord}\,(g_i)}) = \mathrm{ord}\,(g_i)$ is a power of p.

Conversely, let $\operatorname{ord}(g_i)$ be a power of p for every $i \in \{1, \dots, k\}$ and consider a homogenous $C \in \mathcal{B}(G)$ dividing some power of B. Then $g_i | C$ for some $i \in \{1, \dots, k\}$ and thus $\sigma(C) = \operatorname{ord}(g_i)$ is a power of p. □

4. The Rank of a Divisor Class Group

The following definition recalls some group theoretical notions (cf. [**3,** §16]) on which the subsequent arithmetical notions are modelled.

Definition 7a. 1) An element $g \in G$ is said to be independent of a system G_0 of elements of G if there is no dependence relation

$$0 \neq ng = \sum_{i=1}^{k} n_i g_i$$

for some $g_i \in G_0$ and integers $n,\, n_i \in \mathbb{Z}$.

2) A system $G_0 = (g_i)_{i \in I}$ of elements of G is said to be independent if for every $\imath \in I g_\imath$ is independent of $(g_i)_{i \in I \setminus \{\imath\}}$.

3) The rank $r(G)$ of G is the cardinal number of a maximal independent system containing only elements of infinite and prime power orders.

Remarks. 1) An independent system does not contain equal elements, and hence it is a set.

2) A set $G_0 \subset G$ is independent if and only if $\langle G_0 \rangle = \oplus_{g \in G_0} \langle g \rangle$.

3) $r(G) = \sup\{\operatorname{card}(G_0) \mid G_0 \subset G \quad \text{is independent}\}$.

Next we define for every $a \in S$ a corresponding set $M(a)$:

(i) For $a \in S^\times$ we set $M(a) = S^\times$.

(ii) For an irreducible $a \in S$ we set

$$M(a) = \{a^* \in S \mid a \text{ and } a^* \text{ are block equal}\}$$

if $\sigma(a) \leq 2$, and

$$M(a) = \{a^* \in S \mid \sigma(a) = \sigma(a^*) = \max L(aa^*)\}$$

else.

(iii) In all other cases let

$$M(a) = \left\{ \prod_{i=1}^{r} u_i^* \mid u_i^* \in M(u_i) \text{ and } a = u_1 \dots u_r \text{ with irreducibles } u_i \right\}$$

If S is a block semigroup and $B = \prod_{i=1}^{k} g_i \in S = \mathcal{B}(G)$, then $M(B) = \{\prod_{i=1}^{k}(-g_i)\}$. In general we have $M(a) = \{a^* \in S \mid \beta(a^*) \in M(\beta(a))\}$ and $M(\beta(a)) = \beta(M(a))$; if $a^* \in M(a)$ and $aa^* = u_1 \dots u_{\max L(aa^*)}$, then either $\beta(u_i) = 0$ or $\beta(u_i) = g_i(-g_i)$ for some $g_i \in G$.

Definition 7b. 1) An element $a \in S$ is said to be independent of a system S_0 of elements of S, if there exists an irreducible $u_a \in S$ which is not prime such that the following conditions are fulfilled:

(i) $aa^* = u_a u_2 \dots u_{\max L(aa^*)}$ for some $a^* \in M(a)$ and irreducibles $u_2, \dots, u_{\max L(aa^*)}$.

(ii) $u_a \nmid bb^*$ for any $b \in S_0$ and $b^* \in M(b)$.

(iii) If $v \in S$ is irreducible and $v | u_a^i b$ with $i \in \mathbb{N}$ and $b \in [S_0]$, then $v | u_a^i$ or $v | b$.

2) A system $S_0 = (a_i)_{i \in I}$ of elements of S is said to be independent if for every $\imath \in I a_\imath$ is independent of $(a_i)_{i \in I \setminus \{\imath\}}$.

Remarks. 1) If $a \in S$ is independent of a system S_0, then a is neither a unit nor a product of primes in S, whence in particular $\sigma(a) \geq 2$.

2) By property (ii) an independent system does not contain equal elements, hence it is a set.

Let $S_0 = (a_i)_{i \in I}$ be a system of elements of S; we get

$$\beta(S_0) = (\beta(a_i))_{i \in I} \quad \text{and} \quad \gamma(S_0) = \bigcup_{i \in I} \gamma(a_i)\,.$$

Obviously $\gamma(S_0) = \gamma(\beta(S_0))$ and $\gamma(S) = G$.

