Annales Mathematicae Silesianae 12 (1998), 149–156

Prace Naukowe Uniwersytetu Śląskiego nr 1751, Katowice

SETS OF REGULAR SYSTEMS OF DIVISORS OF A GENERALIZED INTEGER

ŠTEFAN PORUBSKÝ

Dedicated to the memory of Professor Ivan Korec

Abstract. The notion of a regular system of divisors of a number underlying a Narkiewicz's idea of the generalization of the familiar Dirichlet and unitary convolution of arithmetical functions is used to extend some combinatorial results about systems of subsets of divisors of a generalized integer.

In 1963 W. Narkiewicz [Nark1963] introduced a class of binary operations on arithmetical functions generalizing the known Dirichlet and unitary convolution. The generalization was based on the idea to associate with every positive integer n not the whole set of all divisors or the set of all unitary divisors of n, resp., but only a subset of the set of all divisors of n which fulfils certain properties. In the original setting these properties were then determined by the properties imposed on the resulting convolution. In what follows we shall not concern more about the original convolution background. The idea is capable of further extension to the so called arithmetical semigroups. Here (cf. [Knop75]), an **arithmetical semigroup** is a commutative semigroup $(G, .)$ with identity element $1 = 1_G$ and with at most countable set P of generators (called **primes** of G) such that every element

Received on September 29, 1998.

1991 *Mathematics Subject Classification.* 05A05, 11B75, 11N80.

Key words and phrases: Generalized integer, arithmetical semigroup, Narkiewicz's regular system of divisors.

The paper was written while the author was visiting Tel Aviv University. The author would like to express his sincere thanks to the School of Mathematical Sciences of Raymond and Beverly Sackler Faculty of Exact Sciences, in particular to Professor Jochanan Schönheim, for the support during the stay. Research was also partially supported by the Grant Agency of the Czech Republic, Grant # 201/97/0433. The author also thanks Professor John Knopfmacher for his comments on an earlier version of the manuscript.

$a \neq 1$ in G can be uniquely (up to the order of the factors) represented in the form

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

where the p_i are distinct elements of P, the α_i are positive integers, and r may be arbitrary. Further, it is supposed that there exists a real–valued norm $|\cdot|$ defined on G such that

(i) $|1| = 1$, $|p| > 1$ for $p \in P$,
(ii) $|mn| = |m||n|$ for all $m, n \in G$,
(iii) the set $\{n \in G : |n| \leqslant x\}$ is finite for all real numbers x.

However, in what follows we shall not need those properties of G which follow from the existence of the norm mapping $|\cdot|$. Mainly because most of our reasoning employs the divisibility relation induced by the multiplication in G and in this situation each element of G has only a finite number of divisors what in the argumentation replaces requirement (iii). Neither, we shall use any consequence of the restriction on the cardinality of the set P of generators of G in the above definition. Note, that dealing with algebraic and combinatorial properties of G without reference to properties of the norm map, the generalized results are not routine consequences of the fact that G is isomorphic algebraically to the set of positive integers $\mathbb{N}$ if P has infinitely many elements, or else to a subsemigroup of $\mathbb{N}$ if P is finite.

The unique factorization in G enables us to define terms like **divisor** in the expected way. We say that an element b, divides $a \in G$, in symbols $b|a$, if $a = bc$ for some $c \in G$. Let

$$D(n) = \{d \in G \ : \ d|n\}$$

denote the set of all divisors of $n \in G$.

Let A be a mapping from the given arithmetical semigroup G into the set of subsets of G such that $A(n)$ is a subset of the set $D(n)$ for every $n \in \mathbb{N}$. The elements of $A(n)$ will be called **A–divisors** of n. The system

(1) $$\{A(n) \ : \ n \in \mathbb{N}\}$$

will be called **regular system of divisors** (or more precisely, **regular system of A–divisors**, if a confusion with the ordinary divisors is possible) provided:

(a) $d \in A(n) \Rightarrow n/d \in A(n)$
(b) if $(m, n) = 1$ then $A(mn) = A(m) \cdot A(n)$, where $A \cdot B = \{ab : a \in A, b \in B\}$
(c) $\{1, n\} \subset A(n)$ for all n
(d) the statement "$d \in A(m), m \in A(n)$" is equivalent to "$d \in A(n), m/d \in A(n/d)$"

(e) if p is a prime, then $A(p^k) = \{1, p^v, p^{2v}, \dots, p^{rv} = p^k\}$ with some $v \in \mathbb{N}$, and moreover $p^v \in A(p^{2v})$, $p^{2v} \in A(p^3 v), \dots, p^{(r-1)v} \in A(p^k)$

