Otakar Borůvka
Studies on multiplicative systems. Part I

Spisy přír. fak. MU, č. 245, 1937, 15 s.

Persistent URL: http://dml.cz/dmlcz/500052

1

S P I S Y
VYDÁVANÉ
PŘÍRODOVĚDECKOU FAKULTOU
MASARYKOVY UNIVERSITY
REDAKTOR

PUBLICATIONS
DE LA
FACULTÉ DES SCIENCES
DE L'UNIVERSITÉ MASARYK
RÉDIGÉES PAR

ANTONÍN ŠIMEK

ROK 1937 — ČÍS. 245

STUDIES ON MULTIPLICATIVE SYSTEMS.

PART I.

BY

O. BORŮVKA.

VYCHÁZÍ S PODPOROU MINISTERSTVA ŠKOLSTVÍ A NÁRODNÍ OSVĚTY

VLASTNÍM NÁKLADEM VYDÁVÁ
PŘIRODOVĚDECKÁ FAKULTA

NA SKLADĚ MA | EN VENTE CHEZ
KNIHKUPECTVÍ A. PÍŠA, BRNO, ČESKÁ 28

STUDIES ON MULTIPLICATIVE SYSTEMS. PART I.

BY

O. BORŮVKA.

In a series of considerations beginning in this paper I shall try a systematic study of multiplicative systems. The fact that most important mathematical theories deal with multiplicative systems for which additional properties are postulated, as well as the presence of well known unsolved problems concerning multiplicative systems which seem of a profound theoretical character[1]), may prove the fitness of such study.

In this paper an extended class of multiplicative systems, which I call *multiplicative systems without kernel*, is considered. A multiplicative system $\mathfrak{M}$ of this kind is characterised by the property (excluding the groups) that there exists for every element a of $\mathfrak{M}$ a positive integer α so that a is product of α but not more than α elements of $\mathfrak{M}$. The theory of these systems is connected with the theory of homomorphic representations of multiplicative systems on the infinite cyclic multiplicative system which of the multiplicative systems without kernel seems to be the simplest.

I. Introduction.

1. Multiplicative systems. An abstract *multiplicative system* (m. system) is an abstract non-vacuous set for which an abstract *associative* multiplication is defined; i. e. an abstract rule by which to every ordered pair of equal or different elements a, b of the set a single further element ab of the set is associated so that the associative law holds

$$(ab)\,c = a\,(bc). \tag{1}$$

ab is the *product* of a and b; a, b are the *factors* of ab. Therefore, the abstract m. systems generalize the abstract groups so far as the existence of the unity and inverse elements is not explicitly postulated. We usually employ the term m. system instead of abstract m. system.

In the sequel the following notations will be used: m. systems (abstract or realized): German capitals; sets: Latin capitals; the vacuous set: 0; matrices: Greek capitals; elements of sets: small Latin letters; numbers varying within a given number-field: small Greek letters. For fundamental concepts of the theory of sets we employ the usual nota-

[1]) A Malcev, On the Immersion of an Algebraic Ring into a field (*Math. Ann.*, 113, 1937, p. 686).

tions, particularly the symbols $\cap$, $\vee$, $\wedge$ for a product, sum, difference of sets. On the contrary, the symbols $\cdot$, $+$ will be employed for expressing associative multiplications, so that we denote by $a \cdot b$, shorter by ab, or, if desired, $a + b$ the product of a and b. Usually we employ the symbol $\cdot$. A m. system can be realized by choosing for its elements the subsets of an abstract set and by giving the symbol $\cdot$ the meaning of $\cap$ or $\vee$.

2. Let $\mathfrak{M}$ be a m. system. Let $a_1, \dots, a_\gamma \,\mathrm{e}\, \mathfrak{M}$, $\gamma > 1$. For every positive integer $\alpha < \gamma$ we denote by $a_1 \dots a_{\alpha+1}$ the element of $\mathfrak{M}$, which is defined by the recurrence formula

$$a_1 \dots a_{\alpha+1} - (a_1 \dots a_\alpha)\, a_{\alpha+1}.$$

Then we have for $1 < \alpha < \alpha + \beta \leq \gamma$ the following equality

$$(a_1 \dots a_\alpha)\,(a_{\alpha+1} \dots a_{\alpha+\beta}) \quad a_1 \dots a_{\alpha+\beta}. \tag{2}$$

If $\mathfrak{M}$ is commutative, i. e., if $ab - ba$ for $a, b \,\mathrm{e}\, \mathfrak{M}$. the element $a_1 \dots a_\alpha$, $1 < \alpha < \gamma$, does not depend on the order of the factors $a_1, \dots, a_\alpha$ [2]).

3. Let $\mathfrak{M}$ be a m. system. Let $A, B \subset \mathfrak{M}$. By the symbol AB we mean 0 if at least one of the factors is 0; if both are $\neq 0$ we mean by it the set of all such elements $x \,\mathrm{e}\, \mathfrak{M}$, that there exist $a \,\mathrm{e}\, A$, $b \,\mathrm{e}\, B$, $x \quad ab$.

Let $A, B, C \subset \mathfrak{M}$. Then

$\cdot 1$ $(AB)\, C = A\,(BC)$;
$\cdot 2$ $(A \vee B)\, C \quad AC \vee BC$; $\quad C\,(A \vee B) \quad CA \vee CB$.

We leave out the proofs of these formulas as they are easy to be given.

According to $\cdot 1$ a m. system can be realized by taking the subsets of an abstract m. system $\mathfrak{M}$ for its elements and defining the multiplication by the contents of the symbol AB. We say that $\mathfrak{M}$ *induces* this concrete m. system. By $\cdot 2$, the m. system just defined is immerged into a concrete system with double associative composition $\cdot$, $\vee$, for which the distributive laws hold.