Lemma 7. *For an element $a \in S$ and a system S_0 of elements of S the following conditions are equivalent:*

1) *a is independent of S_0.*
2) *$\beta(a)$ is independent of $\beta(S_0)$.*
3) *There exists a $g_a \in \gamma(a)$ which is independent of $\gamma(S_0)$.*

If a and every element of S_0 are of finite type, then there is further equivalence:

4) *There exists an irreducible $\pi_a \in S$ which is not prime such that the following conditions are fulfilled:*
   (i) *π_a divides some power of a.*
   (ii) *$\pi_a \nmid b$ for any $b \in [S_0]$.*
   (iii) *If $v \in S$ is irreducible and $v | \pi_a^k b$ for some $k \in \mathbb{N}$ and some $b \in [S_0]$, then $v | \pi_a^k$ or $v | b$.*

Proof. 1) $\Longrightarrow$ 2) Let $u_a \in S$ satisfy the conditions (i)–(iii) of Definition 7b. We contend that $\beta(u_a)$ does the job for $\beta(a)$. Obviously the properties (i) and (iii) are fulfilled and we assume that (ii) is violated. Then there exists an element $b \in S_0$ and an element $g \in \gamma(b)$ such that $\beta(u_a) = g(-g)$. Since u_a satisfies (ii), there are distinct prime divisors $\mathfrak{p}$, $\mathfrak{q}$ with $[\mathfrak{p}] = [\mathfrak{q}] = g$, $\mathfrak{p} | \partial u_a$ and $\mathfrak{q} | \partial b$. We set $\partial u_a = \mathfrak{p}\overline{\mathfrak{p}}$ and choose a $v \in S$ with $\partial v = \mathfrak{q}\overline{\mathfrak{p}}$. Then $v | u_a b$, $v \nmid u_a$ and thus by (iii) $v | b$, which implies that $\overline{\mathfrak{p}} | \partial b$. But then there exists a $b^* \in M(b)$ with $\mathfrak{p} | \partial b^*$ and hence $u_a | bb^*$, a contradiction.

2) $\Longrightarrow$ 3) For $A = \beta(a)$ let U_A be an irreducible block having the properties given in Definition 7b. Then $U_A = g_A(-g_A)$ for some $g_A \in \gamma(A)$. Assume, that g_A depends on $\gamma(S_0)$. Then there exist $g_1, \dots, g_k \in \gamma(S_0)$ and $m_A, n_1, \dots, n_k \in \mathbb{Z}$ such that

$$(*) \qquad 0 \neq m_A g_A = \sum_{j=1}^{k} n_j g_j \, .$$

Since for every g_j there are $g_{j,1}, \dots, g_{j,l_j} \in \gamma(S_0)$ with $-g_j = g_{j,1} + \dots + g_{j,l_j}$, we may assume without restriction that $m_A, n_1, \dots, n_k \in \mathbb{N}_+$. Further we may assume that $(m_A, n_1, \dots, n_k) \in \mathbb{N}_+^{k+1}$ is minimal (with respect to the usual order $\leq$ in $\mathbb{N}_+^{k+1}$) such that (*) holds. We choose blocks $B_j \in \beta(S_0)$ with $g_j | B_j$ and set $V = g_A^{m_A} \prod_{j=1}^k g_j^{n_j}$. Then V is irreducible and divides $U_A^{m_A} B_j^{n_j}$. By property (ii) g_A or $-g_A$ does not divide $\prod_{i=1}^k B_j^{n_j}$ and thus by (iii) V has to divide $U_A^{m_A}$. From this we infer $g_1 \in \{g_A, -g_A\}$ and thus $U_A | B_1 B_1^*$, a contradiction to (ii).

3) $\Longrightarrow$ 1) We choose a prime divisor $\mathfrak{p}_a \in g_a$ with $\mathfrak{p}_a | \partial a$ and an $u_a \in S$ with $\partial u_a = \mathfrak{p}_a \mathfrak{p}_a^*$ for an arbitrary prime divisor $\mathfrak{p}_a^* \in -g_a$. We check the properties (i)–(iii) of Definitions 7b:

(i) is obviously satisfied. If $u_a | bb^*$ for some $b \in S_0$ and $b^* \in M(b)$, then g_a depends on $\gamma(S_0)$, whence (ii) is fulfilled.

Finally let $v \in S$ be irreducible with $v | u_a^{k_a} b$ for some $k_a \in \mathbb{N}$ and $b \in [S_0]$. Assume that $v \nmid u_a^{k_a}$ and $v \nmid b$; then $\partial v = \mathfrak{q}^r \mathfrak{q}_1 \dots \mathfrak{q}_s$ with $r, s \in \mathbb{N}_+$, $\mathfrak{q} \in \{\mathfrak{p}_a, \mathfrak{p}_a^*\}$ and $\mathfrak{q}_1 \dots \mathfrak{q}_s | \partial b$. This, however, implies

$$0 \neq \pm r g_a = [\mathfrak{q}^r] = -\sum_{j=1}^{s} [\mathfrak{q}_j] \, ,$$

i.e. g_a depends on $\gamma(S_0)$, a contradiction.

