[10] Hausdorff, F., *Erweiterung einer Homöomorphie*, Fund. Math. 16 (1930), p. 353-360.

[11] Hurewicz, W., *Beiträge zur Topologie der Deformationen III. Klassen und Homologietypen von Abbildungen*, Proceed. Akad. Amsterdam 39 (1936), p. 117-125.

[12] Kuratowski, C., *Topologie I*, Warszawa-Wrocław 1948.

[13] — *Topologie II*, Warszawa-Wrocław 1950.

[14] Lubański, M., *An example of an absolute neighbourhood retract, which is the common boundary of three regions in the 3-dimensional Euclidean space*, Fund. Math. 40 (1953), p. 29-38.

[15] Mazurkiewicz, S., *Sur les continus absolument indécomposables*, Fund. Math. 16 (1930), p. 151-159.

[16] — *Sur l'espace des continus péaniens*, Fund. Math. 24 (1935), p. 118-134.

[17] Sierpiński, W., *Sur une courbe cantorienne qui contient une image biunivoque et continue de toute courbe donnée*, C. R. de l'Ac. Sc. Paris 162 (1916), p. 629.

[18] White, P. A., *r-Regular convergence spaces*, Amer. Journal of Math. 66 (1944), p. 69-96.

[19] Whyburn, G. T., *On sequences and limiting sets*, Fund. Math. 25 (1935), p. 408-426.

[20] — *Regular convergence and monotone transformations*, Amer. Journ. of Math. 57 (1935), p. 902-906.

INSTYTUT MATEMATYCZNY POLSKIEJ AKADEMII NAUK
MATHEMATICAL INSTITUTE OF THE POLISH ACADEMY OF SCIENCES

Reçu par la Rédaction le 28. 11. 1953

Elementary properties of Abelian groups *)

by

W. Szmielew (Warszawa)

Table of contents

Introduction

The present study is of meta-mathematical origin. In its initial stage the main aim was to solve the decision problem for the *elementary theory of Abelian groups* [1]). By the elementary theory of Abelian groups we understand that part of the general theory of Abelian groups in which we concern ourselves exclusively with group elements and fundamental group operations without involving any set-theoretical notions (like those of subgroup, isomorphism, etc.). Speaking more technically it is that part of general group theory which can be formalized within elementary logic (*i. e.*, the lower predicate calculus) [2]). In an analogous sense we speak of the *elementary theory* of any other kind of algebraic systems — besides the term "elementary theory" we also use in the same sense the term *arithmetic*. The decision problem for the elementary theory of Abelian groups is the problem of existence of a procedure which permits us to decide in each particular case whether a given sentence formulated in terms of the theory holds in all Abelian groups, *i. e.*, whether this sentence is a logical consequence of postulates characterizing the notion

*) This paper includes all results of the Doctoral Dissertation done by author at the University of California in 1950.

[1]) Previously the decision problem has been solved affirmatively for some special Abelian groups; see [4].

[2]) [2] and [10] may be consulted for various logical and meta-mathematical notions and results involved in our discussion.

of an Abelian group. We have succeeded in obtaining a positive and constructive solution of this problem; a decision procedure for the arithmetic of Abelian groups (based upon the so called *method of eliminating quantifiers* [3]) has actually been found [4] [5]).

By analysing the results obtained it can be noticed that the arguments and methods applied in establishing these results have many implications which go far beyond the original aims of this study. In particular, we have obtained in this way an exhaustive description of what are called *arithmetical classes* and *arithmetical types* of Abelian groups. From this description we have derived some further consequences applying to arithmetical classes and types of arbitrary groups, and even of arbitrary algebraic systems. Arithmetical class and arithmetical type are notions of a general algebraic character which only recently have been introduced by Tarski [6]). The notions in question, in view of their intuitive content and the abundance of problems in which they are involved, seem to deserve the attention of modern algebraists and should attract their interest. In the present case additional interest is provided by the fact that the notions of an arithmetical class and an arithmetical type are applied to Abelian groups, thus to a class of algebraic systems which play a fundamental role in modern algebraic research. For all these reasons we have decided, when putting the results in final form, to shift the focal point from the solution of the decision procedure to a discussion of arithmetical classes and types, and to present this discussion as a chapter of the theory of Abelian groups. In consequence the present work has assumed a purely mathematical character and, as we hope, has become easily comprehensible even to those mathematicians who are not acquainted with meta-mathematical technique.

An Abelian group $\mathfrak{A}$ is regarded here as an algebraic system formed by a set A and a binary operation $+$ (on elements of A) which are assumed to satisfy certain well known postulates; the fact that $\mathfrak{A}$ is formed by A and $+$ is expressed by the formula $\mathfrak{A}=\langle A,+\rangle$ [7]). A property of Abelian groups is called *arithmetical* (or *elementary*) if it can be expressed entirely in terms of the arithmetic of Abelian groups — *i. e.*, by using exclusively variables ranging over elements of the group, the symbol $+$, and the terms of elementary logic (sentential connectives, quantifiers and the identity symbol). In formal discussion the term "arithmetical property" is replaced by "arithmetical class": A class of Abelian groups is *arithmetical* if it consists of all those Abelian groups which possess a certain arithmetical property in common; *i. e.* if a necessary and sufficient condition for a group to belong to this class can be put in the form of a sentence from the arithmetic of Abelian groups. This meta-mathematical definition of an arithmetical class will be replaced in the main body of the paper by a purely mathematical one. As examples of arithmetical classes we may mention the following: the class of all groups of order n, the class of all cyclic groups of order n, and the class of all groups in which the order of every element divides n (where n is any given positive integer). Thus all groups in which every non-zero element is of order 2 form an arithmetical class since a group belongs to this class if and only if it satisfies the condition:

$$\textit{For every } x, \qquad x+x+x=x.$$

Similarly the class of all cyclic groups of order 4 is arithmetical since groups of this class are characterized by the following condition:

There is an x such that $x+x\neq x+x+x+x$, and $x\neq x+x+x$, and for every y, either $y=x$, or $y=x+x$, or $y=x+x+x$, or $y=x+x+x+x$.

From the definition of arithmetical classes it is easily seen that the family of these classes is infinitely denumerable. The smallest class in this family is clearly the empty class, the largest is the class of all Abelian groups. The union and intersection of two arithmetical classes is again arithmetical; also the complement of an arithmetical class to the class of all Abelian groups is arithmetical. Thus the family of arithmetical classes is a field in the sense of set theory. Our problem is to obtain a detailed description of this field. We shall apply the familiar notion of *linear independence modulo m* [8]). In addition we use a stronger notion: the elements $x_1,\ldots,x_n$ of a group are called *linearly independent modulo m in the stronger sense* if whenever $k_1x_1+\ldots+k_nx_n$ is congruent to 0 modulo m, then all the coefficients $k_1,\ldots,k_n$ are also congruent to 0 modulo m ($k_1,\ldots,k_n$ being arbitrary integers, and m being a positive integer). We are interested here only in the case when $m=p^k$ where p is a prime number and $k>0$. Given any group $\mathfrak{A}=\langle A,+\rangle$ we denote respectively by

$$\text{(i)}\quad \varrho^{(1)}[p,k](\mathfrak{A}), \qquad \text{(ii)}\quad \varrho^{(2)}[p,k](\mathfrak{A}), \qquad \text{(iii)}\quad \varrho^{(3)}[p,k](\mathfrak{A})$$

the maximum number (if it exists) of elements which are

(i)′ *of order p^k and linearly independent modulo p^k,*
(ii)′ *linearly independent modulo p^k in the stronger sense,*
(iii)′ *of order p^k and linearly independent modulo p^k in the stronger sense;*

[3]) As an example of a discussion applying this method see [8]. For further bibliographical references cf. [8], p. 50, footnote 11.

[4]) See [6].

[5]) This result cannot be extended to the elementary theory of arbitrary groups; see [13].

[6]) See [9], [11], and [12].

[7]) For information regarding group theory, consult *e. g.* [14].

[8]) Compare, for instance, [1], p. 582, theorem E.

if there is no maximum (finite) number of elements satisfying (i)′, (ii)′, or (iii)′, we put respectively $\varrho^{(1)}[p,k](\mathfrak{A})=\infty$, $\varrho^{(2)}[p,k](\mathfrak{A})=\infty$, or $\varrho^{(3)}[p,k](\mathfrak{A})=\infty$ (thus making no distinction between various kinds of infinity). Let $\mathcal{R}^{(i)}[p,k,n]$ (where $i=1,2,3$, p is a prime and $k,n>0$) be the class of all Abelian groups $\mathfrak{A}$ such that $\varrho^{(i)}[p,k](\mathfrak{A})\geqslant n$, and let $\mathcal{K}[n]$ be the class of all Abelian groups $\mathfrak{A}$ such that $nx=0$ for every element x of the group. The classes $\mathcal{R}^{(i)}[p,k,n]$ and $\mathcal{K}[n]$, just defined, together with their complements, are referred to as *basic classes*. It is easily seen that every basic class is arithmetical. The fundamental result of this paper can now be formulated as follows: *Every arithmetical class of Abelian groups is a finite union of finite intersections of basic classes*; in other words, *the family of all arithmetical classes is the smallest field generated by basic classes*.

Using this result we can obtain many examples of non-arithmetical classes. Consider for instance the class of all infinite cyclic groups. The usual definition of an infinite cyclic group is not formulated exclusively in terms of the arithmetic of Abelian groups; nor do we know any characteristic property of these groups which is formulated in such terms. Hence the conjecture arises that the class of infinite cyclic groups is not arithmetical, and our fundamental result permits us to confirm this conjecture with rigorous proof. In a similar way we can show that, for instance, the following classes are not arithmetical: the class of all finite groups, the class of all simple groups, the class of all torsion groups (*i. e.*, groups containing exclusively elements of finite order) and that of all torsion-free groups (*i. e.*, groups containing no element of finite order except 0).

Two Abelian groups are called *arithmetically equivalent* (or *elementarily indistinguishable*), if they have all arithmetical properties in common — or, in other words, if every arithmetical class contains either both these groups or neither of them. The relation of arithmetical equivalence is clearly reflexive, symmetric and transitive; hence by applying to it the partition theorem we obtain a division of all Abelian groups into mutually exclusive classes such that two groups belong to the same class if and only if they are arithmetically equivalent. These classes are referred to as *arithmetical types*. Thus the arithmetical type of a group $\mathfrak{A}$ is simply the class of all groups which are arithmetically equivalent to $\mathfrak{A}$. As a consequence of the fundamental theorem on arithmetical classes we obtain the following fundamental result concerning the arithmetical equivalence of Abelian groups: Let us agree to say that a group $\mathfrak{A}=\langle A,+\rangle$ is of the *first kind* or of the *second kind* according to whether or not there is a positive integer n such that $nx=0$ for every element x in A. Then, *for two groups* $\mathfrak{A}$ *and* $\mathfrak{B}$ *to be arithmetically equivalent it is necessary and sufficient that* $\mathfrak{A}$ *and* $\mathfrak{B}$ *be both of the first or both of the second kind and that* $\varrho^{(i)}[p,k](\mathfrak{A})=\varrho^{(i)}[p,k](\mathfrak{B})$ $(i=1,2,3)$ *for every prime number* p *and every positive integer* k. This result provides us in turn with an exhaustive description of all arithmetical types of Abelian groups; in meta-mathematical interpretation this amounts to the description of all *complete* and *consistent* extensions of the arithmetic of Abelian groups. The notion of arithmetical equivalence is related to that of isomorphism; in fact the two notions coincide when applied to finite groups, in general, however, the notion of arithmetical equivalence is much weaker than that of isomorphism. This follows, if from nothing else, from the fact that for every infinite Abelian group there is an arithmetically equivalent group of an arbitrary infinite power given in advance. Our fundamental results show also that there are two infinite groups of the same power, for instance two denumerable groups, which are arithmetically equivalent without being isomorphic. In particular if $\mathfrak{A}$ is any group of the second kind and $\mathfrak{B}$ is the direct product of $\mathfrak{A}$ and the additive group of rationals, then $\mathfrak{A}$ and $\mathfrak{B}$ are always arithmetically equivalent though in general they are not isomorphic.

A class of Abelian groups is called *arithmetically closed* if together with any Abelian group $\mathfrak{A}$ it also contains all groups which are arithmetically equivalent to $\mathfrak{A}$. The family of all arithmetically closed classes is much more comprehensive than that of all arithmetical classes. Above we have given examples of classes of Abelian groups which are not arithmetical. Among them the class of all finite groups, all simple groups and all torsion-free groups are arithmetically closed, while the classes of all infinite cyclic groups and of all torsion groups are not even arithmetically closed. Every arithmetical type is an arithmetically closed class (without being in general an arithmetical class); an arithmetically closed class can be characterized as a class which is a union of finitely or infinitely many arithmetical types.

The notion of an arithmetical class and all the related notions can be extended from Abelian groups to arbitrary algebras $\mathfrak{A}=\langle A,+\rangle$ (and even, more generally, to arbitrary algebraic systems formed by a set and a sequence of finitary operations under which this set is closed). In particular the class of Abelian groups is an arithmetical subclass of the class of all algebras $\mathfrak{A}=\langle A,+\rangle$, and so is the class of all groups. From the results obtained in the discussion of arithmetical classes of Abelian groups some conclusions can be derived which concern arithmetical classes of arbitrary algebras. Thus, *e. g.*, it turns out that the class of all algebras with one generator, the class of all directly indecomposable algebras and that of all simple algebras are not arithmetical; all these classes are not even arithmetically closed.

The present paper contains the first application in literature of the technique elaborated by Tarski in his theory of arithmetical classes. For the convenience of the reader we give in Chapter 2 a short summary of [12] in which the mathematical definitions of arithmetical classes and related notions, and the fundamental theorems concerning these notions are explicity formulated.

Chapter 1. Set-theoretical notation; auxiliary notions from the theory of Abelian groups

Let the variables $i,x,y,\ldots$ represent arbitrary entities and the variables $I,X,Y,\ldots$ arbitrary sets. The formula

$$x,y,\ldots \in X, \quad \text{or} \quad x,y,\ldots \notin X,$$

will express, as usual, the fact that the elements $x,y,\ldots$ *belong*, or *do not belong*, to X. By

$$\underset{x\in X}{E}(\ldots)$$

where the dots in the parentheses stand for a formula involving x, we mean the set of all elements x in X which satisfy this formula. The formula $X\subseteq Y$ expresses the fact that the set X *is contained* in Y (*i. e.*, is a *subset* of Y). The expressions $X\cup Y$, $X\cap Y$, and $X-Y$ respectively denote the *union*, the *intersection*, and the *difference* of the sets X and Y. The *empty* set will be denoted by 0.

The variables f and g will be used to denote arbitrary *functions*. By $D(f)$ we denote the *domain* of a function f; X being a subset of $D(f)$, the function obtained from f by restricting its domain to X is denoted by $f|X$. To represent function values of a function f we shall sometimes use the notation f_x or $f^{(x)}$, instead of the ordinary notation $f(x)$. This will always be applied to those special functions which are defined below as *sequences*. Whenever we decide to apply this notation, we shall use as the variable denoting the function itself not one of the letters f and g, but one of those variables which will be chosen to represent the function values. For instance, we may use X to denote a function whose values are sets; then X_i denotes the function value correlated with an element i of $D(X)$. Given a function X of this kind and an arbitrary set I contained in $D(X)$, the expressions

$$\bigcup_{i\in I} X_i \quad \text{and} \quad \bigcap_{i\in I} X$$

denote the *union* and the *intersection* of all sets X_i with $i\in I$. Furthermore

$$\prod_{i\in I} X_i$$

denotes the *cardinal* (or *Cartesian*) *product* of all sets X_i with $i\in I$, *i. e.*, the set of all functions f such that $D(f)=I$, and $f(i)\in X_i$ for every $i\in I$. If in particular all the sets X_i are identical with a given set Y, the cardinal product is called the *cardinal power* of Y with the *exponent* I and is denoted by Y^I. Thus Y^I is the set of all functions on I to Y, *i. e.*, of all functions whose domain is I and whose *range* (counter domain) is contained in Y. If I is the set consisting of the two numbers 0 and 1, and if $X_0=Y$ and $X_1=Z$, we set

$$\prod_{i\in I} X_i = Y\times Z.$$

The notion of an *ordinal number* is assumed to be known. It proves convenient to assume that the ordinal numbers have been constructed in set theory in such a way that every ordinal ν coincides with the set of all ordinals smaller than ν. The only ordinals which will be involved in our discussion are the finite ordinals and the ordinal ω, *i. e.*, the smallest transfinite ordinal. The finite ordinals are identified with non-negative integers, and hence ω is the set of all non-negative integers. $\boldsymbol{N}$ will denote the set of all positive integers (natural numbers) and $\boldsymbol{P}$ will denote the set of all prime numbers. It proves convenient to take as *cardinal numbers* special ordinals; namely the smallest ones among all ordinals of the same power. In particular all finite ordinals and the ordinal ω are cardinals.

A function whose domain is a non-negative integer n is referred to as a *finite sequence* and specifically as an *n-termed sequence*; a function whose domain is ω is called an *infinite sequence*. For an n-termed sequence x we shall use the alternative designation $\langle x_0,\ldots,x_{n-1}\rangle$; on the other hand, the range of this sequence x, *i. e.*, the set of all its terms, will be denoted by $\{x_0,\ldots,x_{n-1}\}$. In agreement with our previous convention, X^n denotes the set of all n-termed sequences x with all the terms $x_0,\ldots,x_{n-1}$ in X; similarly for X^ω. However, the symbol m^n where m and n are two non-negative integers will mostly be used in its ordinary arithmetical sense; in those few cases in which this symbol is used to denote the set of all n-termed sequences whose terms are less than m, the special meaning of this symbol will be clear from the context.

By an *algebra* we understand a system constituted by a certain non-empty set A and certain operations $O_1,\ldots,O_{n-1}$ with the assumption that the set A is closed under the operations $O_1,\ldots,O_{n-1}$, *i. e.*, that the operations are performable on arbitrary elements of A, and always yield again an element of A. Formally an algebra can be treated as an n-termed sequence whose 0th term is the set A and the remaining terms are the operations O_i, $1\leqslant i<n$. In this paper we shall be concerned almost ex-

clusively with the case when $n=2$ and the only operation O_1 of the algebra is a binary one. The set A will actually be referred to as $\mathfrak{A}_0$ while for the operation O_1 we shall always use the symbol $+$; hence the notation

$$\mathfrak{A}=\langle\mathfrak{A}_0,+\rangle.$$

The set of all such algebras will be denoted by $\mathcal{A}$.

We shall not always strictly distinguish between an algebra $\mathfrak{A}$ and the correlated set $\mathfrak{A}_0$. Thus instead of elements of $\mathfrak{A}_0$ we shall sometimes speak of elements of the algebra $\mathfrak{A}$ itself. Similarly we shall speak of the power (cardinal number) of an algebra $\mathfrak{A}$, of finite, denumerable (*i. e.*, infinitely denumerable) algebras. The set of all finite algebras in $\mathcal{A}$ will be denoted by $\mathcal{F}$, and that of all n-element algebras in $\mathcal{A}$ by $\mathcal{A}_n$.

Various general algebraic notions, such as a *subalgebra*, a subalgebra *generated by a set of elements*, an algebra *with n generators*, *isomorphism*, *homomorphism*, a *simple* algebra, etc. are assumed to be known; the formula $\mathfrak{A}\cong\mathfrak{B}$ expresses the fact that the algebras $\mathfrak{A}$ and $\mathfrak{B}$ are isomorphic. By the *cardinal* (or *direct*) *product* of algebras $\mathfrak{A}^{(i)}=\langle\mathfrak{A}_0^{(i)},+\rangle$, with i ranging over the elements of a set I, we understand the algebra $\mathfrak{P}=\langle\mathfrak{P}_0,+\rangle$ defined in the following way:

$$\mathfrak{P}_0=\prod_{i\in I}\mathfrak{A}_0^{(i)};$$

f,g being any two functions in $\mathfrak{P}_0$, $f+g$ is the function h such that $D(h)=I$, and $h(i)=f(i)+g(i)$ for every $i\in I$. The fact that the algebra $\mathfrak{P}$ is the cardinal product of $\mathfrak{A}^{(i)}$ with $i\in I$ is expressed by

$$\mathfrak{P}=\prod_{i\in I}\mathfrak{A}^{(i)}.$$

As particular cases of this notion we obtain (as in the case of the cardinal product of sets) the *power* of an algebra, $\mathfrak{B}^I$, and the *cardinal product* of two algebras, $\mathfrak{B}\times\mathfrak{C}$. An algebra $\mathfrak{A}$ is called *indecomposable* (or *directly indecomposable*), if $\mathfrak{A}\notin\mathcal{A}_1$ and if, for any algebras $\mathfrak{B}$ and $\mathfrak{C}$, $\mathfrak{A}\cong\mathfrak{B}\times\mathfrak{C}$ implies that either $\mathfrak{B}\in\mathcal{A}_1$ or $\mathfrak{C}\in\mathcal{A}_1$.

The *Abelian groups* form a subset of $\mathcal{A}$, denoted by $\mathcal{AG}$. The familiar definition of this notion follows:

Definition 1.1. $\mathcal{AG}$ is *the set consisting of all algebras* $\mathfrak{A}=\langle\mathfrak{A}_0,+\rangle$ for which the following three postulates hold:

(i) *For all* x *and* y, $x+y=y+x$,

(ii) *for all* x, y, *and* z, $(x+y)+z=x+(y+z)$,

(iii) *for all* x *and* y *there exists a* z *such that* $x+z=y$.

(The variables x, y, and z are assumed to range over the elements of the set $\mathfrak{A}_0$.)

The most familiar example of an Abelian group is the additive group of integers. This group will be denoted by $\mathfrak{Z}$, hence $\mathfrak{Z}_0$ will denote the set of all integers. The familiar arithmetical notation used for the group $\mathfrak{Z}$ naturally extends to arbitrary Abelian groups. Thus, for any given Abelian group $\mathfrak{A}$, the symbols 0, $-x$, $x-y$, $\sum_{i<n}x_i$ (n — a non-negative integer), and kx (k — an arbitrary integer) are employed in their usual sense. Two elements $x,y\in\mathfrak{A}_0$ are called *congruent modulo* m, in symbols

$$x\equiv y\,(\mathrm{mod}\,m),$$

if for some element $z\in\mathfrak{A}_0$

$$x=y+mz.$$

The formula $x\not\equiv y\,(\mathrm{mod}\,m)$ expresses, of course, the fact that x and y are not congruent modulo m. The use of the formulas $x\equiv y\,(\mathrm{mod}\,m)$ and $x\not\equiv y\,(\mathrm{mod}\,m)$ will be restricted almost entirely to the case when $y=0$. In this particular case we read the formulas: x *is divisible by* m and x *is not divisible by* m, respectively.

For further references we list some elementary properties of congruences:

Theorem 1.2. *Given a group* $\mathfrak{A}\in\mathcal{AG}$, *for all elements* $x,y\in\mathfrak{A}_0$ *and for all integers* m,n,r *we have*

(i) *if* $x\equiv 0\,(\mathrm{mod}\,m)$ *and* $y\equiv 0\,(\mathrm{mod}\,m)$, *then* $x+y\equiv 0\,(\mathrm{mod}\,m)$ *and* $x-y\equiv 0\,(\mathrm{mod}\,m)$,

(ii) $mx\equiv 0\,(\mathrm{mod}\,m)$,

(iii) *if* $nx\equiv 0\,(\mathrm{mod}\,m)$ *and* $n_1x\equiv 0\,(\mathrm{mod}\,m)$, *then* $(n,n_1)x\equiv 0\,(\mathrm{mod}\,m)$,

(iv) *if* $x\equiv 0\,(\mathrm{mod}\,m)$, *then* $-x\equiv 0\,(\mathrm{mod}\,m)$,

(v) *if* $x\equiv 0\,(\mathrm{mod}\,m)$, *then* $nx\equiv 0\,(\mathrm{mod}\,nm)$,

(vi) *if* $x\equiv 0\,(\mathrm{mod}\,mn)$, *then* $x\equiv 0\,(\mathrm{mod}\,m)$,

(vii) *if* $(m,n)=1$, $x\equiv 0\,(\mathrm{mod}\,m)$ *and* $x\equiv 0\,(\mathrm{mod}\,n)$, *then* $x\equiv 0\,(\mathrm{mod}\,mn)$,

(viii) *if* $(m,n)=1$ *and* $nx\equiv 0\,(\mathrm{mod}\,m)$, *then* $x\equiv 0\,(\mathrm{mod}\,m)$.

The proof is quite elementary. The symbol (m,n) denotes as usual the greatest common divisor of the integers m and n.

The notion of the *order* of an element x is certainly familiar to the reader. For a finite group $\mathfrak{A}$, the terms "the order of the group $\mathfrak{A}$" and "the *power* of the group $\mathfrak{A}$" are used interchangably.

In the theory of Abelian groups we apply the general algebraic notions listed previously as well as some related notions of a more specialized nature, such as a *subgroup*, a *cyclic* group (a group with one generator), and a *quotient* group $\mathfrak{A}/\mathfrak{B}$ (where $\mathfrak{B}$ is a subgroup of $\mathfrak{A}$). The following subgroups of an Abelian group $\mathfrak{A}$ are especially important for

our purposes: the group $\mathfrak{Z}$ consisting of the only element 0, the group ${}_m\mathfrak{A}$ consisting of all elements $x \in \mathfrak{A}_0$ with $mx=0$, and the group $m\mathfrak{A}$ consisting of all elements $x \in \mathfrak{A}_0$ which are divisible by m; the quotient group $\mathfrak{A}/m\mathfrak{A}$ will be denoted by ${}^m\mathfrak{A}$.

