DEMONSTRATIO MATHEMATICA
Vol. XIV No 1 1981

Wiesław A. Dudek

ON THE DIVISIBILITY THEORY IN (m, n)-RINGS

1. Introduction

In some papers several authors generalize the study of ordinary rings to the case where the ring operations are respectively m-ary and n-ary. The existence of such theories has motivated us to extend the divisibility theory in ordinary rings to the case (m,n)-rings.

For self-containment we give some definitions and results which will be used in the sequel. A detailed investigation may be found in the papers mentioned in the references. We shall use terminology and notations of [8], [9] and [5].

A non-empty set R is called an (m,n)-ring if the following conditions are satisfied:

(i) There exists an m-ary operation g, called the addition, such that $\langle R,g\rangle$ is a commutative m-group.

(ii) There exists an n-ary operation f, called the multiplication, such that $\langle R,f\rangle$ is an n-semigroup.

(iii) The operation f is distributive with respect to g, i.e.

$$f\left(x_1^{i-1},g\left(y_1^m\right),x_{i+1}^n\right) = g\left(\left\{f\left(x_1^{i-1},y_j,x_{i+1}^n\right)\right\}_{j=1}^m\right) \tag{1}$$

for all $i=1,2,\ldots,n$ and $x_1,\ldots,x_n,y_1,\ldots,y_m \in R$.

This paper and [9] make basic part of the paper which was awarded the prize in J.Marcinkiewicz competition for the best student's work in the academic year 1976/77.

An ordinary ring is a special case of an (m,n)-ring, namely for m=n=2.

The concept of (m,n)-rings was introduced by Čupona [7] and, in a special case, by Boccioni [1]. The more general concept is introduced by Celakoski in [3]. In [6] is generalized the method of constructing quotientrings to the case of (m,n)--rings. The paper [5] is concerned with homomorphism theorems and some idealtheoretic aspects. I described (see [10]) a special class of n-groups $\langle G,f\rangle$ which are (n,n)-rings over itself i.e. $\langle G,f,f\rangle$ are (n,n)-rings. For n=2 this class is trivial.

A zero of $\mathcal{R}$ (if it exists) is an element $z \in R$, such that $f\left(z,x_2^n\right) = f\left(x_2,z,x_3^n\right) = \ldots = f\left(x_2^n,z\right) = z$. If a zero exists, it is unique and it is denoted by θ. R^* denotes the set $R \setminus \{\theta\}$ if θ exists and R otherwise. A neutral element of $\langle R,f\rangle$ is called an identity of $\mathcal{R}$ and it is denoted by e. For $n > 2$ there exists a commutative (n,n)-ring which every element is an identity in this (n,n)-ring [10]. Moreover, there exists an (m,n)-ring without any zero and any identity. For example: a two-elements non-idempotent 3-group considered as a (3,3)-ring has not a zero and an identity (see also §2.3 in [5]).

An element $x \in R$ is called an additive or multiplicative idempotent, if x is an idempotent in $\langle R,g\rangle$ or $\langle R,f\rangle$ respectively. Since the addition is commutative, an additive idempotent is a neutral element for this operation. It is easily verified that if $a_1,\ldots,a_m$, $b \in R$ are additive idempotents, then $g\left(a_1^m\right)$ and $f\left(x_1^{i-1},b,x_{i+1}^n\right)$ are additive idempotents for all $x_1,\ldots,x_n \in R$ and $i=1,2,\ldots,n$. Hence, if $\mathcal{R}$ has only one additive idempotent, this idempotent is a zero of $\mathcal{R}$.

A non-empty subset G of an m-group $\langle R,g\rangle$ is called an m-subgroup of $\langle R,g\rangle$, if it is closed under the operation g and if $x \in G$, then also $\bar{x} \in G$. An m-subgroup $\langle G,g\rangle$ of $\langle R,g\rangle$ is called an ideal of $\langle R,g,f\rangle$, if $f\left(x_1^{i-1},a,x_{i+1}^n\right) \in G$ for all $a \in G$, $x_1,\ldots,x_n \in R$ and $i=1,2,\ldots,n$.

In the sequel by $g(A_1,\dots,A_m)$, where $A_1,\dots,A_m$ are ideals of $\mathfrak{R}$, we mean the set $\left\{g\left(a_1^m\right) : a_i \in A_i\right\}$. The symbol $f(B_1,\dots,B_n)$, where $B_1,\dots,B_n$ are non-empty subsets of R, will denote the set

$$(2) \qquad \left\{g_{(k)}\left(\left\{f\left(a_{i1}^{in}\right)\right\}_{i=1}^{k(m-1)+1}\right) : a_{ij} \in B_j\right\}.$$

The next proposition is very usefull for us in the sequel

P r o p o s i t i o n 1.1. (see [5]). Let $\mathfrak{R}$ be an (m,n)-ring.