These conditions as stated here are not independent. The most known example of regular systems of divisors besides $D(n)$ is the set of **unitary divisors**

$$U(n) = \{d \in G \ : \ d|n, (d, n/d) = 1\}.$$

Here, (a, b) denotes the greatest common divisor. The system $\{D(n) : n \in G\}$ is connected with the well–known Dirichlet and the system $\{U(n) : n \in G\}$ with the so called unitary convolution, resp. That there are infinitely many regular systems of divisors follows from Theorem II of [Nark1963] which can be easily extended to the case of a general G. A way how to construct regular systems of divisors (generally different, though not always) from the given one is described in the next result (originally also formulated only for the case $G = \mathbb{N}$):

LEMMA 1 [Rama1978, Theorem 3.1]. *Let (1) be a regular system of divisors on G and k a fixed positive integer. For each $n \in G$ define*

$$A_k(n) = \{d \ : \ d^k \in A(n^k)\}. \tag{2}$$

Then the family $\{A_k(n) : n \in \mathbb{N}\}$ forms again a regular system of divisors on G.

Note (cf. [Rama1978, Remark 3.2]) that the converse of Lemma 1 is not true in general. System A_k may be regular without being that of A regular one.

In the rest of the paper we shall suppose that the regular system of A–divisors in an arithmetical semigroup G is fixed though arbitrary.

THEOREM 1. *Let G be an arithmetical semigroup and (1) a regular systems of divisors. If $F = \{D_1, \dots, D_s\} \subset A(N)$, $N \in G$, such that*

$$X \in A(D_i) \Rightarrow X \in F, \qquad (\textit{or equivalently} \quad X \in F \Rightarrow A(X) \subset F) \tag{3}$$

then there exists a permutation σ of $\{1, 2, \dots, s\}$ such that

$$D_i \in A\left(\overline{D_{\sigma(i)}}\right),$$

where $\overline{D} = N/D$ denotes the "divisor complement with respect to N".

Note that (a) implies $\overline{D} \in A(N)$ for every $D \in A(N)$. Theorem 1 immediately extends the following result proved by M. Herzog and J. Schönheim:

Corollary 1 [HeSc1972] [Theorem 1]. *If $F = \{D_1, \ldots, D_s\}$ is a family of divisors of a natural integer N satisfying*

$$X|D_i \Rightarrow X \in F \qquad (i = 1, 2, \ldots, s)$$

then there exists a permutation σ of $\{1, 2, \ldots, s\}$ such that

$$D_i|\overline{D_{\sigma(i)}} \quad \textit{for } i = 1, 2, \ldots, s.$$

The proof of Theorem 1 will parallel the ideas used in [HeSc1972].

Let $N = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ be the standard decomposition of $N \in G$ into distinct primes. We shall process by induction on n. If $n = 1$, then (cf. (e))

$$F \subset A(p_1^{\alpha_1}) = \{1, p_1^v, \ldots, p_1^{av} = p_1^{\alpha_1}\}.$$

If $D \in F$ then (3) implies $A(D) \subset F$ and we get using (d) that

$$F = \{1, p_1^v, \ldots, p_1^{rv} = p_1^{\alpha_1}\}$$

for some $r \leqslant a$.

If $D_i = p_1^{vi}$ for some $i = 0, 1, \ldots, r$, then $\overline{D_i} = N/D_i = p_1^{(a-i)v}$ and (a) gives $\overline{D_i} \in A(N) = A(p_1^{av})$. Then we claim that

$$i \mapsto (r - i)$$

generates the required permutation. This means that

$$D_i = p_1^{vi} \in A\left(\overline{D_{r-i}}\right). \tag{4}$$

To prove the last relation observe firstly that $\overline{D_{r-i}} = p^{iv+(a-r)v}$ with $a - r \geqslant 0$. Further, since $p^v \in A(p^{2v})$ and $p^{2v} \in A(p^{3v})$, (d) implies $p^v \in A(p^{3v})$. Similarly, $p^v \in A(p^{3v})$ and $p^{3v} \in A(p^{4v})$ yield $p^v \in A(p^{4v})$. Thus by induction

$$p^v \in A(p^{kv}) \qquad \text{for } k = 1, 2, 3, \ldots \tag{5}$$

Property (e) gives $p^{iv} \in A(p^{iv+v})$. Similarly $p^{(i+1)v} \in A(p^{(i+1)v+v})$. On the other hand, also $p^v \in A(p^{(i+2)v})$ due to (5). Property (d) in turn implies that $p^{iv} \in A(p^{(i+2)v})$. Along similar lines $p^{iv} \in A(p^{(i+3)v})$ and we can continue in increasing the exponent until we reach the exponent $iv + (a - r)v$, i.e. $p^{iv} \in A(p^{iv+(a-r)v})$, and (4) follows.