If for some $m>0$ we have $m\mathfrak{A}=\mathfrak{Z}$, we call $\mathfrak{A}$ a group *of the first kind*, symbolically $\mathfrak{A} \in \mathcal{AG}_1$, otherwise *of the second kind*, symbolically $\mathfrak{A} \in \mathcal{AG}_2$.

It proves convenient to assume that for an arbitrary Abelian group $\mathfrak{A}$

$$\mathfrak{A}^0 = \mathfrak{Z}.$$

Besides cardinal product of Abelian groups we use (and even more frequently) the so-called *weak cardinal product*. The weak cardinal product of Abelian groups $\mathfrak{A}^{(i)}$ with $i \in I$ is the subgroup of $\prod_{i \in I} \mathfrak{A}^{(i)}$ constituted by all the functions f satisfying the following condition: there are at most finitely many elements $i \in I$ for which $f(i)$ differs from the zero-element of $\mathfrak{A}^{(i)}$. Analogously we define the notion of the *weak cardinal power* of a group. To construct the weak cardinal product of an infinite sequence of groups $\mathfrak{A}^{(i)}$ or the *weak ω-power* of a group $\mathfrak{B}$ we can use (instead of infinite sequences in which almost all terms are zeros) finite sequences with arbitrary number of terms. For instance, we may define the weak ω-power of the group $\mathfrak{I}$ of integers as the group $\mathfrak{A}$ constructed in the following way: $\mathfrak{A}_0$ is the set of all finite sequences of integers; a being an m-termed sequence and b an n-termed sequence of integers we set

$$a+b = \langle a_0+b_0, \dots, a_{m-1}+b_{m-1}, b_m, \dots, b_{n-1}\rangle \quad \text{in case} \quad m \leqslant n,$$
$$a+b = \langle a_0+b_0, \dots, a_{n-1}+b_{n-1}, a_n, \dots, a_{m-1}\rangle \quad \text{in case} \quad m > n.$$

Hence the symbols like $-a$, ka, $a \dot{-} b$ automatically acquire a definite meaning for arbitrary finite sequences a and b of integers (and for an arbitrary integer k); for instance

$$ka = \langle ka_0, \dots, ka_{m-1}\rangle.$$

In addition to the group $\mathfrak{I}$, there are some other Abelian groups which are of special importance for our further discussion and for which, therefore, we introduce special symbols. Thus $\mathfrak{R}$ is the additive group of all rationals, and for any given prime number p, $\mathfrak{R}_p$ is the subgroup of $\mathfrak{R}$ constituted by all rationals m/n with $(n,p)=1$. Again, for any given prime number p, $\mathfrak{C}_p$ is the group constituted by all rationals of the form m/p^k with $0 \leqslant m/p^k < 1$ (m and k — arbitrary non-negative integers). The group operation in $\mathfrak{C}_p$ is addition modulo 1, *i. e.*, x and y being any two elements of $\mathfrak{R}_p$, $x+y$ is the unique element of $\mathfrak{C}_p$ which is congruent

modulo 1 to the ordinary arithmetical sum of x and y. Finally, for any given prime number p and for any positive integer k, $\mathfrak{C}_{p^k}$ is the subgroup of $\mathfrak{C}_p$ constituted by all elements of $\mathfrak{C}_p$ which are of the form m/p^k.

The remaining part of this section is devoted to a somewhat more detailed discussion of a few less familiar notions of the theory of Abelian groups:

Definition 1.3. Let $\mathfrak{A}$ be an Abelian group, let m and n be non-negative integers, and let x be a sequence in $\mathfrak{A}_0^n$.

(i) We say that the elements $x_0, \dots, x_{n-1}$ are *independent modulo m* if for every sequence $a \in \mathfrak{I}_0^n$ the formula

$$\sum_{i<n} a_i x_i = 0$$

always implies

$$a_i \equiv 0 \pmod m \quad \text{for} \quad i = 0,1,\dots,n-1.$$

(ii) We say that the elements $x_0, \dots, x_{n-1}$ are *strongly independent modulo m* if for every sequence $a \in \mathfrak{I}_0^n$ the formula

$$\sum_{i<n} a_i x = 0 \pmod m$$

always implies

$$a_i \equiv 0 \pmod m \quad \text{for} \quad i = 0,1,\dots,n-1.$$

The first of the two notions just defined is known in literature as *linear independence modulo m* [9]).

In what follows Definition 1.3 will be applied only in the case when m is a power of a prime. In this particular case the following transformation of 1.3 proves possible and useful:

THEOREM 1.4. *Let $\mathfrak{A} \in \mathcal{AG}$, p be a prime, $k>0$, $n \geqslant 0$, and $x \in \mathfrak{A}_0^n$. For $x_0, \dots, x_{n-1}$ to be* (i) *independent, or* (ii) *strongly independent modulo p^k, it is necessary and sufficient that for every sequence $a \in \mathfrak{I}_0^n$ the formula*

$$\text{(i)} \quad p^{k-1} \sum_{i<n} a_i x_i = 0, \qquad \text{or} \qquad \text{(ii)} \quad p^{k-1} \sum_{i<n} a_i x_i \equiv 0 \pmod{p^k}$$

always implies

$$a_i \equiv 0 \pmod p \quad \text{for} \quad i = 0,1,\dots,n-1.$$

Definition 1.5. Given any group $\mathfrak{A} \in \mathcal{AG}$, any prime p, and any integer $k>0$, we define the ith *rank modulo p^k* of $\mathfrak{A}$ ($i=0,1,2,3$), in symbols

$$\varrho^{(i)}[p,k](\mathfrak{A}),$$

[9]) See footnote 8 on page 205.

as the maximum finite number, if it exists, of elements in $\mathfrak{A}_0$ which are

for $i=0$ *independent modulo* p^k,
for $i=1$ *of order* p^k *and independent modulo* p^k,
for $i=2$ *strongly independent modulo* p^k,
for $i=3$ *of order* p^k *and strongly independent modulo* p^k;

if such a maximum number does not exist, we set

$$\varrho^{(i)}[p,k](\mathfrak{A})=\infty.$$

Instead of "$\varrho^{(0)}$" we shall write simply "ϱ".

It follows from Theorem 1.4 that $\varrho[p,k](\mathfrak{A})=n$ $(n\geqslant 0)$ implies the existence of at least p^n different elements in $p^{k-1}\mathfrak{A}$, also that $p^{k-1}\mathfrak{A}$ is infinite whenever $\varrho[p,k](\mathfrak{A})=\infty$. The analogous statements for the ranks $\varrho^{(1)}[p,k]$, $\varrho^{(2)}[p,k]$ and $\varrho^{(3)}[p,k]$ are stronger:

THEOREM 1.6. *Let* $\mathfrak{A}\in\mathcal{AG}$, p *be a prime,* $k>0$ *and* $n\geqslant 0$. *Then we have*

$$\varrho^{(i)}[p,k](\mathfrak{A})=n \quad (\text{or } \varrho^{(i)}[p,k](\mathfrak{A})=\infty) \qquad (i=1,2,3)$$

if and only if there are exactly p^n *(or infinitely many)*

for $i=1$ *different elements in* ${}_p(p^{k-1}\mathfrak{A})$,
for $i=2$ *elements incongruent modulo* p^k *in* $p^{k-1}\mathfrak{A}$,
for $i=3$ *elements incongruent modulo* p^k *in* ${}_p(p^{k-1}\mathfrak{A})$.

Proof. We shall prove the theorem only for $i=1$. The proofs in the remaining cases are analogous.

Assume that $\varrho^{(1)}[p,k](\mathfrak{A})=n$. Then there exist elements $x_0,x_1,\ldots,x_{n-1}\in\mathfrak{A}_0$ which are of order p^k and independent modulo p^k. The elements $p^{k-1}\sum_{i<n}a_ix_i$ belong to ${}_p(p^{k-1}\mathfrak{A})$ and by Theorem 1.4 they are different for different sequences $a\in p^n$. Hence there are at least p^n different elements in ${}_p(p^{k-1}\mathfrak{A})$.

Let us take an arbitrary element $y=p^{k-1}x_n\in{}_p(p^{k-1}\mathfrak{A})$. Thus

$$p^kx_n=0. \tag{1}$$

The elements $x_0,x_1,\ldots,x_{n-1},x_n$ are not linearly independent modulo p^k, hence there is a sequence $a\in p^{n+1}$ such that

$$p^{k-1}\sum_{i<n+1}a_ix_i=0, \tag{2}$$

but (see (1)) $a_n\not\equiv 0\pmod p$. Thus for some integers r and s we have

$$ra_n+sp=-1. \tag{3}$$

From (1)-(3) we obtain

$$y=p^{k-1}x_n=p^{k-1}\sum_{i<n}(ra_i)x_i=p^{k-1}\sum_{i<n}b_ix_i$$

where $ra_i\equiv b_i\pmod p$ and $b\in p^n$. Hence the group ${}_p(p^{k-1}\mathfrak{A})$ consists of exactly p^n elements.

If $\varrho^{(1)}[p,k](\mathfrak{A})=\infty$, then for each natural n we can find p^n different elements in ${}_p(p^{n-1}\mathfrak{A})$. Hence the group ${}_p(p^{k-1}\mathfrak{A})$ is infinite.

The proof in the opposite direction is obvious.

It can easily be checked that for every prime p and for every integer $k>0$ there is

$$\varrho^{(1)}[p,k](\mathfrak{A})=\varrho[p,k]({}_{p^k}\mathfrak{A}) \quad \text{and} \quad \varrho^{(2)}[p,k](\mathfrak{A})=\varrho[p,k](p^k\mathfrak{A}).$$

The connection between $\varrho^{(3)}$ and ϱ is a little more involved. To state it we start with the following two lemmata:

LEMMA 1. *Let* $\mathfrak{A}\in\mathcal{AG}$. *If*

(4) *the elements* $x_0,\ldots,x_{m-1}\in\mathfrak{A}_0$ $(m\geqslant 0)$ *are of order* p^{k+1} *and linearly independent modulo* p^{k+1}

and

(5) *the elements* $y_0,\ldots,y_{n-1}\in\mathfrak{A}_0$ $(n\geqslant 0)$ *are of order* p^k *and linearly independent modulo* p^k *in the stronger sense,*

then

(6) *the elements* $px_0,\ldots,px_{m-1},y_0,\ldots,y_{n-1}\in\mathfrak{A}_0$ *are of order* p^k *and linearly independent modulo* p^k.

Proof. In fact,

$$p^{k-1}\Big(\sum_{i<m}a_i(px_i)+\sum_{i<n}b_iy_i\Big)=0 \tag{7}$$

implies $p^{k-1}\sum_{i<n}b_iy_i\equiv 0\pmod{p^k}$ from which it follows by (5) that

$$b_i\equiv 0\pmod p \quad \text{for} \quad i=0,1,\ldots,n-1. \tag{8}$$

Now we obtain from (5), (7), and (8) that $p^k\sum_{i<m}a_ix_i=0$, which implies by (4)

$$a_i\equiv 0\pmod p \quad \text{for} \quad i=0,1,\ldots,m-1.$$

LEMMA 2. *Let* $\mathfrak{A}\in\mathcal{AG}$. *If*

(9) *the elements* $x_0,\ldots,x_{m-1}\in\mathfrak{A}_0$ $(m\geqslant 0)$ *are linearly independent modulo* p^{k+1} *in the stronger sense*

and

(10) *the elements* $y_0,\ldots,y_{n-1}\in\mathfrak{A}_0$ $(n\geqslant 0)$ *are of order* p^k *and linearly independent modulo* p^k *in the stronger sense,*

then

(11) *the elements* $x_0,\ldots,x_{m-1},y_0,\ldots,y_{n-1}\in\mathfrak{A}_0$ *are linearly independent modulo* p^k *in the stronger sense.*

Proof. In fact

$$p^{k-1}\Big(\sum_{i<m} a_i x_i + \sum_{i<n} b_i y\Big) \equiv 0 \pmod{p^k} \tag{12}$$

it follows by (10) that $p^k \sum_{i<m} a_i x_i \equiv 0 \pmod{p^{k+1}}$ which implies by (9)

$$a_i \equiv 0 \pmod{p} \quad \text{for} \quad i = 0,1,\ldots,m-1. \tag{13}$$

Now we obtain from (12) and (13) $p^{k-1} \sum_{i<m} b_i y_i \equiv 0 \pmod{p^k}$ which implies by (10)

$$b_i \equiv 0 \pmod{p} \quad \text{for} \quad i = 0,1,\ldots,n-1.$$

THEOREM 1.7. *Let $\mathfrak{A} \in \mathcal{AG}$. For every prime p and for every integer $k>0$ we have*

$$\varrho^{(i)}[p,k](\mathfrak{A}) = \varrho^{(i)}[p,k+1](\mathfrak{A}) + \varrho^{(3)}[p,k](\mathfrak{A}) \quad \text{for} \quad i = 1,2.$$

Proof. It is sufficient to show that for every $r \geqslant 0$ the condition

$$\varrho^{(i)}[p,k](\mathfrak{A}) \geqslant r \tag{14}$$

holds if and only if

$$\varrho^{(i)}[p,k+1](\mathfrak{A}) + \varrho^{(3)}[p,k](\mathfrak{A}) \geqslant r. \tag{15}$$

From Lemmata 1 and 2 it follows immediately that (15) implies (14) for $i=1,2$. The proof in the opposite direction follows by induction with respect to r. Assume that for some $r \geqslant 0$ the condition (14) implies (15) and let

$$\varrho^{(i)}[p,k](\mathfrak{A}) \geqslant r+1. \tag{16}$$

By our inductive assumption (16) implies (15), thus there are integers $m,n \geqslant 0$ such that $m+n=r$, $\varrho^{(i)}[p,k+1](\mathfrak{A}) \geqslant m$ and $\varrho^{(3)}[p,k](\mathfrak{A}) \geqslant n$.

We carry out the proof for $i=1$. Suppose (4) and (5). Thus by Lemma 1 we obtain (6). It can easily be seen that (6) and (16) imply the existence of an element $z \in \mathfrak{A}_0$ such that

(17) *the elements $px_0,\ldots,px_{m-1},y_0,\ldots,y_{n-1},z$ are of order p^k and linearly independent modulo p^k.*

We assert that one of the two following conditions holds: Either

(18) *the elements $y_0,\ldots,y_{n-1},z$ are of order p^k and linearly independent modulo p^k in the stronger sense,*

or there exists an element $z' \in \mathfrak{A}_0$ such that

(19) *the elements $x_0,\ldots,x_{m-1},z'$ are of order p^{k+1} and linearly independent modulo p^{k+1}.*

In fact, if (18) does not hold, then there is a sequence $b \in \omega^{n+1}$ and an integer l, $0 \leqslant l \leqslant n$, such that

$$p^{k-1}\Big(\sum_{i<n} b_i y_i + b_n z\Big) \equiv 0 \pmod{p^k}, \tag{20}$$

$$b_l \not\equiv 0 \pmod{p}. \tag{21}$$

From (20) we have

$$p^{k-1}\Big(\sum_{i<n} b_i y_i + b_n z\Big) = p^k z' \tag{22}$$

for some $z' \in \mathfrak{A}_0$. Suppose now that for a sequence $a \in \omega^{m+1}$ we have $p^k\Big(\sum_{i<m} a_i x_i + a_m z'\Big) = 0$; then by (22)

$$p^{k-1}\Big(\sum_{i<m} a_i (px_i) + a_m\Big(\sum_{i<n} b_i y_i + b_n z\Big)\Big) = 0,$$

by (17)

$$a_i \equiv 0 \pmod{p} \quad \text{for} \quad i = 0,1,\ldots,m-1 \quad \text{and} \quad a_m \cdot b_l \equiv 0 \pmod{p},$$

which together with (21) gives us $a_m \equiv 0 \pmod{p}$. Thus (19) holds.

By (4), (5), and each of the conditions (18) and (19) we conclude that $\varrho^{(i)}[p,k+1](\mathfrak{A}) + \varrho^{(3)}[p,k](\mathfrak{A}) \geqslant r+1$.

We carry out the proof for $i=2$. Suppose (9) and (10). Thus by Lemma 2 we obtain (11). It is easy to see that (11) and (16) imply the existence of an element $z \in \mathfrak{A}_0$ such that

(23) *the elements $x_0,\ldots,x_{m-1},y_0,\ldots,y_{n-1},z$ are linearly independent modulo p^k in the stronger sense.*

We assert that one of the following two conditions holds: Either

(24) *the elements $x_0,\ldots,x_{m-1},z$ are linearly independent modulo p^{k+1} in the stronger sense,*

or there exists an element $z' \in \mathfrak{A}_0$ such that

(25) *the elements $y_0,\ldots,y_{n-1},z'$ are of order p^k and linearly independent modulo p^k in the stronger sense.*

In fact, if (24) does not hold, then there is a sequence $a \in \omega^{m+1}$ and an integer l, $0 \leqslant l < m$, such that

$$p^k\Big(\sum_{i<m} a_i x_i + a_m z\Big) \equiv 0 \pmod{p^{k+1}}, \tag{26}$$

$$a_l \not\equiv 0 \pmod{p}. \tag{27}$$

Let

$$w = \sum_{i<m} a_i x_i + a_m z. \tag{28}$$

It follows from (23) and (27) that

$$p^{k-1}w \not\equiv 0 \pmod{p^k}, \tag{29}$$

then by (26), (28) and (29) there are elements $z', w' \in \mathfrak{A}_0$ such that $p^k w = p^{k+1}w'$ and

$$p^{k-1}w = p^k w' + p^{k-1}z', \tag{30}$$

where $p^{k-1}z' \not\equiv 0 \pmod{p^k}$ and $p^k z' = 0$. Assume now that for a sequence $b \in \omega^{n+1}$ there is

$$p^{k-1}\Big(\sum_{i<n} b_i y_i + b_n z'\Big) \equiv 0 \pmod{p^k}.$$

Then from (28) and (30) we obtain

$$p^{k-1}\Big(\sum_{i<n} b_i y_i + b_n\Big(\sum_{i<m} a_i x_i + a\, z_m\Big)\Big) \equiv 0 \pmod{p^k};$$

from (23) it follows that $b_i \equiv 0 \pmod{p}$ for $i = 0,1,\ldots,n-1$ and that $b_n a_l \equiv 0 \pmod{p}$, which together with (27) gives us $b_n \equiv 0 \pmod{p}$. Thus (25) holds.

By (9), (10) and each of the conditions (24) and (25) we conclude that

$$\varrho^{(2)}[p,k+1](\mathfrak{A}) + \varrho^{(3)}[p,k](\mathfrak{A}) \geqslant r+1.$$

Hence the proof is completed.

For fixed $\mathfrak{A}$, p, and i ($i=1$ or $i=2$) let

$$f(k) = \varrho^{(i)}[p,k](\mathfrak{A}) \quad \text{and} \quad g(k) = \varrho^{(3)}[p,k](\mathfrak{A}).$$

Then by Theorem 1.7 we have

$$f(k) = f(k+1) + g(k). \tag{31}$$

Consider now two arbitrary functions $f, g \in (\omega + \{\infty\})^N$ satisfying equality (31). It follows immediately from (31) that

$$f(k) \geqslant f(k+1), \qquad f(k) \geqslant g(k), \tag{32}$$

$$f(k) = f(k+l) + \sum_{j<l} g(k+j) \quad \text{for} \quad l = 1,2,\ldots \tag{33}$$

The last equality implies $f(k) \geqslant \sum_{j<l} g(k+j)$ for $l = 1,2,\ldots$, hence

$$f(k) \geqslant \sum_{j\in\omega} g(k+j). \tag{34}$$

Assume now that $f(k_0) = 0$ for some $k_0 > 0$. In this case we have

$$f(k) = \sum_{j\in\omega} g(k+j). \tag{35}$$

In fact, with respect to (32) and (34) it is obvious in case $k \geqslant k_0$ and follows from (33) in case $k_0 = k+l$ for some $l \geqslant 1$.

Returning to the ranks, we obtain by (34) and (35) the following

THEOREM 1.8. *Let $\mathfrak{A} \in \mathcal{AG}$. For every prime p and for every integer $k > 0$ we have*

$$\varrho^{(i)}[p,k](\mathfrak{A}) \geqslant \sum_{j<\omega} \varrho^{(3)}[p,k+j](\mathfrak{A}) \qquad (i=1,2).$$

The equality

$$\varrho^{(i)}[p,k](\mathfrak{A}) = \sum_{j<\omega} \varrho^{(3)}[p,k+j](\mathfrak{A}) \qquad (i=1,2)$$

holds whenever for some $k_0 > 0$ we have $\varrho^{(i)}[p,k_0](\mathfrak{A}) = 0$.

Let us consider now the special groups mentioned on page 212 and 213. It is quite easy to determine their ranks.

THEOREM 1.9. *For arbitrary primes p and q and for arbitrary positive integers k and l we have*

$$\varrho^{(i)}[p,k](\mathfrak{Z}) = 0 \qquad (i=1,2,3),$$

$$\varrho^{(i)}[p,k](\mathfrak{R}) = 0 \qquad (i=1,2,3),$$

$$\varrho^{(2)}[p,k](\mathfrak{R}_q) = \begin{cases} 1 & \text{if} \quad p=q \\ 0 & \text{otherwise} \end{cases}$$

$$\varrho^{(i)}[p,k](\mathfrak{R}_q) = 0 \qquad (i=1,3),$$

$$\varrho^{(i)}[p,k](\mathfrak{C}_q) = \begin{cases} 1 & \text{if} \quad p=q \\ 0 & \text{otherwise} \end{cases}$$

$$\varrho^{(i)}[p,k](\mathfrak{C}_q) = 0 \qquad (i=2,3),$$

$$\varrho^{(3)}[p,k](\mathfrak{C}_{ql}) = \begin{cases} 1 & \text{if} \quad p=q \quad \text{and} \quad k=l \\ 0 & \text{otherwise} \end{cases}$$

$$\varrho^{(i)}[p,k](\mathfrak{C}_{ql}) = \begin{cases} 1 & \text{if} \quad p=q \quad \text{and} \quad k \leqslant l \\ 0 & \text{otherwise} \end{cases} \qquad (i=1,2).$$

Also the following theorem determining the ranks of cardinal products of algebras can be proved without any difficulties:

THEOREM 1.10. *For arbitrary groups $\mathfrak{A}^{(j)} \in \mathcal{AG}$ with j ranging over elements of a set J we have*

$$\varrho^{(i)}[p,k]\Big(\prod_{j\in J} \mathfrak{A}^{(j)}\Big) = \sum_{j\in J} \varrho^{(i)}[p,k](\mathfrak{A}^{(j)}) \qquad (i=1,2,3)$$

for any prime p and for any integer $k > 0$.

Let us consider now an arbitrary Abelian group $\mathfrak{A}$ of the first kind (see page 212). Since the cyclic group of order p^k is isomorphic to the

group $\mathfrak{C}_{pk}$, there exists a uniquely determined function α such that $\alpha(p,k)$ is a cardinal number and

(36) $\alpha(p,k)\neq 0$ for at most finitely many couples $\langle p,k\rangle$,

(37) $$\mathfrak{A}\cong\prod_{p\in P}\prod_{k\in N}\mathfrak{C}_{pk}^{\alpha(p,k)}$$ [10]).

Using Theorems 1.9 and 1.10 we obtain from (37)

(38) $$\varrho^{(3)}[p,k](\mathfrak{A})=\begin{cases}\alpha(p,k) & \text{whenever } \alpha(p,k) \text{ is finite}\\ \infty & \text{whenever } \alpha(p,k) \text{ is infinite.}\end{cases}$$

If $n\mathfrak{A}=\mathfrak{Z}$, then from (37) we get

(39) $$\mathfrak{A}\cong\prod_{\langle p,k\rangle\in Q}\mathfrak{C}_{pk}^{\alpha(p,k)}$$

where the set $Q\subset\boldsymbol{P}\times\boldsymbol{N}$ is determined by the condition

(40) $\langle p,k\rangle\in Q$ if and only if $n\equiv 0 \pmod{p^k}$.

From (36)-(40) we derive

THEOREM 1.11. *If $\mathfrak{A}\in\mathcal{AG}_1$, then $\varrho^{(i)}[p,k](\mathfrak{A})\neq 0$ for at most finitely many couples $\langle p,k\rangle$ $(i=1,2,3)$. And, in particular, if $n\mathfrak{A}=\mathfrak{Z}$, then*

$$n\not\equiv 0 \pmod{p^k} \quad \textit{implies} \quad \varrho^{(3)}[p,k](\mathfrak{A})=0.$$

In conclusion, we shall prove an important existence-theorem:

THEOREM 1.12. *For three arbitrary functions*

$$\varphi^{(1)},\varphi^{(2)},\varphi^{(3)}\in(\omega+\{\infty\})^{P\times N}$$

satisfying the formula

(41) $\varphi^{(i)}(p,k)=\varphi^{(i)}(p,k+1)+\varphi^{(3)}(p,k)$ *for any* $p\in\boldsymbol{P}$ *and* $k>0$ $(i=1,2)$

there is a group $\mathfrak{A}\in\mathcal{AG}_2$ such that

(42) $\varrho^{(i)}[p,k](\mathfrak{A})=\varphi^{(i)}(p,k)$ *for any* $p\in\boldsymbol{P}$ *and* $k>0$ $(i=1,2,3)$.

If moreover

(43) $\varphi^{(i)}(p,k)\neq 0$ *for at most finitely many couples* $\langle p,k\rangle$ $(i=1,2,3)$

then one can find such a group $\mathfrak{A}$ in $\mathcal{AG}_1$ as well.