(i) $\overline{f\left(x_1^n\right)} = f\left(x_1^{i-1},\bar{x}_i,x_{i+1}^n\right)$ for all $x_1,\dots,x_n \in R$ and $i=1,2,\dots,n$.

(ii) The intersection an arbitrary number of ideals of $\mathfrak{R}$ is also an ideal of $\mathfrak{R}$,

(iii) $g(A_1,\dots,A_m)$ is an ideal of $\mathfrak{R}$, if $A_1,\dots,A_m$ are ideals of $\mathfrak{R}$.

(iv) If $\mathfrak{R}$ is commutative and some B_i is an ideal of $\mathfrak{R}$, then $f(B_1,\dots,B_n)$ is an ideal, too.

For a non-empty subset A of an (m,n)-ring $\mathfrak{R}$, we define:

$$\bar{A} = \left\{\bar{x} \in R : x \in A\right\},$$

$$\tilde{A} = \left\{x \in R : \tilde{x} \in A\right\}.$$

The following proposition is very easy and we omit the proof.

P r o p o s i t i o n 1.2. Let $\mathfrak{R}$ be an (m,n)-ring.

(i) If A is a m-subgroup of $<R,g>$, then $\bar{A} \subset A$.

(ii) If there exists a natural number k such that $x = \overline{\{x\}}^k$ for all elements of an m-subgroup $\bar{A}$, then $\bar{A} = A$.

(iii) A is an ideal of $\mathfrak{R}$ if and only if, $\bar{A}$ is an ideal.

(iv) If A is an ideal, then $\tilde{A}$ is an ideal, too.

Direct computation show that

P r o p o s i t i o n 1.3. If $\bar{A}$ is a 3-subgroup of a 3-group, then $\bar{A} = A$.

By an i-center of $\mathfrak{R}$ we mean the set

$$(3)\quad C_i(\mathfrak{R}) = \left\{a \in R:\ f\left(a,x_2^n\right) = f\left(x_2^i,a,x_{i+1}^n\right) \text{ for } x_2,\ldots,x_n \in R\right\}.$$

The set $C(\mathfrak{R}) = \bigcap_{i=1}^{n} C_i(\mathfrak{R})$ is called the center of an (m,n)--ring $\mathfrak{R}$. Obviously $C_1(\mathfrak{R}) = R$ for all (m,n)-rings. Moreover, there exists (m,n)-rings such that an i-center is empty for some i=2,3,...,n. Indeed, it is easily verified that if $\langle R,g\rangle$ is an idempotent commutative m-group (m>2) and e_k is an n-ary projection (i.e. $e_k\left(x_1^n\right) = x_k$), then $\mathfrak{R}_k = \langle R,g,e_k\rangle$ is an (m,n)-ring for k=1 and k=n. Obviously, the set $C_i(\mathfrak{R}_k)$ is empty for all i=k.

P r o p o s i t i o n 1.4. If $C_i(\mathfrak{R})$ is non-empty, then it is an (m,n)-subring of $\mathfrak{R}$.

P r o o f . Let $a_1,\ldots,a_m \in C_i(\mathfrak{R})$, then for all $x_2,\ldots,x_n \in R$, we have $f\left(x_2^i,g\left(a_1^m\right),x_{i+1}^n\right) = g\left(\left\{f\left(x_2^i,a_j,x_{i+1}^n\right)\right\}_{j=1}^m\right) = g\left(\left\{f\left(a_j,x_2^n\right)\right\}_{j=1}^m\right) = f\left(g\left(a_1^m\right),x_2^n\right)$ by distributivity. This implies that $g\left(a_1^m\right) \in C_i(\mathfrak{R})$.

Now, if $a \in C_i(\mathfrak{R})$, then $f\left(x_2^i,\bar{a},x_{i+1}^n\right) = f\left(\bar{x}_2,x_3^i,a,x_{i+1}^n\right) = f\left(a,\bar{x}_2,x_3^n\right) = f\left(\bar{a},x_2^n\right)$ by Prop.1.1. Hence $a \in C_i(\mathfrak{R})$, i.e. $C_i(\mathfrak{R})$ is an m-subgroup of $\langle R,g\rangle$.