4. *Multiplicative subsystems and oversystems.* Let $\mathfrak{M}$ be a m. system. Let $A \subset \mathfrak{M}$, $A \neq 0$. If A has the property that for $a, b \,\mathrm{e}\, A$ we have $ab \,\mathrm{e}\, A$, then A is a *m. subsystem* of $\mathfrak{M}$. If A is a m. subsystem of $\mathfrak{M}$, then it is evidently a m. system and we say that $\mathfrak{M}$ is a *m. oversystem* of A. $\mathfrak{M}$ is a m. subsystem and at the same time a m. oversystem of $\mathfrak{M}$. If $\mathfrak{A}$ is a m. subsystem of $\mathfrak{M}$ and $\mathfrak{A} \neq \mathfrak{M}$, we state this inequality saying that $\mathfrak{A}$ is a *proper m. subsystem* of $\mathfrak{M}$ or that $\mathfrak{M}$ is a *proper m. oversystem* of $\mathfrak{A}$. It is clear that the m. system induced by a m. subsystem of $\mathfrak{M}$ is a m. subsystem of the m. system induced by $\mathfrak{M}$.

---

[2] B. L. van der Waerden, Moderne Algebra, I T., Berlin 1930, p. 20.

$\cdot 1$. *Let $A \subset \mathfrak{M}$, $A \neq 0$. A is a m. subsystem of $\mathfrak{M}$ if and only if $A^2 \subset A$.*

In fact, if A is a m. subsystem of $\mathfrak{M}$, then the product of any two elements of A belongs to A and vice-versa. As the set of products of any two elements of A is precisely A^2, the theorem results.

$\cdot 2$. *Let $\mathfrak{A}$ be a m. subsystem of $\mathfrak{M}$. Then $\mathfrak{A} \supset \mathfrak{A}^2 \supset \mathfrak{A}^3 \supset \dots$*

Consider a positive integer α. Let $u \in \mathfrak{A}^{\alpha+1}$ so that $u - a_1 \dots a_{\alpha+1}$ for some suitable $a_1, \dots, a_{\alpha+1} \in \mathfrak{A}$. By (2) we have $u = (a_1 \dots a_{\alpha-1}) \cdot (a_\alpha a_{\alpha+1})$, where the symbol $(a_1 \dots a_{\alpha-1})$ is to be omitted for $\alpha = 1$. By $\cdot 1$ we have $a'_\alpha = a_\alpha a_{\alpha+1} \in \mathfrak{A}^2 \subset \mathfrak{A}$. Hence $u - a_1 \dots a_{\alpha-1} a'_\alpha \in \mathfrak{A}^\alpha$ and $\mathfrak{A}^\alpha \supset \mathfrak{A}^{\alpha+1}$ follows.

$\cdot 3$. *If $\mathfrak{A}$ is a m. subsystem of $\mathfrak{M}$, so is $\mathfrak{A}^\alpha$ for every positive integer α.*

In fact, by $\cdot 1$ and 3 $\cdot 1$ we have $\mathfrak{A}^\alpha \supset \mathfrak{A}^{2\alpha} = (\mathfrak{A}^\alpha)^2$ for every positive integer α. Hence $\mathfrak{A}^\alpha \supset (\mathfrak{A}^\alpha)^2$ and the theorem follows from $\cdot 1$.

5. **Projection.** Let $\mathfrak{M}$ be a m. system. Let N be an overset of $\mathfrak{M}$ so that $\mathfrak{M} \subset N$. Each representation f of N into $\mathfrak{M}$ such that the equality $f(a) = a$ holds for every $a \in \mathfrak{M}$, will be termed *projection* of the set N into $\mathfrak{M}$. The element $f(a) \in \mathfrak{M}$, for an arbitrary $a \in N$, is the *trace* of a in $\mathfrak{M}$ at the projection f.

Let f be a projection of the set N into $\mathfrak{M}$. For N we define a multiplication in the following way:

$$ab = f(a) f(b) \quad \text{for} \quad a, b \in N.$$

We shall show that this multiplication is associative. According to the definition and with regard to the assumption that $\mathfrak{M}$ is a m. system, we get for $a, b, c \in N$

$$\begin{aligned} a(bc) &= a[f(b)f(c)] = f(a) \cdot f[f(b)f(c)] = f(a)[f(b)f(c)] = \\ &= [f(a)f(b)]f(c) = f[f(a)f(b) \; f(c) = [f(a)f(b)]\, c = (ab)\, c. \end{aligned}$$

It is evident that the m. system N, defined in this way, is a m. oversystem of $\mathfrak{M}$. We say that N is the m. oversystem of $\mathfrak{M}$ at the projection f; $\mathfrak{M}$ is the m. subsystem of N at the projection f.

We remark the following simple theorem:

Let $\mathfrak{N}$ be the m. oversystem of $\mathfrak{M}$ at an arbitrary projection f. Then we have $\mathfrak{N}^\alpha = \mathfrak{M}^\alpha$ for every positive integer $\alpha > 1$.

As a simple example of a projection consider the m. system

$$\begin{matrix} \{(a_1, b_1), & (a_2, b_1), & (a_3, b_1), \dots\dots\} \\ & (a_2, b_2), & (a_3, b_2), \dots\dots \\ & & (a_3, b_3), \dots\dots \\ & & \dots\dots \end{matrix} \tag{3}$$

for which the multiplication is defined by the formula

$$(a_\alpha, b_\beta)\,(a_\gamma, b_\delta) = (a_{\alpha+\beta}, b_1);\ \ \alpha, \gamma = 1, 2, \ldots,\ 1 \leq \beta \leq \alpha,\ 1 < \delta < \gamma.$$

This m. system is evidently the m. oversystem of the m. system

$$\{(a_1, b_1), (a_2, b_1), (a_3, b_1), \ldots\ldots\} \tag{4}$$

the multiplication being given by

$$(a_\alpha, b_1)\,(a_\gamma, b_1) = (a_{\alpha+\gamma}, b_1);\ \ \alpha, \gamma = 1, 2, \ldots\ldots,$$

at the following projection

$$f[(a_\alpha,\ b_\beta)] = (a_\alpha, b_1);\ \ \alpha = 1, 2, \ldots;\ 1 < \beta \leq \alpha. \tag{5}$$

6. **Excentrum.** Let $\mathfrak{M}$ be a m. system. For every positive integer α let M_α be the set defined as follows

$$\mathfrak{M}^\alpha \quad \mathfrak{M}^{\alpha+1} \vee M_\alpha,\ \mathfrak{M}^{\alpha+1} \cap M_\alpha = 0.$$

In particular, the set M_1 will be called the *excentrum* of the m. system $\mathfrak{M}$. The elements of M_1 are the *prime factors* of $\mathfrak{M}$. If $M_1 = 0$ we say that $\mathfrak{M}$ has no excentrum.