3) $\Longrightarrow$ 4) Let $\mathfrak{p}_a \in g_a$ be a prime divisor with $\mathfrak{p}_a | \partial a$, and let $\pi_a \in S$ be an element with $\partial \pi_a = \mathfrak{p}_a^{\operatorname{ord}(g_a)}$. Since $g_a \neq 0$, π_a is not prime. We verify the properties (i)–(iii) of condition 4).

(i) is satisfied by construction. Since g_a is independent of $\gamma(S_0)$ we infer that $g_a \nmid \beta(b)$ and thus $\mathfrak{p}_a \nmid \partial b$ for any $b \in [S_0]$, which implies (ii).

Let $v \in S$ be irreducible with $v | \pi_a^{k_a} b$ for some $k_a \in \mathbb{N}$ and some $b \in [S_0]$. Then $\partial v = \mathfrak{p}_a^{m_a} \mathfrak{q}_1 \dots \mathfrak{q}_r$ with $\mathfrak{q}_1 \dots \mathfrak{q}_r | \partial b$. Since g_a is independent of $\gamma(S_0)$ it follows that $m_a \in \{0, \operatorname{ord}(g_a)\}$ and thus (iii) holds.

4) $\Longrightarrow$ 3) There is a prime divisor $\mathfrak{p}_a$ with $\mathfrak{p}_a | \partial \pi_a$ but $\mathfrak{p}_a \nmid \partial b$ for any $b \in [S_0]$. We set $g_a = [\mathfrak{p}_a]$ and assume to the contrary that g_a depends on $\gamma(S_0)$. Now the arguments run along the lines of the proof of 2) $\Longrightarrow$ 3). $\square$

Corollary 1. *For a system $S_0 = (a_i)_{i \in I}$ of elements of S the following conditions are equivalent:*

1) *S_0 is independent.*
2) *$\beta(S_0)$ is independent.*
3) *For every $\imath \in I$ there exists a $g_\imath \in \gamma(a_\imath)$ which is independent of $\gamma((a_i)_{i \in I \setminus \{\imath\}})$. (In particular this implies that $\{g_\imath \mid \imath \in I\} \subset G$ is independent).*

If all a_i, $i \in I$ are of finite type, then there is further equivalence:

4) *For every $\imath \in I$ there exists an irreducible $\pi_\imath \in S$ which is not prime and satisfies the conditions of point 4) of Lemma 7 with $(a_i)_{i \in I \setminus \{\imath\}}$ instead of S_0.*

Proof. 1) $\Longrightarrow$ 2) We have to show that for every $\imath \in I \beta(a_\imath)$ is independent of $(\beta(a_i))_{i \in I \setminus \{\imath\}}$. Let $\imath \in I$; since $a_\imath$ is independent of $(a_i)_{i \in I \setminus \{\imath\}}$, Lemma 7 implies that $\beta(a_\imath)$ is independent of $(\beta(a_i))_{i \in I \setminus \{\imath\}}$.

All remaining implications are similar. □

Theorem 1. *Let S be a semigroup with divisor theory where every class contains a prime divisor and let G be the divisor class group with* $\operatorname{card}(G) > 2$. *Then* $r(G) = \sup\{\operatorname{card}(S_0) \mid S_0 \subset S$ *is an independent subset*$\}$.

Proof. By Corollary 1 it suffices to proof the assertion for block semigroups. Again by Corollary 1 an independent set $S_0 \subset S$ gives rise to an independent set $G_0 \subset G$ and by Remark 3 after Definition 7a we infer $\operatorname{card}(G_0) \le r(G)$.

Let on the other hand G_0 be an independent set with $\operatorname{card}(G_0) = r(G)$. Then $\{g(-g) \mid g \in G_0\} \subset \mathcal{B}(G)$ is an independent subset. □

Remark. Using the notions finite type, infinite type and p-type, which were defined in Section 3, we obtain analogous arithmetical descriptions of the torsion rank, the torsionfree rank and the p-rank of G.

We close this section by verifying that independent sets satisfy a universal property.

Definition 8. We say that the rank of G can be extracted from a set $S_0 \subset S$, if $r(\langle\gamma(S_0)\rangle) = r(G)$.