If $a_1,\ldots,a_n \in C_i(\mathfrak{R})$, then we obtain

$$f\left(x_2^i,f\left(a_1^n\right),x_{i+1}^n\right) = f\left(f\left(x_2^i,a_1^{n-i+1}\right),a_{n-i+2}^n,x_{i+1}^n\right) =$$
$$= f\left(f\left(a_1,x_2^i,a_2^{n-i+1}\right),a_{n-i+2}^n,x_{i+1}^n\right) = f\left(a_1,f\left(x_2^i,a_2^{n-i+2}\right),a_{n-i+3}^n,x_{i+1}^n\right) =$$
$$= f\left(a_1,f\left(a_2,x_2^i,a_3^{n-i+2}\right),a_{n-i+3}^n,x_{i+1}^n\right) = f\left(a_1^2,f\left(x_2^i,a_3^{n-i+3}\right),a_{n-i+4}^n,x_{i+1}^n\right) =$$
$$= \ldots = f\left(f\left(a_1^n\right),x_2^n\right)$$

for all $x_2,\dots,x_n \in R$. Hence $f\left(a_1^n\right) \in C_i(\mathcal{R})$, which completes the proof.

P r o p o s i t i o n 1.5. If $C(\mathcal{R})$ is non-empty, then it is a maximal commutative (m,n)-subring of $\mathcal{R}$.

C o r o l l a r y 1.6. An (m,n)-ring $\mathcal{R}$ is commutative if and only if, $C(\mathcal{R}) = R$.

It is well known that the group S_n is generated by cycles $(1,2)$ and $(1,2,\dots,n)$. Hence

C o r o l l a r y 1.7. An (m,n)-ring $\mathcal{R}$ is commutative if and only if, $C_2(\mathcal{R}) = C_n(\mathcal{R}) = R$.

P r o p o s i t i o n 1.8. An (m,n)-sfield $\mathcal{R}$ is commutative if and only if, $C_i(\mathcal{R}) = R$ for some $i=2,\dots,n$.

P r o o f. Ar (m,n)-ring $\mathcal{R}$ is an (m,n)-sfield, if $\langle R,f\rangle$ is an n-group. Let $\hat{x}$ be a skew element (under f) to x. Since $C_i(\mathcal{R}) = R$, we have $a = f\left(a,\hat{x},\overset{(n-2)}{x}\right) = f\left(x,a,\hat{x},\overset{(n-3)}{x}\right)$ for all $a,x \in R$. Applying Corollary 9 in [8], we infer that $\mathcal{R}$ is commutative.

Observe that the standard i-center of an n-semigroup $\langle R,f\rangle$, i.e. the set

$$(4)\quad Z_i(\mathcal{R}) = \left\{a \in R : f\left(a,x_2^n\right) = f\left(x_i,x_2^{i-1},a,x_{i+1}^n\right) \text{ for } x_2,\dots,x_n \in R\right\}$$

is an m-subgroup of $\langle R,g\rangle$. In general, it is not an (m,n)-subring of $\mathcal{R}$. Indeed, if $\mathcal{R}$ is a non-commutative $(m,4)$-ring, then we have $f\left(x_1^2,f\left(a_1^4\right),x_4\right) = f\left(f\left(a_1^4\right),x_1^2,x_4\right)$ for all $a_1,\dots,a_4 \in Z_3(\mathcal{R})$ and $x_1,x_2,x_4 \in R$. Hence, in general, it is not true that $f\left(a_1^4\right) \in Z_3(\mathcal{R})$.

An (m,n)-ring $\mathcal{R}$ is called cancellative, if an n-semigroup $\langle R,f\rangle$ is cancellative [9]. A cancellative (m,n)-ring has not zero-divisors [6]. I proved in [10] that a cancellative (m,n)-ring $\mathcal{R}$ has not additive idempotents, or only zero (if it exists) is an additive idempotent, or $\langle R,g\rangle$ is an idempotent m-group.

2. (m,n)-domains

A commutative and cancellative (m,n)-ring $\mathfrak{R}$ is called an (m,n)-domain, if for all $y \in R$ there exist $x_2,\dots,x_n \in R$ such that $y = f\left(y,x_2^n\right)$. In other words, an (m,n)-ring $\mathfrak{R}$ is an (m,n)-domain, if $\langle R,f\rangle$ is an n-domain [9].

Let x and y be elements of $\mathfrak{R}$. We say that x divides y if and only if, x divides y in $\langle R,f\rangle$, i.e. if there exist $x_2,\dots,x_n \in R$ such that $y = f\left(x,x_2^n\right)$.

P r o p o s i t i o n 2.1. Let $\mathfrak{R}$ be an (m,n)-domain and let $a,b \in R$.

(i) $a \mid \bar{a}\}^k$ for all natural k.

(ii) If $\bar{a} \mid b$, then $a \mid b$.

(iii) If $a \mid b$, then $\bar{a} \mid \bar{b}$.

(iv) If $\bar{a} \mid \bar{b}$, then $a \mid \bar{b}$.