Proof. It follows from (39) that with a constant p the functions $\varphi^{(i)}$ $(i=1,2)$ and $\varphi^{(3)}$ together satisfy the functional equation (31). Hence by (33) and (34) we have, for an arbitrary prime p,

(44) $$\varphi^{(i)}(p,k)=\varphi^{(i)}(p,k+l)+\sum_{j<l}\varphi^{(3)}(p,k+j) \qquad (i=1,2),$$

(45) $$\varphi^{(i)}(p,k)\geqslant\sum_{j<\omega}\varphi^{(3)}(p,k+j).$$

[10]) See [3], p. 123 and 156 (the first theorem of Prüfer).

Now let us define two functions $\psi^{(1)},\psi^{(2)}\in(\omega+\{\infty\})^P$ by setting for every prime p

(46) $$\psi^{(i)}(p)=\varphi^{(i)}(p,k_p) \qquad (i=1,2),$$

where k_p is the smallest positive integer, if it exists, such that

(47) $$\varphi^{(3)}(p,l)=0 \quad \text{for} \quad l\geqslant k_p;$$

if such an integer does not exist, we set $\psi^{(i)}(p)=0$.

Consider now the weak (it may also be strong) cardinal product

$$\mathfrak{A}=\prod_{q\in P}\mathfrak{R}_q^{\psi^{(2)}(q)}\times\prod_{q\in P}\mathfrak{C}_q^{\psi^{(1)}(q)}\times\prod_{q\in P}\prod_{l\in N}\mathfrak{C}_{ql}^{\psi^{(3)}(q,l)}.$$

(Remark: For an arbitrary group $\mathfrak{A}$ we set $\mathfrak{A}^\infty=\mathfrak{A}^\omega$.) Using Theorems 1.9 and 1.10 we conclude immediately that for an arbitrary prime p and for an arbitrary integer $k>0$

$$\varrho^{(3)}[p,k](\mathfrak{A})=\varphi^{(3)}(p,k) \text{ and } \varrho^{(i)}[p,k](\mathfrak{A})=\psi^{(i)}(p)+\sum_{j<\omega}\varphi^{(3)}(p,k+j) \ (i=1,2).$$

Suppose that for a prime p there exists an integer $k_p>0$ such that (47) holds. Then by (46) and (44) we have for $k\geqslant k_p$

(48) $$\psi^{(i)}(p)=\varphi^{(i)}(p,k_p)=\varphi^{(i)}(p,k)+\sum_{j<k-k_p}\varphi^{(3)}(p,k_p+j)=\varphi^{(i)}(p,k)$$

and $\sum_{j<\omega}\varphi^{(3)}(p,k+j)=0$, hence $\varrho^{(i)}[p,k](\mathfrak{A})=\varphi^{(i)}(p,k)$; and for $k<k_p$

$$\varrho^{(i)}[p,k](\mathfrak{A})=\varphi^{(i)}(p,k_p)+\sum_{j<k_p-k}\varphi^{(3)}(p,k+j)=\varphi^{(i)}(p,k).$$

If for a prime p such a number k_p does not exist, we have

$$\psi^{(i)}(p)=0 \quad \text{and} \quad \sum_{j<\omega}\varphi^{(3)}(p,k+j)=\infty,$$

hence $\varrho^{(i)}[p,k](\mathfrak{A})=\infty$ and by (45) also $\varphi^{(i)}[p,k](\mathfrak{A})=\infty$.

In this way we have checked that the group $\mathfrak{A}$, and thus also the group $\mathfrak{R}\times\mathfrak{A}$ (see Theorems 1.9 and 1.10), satisfy condition (42). But $\mathfrak{R}\times\mathfrak{A}$ is always of the second kind, while $\mathfrak{A}$ proves to be of the first kind whenever condition (43) is satisfied (since it follows from (48) that in this case $\psi^{(1)}(q)=\psi^{(2)}(q)$ for every $q\in\boldsymbol{P}$). We infer from Theorem 1.11, that if (43) does not hold then there is no group of the first kind satisfying condition (42).

Chapter 2. General properties of arithmetical functions, classes, and types

In the Introduction we have roughly characterized, by using meta-mathematical language, the notion of an arithmetical class and several related notions as applied to Abelian groups. In the present chapter we shall define these notions in a general and purely mathematical way and we shall discuss (without proof) their fundamental properties, restricting ourselves entirely to the facts which are essential for our further study [11]).

We have agreed (in Chapter 1) to denote by $\mathcal{A}$ the set of all algebras $\mathfrak{A}=\langle \mathfrak{A}_0, + \rangle$.

Definition 2.1. By $\boldsymbol{F}$ we denote the set of all functions F such that

$$D(F)=\mathcal{A} \quad \text{and} \quad F(\mathfrak{A}) \subseteq \mathfrak{A}_0^{\omega} \quad \text{for every algebra} \quad \mathfrak{A} \in \mathcal{A}.$$

Definition 2.2. Let F and G be functions in $\boldsymbol{F}$ and let $k \geqslant 0$. Then

(i) The *union* $F \cup G$ and the *intersection* $F \cap G$ of the functions F and G are the functions in $\boldsymbol{F}$ defined by the conditions:

$$F \cup G(\mathfrak{A})=F(\mathfrak{A}) \cup G(\mathfrak{A}) \quad \text{and} \quad F \cap G(\mathfrak{A})=F(\mathfrak{A}) \cap G(\mathfrak{A})$$

for every algebra $\mathfrak{A} \in \mathcal{A}$.

Analogously we define the *union* $\bigcup_{i \in I} H_i$ and the *intersection* $\bigcap_{i \in I} H_i$ for arbitrary functions H_i in $\boldsymbol{F}$ correlated with elements i of a certain set I.

(ii) The *complement* $\overline{F}$ of the function F is a function in $\boldsymbol{F}$ defined by the condition

$$\overline{F}(\mathfrak{A})=\mathfrak{A}_0^{\omega}-F(\mathfrak{A}) \quad \textit{for every algebra } \mathfrak{A} \in \mathcal{A}.$$

(iii) $\vee_k F$ and $\wedge_k F$ are functions in $\boldsymbol{F}$ defined by the conditions

for every algebra $\mathfrak{A}$, $\vee_k F(\mathfrak{A})$ *is the set of all* $x \in \mathfrak{A}_0^{\omega}$ *such that there is a* $y \in F(\mathfrak{A})$ *with* $y_i=x_i$ *for every* $i \neq k$,

for every algebra $\mathfrak{A} \in \mathcal{A}$, $\wedge_k F(\mathfrak{A})$ *is the set of all* $x \in \mathfrak{A}_0^{\omega}$ *such that for every* $y \in \mathfrak{A}_0^{\omega}$, *if* $y_i=x_i$ *for every* $i \neq k$, *then* $y \in F(\mathfrak{A})$.

We shall refer to the operations $\vee_k$ and $\wedge_k$ as the *existential quantification* (or *outer cyliudrification*) and the *universal quantification* (or *inner cylindrification*) with respect to k.

[11]) Confront with the last section of the Introduction. For the intuitive content of the notions introduced in this chapter and for their meta-mathematical adequates see [12].

Definition 2.3. 0 and U are the functions in $\boldsymbol{F}$ defined by the condition

$$0(\mathfrak{A})=0 \quad \textit{and} \quad U(\mathfrak{A})=\mathfrak{A}_0^{\omega} \quad \textit{for every} \quad \mathfrak{A} \in \mathcal{A}.$$

Definition 2.4. We say that the function F is *included* in the function G, in symbols

$$F \subseteq G,$$

if $F(\mathfrak{A}) \subseteq G(\mathfrak{A})$ for every $\mathfrak{A} \in \mathcal{A}$.

The notion of a *Boolean algebra* and the elements of the general theory of Boolean algebras are assumed to be familiar to the reader. Boolean algebras will be treated here as algebras with two binary operations, $+$ (*join* operation) and $\cdot$ (*meet* operation), and one unary operation, $^-$ *(complementation)*.

From the Definitions 2.1-2.4 we obtain immediately

THEOREM 2.5.

(i) *The set* $\boldsymbol{F}$ *together with the operations* $\cup$, $\cap$, *and* $^-$ *forms a Boolean algebra.*

In this algebra

(ii) 0 *and* U *are respectively the zero element and the unit element, and* $\subseteq$ *is the inclusion relation,*

(iii) $\bigcup$ *and* $\bigcap$ *are the join and meet operations on arbitrary systems of elements.*

As a consequence of this theorem, the notions defined in 2.2 (i) (ii) and 2.4 have all formal properties of the corresponding set-theoretical notions (union, intersection, etc.).

From Definitions 2.1-2.4 we obtain the following two theorems:

THEOREM 2.6. *If* $F \in \boldsymbol{F}$ *and* $k \geqslant 0$, *then*

$$\wedge_k F=\overline{\vee_k \overline{F}}.$$

THEOREM 2.7. *For any* $F, G \in \boldsymbol{F}$ *and* $k \geqslant 0$, *we have*

(i) $\quad \vee_k 0=0 \quad \textit{and} \quad \wedge_k 0=0,$

(ii) $\quad \vee_k U=U \quad \textit{and} \quad \wedge_k U=U,$

(iii) $\quad F \subseteq \vee_k F \quad \textit{and} \quad \wedge_k F \subseteq F,$

(iv) $\quad \vee_k \vee_l F=\vee_l \vee_k F \quad \textit{and} \quad \wedge_k \wedge_l F=\wedge_l \wedge_k F,$

(v) $\quad \vee_k(F \cup G)=\vee_k F \cup \vee_k G \quad \textit{and} \quad \wedge_k(F \cap G)=\wedge_k F \cap \wedge_k G,$

(vi) $\quad \vee_k(F \cap G) \subseteq \vee_k F \cap \vee_k G \quad \textit{and} \quad \wedge_k F \cup \wedge_k G \subseteq \wedge_k(F \cup G),$

(vii) $\quad F \subseteq G \quad \textit{implies} \quad \vee_k F \subseteq \vee_k G \quad \textit{and} \quad \wedge_k F \subseteq \wedge_k G,$

(viii) $\quad \vee_k \wedge_l F \subseteq \wedge_l \vee_k F.$

Definition 2.8. By the *dimension index* of a function $F \in \boldsymbol{F}$, in symbols $\mathrm{Dm}(F)$, we understand the set determined by the formula

$$\mathrm{Dm}(F) = \underset{k\in\omega}{E}(\vee_k F \neq F).$$

In other words, the set $\mathrm{Dm}(F)$ consists of all non-negative integers k for which there is an algebra $\mathfrak{A} \in \mathcal{A}$ and there are sequences $x, y \in \mathfrak{A}_0^\omega$ such that

$$x_i = y_i \quad \text{for} \quad i \neq k, \qquad x \in F(\mathfrak{A}) \quad \text{but} \quad y \notin F(\mathfrak{A}).$$

The fundamental properties of the dimension index are gathered in the following

THEOREM 2.9.

(i) $$\mathrm{Dm}(0) = \mathrm{Dm}(U) = 0.$$

Furthermore, for any $F, G \in \boldsymbol{F}$ *and* $k \geqslant 0$, *we have*:

(ii) $\mathrm{Dm}(F \cup G) \subseteq \mathrm{Dm}(F) \cup \mathrm{Dm}(G)$ *and* $\mathrm{Dm}(F \cap G) \subseteq \mathrm{Dm}(F) \cup \mathrm{Dm}(G)$,

(iii) $$\mathrm{Dm}(\overline{F}) = \mathrm{Dm}(F),$$

(iv) $\mathrm{Dm}(\vee_k F) \subseteq \mathrm{Dm}(F) - \{k\}$ *and* $\mathrm{Dm}(\wedge_k F) \subseteq \mathrm{Dm}(F) - \{k\}$.

Then we have

THEOREM 2.10. *For any* $F, G \in \boldsymbol{F}$ *and* $k \geqslant 0$, *if* $k \notin \mathrm{Dm}(F)$, *then*

$$\vee_k(F \cap G) = F \cap \vee_k G \quad \text{and} \quad \wedge_k(F \cup G) = F \cup \wedge_k G.$$

Definition 2.11.

(i) For any $k, l, m \geqslant 0$, $I[k,l]$ and $S[k,l,m]$ are the functions in $\boldsymbol{F}$ defined by the following conditions:

$$I[k,l](\mathfrak{A}) = \underset{x\in\mathfrak{A}_0^\omega}{E}(x_k = x_l) \quad \text{and} \quad S[k,l,m](\mathfrak{A}) = \underset{x\in\mathfrak{A}_0^\omega}{E}(x_k + x_l = x_m)$$

for every algebra $\mathfrak{A} \in \mathcal{A}$.

(ii) The functions $I[k,l]$ and $S[k,l,m]$ for any $k, l, m \geqslant 0$ are called *elementary functions* and the set of these functions is denoted by $\boldsymbol{EF}$.

Definition 2.12. The set of the *arithmetical functions*, in symbols $\boldsymbol{AF}$, is taken to be the intersection of all the sets $\boldsymbol{X} \subseteq \boldsymbol{F}$ which include $\boldsymbol{EF}$ as a subset and are closed under the operations $\cup$, $^-$, and $\vee_k$ for $k = 0, 1, \ldots$

From 2.5, 2.6 and 2.12 we obtain

THEOREM 2.13.

(i) $$\boldsymbol{EF} \subseteq \boldsymbol{AF} \subseteq \boldsymbol{F}.$$

(ii) *The system* $\langle \boldsymbol{AF}, \cup, \cap, ^- \rangle$ *is a Boolean algebra (and, in fact, a subalgebra of* $\langle \boldsymbol{F}, \cup, \cap, ^- \rangle$). 2.5 (ii), *as well as* 2.5 (iii) *restricted to finite systems of elements, apply to this algebra.*

(iii) *The set* $\boldsymbol{AF}$ *is closed under the operations* $\vee_k$ *and* $\wedge_k$ *for* $k = 0, 1, \ldots$

It can be proved that every function $F \in \boldsymbol{AF}$ can be represented in the form

$$F = O_0, \ldots, O_{m-1} G,$$

where each of the operations O $(i = 0, 1, \ldots, m-1)$ coincides with one of the operations $\vee_0, \vee_1, \ldots$ and $\wedge_0, \wedge_1, \ldots$, and where G belongs to the subalgebra of the Boolean algebra $\langle \boldsymbol{AF}, \cup, \cap, ^- \rangle$ generated by the set $\boldsymbol{EF}$ (*i. e.*, G is a finite union of finite intersections of elementary functions and their complements). From this it follows easily that the set $\boldsymbol{AF}$ is denumerable.

Definition 2.14. A function F is called a *simple arithmetical function* or, for brevity, a *simple function* if

$$F \subseteq \boldsymbol{AF} \quad \text{and} \quad \mathrm{Dm}(F) = 0.$$

The set of all such functions is denoted by $\boldsymbol{SF}$.

In other words, an arithmetical function F is in $\boldsymbol{SF}$ if and only if

$$F = \vee_k F \quad \text{for every} \quad k \geqslant 0,$$

or if and only if

$$F(\mathfrak{A}) \in \{0, \mathfrak{A}_0^\omega\} \quad \text{for every} \quad \mathfrak{A} \in \mathcal{A}.$$

The system $\langle \boldsymbol{SF}, \cup, \cap, ^- \rangle$ is a denumerable Boolean algebra (and in fact, a subalgebra of $\langle \boldsymbol{AF}, \cup, \cap, ^- \rangle$). 2.5 (ii), as well as 2.5 (iii) restricted to finite systems of elements, apply to this algebra.

Definition 2.15.

(i) For every function $F \in \boldsymbol{SF}$, we set

$$\mathrm{Cl}(F) = \underset{\mathfrak{A}\in\mathcal{A}}{E}\left(F(\mathfrak{A}) = \mathfrak{A}_0^\omega\right).$$

(ii) A set $S \subseteq \mathcal{A}$ is called an *arithmetical class* if there is a function $F \in \boldsymbol{SF}$ for which

$$S = \mathrm{Cl}(F).$$

The family of all arithmetical classes is denoted by $\boldsymbol{AC}$.

The function Cl maps the system $\langle \boldsymbol{SF}, \cup, \cap, {}^{-} \rangle$ isomorphically onto the system $\langle \boldsymbol{AC}, \cup, \cap, {}^{-(\mathcal{A})} \rangle$, where the operation $^{-(\mathcal{A})}$ is determined by the equality

$$\bar{S}^{(\mathcal{A})} = \mathcal{A} - S \quad \text{for every} \quad S \subseteq \mathcal{A}.$$

Hence the system $\langle \boldsymbol{AC}, \cup, \cap, {}^{-(\mathcal{A})} \rangle$ is a denumerable Boolean algebra. In other words, the family $\boldsymbol{AC}$ is a denumerable field of subsets of $\mathcal{A}$.

Many different instances of arithmetical classes can be found among sets of algebraic systems discussed in modern algebra. For instance, the class $\mathcal{G}$ of all groups and the class $\mathcal{AG}$ of all Abelian groups are in $\boldsymbol{AC}$. In fact, let

$$F = \wedge_0 \wedge_1 \vee_2 (S[0,1,2] \cap S[1,0,2]),$$

$$G = \wedge_0 \wedge_1 \wedge_2 \vee_3 \vee_4 \vee_5 (S[0,1,3] \cap S[1,2,4] \cap S[3,2,5] \cap S[0,4,5]) \cap \wedge_0 \wedge_1 \vee_2 S[0,2,1] \cap \wedge_0 \wedge_1 \vee_2 S[2,0,1].$$

Then $F, G \in \boldsymbol{SF}$ and

$$\mathcal{G} = \mathrm{Cl}(G), \qquad \mathcal{AG} = \mathrm{Cl}(F \cap G).$$

The isomorphism type of each finite algebra $\mathfrak{A} \in \mathcal{A}$ and the class $\mathcal{A}_n$ (of all n-element algebras in $\mathcal{A}$), for every $n \geqslant 0$, are further examples of arithmetical classes.

We shall consider also two families which are more comprehensive than $\boldsymbol{AC}$, in fact, $\boldsymbol{AC}_\sigma$ and $\boldsymbol{AC}_\delta$. Since $\boldsymbol{AC}$ is denumerable, $\boldsymbol{AC}_\sigma$ is the family of all (finite or infinite) unions of arithmetical classes and, similarly, $\boldsymbol{AC}_\delta$ is the family of all intersections. Fundamental properties of $\boldsymbol{AC}_\sigma$ and $\boldsymbol{AC}_\delta$ can easily be derived from those of $\boldsymbol{AC}$.

Definition 2.16.

(i) Two algebras $\mathfrak{A}, \mathfrak{B} \in \mathcal{A}$ are said to be *arithmetically equivalent*, symbolically

$$\mathfrak{A} \approx \mathfrak{B},$$

if, for every set $S \in \boldsymbol{AC}$,

$$\text{either} \quad \mathfrak{A}, \mathfrak{B} \in S \quad \text{or} \quad \mathfrak{A}, \mathfrak{B} \notin S.$$

(ii) For every algebra $\mathfrak{A} \in \mathcal{A}$, the set

$$\underset{\mathfrak{B} \in \mathcal{A}}{E} (\mathfrak{A} \approx \mathfrak{B})$$

is called the *arithmetical type* of $\mathfrak{A}$, in symbols $\boldsymbol{T}(\mathfrak{A})$.

(iii) The family of all arithmetical types $\boldsymbol{T}(\mathfrak{A})$ of algebras $\mathfrak{A} \in \mathcal{A}$ is denoted by $\boldsymbol{AT}$.

By 2.16 arithmetical types are partition sets under the equivalence relation $\approx$, and for every algebra $\mathfrak{A} \in \mathcal{A}$,

$$\boldsymbol{T}(\mathfrak{A}) = \bigcap_{\mathfrak{A} \in S \in \boldsymbol{AC}} S.$$

Hence $\boldsymbol{AT} \subseteq \boldsymbol{AC}_\delta$. Thus $\boldsymbol{AT}$ has at most the power of the continuum. In fact, $\boldsymbol{AT}$ hat exactly the power of the continuum. To show this it suffices to construct a subfamily $\boldsymbol{K}$ of $\boldsymbol{AT}$ with the power of the continuum. Many families $\boldsymbol{K}$ with this property are known; it will be seen in Chapter 5 that one of them is the family of all arithmetical types of Abelian groups.

As the last in the series of notions defined exclusively in terms of $\boldsymbol{AC}$ and general set-theoretical notions, we introduce the notions of an arithmetically closed class of algebras.

Definition 2.17. A set $S \subseteq \mathcal{A}$ is called an *arithmetically closed class* if together with every algebra $\mathfrak{A}$ it contains all algebras $\mathfrak{B} \in \mathcal{A}$ such that $\mathfrak{A} \approx \mathfrak{B}$. The family of all arithmetically closed classes is denoted by $\boldsymbol{ACC}$.

From Definitions 2.16 and 2.17 we infer immediately that $\boldsymbol{ACC}$ is a complete and atomistic field of subsets of $\mathcal{A}$, and that $\boldsymbol{AT}$ is the set of atoms of this field. Hence $\boldsymbol{AC}, \boldsymbol{AC}_\sigma, \boldsymbol{AC}_\delta \subseteq \boldsymbol{ACC}$.

All the notions discussed so far in this section apply to arbitrary algebras (in $\mathcal{A}$). In algebraic discussion, however, we are usually interested not in arbitrary algebras but in algebras having some special properties and constituting a well determined set $\mathcal{U}$ that remains fixed throughout the discussion, thus *e. g.*, we discuss groups, or Abelian groups, etc. To obtain an adequate apparatus for studying arithmetical properties of algebras which constitute an arbitrary set $\mathcal{U}$, we first generalize the notions previously introduced and, in fact, we subject them to a process of relativization. As opposed to the new, *relative* notions, the old notions will be referred to as *absolute* ones. If $\mathcal{U}$ is a subset of $\mathcal{A}$, the definitions of relativized notions are obtained from those of absolute notions in the following way: by modifying Definition 2.1, we agree to denote by $\boldsymbol{F}(\mathcal{U})$ the set of all functions F such that $D(F) = \mathcal{U}$ and $F(\mathfrak{A}) \subseteq \mathfrak{A}_0^\omega$ for every algebra $\mathfrak{A} \in \mathcal{U}$; in all the subsequent definitions we replace $\boldsymbol{F}$ by $\boldsymbol{F}(\mathcal{U})$. In such a way we obtain successively the definitions of $\boldsymbol{EF}(\mathcal{U})$ (the set of all *elementary functions on* $\mathcal{U}$), $\boldsymbol{AF}(\mathcal{U})$, $\boldsymbol{SF}(\mathcal{U})$, $\boldsymbol{AC}(\mathcal{U})$ (the family of all *arithmetical classes in* $\mathcal{U}$), $\approx_{\mathcal{U}}$, $\boldsymbol{T}_{\mathcal{U}}$, $\boldsymbol{AT}(\mathcal{U})$, $\boldsymbol{ACC}(\mathcal{U})$.

Obviously the absolute notions are particular cases of the corresponding relative notions, obtaining by taking $\mathcal{A}$ for $\mathcal{U}$, *e. g.*, we have $\boldsymbol{AC} = \boldsymbol{AC}(\mathcal{A})$.

If $\mathcal{U}$ is itself an arithmetical class in the absolute sense (in the present paper we are interested only in this case), then many of the rela-

tive notions simply coincide with the corresponding absolute notions. In fact, we have then

$$S \in \boldsymbol{AC}(\mathcal{U}) \quad \text{if and only if} \quad S \subseteq \mathcal{U} \quad \text{and} \quad S \in \boldsymbol{AC}$$

and a similar conclusion holds for $S \in \boldsymbol{AC}(\mathcal{U})_\sigma$, $S \in \boldsymbol{AC}(\mathcal{U})_\delta$, $S \in \boldsymbol{AT}(\mathcal{U})$ and $S \in \boldsymbol{ACC}(\mathcal{U})$,

$$\text{for any} \quad \mathfrak{A}, \mathfrak{B} \in \mathcal{U}, \quad \mathfrak{A} \underset{\mathcal{U}}{\approx} \mathfrak{B} \quad \text{if and only if} \quad \mathfrak{A} \approx \mathfrak{B} \text{ [12])},$$

$$\text{for any} \quad \mathfrak{A} \in \mathcal{U}, \quad \boldsymbol{T}_{\mathcal{U}}(\mathfrak{A}) = \boldsymbol{T}(\mathfrak{A}).$$

Hence there is no need for using relative notions referring to sets of algebras, like $\boldsymbol{AC}(\mathcal{U})$, if $\mathcal{U}$ is an arithmetical class; the same applies to the notions $\mathfrak{A} \underset{\mathcal{U}}{\approx} \mathfrak{B}$ and $\boldsymbol{T}_{\mathcal{U}}(\mathfrak{A})$. On the other hand, even in the case where $\mathcal{U}$ is an arithmetical class, it proves convenient to use relative notions referring to functions on algebras, like $\boldsymbol{AF}(\mathcal{U})$.

A great majority of theorems concerning absolute notions can be extended to relative notions. If $\mathcal{U}$ is an arithmetical class all the theorems of this chapter remain true by the relativisation to $\mathcal{U}$. The statements concerning the powers of certain sets have to be written in a weaker form; in fact, the phrases *is denumerable* and *has the power of continuum* should be replaced by *is at most denumerable* and *has at most the power of continuum*.

When studying a set $\mathcal{U}$ of algebras from the view point of its arithmetical properties, we attempt to obtain an exhaustive description of arithmetical classes. So far these attempts have been successful only in a restricted number of cases. In all those cases essentially the same procedure has been applied, which we want to discuss here in some detail.