Proposition 1. *If the rank of G can be extracted from a set S_0 but not from a proper subset, then S_0 is independent.*

Proof. Assume S_0 to be not independent. By Lemma 7 there is an $a \in S_0$ such that every $g \in \gamma(a)$ depends on $\gamma(S_0 \setminus \{a\})$. This implies

$$r(\langle\gamma(S_0 \setminus \{a\})\rangle) = r(\langle\gamma(S_0 \setminus \{a\}) \cup \gamma(a)\rangle) = r(G)\,,$$

and hence the rank of G can be extracted from $S_0 \setminus \{a\}$, a contradiction. □

5. Pure Subgroups of a Divisor Class Group

In this section we assume G to be a torsion group. Our first aim is to derive an arithmetical analogue to pure subgroups (Definition 9b, Lemma 9). After dealing with the type of an independent subset we introduce pure-independent subsets (Definition 11), which provide the central notion in our discussion. We establish a correspondence between the type of a pure-independent subset $S_0 \subset S$ and the type of a pure-independent subset $G_0 \subset G$. This finally allows us to describe the type of a basic subgroup of G (Theorem 2).

Definition 9a. A subset $H \subset G$ is called pure, if it generates a pure subgroup i.e. if $nG \cap \langle H \rangle = n \langle H \rangle$ for all $n \in \mathbb{N}_+$.

Remarks. 1) Obviously, $H \subset G$ is pure if and only if $nG \cap \langle H \rangle \subset n \langle H \rangle$ for all $2 \leq n \in \mathbb{N}_+$.

2) Let $H < G$ be a subgroup. If H is a direct summand then it is pure; conversely, if $H < G$ is a bounded pure subgroup, then it is a direct summand.

For a subset $U \subset S$ we set

$$U^d = \{ a \in S \mid a \text{ divides some } b \in U \}$$

and

$$\begin{aligned}\langle U \rangle = \{ a \in S \mid\ & \text{if } \pi \text{ is a homogenous divisor of some power of } a, \\ & \text{not block equal with any } \pi' \in [U]^d, \text{ then } \pi \text{ and} \\ & a \text{ are not block equal but } \pi^{-1} a^{\sigma(\pi)} \in [U]^d \}.\end{aligned}$$

$\langle U \rangle$ is defined in such a way, that Lemma 8.5 holds.

Lemma 8. *Let $U \subset S$ be a subset.*

1) $\beta(U^d) = \beta(U)^d$.

2) $[\beta(U)] = \beta([U])$.

3) $\mathcal{B}(\gamma(U) = [\beta(U)]^d$.

4) $\beta(\langle U \rangle) = \langle \beta(U) \rangle$.

5) $\gamma(\langle U \rangle) = \langle \gamma(U) \rangle$.

6) $\mathcal{B}(\langle \gamma(U) \rangle) = [\langle \beta(U) \rangle]^d = \beta([\langle U \rangle]^d)$.

Proof. 1) Let $B \in \beta(U^d)$; then there are an $a \in U^d$ and a $b \in U$ with $a|b$ and $B = \beta(a)$. Thus $\beta(a)|\beta(b)$, $\beta(b) \in \beta(U)$ and $B = \beta(a) \in \beta(U)^d$.

Conversely, let $B \in \beta(U)^d$; then $B|\beta(b)$ for some $b \in U$. Since there is an $a \in S$ with $a|b$ and $B = \beta(a)$, we infer that $B = \beta(a) \in \beta(U^d)$.

2) Let $B \in \mathcal{B}(G)$; $B \in \beta([U])$ if and only if $B = \beta(\prod_{i=1}^r b_i)$, with $b_i \in U$, if and only if $B = \prod_{i=1}^r \beta(b_i) \in [\beta(U)]$.

3) Let $B = \prod_{i=1}^r g_i \in \mathcal{B}(\gamma(U))$; then for every $1 \leq i \leq r$ there is an $a_i \in U$ with $g_i|\beta(a_i)$ and thus $B = \prod_{i=1}^r g_i | \prod_{i=1}^r \beta(a_i)$ i.e. $B \in [\beta(U)]^d$.

Conversely, let $B \in [\beta(U)]^d$; thus there are $a_1, \ldots, a_r \in U$ such that $B | \prod_{i=1}^r \beta(a_i)$. Therefore $\gamma(B) \subset \gamma(U)$ and consequently $B \in \mathcal{B}(\gamma(U))$.

4) We start with a description of $\langle \beta(U) \rangle$:

$$\begin{aligned}\langle \beta(U) \rangle = \{\, A \in \mathcal{B}(G) \mid\ & \text{if } C = g^{\operatorname{ord}(g)} \text{ divides some power of } A \\ & \text{and } C \notin [\beta(U)]^d = \mathcal{B}(\gamma(U)), \text{ then} \\ & A \neq C \text{ and } C^{-1} A^{\operatorname{ord}(g)} \in \mathcal{B}(\gamma(U)) \,\} \\ = \{\, A \in \mathcal{B}(G) \mid\ & \text{if } g \in \gamma(A) \setminus \gamma(U), \text{ then } A \neq g^{\operatorname{ord}(g)} \\ & \text{and } g^{-\operatorname{ord}(g)} A^{\operatorname{ord}(g)} \in \mathcal{B}(\gamma(U)) \,\} \\ = \mathcal{B}(\gamma(U)) \cup \{\, & \prod_{i=0}^r g_i \mid r \in \mathbb{N}_+,\, g_0 \notin \gamma(U) \text{ but } g_i \in \gamma(U) \\ & \text{for } 1 \le i \le r \,\}\,.\end{aligned} \tag{*}$$