From the definition follows, that for every positive integer α, M_α is the set of elements of $\mathfrak{M}$ which are products of α but not more than α elements of $\mathfrak{M}$. The prime factors of $\mathfrak{M}$ are precisely the elements of $\mathfrak{M}$ which are not products of two elements of $\mathfrak{M}$. The sets $M_1, M_2, \ldots$ are evidently mutually exclusive.

·1. *If the equality $M_\alpha = 0$ holds for a positive integer α, then*

$$0 = M_\alpha \quad M_{\alpha+1} \quad M_{\alpha+2} - \ldots\ldots$$

In fact, if the equalities $0 = M_\alpha = M_{\alpha+1} = \ldots = M_{\alpha+\beta-1}$ hold, then $\mathfrak{M}^{\alpha+\beta-1} = \mathfrak{M}^{\alpha+\beta}$ and $\mathfrak{M}^{\alpha+\beta} = \mathfrak{M}^{\alpha+\beta+1}$; hence $M_{\alpha+\beta} = 0$.

·2. *For every positive integer α the excentrum of $\mathfrak{M}^\alpha$ is the set $M_\alpha \vee M_{\alpha+1} \vee \ldots \vee M_{2\alpha-1}$.*

From the equality

$$\mathfrak{M}^{\alpha+\beta-1} = \mathfrak{M}^{\alpha+\beta} \vee M_{\alpha+\beta-1},$$

which according to the definition holds for any positive integers α, β, follows

$$\mathfrak{M}^\alpha = M_\alpha \vee M_{\alpha+1} \vee \ldots \vee M_{\alpha+\beta-1} \vee \mathfrak{M}^{\alpha+\beta}. \tag{6}$$

Every element of the set $M_\alpha \vee M_{\alpha+1} \vee \ldots \vee M_{\alpha+\beta-1}$ is product of $\alpha + \beta - 1$ elements of $\mathfrak{M}$ to the utmost, while every element of $\mathfrak{M}^{\alpha+\beta}$ is product of $\alpha + \beta$ elements. Hence

$$(M_\alpha \vee M_{\alpha+1} \vee \ldots \vee M_{\alpha+\beta-1}) \cap \mathfrak{M}^{\alpha+\beta} = 0.$$

Erom this and (6) the theorem follows for $\beta = \alpha$.

·3. *Let $\mathfrak{N}$ be a m. oversystem of $\mathfrak{M}$ at some projection f. Let the sets N_α, $\alpha - 1, 2, \ldots,$ have for $\mathfrak{N}$ the same meaning as M_α have for $\mathfrak{M}$. Then*

$$N_1 \wedge M_1 \quad \mathfrak{N} \wedge \mathfrak{M},\ \ N_\alpha - M_\alpha \textit{ for } \alpha > 1.$$

The proof results easily from the theorem of n° 5.

·*4. For any positive integers α, β is $M_{\alpha+\beta} \subset M_\alpha M_\beta$.*

It is evident that the affirmation holds, if $M_{\alpha+\beta} = 0$. Let us therefore assume $u \in M_{\alpha+\beta}$, so that u is product of $\alpha + \beta$ but not more than $\alpha + \beta$ elements of $\mathfrak{M}$. Then we have $u - a_1 \ldots . a_\alpha a_{\alpha+1} \ldots . a_{\alpha+\beta}$ at suitably chosen $a_1, \ldots, a_{\alpha+\beta} \in \mathfrak{M}$. The element $a_1 \ldots a_\alpha$ is a clear product of at least α elements of $\mathfrak{M}$, but not more than $\alpha + \beta - 1$ elements; for otherwise u would consist of more than $\alpha + \beta$ elements of $\mathfrak{M}$. Hence $a_1 \ldots a_\alpha \in M_{\alpha+\gamma}$ for a suitable positive integer γ, $0 \leq \gamma < \beta - 1$, and likewise $a_{\alpha+1} \ldots a_{\alpha+\beta} \in M_{\beta+\delta}$ for a suitable positive integer δ, $0 < \delta \leq \alpha - 1$. Then $u \in M_{\alpha+\gamma} M_{\beta+\delta}$ and it follows that u consists of at least $\alpha + \gamma + \beta + \delta$ elements of $\mathfrak{M}$. Therefore $\gamma = \delta = 0$.

In particular, there exists the relation $M_\alpha \subset M_1{}^\alpha$ for every positive integer α; i. e., every element of M_α is product of α prime factors.

7. **Kernel.** Let $\mathfrak{M}$ be a m. system and the symbols $M_1, M_2, \ldots$ have (everywhere in the sequel) the above meaning. There are precisely two possibilities:

1° There exists such a positive integer α that $M_\alpha = 0$, while (if $\alpha > 1$) $M_\beta \neq 0$ for $\beta \quad 1, 2, \ldots, \alpha - 1$.

In this case we get by 6 ·*1*

$$0 = M_\alpha = M_{\alpha+1} = M_{\alpha+2} = \ldots ; \quad \mathfrak{M}^\alpha = \mathfrak{M}^{\alpha+1} = \mathfrak{M}^{\alpha+2} = \ldots ;$$

from this follows

$$\mathfrak{M} = M_1 \vee M_2 \vee \ldots \vee M_{\alpha-1} \vee \mathfrak{M}^\alpha$$

and all sets on the right are different from 0. The m. system $\mathfrak{M}^\alpha$ has no excentrum; we call it the *kernel* of $\mathfrak{M}$.

2° There holds for every positive integer α the inequality $M_\alpha \neq 0$.

In this case we ~~write~~ put

$$\mathfrak{M} = M_1 \vee M_2 \vee \ldots$$

and say that the m. system $\mathfrak{M}$ is without kernel.

To the m. systems which possess a kernel belong e. g. the groups or more generally all m. systems containing the unity-element. For if $\mathfrak{M}$ contains the unity-element e, so that $e \in \mathfrak{M}$, $\{e\} \mathfrak{M} - \mathfrak{M} \{e\} = \mathfrak{M}$, it follows $\mathfrak{M} = \{e\} \mathfrak{M} \subset \mathfrak{M}^2$ and thus $\mathfrak{M} = \mathfrak{M}^2$; hence $\mathfrak{M}$ has the kernel $\mathfrak{M}$.