In view of 2.15 the description of arithmetical classes amounts to that of simple functions; in practice the latter result is always obtained as a consequence of an analogous, though more general, result concerning all arithmetical functions. By definition arithmetical functions are recursively constructed from the elementary functions, $I[k,l]|\mathcal{U}$ and $S[k,l,m]|\mathcal{U}$ by means of the operations $\cup$, $^-$, and $\vee_k$. The first two operations have a very elementary character and are closely related to the set-theoretical operations of addition and complementation, while the third one — the operation of (existential) quantification — is more involved and may considerably change the nature of an arithmetical function to which it is applied. Hence we obtain a clearer insight into the structure of arithmetical functions if we succeed in replacing the original construction of those functions by another recursive procedure

[12]) It remains true for arbitrary $\mathcal{U} \subseteq \mathcal{A}$.

in which $\cup$ and $^-$ are the only operations applied. This is achieved by singling out a certain set $\boldsymbol{B}$ of arithmetical functions (which is usually more comprehensive than the set of all elementary functions) and by proving in an effective way that every arithmetical function can be obtained from functions in $\boldsymbol{B}$ by means of the operations $\cup$ and $^-$, *i. e.*, belongs to the set $|\boldsymbol{B}|$ consisting of finite unions of finite intersections of functions in $\boldsymbol{B}$ and their complements; consequently the formula

$$\boldsymbol{AF}(\mathcal{U}) = |\boldsymbol{B}| \tag{1}$$

is established. The functions constituting $\boldsymbol{B}$ will be referred to as *basic functions*. The set $\boldsymbol{B}$ is selected in such a way that for any two functions represented as finite unions of finite intersections of basic functions and their complements we are able to check whether or not they coincide.

It is important to realize that no mechanical prescription for defining the set $\boldsymbol{B}$ can be given; an appropriate selection of basic functions for a given set $\mathcal{U}$ of algebras is often the most creative and difficult point in the whole procedure. In showing that the set $\boldsymbol{B}$ satisfies formula (1) the crucial point is the proof that the operation $\vee_k$ performed on a function $F \in |\boldsymbol{B}|$ yields again a function in $|\boldsymbol{B}|$. As can easily be seen, it suffices to establish this fact for special functions F in $|\boldsymbol{B}|$, namely for functions which are finite intersections of basic functions and their complements; moreover we can restrict ourselves to basic functions whose dimension index contains k.

With the help of formula (1) we are usually able to derive the formula

$$\boldsymbol{SF}(\mathcal{U}) = |\boldsymbol{B} \cap \boldsymbol{SF}(\mathcal{U})|. \tag{2}$$

If we now agree to understand by a *basic class* every arithmetical class S of the form $S = \mathrm{Cl}(F)$ where $F \in \boldsymbol{B} \cap \boldsymbol{SF}(\mathcal{U})$ and to denote the set of all basic classes by $\boldsymbol{C}$, we conclude from (2) that

$$\boldsymbol{AC}(\mathcal{U}) = |\boldsymbol{C}|, \tag{3}$$

where the set $|\boldsymbol{C}|$ consists of finite unions of finite intersections of basic classes and their complements (to $\mathcal{U}$). This is the form in which the desired description of all arithmetical classes is obtained. Using this result we obtain in turn a characterization of other families defined in terms of $\boldsymbol{AC}(\mathcal{U})$, and in particular of the family $\boldsymbol{AT}(\mathcal{U})$ of all arithmetical types.

For obvious reasons the procedure just outlined is called the method of *eliminating quantification*.

In applications the set $\boldsymbol{B}$ usually satisfies an additional assumption: if $k \neq l$ and $F \in \boldsymbol{B}$, then $\vee_k(I[k,l]|\mathcal{U} \cap F) \in \boldsymbol{B}$. If we now agree to under-

stand by *basic sentential functions* all the sentential functions in the formalized arithmetic of $\mathcal{U}$ [13]) with which functions in $\boldsymbol{B}$ are correlated [14]), then our assumption concerning $\boldsymbol{B}$ can be formulated in meta-mathematical terms as follows: Φ being a basic sentential function, every sentential function Ψ obtained by substituting arbitrary variables for some or all free variables in Φ is again a basic sentential function. This assumption implies, for instance, that if $S[k,l,m]|\mathcal{U}$ (where k,l,m are three distinct integers) is in $\boldsymbol{B}$, then $S[k',l',m']|\mathcal{U}$ (where k',l',m' are three arbitrary integers) is also in $\boldsymbol{B}$. Under the above assumption it suffices to carry the process of eliminating quantification for a single, arbitrarily chosen value of k, *e. g.*, for $k=0$.

Various conditions under which formula (1) implies formula (2) — hence also formula (3) — are known. We shall indicate one of them which is applicable in the case where $\mathcal{U}$ coincides with the set $\mathcal{AG}$ of Abelian groups. In this condition we make two assumptions regarding $\mathcal{U}$ and $\boldsymbol{B}$ which in meta-mathematical terminology are reducible to the following ones: First we assume that a certain individual constant, say "c", denoting an element of an algebra is definable in the arithmetic of $\mathcal{U}$; in other words, a sentential function Φ with just one free variable can be constructed of which it can be shown that in every algebra $\mathfrak{A}\in\mathcal{U}$ there is only one element which satisfies Φ, and this element is denoted by c. (If, for instance, $\mathcal{U}$ is the set of all Abelian groups, we can take $x+x=x$ for Φ and c coincides then with the zero element of a group.) Secondly, we assume that if $\mathcal{U}$ is a set of algebras for which such a constant c has been arithmetically defined, then the basic sentential functions selected for $\mathcal{U}$ satisfy the following condition: Φ being a basic sentential function, every sentential function Ψ obtained by substituting the constant c for some or all free variables in Φ is again a basic sentential function.

We shall now give a theorem which provides a formal foundation for the method described above:

THEOREM 2.18 [15]). *Let $\mathcal{U}\subseteq\mathcal{A}$ and let $\boldsymbol{B}$ a set satisfying the following conditions:*

(i) $$\boldsymbol{B}\subseteq\boldsymbol{AF}(\mathcal{U}),$$

(ii) $$\boldsymbol{EF}(\mathcal{U})\subseteq|\boldsymbol{B}|,$$

(iii) *given any integers $k,l\geqslant 0$ with $k\neq l$ and a function $F\in\boldsymbol{B}$, we have*

$$\vee_k(I[k,l]|\mathcal{U}\cap F)\in\boldsymbol{B},$$

[13]) See the first section of the Introduction.
[14]) See [12], p. 706, 707.
[15]) This theorem is not formulated in [12] but it is also due to Tarski.

(iv) *given a sequence $\langle F_0,\ldots,F_{n-1}\rangle$ such that, for $i=0,1,\ldots,n-1$, $0\in\mathrm{Dm}(F_i)$, and $F\in\boldsymbol{B}$ or $\overline{F}_i\in\boldsymbol{B}$, we have*

$$\vee_0\bigcap_{i<n}F_i\in|\boldsymbol{B}|.$$

Then

(I) $$\boldsymbol{AF}(\mathcal{U})=|\boldsymbol{B}|;$$

(II) $$\boldsymbol{SF}(\mathcal{U})=|\boldsymbol{B}\cap\boldsymbol{SF}(\mathcal{U})|$$

if the sets $\mathcal{U}$ and $\boldsymbol{B}$ satisfy moreover the following condition:

(v) *there is a function $G\in\boldsymbol{AF}(\mathcal{U})$ such that*

$$\vee_0\big(G\cap\wedge_1(I[0,1]|\mathcal{U}\cup\overline{\vee_0(I[0,1]|\mathcal{U}\cap G)}\big)=\mathcal{U}$$

and that, for every F,

$$F\in\boldsymbol{B}\ \text{ implies }\ \vee_0(G\cap F)\in\boldsymbol{B}.$$

Chapter 3. Basic functions for Abelian groups

In the present chapter we shall define the set $\boldsymbol{B}$ of basic functions for Abelian groups. The set $\boldsymbol{B}$ will be seen to satisfy the conditions (i)-(v) of Theorem 2.18. We shall establish the dimension indices of all basic functions and distinguish among them the simple basic functions. By means of the simple basic functions we shall construct the set $\boldsymbol{C}$ of basic arithmetical classes. In conclusion we shall discuss connections between various basic functions.

Throughout the present chapter we shall write

$$\begin{aligned} I[k,l] &\quad\text{instead of}\quad I[k,l]|\mathcal{AG},\\ S[k,l,m] &\quad\text{instead of}\quad S[k,l,m]|\mathcal{AG},\\ U &\quad\text{instead of}\quad U|\mathcal{AG}.\end{aligned}$$

Definition 3.1. Given an arbitrary integer $n>0$ and two finite sequences of integers

$$a=(a_0,a_1,\ldots,a_{n-1})\quad\text{and}\quad a'=(a_1,\ldots,a_{n-1}),$$

we define for every algebra $\mathfrak{A}\in\mathcal{AG}$

(i) $$E[a](\mathfrak{A})=E[a_0,a'](\mathfrak{A})=\underset{x\in\mathfrak{A}_0^\omega}{E}\Big(\sum_{i<n}a_ix_i=0\Big),$$

given still another integer $m>0$, we define for $\mathfrak{A}\in\mathcal{AG}$

(ii) $$C[m;a](\mathfrak{A})=C[m;a_0,a'](\mathfrak{A})=\underset{x\in\mathfrak{A}^\omega}{E}\Big(\sum_{i<n}a_ix_i\equiv 0\ (\mathrm{mod}\ m)\Big).$$

We set

$$\bar{E}[a]=\overline{E[a]}, \qquad \bar{E}[a_0,a']=\overline{E[a_0,a']},$$
$$\bar{C}[m;a]=\overline{C[m;a]}, \qquad \bar{C}[m;a_0,a']=\overline{C[m;a_0,a']}.$$

We shall refer to the functions of the form $E[a]$, $\bar{E}[a]$, $C[m;a]$, $\bar{C}[m;a]$ as an *equality* function, an *inequality* function, a *congruence* function and an *incongruence* function, respectively.

We shall refer to the function of the form

$$C[p^{l-1};a]\cap\bar{C}[p^l;a]$$

where p is a prime and $l>0$, as a *complex* function.

Remark. We can always assume the sequence a to have as many terms as we actually need, since the zero-terms do not affect the values of the functions $E[a]$ and $C[m;a]$; hence, in particular, we can always assume the sequence a' to be non-empty.

Throughout the rest of our paper, by sequences we shall mean finite, non-empty sequences of integers, unless otherwise specified.

Definition 3.2. Given a prime p and any integers $k>0$, $n\geqslant 0$ we define for every algebra $\mathfrak{A}\in\mathcal{AG}$

$$R^{(i)}[p,k,n](\mathfrak{A})=\begin{cases}\mathfrak{A}_0^{\omega} & \text{whenever } \varrho^{(i)}[p,k](\mathfrak{A})\geqslant n\\ 0 & \text{otherwise}\end{cases} \qquad (i=1,2,3).$$

We set

$$\bar{R}^{(i)}[p,k,n]=\overline{R^{(i)}[p,k,n]}.$$

Definition 3.3. Given an integer $n>0$, we define for every algebra $\mathfrak{A}\in\mathcal{AG}$

$$K[n](\mathfrak{A})=\begin{cases}\mathfrak{A}_0^{\omega} & \text{whenever } n\mathfrak{A}=3,\\ 0 & \text{otherwise.}\end{cases}$$

We set

$$\bar{K}[n]=\overline{K[n]}.$$

Definition 3.4. The following functions in $F(\mathcal{AG})$:

(1) $E[a]$ for every sequence a,

(2) $C[p^k;a]$ for every prime p, for every integer $k>0$ and for every sequence a,

(3) $R^{(i)}[p,k,n]$ for every prime p and for all integers $k,n>0$ $(i=1,2,3)$,

(4) $K[n]$ for every integer $n>0$

we specify as *basic functions*. The set of all basic functions we denote by $\boldsymbol{B}$. By $|\boldsymbol{B}|$ we denote, as in Chapter 2, the set consisting of finite unions of finite intersections of functions in $\boldsymbol{B}$ and their complements.

Remark. We can restrict the basic functions $E[a]$ to those for which the sequence a has at least one term different from 0, and the basic functions $C[m;a]$ to those for which the sequence a has at least one term not divisible by m; by this restriction the set $|\boldsymbol{B}|$ does not change.

THEOREM 3.5.

$$\boldsymbol{EF}(\mathcal{AG})\subseteq\boldsymbol{B}.$$

In fact, all the elementary functions $I[k,l]$ and $S[k,l,m]$ are among the basic functions $E[a]$.

THEOREM 3.6.

$$\boldsymbol{B}\subseteq\boldsymbol{AF}(\mathcal{AG}).$$

Proof. First of all we shall prove that

(1) $$E[a]\in\boldsymbol{AF}(\mathcal{AG}) \quad \text{for every sequence } a.$$

Given any integers $m,n\geqslant 0$ and arbitrary sequences $b\in\omega^m$ and $c\in\omega^n$, let us define an auxiliary function $H[b,c]$ in $\boldsymbol{F}(\mathcal{AG})$ by the condition

$$H[b,c](\mathfrak{A})=\underset{x\in\mathfrak{A}_0^{\omega}}{E}\Big(\sum_{i<m}x_{b_i}=\sum_{i<n}x_{c_i}\Big) \quad \text{for every } \mathfrak{A}\in\mathcal{AG},$$

with the additional assumption that in case $m=0$ or $n=0$ we replace the corresponding sum by 0.

It is obvious that for every sequence a there exist two sequences b and c of non-negative integers such that

$$E[a]=H[b,c],$$

and that for any two sequences b,c of non-negative integers we have

$$H[b,c]=H[c,b].$$

Thus to prove (1) it is sufficient to show that for any two integers $m\geqslant n\geqslant 0$ and for any sequences $b\in\omega^m$ and $c\in\omega^n$

(2) $$H[b,c]\in\boldsymbol{AF}(\mathcal{AG}).$$

We carry out the proof by means of induction with respect to m. Now

$$m=n=0 \text{ implies } H[b,c]=U\in\boldsymbol{AF}(\mathcal{AG}),$$
$$m=1 \text{ and } n=0 \text{ implies } H[b,c]=S[b_0,b_0,b_0]\in\boldsymbol{AF}(\mathcal{AG}),$$
$$m=n=1 \text{ implies } H[b,c]=I[b_0,c_0]\in\boldsymbol{AF}(\mathcal{AG}).$$

Given now any two sequences

$$b \in \omega^{m+1} \quad \text{and} \quad c \in \omega^n \quad \text{where} \quad m>0 \quad \text{and} \quad m+1 \geqslant n,$$

let

$$r = \max(b_0, \ldots, b_m, c_0, \ldots, c_{n-1}) + 1.$$

With these assumptions $m+1>n$ implies

$$H[b,c] = \vee_r (S[b_{m-1}, b_m, r] \cap H[\langle b_0, \ldots, b_{m-2}, r\rangle, c]),$$

and $m+1=n$ implies

$$H[b,c] = \vee_r \vee_{r+1} (S[b_{m-1}, b_m, r] \cap S[c_{n-2}, c_{n-1}, r+1] \cap H[\langle b_0 \ldots, b_{m-2}, r\rangle, \langle c_0, \ldots, c_{n-3}, r+1\rangle]).$$

Hence by 2.13 the problem is reduced to proving (2) for

$$b = \langle b_0, \ldots, b_{m-2}, r\rangle \in \omega^m \quad \text{and} \quad c \in \omega^n$$

where $m \geqslant n$, or for

$$b = \langle b_0, \ldots, b_{m-2}, r\rangle \in \omega^m \quad \text{and} \quad c = \langle c_0, \ldots, c_{n-3}, r+1\rangle \in \omega^{n-1}$$

where $m = n-1$.

Thus formula (2), and in consequence formula (1), are proved.

To complete the proof it is sufficient to notice that

1° By Definition 3.1, for any integers $m, n>0$ and for any n-termed sequence a, we have $C[m;a] = \vee_n E[\langle a_0, \ldots, a_{n-1}, -m\rangle]$.

2° By Definition 3.2 and by Theorem 1.4, for any prime p and for any integers $k, n>0$, we have

$$R^{(1)}[p,k,n] = \vee_0 \vee_1 \ldots \vee_{n-1} \Big(\bigcap_{a \in Q_1} \bar{E}[p^{k-1}a] \cap \bigcap_{a \in Q_2} E[p^k a] \Big),$$

$$R^{(2)}[p,k,n] = \vee_0 \vee_1 \ldots \vee_{n-1} \bigcap_{a \in Q_1} \bar{C}[p^k; p^{k-1}a],$$

$$R^{(3)}[p,k,n] = \vee_0 \vee_1 \ldots \vee_{n-1} \Big(\bigcap_{a \in Q_1} \bar{C}[p^k; p^{k-1}a] \cap \bigcap_{a \in Q_2} E[p^k a] \Big),$$

where Q_1 is the set of all sequences $a \in p^n$ with at least one term $a_i \neq 0$, and Q_2 is the set of all sequences $a \in \{0,1\}^n$ with exactly one term $a_i \neq 0$.

3° By Definition 3.3, for any integer $n>0$, we have $K[n] = \wedge_0 E[\langle n\rangle]$.

Now let us determine the dimension index of each of the basic functions:

THEOREM 3.7. *For every sequence a*

$$\mathrm{Dm}(E[a]) = \underset{k \in D(a)}{E} (a_k \neq 0). \tag{1}$$

For every sequence a and for an arbitrary integer $m>1$

$$\mathrm{Dm}(C[m;a]) = \underset{k \in D(a)}{E} (a_k \not\equiv 0 \pmod m). \tag{2}$$

For any prime p and for any integers $k, n>0$

$$R^{(i)}[p,k,n] \in \boldsymbol{SF}(\mathcal{AG}) \qquad (i=1,2,3). \tag{3}$$

For arbitrary integer $n>0$

$$K[n] \in \boldsymbol{SF}(\mathcal{AG}). \tag{4}$$

Proof. It is obvious that $a_k=0$ implies $k \notin \mathrm{Dm}(E[a])$. Assume now that $a_k \neq 0$. Consider the group $\mathfrak{Z}$ of integers and two sequences $x, y \in \mathfrak{Z}^{\omega}$ given by the conditions

$$x_i = 0 \quad \text{for} \quad i = 0,1,2,\ldots,$$

$$y_i = \begin{cases} 1 & \text{for} \quad i=k, \\ 0 & \text{otherwise.} \end{cases}$$

Then $x \in E[a](\mathfrak{Z})$ but $y \notin E[a](\mathfrak{Z})$. Hence $k \in \mathrm{Dm}(E[a])$.

The proof of (2) is analogous; (3) and (4) are obvious by Definitions 3.2 and 3.3.

Remark. In conclusion of Theorem 3.7 we obtain (see the Remark following Definition 3.4) that the only simple functions among basic functions are $R^{(i)}[p,k,n]$ and $K[n]$. Hence as *basic classes* (see Chapter 2, page 229) we specify the arithmetical classes

$$\mathcal{R}^{(i)}[p,k,n] = \mathrm{Cl}(R^{(i)}[p,k,n]) \qquad (i=1,2,3),$$

$$\mathcal{K}[n] = \mathrm{Cl}(K[n]).$$

The set of all basic classes we denote by $\boldsymbol{C}$. By $|\boldsymbol{C}|$ we denote, as in Chapter 2, the smallest field over $\boldsymbol{C}$, *i. e.*, the set consisting of finite unions of finite intersections of basic classes and their complements to $\mathcal{AG}$.

We set

$$\overline{\mathcal{R}}^{(i)}[p,k,n] = \overline{\mathcal{R}^{(i)}[p,k,n]} \quad \text{and} \quad \overline{\mathcal{K}}[n] = \overline{\mathcal{K}[n]}.$$

THEOREM 3.8. *Given any integers $k, l \geqslant 0$ with $k \neq l$ and a function $F \in \boldsymbol{B}$, we have*

$$\vee_k (I[k,l] \cap F) \in \boldsymbol{B}.$$

Proof. Let $F=E[a]$. We can assume (see the Remark following Definition 3.1) that $k,l \in D(a)$. Then we easily verify that

$$\vee_k(I[k,l]\cap E[a])=E[a'], \tag{1}$$

where the sequence a' is given by conditions $D(a')=D(a)$ and

$$a'_k=0, \qquad a'_l=a_k+a_l, \qquad a'_i=a_i \quad \text{for} \quad i\in D(a')-\{k,l\}.$$

For $F=C[m;a]$ the procedure is analogous.

If F is a simple function we have

$$\vee_k(I[k,l]\cap F)=\vee_k I[k,l]\cap F=U\cap F=F.$$

Thus the proof is completed.

THEOREM 3.9. *Let $G=E[\langle 1\rangle]$. Then we have*

(i) $$\vee_0\big(G\cap \vee_1[I[0,1]\cap \overline{\vee_0(I[0,1]\cap G)}]\big)=U;$$

(ii) *if $F\in \boldsymbol{B}$, then $\vee_0(G\cap F)\in \boldsymbol{B}$.*

Proof. Using the equality (1) from the proof of Theorem 3.8, we can put the left side of the equality (i) in the form

$$\vee_0(E[\langle 1\rangle]\cap \wedge_1(I[0,1]\cup \bar{E}[\langle 0,1\rangle])).$$

Since in every group there is exactly one zero-element, it is easy to check that the last arithmetical function is equal to U.

Let F be a basic function. First of all assume that $F=E[a]$. Then we easily check that $\vee_0(G\cap E[a])=E[a']$, where the sequence a' is given by conditions

$$D(a')=D(a), \qquad a'_0=0, \qquad a'_i=a_i \quad \text{for} \quad i\in D(a')-\{0\}.$$

For $F=C[m;a]$ the procedure is analogous.

If F is a simple function we have

$$\vee_0(G\cap F)=\vee_0 G\cap F=U\cap F=F.$$

Thus the proof is completed.

By Theorems 3.5, 3.6, 3.8 and 3.9 the set $\boldsymbol{B}$ of basic functions for Abelian groups satisfies conditions (i)-(iii) and (v) of Theorem 2.18. The proof that the set $\boldsymbol{B}$ satisfies also condition (iv) of Theorem 2.18, *i. e.*, the whole procedure of eliminating the qualification $\vee_0$, is given in the next chapter.

Let us now formulate some fundamental properties of basic functions. First of all, Definition 3.1 and Theorem 1.2 indicate the following elementary properties of $E[a]$ and $C[m;a]$:

THEOREM 3.10. *For all sequences a,b and for all integers $m,n>0$ we have*

(i) $$E[a]\subseteq C[m;a],$$

(ii) $$E[a]\cap E[b]\subseteq E[a+b] \quad \text{and} \quad E[a]\cap E[b]\subseteq E[a-b],$$

(iii) $$C[m;a]\cap C[m;b)\subseteq C[m;a+b] \quad \text{and} \quad C[m;a]\cap C[m;b]\subseteq C[m;a-b],$$

(iv) $$E[a]\cap \bar{E}[b]\subseteq \bar{E}[a+b] \quad \text{and} \quad E[a]\cap \bar{E}[b]\subseteq \bar{E}[a-b],$$

(v) $$C[m;a]\cap \bar{C}[m;b]\subseteq \bar{C}[m;a+b] \quad \text{and} \quad C[m;a]\cap \bar{C}[m;b]\subseteq \bar{C}[m;a-b],$$

(vi) $$E[a]=E[-a] \quad \text{and} \quad C[m;a]=C[m;-a],$$

(vii) $$E[a]\subseteq E[na] \quad \text{and} \quad C[m;a]\subseteq C[n\cdot m;na],$$

(viii) $$E[na]\cap E[n_1 a]=E[(n,n_1)a] \quad \text{and} \quad C[m;na]\cap C[m,n_1 a]=C[m;(n,n_1)a],$$

(ix) $$C[m\cdot n;a]\subseteq C[m;a],$$

(x) $$C[m\cdot n;a]=C[m;a]\cap C[n;a] \quad \text{whenever} \quad (m,n)=1,$$

(xi) $$C[m;na]=C[m;a] \quad \text{whenever} \quad (m,n)=1.$$

From 3.10 we can easily deduce the following five theorems:

THEOREM 3.11.