Further we have

$$\begin{aligned}\beta(\langle U \rangle) = \{\, \beta(a) \in \mathcal{B}(G) \mid\ & \text{if a homogenous } \pi \in S \text{ divides some power} \\ & \text{of } a \in S \text{ and } \pi \text{ is not block equal with} \\ & \text{any } \pi' \in [U]^d, \text{ then } \pi \text{ and } a \text{ are not block} \\ & \text{equal but } \pi^{-1} a^{\sigma(\pi)} \in [U]^d \,\} \\ = \{\, \beta(a) \in \mathcal{B}(G) \mid\ & \text{if a homogenous } \pi \in S \text{ divides some power} \\ & \text{of } a \text{ and } \beta(\pi) \notin \beta([U]^d) = \mathcal{B}(\gamma(U)), \text{ then} \\ & \beta(\pi) \neq \beta(a) \text{ but } \pi^{-1} a^{\sigma(\pi)} \in [U]^d \,\}.\end{aligned}$$

Let $\beta(a) \in \beta(\langle U \rangle)$ and let C be a homogenous divisor of some power of $\beta(a)$ with $C \notin \mathcal{B}(\gamma(U))$. Then there is a homogenous π dividing some power of a with $\beta(\pi) = C$. Then $C \neq \beta(a)$ and $\pi^{-1} a^{\sigma(\pi)} \in [U]^d$, which implies $\beta(\pi)^{-1} \beta(a)^{\sigma(\pi)} \in \beta([U]^d) = \mathcal{B}(\gamma(U))$. Therefore $\beta(a) \in \langle \beta(U) \rangle$.

Conversely, let $A \in \langle \beta(U) \rangle$. Firstly, if $A \in \mathcal{B}(\gamma(U))$, then there is an $a \in [U]^d$ with $A = \beta(a) \in \beta(\langle U \rangle)$. Secondly, if $A = \prod_{i=0}^r g_i$ with $g_0 \notin \gamma(U)$ and $g_i \in \gamma(U)$ for $1 \le i \le r$, then there is an $a \in S$ with $\partial a = \prod_{i=0}^r \mathfrak{p}_i$, $\mathfrak{p}_i \in g_i$ and $\mathfrak{p}_i | \partial a_i$ for some $a_i \in [U]^d$, $1 \le i \le r$. So if π is a homogenous divisor of some power of a with $\beta(\pi) \notin \mathcal{B}(\gamma(U))$, then $\beta(\pi) = g_0^{\operatorname{ord}(g_0)}$ and we infer that $\beta(\pi) \neq A$ and $\pi^{-1} a^{\sigma(\pi)} \in [U]^d$.

5) Because $\langle \gamma(U) \rangle = \langle \gamma(\beta(U)) \rangle$ and $\gamma(\langle U \rangle) = \gamma(\beta(\langle U \rangle)) = \gamma(\langle \beta(U) \rangle)$ it remains to show that $\langle \gamma(V) \rangle = \gamma(\langle V \rangle)$ for $V = \beta(U) \subset \mathcal{B}(G)$.
By relation (*) we obtain

$$\gamma(\langle V \rangle) = \gamma(V) \cup \{\, g_0 \in G \mid g_0 = -\sum_{i=1}^r g_i \text{ with } g_i \in \gamma(V) \,\} = \langle \gamma(V) \rangle\,.$$

6) $\mathcal{B}(\langle\gamma(U)\rangle) \overset{5)}{=} \mathcal{B}(\gamma(\langle U\rangle)) \overset{3)}{=} [\beta(\langle U\rangle)]^d \overset{2)}{=} \beta([\langle U\rangle])^d \overset{1)}{=} \beta([\langle U\rangle]^d)$.
Furthermore $\mathcal{B}(\langle\gamma(U)\rangle) = \mathcal{B}(\langle\gamma(\beta(U))\rangle) \overset{5)}{=} \mathcal{B}(\gamma(\langle\beta(U)\rangle)) \overset{3)}{=} [\langle\beta(U)\rangle]^d$. □

Definition 9b. A subset $U \subset S$ is called pure if for all $2 \le n \in \mathbb{N}_+$ and all n-simple elements $a \in S$ with $\overline{a} \in [\langle U\rangle]^d$ there is an n-simple element $b \in [\langle U\rangle]^d$ with $\overline{a} \simeq \overline{b}$.