In the remaining pages of this paper we shall be concerned only with m. systems without kernel.

II. Multiplicative systems without kernel.

8. **Fundamental properties.** Let $\mathfrak{M} = M_1 \vee M_2 \vee \ldots$ be a m. system without kernel.

·*1. For any positive integers* α, β *is*

$$M_\alpha M_\beta \subset M_{\alpha+\beta} \vee M_{\alpha+\beta+1} \vee \cdots$$

Let $u \in M_\alpha M_\beta$ so that there exist $a \in M_\alpha$, $b \in M_\beta$, $u = ab$. By 6 ·*4* the element $a\,(b)$ is product of $\alpha\,(\beta)$ prime factors of $\mathfrak{M}$. Consequently $u = ab$ is product of $\alpha + \beta$ prime factors of $\mathfrak{M}$. As no element of M_γ, $\gamma = 1, 2, \ldots$, is product of more than γ elements of $\mathfrak{M}$, we get $u \in M_{\alpha+\beta} \vee M_{\alpha+\beta+1} \vee \cdots$

·*2. Let* $\mathfrak{A}$ *be a m. subsystem of* $\mathfrak{M}$. *Then* $\mathfrak{A}$ *is without kernel.*

Otherwise there exists such a positive integer α, that $\mathfrak{A}^\alpha = \mathfrak{A}^{\alpha+1} = \ldots$ Let $a \in \mathfrak{A}^\alpha$ so that $a \in \mathfrak{A}^{\alpha+\beta}$ for every positive integer β. Then a is product of $\alpha + \beta$ suitable elements of $\mathfrak{A} \subset \mathfrak{M}$. As $a \in \mathfrak{M}$, we have $a \in M_\gamma$ for a suitable γ, so that a does not consist of more than γ elements of $\mathfrak{M}$. Taking β in manner that $\alpha + \beta > \gamma$, we get a contradiction.

In particular, the m. system $\mathfrak{M}^\alpha$ is without kernel for every positive integer α.

·*3. Let* $\mathfrak{N}$ *be a m. oversystem of* $\mathfrak{M}$ *at a projection* f. *Then* $\mathfrak{N}$ *is without kernel.*

The proof follows easily from 6 ·*3*.

9. **Indices.** Let $\mathfrak{M} = M_1 \vee M_2 \vee \ldots$ be a m. system without kernel. Let $a \in \mathfrak{M}$. The sets $M_1, M_2, \ldots$ being mutually exclusive, there exists such a single positive integer α, that $a \in M_\alpha$. We call α the *index* of a.

From the definition follows that every element $a \in \mathfrak{M}$ has precisely one index. The sets $M_1, M_2, \ldots$ being all different from 0, there exists for every positive integer α an element of $\mathfrak{M}$, the index of which is α. By 6 ·*4* every element of index α is product of α prime factors of $\mathfrak{M}$ but (by the definition of the sets M) not more than α elements of $\mathfrak{M}$. By 8 ·*1* the index of a product of any two elements of $\mathfrak{M}$ is at least equal to the sum of the indices of both factors.

10. **Infinite cyclic m. system.** Of the m. systems without kernel the *infinite cyclic m. system* seems to be the simplest. We denote it by $\mathfrak{Z}$. This m. system is an infinite sequence of elements $\{z_1, z_2, z_3, \ldots\}$ for which the multiplication is defined by the formula: $z_\alpha z_\beta = z_{\alpha+\beta}$; $\alpha, \beta = 1, 2, \ldots$ Writing z instead of z_1 we get

$$\mathfrak{Z} = \{z, z^2, z^3, \ldots\}.$$

It is clear that $\mathfrak{Z}$ is commutative. $\mathfrak{Z}$ is isomorphic to the m. system, the elements of which are positive integers and the multiplication is the usual addition; the corresponding isomorphic representation (isomorphism) is $z^\alpha \longleftrightarrow \alpha$ for $\alpha = 1, 2, \ldots$ We evidently have

$$\mathfrak{Z}^2 = \{z^2, z^3, \ldots\}, \quad \mathfrak{Z}^3 = \{z^3, \ldots\}, \ldots$$

so that the respective sets M which we denote by $Z_1, Z_2, \dots$ are

$$Z_1 = \{z\}, \quad Z_2 = \{z^2\}, \quad Z_3 = \{z^3\}, \dots$$

Thus $\mathfrak{Z}$ is a m. system without kernel. By 6 ·*2* the set $\{z^{\alpha}, z^{\alpha+1}, \dots, z^{2\alpha-1}\}$ is the excentrum of the m. system $\mathfrak{Z}^{\alpha}$, for every positive integer α.

Let $\mathfrak{M}$ be a m. system without kernel. Let $z \in \mathfrak{M}$. Then the elements of the infinite cyclic m. subsystem $\mathfrak{Z} = \{z, z^2, z^3 \dots\}$ of $\mathfrak{M}$ differ from each other.

Let us assume, on the contrary, that we have for suitable α, β: $z^{\alpha} = z^{\alpha+\beta}$. Let γ be the index of z^{α}, so that the element $z^{\alpha} = p_1 \dots p_{\gamma}$ is product of γ prime factors of $\mathfrak{M}$, but not more than γ elements of $\mathfrak{M}$. From the equalities $z^{\alpha} = z^{\alpha} z^{\beta} = p_1 \dots p_{\gamma} z^{\beta}$ follows that z^{α} is product of more than γ elements of $\mathfrak{M}$ and we get a contradiction.

11. **Homogeneous and inhomogeneous m. systems.** Let $\mathfrak{M} = M_1 \vee M_2 \vee \dots$ be a m. system without kernel. If any element $a \in \mathfrak{M}$ of index α, $\alpha = 1, 2, \dots$, does not consist of less than α prime factors of $\mathfrak{M}$, then $\mathfrak{M}$ is said to be *homogeneous*. Otherwise $\mathfrak{M}$ is *inhomogeneous*.