(i) *For any sequence a and for any integer $n>0$ we have*

$$E[n,a)\subseteq C[n;0,a].$$

(ii) *For any sequence a and for any integers $m,n>0$ we have*

$$E[na]\subseteq C[m;a] \quad \text{whenever} \quad (m,n)=1.$$

THEOREM 3.12. *Given any integers $n_1,n_2>0$ and arbitrary sequences $a^{(1)},a^{(2)}$, we can find (effectively) sequence $a,b^{(1)},b^{(2)}$ such that for $d=(n_1,n_2)$ we have*

$$E[n_1,a^{(1)}]\cap E[n_2,a^{(2)}]=E[d,a]\cap E[0,b^{(1)}]\cap E[0,b^{(2)}],$$

$$E[n_1,a^{(1)}]\cap \bar{E}[n_2,a^{(2)}]=(E[d,a]\cap \bar{E}[0,b^{(1)}]\cap E[0,b^{(2)}])\cup(E[n_1,a^{(1)}]\cap \bar{E}[d,a]).$$

Proof. For some integers k_1,k_2

$$k_1 n_1+k_2 n_2=d.$$

It is easy to check that the sequences $a,b^{(1)},b^{(2)}$ are determined in the following way:

$$a=k_1 a^{(1)}+k_2 a^{(2)},$$

and

$$\text{if} \quad b=\frac{n_2}{d}a^{(1)}-\frac{n_1}{d}a^{(2)}, \quad \text{then} \quad b^{(1)}=k_1 b, \quad b^{(2)}=k_2 b.$$

THEOREM 3.13. *Given a prime p, arbitrary integers k_1,k_2,l_1,l_2 such that*

$$0 \leqslant k_1 \leqslant k_2, \qquad k_1 < l_1 \quad \text{and} \quad k_2 < l_2, \qquad l_1 \geqslant l_2,$$

and any two sequences $a^{(1)}$ and $a^{(2)}$, we have

$$C[p^{l_1};p^{k_1},a^{(1)}] \cap C[p^{l_2};p^{k_2},a^{(2)}] = C[p^{l_1};p^{k_1},a^{(1)}] \cap C[p^{l_2};0,p^{k_2-k_1}a^{(1)}-a^{(2)}],$$

$$C[p^{l_1};p^{k_1},a^{(1)}] \cap \bar{C}[p^{l_2};p^{k_2},a^{(2)}] = C[p^{l_1};p^{k_1},a^{(1)}] \cap \bar{C}[p^{l_2};0,p^{k_2-k_1}a^{(1)}-a^{(2)}].$$

THEOREM 3.14. *Given a prime p, arbitrary positive integers n,k,l, such that*

(1) $$k \leqslant l \quad \text{and} \quad n \not\equiv 0 \pmod{p^{k+1}},$$

and arbitrary sequences a and b, we can find (effectively) a sequence c such that

$$E[n,a] \cap C[p^l;p^k,b] = E[n,a] \cap C[p^l;0,c],$$

$$E[n,a] \cap \bar{C}[p^l;p^k,b] = E[n,a] \cap \bar{C}[p^l;0,c].$$

Proof. Let $n = p^m r$ where $(p,r)=1$. By (1) it is $m \leqslant k$. It is easy to check that $c = rb - p^{k-m}a$.

THEOREM 3.15. *Given any integers k,l,m,n,r such that*

$$m,n,r>0 \qquad (m,r)=1, \qquad km+lr=1,$$

we have, for any sequence a,

$$C[m;rn,a] = C[m;n,la].$$

Finally let us consider some relations between the simple basic functions.

THEOREM 3.16. *For any prime p, for any integers $k,m,n>0$, and for $i=1,2,3$, we have*

(1) $R^{(i)}[p,k,m] \subseteq R^{(i)}[p,k,n]$ *and* $R^{(3)}[p,k,m] \subseteq R^{(i)}[p,k,n]$ *whenever* $m \geqslant n$.

For any prime p, for any integers $k,n>0$, and for $i=1,2$, we have

(2) $$R^{(i)}[p,k,n] = R^{(3)}[p,k,n] \cup \bigcup_{0<m<n} (R^{(i)}[p,k+1,m] \cap R^{(3)}[p,k,n-m]) \cup R^{(i)}[p,k+1,n].$$

For any two integers $m,n>0$, we have

(3) $$K[m] \subseteq K[n] \quad \text{whenever} \quad n \equiv 0 \pmod{m}.$$

For any prime p, and for any integers $k,r>0$, we have

(4) $$K[p^k r] = K[p^{k+1}r] \cap \bar{R}^{(3)}[p,k+1,1] \quad \text{whenever} \quad (p,r)=1.$$

For any prime p, and for any integers $k,n,r>0$, we have

(5) $$K[p^k r] \cap R^{(i)}[p,k,n] = K[p^k r] \cap R^{(3)}[p,k,n] \quad \text{whenever} \quad (p,r)=1.$$

Remark. We obtain analogous formulas for basic classes if in (1)-(5) we replace "K" and "R" by "$\mathcal{K}$" and "$\mathcal{R}$", respectively.

Proof. (1) results at once from Definition 3.2 and Theorem 1.8, (2) follows immediately from Theorem 1.7, (3) is obvious by Definition 3.3, (4) is implied by the form (39) (in Chapter 1) of groups of the first kind and by Theorems 1.9 and 1.10, (5) results simply from Theorems 1.11 and 1.8.

In conclusion we introduce some auxiliary functions in $\boldsymbol{F}(\mathcal{AG})$ which will be seen to be in $|\boldsymbol{B}|$.

Definition 3.17. Given a prime p and any integers $k,n>0$, we define for every algebra $\mathfrak{A} \in \mathcal{AG}$

(i) $$L^{(1)}[p,k,n](\mathfrak{A}) = \begin{cases} \mathfrak{A}_0^{\omega} & \text{whenever there are at least } n \text{ different elements in } {}_p(p^{k-1}\mathfrak{A}), \\ 0 & \text{otherwise,} \end{cases}$$

(ii) $$L^{(2)}[p,k,n](\mathfrak{A}) = \begin{cases} \mathfrak{A}_0^{\omega} & \text{whenever there are at least } n \text{ elements incongruent modulo } p^k \text{ in } p^{k-1}\mathfrak{A}, \\ 0 & \text{otherwise,} \end{cases}$$

(iii) $$L^{(3)}[p,k,n](\mathfrak{A}) = \begin{cases} \mathfrak{A}_0^{\omega} & \text{whenever there are at least } n \text{ elements incongruent modulo } p^k \text{ in } {}_p(p^{k-1}\mathfrak{A}), \\ 0 & \text{otherwise.} \end{cases}$$

Definition 3.18. Given arbitrary integers $m,n>0$, we define for every algebra $\mathfrak{A} \in \mathcal{AG}$

$$L[m,n] = \begin{cases} \mathfrak{A}_0^{\omega} & \text{whenever there are at least } n \text{ different elements in } m\mathfrak{A}, \\ 0 & \text{otherwise.} \end{cases}$$

THEOREM 3.19. *For every prime p and for any integers $k,n>0$*

$$L^{(i)}[p,k,n] \in \boldsymbol{B} \qquad (i=1,2,3).$$

Proof. Let l be the integer determined by the condition $p^{-1} < n \leqslant p^l$. Then by Theorem 1.6 we have $L^{(i)}[p,k,n] = R^{(i)}[p,k,l] \in \boldsymbol{B}$.

THEOREM 3.20. *For any integers $m,n>0$*

$$L[m,n] \in |\boldsymbol{B}|.$$

Proof. For the time being let p be the sequence of all primes ordered by the relation $<$. Let the integer r be determined by the condition

(1) $$p_{r-1} \leqslant n < p_r.$$

The integer m can be put in the form

(2) $$m = \prod_{i<s} p_i^{l_i} \quad \text{where} \quad s \geqslant r \quad \text{and} \quad l_i \geqslant 0.$$

We determine now an s-termed sequence k of positive integers by the condition

$$p_i^{k_i-1} < n \leqslant p_i^{k_i} \quad \text{for} \quad i = 0,1,\ldots,s-1 \tag{3}$$

and we set

$$t = \prod_{i<s} p_i^{(k_i-1)+l_i}. \tag{4}$$

We have

$$L[m,n] = L[m,n] \cap (K[t] \cup \bar{K}[t]) = (L[m,n] \cap K[t]) \cup (L[m,n] \cap \bar{K}[t]).$$

But from (1)-(4) it follows that

$$\bar{K}[t] \subseteq L[m,n]. \tag{5}$$

To show it we take an Abelian group $\mathfrak{A}$ such that $\bar{K}[t](\mathfrak{A}) = \mathfrak{A}_0^\omega$. By (4) there is in $\mathfrak{A}$ an element x either of infinite order, or of order $p_i^{k_i+l_i}$, or at last of a prime order $q \geqslant p_s$. It follows from (1)-(3) that in each of the three cases the elements

$$mx,\ 2(mx),\ldots,n(mx),$$

of course divisible by m, are all different. Hence $L[m,n](\mathfrak{A}) = \mathfrak{A}_0^\omega$. Thus formula (5) is proved and therefore

$$L[m,n] = (L[m,n] \cap K[t]) \cup \bar{K}[t].$$

Thus to prove that $L[m,n] \in |\boldsymbol{B}|$, it is sufficient to prove that

$$L[m,n] \cap K[t] \in |\boldsymbol{B}|.$$

Take an Abelian group $\mathfrak{A}$ such that $L[m,n] \cap K[t](\mathfrak{A}) = \mathfrak{A}_0^\omega$. Thus $t\mathfrak{A} = \mathfrak{Z}$ and $\overline{\overline{m\mathfrak{A}}} \geqslant n$. Using the form (39) from Chapter 1 we have

$$\mathfrak{A} \cong \prod_{i<s} \prod_{0<k<k_i+l_i} \mathfrak{C}_{p_i,k}^{\alpha(p_i,k)}$$

and then

$$m\mathfrak{A} \cong \prod_{i<s} \prod_{l_i<k<k_i+l_i} \mathfrak{C}_{p_i,k-l_i}^{\alpha(p_i,k)},$$

or, putting $j = k - l_i$,

$$m\mathfrak{A} \cong \prod_{i<r} \prod_{0<j<k_i} \mathfrak{C}_{p_i,j}^{\alpha(p_i,l_i+j)}.$$

If $m\mathfrak{A}$ is a finite group, then the cardinals $\alpha(p_i,l_i+j)$ are finite and by formula (38) from Chapter 1

$$\alpha(p_i,l_i+j) = \varrho^{(3)}[p_i,l_i+j](\mathfrak{A}).$$

Hence

$$\overline{\overline{m\mathfrak{A}}} = \prod_{i<r} \prod_{0<j<k_i} p_i^{j \cdot \varrho^{(3)}[p_i,l_i+j](\mathfrak{A})}$$

and putting

$$u_i = \sum_{0<j<k_i} j \cdot \varrho^{(3)}[p_i,l_i+j](\mathfrak{A}),$$

we get $\prod_{i<r} p_i^{u_i} \geqslant n$.

From these considerations it follows easily that

$$L[m,n] \cap K[t] = \bigcup_{f \in Q} \bigcap_{i<r} \bigcap_{0<j<k_i} R^{(3)}[p_i,l_i+j,f(i,j)],$$

where the set Q ranges over all functions f such that $f(i,j)$ is a non-negative integer determined for $i<r$ and $0<j<k_i$, and that the following two conditions are satisfied:

$$r_i = \sum_{0<j<k_i} j \cdot f(i,j) \leqslant k_i \tag{6}$$

(because of (3)) and $\prod_{i<r} p_i^{v_i} \geqslant n$. Since, by (6), the set Q is finite, the function $L[m,n] \cap K[t]$ belongs to $|\boldsymbol{B}|$. Thus the proof is finished.

Chapter 4. Fundamental theorems on arithmetical functions and on arithmetical classes

In the present chapter we shall show that the set $\boldsymbol{B}$ of basic functions for Abelian groups satisfies condition (iv) of Theorem 2.18, *i. e.*, that given a function $F = \bigcap_{i<m} F_i$ such that for $i = 0,1,\ldots,m-1$, $F_i \in \boldsymbol{B}$ or $\bar{F} \in \boldsymbol{B}$ and $0 \in \mathrm{Dm}(F_i)$, we have $\vee_0 F \in |\boldsymbol{B}|$.

Since $0 \in \mathrm{Dm}(F_i)$, the functions F_i are (by Definition 2.14 and Theorems 3.7 and 3.10 (vi)) of the form

$$E[n,a] \quad \text{or} \quad \bar{E}[n,a] \quad \text{or} \quad C[p^k;r,b] \quad \text{or} \quad \bar{C}[p^k;r,b] \tag{1}$$

where $n,r>0$ and $r \not\equiv 0 \pmod{p^k}$.

We shall start with the simplest intersections F, passing step by step to the general case when F is an arbitrary intersection of functions of the form (1).

In the proof we shall repeatedly use two methods; it seems convenient to give them some special names:

1° The sequence method. It is used when the inclusion

$$F \subseteq G \tag{2}$$

is to be proved. By Definition 2.4 the condition (2) is equivalent to

$$F(\mathfrak{A}) \subseteq G(\mathfrak{A}) \quad \text{for every group} \quad \mathfrak{A} \in \mathcal{AG}. \tag{3}$$

To prove (3) we must check the fact that for every group $\mathfrak{A} \in \mathcal{AG}$ and for every sequence $x \in \mathfrak{A}_0^\omega$

$$x \in F(\mathfrak{A}) \quad \text{implies} \quad x \in G(\mathfrak{A}).$$

That is the point of the sequence method.

2° The method of adjunction. Consider an arithmetical function F. Given an arbitrary arithmetical function G, we can (by 2.13) *decompose F by means of G*:

$$F = (F \cap G) \cup (F \cap \bar{G}).$$

In general, given arbitrary arithmetical functions $G_0, G_1, \ldots, G_{m-1}$, we set

$$G_i^{(0)} = G_i \quad \text{and} \quad G_i^{(1)} = \bar{G}_i \quad \text{for} \quad i = 0,1,\ldots,m-1$$

and we *decompose the function F by means of the functions $G_0, G_1, \ldots, G_{m-1}$*:

$$F = \bigcup_{r \in 2^m} (F \cap \bigcap_{i<m} G_i^{(r_i)}).$$

Assume now that F is an intersection of functions of the form (1) and that G_i (for $i = 0,1,\ldots,m-1$) are basic functions. By Theorem 2.8 (iii) we have

$$\vee_0 F = \bigcup_{r \in 2^m} \vee_0 (F \cap \bigcap_{i<m} G_i^{(r_i)})$$

and the problem of proving that $\vee_0 F \in |\boldsymbol{B}|$ is reduced to the problem of proving that

$$\vee_0 (F \cap \bigcap_{i<m} G_i^{(r_i)}) \in |\boldsymbol{B}|$$

for every sequence $r \in 2^m$. By a suitable choice of the functions G the last problem may prove to be much easier that the original one. That is the point of the method of adjunction.

Throughout the rest of this chapter instead of saying that the problem of proving that $\vee_0 F \in |\boldsymbol{B}|$ is reduced to the problem of proving that $\vee_0 F_1, \ldots, \vee_0 F_n \in |\boldsymbol{B}|$ we shall say shortly that we *pass from the function F to the functions $F_1, \ldots, F_n$*.

LEMMA 4.1. *For every sequence a,*

$$\text{if} \quad F = \bar{E}[1,a], \quad \text{then} \quad \vee_0 F \in |\boldsymbol{B}|.$$

Proof. Let $\mathfrak{A} \in \mathcal{AG}$, $x \in \mathfrak{A}_0^\omega$. By Definition 3.1 (i) we have

$$x \in F(\mathfrak{A}) \quad \text{whenever} \quad x_0 = -\sum_{i \in D(a)} a_i x_{i+1}$$

therefore by Definition 2.2 (iii) we have $x \in \vee_0 F(\mathfrak{A})$ for every $x \in \mathfrak{A}_0^\omega$. Hence $\vee_0 F(\mathfrak{A}) = \mathfrak{A}_0^\omega$ for every $\mathfrak{A} \in \mathcal{AG}$, that is $\vee_0 F = U \in |\boldsymbol{B}|$.

LEMMA 4.2. *For every integer $n>1$ and for every sequence a,*

$$\text{if} \quad F = E[n,a], \quad \text{then} \quad \vee_0 F \in |\boldsymbol{B}|.$$

Proof. Let $n = \prod_{i<r} p_i^{k_i}$ be the decomposition of n into prime factors. By Definitions 3.1 and 3.4, and by Theorem 3.10 (x) we have

$$\vee_0 F = C[n;0,a] = \bigcap_{i<r} C[p_i^{k_i};0,a] \in |\boldsymbol{B}|.$$

LEMMA 4.3. *For any integers $m>1$, $n>0$ and for any sequences $a^{(0)}, \ldots, a^{(m-1)}$*

$$\text{if} \quad F = \bigcap_{i<m} E[n,a^{(i)}], \quad \text{then} \quad \vee_0 F \in |\boldsymbol{B}|.$$

Proof. We have (by 3.10 (ii))

$$F = E[n,a^{(0)}] \cap \bigcap_{0<i<m} E[0,a^{(i)} - a^{(0)}],$$

hence by Theorems 3.7, 2.9 (ii) and 2.10 we obtain

$$\vee_0 F = \vee_0 E[n,a^{(0)}] \cap \bigcap_{0<i<m} E[0,a^{(i)} - a^{(0)}].$$

Thus, by Definition 3.4, the problem is reduced to 5.1 or 5.2.

LEMMA 4.4. *For any integers $m,n>0$ and for any sequences $a^{(0)}, \ldots, a^{(m-1)}$,*

$$\text{if} \quad F = \bigcap_{i<m} \bar{E}[n,a^{(i)}], \quad \text{then} \quad \vee_0 F \in |\boldsymbol{B}|.$$

Proof. Let us consider the more difficult case when $n>1$. The procedure for $n=1$ is essentially the same, only some steps can be omitted. We use the method of adjunction:

Let us decompose the function F by means of the functions $C[n;0,a^{(i)}]$ for $i = 0,1,\ldots,m-1$. Then we pass from the function F to the functions

$$F_1 = \bigcap_{i<m} (\bar{E}[n,a^{(i)}] \cap C[n;0,a^{(i)}]),$$

$$F_2 = \bigcap_{i \in N} (\bar{E}[n,a^{(i)}] \cap C[n;0,a^{(i)}]) \cap \bigcap_{i \in m-N} (\bar{E}[n,a^{(i)}] \cap C[n;0,a^{(i)}])$$

for $0 \neq N \subseteq m$. (In case $N = m$ we assume the second factor equal to U).

By 3.11 we have $\bar{E}[n,a] \cap \bar{C}[n;0,a^{(i)}] = \bar{C}[n;0,a^{(i)}]$. Hence

$$F_1 = \bigcap_{i<m} \bar{C}[n;0,a^{(i)}] \quad \text{and} \quad \vee_0 F_1 = F_1 \in |\boldsymbol{B}|,$$

then

$$F_2 = \bigcap_{i \in N} (\bar{E}[n,a^{(i)}] \cap C[n;0,a^{(i)}]) \cap \bigcap_{i \in m-N} \bar{C}[n;0,a^{(i)}],$$

$$\vee_0 F_2 = \vee_0 \bigcap_{i \in N} (\bar{E}[n;a^{(i)}] \cap C[n;0,a^{(i)}]) \cap \bigcap_{i \in m-N} \bar{C}[n;0,a^{(i)}].$$

Since $\bigcap_{i\in m-N} \bar{C}[n;0,a^{(0)}] \in |\boldsymbol{B}|$, we pass from F_2 to the function

$$F_3 = \bigcap_{i\in N} (\bar{E}[n,a^{(0)}] \cap C[n;0,a^{(0)}]$$

for $0 \neq N \subseteq m$.

In turn let us decompose the function F_3 by means of the functions $E[0,a^{(0)}-a^{(j)}]$ for $i,j \in N$ and $i<j$. We have

$$\bar{E}[n,a^{(0)}] \cap \bar{E}[n;a^{(j)}] \cap E[0,a^{(0)}-a^{(j)}] = \bar{E}[n;a^{(0)}] \cap E[0,a^{(0)}-a^{(j)}],$$

hence we pass from F_3 to the function

$$G = \bigcap_{i\in M} (\bar{E}[n;a^{(0)}] \cap C[n;0,a^{(0)}]) \cap \bigcap_{\substack{i,j\in M \\ i<j}} \bar{E}[0,a^{(0)}-a^{(j)}]$$

where $0 \neq M \subseteq N$.

Now suppose that M consists of exactly r integers, and set

$$G' = L[n,r+1] \cap \bigcap_{i\in M} C[n;0,a^{(0)}] \cap \bigcap_{\substack{i,j\in M \\ i<j}} \bar{E}[0,a^{(0)}-a^{(j)}]. \tag{1}$$

We shall prove that $\vee_0 G = G'$.

First we shall prove, using the sequence method, that $\vee_0 G \subset G'$. Let $\mathfrak{A} \in \mathcal{AG}$ and $x \in \vee_0 G(\mathfrak{A})$. Thus there is a sequence $x^{(\mathfrak{A})} \in \mathfrak{A}_0^\omega$ such that

$$x_i^{(\mathfrak{A})} = x_i \quad \text{for} \quad i>0, \tag{2}$$

$$x^{(\mathfrak{A})} \in \bar{E}[n,a^{(0)}](\mathfrak{A}) \quad \text{for} \quad i \in M, \tag{3}$$

$$x^{(\mathfrak{A})} \in C[n;0,a^{(0)}](\mathfrak{A}) \quad \text{for} \quad i \in M, \tag{4}$$

$$x^{(\mathfrak{A})} \in \bar{E}[0,a^{(0)}-a^{(j)}](\mathfrak{A}) \quad \text{for} \quad i,j \in M \quad \text{and} \quad i<j. \tag{5}$$

Let $y_i = \sum_{j\in D(a^{(0)})} a_j^{(i)} x_{j+1}$ for $i \in M$ and consider the elements $-nx_0$ and y_i for $i \in M$. It follows from (3) and (5) that they are all different, and we infer from (4) that they are in $(n\mathfrak{A})_0$. Thus by Definition 3.18

$$L[n,r+1](\mathfrak{A}) = \mathfrak{A}_0^\omega;$$

hence

$$x \in L[n,r+1](\mathfrak{A}). \tag{6}$$

But by (2), (4), and (5) we also have $x \in C[n;0,a^{(0)}](\mathfrak{A})$ for $i \in M$ and $x \in \bar{E}[0,a^{(0)}-a^{(j)}](\mathfrak{A})$ for $i,j \in M$ and $i<j$ which together with (6) implies by (1) that $x \in G'(\mathfrak{A})$.

In this way we have proved that $x \in \vee_0 G(\mathfrak{A})$ implies $x \in G'(\mathfrak{A})$ for every $\mathfrak{A} \in \mathcal{AG}$ and for every $x \in \mathfrak{A}_0^\omega$. Hence $\vee_0 G \subseteq G'$.

The proof that $G' \subseteq \vee_0 G$ is analogous. Therefore $\vee_0 G = G'$. But from (1) it follows by 3.20 that $G' \in |\boldsymbol{B}|$, which concludes the proof.

LEMMA 4.5. *For any integers* $m>0$, $n_0,\dots,n_{m-1}>0$, *and for any sequences* $a, a^{(0)},\dots,a^{(m-1)}$,

$$\text{if} \quad F = E[1,a] \cap \bigcap_{i<m} \bar{E}[n_i,a^{(0)}], \quad \text{then} \quad \vee_0 F \in |\boldsymbol{B}|.$$

Proof. By 3.10 (vii), (iv)

$$\vee_0 F = \vee_0 (E[1,a] \cap \bigcap_{i<m} \bar{E}[0,a^{(0)}-n_i a]) = \vee_0 E[1,a] \cap \bigcap_{i<m} \bar{E}[0,a^{(0)}-n_i a],$$

hence the problem is reduced to 5.1.

LEMMA 4.6. *For any integers* $m>0$, $n>1$ *and for any sequences* $a, a^{(0)},\dots,a^{(m-1)}$,

$$\text{if} \quad F = E[n,a] \cap \bigcap_{i<m} \bar{E}[n,a^{(0)}], \quad \text{then} \quad \vee_0 F \in |\boldsymbol{B}|.$$

Proof. In fact $\vee_0 F = \vee_0 E[n,a] \cap \bigcap_{i<m} \bar{E}[0,a^{(0)}-a]$ and the problem is reduced to 4.2.

LEMMA 4.7. *For any integers* $m,n>0$, *for any prime* p *and for any sequences* $a^{(0)},\dots,a^{(m-1)}$,

$$\text{if} \quad F = \bigcap_{i<m} (E[n,a^{(0)}] \cap E[pn,pa^{(0)}]), \quad \text{then} \quad \vee_0 F \in |\boldsymbol{B}|.$$

Proof. We proceed just as in 4.4. We consider the more difficult case when $n>1$, decompose F by means of the functions $C[n,0,a^{(0)}]$ and $E[0,a^{(0)}-a^{(j)}]$, and using the method of adjunction we either reduce the problem to 4.3 or we pass from F to the functions

$$G = \bigcap_{i\in M} (\bar{E}[n,a^{(0)}] \cap E[pn,pa^{(0)}] \cap C[n;0,a^{(0)}]) \cap \bigcap_{\substack{i,j\in M \\ i<j}} \bar{E}[0,a^{(0)}-a^{(j)}]$$

where $0 \neq M \subseteq m$.

Let $n = p^k s$, where $k \geqslant 0$ and $(p,s)=1$. Since $C[n;n,0)=U$, we obtain by 3.10 (iii), (v), (x)

$$C[n;0,a^{(0)}] = C[n;n,a^{(0)}] = C[p^k;n,a^{(0)}] \cap C[s;n,a^{(0)}];$$

then by 3.10 (i), (xi)

$$E[pn,pa^{(0)}] \subseteq C[s;pn,pa^{(0)}] = C[s;n,a^{(0)}].$$

Hence

$$G = \bigcap_{i\in M} (\bar{E}[n,a^{(0)}] \cap E[pn,pa^{(0)}] \cap C[p^k;n,a^{(0)}]) \cap \bigcap_{\substack{i\in M \\ i<j}} \bar{E}[0,a^{(0)}-a^{(j)}].$$

Let the set M consist of exactly r integers and assume for simplicity that $0 \in M$. Using (twice) the sequence method we can easily check (see Definition 3.17) that

$$\vee_0 G = L^{(1)}[p, k+1, r+1] \cap \bigcap_{0<i\in M} (\bar{E}[0, a^{(0)}-a^{(i)}] \cap E[0, p(a^{(0)}-a^{(i)})] \cap C[p^k; 0, a^{(0)}-a^{(i)}]) \cap \bigcap_{0<i,j\in M,\ i<j} \bar{E}[0, a^{(i)}-a^{(j)}] \cap C[n; 0, a^{(0)}],$$

which, by Theorem 3.19, completes the proof.