Lemma 9. *For a subset $U \subset S$ the following conditions are equivalent:*

1) *$U \subset S$ is pure.*
2) *$\beta(U) \subset \beta(S) = \mathcal{B}(G)$ is pure.*
3) *$\gamma(U) \subset \gamma(S) = G$ is pure.*

Proof. Obviously 3) holds if and only if

3)' $\langle\gamma(U)\rangle < G$ is pure

holds. Further 3)' is equivalent to

2)' for all $2 \le n \in \mathbb{N}_+$ and all n-simple blocks $A \in \mathcal{B}(G)$ with $\overline{A} \in \mathcal{B}(\langle\gamma(U)\rangle)$ there is an n-simple block $B \in \mathcal{B}(\langle(U)\rangle)$ with $\overline{A} = \overline{B}$.

By Lemma 8 $\mathcal{B}(\langle\gamma(U)\rangle) = [\langle\beta(U)\rangle]^d$, and thus 2)' is equivalent to 2) by definition. Again by Lemma 8 $[\langle\beta(U)\rangle]^d = \beta([\langle U\rangle]^d)$ and thus 2)' is equivalent to

2)" for all $2 \le n \in \mathbb{N}_+$ and all n-simple elements $A \in \mathcal{B}(G)$ with $\overline{A} \in \beta([\langle U\rangle]^d)$ there is an n-simple block $B \in \beta([\langle U\rangle]^d)$ with $\overline{A} = \overline{B}$.

So it remains to verify the equivalence between 1) and 2)".

1) $\implies$ 2)" Let $2 \le n \in \mathbb{N}_+$, $A \in \mathcal{B}(G)$ n-simple with $\overline{A} \in \beta([\langle U\rangle]^d)$. Then there exists an n-simple $a \in S$ with $\beta(a) = A$, $\beta(\overline{a}) = \overline{\beta(a)} = \overline{A}$ and $\overline{a} \in [\langle U\rangle]^d$. Since $U \subset S$ is pure, there is an n-simple $b \in [\langle U\rangle]^d$ with $\overline{a} \simeq \overline{b}$; therefore $B = \beta(b) \in \beta([\langle U\rangle]^d)$ and $\overline{B} = \overline{\beta(b)} = \beta(\overline{b}) = \beta(\overline{a}) = \overline{A}$.

2)" $\implies$ 1) Let $2 \le n \in \mathbb{N}_+$ and $a \in S$ n-simple with $\overline{a} \in [\langle U\rangle]^d$. Then $A = \beta(a) \in \mathcal{B}(G)$ is n-simple and $\overline{A} = \overline{\beta(a)} = \beta(\overline{a}) \in \beta([\langle u\rangle]^d)$. Therefore there is an n-simple $B \in \beta([\langle U\rangle]^d)$ with $\overline{B} = \overline{A}$ i.e. $B = \beta(b)$ for some n-simple $b \in [\langle U\rangle]^d$ and $\beta(\overline{b}) = \overline{\beta(b)} = \overline{B} = \overline{A}$. Thus there is also an n-simple $c \in [\langle U\rangle]^d$ with $\beta(c) = \beta(b)$ and $\overline{a} \simeq \overline{c}$. □

Definition 10. For every element a of an independent set $S_0 \subset S$ we set

$$n_a(S_0 \setminus \{a\}) = n_a = \max\{\, \sigma(u_a) \mid u_a \text{ is a homogenous divisor of some power of } a \text{ and is independent of } S_0 \setminus \{a\}\,\}$$

and we call $(n_a)_{a\in S_0} \in \mathbb{N}_+^{S_0}$ the type of S_0.

By Remark 1 after Definition 7b we infer $n_a \ge 2$ for every $a \in S_0$.

Lemma 10. *Let $S_0 \subset S$ be independent. Then for every $a \in S_0$*

$$\begin{aligned} n_a(S_0 \setminus \{a\}) &= n_{\beta(a)}(\beta(S_0 \setminus \{a\})) \\ &= \max\{\operatorname{ord}(g_a) \mid g_a \in \gamma(a) \textit{ is independent of } \gamma(S_0 \setminus \{a\})\}\,. \end{aligned}$$