·*1. $\mathfrak{M}$ is homogeneous if and only if $M_{\alpha} = M_1^{\alpha}$ for every positive integer α, so that*

$$\mathfrak{M} = M_1 \vee M_1^2 \vee M_1^3 \vee \dots$$

a) Let us assume that $\mathfrak{M}$ is homogeneous. Then the product of any α prime factors, $\alpha = 1, 2, \dots$, obviously belongs to the set M_{α}. Hence $M_1^{\alpha} \subset M_{\alpha}$ and thus $M_{\alpha} = M_1^{\alpha}$, by 6 ·*4*.

b) Suppose $M_{\alpha} = M_1^{\alpha}$ for every positive integer α. Consider an element $a \in \mathfrak{M}$. Let $a = p_1 \dots p_{\alpha} = p'_1 \dots p'_{\beta}$ be two decompositions of a into prime factors. Then $a \in M_1^{\alpha} \cap M_1^{\beta} = M_{\alpha} \cap M_{\beta}$ and therefore $\alpha = \beta$ because the sets M are mutually exclusive. Hence $\mathfrak{M}$ is homogeneous.

A simple example of a homogeneous m. system is given by the infinite cyclic m. system $\mathfrak{Z}$. We evidently get $Z_{\alpha} = Z_1^{\alpha}$ for $\alpha = 1, 2, \dots$

·*2 Let $\mathfrak{M}$ be homogeneous. Then there exists such a homomorphic representation of $\mathfrak{M}$ on $\mathfrak{Z}$, that every prime factor of $\mathfrak{M}$ is represented on the single prime factor of $\mathfrak{Z}$.*

In fact, the correspondence $\mathfrak{F}$, which makes each element of M_{α} correspond with the element z^{α} of $\mathfrak{Z}$, $\alpha = 1, 2, \dots$, is evidently a representation of $\mathfrak{M}$ on $\mathfrak{Z}$ and has the property that every prime factor of $\mathfrak{M}$ is represented on the single prime factor of $\mathfrak{Z}$. Let $a \in M_{\alpha}$, $b \in M_{\beta}$ at some α, β, so that in the correspondence $\mathfrak{F}: a \to z^{\alpha}$, $b \to z^{\beta}$. As $\mathfrak{M}$ is homogeneous, we get $ab \in M_{\alpha} M_{\beta} = M_{\alpha+\beta}$ and thus $ab \to z^{\alpha+\beta} = z^{\alpha} z^{\beta}$. Hence $\mathfrak{F}$ is a homomorphic representation (homomorphism) of $\mathfrak{M}$ on $\mathfrak{Z}$.

12. Let $\mathfrak{M}$ be without kernel.

·*1. For every positive integer $\alpha > 1$ the m. system $\mathfrak{M}^{\alpha}$ is inhomogeneous.*

Let α be a positive integer. Let the symbol $M_{\alpha,\beta}$ have the same meaning for $\mathfrak{M}^{\alpha}$ as M_{β} has for $\mathfrak{M}$, for an arbitrary β, so that

$$\mathfrak{M}^{\alpha\beta} = \mathfrak{M}^{\alpha(\beta+1)} \vee M_{\alpha,\beta}; \quad \mathfrak{M}^{\alpha(\beta+1)} \cap M_{\alpha,\beta} = 0$$

and $M_{\alpha,1}$ denotes the excentrum of the m. system $\mathfrak{M}^{\alpha}$. According to (6) we get

$$M_{\alpha,\beta} = M_{\alpha\beta} \vee M_{\alpha\beta+1} \vee \ldots \vee M_{\alpha\beta+\alpha-1}.$$

If $\mathfrak{M}^{\alpha}$ is homogeneous, we obtain according to 11 $\cdot 1$: $M_{\alpha,\beta} - M_{\alpha,1}{}^{\beta}$ and thus

$$M_{\alpha\beta} \vee M_{\alpha\beta+1} \vee \ldots \vee M_{\alpha\beta+\alpha-1} = (M_{\alpha} \vee M_{\alpha+1} \vee \ldots \vee M_{2\alpha-1})^{\beta},$$
$$\beta = 1, 2 \ldots$$

In the set on the left there are elements whose greatest index is $\alpha\beta+\alpha-1$; whereas of those on the right the greatest index is $\geq \beta(2\alpha-1)$, according to 3 $\cdot 2$ and 8 $\cdot 1$. Hence $\alpha\beta+\alpha-1 > \beta(2\alpha-1)$ and thus $(\alpha-1)(\beta-1) < 0$. Therefore $\alpha \quad 1$.

$\cdot 2$. $\mathfrak{M}$ is a proper m. subsystem of a suitable inhomogeneous m. system.

Consider an element $a \in \mathfrak{M}$, the index of which is at least 3, so that there exist prime factors of $\mathfrak{M}$, $p_1, \ldots, p_\alpha$, $\alpha \geqq 3$, for which $a \quad p_1 \ldots p_\alpha$. Let $\mathfrak{N}$ be a proper m. oversystem of $\mathfrak{M}$ at a projection f. We can choose f in such a way that $f(p_0) = p_2 \ldots p_\alpha$ for some element $p_0 \in \mathfrak{N} \wedge \mathfrak{M}$. Because of 6 $\cdot 3$ the elements $p_0, p_1, \ldots, p_\alpha$ are prime factors of $\mathfrak{N}$. According to the definition of the multiplication in $\mathfrak{N}$ we get $p_1 p_0 = f(p_1) f(p_0) = p_1 p_2 \ldots p_\alpha = a$, so that a is product of two as well as at least three prime factors of $\mathfrak{N}$. Hence $\mathfrak{N}$ is inhomogeneous.

For instance (3) is a proper m. oversystem of the infinite cyclic m. system (4) at the projection (5) and is inhomogeneous. In fact, let (a_α, b_1) be of an index at least equal to 3, so that $\alpha \geqq 3$. According to 6 $\cdot 3$ both (a_1, b_1) as well as $(a_{\alpha-1}, b_\beta)$, for $2 < \beta < \alpha - 1$, are prime factors of (3). By the definition of the multiplication we get $(a_1, b_1)(a_{\alpha-1}, b_\beta) - (a_1, b_1)^{\alpha}$, so that this element is product of two as well as at least three prime factors. — It can be shown that generally every element (a_α, b_1), $\alpha > 2$, is product of an arbitrary number β, $2 \leqq \beta < \alpha$, of prime factors of (3).