(v) If $a \mid b_i$ for $i=1,\dots,m$, then $a \mid g\left(b_1^m\right)$.

P r o o f . From Proposition 1.1 immediately follows (i)-(iv). The condition (1) implies (v).

Notice that the inverse implications are not true. For example: if $\mathfrak{R}$ is an (5,3)-ring derived from Galois field GF(3), then we put $a = \bar{a} = \bar{b} = \bar{c}$, where a is a zero of GF(3). It is easily verified that $a \mid \bar{b}$ but $\bar{a} \nmid b$, $\bar{a} \mid \bar{b}$ but $a \nmid b$, etc.

As in the binary case, we can prove

P r o p o s i t i o n 2.2. Let $\mathfrak{R}$ be an (2,n)-domain. If there exist $GCD\{a,b\}$ and $GCD\{a,a+b\}$, then they are equal.

Observe that if $\mathfrak{R}$ is an (m+1,n)-ring of integers numbers, then $GCD\{m,\underbrace{1,\dots,1}_{m}\} = [1]$ but $GCD\{m,\underbrace{m+1+\dots+1}_{m}\} = GCD\{m,2m\} = [m]$. Hence, in general, it is not true that $GCD\{a_1,\dots,a_m\} = GCD\{a_1,g(a_1^m)\}$ for $m \geqslant 2$.

From Proposition 2.1 and Proposition 1.2, we obtain

P r o p o s i t i o n 2.3. The set $A = \{x \in R: a \mid x\}$ is an ideal of an (m,n)-domain $\mathfrak{R}$ for every $a \in R$. Moreover, $\bar{A} = \{\bar{x} \in R: a \mid x\}$ and $\tilde{A} = \{x \in R: a \mid \bar{x}\}$ are ideals, too.

The ideal generated by an element $a \in R$ is called a principal ideal and is denoted by $\langle a \rangle$. Observe that an ideal B is a principal ideal generated by b if and only if $B = \{x \in R: b|x\}$. Obviously $\langle b \rangle = R$ if and only if $b \in D_R$.

P r o p o s i t i o n 2.4. If $a,b \in R$, where $\mathfrak{R}$ is an (m,n)-domain, then

(i) $a|b$ if and only if $\langle b \rangle \subset \langle a \rangle$.

(ii) $a \sim b$ if and only if $\langle b \rangle = \langle a \rangle$.

(iii) $\overline{\langle a \rangle} = \langle \bar{a} \rangle \subset \langle a \rangle$.

(iv) If $a = g(a_1^m)$, then $\langle a \rangle \subset g\left(\langle a_1 \rangle, \ldots, \langle a_m \rangle\right)$.

(v) If b is an additive idempotent, then $\langle b \rangle$ is an additive idempotent ideal.

(vi) $f\left(\langle a_1 \rangle, \ldots, \langle a_n \rangle\right) = \langle f(a_1^n) \rangle$.

P r o o f . If $b \in \langle a \rangle = \langle g(a_1^m) \rangle$, then $b = f\left(g(a_1^m), x_2^n\right) = g\left(\left\{f\left(a_i, x_2^n\right)\right\}_{i=1}^m\right)$. Hence (iv). On the other hand, if $b \in g\left(\langle a \rangle, \ldots, \langle a \rangle\right)$ and a is an idempotent, then $b = g\left(\left\{f\left(a, x_{i2}^{in}\right)\right\}_{i=1}^m\right) = g\left(\left\{f\left(a, t_2^{n-1}, z_i\right)\right\}_{i=1}^m\right) = f\left(a, t_2^{n-1}, g(z_1^m)\right) \in \langle a \rangle$, where $t_i \in D_a$ and $z_i = f\left(t_n, x_{i2}^{in}\right)$. This implies (v). The condition (vi) follows from (1) and Proposition 1.1.

C o r o l l a r y 2.5. If $\mathfrak{R}$ is an (m,n)-domain such that $a = \bar{a}^{\}k}$ for all $a \in R$ and some fixed k (in particular, if $\mathfrak{R}$ is a $(3,n)$-domain), then $\langle a \rangle = \langle \bar{a} \rangle$.

An ideal B is called prime, if $f(a_1^n) \in B$ implies that $a_i \in B$ for some $i=1,2,\ldots,n$. A principal ideal of $\mathfrak{R}$ is called a maximal principal ideal, if it is maximal (with respect to inclusion) in the set of proper principal ideals of $\mathfrak{R}$.

P r o p o s i t i o n 2.6. Let $\mathfrak{R}$ be an (m,n)-domain and let $b \in R^*$.

(i) b is an invertible element of $\mathfrak{R}$ if and only if $\langle b \rangle = R$.

(ii) b is irreducible if and only if $\langle b\rangle$ is a maximal principal ideal.