Proof. 1 i) Let u_a be a homogenous divisor of some power of a, which is independent of $S_0 \setminus \{a\}$ with $\sigma(u_a) = n_a$. Then $\beta(u_a)$ is a homogenous divisor of some power of $\beta(a)$, $\beta(u_a)$ is independent of $\beta(S_0 \setminus \{a\})$ and thus

$$n_a = \sigma(u_a) = \sigma(\beta(u_a)) \leq n_{\beta(a)}(\beta(S_0 \setminus \{a\}))\,.$$

ii) Let B be a homogenous divisor of some power of $\beta(a)$, which is independent of $\beta(S_0 \setminus \{a\})$ with $\sigma(B) = n_{\beta(a)}(\beta(S_0 \setminus \{a\}))$. Then there is a homogenous u_a with $\beta(u_a) = B$ such that u_a divides some power of a and u_a is independent of $S_0 \setminus \{a\}$. Therefore

$$n_{\beta(a)} = \sigma(B) = \sigma(u_a) \leq n_a(S_0 \setminus \{a\})\,.$$

2 i) Let B be a homogenous divisor of some power of $\beta(a)$ which is independent of $\beta(S_0 \setminus \{a\})$ with $\sigma(B) = n_{\beta(a)}(\beta(S_0 \setminus \{a\}))$. Then there exists a $g \in \gamma(B)$ which is independent of $\gamma(S_0 \setminus \{a\})$. Thus

$$n_{\beta(a)} = \sigma(B) = \operatorname{ord}(g) \leq \max\{\operatorname{ord}(g_a) \mid \ldots\}\,.$$

ii) Let $g_a \in \gamma(a)$ be independent of $\gamma(S_0 \setminus \{a\})$ with $\operatorname{ord}(g_a) = \max\{\ldots\}$. Then $B = g_a^{\operatorname{ord}(g_a)}$ is a homogenous divisor of $\beta(a)^{\operatorname{ord}(g_a)}$ and B is independent of $\beta(S \setminus \{a\})$. Thus

$$\max\{\ldots\} = \operatorname{ord}(g_a) = \sigma(B) \leq n_{\beta(a)}\,.$$

□

Definition 11. a) A subset $H \subset G$ is called pure-independent, if it is pure and independent.

b) An independent set $S_0 \subset S$ is called pure-independent, if for every $a \in S_0$ there exists a homogenous u_a dividing some power of a such that u_a is independent of $S_0 \setminus \{a\}$, $\sigma(u_a) = n_a$ and $(u_a)_{a \in S_0}$ is pure.

Remark. Bourbaki uses the notion pseudofree instead of pure-independent cf. [**2,** A. VII. 55].

We combine the results of Lemma 7, Lemma 9 and Lemma 10.

Corollary 2. *For an independent subset $S_0 \subset S$ of type $(n_a)_{a \in S_0}$ the following conditions are equivalent:*

1) *S_0 is pure-independent.*
2) *$\beta(S_0)$ is pure-independent.*
3) *For every $a \in S_0$ there exists a $g_a \in \gamma(a)$ such that g_a is independent of $\gamma(S_0 \setminus \{a\})$, $\operatorname{ord}(g_a) = n_a$ and $(g_a)_{a \in S_0}$ is pure-independent.*

Proof. Obvious. □

Definition 12. A subgroup $H < G$ is a basic subgroup of G if
1) H is a direct sum of cyclic groups.
2) $H < G$ is pure.
3) G/H is divisible.

Remarks. 1) Every abelian torsion group G contains a basis subgroup and all basic subgroups are isomorphic ([**14,** 4.3.4 and 4.3.6]).

2) If G is bounded and $H < G$ a basic subgroup, then G/H is bounded and divisible; thus $G/H = \{0\}$ and $G = H$.

Theorem 2. *Let S be a semigroup with divisor theory such that the divisor class group G is a torsion group with* $\operatorname{card}(G) > 2$ *and every class contains a prime divisor.*

1) *Let $S_0 \subset S$ be a (pure)-independent subset of type $(n_a)_{a\in S_0}$ and $H = \oplus_{a\in S_0} C_{n_a}$. Then H is isomorphic to a (pure) subgroup of G. If S_0 is a maximal pure-independent subset consisting of homogenous elements, then H is isomorphic to a basic subgroup of G.*

2) *Let $H < G$ be a non-trivial (pure) subgroup which is a direct sum of cyclic groups. Then there exists a (pure)-independent subset $S_0 \subset S$ of type $(n_a)_{a\in S_0}$ such that $H \simeq \oplus_{a\in S_0} C_{n_a}$.*

Remark. If G is direct sum of cyclic groups, then also every subgroup $H < G$ ([**3,** Theorem 18.1]).

Proof. We may restrict to block semigroups.

1) For $A \in S_0 \subset \mathcal{B}(G)$ let $g_A \in \gamma(A)$ be independent of $\gamma(S_0 \setminus \{A\})$ with $\operatorname{ord}(g_A) = n_A$. Then obviously $H = \oplus_{A\in S_0} C_{n_A} \simeq \oplus_{A\in S_0}\langle g_A\rangle < G$. If S_0 is pure-independent, then by Corollary 2 g_A may be chosen in such a way that $\oplus_{A\in S_0}\langle g_A\rangle < G$ is pure.