13. **Homomorphic representations on $\mathfrak{Z}$.** By the theorem 11 $\cdot 2$ we are conducted to the study of homomorphic representations of m. systems $\mathfrak{M}$ on the infinite cyclic m. system $\mathfrak{Z} = \{z, z^2, z^3, \ldots\}$. For such a representation: 1° every element $a \in \mathfrak{M}$ is represented on a single element (the *counterpart* of a) $z^{\alpha} \in \mathfrak{Z}$; we write $a \rightarrow z^{\alpha}$ 2° every element of $\mathfrak{Z}$ is the counterpart of at least one element of $\mathfrak{M}$ 3° for $a, b \in \mathfrak{M}$, $a \rightarrow z^{\alpha}$, $b \rightarrow z^{\beta}$ there holds $ab \rightarrow z^{\alpha+\beta}$.

Let $\mathfrak{M}$ be a m. system.

·1. $\mathfrak{M}$ is homomorphically representable on $\mathfrak{Z}$ if and only if there exists a sequence of non-vacuous and mutually exclusive sets F_α, $\alpha - 1, 2, \ldots$, so that

$$\mathfrak{M} = F_1 \vee F_2 \vee \ldots \tag{7}$$

and $F_\alpha F_\beta \subset F_{\alpha+\beta}$ for $\alpha, \beta = 1, 2, \ldots$

a) Suppose a homomorphic representation $\mathfrak{F}$ of $\mathfrak{M}$ on $\mathfrak{Z}$. Let F_α be the set of those elements of $\mathfrak{M}$ which are represented on z^α in $\mathfrak{F}$, $\alpha = 1, 2, \ldots$ As every element of $\mathfrak{Z}$ is the counterpart of at least one element of $\mathfrak{M}$, the F_α are non-vacuous. As every element of $\mathfrak{M}$ is represented on a single element of $\mathfrak{Z}$, the F_α, $\alpha - 1, 2, \ldots$, are mutually exclusive. Obviously (7) holds. Let $u \in F_\alpha F_\beta$ for some positive integers α, β, so that there exist $a \in F_\alpha$, $b \in F_\beta$, $u = ab$. According to the definition of the sets F we get $a \to z^\alpha$, $b \to z^\beta$ and therefore $u = ab \to z^{\alpha+\beta}$. Hence $u \in F_{\alpha+\beta}$, and $F_\alpha F_\beta \subset F_{\alpha+\beta}$.

a) Consider a sequence of sets F_α, $\alpha = 1, 2, \ldots$, which has the above properties. The correspondence by which every element $a \in F_\alpha$ corresponds with the element z^α of $\mathfrak{Z}$, $\alpha = 1, 2, \ldots$, is apparently a homomorphic representation of $\mathfrak{M}$ on $\mathfrak{Z}$.

The sequence of sets F_α, $\alpha = 1, 2, \ldots$, defined by a homomorphic representation $\mathfrak{F}$ of the m. system $\mathfrak{M}$ on $\mathfrak{Z}$ as in ·*1* a), will be called the *determining sequence* for the homomorphism $\mathfrak{F}$. A homomorphism $\mathfrak{F}$ with the determining sequence $F_1, F_2, \ldots$ will be denoted in the following way: $\mathfrak{F}(F_1, F_2, \ldots)$.

·2. Let $\mathfrak{M}$ be homomorphically representable on $\mathfrak{Z}$. Let $\mathfrak{F}(F_1, F_2, \ldots)$ be a homomorphism of $\mathfrak{M}$ on $\mathfrak{Z}$. For every decomposition of an element $u \in F_\alpha$, $\alpha - 1, 2, \ldots$, in a product $u = a_1 \ldots a_\beta$ of elements $a_1, \ldots, a_\beta$ of $\mathfrak{M}$, there holds

$$\text{a) } \beta < \alpha, \quad \text{b) } a_1, \ldots, a_\beta \in F_1 \vee F_2 \vee \ldots \vee F_\alpha,$$
$$\text{c) } \pi_1 + 2\pi_2 + \ldots + \alpha\pi_\alpha = \alpha,$$

the π_γ being the number of the elements a which belong to F_γ.

In fact, for suitable positive integers $\alpha_1, \ldots, \alpha_\beta$ we get $a_1 \in F_{\alpha_1}, \ldots, a_\beta \in F_{\alpha_\beta}$, so that $u = a_1 \ldots . a_\beta \in F_{\alpha_1} \ldots . F_{\alpha_\beta} \subset F_{\alpha_1 + \ldots . + \alpha_\beta} = F_\alpha$. Hence $\alpha_1 + \ldots . + \alpha_\beta = \alpha$. It follows a) $\beta \leq \alpha$, b) $\alpha_1, \ldots ., \alpha_\beta \leq \alpha$ and thus $a_1, \ldots ., a_\beta \in F_1 \vee F_2 \vee \ldots . \vee F_\alpha$, c) $\alpha = \alpha_1 + \ldots . + \alpha_\beta = \pi_1 + 2\pi_2 + \ldots + \alpha\pi_\alpha$, because by definition of π_γ, the number *1* appears in the series $\alpha_1, \ldots, \alpha_\beta$ π_1-times, *2* appears π_2-times, $\ldots$, α appears π_α-times.

·3. Let $\mathfrak{M}$ be homomorphically representable on $\mathfrak{Z}$. Then $\mathfrak{M}$ is without kernel.