(iii) b is prime if and only if the proper ideal $\langle b\rangle$ is prime.

P r o o f . As an example we prove (iii). If b is prime and $f(a_1^n) \in \langle b\rangle$, then $b \mid f(a_1^n)$. Since b is prime, $b \mid a_i$ for some i. Hence $a_i \in \langle b\rangle$, i.e. $\langle b\rangle$ is a prime ideal of $\mathcal{R}$.

Now, let $\langle b\rangle$ be a prime ideal and let $b \mid f(a_1^n)$. Then $f(a_1^n) \in \langle b\rangle$. This means that $a_i \in \langle b\rangle$ for some i. Therefore $b \mid a_i$ and b is prime.

P r o p o s i t i o n 2.7. Let $\mathcal{R}$ be an (m,n)-domain. If $a_1,\dots,a_p \in R^*$ and $g_{(k)}\left(\langle a_1\rangle,\dots,\langle a_p\rangle\right) = \langle d\rangle$, where $p = k(m-1)+1$, then $GCD\{a_1,\dots,a_p\}_p = [d]$.

P r o o f . From Proposition 1.1, $\bigcap_{i=1}^{p} \langle a_i\rangle$ is an ideal of $\mathcal{R}$. If $c \in \bigcap_{i=1}^{p} \langle a_i\rangle$, then $\bar{c}$, too. Hence, by commutativity, we have

$$a_j = g_{(k)}\left(\bar{c}, \overset{(j-2)}{c}, a_j, \overset{(n-j)}{c}, \bar{c}, \overset{(n-2)}{c}, \bar{c}, \overset{(n-2)}{c}, \dots, \bar{c}, \overset{(n-2)}{c}\right),$$

i.e. $a_j \in g_{(k)}\left(\langle a_1\rangle,\dots,\langle a_p\rangle\right)$ for all $j=1,2,\dots,p$. Therefore $d \mid a_j$ for every a_j. If there exists $b \in R$ such that $b \mid a_i$, then $a_i = f\left(b, z_{i2}^{in}\right)$ and $d = g_{(k)}\left(\left\{f_{(2)}\left(b, z_{i2}^{in}, x_{i2}^{in}\right)\right\}_{i=1}^{p}\right) = g_{(k)}\left(\left\{f\left(b, t_2^{n-1}, u_i\right)\right\}_{i=1}^{p}\right) = f\left(b, t_2^{n-1}, g_{(k)}\left(u_1^p\right)\right)$, where $t_i \in E_a$, $u_j = f_{(2)}\left(t_n, z_{i2}^{in}, x_{i2}^{in}\right)$. This implies that $GCD\{a_1,\dots,a_p\} = [d]$.

P r o p o s i t i o n 2.8. Let $\mathcal{R}$ be an (m,n)-domain. If $a_1,\dots,a_p \in R^*$, then $LCM\{a_1,\dots,a_p\} = [d]$ if and only if $\bigcap_{i=1}^{p} \langle a_i\rangle = \langle d\rangle$.

P r o o f . If $[d] = LCM\{a_1,\dots,a_p\}$, then $d \in \bigcap_{i=1}^{p} \langle a_i\rangle$. Hence $\langle d\rangle \subset \bigcap_{i=1}^{p} \langle a_i\rangle$. On the other hand, any element

$c \in \bigcap_{i=1}^{p} \langle a_i \rangle$ is a common multiple of each of the a_i. But $[d] = \mathrm{LCM}\{a_1,\ldots,a_p\}$, so that $d \mid c$. This means that $c \in \langle d \rangle$, i.e. $\bigcap_{i=1}^{p} \langle a_i \rangle \subset \langle d \rangle$. Therefore $\bigcap_{i=1}^{p} \langle a_i \rangle = \langle d \rangle$.

Conversely, if $\langle d \rangle = \bigcap_{i=1}^{p} \langle a_i \rangle$, then for all $i=1,2,\ldots,p$ we have $c = f\left(a_i, x_{i2}^{in}\right)$. If there exists $b \in R$ such that $a_i \mid b$ for every i, then $b \in \bigcap_{i=1}^{p} \langle a_i \rangle = \langle d \rangle$ i.e. $[d] = \mathrm{LCM}\{a_1,\ldots,a_p\}$.

An (m,n)-domain $\mathfrak{R}$ is called a principal ideal (m,n)-domain, if every ideal of $\mathfrak{R}$ is a principal ideal.

P r o p o s i t i o n 2.9. Let $\mathfrak{R}$ be a principal ideal (m,n)-domain and let $a_1,\ldots,a_p \in R^*$, where $p = k(m-1)+1$. Then $\mathrm{GCD}\{a_1,\ldots,a_p\} = [d]$ if and only if, $g_{(k)}\left(\langle a_1 \rangle, \langle a_2 \rangle, \ldots, \langle a_p \rangle\right) = \langle d \rangle$.