Suppose that the Theorem is true for positive integers N with less than n distinct prime factors in its standard decomposition.

Let p be a prime dividing (with respect to the ordinary division) some element of F and let α be the exponent of p in the standard decomposition of N. If a power p^b of p belongs to $A(d)$ for some $d \in A(N)$, then (d), or (b) and (c), shows that $p^b \in A(N)$. It follows from (b) that

$$A(N) = A(p^\alpha) \cdot A(N'), \qquad N' = N/p^\alpha,$$

and consequently $p^b \in A(p^\alpha)$. Property (e) implies that

$$A(p^\alpha) = \{1, p^v, p^{2v}, \dots, p^{av}\}$$

with suitable a, v such that $av = \alpha$. Therefore, if a power p^b A–divides an A–divisor of N, then

$$p^b \in A(p^\alpha) = \{1, p^v, p^{2v}, \dots, p^{av} = p^\alpha\}$$

and $v|b$. If $p^t, t \leqslant \alpha$, is the highest power of p dividing (or, what is the same A–dividing) any of the elements of F, then $t = vr$ for some r such that $1 \leqslant r \leqslant a$, and the set of A–divisors of elements of F which are powers of p is of the form

$$\{1, p^v, p^{2v}, \dots, p^{vr} = p^t\}.$$

Let

$$F = \bigcup_{j=0}^{r} F_j$$

be a partition of F into subfamilies $F_j, j = 0, 1, \dots, r$, where each F_j contains those $D \in F$ for which the standard g.c.d. $(D, p^t) = p^{vj}$, and

$$F_j' = \left\{d \; : \; d = D/p^{vj}, D \in F_j\right\}, j = 0, 1, \dots, r.$$

Denote by s_j the cardinality of F_j, or what is the same, the cardinality of F_j' for $j = 0, 1, \dots, r$.

Clearly, $F_j' \subset A(N')$, $(j = 0, 1, \dots, r)$, where $N' = N/p^\alpha$. We intend to apply the induction hypothesis on each of the sets

$$F_j', \quad j = 0, 1, \dots, r.$$

Let j, $j = 0, 1, \dots, r$, be fixed. Let $D \in F_j'$, then $D \in A(N')$, but also $p^\alpha \in A(p^\alpha)$, as (c) shows. Consequently, $p^\alpha D \in A(N)$, and $N/(p^\alpha D) \in A(N)$, even $N/(p^\alpha D) = N'/D \in A(N')$. Denote by $\widehat{\ }$ the modification of the above obliteration operation of taking the divisor complement but now with respect to $N' = N/p^\alpha$ instead of with respect to N, that is

$$\widehat{D} = N/(p^\alpha D).$$

Moreover, if $X \in A(D)$ and $D \in F'_j$, then $p^{jv}X \in F_j$ and $X \in F'_j$.

This altogether shows that the assumptions of the Theorem are satisfied if we replace $F, N, \overline{D}$ by $F'_j, N/p^\alpha, \widehat{D}$ (for every $j = 0, 1, \dots, r$). Since $N' = N/p^\alpha$ has only $n-1$ different prime factors, we can apply the induction hypothesis to obtain a permutation τ_j of $[1, \dots, s_j]$ for which

$$d_\nu \in A\left(\widehat{d_{\tau_j(\nu)}}\right), \qquad 1 \leqslant \nu \leqslant s_j \tag{6}$$

for every $j = 0, 1, \dots, t$.

Observe that the sets $F'_j, j = 0, 1, \dots, r$ can be endowed with a certain multilateral structural dependence. To see this let $0 \leqslant h < k \leqslant r$ and $d \in F'_k$. Then

$$d = \frac{D}{p^{vk}} = \frac{D}{p^{(k-h)v}} \cdot \frac{1}{p^{hv}}$$

and (3) implies that $D/p^{(k-h)v} \in F_k$, $d \in F'_h$, i.e. $F'_h \supset F'_k$. Hence $s_0 \geqslant s_h \geqslant s_k \geqslant s_r$, and we can order the elements of the sets F'_j for $j = 0, 1, \dots, r$ in such a way that if $F_0 = \{d_1, d_2, \dots, d_{s_0}\}$ then

$$F'_j = \{d_1, d_2, \dots, d_{s_j}\} \quad j = 0, 1, \dots, r.$$

We saw that the elements of F_j are of the form $p^{jv}d_\nu$, $\nu = 1, \dots, s_j$. If we denote $D_{j,\nu} = p^{jv}d_\nu$, then

$$F = \{D_{j,\nu} \ : \ j = 0, \dots, r, \ \nu = 1, \dots, s_j\}. \tag{7}$$

Given a permutation σ_ℓ for $\ell = 0, 1, \dots, r$ of $[1, 2, \dots, s_j]$, define a permutation τ of the index set of (7) by

$$\tau(j, \nu) = \begin{cases} (j, \sigma_j(\nu)), & \text{if } j < r/2 \quad \text{and} \quad 1 \leqslant \nu \leqslant s_j \\ (r - j, \sigma_{r-j}(\nu)), & \text{if } j \geqslant r/2 \quad \text{and} \quad 1 \leqslant \nu \leqslant s_j. \end{cases}$$