Consider an arbitrary homomorphism $\mathfrak{F}(F_1, F_2, \ldots)$ of $\mathfrak{M}$ on $\mathfrak{Z}$. Let us assume on the contrary that $M_\alpha = 0$ for some positive integer α. Then $\mathfrak{M}^\alpha = \mathfrak{M}^{\alpha+1}$, so that every element $a \in \mathfrak{M}^\alpha$ is product of more than α elements of $\mathfrak{M}$. By ·*1* we get $F_1{}^\alpha \subset F_\alpha$ and on the other hand apparently $F_1^{\alpha} \subset \mathfrak{M}^{\alpha}$, so that there exists an $a \in F_{\alpha} \cap \mathfrak{M}^{\alpha}$. Hence a is product of more than α elements of $\mathfrak{M}$ and at the same time, by $\cdot 2$ a), it is product of α elements of $\mathfrak{M}$ to the utmost. Therefore we have a contradiction. Hence $M_{\alpha} \neq 0$ for $\alpha \quad 1, 2, \dots$

$\cdot 4$. *Let $\mathfrak{M}$ be homomorphically representable on $\mathfrak{Z}$, so that $\mathfrak{M} = M_1 \vee M_2 \dots$ Let $\mathfrak{F}(F_1, F_2, \dots)$ be an arbitrary homomorphism of $\mathfrak{M}$ on $\mathfrak{Z}$. Then for any positive integers $\alpha_1, \alpha_2, \dots, \alpha_{\beta}$ there holds*

$$F_{\alpha_1} F_{\alpha_2} \dots F_{\alpha_{\beta}} \subset M_{\beta} \vee M_{\beta+1} \vee \dots \vee M_{\alpha_1+\alpha_2+\dots+\alpha_{\beta}}. \tag{8}$$

In fact, consider an $a \in F_{\alpha}$, α being some positive integer. a has a fixed index γ, so that $a \in M_{\gamma}$. By $\cdot 2$ a) the number of factors at every decomposition of a in a product of elements of $\mathfrak{M}$ does not exceed α. Hence $\gamma \leq \alpha$ and thus

$$F_{\alpha} \subset M_1 \vee M_2 \vee \dots \vee M_{\alpha}.$$

If we take for α some positive integers $\alpha_1, \dots, \alpha_{\beta}$ and multiply, we get

$$F_{\alpha_1} F_{\alpha_2} \dots F_{\alpha_{\beta}} \subset (M_1 \vee M_2 \vee \dots \vee M_{\alpha_1})(M_1 \vee M_2 \vee \dots \vee M_{\alpha_2}) \dots$$
$$\dots (M_1 \vee M_2 \vee \dots \vee M_{\alpha_{\beta}}) \quad M_1^{\beta} \vee \dots \vee M_{\alpha_1} M_{\alpha_2} \dots M_{\alpha_{\beta}}.$$

By 8 $\cdot 1$ follows

$$F_{\alpha_1} F_{\alpha_2} \dots F_{\alpha_{\beta}} \subset M_{\beta} \vee M_{\beta+1} \vee \dots$$

At the same time we get

$$F_{\alpha_1} F_{\alpha_2} \dots F_{\alpha_{\beta}} \subset F_{\alpha_1+\alpha_2+\dots+\alpha_{\beta}} \subset M_1 \vee M_2 \vee \dots \vee M_{\alpha_1+\alpha_2+\dots+\alpha_{\beta}}$$

and therefore (8) holds.

$\cdot 5$. *Let $\mathfrak{M}$ be homomorphically representable on $\mathfrak{Z}$ in such a way, that every prime factor of $\mathfrak{M}$ corresponds with the single prime factor of $\mathfrak{Z}$. Then $\mathfrak{M}$ is homogeneous.*

Let $\mathfrak{F}(F_1, F_2, \dots)$ be a homomorphism of $\mathfrak{M} \quad M_1 \vee M_2 \vee \dots$ on $\mathfrak{Z}$ having the above property, so that $M_1 - F_1$. By 6 $\cdot 4$ we have $M_{\alpha} \subset M_1^{\alpha}$ and by (8) $(\alpha_1 - \alpha_2 = \dots \quad \alpha_{\beta} - 1) M_1^{\alpha} \subset M_{\alpha}$, for $\alpha = 1, 2, \dots$ Hence $M_{\alpha} - M_1^{\alpha}$ for $\alpha = 1, 2, \dots$ and $\mathfrak{M}$ is homogeneous (by 11 $\cdot 1$).

14. By the theorem 13 $\cdot 5$ we can construct a simple example of a homogeneous m. system whose elements are matrices of an arbitrary order ν in the continuum of complex numbers.

Let α, ν be arbitrary positive integers, $\alpha < \nu$. Let ${}_{\alpha}A$ denote the αth compound of A for an arbitrary matrix A of order ν in the continuum of complex numbers. From elementary theorems follows that in the mentioned continuum there exist such matrices A of order ν, for which all matrices of the sequence

$${}_{\alpha}A, \ ({}_{\alpha}A)^2, \ ({}_{\alpha}A)^3, \dots \tag{9}$$

are mutually different.

Consider a matrix A having this property. Let us denote by A a set of matrices of order ν in the continuum of complex numbers whose αth compounds are equal to ${}_{\alpha}A$. If, for instance, the rank of A is $> \alpha$, every matrix of the set A is ωA, where ω is an αth root of unity[3]). We suppose $A \in \mathsf{A}$.

Let $\mathfrak{M}$ be the m. system of matrices of order ν, the elements of which are the matrices of the set A and all others derived from them by the usual composition. Then $\mathfrak{M}$ is homogeneous.

In fact, according to 13 $\cdot$ *5* it is sufficient to prove that $\mathfrak{M}$ is homomorphically representable on the concrete infinite cyclic m. system (9) in such a way, that every prime factor of $\mathfrak{M}$ corresponds with ${}_{\alpha}A$.

For any two matrices Ξ, H of order ν there holds the well known equality

$$ {}_{\alpha}(\Xi H) = {}_{\alpha}\Xi \cdot {}_{\alpha}H. \tag{10} $$

Let $\mathfrak{F}$ be the correspondence by which every matrix $\Xi \in \mathfrak{M}$ corresponds with ${}_{\alpha}\Xi$. According to (10), the matrix ${}_{\alpha}\Xi$ belongs to the m. system (9) for every matrix $\Xi \in \mathfrak{M}$ and the matrix $({}_{\alpha}A)^{\beta}$ is the αth compound of $A^{\beta} \in \mathfrak{M}$ for every positive integer β. Hence $\mathfrak{F}$ is a representation of $\mathfrak{M}$ on the infinite cyclic m. system (9) and, by (10), precisely a homomorphic representation. By the definition of $\mathfrak{M}$ the relation $M_1 \subset \mathsf{A}$ apparently holds for the excentrum M_1 of $\mathfrak{M}$. If some matrix $B \in \mathsf{A}$ does not belong to M_1, there exist $A_1, A_2, \ldots A_{\gamma} \in M_1, \gamma \geq 2$, so that $B = A_1 A_2 \ldots A_{\gamma}$ and therefore ${}_{\alpha}A = {}_{\alpha}B \quad {}_{\alpha}A_1 \cdot {}_{\alpha}A_2 \ldots {}_{\alpha}A_{\gamma} = ({}_{\alpha}A)^{\gamma}$. This contradicts the assumption that all matrices of the sequence (9) are mutually different. Hence $M_1 - \mathsf{A}$ and therefore every prime factor of $\mathfrak{M}$ corresponds with ${}_{\alpha}A$.