LEMMA 4.8. *For any integers $m>0$, and $n>1$, for any (not necessarily different) prime divisors $p_0, \dots, p_{m-1}$ of n, and for any sequences $a^{(0)}, \dots, a^{(m-1)}$,*

$$\text{if} \quad F = \bigcap_{i<m} \left(\bar{E}\left[\frac{n}{p_i}, a^{(i)}\right] \cap E[n, p_i a^{(i)}] \right), \quad \text{then} \quad \vee_0 F \in |\boldsymbol{B}|.$$

Proof. The proof is by induction with respect to the number r of different primes among $p_0, \dots, p_{m-1}$. If $r=1$, the theorem is reduced to 4.7. Assume now that the theorem is proved for $r \geqslant 1$ and that there are $r+1$ different primes among $p_0, \dots, p_{m-1}$. For simplicity let us assume that for some $l<m$ it is $p_0 = p_1 = \dots = p_{l-1} = p$ and $p_i \neq p$ for $i \geqslant l$. Hence among $p_l, p_{l+1}, \dots, p_{m-1}$ there are exactly r different primes. Let us denote their product by q. Then for some integers k and l

$$kp + lq = 1. \tag{1}$$

Consider the following three functions:

$$F_1 = \bigcap_{i<l} \left(\bar{E}\left[\frac{n}{p}, a^{(i)}\right] \cap E[n, pa^{(i)}] \right), \tag{2}$$

$$F_2 = \bigcap_{l\leqslant i<m} \left(\bar{E}\left[\frac{n}{p_i}, a^{(i)}\right] \cap E[n, pa^{(i)}] \right), \tag{3}$$

$$G = E[0, pa^{(0)} - p_l a^{(l)}]. \tag{4}$$

With respect to Lemma 4.7 and to the induction hypothesis it is sufficient to prove that $\vee_0 F = \vee_0 F_1 \cap \vee_0 F_2 \cap G$.

We use the sequence method: Consider an arbitrary group $\mathfrak{A} \in \mathcal{AG}$ and let $x \in \vee_0 F_1 \cap \vee_0 F_2 \cap G(\mathfrak{A})$.

Then $x \in \vee_0 F_1(\mathfrak{A})$ and $x \in \vee_0 F_2(\mathfrak{A})$, and

$$x \in G(\mathfrak{A}). \tag{5}$$

Hence there are sequences $x^{(1)}, x^{(2)} \in \mathfrak{A}_0^\omega$ such that

$$x_i^{(1)} = x_i^{(2)} = x_i \quad \text{for} \quad i>0, \tag{6}$$

$$x^{(1)} \in F_1(\mathfrak{A}) \quad \text{and} \quad x^{(2)} \in F_2(\mathfrak{A}). \tag{7}$$

It follows from (4)-(6) that

$$x^{(1)} \in G(\mathfrak{A}); \tag{8}$$

from (2), (3), and (7) that

$$x^{(1)} \in E[n, pa^{(0)}](\mathfrak{A}), \tag{9}$$

$$x^{(2)} \in E[n, p_l a^{(l)}](\mathfrak{A}), \tag{10}$$

from (4), (8), and (9) that $x^{(1)} \in E[n, p_l a^{(l)}](\mathfrak{A})$; hence by (10) and (6)

$$nx_0^{(1)} = nx_0^{(2)}. \tag{11}$$

Now consider the sequence $y \in \mathfrak{A}_0^\omega$ determined in the following way (see (1)):

$$y_0 = (kp)x_0^{(2)} + (lq)x_0^{(1)}, \tag{12}$$

$$y_i = x_i \quad \text{for} \quad i>0. \tag{13}$$

We assert that $y \in F(\mathfrak{A})$. In fact the conditions (11), (12) and (1) imply

$$\frac{n}{p} y_0 = \frac{n}{p} x_0^{(1)}, \tag{14}$$

$$\frac{n}{p_i} y_0 = \frac{n}{p_i} x_0^{(2)} \quad \text{for} \quad i = l, l+1, \dots, m-1, \tag{15}$$

$$n y_0 = n x_0^{(1)} = n x_0^{(2)}; \tag{16}$$

and from the conditions (6), (7) and (13)-(16) it follows that $y \in F(\mathfrak{A})$. Hence by (13) we have $x \in \vee_0 F(\mathfrak{A})$.

To prove the inclusion in the opposite direction let us observe that by (2)-(4) we have $F \subseteq F_1 \cap F_2 \cap E[n, pa^{(0)}] \cap E[n, p_l a^{(l)}] \subseteq F_1 \cap F_2 \cap G$; hence it follows from Theorem 2.8 (v), (iv) that $\vee_0 F \subseteq \vee_0 F_1 \cap \vee_0 F_2 \cap G$.

As simple consequences of Lemma 4.8 we obtain the following two lemmata:

LEMMA 4.9. *For any integers $m>0$, $n>1$, for any (not necessarily different) prime divisors $p_0, \dots, p_{m-1}$ of n, and for any sequences $a, a^{(0)}, \dots, a^{(m-1)}$*

$$\text{if} \quad F = E[n, a] \cap \bigcap_{i<m} \left(\bar{E}\left[\frac{n}{p_i}, a^{(i)}\right] \cap E[n, p_i a^{(i)}] \right), \quad \text{then} \quad \vee_0 F \in |\boldsymbol{B}|.$$

LEMMA 4.10. *For any integers $m, r>0$ and $n>1$, for any (not necessarily different) prime divisors $p_0, \dots, p_{m-1}$ of n, and for any sequences $a, a^{(0)}, \dots, a^{(m-1)}, b^{(0)}, \dots, b^{(r-1)}$*

$$\text{if} \quad F = E[n, a] \cap \bigcap_{i<m} \left(\bar{E}\left[\frac{n}{p_i}, a^{(i)}\right] \cap E[n, p_i a^{(i)}] \right) \cap \bigcap_{i<r} \bar{E}[n, b^{(i)}], \text{ then } \vee_0 F \in |\boldsymbol{B}|.$$

LEMMA 4.11. *For any integers $m>0$, $n>1$, for any (not necessarily different) prime divisors $p_0,\dots,p_{m-1}$ of n, and for any sequences $a,a^{(0)},\dots,a^{(m-1)}$*

$$\text{if}\quad F=E[n,a]\cap\bigcap_{i<m}\bar{E}\left[\frac{n}{p_i},a^{(i)}\right],\quad\text{then}\quad \vee_0 F\in|\boldsymbol{B}|.$$

Proof. We decompose F by means of the functions $E[n,p_ia^{(i)}]$ for $i<m$. Since

$$\bar{E}\left[\frac{n}{p_i},a^{(i)}\right]\cap\bar{E}[n,p_ia^{(i)}]=\bar{E}[n,p_ia^{(i)}],$$

by the method of adjunction we reduce the problem to 4.6, 4.9 and 4.10.

LEMMA 4.12. *For any integers $l,m>0$ and $n>1$, for any (not necessarily different) prime divisors $p_0,\dots,p_{l-1}$ of n, and for any sequences $a,a^{(0)},\dots,a^{(l-1)},b^{(0)},\dots,b^{(m-1)}$*

$$\text{if}\quad F=E[n,a]\cap\bigcap_{i<l}\bar{E}\left[\frac{n}{p_i},a^{(i)}\right]\cap\bigcap_{i<m}E[n,b^{(i)}],\quad\text{then}\quad \vee_0 F\in|\boldsymbol{B}|.$$

Proof. Obvious by 4.11.

LEMMA 4.13. *For any integers $m>0$, $n,n_0,\dots,n_{m-1}>0$, and for any sequences $a,a^{(0)},\dots,a^{(m-1)}$*

$$\text{if}\quad F=E[n,a]\cap\bigcap_{i<m}\bar{E}[n_i,a^{(i)}],\quad\text{then}\quad \vee_0 F\in|\boldsymbol{B}|.$$

Proof. We assume that:

1° Among $n_0,\dots,n_{m-1}$ there are exactly r ($r\geqslant 0$) integers which are not divisors of n.

2° If n_i is a divisor of n, then n/n_i is a product of k_i (not necessarily different) primes. We consider 1 as a product of 0 primes. And we set $k_i=0$ in the case when n_i is not a divisor of n. Let $k=\max(k_i)$ for $i<m$. We have $k_i\geqslant 0$.

3° Among $k_0,\dots,k_{m-1}$ there are exactly l ($l\geqslant 1$) integers equal to k.

Let us refer to n,r,k,l as the first, the second, the third, and the fourth index of F. We carry out a simultaneous induction with respect to n,r,k,l.

If $n=1$, the problem is reduced to 4.5.

Let $n>1$ and suppose that the theorem is already proved for arbitrary r,k,l in the case when the first index is less than n.

Suppose $r=0$.

If $k=0$, then for $i=0,1,\dots,m-1$ we have $n_i=n$ and the problem is reduced to 4.6.

If $k=1$, then for $i=0,1,\dots,m-1$ we have $n_i=n$ or $n_i=n/p_i$ for some prime divisor p_i of n. Thus the problem is reduced to 4.11 or 4.12.

Consider the case when $k>1$ and suppose that the theorem is already proved for arbitrary l in the case when the third index is less than k. For simplicity let us assume that $k_0=k$. Thus $n=pn_0s$ for a certain prime divisor p of n and a certain $s>1$. Let us decompose F by means of the function $E[pn_0,pa^{(0)}]$. By the method of adjunction we pass from F to the functions

$$G=E[n,a]\cap E[pn_0,pa^{(0)}]\cap\bigcap_{i<m}\bar{E}[n_i,a^{(i)}],$$

$$H=E[n,a]\cap\bar{E}[pn_0,pa^{(0)}]\cap\bigcap_{0<i<m}\bar{E}[n_i,a^{(i)}].$$

Consider G. We have

$$G=E[0,a-(sp)a^{(0)}]\cap G_1\quad\text{where}\quad G_1=E[pn_0,pa^{(0)}]\cap\bigcap_{i<m}\bar{E}[n_i,a^{(i)}],$$

but the first index of G_1 equals $pn_0<n$. Consider H. The first index of H is equal to n, the second index — to 0. If $l=1$, then the third index of H is less then k. If $l>1$, then the third index of H is equal to k, but the fourth index of H equals $l-1$.

Finally let $r>1$ and assume that the theorem is already proved for arbitrary k and l in the case when the second index is less than r. For simplicity let us assume that n_0 is not a divisor of n. It may be that n_0 is divisible by n. In that case

$$F=\bar{E}\left[0,a^{(0)}-\frac{n_0}{n}a\right]\cap F_1\quad\text{where}\quad F_1=E[n,a]\cap\bigcap_{0<i<m}\bar{E}[n_i,a^{(i)}].$$

But the first index of F_1 is equal to n and the second index of F_1 is equal to $r-1$. If n is not divisible by n, let $d=(n,n_0)$. By 3.12 there are sequences $b,c^{(1)}$ and $c^{(2)}$ such that

$$E[n,a]\cap\bar{E}[n_0,a^{(0)}]=(E[d,b]\cap\bar{E}[0,c^{(1)}]\cap E[0,c^{(2)}])\cap(E[n,a]\cap\bar{E}[d,b]).$$

Hence

$$F=(\bar{E}[0,c^{(1)}]\cap E[0,c^{(2)}]\cap G)\cup H$$

where

$$G=E[d,b]\cap\bigcap_{0<i<m}\bar{E}[n_i,a^{(i)}],\qquad H=E[n,a]\cap\bar{E}[d,b]\cap\bigcap_{0<i<m}\bar{E}[n_i,a^{(i)}].$$

Consider G. The first index of G equals $d<n$. Consider H. The first index of H is equal to n, but the second index of H is equal to $r-1$.

Thus the proof is completed.

LEMMA 4.14. *For any integers $m>0$, $n_0,\dots,n_{m-1}>0$ and for any sequences $a^{(0)},\dots,a^{(m-1)}$,*

$$\text{if}\quad F=\bigcap_{i<m}\bar{E}[n_i,a^{(i)}],\quad\text{then}\quad \vee_0 F\in|\boldsymbol{B}|.$$

Proof. Let n be the least common multiple of $n_0,\dots,n_{m-1}$. We assume that:

1^0 n/n_i is a product of k_i primes and $k=\max(k_i)$.

2^0 Among $k_0,\dots,k_{m-1}$ there are exactly l integers equal to k.

Let us refer to k and l as the first and the second index of F. We carry out a simultaneous induction with respect to k and l.

If $k=0$, the problem is reduced to 4.4.

Suppose that $k>0$ and assume that the theorem is already proved for arbitrary l in the case when the first index is less than k. For simplicity let $k_0=k$. We decompose F by means of the function $E[pn_0,pa^{(0)}]$ and by the method of adjunction we pass from F to the functions

$$G=E[pn_0,pa^{(0)}]\cap\bigcap_{i<m}\bar{E}[n_i,a^{(i)}] \quad\text{and}\quad H=\bar{E}[pn_0,pa^{(0)}]\cap\bigcap_{0<i<m}\bar{E}[n_i,a^{(i)}].$$

G is subject to 4.13. Consider H. If $l=1$, then the first index of H is less than k. If $l>1$, then the first index of H is equal to k, but the second index of H is equal to $l-1$.

Thus the proof is completed.

LEMMA 4.15. *For any prime p, for any integer $l>0$, and for any sequence a*

$$\text{if}\quad F=C[p^l;1,a],\quad \text{then}\quad \vee_0 F\in|\boldsymbol{B}|.$$

Proof. We have $\vee_0 F=U\in|\boldsymbol{B}|$.

LEMMA 4.16. *For any prime p, for any integers k,l such that $l>k\geqslant 0$, and for any sequence a,*

$$\text{if}\quad F=C[p^l;p^k,a],\quad \text{then}\quad \vee_0 F\in|\boldsymbol{B}|.$$

Proof. By 3.10 (ix), (iii) we have

$$F\subseteq C[p^k;p^k,a]\subseteq C[p^k;0,a],$$

hence by 2.7 (ii) we obtain $\vee_0 F\subseteq C[p^k;0,a]$. Using the sequence method we can show that also $C[p^k;0,a]\subseteq\vee_0 F$. Thus $\vee_0 F=C[p^k;0,a]\in|\boldsymbol{B}|$.

LEMMA 4.17. *For any prime p, for any integers $m>0$, and k,l such that $l>k\geqslant 0$, and for any sequences $a^{(0)},\dots,a^{(m-1)}$,*

$$\text{if}\quad F=\bigcap_{i<m}(C[p^{l-1};p^k,a^{(i)}]\cap\bar{C}[p^l;p^k,a^{(i)}]),\quad \text{then}\quad \vee_0 F\in|\boldsymbol{B}|.$$

(Remark. If $l=1$, we consider $F=\bigcap_{i<m}\bar{C}[p;1,a^{(i)}]$.)

Proof. The procedure is similar to that used in the proof of 4.7. We consider the more difficult case when $k>0$ and decompose F by

means of the functions $C[p^l;a^{(i)}-a^{(j)}]$ for $i<j<m$. By the method of adjunction we pass from F to the function

$$G=\bigcap_{i\in M}(C[p^{l-1},p^k,a^{(i)}]\cap\bar{C}[p^l;p^k,a^{(i)}]\cap\bigcap_{\substack{i,j\in M\\ i<j}}\bar{C}[p^l;0,a^{(i)}-a^{(j)}]$$

where $0\neq M\subseteq m$. Let the set M consist of r integers and assume for simplicity that $0\in M$. By the sequence method we can now show easily (see Definition 3.17) that

$$\vee_0 G=L^{(2)}[p,l,r+1]\cap\bigcap_{0<i\in M}(C[p^{l-1};0,a^{(0)}-a^{(i)}]\cap\bar{C}[p^l;0,a^{(0)}-a^{(i)}]$$
$$\cap\bigcap_{\substack{0<i,j\in M\\ i<j}}\bar{C}[p^l;0,a^{(i)}-a^{(j)}]\cap C[p^k;0,a^{(0)}],$$

which, by Theorem 3.19, completes the proof.

LEMMA 4.18. *Given an integer $m>0$; let*

$$F=\bigcap_{i<m}F_i,$$

where, for $i=0,1,\dots,m-1$, F_i is either

an equality function $E[n,a]$ or an inequality function $\bar{E}[n,a]$, where $n>0$,

or

a congruence function $C[p^l;p^k,a]$ or a complex function $C[p^{l-1};p^k,a]\cap\bar{C}[p^l;p^k,a]$, where $l>k\geqslant 0$.

With these assumptions $\vee_0 F\in|\boldsymbol{B}|$.

Proof. We shall refer to n,p,k,l,a as $n_i,p_i,k_i,l_i,a^{(i)}$ whenever dealing with a special F_i.

Our proof is divided into two parts. In the first part we prove the lemma by the additional assumption that

(1) *whenever F_i $(i=0,1,\dots,m-1)$ is a congruence function or a complex function and F_j $(j=0,1,\dots,m-1)$ is an inequality function, then $p_i^{k_i}$ is a divisor of n_j.*

In the second part we reduce the general case to the preceeding one.

I. The condition (1) holds. We carry out the induction with respect to m. We shall refer to m as the length of F. For $m=1$ the problem is reduced to one of lemmata 4.1, 4.2, 4.4, 4.15, 4.16 and 4.17. Now assume that the lemma is already proved in the case when the length of F is less than m and suppose that F is of the length $m>1$. Several cases will be now considered. In some of them we shall combine the fundamental induction with respect to m with another induction with respect to a variable which will be mentioned separately each time.

1^0 For some different non-negative integers $r,s<m$, F_r and F_s are equality functions.

Let $d=(n_r,n_s)$. By 4.15 (i) there are sequences $a,b^{(1)}$, and $b^{(2)}$ such that $F_r\cap F_s=E[d,a]\cap E[0,b^{(1)}]\cap E[0,b^{(2)}]$. Hence we can easily pass from F to a function of the length $m-1$.

Analogous reasoning leads from F to a function of the length $m-1$ when one of the following three conditions 2^0, 3^0 and 4^0 is satisfied:

2^0 For some non-negative integers $r,s<m$, F_r is an equality function, F_s is a congruence or a complex function and $p_s^{k_s+1}$ is not a divisor of n_r (cf. Theorem 3.14).

3^0 For some different non-negative integers $r,s<m$, F_r is a congruence function, F_s is a congruence or a complex function and $p_r=p_s$, $k_r\leqslant k_s$, $l_r-k_r\geqslant l_s-k_s$ (cf. Theorem 3.13).

4^0 For some non-negative integers $r,s<m$, F_r and F_s are complex functions and $p_r=p_s$, $k_r=k_s$, $l_r\neq l_s$ (cf. again Theorem 3.13).

5^0 For a non-negative integer $r<m$, F_r is a congruence function and whenever F_i $(i=0,1,\dots,m-1)$ is a congruence or a complex function with $p_i=p_r$, then $k_i\geqslant k_r$.

Assume, for simplicity, that $r=0$ and let $p_0=p$, $k_0=k$, $l_0=l$ and $a^{(0)}=a$. Hence we have $F_0=C[p^l;p^k,a]$ and

(2) *whenever* F_i $(i=1,2,\dots,m-1)$ *is a congruence or a complex function with* $p_i=p$, *then* $k_i\geqslant k$.

Since the cases 2^0 and 3^0 are already taken care of, we can also assume that

(3) *whenever* F_i $(i=1,2,\dots,m-1)$ *is an equality function, then* p^{k+1} *is a divisor of* n_i,

(4) *whenever* F_i $(i=1,2,\dots,m-1)$ *is a congruence or a complex function with* $p_i=p$, *then* $l_i-k_i>l-k$.

Now we define two sequences d and b in the following way:

(5) *For* $i=0,1,\dots,m-1$

$d_i=n_i$ *and* $b^{(i)}=a^{(i)}$ *whenever* F_i *is an equality or an inequality function*;

$d_i=p_i^{k_i}$ *and* $b^{(i)}=a^{(i)}$ *whenever* F_i *is a congruence or a complex function with* $p_i=p$;

$d_i=p^kp_i^{k_i}$ *and* $b^{(i)}=p^ka^{(i)}$ *whenever* F *is a congruence or a complex function with* $p_i\neq p$.

Then let for $i=1,2,\dots,m-1$, for every integer $t>0$, and for every sequence c

$$G[t,c]=\begin{cases} E[t,c] & \text{whenever } F_i \text{ is an equality function,}\\ \bar{E}[t,c] & \text{whenever } F \text{ is an inequality function,}\\ C[p_i^l;t,c] & \text{whenever } F_i \text{ is a congruence function,}\\ C[p^{l_i-1};t,c]\cap\bar{C}[p_i^{l_i};t,c] & \text{whenever } F_i \text{ is a complex function.}\end{cases}$$

If $k=0$, one can easily check by the sequence method that

$$\vee_0F=\vee_0\bigcap_{0<i<m}G_i[p^ld_i,b^{(i)}-d_ia].$$

Hence (using Theorem 3.15) we can pass from F to a function of the length $m-1$.

If $k>1$, then by (1), (2), (3), and (5) we have, for $i=1,2,\dots,m-1$, $d_i=p^ks_i$ for some $s_i>0$ and one can easily check by the sequence method

$$\vee_0F=\vee_0\{C[p^k;1,\langle 0\rangle]\cap C[p^l;1,a]\cap\bigcap_{0<i<m}G_i[s_i,b^{(i)}]\}.$$

But

$$C[p^k;1,\langle 0\rangle]\cap C[p^l;1,a]=C[p^k;0,a]\cap C[p^l;1,a]$$

hence we return to the preceding case when $k_0=0$ (in fact, $1=p^0$).

6^0 For a non-negative integer $s<m$, F_s is a complex function and, for $i=0,1,\dots,m-1$, whenever F is a congruence function with $p_i=p_s$, then $k_i>k_s$; whenever F_i is a complex function with $p=p_s$, then $k_i\geqslant k_s$; whenever F_i is an inequality function, then p_s is a divisor of n_i.

Assume for simplicity that $s=0$ and set $p_0=p$, $k_0=k$, $l_0=l$ and $a^{(0)}=a$. Hence we have $F_0=C[p^{l-1};p^k,a]\cap\bar{C}[p^l;p^k,a]$ and

(6) *whenever* F_i $(i=1,2,\dots,m-1)$ *is a congruence function with* $p_i=p$, *then* $k_i>k$,

(7) *whenever* F_i $(i=1,2,\dots,m-1)$ *is a complex function with* $p_i=p$, *then* $k_i\geqslant k$,

(8) *whenever* F_i $(i=1,2,\dots,m-1)$ *is an inequality function, then* p^{k+1} *is a divisor of* n_i.

Since the cases 2^0 and 4^0 are already taken care of, we can assume (3) and

(9) *whenever* F_i $(i=1,2,\dots,m-1)$ *is a complex function with* $p_i=p$ *and* $k_i=k$, *then* $l_i=l$.

Let us assume for simplicity that there exists a positive integer $r\leqslant m$ such that the functions F_i for $i<r$ are all complex functions with $p=p$, $k_i=k$ and $l_i=l$. If $r=m$, the problem is reduced to 4.17. Suppose now that $r<m$. Putting for $i=0,1,\dots,m-1$

$$e_i=\begin{cases} n_i & \text{whenever } F_i \text{ is an equality or an inequality function,}\\ p_i^{k_i} & \text{whenever } F \text{ is a congruence or a complex function}\end{cases}$$

we define e as the least common multiple of $e_0,\dots,e_{m-1}$. Of course e is divisible by p^k. Let $e=p^{k+h}e'$, where $(p,e')=1$. We start the induction with respect to h. We shall refer to h as the first index of F.

Consider the case when $h=0$. It follows from (3) and (6)-(9) that

(10) *for* $i=r,r+1,\dots,m-1$, F_i *is a congruence or a complex function with* $p_i \neq p$.

We assert that $\vee_0 F = \vee_0 \bigcap_{i<r} F_i \cap \vee_0 \bigcap_{r\leqslant i<m} F_i$. In the proof we use the sequence method. Let $\mathfrak{A} \in \mathcal{AG}$ and

$$x \in \vee_0 \bigcap_{i<r} F_i \cap \vee_0 \bigcap_{r\leqslant i<m} F_i(\mathfrak{A}).$$

Then there are sequences $x^{(1)}, x^{(2)} \in \mathfrak{A}_0^\omega$ such that

$$x_i^{(1)} = x_i^{(2)} = x_i \quad \text{for} \quad i>0, \tag{11}$$

$$x^{(1)} \in \bigcap_{i<r} F_i(\mathfrak{A}), \tag{12}$$

$$x^{(2)} \in \bigcap_{r\leqslant i<m} F_i(\mathfrak{A}). \tag{13}$$

Let

(14) t *=the least common multiple of* $p_i^{l_i-k_i}$ for $i=r,r+1,\dots,m-1$

and (see (10))

$$up^l + vt = 1. \tag{15}$$

Consider now a sequence $x^{(3)}$ defined in the following way:

$$x_0^{(3)} = (up^l)x_0^{(1)} + (vt)x_0^{(2)}, \tag{16}$$

$$x_i^{(3)} = x_i \quad \text{for} \quad i>0. \tag{17}$$

By (14)-(16) we have for $i=r,r+1,\dots,m-1$

$$p^k x_0^{(3)} = p^k(up^l)x_0^{(1)} + p^k(1-up^l)x_0^{(2)} = p^k x_0^{(2)} + p^l(up^k)(x_0^{(1)} - x_0^{(2)}),$$

$$p_i^{k_i} x_0^{(3)} = p_i^{k_i}(1-vt)x_0^{(1)} + p_i^{k_i}(vt)x_0^{(2)} = p_i^{k_i}x_0^{(1)} + p_i^{l_i}\left(v\frac{t}{p_i^{l_i-k_i}}\right)(x_0^{(2)} - x_0^{(1)}),$$

hence we obtain $p^k x_0^{(3)} \equiv p^k x_0^{(2)} \pmod{p^l}$ and $p_i^{k_i} x_0^{(3)} \equiv p_i^{k_i} x_0^{(1)} \pmod{p_i^{l_i}}$ for $i=r,r+1,\dots,m-1$, which together with (11)-(13) and (17) implies that $x^{(3)} \in F(\mathfrak{A})$. Therefore $x \in \vee_0 F(\mathfrak{A})$ and

$$\vee_0 \bigcap_{i<r} F_i \cap \vee_0 \bigcap_{r\leqslant i<m} F_i \subset \vee_0 F.$$

The inclusion in the opposite direction follows immediately from 2.8 (iv). Hence $\vee_0 F = \vee_0 \bigcap_{i<r} F_i \cap \vee_0 \bigcap_{r\leqslant i<m} F_i$ and the problem is reduced to studying functions of the length less than m.