P r o o f . If $\langle b \rangle = g_{(k)}\left(\langle a_1 \rangle, \langle a_2 \rangle, \ldots, \langle a_p \rangle\right)$, then $[b] = \mathrm{GCD}\{a_1,\ldots,a_p\}$, from Proposition 2.7. Hence $b \sim d$ and $\langle b \rangle = \langle d \rangle$.

As in the binary case (see e.g. [2] Theorem 6-9), we prove:

P r o p o s i t i o n 2.10. If $B_1 \subset B_2 \subset B_3 \subset \ldots$ is any infinite sequence of ideals of a principal ideal (m,n)-domain $\mathfrak{R}$, then there exists an integer p such that $B_p = B_s$ for all $s \geqslant p$.

C o r o l l a r y 2.11. If $a_1,a_2,a_3,\ldots$ is any infinite sequence of elements of a principal ideal (m,n)-domain and $a_{i+1} \mid a_i$ for all i, then $a_p \sim a_s$ for some p and all $s \geqslant p$.

An (m,n)-domain $\mathfrak{R}$ is a factorization (unique factorization) (m,n)-domain, if $\langle R,f \rangle$ is a factorization (unique factorization) n-domain. Therefore Proposition 4.8 from [9] implies that an (m,n)-domain is a unique factorization (m,n)-domain if and only if, $\mathfrak{R}$ is a factorization (m,n)-domain and each irreducible element is prime.

P r o p o s i t i o n 2.12. Each principal ideal (m,n)-domain is a unique factorization (m,n)-domain.

P r o o f . First we prove that a principal ideal (m,n)-domain $\mathcal{R}$ is a factorization (m,n)-domain. Observe that for every $a \in R^* \setminus D_R$ there exists $d \in R$ such that $d|a$ and d is an irreducible element. Indeed, if a is irreducible, then $d = a$. On the other hand, if a has a factorization

$$a = f_{(t)}\left(a_1,\dots,a_k,b_{k+1},\dots,b_{t(n-1)+1}\right), \tag{5}$$

where $k \geqslant 2$, $b_i \in D_R$ and $a_j \in R^* \setminus D_R$, then some a_j is irreducible. If any a_j is not irreducible, then every a_j has a factorization. Let a_1 has a factorization

$$a_1 = f_{(t_1)}\left(a_1^{(1)},\dots,a_{k_1}^{(1)},b_{k_1+1}^{(1)},\dots,b_{t_1(n-1)+1}^{(1)}\right),$$

where $a_i^{(1)} \in R^* \setminus D_R$, $b_j^{(1)} \in D_R$ and $k_j \geqslant 2$. If any $a_i^{(1)}$ is not irreducible, then we have

$$a_1^{(1)} = f_{(t_1')}\left(a_1^{(2)},\dots,a_{k_2}^{(2)},b_{k_2+1}^{(2)},\dots,b_{t_1'(n-1)+1}^{(2)}\right).$$

Continuing this argument, we arrive (after p steps) at some $a_i^{(p)}$. Indeed, if all $a_i^{(p)}$ can be factored into a finite product of irreducible elements, then we have an infinite sequence of elements $a_1^{(0)} = a_1, a_1^{(1)}, a_1^{(2)}, \dots$ such that $a_1^{(s)} \mid a_1^{(s-1)}$ for all natural s. Corollary 2.11 shows that there exists an integer k such that $a_1^{(k)} \sim a_1^{(p)}$ for all $p \geqslant k$. Hence $a_1^{(k)} = f\left(a_1^{(k+1)},x_2,\dots,x_n\right)$ for some $x_2,\dots,x_n \in D_R$ (see Proposition 2.7 in [9]). Therefore

$$a_1^{(k)} = f\left(a_1^{(k+1)},x_2,\dots,x_2,z\right) =$$
$$= f_{(p)}\left(a_1^{(k+1)},\dots,a_s^{(k+1)},b_{s+1}^{(k+1)},\dots,b_{p(n-1)+1}^{(k+1)}\right) =$$
$$= f\left(a_1^{(k+1)},x_2,\dots,x_2,u\right),$$

where $a_i^{(k+1)} \in R^* \setminus D_R$, $z,u,x_i,b_j^{(k+1)} \in D_R$ and

$$u = f_{(p)}\left(a_2^{(k+1)},a_3^{(k+1)},\dots,a_s^{(k+1)},b_{s+1}^{(k+1)},\dots,b_{p(n-1)+1}^{(k+1)},y\right).$$

The cancellative law implies that $u = z$, i.e. $a_2^{(k+1)},\dots,a_s^{(k+1)} \in D_R$, which is impossible. Hence every $a \in R^* \setminus D_R$ has an irreducible divisor.