15. As to the inhomogeneous m. systems, some are and some not homomorphically representable on $\mathfrak{Z}$.

For instance, the inhomogeneous (s. n° 12) m. oversystem (3) of the infinite cyclic m. system (4) at the projection (5), is homomorphically representable on $\mathfrak{Z}$. For the sets

$$ F_{\alpha} = \{(a_{\alpha}, b_1), (a_{\alpha}, b_2), \ldots, (a_{\alpha}, b_{\alpha})\}, \quad \alpha = 1, 2, \ldots $$

are non-vacuous and they are mutually exclusive; further, their sum is the m. system (3) and there apparently holds $F_{\alpha} F_{\beta} \mathrel{\dot{-}} \{(a_{\alpha+\beta}, b_1)\} \subset F_{\alpha+\beta}$ for $\alpha, \beta \quad 1, 2, \ldots$ Hence (3) is homomorphically representable on $\mathfrak{Z}$ (by 13 $\cdot$ *1*).

On the contrary, the following theorem holds:

Let $\mathfrak{M}$ be an arbitrary m. system without kernel. Then for every positive integer $\alpha > 1$ the m. system $\mathfrak{M}^{\alpha}$ is (by 12 $\cdot$ 1 inhomogeneous and is) not homomorphically representable on $\mathfrak{Z}$.

---

[3]) John Williamson, Matrices whose sth compounds are equal (Bull. Amer Math. Soc., Vol. XXXIX, 1933, p. 108).

Let us assume, on the contrary, that for some positive integer $\alpha > 1$ the m. system $\mathfrak{M}^\alpha$ is homomorphically representable on $\mathfrak{Z}$. Let $\mathfrak{F}(F_1, F_2, \ldots)$ be a homomorphism of $\mathfrak{M}^\alpha$ on $\mathfrak{Z}$. Let us choose an arbitrary prime factor p of $\mathfrak{M}$. Let $\nu = 0, 1$. By 8 $\cdot 1$ we get

$$p^{\alpha+\nu} \mathrm{e}\, M_{\alpha+\nu} \vee M_{\alpha+\nu+1} \vee \cdots$$

and therefore, for a suitable positive integer β_ν, holds

$$p^{\alpha+\nu} \mathrm{e}\, F_{\beta_\nu}.$$

Hence

$$p^{\alpha(\alpha+1)} = \begin{cases} (p^\alpha)^{\alpha+1} \mathrm{e}\, F_{\beta_0(\alpha+1)} \\ (p^{\alpha+1})^\alpha \mathrm{e}\, F_{\beta_1 \alpha} \end{cases}$$

and thus

$$\beta_0 (\alpha + 1) = \beta_1 \alpha.$$

Therefore there exists such a positive integer γ ($\beta_1 - \beta_0$) that

$$\beta_0 - \gamma\alpha, \quad \beta_1 = \gamma(\alpha + 1)$$

and consequently

$$p^\alpha \mathrm{e}\, F_{\gamma\alpha}, \quad p^{\alpha+1} \mathrm{e}\, F_{\gamma(\alpha+1)}. \tag{11}$$

Let a be an arbitrary element of F_1. By 13 $\cdot 4$ and 6 $\cdot 2$ we get

$$F_1 \subset M_\alpha \vee M_{\alpha+1} \vee \cdots \vee M_{2\alpha-1},$$

so that there exist such $p_1, p_2, \ldots, p_{\alpha+\beta} \mathrm{e}\, M_1$, $0 \leq \beta < \alpha - 1$, that

$$a - p_1 p_2 \cdots p_{\alpha+\beta}.$$

If $\beta \geqq 1$ then $p_2 p_3 \cdots p_{\alpha+\beta} \mathrm{e}\, \mathfrak{M}^\alpha$ and therefore $p_2 p_3 \cdots p_{\alpha+\beta} \mathrm{e}\, F_\delta$ for some suitable δ. Then from the equality

$$p_1^\alpha a = p_1^{\alpha+1} (p_2 p_3 \cdots p_{\alpha+\beta})$$

follows [by (11)] the relation

$$p_1^\alpha a \mathrm{e}\, F_{\gamma\alpha+1} \cap F_{\gamma(\alpha+1)+\delta}$$

for some suitable positive integer γ, so that $\gamma\alpha + 1 = \gamma(\alpha + 1) + \delta$, which is absurd. Therefore $\beta = 0$. Thus every element $a \mathrm{e}\, F_1$ is product of at most α prime factors of $\mathfrak{M}$.

Let us choose an $a \mathrm{e}\, F_1$, so that $a = p_1 p_2 \cdots p_\alpha$; $p_1, p_2, \ldots p_\alpha \mathrm{e}\, M_1$. As $\alpha > 1$, we get $p_2 p_3 \cdots p_\alpha \cdot p_1 p_2 \cdots p_\alpha \mathrm{e}\, F_\beta$ for some suitable positive integer $\beta > 1$. But

$$p_1^\alpha a^2 = p_1^{\alpha+1} \cdot (p_2 p_3 \cdots p_\alpha p_1 p_2 \cdots p_\alpha),$$

from which follows by (11)

$$p_1^\alpha a^2 \mathrm{e}\, F_{\gamma\alpha+2} \cap F_{\gamma(\alpha+1)+\beta},$$

for a suitable $\gamma > 0$. Hence $\gamma\alpha + 2 \quad \gamma(\alpha + 1) + \beta$ and thus $\beta + \gamma = 2$, which is contradictory with regard to $\beta > 1$, $\gamma > 0$.

From the results of this n° follows, that the inhomogeneous m. systems of the type $\mathfrak{M}^\alpha$, $\mathfrak{M}$ being a m. system without kernel and $\alpha > 1$, are of a special character: A given inhomogeneous m. system is generally not a power with an exponent greater than 1 of a suitable m. system without kernel.