Assume now that $h>0$ and let $G = \bigcap_{r\leqslant i<m} F$. We decompose F by means of the functions $C[p^{l+1}; p^{k+1}, pa^{(i)}]$ for $i=0,1,\dots,r-1$ and by the method of adjunction we pass from F to the functions

$$F^{(1)} = \bigcap_{i<r} (F_i \cap \bar{C}[p^{l+1}; p^{k+1}, pa^{(i)}]) \cap G,$$

$$F^{(2)} = \bigcap_{i\in M} (F_i \cap C[p^{l+1}; p^{k+1}, pa^{(i)}]) \cap \bigcap_{i\in r-M} (F_i \cap \bar{C}[p^{l+1}; p^{k+1}, pa^{(i)}]) \cap G$$

for $0 \neq M \subseteq r$.

By 3.10 (vii) we have

$$F^{(1)} = \bigcap_{i<r} (C[p^{l-1}; p^k, a^{(i)}] \cap C[p^l; p^{k+1}, pa^{(i)}] \cap \bar{C}[p^{l+1}; p^{k+1}, pa^{(i)}]) \cap G$$
$$= \bigcap_{0<i<r} C[p^{l-1}; 0, a^{(i)} - a] \cap F^{(3)}$$

where

$$F^{(3)} = C[p^{l-1}; p^k, a] \cap \bigcap_{i<r} (C[p^l; p^{k+1}, pa^{(i)}] \cap \bar{C}[p^{l+1}; p^{k+1}, pa^{(i)}]) \cap G.$$

It should be noticed that the length of $F^{(3)}$ equals $m+1$, but it is easy to check that if we proceed as in case 5° we pass to a function of the kind 6° whose length equals m and whose first index is less than h.

Let us consider $F^{(2)}$ for a fixed M and assume for simplicity that $0 \in M$. Hence we have

$$F^{(2)} = \bigcap_{i\in r-M} (C[p^{l-1}, 0, a^{(i)} - a] \cap \bar{C}[p^{l+1}; 0, pa^{(i)} - pa] \cap F^{(4)}$$

where

$$F^{(4)} = \bigcap_{i\in M} (F_i \cap C[p^{l+1}; p^{k+1}, pa^{(i)}]) \cap G.$$

Thus it is sufficient to study the function $F^{(4)}$.

We decompose F by means of the functions $C[p^l; 0, a^{(i)} - a^{(j)}]$ for $i,j \in M$ and $i<j$. Since

$$C[p^{l-1}; p^k, a^{(i)}] \cap \bar{C}[p^l; p^k, a^{(i)}] \cap C[p^{l+1}; p^{k+1}, pa^{(i)}]$$
$$\cap C[p^{l-1}; p^k, a^{(j)}] \cap \bar{C}[p^l; p^k, a^{(j)}] \cap C[p^{l+1}; p^{k+1}, pa^{(j)}] \cap C[p^l; 0, a^{(i)} - a^{(j)}]$$
$$= C[p^{l-1}; p^k, a^{(i)}] \cap \bar{C}[p^l; p^k, a^{(i)}] \cap C[p^{l+1}; p^{k+1}, pa^{(i)}] \cap C[p^l; 0, a^{(i)} - a^{(j)}],$$

therefore we pass by the method of adjunction from $F^{(4)}$ to the functions

$$F^{(5)} = \bigcap_{i\in N} (F_i \cap C[p^{l+1}; p^{k+1}, pa^{(i)}]) \cap \bigcap_{\substack{i,j\in N \\ i<j}} \bar{C}[p^l; 0, a^{(i)} - a^{(j)}] \cap G$$

for $0 \neq N \subseteq M$.

Suppose that

(18) N *consists of* n *(different) integers,*

and let

$$F^{(6)}=L^{(3)}[p;l,n+1]\cap\bigcap_{i\in N}(C[p^{l-1};p^k,a^{(i)}]\cap C[p^{l+1};p^{k+1},pa^{(i)}])$$
$$\cap\bigcap_{\substack{i,j\in N\\ i<j}}\bar{C}[p^l;0,a^{(i)}-a^{(j)}]\cap G.$$

We assert that $\vee_0F^{(6)}=\vee_0F^{(6)}$. To show it we use the sequence method. Consider an arbitrary group $\mathfrak{A}\in\mathcal{AG}$ and let $x^{(1)}\in\vee_0F^{(6)}(\mathfrak{A})$.

Thus for some $x\in\mathfrak{A}_0^\omega$ we have

(19) $$x_i=x_i^{(1)} \quad \text{for} \quad i>0,$$

(20) $$x\in C[p^{l-1};p^k,a^{(i)}](\mathfrak{A}) \quad \text{for} \quad i\in N,$$

(21) $$x\in\bar{C}[p^l;p^k,a^{(i)}](\mathfrak{A}) \quad \text{for} \quad i\in N,$$

(22) $$x\in C[p^{l+1};p^{k+1},pa^{(i)}](\mathfrak{A}) \quad \text{for} \quad i\in N,$$

(23) $$x\in\bar{C}[p^l;0,a^{(i)}-a^{(j)}](\mathfrak{A}) \quad \text{for} \quad i,j\in N \quad \text{and} \quad i<j,$$

(24) $$x\in G(\mathfrak{A}).$$

Let

(25) $$w_i=\sum_{j\in D(a^{(i)})}a_j^{(i)}x_{j+1} \quad \text{for} \quad i\in N.$$

It follows from (37)-(40) that

(26) $$p^kx_0+w_i\equiv 0 \pmod{p^{l-1}} \quad \text{for} \quad i\in N,$$
$$p^kx_0+w_i\not\equiv 0 \pmod{p^l} \quad \text{for} \quad i\in N,$$

(27) $$p^{k+1}x_0+pw\equiv 0 \pmod{p^{l+1}} \quad \text{for} \quad i\in N,$$

(28) $$w_i\not\equiv w_j \pmod{p^l} \quad \text{for} \quad i,j\in N \quad \text{and} \quad i<j;$$

therefore there exists a $y\in\mathfrak{A}_0^N$ such that $p(p^kx_0+w_i)=p^{l+1}y_i$ for $i\in N$, and then a $z\in\mathfrak{A}_0^N$ such that $p^kx_0+w_i=p^ly_i+z_i$ for $i\in N$,

(29) $$z_i\equiv 0 \pmod{p^{l-1}} \quad \text{for} \quad i\in N,$$

(30) $$z_i\not\equiv 0 \pmod{p^l} \quad \text{for} \quad i\in N,$$

(31) $$pz_i=0 \quad \text{for} \quad i\in N,$$

(32) $$z_i\not\equiv z_j \pmod{p^l} \quad \text{for} \quad i,j\in N \text{ and } i\neq j.$$

Thus from (18), (29)-(32) and Definition 3.17 (iii) we obtain

(33) $$L^{(3)}[p,l,n+1](\mathfrak{A})=\mathfrak{A}_0^\omega$$

hence

(34) $$x\in L^{(3)}[p,l,n+1](\mathfrak{A}),$$

which together with (19), (20), and (22)-(24) gives $x^{(1)}\in\vee_0F^{(6)}$. Hence

(35) $$\vee_0F^{(3)}\subseteq\vee_0F^{(6)}.$$

Conversely, assume that $x^{(1)}\in\vee_0F^{(6)}$. Then we have (19), (20), (22)-(24), and (34) for some $x\in\mathfrak{A}_0^\omega$. If we also have (21), we immediately conclude that $x^{(1)}\in\vee_0F^{(6)}(\mathfrak{A})$. Thus let us assume for simplicity that

(36) $$0\in N,$$

(37) $$x\in C[p^l;p^k,a^{(0)}](\mathfrak{A}).$$

Assume (25). We again have (26)-(28) and we obtain from (37)

(38) $$p^kx_0+w_0\equiv 0 \pmod{p^l},$$

from (28) and (38)

$$p^kx_0+w_i\not\equiv 0 \pmod{p^l} \quad \text{for} \quad i\in N-\{0\},$$

hence for some $y,z\in\mathfrak{A}_0^{N-\{0\}}$

(39) $$p^kx_0+w_i=p^ly_i+z_i,$$

$z_i\equiv 0 \pmod{p^{l-1}}$, $z_i\not\equiv 0 \pmod{p^l}$, $pz_i=0$, and $z_i\not\equiv z_j \pmod{p^l}$ for $i\neq j$.

Then we obtain (33) from (34). Thus it can easily be shown by (18) and (36) that there must be an element $z_0\in\mathfrak{A}_0$ with the following properties:

$$z_0\equiv 0 \pmod{p^{l-1}},$$

(40) $$z_0\not\equiv 0 \pmod{p^l},$$

(41) $$pz_0=0,$$

(42) $$z_0\not\equiv z_i \pmod{p^l} \quad \text{for} \quad i\in N-\{0\}.$$

Let

(43) $$z_0=p^{l-1}z_0'.$$

Now we construct a sequence $x^{(2)}\in\mathfrak{A}_0^\omega$ as follows:

(44) $$x_0^{(2)}=x_0-p^{l-1-k}z_0',$$

(45) $$x_i^{(2)}=x_i \quad \text{for} \quad i>0.$$

We obtain from (25) and (45)

$$w_i=\sum_{j\in D(a^{(i)})}a_j^{(i)}x_{j+1},$$

from (26)

$$p^kx_0^{(2)}+w_i\equiv 0 \pmod{p^{l-1}} \quad \text{for} \quad i\in N.$$

Then it follows from (43) and (44) that

$$p^kx_0^{(2)}+w_i=p^kx_0-z_0+w_i \quad \text{for} \quad i\in N,$$

hence by (39) and (42)

$$p^k x_0^{(2)} + w_i \not\equiv 0 \pmod{p^l} \quad \text{for} \quad i \in N - \{0\}$$

and by (38) and (40)

$$p^k x_0^{(2)} + w_0 \not\equiv 0 \pmod{p^l}.$$

Finally by (41), (43), and (44) we have $p^{k+1} x_0^{(2)} = p^{k+1} x_0$. Thus we obtain

$$x^{(2)} \in C[p^{l-1}; p^k, a^{(i)}](\mathfrak{A}) \quad \text{for} \quad i \in N,$$

$$x^{(2)} \in \bar{C}[p^l; p^k, a^{(i)}](\mathfrak{A}) \quad \text{for} \quad i \in N,$$

$$x^{(2)} \in C[p^{l+1}; p^{k+1}, pa^{(i)}](\mathfrak{A}) \quad \text{for} \quad i \in N,$$

then by (28)

$$x^{(2)} \in \bar{C}[p^l; 0, a^{(i)} - a^{(j)}](\mathfrak{A}) \quad \text{for} \quad i, j \in N \text{ and } i < j,$$

finally by (3) and (6)-(9) we have $x^{(2)} \in G(\mathfrak{A})$. Hence it follows from (19) and (45) that $x^{(1)} \in \vee_0 F^{(5)}(\mathfrak{A})$ and we obtain $\vee_0 F^{(6)} \subseteq \vee_0 F^{(5)}$ which together with (35) gives $\vee_0 F^{(6)} = \vee_0 F^{(5)}$.

In this way (see Theorem 3.19) we have reduced the problem to that of studying the function

$$F^{(7)} = \bigcap_{i \in N} (C[p^{l-1}; p^k, a^{(i)}] \cap C[p^{l+1}; p^{k+1}, pa^{(i)}]) \cap G.$$

But

$$F^{(7)} = \bigcap_{0 < i \in N} C[p^{l-1}; 0, a^{(i)} - a^{(0)}] \cap F^{(8)},$$

where

$$F^{(8)} = C[p^{l-1}; p^k, a^{(0)}] \cap \bigcap_{i \in N} C[p^{l+1}; p^{k+1}, pa^{(i)}] \cap G.$$

Notice that the length of the function $F^{(8)}$ is $\leqslant m+1$. But it is easy to check that if we proceed as in case 5° we pass to a function of the kind 5°, whose length is $\leqslant m$.

7° As in 6°, we assume that

$$F_0 = C[p^{l-1}; p^k, a] \cap \bar{C}[p^l, p^k, a] \tag{46}$$

and that (6) and (7) hold. But we do not assume (8).

Among the functions $F_1, \ldots, F_{m-1}$ let there be exactly r inequality functions F_i with n_i not divisible by p^{k+1}. We carry out the induction with respect to r. We shall refer to r as the second index of F. If $r=0$, the problem is reduced to the case 6°. Thus let $r>0$ and assume for simplicity that F_1 is an inequality function and n_1, which by (1) is divisible by p^k, is not divisible by p^{k+1}. Let $n = n_1$ and $b = a^{(1)}$. Hence

$$F_1 = \bar{E}[n, b], \tag{47}$$

$$n = p^k s, \tag{48}$$

where

$$(p, s) = 1. \tag{49}$$

Then let

$$tp^l + us = 1. \tag{50}$$

By (46) and (47) we have

$$F_0 \cap F_1 = F_0 \cap F_1 \cap (\bar{C}[p^{l-1}; n, b] \cup C[p^{l-1}; n, b])$$
$$= (F_0 \cap \bar{C}[p^{l-1}; n, b]) \cup (F_0 \cap F_1 \cap C[p^{l-1}; n, b];$$

then from (48) we obtain

$$F_0 \cap \bar{C}[p^{l-1}; n, b] = F_0 \cap \bar{C}[p^{l-1}; 0, b - sa],$$

and we obviously have

$$F_0 \cap F_1 \cap C[p^{l-1}; n, b] = F_0 \cap F_1 \cap C[p^{l-1}; n, b] \cap (\bar{C}[p^l; n, b] \cup C[p^l; n, b])$$
$$= (F_0 \cap C[p^{l-1}; n, b] \cap \bar{C}[p^l; n, b]) \cup (F_0 \cap F_1 \cap C[p^l; n, b]).$$

Finally from (49) and (50) it follows by means of Theorem 3.15 that

$$F_0 \cap C[p^{l-1}; n, b] \cap \bar{C}[p^l; n, b] = F_0 \cap C[p^{l-1}; p^k, ub] \cap \bar{C}[p^l; p^k, ub],$$

$$F_0 \cap F_1 \cap C[p^l; n, b] = F_0 \cap F_1 \cap C[p^l; p^k, ub]$$
$$= C[p^{l-1}; 0, a - ub] \cap C[p^l; 0, a - ub] \cap F_1 \cap C[p^l; p^k, ub].$$

Hence it is sufficient to consider the following three functions:

$$F^{(1)} = F_0 \cap \bigcap_{1 < i < m} F_i,$$

$$F^{(2)} = F_0 \cap (C[p^{l-1}; p^k, ub] \cap \bar{C}[p^l; p^k, ub]) \cap \bigcap_{1 < i < m} F_i,$$

$$F^{(3)} = C[p^l; p^k, ub] \cap \bigcap_{0 < i < m} F_i.$$

But $F^{(1)}$ is of the length $m-1$, $F^{(2)}$ is of the length m but its second index is equal to $r-1$; finally $F^{(3)}$ is of the length m and is submitted to case 5°.

Hence case 7° is settled, which together with 1°-6° and Theorem 4.14 completes the proof of part I.

II. We do not assume (1). Assume that in the cardinal product $m \times m$ there are exactly r pairs $\langle i, j \rangle$ which satisfy the following condition: F_i is a congruence or a complex function, F_j is an inequality function, $p_i^{k_i}$ is not a divisor of n_j.

We carry out the induction with respect to r. We shall refer to r as the third index of F. If $r=0$, the problem is reduced to I. Assume now that $r>0$ and let, for simplicity, F_0 be a congruence function,

$$F_0 = C[p^l; p^k, a]$$

(the proof in the case when F_0 is a complex function is analogous), F_1 — an inequality function, $F_1 = \bar{E}[n, b]$, and p^k not a divisor of n. Let $n = p^d s$,

where $(p,s)=1$. We clearly have $d<k$. Then, by Theorem 3.14, there is a sequence c such that

$$F_0 \cap F_1 = F_0 \cap F_1 \cap (E[p^k s, p^{k-d}b] \cup \bar{E}[p^k s, p^{k-d}b])$$
$$= (C[p^l; 0, c] \cap E[p^k s, p^{k-d}b] \cap F_1) \cup (F_0 \cap \bar{E}[p^k s, p^{k-d}b]).$$

Thus the problem is reduced to studying two functions

$$F^{(1)} = E[p^k s, p^{k-d}b] \cap \bigcap_{0<i<m} F_i \quad \text{and} \quad F_2 = F_0 \cap \bar{E}[p^k s, p^{k-d}b] \cap \bigcap_{1<i<m} F_i$$

both having the third index less than r.

LEMMA 4.19. *Given an integer $m>0$, let*

$$F = \bigcap_{i<m} F_i,$$

where, for $i=0,1,\ldots,m-1$, F is either

(1) *an equality function $E[n,a]$ or an inequality function $\bar{E}[n,a]$, where $n>0$,*

or

(2) *a congruence function $C[p^l; p^k, a]$ or an incongruence function $\bar{C}[p^l; p^k, a]$, where $l>k\geqslant 0$.*

With these assumptions

(3) $$\vee_0 F \in |\boldsymbol{B}|.$$

Proof. It is convenient to prove an apparently more general statement:

Given an integer $m>0$, let $F=\bigcap_{i<m} F_i$, where, for $i=0,1,\ldots,m-1$, F_i is either (1), or (2), or a complex function $C[p^{l-1}; p^k, a] \cap \bar{C}[p^l; p^k, a]$, where $l>k\geqslant 0$. With these assumptions (3) holds.

We shall refer to n,p,k,l,a as $n_i,p_i,k_i,l_i,a^{(i)}$ whenever dealing with a special F_i.

Assume that there are exactly r incongruence functions among F_i $(i=0,1,\ldots,m-1)$; for simplicity let $F_0,\ldots,F_{r-1}$ be those functions. Let s be the minimum of all differences l_i-k_i for $i<r$. We carry out the double induction with respect to r and s. We shall refer to r and s as the first and the second index of F, respectively. If $r=0$, then the problem is reduced to 4.18. Let $r>0$ and suppose that the theorem is already proved for arbitrary s in the case when the first index equals $r-1$. F_0 is an incongruence function now. Let $p=p_0$, $k=k_0$, $l=l_0$, $a=a^{(0)}$ and assume for simplicity that $s=l-k$. We have

$$\bar{C}[p^l; p^k, a] = (C[p^{l-1}; p^k, a] \cap \bar{C}[p^l; p^k, a]) \cup \bar{C}[p^{l-1}; p^k, a],$$

therefore the problem is reduced to studying two functions

$$F^{(1)} = C[p^{l-1}; p^k, a] \cap \bar{C}[p^l; p^k, a] \cap \bigcap_{0<i<m} F_i \quad \text{and} \quad F^{(2)} = \bar{C}[p^{l-1}; p^k, a] \cap \bigcap_{0<i<m} F_i.$$

The function $F^{(1)}$ has the first index equal to $r-1$. In turn consider the function $F^{(2)}$. If $s=1$, then $l-1=k$ and we obtain

$$F^{(2)} = \bar{C}[p^{l-1}; 0, a] \cap \bigcap_{0<i<m} F_i,$$

but the function $\bigcap_{0<i<m} F_i$ has the first index equal to $r-1$. If $s>1$, then the function $F^{(2)}$ has the first index equal to r, but the second index equal to $s-1$.

From Lemma 4.19 follows at once (by means of Theorem 3.10 (xi))

THEOREM 4.20. *Given a sequence $\langle F_0,\ldots,F_{m-1}\rangle$ such that for $i=0,1,\ldots,m-1$, $F_i \in \boldsymbol{B}$ or $\bar{F}_i \in \boldsymbol{B}$ and $0 \in \mathrm{Dm}(F_i)$, we have*

$$\vee_0 \bigcap_{i<m} F_i \in |\boldsymbol{B}|.$$

By Theorems 3.5, 3.6, 3.8, 3.9, and 4.20 the set $\boldsymbol{B}$ of basic functions for Abelian groups satisfies the conditions (i)-(v) of Theorem 2.18. Thus the following two theorems hold

THEOREM 4.21 (Fundamental theorem on arithmetical functions).

$$\boldsymbol{AF}(\mathcal{AG}) = |\boldsymbol{B}|.$$

THEOREM 4.22 (Fundamental theorem on arithmetical classes) [16].

$$\boldsymbol{AC}(\mathcal{AG}) = |\boldsymbol{C}|.$$

(The set $|\boldsymbol{C}|$ is determined in the Remark following Theorem 3.7.)

Thus we have arrived at a complete description of all arithmetical classes of Abelian groups: Every arithmetical class in $\mathcal{AG}$ can be represented as a union of intersections of basic arithmetical classes and complements of basic arithmetical classes. Of course, this representation is not unique and the problem arises when two unions of intersections of arithmetical classes and complements of arithmetical classes are identical. It is easy to see that this problem is reducible to the problem of finding a necessary and sufficient condition for

(1) $$\bigcup_{i<m} \bigcap_{j<n_i} S_{ij} = \mathcal{AG}$$

where for $i=0,1,\ldots,m-1$ and $j=0,1,\ldots,n_i-1$, either $S_{ij} \in \boldsymbol{C}$ or $\bar{S}_{ij} \in \boldsymbol{C}$. In this form the problem is very important from a meta-mathematical point of view; this will be considered at the end of Chapter 6.

[16] This theorem is formulated (without proof) in [7].

Of course, instead of (1), we can study the equalities of the form

$$\bigcup_{i<m} \bigcap_{j<n_i} S_{ij} = 0,$$

hence the problem is reduced to finding a necessary and sufficient condition for $\bigcap_{j<n} S_j = 0$ where for $j = 0,1,\ldots,n-1$, either $S_j \in \boldsymbol{C}$ or $\overline{S} \in \boldsymbol{C}$. This condition is easily found, yet rather involved in formulation; for these reasons we shall not state it explicitly. We only observe that by Theorem 3.16 we can easily reduce the problem which involves arbitrary intersections to that of studying intersections of a certain standard form, which are empty only if they contain two complementary factors S and $\overline{S}$, since otherwise, in each particular case, an Abelian group (in fact, a cardinal product of certain among groups $\mathfrak{R}_p$, $\mathfrak{C}_p$, and $\mathfrak{C}_{pk}$) which belongs to this intersection can be found.

Chapter 5. Fundamental theorem on arithmetical types of Abelian groups

As an immediate consequence of Definition 2.16 and Fundamental theorem on arithmetical classes we obtain the following condition sufficient for two Abelian groups to be arithmetically equivalent.

THEOREM 5.1. *Two Abelian groups* $\mathfrak{A}$ *and* $\mathfrak{B}$ *are given. If for every basic arithmetical class* S $(S \in \boldsymbol{C})$

$$\text{either} \quad \mathfrak{A},\mathfrak{B} \in S \quad \text{or} \quad \mathfrak{A},\mathfrak{B} \notin S,$$

then $\mathfrak{A} \approx \mathfrak{B}$.

THEOREM 5.2 (Fundamental theorem on arithmetical equivalence). *Two algebras* $\mathfrak{A},\mathfrak{B} \in \mathcal{AG}$ *are given. For*

$$\mathfrak{A} \approx \mathfrak{B}$$

it is necessary and sufficient that the following two conditions be satisfied:

(I) *For every prime* p *and for every integer* $k>0$

$$\varrho^{(i)}[p,k](\mathfrak{A}) = \varrho^{(i)}[p,k](\mathfrak{B}) \qquad (i=1,2,3),$$

(II) $\mathfrak{A}$ *and* $\mathfrak{B}$ *are either both of the first or both of the second kind.*

Proof. Suppose that $\mathfrak{A} \approx \mathfrak{B}$. By Definition 2.16 (i) for an arbitrary prime p, for an arbitrary integer $k>0$, and for $i=1,2,3$, three eventualities are possible:

1° $\quad \mathfrak{A},\mathfrak{B} \notin \mathcal{R}^{(i)}[p,k,1]$,

hence

$$\varrho^{(i)}[p,k](\mathfrak{A}) = \varrho^{(i)}[p,k](\mathfrak{B}) = 0.$$

2° There is an integer n such that

$$\mathfrak{A},\mathfrak{B} \in \mathcal{R}^{(i)}[p,k,n] \quad \text{and} \quad \mathfrak{A},\mathfrak{B} \notin \mathcal{R}^{(i)}[p,k,n+1],$$

hence

$$\varrho^{(i)}[p,k](\mathfrak{A}) = \varrho^{(i)}[p,k](\mathfrak{B}) = n.$$

3° For every $n>0$ we have

$$\mathfrak{A},\mathfrak{B} \in \mathcal{R}^{(i)}[p,k,n],$$

hence

$$\varrho^{(i)}[p,k](\mathfrak{A}) = \varrho^{(i)}[p,k](\mathfrak{B}) = \infty.$$

Then either for some $n>0$ we have $\mathfrak{A},\mathfrak{B} \in \mathcal{K}[n]$, hence $\mathfrak{A}$ and $\mathfrak{B}$ are both of the first kind, or for every $n>0$ we have $\mathfrak{A},\mathfrak{B} \notin \mathcal{K}[n]$, hence $\mathfrak{A}$ and $\mathfrak{B}$ are both of the second kind.