The proof will be finished if we show that with $\sigma_\ell = \tau_\ell$ for $\ell = 0, \dots, r$ we have

$$D_{\tau(j,\nu)} \in F \tag{8}$$

and

$$D_{j,v} \in A\left(\overline{D_{\tau(j,\nu)}}\right). \tag{9}$$

To prove this we shall treat the cases given above separately:

(i) $j < r/2$ and $1 \leqslant \nu \leqslant s_j$: If $j < r/2$ then $j < r - j$. The definition of τ_j gives that

$$D_{\tau(j,\nu)} = p^{jv} d_{\tau_j(\nu)}.$$

Since the power of p in both, $D_{j,\nu}$ and $D_{\tau(j,\nu)}$ is the same, $D_{j,\nu}$, as well as $D_{\tau(j,\nu)}$ belong to the same F_j. On the other hand

$$\overline{D_{\tau(j,\nu)}} = \frac{N}{D_{\tau(j,\nu)}} = \frac{N}{p^{jv}.d_{\tau_j(\nu)}} = p^{(a-j)v}.\widehat{d_{\tau_j(\nu)}}.$$

Here we have, $j < r - j \leqslant a - j$, which implies $p^{jv} \in A(p^{(a-j)v})$. This together with (6) implies (9), as required.

(ii) $j \geqslant r/2$ and $1 \leqslant \nu \leqslant s_j$: In this case $j \geqslant r - j$ and thus $s_j \leqslant s_{r-j}$, and

$$D_{\tau(j,\nu)} = p^{(r-j)v} d_{\tau_{r-j}(\nu)}.$$

Since $F'_j \subset F'_{r-j}$, the above description of the structure of F''s implies that τ_{r-j} can be contracted to F'_j, and consequently $D_{\tau(j,\nu)} \in F'_{r-j}$. Moreover (6) remains true. Further,

$$\overline{D_{\tau(j,\nu)}} = \frac{N}{D_{\tau(j,\nu)}} = \frac{N}{p^{(r-j)v}.d_{\tau_{r-j}(\nu)}} = p^{(a-r+j)v}.\widehat{d_{\tau_{r-j}(\nu)}}.$$

Now, $a-r+j \geqslant j$, and thus $p^{jv} \in A(p^{(a-r+j)v})$, and the proof is finished. □

If N is a square–free number then the result of Corollary 1 extends the following result on sets of subsets (the reader is referred for more details in this connection to [ErSc1996]):

Corollary 2. *Let A and M be sets, $A \subset M$. Denote $\overline{A} = M \setminus A$. If $F = \{A_1, A_2, \ldots, A_s\}$ is a family of subsets of M satisfying*

$$X \subset A_i \Rightarrow X \in F \qquad (i = 1, 2, \ldots, s),$$

then there exists a permutation σ of $\{1, 2, \ldots, s\}$ such that

$$\overline{A}_{\sigma(i)} \supset A_i \qquad (i = 1, 2, \ldots, s).$$

References

[ErSc1996] P. Erdős, J. Schönheim, *Sets versus divisors*, In: *Combinatorics, Paul Erdős is Eighty*, Vol. 2; Bolayi Society Mathematical Studies, 2 (Keszthely, 1993), Budapest (1996), 193–212.

[HeSc1972] H. Herzog, J. Schönheim, *On certain sets of divisors of a number*, Discrete Math., **1** (1972), 329–332.

[Knop75] J. Knopfmacher, *Abstract Analytic Number Theory*, North-Holland Mathematical Library, Vol.12, North-Holland & American Elsevier, Amsterdam–Oxford–New York 1975; corr. and enlarged ed. Dover Publications, Inc., New York (1990).

[Nark1963] W. Narkiewicz, *On a class of arithmetical convolutions*, Coll. Math., **10** (1963), 81–94.

[Rama1978] V.S. Ramaiah, *Arithmetical sums in regular convolutions*, J. reine angew. Math., **303/304** (1978), 265–283.

Department of Mathematics
Institute of Chemical Technology
Technická 5
166–28 Prague 6
Czech Republic

e-mail:
porubsks@vscht.cz