If S_0 is a maximal pure-independent subset consisting of homogenous elements, then $\{g_A | A \in S_0\}$ is a maximal pure-independent subset. In order to show that $\oplus_{A\in S_0}\langle g_A\rangle$ is a basic subgroup of G, it is sufficient to proof that $G/\oplus_{A\in S_0}\langle g_A\rangle$ is divisible, which follows from Lemma 10.31 in [**15**]. Indeed, Lemma 10.31 is formulated for p-groups but is valid for arbitrary abelian torsion groups. For this one has to derive Lemma 10.29 in [**15**] for abelian torsion groups and then the proof of the general case is entirely the same as the proof for p-groups.

2) Since H is a direct sum of cyclic groups, there exists a basis $H_0 \subset H$ such that $H = \oplus_{g\in H_0}\langle g\rangle$. Then $S_0 = \{g^{\operatorname{ord}(g)} | g \in H_0\} \subset \mathcal{B}(G)$ is independent of type $(\operatorname{ord}(g))_{g\in H_0}$. If $H < G$ is pure, then S_0 is pure-independent by Corollary 2. $\square$

Finally we verify a universal property of the type of an independent set.

Definition 13. We say that the structure of a subgroup $H < G$ can be extracted from an independent set $S_o \subset S$ if $\langle\gamma(S_0)\rangle = H$.

Proposition 2. *Let $H < G$ be a (pure) subgroup which is a direct sum of finite cyclic groups and $S_0 \subset S$ an independent set. If the structure of H can be extracted from every independent set $S_0' = \{c_a \in S \mid a \in S_0\}$ where c_a divides some power of a, then S_0 is (pure-) independent of type $(n_a)_{a \in S_0}$, where $\oplus_{a \in S_0} C_{n_a} \simeq H$.*

Proof. Without restriction we assume $S = \mathcal{B}(G)$. For $A \in S_0$ let $g_A \in \gamma(A)$ be independent of $\gamma(S_0 \setminus \{A\})$ with $\operatorname{ord}(g_A) = n_A$. Then $S_0' = \{g_A^{n_A} | A \in S_0\}$ is an independent set. Since the structure of H can be extracted from it we obtain

$$H = \langle \gamma(S_0') \rangle = \bigoplus_{A \in S_0} \langle g_A \rangle \simeq \bigoplus_{A \in S_0} C_{n_A}\,.$$

If $H < G$ is pure, then $(g_A)_{A \in S_0}$ is pure-independent, and by Corollary 2 S_0 is pure-independent. □

References

1. Borewicz S. I. and Šafarevič I. R., *Zahlentheorie*, Birkhäuser, 1966.
2. Bourbaki N., *Algebra II*, Springer, 1990.
3. Fuchs L., *Infinite abelian groups I*, Academic Press, 1970.
4. Geroldinger A., *Arithmetical characterizations of divisors class groups*, Arch. Math. **54** (1990), 455–464.
5. ———, *Systeme von Längenmengen*, Abh. Math. Sem. Univ. Hamburg **60** (1990), 115–130.
6. Geroldinger A. and Halter-Koch F., *Realization theorems for semigroups with divisor theory*, Semigroup Forum **44** (1992), 229–237.
7. Gilmer R., *Commutative semigroup rings*, The University of Chicago Press, 1984.
8. Halter-Koch F., *Factorisation of algebraic integers*, Bericht Nr. 191 (1983) der Math. Statist. Sektion d. Forschungszentrums Graz.
9. ———, *Halbgruppen mit Divisorentheorie*, Expo. Math. **8** (1990), 27–66.
10. ———, *Ein Approximationssatz für Halbgruppen mit Divisorentheorie*, Results in Math. **19** (1991), 74–82.
11. Kaczorowski J., *A pure arithmetical definition of the class group*, Coll. Math. **48** (1984), 265–267.
12. Krause U. and Zahlten C., *Arithmetic in Krull monoids and the cross number of divisor class groups*, Mitteilungen d. Math. Gesellschaft Hamburg **12** (1991), 681–696.
13. Narkiewicz W., *Elementary and analytic theory of algebraic numbers*, PWN, 1974.
14. Robinson D., *A course in the theory of groups*, Springer, 1982.
15. Rotman J., *An introduction to the theory of groups*, Allyn and Bacon, 1984.
16. Rush D. E., *An arithmetic characterization of algebraic number fields with a given class group*, Math. Proc. Cambr. Phil. Soc. **94** (1983), 23–28.
17. Skula L., *Divisorentheorie einer Halbgruppe*, Math. Z. **114** (1970), 113–120.
18. ———, *On c-semigroups*, Acta Arith. **31** (1976), 247–257.

A. Geroldinger, Institut für Mathematik, Karl-Franzens-Universität, Heinrichstrasse 36/IV, A-8010 Graz, Austria