In the same manner we prove that every a_i from (5) has an irreducible divisor c_i, i.e. $a_i = f\left(c_i,x_2^{(i)},x_3^{(i)},\dots,x_n^{(i)}\right)$. Therefore

$$(6) \qquad a = f_{(t)}\left(c_1,c_2,\dots,c_k,z,b_{k+1},b_{k+2},\dots,b_{t(n-1)}\right),$$

where

$$(7) \qquad z = f_{(k)}\left(x_2^{(1)},x_3^{(1)},\dots,x_n^{(1)},\dots,x_2^{(k)},\dots,x_n^{(k)},b_{t(n-1)+1}\right).$$

If $z \in D_R$, then a has a factorization (6). If $z \notin D_R$, then using above procedure we may prove that z has a factorization into a finite product of irreducible elements. Hence every $a \in R^* \setminus D_R$ has a factorization, i.e. $\mathfrak{R}$ is a factorization (m,n)-domain.

Now, we prove that every irreducible element d is prime. Let $d \mid f\, a_1^n$. In view of commutativity, there is no loss of generality, if we assume that $d \mid a_i$ for $i=2,3,\dots,n$. Hence $GCD\{d,a_i\} = D_R$ for all $i=2,3,\dots,n$. Since $\mathfrak{R}$ is a (m,n)-do-

main, then $a_1 = f\left(a_1, t_2^n\right)$ for some $t_2, t_3, \ldots, t_n \in D_R$. On the other hand (see Proposition 2.9), there exists $x_{jk}^{(i)} \in R$ such that

$$t_i = g\Big(f\big(a_i, x_{12}^{(i)}, \ldots, x_{1n}^{(i)}\big), f\big(d, x_{22}^{(i)}, \ldots, x_{2n}^{(i)}\big), \ldots, f\big(d, x_{m2}^{(i)}, \ldots, x_{mn}^{(i)}\big)\Big) .$$

The distributive law and direct computation show that

$$\begin{aligned} a_1 &= f(a_1, t_2, t_3, \ldots, t_n) = \\ &= f\Big(a_1, g\Big(f\big(a_2, x_{12}^{(2)}, \ldots, x_{1n}^{(2)}\big), f\big(d, x_{22}^{(2)}, \ldots, x_{2n}^{(2)}\big), \ldots, f\big(d, x_{m2}^{(2)}, \ldots, x_{mn}^{(2)}\big)\Big), \\ &\quad g\Big(f\big(a_3, x_{12}^{(3)}, \ldots, x_{1n}^{(3)}\big), f\big(d, x_{22}^{(3)}, \ldots, x_{2n}^{(3)}\big), \ldots, f\big(d, x_{m2}^{(3)}, \ldots, x_{mn}^{(3)}\big)\Big), \\ &\quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\quad g\Big(f\big(a_n, x_{12}^{(n)}, \ldots, x_{1n}^{(n)}\big), f\big(d, x_{22}^{(n)}, \ldots, x_{2n}^{(n)}\big), \ldots, f\big(d, x_{m2}^{(n)}, \ldots, x_{mn}^{(n)}\big)\Big)\Big) = \\ &= g\Big(f\big(f\big(a_1^n\big), z_{12}^{1n}\big), f\big(d, z_{22}^{2n}\big), \ldots, f\big(d, z_{m2}^{mn}\big)\Big) \end{aligned}$$

for some $z_{ij} \in R^*$.

Since $d \mid f\left(a_1^n\right)$ and $d \mid f\left(d, x_{i2}^{in}\right)$, we have $d \mid a_1$. Hence d is prime, which completes our proof.

3. Final remarks

An (m,n)-domain $\mathcal{R}_0$ with θ is called Euclidean, if there exists a function δ (the Euclidean valuation) such that the following conditions are satisfied:

(i) $\delta(x)$ is a positive integral number for every $x \in R_0$,

(ii) $\delta(x) = 0$ if and only if $a = \theta$,

(iii) $\delta\left(f\left(x_1^n\right)\right) = \delta(x_1)\cdot\delta(x_2)\cdot\ldots\cdot\delta(x_n)$ for all $x_1, x_2, \ldots, x_n$, $y \in R_0$ such that $a = g\left(f\left(b, x_2^n\right), y, \theta, \ldots, \theta\right)$, where either $y = \theta$ or $\delta(y) < \delta(b)$.

It is clear that $\delta(x) = 1$ if and only if, $x \in D_{R_0}$. Moreover, if two elements $a,b \in R_0$ are associates, then $\delta(a) = \delta(b)$.