Conversely, assume (I) and (II). By a procedure similar to that used above we obtain, for every prime p and for every integers $k,n>0$,

(1) $\qquad \mathfrak{A} \in \mathcal{R}^{(i)}[p,k,n]$ if and only if $\mathfrak{B} \in \mathcal{R}^{(i)}[p,k,n]$ $(i=1,2,3)$.

Now we distinguish two cases:

1° The groups $\mathfrak{A}$ and $\mathfrak{B}$ are both of the first kind. Using the form (39) for groups of the first kind together with formula (38) (in Chapter 1) we infer by means of Theorem 1.11 and condition (I) that for arbitrary $n>0$

$$n\mathfrak{A} = 3 \quad \text{if and only if} \quad n\mathfrak{B} = 3,$$

hence for arbitrary $n>0$

(2) $\qquad \mathfrak{A} \in \mathcal{K}[n]$ if and only if $\mathfrak{B} \in \mathcal{K}[n]$.

2° The groups $\mathfrak{A}$ and $\mathfrak{B}$ are both of the second kind; hence

$$\mathfrak{A},\mathfrak{B} \notin \mathcal{K}[n] \quad \text{for every} \quad n>0.$$

Thus in both cases condition (2) holds for every $n>0$, what together with (1) implies by means of Theorem 5.1 that $\mathfrak{A} \approx \mathfrak{B}$.

THEOREM 5.3 (Fundamental theorem on arithmetical types). *Let* Q *be the set of all triples*

$$\varphi = \langle \varphi^{(1)}, \varphi^{(2)}, \varphi^{(3)} \rangle$$

where $\varphi^{(1)},\varphi^{(2)},\varphi^{(3)} \in (\omega + \{\infty\})^{P \times N}$ *are functions which satisfy the condition*

(1) $\quad \varphi^{(i)}(p,k) = \varphi^{(i)}(p,k+1) + \varphi^{(3)}(p,k)$ *for every* $p \in \boldsymbol{P}$ *and* $k>0$ $(i=1,2)$;

and let

$$S^{(1)}_{\varphi} = \underset{\mathfrak{A} \in \mathcal{AG}_1}{E} \left(\varrho^{(i)}[p,k](\mathfrak{A}) = \varphi^{(i)}(p,k)\right) \quad \text{and} \quad S^{(2)}_{\varphi} = \underset{\mathfrak{A} \in \mathcal{AG}_2}{E} \left(\varrho^{(i)}[p,k](\mathfrak{A}) = \varphi^{(i)}(p,k)\right)$$

(equalities in parentheses should hold for every prime p*, for every integer* $k>0$ *and for* $i=1,2,3$*).*

The arithmetical types of Abelian groups are identical with the non-empty sets $S_\varphi^{(1)}$ and $S_\varphi^{(2)}$ for $\varphi \in Q$.

Remark. By Theorem 1.12 we have $S_\varphi^{(2)} \neq 0$ for every $\varphi \in Q$, and by Theorems 1.11 and 1.12 we have $S_\varphi^{(1)} \neq 0$ if and only if for $i=1,2,3$, $\varphi^{(i)}(p,k) \neq 0$ for at most finitely many couples $\langle p,k \rangle$.

Proof. Suppose that $S \in \boldsymbol{AT}(\mathcal{AG})$. By Definition 2.16 there is an algebra $\mathfrak{B} \in \mathcal{AG}$ such that

$$S = \boldsymbol{T}(\mathfrak{B}). \tag{2}$$

We define three functions $\varphi^{(1)}, \varphi^{(2)}, \varphi^{(3)}$ as follows:

$$\varphi^{(i)}(p,k) = \varrho^{(i)}[p,k](\mathfrak{B}) \quad \text{for every } p \in \boldsymbol{P} \text{ and } k>0 \quad (i=1,2,3).$$

Hence by Theorem 1.7 the condition (1) is satisfied.

It follows from (2) that, for an arbitrary Abelian group $\mathfrak{A}$,

$$\mathfrak{A} \in S \text{ if and only if } \mathfrak{A} \approx \mathfrak{B}.$$

Hence by Theorem 5.2

$$S = S_\varphi^{(1)} \text{ in case } \mathfrak{B} \in \mathcal{AG}_1 \text{ and } S = S_\varphi^{(2)} \text{ in case } \mathfrak{B} \in \mathcal{AG}_2.$$

The proof in the opposite direction is similar.

Thus we have a complete description of all arithmetical types of Abelian groups. It remains to characterize those arithmetical types which are at the same time arithmetical classes.

THEOREM 5.4. *For every group $\mathfrak{A} \in \mathcal{AG}$*

$$T(\mathfrak{A}) \in \boldsymbol{AC} \text{ if and only if } \mathfrak{A} \text{ is finite.}$$

Proof. It is known from the general theory of arithmetical classes [17]) that $\boldsymbol{T}(\mathfrak{A}) \in \boldsymbol{AC}$ whenever $\mathfrak{A}$ is a finite Abelian group. It remains to prove that $\boldsymbol{T}(\mathfrak{A}) \notin \boldsymbol{AC}$ whenever $\mathfrak{A}$ is an infinite Abelian group.

Assume — on the contrary — that there exists an infinite Abelian group $\mathfrak{A}$ such that

$$\boldsymbol{T}(\mathfrak{A}) \in \boldsymbol{AC}. \tag{1}$$

Therefore by 4.22 we have $\boldsymbol{T}(\mathfrak{A}) = \bigcup_{i<r} S_i$ for some $r>0$, where each S_i is an intersection of basic arithmetical classes and complements of basic arithmetical classes. It is clear that

$$\mathfrak{A} \in S_d \tag{2}$$

[17]) See [12], p. 713, remark following Theorem 26.

for some d, $0 \leqslant d < r$. Now

$$S_d = \bigcap_{i<s} T_i \tag{3}$$

where $s>0$ and each T_i is a basic arithmetical class or the complement of a basic arithmetical class.

Let us consider first the case when

$$T_i \neq \mathcal{K}[m] \quad \text{for } i=0,1,\ldots,s-1 \text{ and for every } m>0. \tag{4}$$

There is, of course, a prime q such that for every $k,n>0$

$$T_i \neq \mathcal{R}^{(j)}[q,k,n] \quad \text{and} \quad T_i \neq \overline{\mathcal{R}}^{(j)}[q,k,n] \qquad (i=0,1,\ldots,s-1;\ j=1,2,3)$$

and for every $m>0$

$$T_i = \overline{\mathcal{K}}[qm] \qquad (i=0,1,\ldots,s-1).$$

Now we define three functions $\varphi^{(1)}, \varphi^{(2)}, \varphi^{(3)}$ as follows:

$$\varphi^{(i)}(p,k) = \varrho^{(i)}[p,k](\mathfrak{A}) \quad \text{whenever } p \neq q \text{ or } k>1 \qquad (i=1,2,3),$$

$$\varphi^{(3)}(q,1) = \begin{cases} 0 & \text{whenever } \varrho^{(3)}[q,1](\mathfrak{A}) = \infty \\ \varrho^{(3)}[q,1](\mathfrak{A}) + 1 & \text{otherwise,} \end{cases}$$

$$\varphi^{(i)}(q,1) = \begin{cases} \varphi^{(i)}(q,2) & \text{whenever } \varphi^{(3)}(q,1) = 0 \\ \varrho^{(i)}[q,1](\mathfrak{A}) + 1 & \text{otherwise} \end{cases} \qquad (i=1,2).$$

We can easily check that

$$\varphi^{(i)}(p,k) = \varphi^{(i)}(p,k+1) + \varphi^{(3)}(p,k) \quad \text{for } p \in \boldsymbol{P} \text{ and } k>0 \quad (i=1,2) \tag{5}$$

hence from 1.12 we obtain the existence of a group $\mathfrak{B} \in \mathcal{AG}$ such that

$$\varrho^{(i)}[p,k](\mathfrak{B}) = \varphi^{(i)}(p,k) \quad \text{for } p \in \boldsymbol{P} \text{ and } k>0 \quad (i=1,2,3). \tag{6}$$

But the way in which the prime q has been chosen guarantees that

$$\mathfrak{B} \in S_d \tag{7}$$

which implies

$$\mathfrak{B} \in \boldsymbol{T}(\mathfrak{A}); \tag{8}$$

on the other hand $\varrho^{(3)}[q,1](\mathfrak{B}) \neq \varrho^{(3)}[q,1](\mathfrak{A})$, therefore it follows from Theorem 5.2 that $\mathfrak{B}$ non $\approx \mathfrak{A}$, which contradicts (8). Hence our assumption (4) proves to be false, and therefore for some $e<s$ and for some $m>0$

$$T_e = \mathcal{K}[m].$$

Let $m = \prod_{i<t} q_i^{k_i}$ $(k_i>0)$ be a decomposition of m into prime factors. From (2) and (3) we obtain now that $m\mathfrak{A} = \mathfrak{Z}$, and since $\mathfrak{A}$ is infinite we have

$$\varrho^{(3)}[q_h,l](\mathfrak{A}) = \infty$$

for some h and l such that $0 \leqslant h < t$ and $0 < l \leqslant k_h$ (see formulas (38) and (39) from Chapter 1). Put $q_h = q$. It is clear that there is an integer $u > 0$ such that

$$T_i = \mathcal{R}^{(3)}[q,l,n] \quad \text{implies} \quad n \leqslant u \qquad (i = 0,1,\ldots,s-1),$$

$$T_i = \mathcal{R}^{(j)}[q,k,n] \quad \text{implies} \quad n \leqslant u \quad (i = 0,1,\ldots,s-1,\ k = 1,2,\ldots,l,\ j = 1,2).$$

Now we define three functions $\varphi^{(1)}, \varphi^{(2)}, \varphi^{(3)}$ in the following manner:

$$\varphi^{(i)}(p,k) = \varrho^{(i)}[p,k](\mathfrak{N}) \quad \text{whenever} \quad p \neq q \quad \text{or} \quad k > l \qquad (i = 1,2,3),$$

$$\varphi^{(3)}(q,k) = \begin{cases} u & \text{for} \quad k = l \\ \varrho^{(3)}[q,k](\mathfrak{N}) & \text{for} \quad k < l \end{cases}$$

$$\varphi^{(i)}(q,k) = \varphi^{(i)}(q,l+1) + \sum_{k \leqslant j \leqslant l} \varphi^{(3)}(q,j) \quad \text{for} \quad k \leqslant l \qquad (i = 1,2).$$

Again we can easily check that condition (5) holds; hence there is a group $\mathfrak{B} \in \mathcal{AG}$ which satisfies (6). Furthermore, we have (7) and (8), but

$$\varrho^{(3)}[q,l](\mathfrak{B}) \neq \varrho^{(3)}[q,l](\mathfrak{N}),$$

thus we again get a contradiction. Hence our assumption (1) proves to be wrong and therefore $\boldsymbol{T}(\mathfrak{N}) \notin \boldsymbol{AC}$, which completes the proof.

Chapter 6. Applications

By means of the results obtained in Chapters 4 and 5, which concern exclusively the class $\mathcal{AG}$ of Abelian groups, we are able to solve some problems concerning not only the class $\mathcal{AG}$ but also the class $\mathcal{G}$ of all groups and the class $\mathcal{A}$ of all algebras with one binary operation. We shall also mention some known results whenever they can now be obtained by essentially simpler proofs. The problems which we have in mind consist in stating whether certain important classes of algebras are arithmetical, or at least arithmetically closed.

We start with the following preliminary

THEOREM 6.1. *If a class $S \in \boldsymbol{AC}(\mathcal{AG})$ is such that for every integer $n > 0$ there is a prime $p > n$ such that S contains a group $\mathfrak{A}$ of order p, then S contains also the (additive) group $\mathfrak{R}$ of rational numbers.*

Proof. To begin with let us observe that the class S contains, together with an algebra $\mathfrak{A}$, all algebras isomorphic to $\mathfrak{A}$ (since $\mathfrak{A} \cong \mathfrak{B}$ implies $\mathfrak{A} \approx \mathfrak{B}$ [18])); hence

(1) *for every $n > 0$ there is a prime $p > n$ such that $\mathfrak{C}_{p1} \in S$.*

[18]) See [12], p. 712, Theorem 22 (i).

Then by theorem 4.22 we have for a certain integer $r > 0$

$$S = \bigcup_{i<r} S_i,$$

where each S_i is an intersection of basic arithmetical classes and complements of basic arithmetical classes. Since S is a finite union of S, therefore, by (1), there must be an integer d, $0 \leqslant d < r$, such that

(2) *for every $n > 0$ there is a prime $p > n$ such that $\mathfrak{C}_{p1} \in S_d$.*

The class S_d is an intersection: $S_d = \bigcap_{i<s} T_i$, where $s > 0$ and each T_i is a basic arithmetical class or the complement of a basic arithmetical class. Consider an arbitrary class T_i $(i = 0,1,\ldots,s-1)$. Since $S_d \subseteq T_i$, it follows from (2) that

for every $n > 0$ there is a prime $p > n$ such that $\mathfrak{C}_{p1} \in T_i$.

Hence

$$T_i \neq \mathcal{K}[m] \quad \text{for every} \quad m > 0,$$

$$T_i \neq \mathcal{R}^{(j)}[p,k,n] \quad \text{for} \quad p \in \boldsymbol{P} \quad \text{and} \quad k,n > 0 \qquad (j = 1,2,3)$$

(see Theorem 1.9) and therefore each T_i is the complement of a basic arithmetical class. Thus, it is easy to see that $\mathfrak{R} \in T_i$ for $i = 0,1,\ldots,s-1$, hence $\mathfrak{R} \in S_d$, which implies that $\mathfrak{R} \in S$.

From Theorem 6.1 we derive at once many interesting consequences:

COROLLARY 6.2. *The following two classes of algebras are not ariht-metical:*

1. *The class $\mathcal{AG} \cap \mathcal{F}$ of all finite Abelian groups.*
2. *The class $\mathcal{AG} \cap \mathcal{S}$ of all simple Abelian groups.*

(Recall that the only simple Abelian groups are those of prime orders.)

Corollary 6.2 is also an immediate conclusion from a general law (of the theory of arithmetical classes) which gives a necessary (and sufficient) condition for a class of finite algebras to be arithmetical [19]). But the proof of this law is based essentially on the *compactness theorem* for arithmetical classes [20]), while by means of the Fundamental theorem on arithmetical classes of Abelian groups we have obtained Corollary 6.2 using only finitary methods.

Since the class $\mathcal{AG}$ is arithmetical, Corollary 6.2 can be generalized to

[19]) See [12], p. 711, Theorem 20 (i).
[20]) See [12], p. 711, Theorems 17-19, and [5].

COROLLARY 6.3. *For an arbitrary class $T \subseteq \mathcal{A}$, if $\mathcal{AG} \subseteq T$, then the class $T \cap \mathcal{F}$ of all finite algebras in T and the class $T \cap \mathcal{S}$ of all simple algebras in T are not arithmetical.*

In particular the following classes of algebras are not arithmetical:

1. *The class $\mathcal{G} \cap \mathcal{F}$ of all finite groups.*
2. *The class $\mathcal{F}$ of all finite algebras in $\mathcal{A}$.*
3. *The class $\mathcal{G} \cap \mathcal{S}$ of all simple groups.*
4. *The class $\mathcal{S}$ of all simple algebras in $\mathcal{A}$.*

The first two statements concerning the classes $\mathcal{G} \cap \mathcal{F}$ and $\mathcal{F}$ can be derived also from the general law mentioned above [19]).

To complete the discussion let us observe that $\mathcal{F}$ is in $\boldsymbol{AC}_\sigma$, hence also the classes $\mathcal{AG} \cap \mathcal{F}$ and $\mathcal{G} \cap \mathcal{F}$. Thus the classes $\mathcal{AG} \cap \mathcal{F}$, $\mathcal{G} \cap \mathcal{F}$, and $\mathcal{F}$ are arithmetically closed. Then we have

$$\mathcal{AG} \cap \mathcal{S} = \bigcup_{p \in P} (\mathcal{AG} \cap \mathcal{A}_p),$$

therefore the class $\mathcal{AG} \cap \mathcal{S}$ is in $\boldsymbol{AC}_\sigma$ and hence the class $\mathcal{AG} \cap \mathcal{S}$ is arithmetically closed [21]).

COROLLARY 6.4. *The class of all torsion-free (i. e., without elements of finite order) Abelian groups is not arithmetical.*

In fact, if the class of all torsion-free Abelian groups were arithmetical, then also its complement to $\mathcal{AG}$ would be arithmetical which is impossible by Theorem 6.1.

From Corollary 6.4 we immediately obtain

COROLLARY 6.5. *The class of all torsion-free groups is not arithmetical.*

To complete the discussion let us observe that the class of all torsion-free groups (therefore also the class of all torsion-free Abelian groups) is in $\boldsymbol{AC}_\delta$, hence it is arithmetically closed. In fact, for arbitrary $n > 0$, let

$$S_n = \underset{\mathfrak{A} \in \mathcal{AG}}{E} (\textit{for every } x \in \mathfrak{A}_0,\ nx = 0 \textit{ implies } x = 0).$$

Of course every class S_n is arithmetical and the class of all torsion-free groups is identical with the intersection $\bigcap_{n \in \omega} S_{n+1}$.

Now we are going to give some examples of classes which are not arithmetically closed.

We start with the following preliminary

THEOREM 6.6. *For every group $\mathfrak{A} \in \mathcal{AG}$*

$$\textit{if } \mathfrak{A} \in \mathcal{AG}_2, \textit{ then } \mathfrak{A} \approx \mathfrak{A} \times \mathfrak{R}.$$

[21]) The class $\mathcal{G} \cap \mathcal{S}$ (and therefore also the class $\mathcal{S}$) is not arithmetically closed. See [12], p. 717, footnote 17.

Proof. In fact, by Theorems 1.9 and 1.10, for every prime p and or every integer $k > 0$

$$\varrho^{(i)}[p,k](\mathfrak{A}) = \varrho^{(i)}[p,k](\mathfrak{A} \times \mathfrak{R}) \qquad (i = 1,2,3);$$

furthermore, the group $\mathfrak{A} \times \mathfrak{R}$ is always of the second kind. Hence it follows from Theorem 5.2 that $\mathfrak{A} \approx \mathfrak{A} \times \mathfrak{R}$.

From Theorem 6.6 we derive at once many interesting consequences:

COROLLARY 6.7. *The following classes of algebras are not arithmetically closed:*

1. *The class $\mathcal{AG} \cap \mathcal{J}$ of all indecomposable Abelian groups.*
2. *The class $\mathcal{AG} \cap \mathcal{A}^{(n)}$ of all Abelian groups with n generators (for arbitrary $n > 0$).*

Remark. Notice that $\mathcal{AG} \cap \mathcal{A}^{(1)}$ is identical with the class of all cyclic groups.

Since the class $\mathcal{AG}$ is arithmetical, Corollary 6.7 can be generalized to

COROLLARY 6.8. *For an arbitrary class $T \subseteq \mathcal{A}$, if $\mathcal{AG} \subseteq T$, then the class $T \cap \mathcal{J}$ of all indecomposable algebras in T and the class $T \cap \mathcal{A}^{(n)}$ of all algebras with n generators in T are not arithmetically closed. In particular, the following classes of algebras are not arithmetically closed:*

1. *The class $\mathcal{G} \cap \mathcal{J}$ of all indecomposable groups.*
2. *The class $\mathcal{J}$ of all indecomposable algebras in $\mathcal{A}$.*
3. *The class $\mathcal{G} \cap \mathcal{A}^{(n)}$ of all groups with n generators.*
4. *The class $\mathcal{A}^{(n)}$ of all algebras with n generators in $\mathcal{A}$.*

COROLLARY 6.9. *The class of all torsion (i. e., with each element of finite order) Abelian groups is not arithmetically closed.*

From Corollary 6.8 we immediately obtain

COROLLARY 6.10. *The class of all torsion groups is not arithmetically closed.*

It should be observed that all the results of this section which involve $\mathcal{A}$ can be extended to the class of all algebras in which at least one operation has the rank not less than two.

The concluding remarks will be devoted to the discussion of the meta-mathematical aspect of our work. As was pointed out in the introduction, the original aim of our study was to establish a decision procedure for the elementary theory of Abelian groups. The aim has actually been achieved, also — owing to the mathematical form which we have chosen to present our results — this point has not been, perhaps, made entirely clear to the reader and requires some explanation. As is well known, the decision procedure for a mathematical theory is a method which permits us to decide in each particular case whether or not a given sentence (formulated in the language of the theory) can

be derived from the axioms. In application to the elementary theory of Abelian groups this procedure can be described as follows: We choose certain special sentences which are denoted by $\Phi^{(i)}[p,k,n]$ $(i=1,2,3)$ and $\Psi[n]$. Each of these sentences expresses the fact that the Abelian group under discussion belongs to the corresponding basic arithmetical class $\mathcal{R}^{(i)}[p,k,n]$ and $\mathcal{K}[n]$ (see Definitions 3.2, 3,3, and the Remark following Theorem 3.7); the sentences $\Phi^{(i)}[p,k,n]$ and $\Psi[n]$ (for any particular values of p,k,n) are expressed in the language of the elementary theory of Abelian groups. These sentences and their negations are referred to as *basic sentences*, a sentence which is a disjunction of conjunctions of basic sentences is said to be of *normal form*. Given now an arbitrary sentence Σ of the elementary theory of Abelian groups, we can construct a sentence Σ' of normal form which is provably equivalent to Σ (in the sense that the sentence stating the equivalence of Σ and Σ' is derivable from the axioms). The existence of such a sentence Σ' is an immediate consequence of the Fundamental theorem on arithmetical classes in its meta-mathematical interpretation; and the proof of this theorem and of the theorems and lemmata upon which it is based provides a method of constructing Σ'. Thus the problem is reduced to finding a decision procedure for sentences of normal form. This meta-mathematical problem is equivalent to the mathematical problem of finding a necessary and sufficient condition for a union of intersections of basic arithmetical classes to be identical with the class $\mathcal{AG}$; the remarks at the end of Chapter 4 give, we hope, an adequate idea how this can be carried through.

The results obtained in this work have also some further meta-mathematical implications. The elementary theory of Abelian groups is clearly incomplete, *i. e.*, there are sentences Σ formulated in the language of this theory such that neither Σ nor the negation of Σ is derivable from the axioms of the theory. Hence the problem arises how the axiom system can be extended so as to form a basis for a complete and consistent theory (without changing the logical framework or introducing new undefined constants). This meta-mathematical problem is essentially equivalent to the mathematical problem of describing all arithmetical types of Abelian groups, and hence the Fundamental theorem on arithmetical types provides a full solution of the problem. We see from this theorem that there are continuously many ways of extending the elementary theory of Abelian groups to a complete and consistent theory. In contrast to the original theory, however, most of those extensions are based upon infinite axiom systems. Theorem 5.4 implies that the only complete and consistent extensions which are finitely axiomatizable are those whose models are finite Abelian groups.

References

[1] Alexandroff, P. and Hopf, H., *Topologie*, vol. 1, Berlin 1935.

[2] Hilbert, D., and Bernays, P., *Grundlagen der Mathematik*, vol. 1, Berlin 1934; vol. 2, Berlin 1939.

[3] Курош, А. Г., *Теория групп*, Издание второе, Москва 1953.

[4] Presburger, M., *Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt*, Sprawozdanie z I Kongresu Matematyków Krajów Słowiańskich (Comptes-rendus du 1er Congrès des Mathématiciens des Pays Slaves), Warszawa 1930, p. 92-101.

[5] Rasiowa, H., *A proof of the compactness theorem for arithmetical classes*, Fundamenta Mathematicae 39 (1952), p. 8-14.

[6] Szmielew, W., *Decision problem in group theory*, Proceedings of the Xth International Congress of Philosophy, vol. 1, fascicule 2, Amsterdam 1949, p. 763-766.

[7] — *Arithmetical classes and types of Abelian groups*, Bulletin of the American Mathematical Society 55 (1949), p. 65.

[8] Tarski, A., *A decision method for elementary algebra and geometry*, Santa Monica 1948.

[9] — *Arithmetical classes and types of mathematical systems*, Bulletin of the American Mathematical Society 55 (1949), p. 63.

[10] — *Grundzüge des Systemenkalküls. I*, Fundamenta Mathematicae 25 (1935), p. 503-526; *II*, Fundamenta Mathematicae 26 (1936), p. 283-301.

[11] — *Metamathematical aspect of arithmetical classes and types*, Bulletin of the American Mathematical Society 55 (1949), p. 63-64.

[12] — *Some notions and methods on the borderline of algebra and metamathematics*, Proceedings of the International Congress of Mathematicians, vol. 1, Cambridge (USA) 1950, p. 705-720.

[13] — *Undecidability of group theory*, The Journal of Symbolic Logic 14 (1949), p. 76.

[14] van der Waerden, B. L., *Moderne Algebra*, vol. 1, second edition, Berlin 1937.

Reçu par la Rédaction le 17. 1. 1954