P r o p o s i t i o n 3.1. Every Euclidean (m,n)-domain is a principal ideal (m,n)-domain. Moreover, it is a unique factorization (m,n)-domain.

The proof is standard.

Let $\mathfrak{R}_0$ be a Euclidean (m,n)-domain with valuation δ. From (iv) for any $a \in R_0$ and $b \in R_0^*$ we have $a = g\left(f\left(b,x_2^n\right),y,\theta,\ldots,\theta\right)$ for some $x_2,\ldots,x_n,y \in R_0$. If $y = \theta$, then $b|a$. If $y \neq \theta$, then $\delta(y) < \delta(b)$ and there exists $z_2,z_3,\ldots,z_n,y_1 \in R_0$ such that $b = g\left(f\left(y,z_2^n\right),y_1,\theta,\ldots,\theta\right)$. As in a binary case we can prove that the final nonzero remainder of this n-ary Division Algorithm is a greast common divisor of a and b.

A very important role in the theory of (m,n)-rings is played by $(m,2)$-rings. We give several particular interesting properties of $(m,2)$-rings. In general, these properties are not true for (m,n)-rings, if $n > 2$.

P r o p o s i t i o n 3.2. Let $a_1,\ldots,a_p,b_p \in R^*$, where $\mathfrak{R}$ is an $(m,2)$-domain and $a_1b_1 = a_2b_2 = \ldots = a_pb_p = d$.

(i) If $\mathrm{LCM}\{a_1,\ldots,a_p\}$ exists, then $\mathrm{GCD}\{b_1,\ldots,b_p\}$ also exists and $\mathrm{LCM}\{a_1,\ldots,a_p\}\cdot\mathrm{GCD}\{b_1,\ldots,b_p\} = [d]$.

(ii) If $\mathrm{GCD}\{ra_1,\ldots,ra_p\}$ exists for all $r \in R^*$, then $\mathrm{LCM}\{b_1,\ldots,b_p\}$ also exists and we have $\mathrm{GCD}\{a_1,\ldots,a_p\}\cdot\mathrm{LCM}\{b_1,\ldots,b_p\} = [d]$.

(iii) $\mathrm{LCM}\{a_1,\ldots,a_p\}$ exists if and only if $\mathrm{GCD}\{a_1,\ldots,a_p\}$ exists.

(iv) If $\mathfrak{R}$ is a principal ideal $(m,2)$-domain, then every nontrivial ideal of $\mathfrak{R}$ is the product of a finite number of prime ideals.

The proof is analogous to the case of ordinary rings (see [2] p.96-101).

The author wishes to express his sincere thanks to Doctor K.Głazek, who examined the manuscript and suggested many improvements.

REFERENCES

[1] D. B o c c i o n i : Caracterizzatione di una classa di anelli generalizati, Rend. Sem. Mat. Univ. Padova 35 (1965) 116-127.

[2] D.M. B u r t o n : A first course in rings and ideals. Reading, Mass. 1970.

[3] N. C e l a k o s k i : On (F,G)-rings. God.Sb.Mat.Fak. Skopje 28 (1977) 5-15.

[4] G. C r o m b e z : On partially ordered n-groups, Abh. Math. Sem. Univ. Hamburg 38 (1972) 141-146.

[5] G. C r o m b e z : On (n,m)-rings, Abh. Math. Sem. Univ. Hamburg 37 (1972) 180-199.

[6] G. C r o m b e z , J. T i m m : On (n,m)-quotient rings, Abh. Math. Sem. Univ. Hamburg 37 (1972) 200-203.

[7] Г. Чупона : За [m,n]-простените, Билтен ДМФ на СРМ 16 (1965) 5-10.

[8] W.A. D u d e k : Remarks on n-groups, Demonstratio Math. 13 (1980) 165-181.

[9] W.A. D u d e k : On divisibility in n-semigroups, Demonstratio Math. 13 (1980) 355-367.

[10] W.A. D u d e k : Autodistributive n-groups, Comm. Math., Prace Matematyczne, to appear.

[11] W.A. D u d e k , K. G ł a z e k , B. G l e i c h g e w i c h t : A note on the axioms of n-groups, Colloq. Math. Soc. J. Bolyai, (Proceedings of the Conference on Universal Algebra, Esztergom 1977, Hungary).

[12] K. G ł a z e k , B. G l e i c h g e w i c h t : Abelian n-groups, Colloq. Math. Soc. J. Bolyai, Esztergom 1977.

INSTITUTE OF MATHEMATICS, PEDAGOGICAL UNIVERSITY, CZĘSTOCHOWA

Received April 12, 1978.